Annotated Ada Reference Manual


Copyright © 2000  The MITRE Corporation, Inc.

Copyright © 2004, 2005, 2006  AXE Consultants

Copyright © 2004, 2005, 2006  Ada-Europe

EXEMPLARY, OR SPECIAL DAMAGES, EVEN IF ADA-EUROPE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
# Table of Contents

Table of Contents............................................................................................................i

Foreword .........................................................................................................................xiii

Introduction .....................................................................................................................xv

1 General .........................................................................................................................1
   1.1 Scope .......................................................................................................................3
      1.1.1 Extent ...............................................................................................................3
      1.1.2 Structure .........................................................................................................4
      1.1.3 Conformity of an Implementation ..................................................................12
      1.1.4 Method of Description and Syntax Notation ................................................16
      1.1.5 Classification of Errors ..................................................................................18
   1.2 Normative References ............................................................................................20
      1.2.1 Bibliography ..................................................................................................21
   1.3 Terms and Definitions ..........................................................................................22
      1.3.1 Types, Objects, and their Properties ...............................................................23
      1.3.2 Subprograms and their Properties ................................................................26
      1.3.3 Other Syntactic Constructs ..........................................................................27
      1.3.4 Runtime Actions ............................................................................................29
      1.3.5 Exceptional Situations ...................................................................................29
   1.4 Scope of the Normative References ......................................................................29
   1.5 Normative References ..........................................................................................31

2 Lexical Elements .........................................................................................................31
   2.1 Character Set .........................................................................................................31
   2.2 Lexical Elements, Separators, and Delimiters .......................................................37
   2.3 Identifiers ..............................................................................................................38
   2.4 Numeric Literals ....................................................................................................41
      2.4.1 Decimal Literals ..............................................................................................41
      2.4.2 Based Literals .................................................................................................42
   2.5 Character Literals ..................................................................................................43
   2.6 String Literals ........................................................................................................43
   2.7 Comments ............................................................................................................44
   2.8 Pragmas ................................................................................................................49

3 Declarations and Types .............................................................................................53
   3.1 Declarations ..........................................................................................................53
   3.2 Types and Subtypes ..............................................................................................56
      3.2.1 Type Declarations ..........................................................................................61
      3.2.2 Subtype Declarations ....................................................................................63
      3.2.3 Classification of Operations .........................................................................64
      3.2.4 Subtype Predicates .......................................................................................65
   3.3 Objects and Named Numbers ..............................................................................71
      3.3.1 Object Declarations ......................................................................................75
      3.3.2 Number Declarations ....................................................................................80
   3.4 Derived Types and Classes ..................................................................................82
      3.4.1 Derivation Classes .......................................................................................88
   3.5 Scalar Types .........................................................................................................90
      3.5.1 Enumeration Types .....................................................................................100
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5.4 Unary Adding Operators</td>
<td>267</td>
</tr>
<tr>
<td>4.5.5 Multiplying Operators</td>
<td>267</td>
</tr>
<tr>
<td>4.5.6 Highest Precedence Operators</td>
<td>271</td>
</tr>
<tr>
<td>4.5.7 Conditional Expressions</td>
<td>272</td>
</tr>
<tr>
<td>4.5.8 Quantified Expressions</td>
<td>275</td>
</tr>
<tr>
<td>4.5.9 Declare Expressions</td>
<td>276</td>
</tr>
<tr>
<td>4.5.10 Reduction Expressions</td>
<td>278</td>
</tr>
<tr>
<td>4.6 Type Conversions</td>
<td>282</td>
</tr>
<tr>
<td>4.7 Qualified Expressions</td>
<td>293</td>
</tr>
<tr>
<td>4.8 Allocators</td>
<td>295</td>
</tr>
<tr>
<td>4.9 Static Expressions and Static Subtypes</td>
<td>300</td>
</tr>
<tr>
<td>4.9.1 Statically Matching Constraints and Subtypes</td>
<td>308</td>
</tr>
<tr>
<td>4.10 Image Attributes</td>
<td>310</td>
</tr>
<tr>
<td>5 Statements</td>
<td>317</td>
</tr>
<tr>
<td>5.1 Simple and Compound Statements - Sequences of Statements</td>
<td>317</td>
</tr>
<tr>
<td>5.2 Assignment Statements</td>
<td>320</td>
</tr>
<tr>
<td>5.2.1 Target Name Symbols</td>
<td>323</td>
</tr>
<tr>
<td>5.3 If Statements</td>
<td>324</td>
</tr>
<tr>
<td>5.4 Case Statements</td>
<td>325</td>
</tr>
<tr>
<td>5.5 Loop Statements</td>
<td>328</td>
</tr>
<tr>
<td>5.5.1 User-Defined Iterator Types</td>
<td>332</td>
</tr>
<tr>
<td>5.5.2 Generalized Loop Iteration</td>
<td>335</td>
</tr>
<tr>
<td>5.5.3 Procedural Iterators</td>
<td>340</td>
</tr>
<tr>
<td>5.6 Block Statements</td>
<td>344</td>
</tr>
<tr>
<td>5.6.1 Parallel Block Statements</td>
<td>345</td>
</tr>
<tr>
<td>5.7 Exit Statements</td>
<td>347</td>
</tr>
<tr>
<td>5.8 Goto Statements</td>
<td>348</td>
</tr>
<tr>
<td>6 Subprograms</td>
<td>351</td>
</tr>
<tr>
<td>6.1 Subprogram Declarations</td>
<td>351</td>
</tr>
<tr>
<td>6.1.1 Preconditions and Postconditions</td>
<td>355</td>
</tr>
<tr>
<td>6.1.2 The Global and Global'Class Aspects</td>
<td>367</td>
</tr>
<tr>
<td>6.2 Formal Parameter Modes</td>
<td>370</td>
</tr>
<tr>
<td>6.3 Subprogram Bodies</td>
<td>373</td>
</tr>
<tr>
<td>6.3.1 Conformance Rules</td>
<td>375</td>
</tr>
<tr>
<td>6.3.2 Inline Expansion of Subprograms</td>
<td>380</td>
</tr>
<tr>
<td>6.4 Subprogram Calls</td>
<td>381</td>
</tr>
<tr>
<td>6.4.1 Parameter Associations</td>
<td>384</td>
</tr>
<tr>
<td>6.5 Return Statements</td>
<td>392</td>
</tr>
<tr>
<td>6.5.1 Nonreturning Subprograms</td>
<td>401</td>
</tr>
<tr>
<td>6.6 Overloading of Operators</td>
<td>403</td>
</tr>
<tr>
<td>6.7 Null Procedures</td>
<td>404</td>
</tr>
<tr>
<td>6.8 Expression Functions</td>
<td>405</td>
</tr>
<tr>
<td>7 Packages</td>
<td>409</td>
</tr>
<tr>
<td>7.1 Package Specifications and Declarations</td>
<td>409</td>
</tr>
<tr>
<td>7.2 Package Bodies</td>
<td>411</td>
</tr>
<tr>
<td>7.3 Private Types and Private Extensions</td>
<td>412</td>
</tr>
<tr>
<td>7.3.1 Private Operations</td>
<td>419</td>
</tr>
<tr>
<td>7.3.2 Type Invariants</td>
<td>424</td>
</tr>
</tbody>
</table>
7.3.3 Default Initial Conditions ................................................................. 431
7.3.4 Stable Properties of a Type ................................................................. 433
7.4 Deferred Constants ............................................................................ 436
7.5 Limited Types .................................................................................... 438
7.6 Assignment and Finalization ............................................................... 443
    7.6.1 Completion and Finalization ......................................................... 450
8  Visibility Rules ...................................................................................... 461
    8.1 Declarative Region ........................................................................... 461
    8.2 Scope of Declarations ..................................................................... 463
    8.3 Visibility ......................................................................................... 466
        8.3.1 Overriding Indicators .............................................................. 474
    8.4 Use Clauses .................................................................................... 475
    8.5 Renaming Declarations ................................................................. 478
        8.5.1 Object Renaming Declarations ............................................... 478
        8.5.2 Exception Renaming Declarations .......................................... 482
        8.5.3 Package Renaming Declarations ............................................ 483
        8.5.4 Subprogram Renaming Declarations ..................................... 484
        8.5.5 Generic Renaming Declarations ............................................ 488
    8.6 The Context of Overload Resolution .............................................. 489
9  Tasks and Synchronization ................................................................. 497
    9.1 Task Units and Task Objects .......................................................... 498
    9.2 Task Execution - Task Activation .................................................. 502
    9.3 Task Dependence - Termination of Tasks ...................................... 504
    9.4 Protected Units and Protected Objects ......................................... 505
    9.5 Intertask Communication .............................................................. 511
        9.5.1 Protected Subprograms and Protected Actions .................... 519
        9.5.2 Entries and Accept Statements ............................................. 522
        9.5.3 Entry Calls ........................................................................... 527
        9.5.4 Requeue Statements ............................................................ 531
    9.6 Delay Statements, Duration, and Time ......................................... 534
        9.6.1 Formatting, Time Zones, and other operations for Time ........ 538
    9.7 Select Statements ........................................................................... 546
        9.7.1 Selective Accept ................................................................. 546
        9.7.2 Timed Entry Calls ............................................................... 548
        9.7.3 Conditional Entry Calls ....................................................... 550
        9.7.4 Asynchronous Transfer of Control ....................................... 551
    9.8 Abort of a Task - Abort of a Sequence of Statements .................. 552
    9.9 Task and Entry Attributes ............................................................ 555
    9.10 Shared Variables ......................................................................... 555
        9.10.1 Conflict Check Policies ....................................................... 558
    9.11 Example of Tasking and Synchronization .................................... 561
10 Program Structure and Compilation Issues ....................................... 563
    10.1 Separate Compilation ................................................................. 563
        10.1.1 Compilation Units - Library Units ....................................... 564
        10.1.2 Context Clauses - With Clauses ......................................... 571
        10.1.3 Subunits of Compilation Units ............................................. 576
        10.1.4 The Compilation Process ................................................... 579
        10.1.5 Pragmas and Program Units ............................................... 581
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.6 Environment-Level Visibility Rules</td>
<td>583</td>
</tr>
<tr>
<td>10.2 Program Execution</td>
<td>585</td>
</tr>
<tr>
<td>10.2.1 Elaboration Control</td>
<td>590</td>
</tr>
<tr>
<td>11 Exceptions</td>
<td>601</td>
</tr>
<tr>
<td>11.1 Exception Declarations</td>
<td>601</td>
</tr>
<tr>
<td>11.2 Exception Handlers</td>
<td>602</td>
</tr>
<tr>
<td>11.3 Raise Statements and Raise Expressions</td>
<td>604</td>
</tr>
<tr>
<td>11.4 Exception Handling</td>
<td>606</td>
</tr>
<tr>
<td>11.4.1 The Package Exceptions</td>
<td>607</td>
</tr>
<tr>
<td>11.4.2 Pragmas Assert and Assertion_Policy</td>
<td>613</td>
</tr>
<tr>
<td>11.4.3 Example of Exception Handling</td>
<td>617</td>
</tr>
<tr>
<td>11.5 Suppressing Checks</td>
<td>618</td>
</tr>
<tr>
<td>11.6 Exceptions and Optimization</td>
<td>624</td>
</tr>
<tr>
<td>12 Generic Units</td>
<td>627</td>
</tr>
<tr>
<td>12.1 Generic Declarations</td>
<td>627</td>
</tr>
<tr>
<td>12.2 Generic Bodies</td>
<td>629</td>
</tr>
<tr>
<td>12.3 Generic Instantiation</td>
<td>630</td>
</tr>
<tr>
<td>12.4 Formal Objects</td>
<td>639</td>
</tr>
<tr>
<td>12.5 Formal Types</td>
<td>641</td>
</tr>
<tr>
<td>12.5.1 Formal Private and Derived Types</td>
<td>645</td>
</tr>
<tr>
<td>12.5.2 Formal Scalar Types</td>
<td>651</td>
</tr>
<tr>
<td>12.5.3 Formal Array Types</td>
<td>651</td>
</tr>
<tr>
<td>12.5.4 Formal Access Types</td>
<td>652</td>
</tr>
<tr>
<td>12.5.5 Formal Interface Types</td>
<td>654</td>
</tr>
<tr>
<td>12.6 Formal Subprograms</td>
<td>654</td>
</tr>
<tr>
<td>12.7 Formal Packages</td>
<td>659</td>
</tr>
<tr>
<td>12.8 Example of a Generic Package</td>
<td>663</td>
</tr>
<tr>
<td>13 Representation Issues</td>
<td>665</td>
</tr>
<tr>
<td>13.1 Operational and Representation Aspects</td>
<td>665</td>
</tr>
<tr>
<td>13.1.1 Aspect Specifications</td>
<td>680</td>
</tr>
<tr>
<td>13.2 Packed Types</td>
<td>687</td>
</tr>
<tr>
<td>13.3 Operational and Representation Attributes</td>
<td>689</td>
</tr>
<tr>
<td>13.4 Enumeration Representation Clauses</td>
<td>707</td>
</tr>
<tr>
<td>13.5 Record Layout</td>
<td>709</td>
</tr>
<tr>
<td>13.5.1 Record Representation Clauses</td>
<td>709</td>
</tr>
<tr>
<td>13.5.2 Storage Place Attributes</td>
<td>713</td>
</tr>
<tr>
<td>13.5.3 Bit Ordering</td>
<td>715</td>
</tr>
<tr>
<td>13.6 Change of Representation</td>
<td>716</td>
</tr>
<tr>
<td>13.7 The Package System</td>
<td>716</td>
</tr>
<tr>
<td>13.7.1 The Package System.Storage.Elements</td>
<td>720</td>
</tr>
<tr>
<td>13.7.2 The Package System.Address.To_Access.Conversions</td>
<td>721</td>
</tr>
<tr>
<td>13.8 Machine Code Insertions</td>
<td>722</td>
</tr>
<tr>
<td>13.9 Unchecked Type Conversions</td>
<td>724</td>
</tr>
<tr>
<td>13.9.1 Data Validity</td>
<td>726</td>
</tr>
<tr>
<td>13.9.2 The Valid Attribute</td>
<td>729</td>
</tr>
<tr>
<td>13.10 Unchecked Access Value Creation</td>
<td>730</td>
</tr>
<tr>
<td>13.11 Storage Management</td>
<td>731</td>
</tr>
<tr>
<td>13.11.1 Storage Allocation Attributes</td>
<td>738</td>
</tr>
</tbody>
</table>
### Table of Contents

**Annex A**

- **The Standard Libraries** ........................................................................................................ 785
- **Annex A (normative) Predefined Language Environment** .................................................. 787
  - A.1 The Package Standard ..................................................................................................... 791
  - A.2 The Package Ada ........................................................................................................... 797
  - A.3 Character Handling ....................................................................................................... 797
    - A.3.1 The Packages Characters, Wide_Characters, and Wide_Wide_Characters ........ 798
    - A.3.2 The Package Characters.Handling ..................................................................... 799
    - A.3.3 The Package Characters.Latin_1 ....................................................................... 803
    - A.3.4 The Package Characters.Conversions ................................................................. 807
    - A.3.5 The Package Wide_Characters.Handling ............................................................ 809
    - A.3.6 The Package Wide_Wide_Characters.Handling .................................................. 813
  - A.4 String Handling .............................................................................................................. 813
    - A.4.1 The Package Strings ............................................................................................ 814
    - A.4.2 The Package Strings.Maps .................................................................................. 814
    - A.4.3 Fixed-Length String Handling ............................................................................. 817
    - A.4.4 Bounded-Length String Handling ....................................................................... 827
    - A.4.5 Unbounded-Length String Handling ................................................................... 835
    - A.4.6 String-Handling Sets and Mappings .................................................................... 841
    - A.4.7 Wide_String Handling ......................................................................................... 842
    - A.4.8 Wide_Wide_String Handling .............................................................................. 845
    - A.4.9 String Hashing ...................................................................................................... 848
    - A.4.10 String Comparison ............................................................................................ 850
    - A.4.11 String Encoding ................................................................................................. 851
    - A.4.12 Universal Text Buffers ..................................................................................... 857
  - A.5 The Numerics Packages ................................................................................................ 859
    - A.5.1 Elementary Functions .......................................................................................... 860
    - A.5.2 Random Number Generation .............................................................................. 864
    - A.5.3 Attributes of Floating Point Types ....................................................................... 871
    - A.5.4 Attributes of Fixed Point Types .......................................................................... 877
    - A.5.5 Big Numbers ....................................................................................................... 877
    - A.5.6 Big Integers ......................................................................................................... 878
    - A.5.7 Big Reals ............................................................................................................ 880
  - A.6 Input-Output .................................................................................................................... 882
  - A.7 External Files and File Objects .................................................................................... 883
  - A.8 Sequential and Direct Files .......................................................................................... 884
    - A.8.1 The Generic Package Sequential_IO ................................................................ 885
    - A.8.2 File Management ................................................................................................. 887
    - A.8.3 Sequential Input-Output Operations ................................................................... 890

---

**The Standard Libraries** ........................................................................................................ 785

**Annex A (normative) Predefined Language Environment** .................................................. 787

- **A.1 The Package Standard** ............................................................................................. 791
- **A.2 The Package Ada** ..................................................................................................... 797
- **A.3 Character Handling** ............................................................................................... 797
  - **A.3.1 The Packages Characters, Wide_Characters, and Wide_Wide_Characters** .... 798
  - **A.3.2 The Package Characters.Handling** .................................................................. 799
  - **A.3.3 The Package Characters.Latin_1** .................................................................. 803
  - **A.3.4 The Package Characters.Conversions** ............................................................. 807
  - **A.3.5 The Package Wide_Characters.Handling** ....................................................... 809
  - **A.3.6 The Package Wide_Wide_Characters.Handling** ............................................. 813
- **A.4 String Handling** ...................................................................................................... 813
  - **A.4.1 The Package Strings** ....................................................................................... 814
  - **A.4.2 The Package Strings.Maps** .............................................................................. 814
  - **A.4.3 Fixed-Length String Handling** ......................................................................... 817
  - **A.4.4 Bounded-Length String Handling** ................................................................... 827
  - **A.4.5 Unbounded-Length String Handling** ............................................................... 835
  - **A.4.6 String-Handling Sets and Mappings** ............................................................... 841
  - **A.4.7 Wide_String Handling** .................................................................................. 842
  - **A.4.8 Wide_Wide_String Handling** ........................................................................ 845
  - **A.4.9 String Hashing** ............................................................................................... 848
  - **A.4.10 String Comparison** ...................................................................................... 850
  - **A.4.11 String Encoding** ........................................................................................... 851
  - **A.4.12 Universal Text Buffers** .................................................................................. 857
- **A.5 The Numerics Packages** .......................................................................................... 859
  - **A.5.1 Elementary Functions** ..................................................................................... 860
  - **A.5.2 Random Number Generation** .......................................................................... 864
  - **A.5.3 Attributes of Floating Point Types** ................................................................ 871
  - **A.5.4 Attributes of Fixed Point Types** .................................................................... 877
  - **A.5.5 Big Numbers** .................................................................................................. 877
  - **A.5.6 Big Integers** .................................................................................................... 878
  - **A.5.7 Big Reals** ........................................................................................................ 880
- **A.6 Input-Output** ............................................................................................................ 882
- **A.7 External Files and File Objects** ............................................................................... 883
- **A.8 Sequential and Direct Files** .................................................................................... 884
  - **A.8.1 The Generic Package Sequential_IO** ............................................................ 885
  - **A.8.2 File Management** ........................................................................................... 887
  - **A.8.3 Sequential Input-Output Operations** ............................................................... 890
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>D.2.2 Task Dispatching Pragmas</td>
<td>1274</td>
</tr>
<tr>
<td>D.2.3 Preemptive Dispatching</td>
<td>1277</td>
</tr>
<tr>
<td>D.2.4 Non-Preemptive Dispatching</td>
<td>1278</td>
</tr>
<tr>
<td>D.2.5 Round Robin Dispatching</td>
<td>1280</td>
</tr>
<tr>
<td>D.2.6 Earliest Deadline First Dispatching</td>
<td>1282</td>
</tr>
<tr>
<td>D.3 Priority Ceiling Locking</td>
<td>1286</td>
</tr>
<tr>
<td>D.4 Entry Queuing Policies</td>
<td>1290</td>
</tr>
<tr>
<td>D.4.1 Admission Policies</td>
<td>1293</td>
</tr>
<tr>
<td>D.5 Dynamic Priorities</td>
<td>1294</td>
</tr>
<tr>
<td>D.5.1 Dynamic Priorities for Tasks</td>
<td>1294</td>
</tr>
<tr>
<td>D.5.2 Dynamic Priorities for Protected Objects</td>
<td>1297</td>
</tr>
<tr>
<td>D.6 Preemptive Abort</td>
<td>1298</td>
</tr>
<tr>
<td>D.7 Tasking Restrictions</td>
<td>1299</td>
</tr>
<tr>
<td>D.8 Monotonic Time</td>
<td>1304</td>
</tr>
<tr>
<td>D.9 Delay Accuracy</td>
<td>1308</td>
</tr>
<tr>
<td>D.10 Synchronous Task Control</td>
<td>1310</td>
</tr>
<tr>
<td>D.10.1 Synchronous Barriers</td>
<td>1311</td>
</tr>
<tr>
<td>D.11 Asynchronous Task Control</td>
<td>1312</td>
</tr>
<tr>
<td>D.12 Other Optimizations and Determinism Rules</td>
<td>1314</td>
</tr>
<tr>
<td>D.13 The Ravenscar and Jorvik Profiles</td>
<td>1315</td>
</tr>
<tr>
<td>D.14 Execution Time</td>
<td>1318</td>
</tr>
<tr>
<td>D.14.1 Execution Time Timers</td>
<td>1321</td>
</tr>
<tr>
<td>D.14.2 Group Execution Time Budgets</td>
<td>1323</td>
</tr>
<tr>
<td>D.14.3 Execution Time of Interrupt Handlers</td>
<td>1326</td>
</tr>
<tr>
<td>D.15 Timing Events</td>
<td>1326</td>
</tr>
<tr>
<td>D.16 Multiprocessor Implementation</td>
<td>1329</td>
</tr>
<tr>
<td>D.16.1 Multiprocessor Dispatching Domains</td>
<td>1331</td>
</tr>
<tr>
<td>E.1 Partitions</td>
<td>1335</td>
</tr>
<tr>
<td>E.2 Categorization of Library Units</td>
<td>1337</td>
</tr>
<tr>
<td>E.2.1 Shared Passive Library Units</td>
<td>1339</td>
</tr>
<tr>
<td>E.2.2 Remote Types Library Units</td>
<td>1341</td>
</tr>
<tr>
<td>E.2.3 Remote Call Interface Library Units</td>
<td>1344</td>
</tr>
<tr>
<td>E.3 Consistency of a Distributed System</td>
<td>1348</td>
</tr>
<tr>
<td>E.4 Remote Subprogram Calls</td>
<td>1349</td>
</tr>
<tr>
<td>E.4.1 Asynchronous Remote Calls</td>
<td>1352</td>
</tr>
<tr>
<td>E.4.2 Example of Use of a Remote Access-to-Class-Wide Type</td>
<td>1354</td>
</tr>
<tr>
<td>E.5 Partition Communication Subsystem</td>
<td>1355</td>
</tr>
<tr>
<td>F.1 Machine_Radix Attribute Definition Clause</td>
<td>1361</td>
</tr>
<tr>
<td>F.2 The Package Decimal</td>
<td>1362</td>
</tr>
<tr>
<td>F.3 Edited Output for Decimal Types</td>
<td>1363</td>
</tr>
<tr>
<td>F.3.1 Picture String Formation</td>
<td>1364</td>
</tr>
<tr>
<td>F.3.2 Edited Output Generation</td>
<td>1368</td>
</tr>
<tr>
<td>F.3.3 The Package Text_IO.Editing</td>
<td>1372</td>
</tr>
<tr>
<td>F.3.4 The Package Wide_Text_IO.Editing</td>
<td>1376</td>
</tr>
<tr>
<td>F.3.5 The Package Wide_Wide_Text_IO.Editing</td>
<td>1376</td>
</tr>
<tr>
<td>G.1 Numerics</td>
<td>1377</td>
</tr>
</tbody>
</table>
# Table of Contents

**Annex J**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>J.1</td>
<td>Renamings of Library Units</td>
<td>1443</td>
</tr>
<tr>
<td>J.2</td>
<td>Allowed Replacements of Characters</td>
<td>1444</td>
</tr>
<tr>
<td>J.3</td>
<td>Reduced Accuracy Subtypes</td>
<td>1444</td>
</tr>
<tr>
<td>J.4</td>
<td>The Constrained Attribute</td>
<td>1446</td>
</tr>
<tr>
<td>J.5</td>
<td>ASCII</td>
<td>1446</td>
</tr>
<tr>
<td>J.6</td>
<td>Numeric_Error</td>
<td>1447</td>
</tr>
<tr>
<td>J.7</td>
<td>At Clauses</td>
<td>1447</td>
</tr>
<tr>
<td>J.7.1</td>
<td>Interrupt Entries</td>
<td>1447</td>
</tr>
<tr>
<td>J.8</td>
<td>Mod Clauses</td>
<td>1449</td>
</tr>
<tr>
<td>J.9</td>
<td>The Storage_Size Attribute</td>
<td>1450</td>
</tr>
<tr>
<td>J.10</td>
<td>Specific Suppression of Checks</td>
<td>1450</td>
</tr>
<tr>
<td>J.11</td>
<td>The Class Attribute of Untagged Incomplete Types</td>
<td>1451</td>
</tr>
<tr>
<td>J.12</td>
<td>Pragma Interface</td>
<td>1451</td>
</tr>
<tr>
<td>J.13</td>
<td>Dependence Restriction Identifiers</td>
<td>1452</td>
</tr>
<tr>
<td>J.14</td>
<td>Character and Wide_Character Conversion Functions</td>
<td>1452</td>
</tr>
<tr>
<td>J.15</td>
<td>Aspect-related Pragmas</td>
<td>1452</td>
</tr>
<tr>
<td>J.15.1</td>
<td>Pragma Inline</td>
<td>1454</td>
</tr>
<tr>
<td>J.15.2</td>
<td>Pragma No_Return</td>
<td>1455</td>
</tr>
<tr>
<td>J.15.3</td>
<td>Pragma Pack</td>
<td>1455</td>
</tr>
<tr>
<td>J.15.4</td>
<td>Pragma Storage_Size</td>
<td>1456</td>
</tr>
</tbody>
</table>

**Annex H**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.1</td>
<td>Pragma Normalize_Scalars</td>
<td>1425</td>
</tr>
<tr>
<td>H.2</td>
<td>Documentation of Implementation Decisions</td>
<td>1426</td>
</tr>
<tr>
<td>H.3</td>
<td>Reviewable Object Code</td>
<td>1427</td>
</tr>
<tr>
<td>H.3.1</td>
<td>Pragma Reviewable</td>
<td>1427</td>
</tr>
<tr>
<td>H.3.2</td>
<td>Pragma Inspection_Point</td>
<td>1429</td>
</tr>
<tr>
<td>H.4</td>
<td>High Integrity Restrictions</td>
<td>1430</td>
</tr>
<tr>
<td>H.4.1</td>
<td>Aspect No_Controlled_Parts</td>
<td>1436</td>
</tr>
<tr>
<td>H.5</td>
<td>Pragma Detect_Blocking</td>
<td>1437</td>
</tr>
<tr>
<td>H.6</td>
<td>Pragma Partition_Elaboration_Policy</td>
<td>1437</td>
</tr>
<tr>
<td>H.7</td>
<td>Extensions to Global and Global'Class Aspects</td>
<td>1439</td>
</tr>
<tr>
<td>H.7.1</td>
<td>The Use_Formal and Dispatching Aspects</td>
<td>1440</td>
</tr>
</tbody>
</table>

**Annex J**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>J.15</td>
<td>Aspect-related Pragmas</td>
<td>1452</td>
</tr>
<tr>
<td>J.15.1</td>
<td>Pragma Inline</td>
<td>1454</td>
</tr>
<tr>
<td>J.15.2</td>
<td>Pragma No_Return</td>
<td>1455</td>
</tr>
<tr>
<td>J.15.3</td>
<td>Pragma Pack</td>
<td>1455</td>
</tr>
<tr>
<td>J.15.4</td>
<td>Pragma Storage_Size</td>
<td>1456</td>
</tr>
</tbody>
</table>

**G**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1</td>
<td>Complex Arithmetic</td>
<td>1377</td>
</tr>
<tr>
<td>G.1.1</td>
<td>Complex Types</td>
<td>1378</td>
</tr>
<tr>
<td>G.1.2</td>
<td>Complex Elementary Functions</td>
<td>1383</td>
</tr>
<tr>
<td>G.1.3</td>
<td>Complex Input-Output</td>
<td>1388</td>
</tr>
<tr>
<td>G.1.4</td>
<td>The Package Wide_Text_IO.Complex_IO</td>
<td>1391</td>
</tr>
<tr>
<td>G.1.5</td>
<td>The Package Wide_Wide_Text_IO.Complex_IO</td>
<td>1391</td>
</tr>
<tr>
<td>G.2</td>
<td>Numeric Performance Requirements</td>
<td>1392</td>
</tr>
<tr>
<td>G.2.1</td>
<td>Model of Floating Point Arithmetic</td>
<td>1392</td>
</tr>
<tr>
<td>G.2.2</td>
<td>Model-Oriented Attributes of Floating Point Types</td>
<td>1394</td>
</tr>
<tr>
<td>G.2.3</td>
<td>Model of Fixed Point Arithmetic</td>
<td>1396</td>
</tr>
<tr>
<td>G.2.4</td>
<td>Accuracy Requirements for the Elementary Functions</td>
<td>1399</td>
</tr>
<tr>
<td>G.2.5</td>
<td>Performance Requirements for Random Number Generation</td>
<td>1401</td>
</tr>
<tr>
<td>G.2.6</td>
<td>Accuracy Requirements for Complex Arithmetic</td>
<td>1403</td>
</tr>
<tr>
<td>G.3</td>
<td>Vector and Matrix Manipulation</td>
<td>1405</td>
</tr>
<tr>
<td>G.3.1</td>
<td>Real Vectors and Matrices</td>
<td>1406</td>
</tr>
<tr>
<td>G.3.2</td>
<td>Complex Vectors and Matrices</td>
<td>1412</td>
</tr>
</tbody>
</table>

**G**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1.5.2</td>
<td>Pragma Pack</td>
<td>1455</td>
</tr>
<tr>
<td>G.1.4.1</td>
<td>Aspect No_Controlled_Parts</td>
<td>1436</td>
</tr>
<tr>
<td>G.1.7.1</td>
<td>The Use_Formal and Dispatching Aspects</td>
<td>1440</td>
</tr>
<tr>
<td>G.2.6</td>
<td>Accuracy Requirements for Complex Arithmetic</td>
<td>1403</td>
</tr>
<tr>
<td>G.3.2.2</td>
<td>Complex Vectors and Matrices</td>
<td>1412</td>
</tr>
</tbody>
</table>

**Annex H**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.7</td>
<td>Extensions to Global and Global'Class Aspects</td>
<td>1439</td>
</tr>
<tr>
<td>H.7.1</td>
<td>The Use_Formal and Dispatching Aspects</td>
<td>1440</td>
</tr>
</tbody>
</table>

**Annex J**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>J.15.4</td>
<td>Pragma Storage_Size</td>
<td>1456</td>
</tr>
</tbody>
</table>

**Obsolescent Features**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>J</td>
<td>Renamings of Library Units</td>
<td>1443</td>
</tr>
<tr>
<td>J.3</td>
<td>Reduced Accuracy Subtypes</td>
<td>1444</td>
</tr>
<tr>
<td>J.4</td>
<td>The Constrained Attribute</td>
<td>1446</td>
</tr>
<tr>
<td>J.5</td>
<td>ASCII</td>
<td>1446</td>
</tr>
<tr>
<td>J.6</td>
<td>Numeric_Error</td>
<td>1447</td>
</tr>
<tr>
<td>J.7</td>
<td>At Clauses</td>
<td>1447</td>
</tr>
<tr>
<td>J.7.1</td>
<td>Interrupt Entries</td>
<td>1447</td>
</tr>
<tr>
<td>J.8</td>
<td>Mod Clauses</td>
<td>1449</td>
</tr>
<tr>
<td>J.9</td>
<td>The Storage_Size Attribute</td>
<td>1450</td>
</tr>
<tr>
<td>J.10</td>
<td>Specific Suppression of Checks</td>
<td>1450</td>
</tr>
<tr>
<td>J.11</td>
<td>The Class Attribute of Untagged Incomplete Types</td>
<td>1451</td>
</tr>
<tr>
<td>J.12</td>
<td>Pragma Interface</td>
<td>1451</td>
</tr>
<tr>
<td>J.13</td>
<td>Dependence Restriction Identifiers</td>
<td>1452</td>
</tr>
<tr>
<td>J.14</td>
<td>Character and Wide_Character Conversion Functions</td>
<td>1452</td>
</tr>
<tr>
<td>J.15</td>
<td>Aspect-related Pragmas</td>
<td>1452</td>
</tr>
</tbody>
</table>

**High Integrity Systems**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.1</td>
<td>Pragma Normalize_Scalars</td>
<td>1425</td>
</tr>
<tr>
<td>H.2</td>
<td>Documentation of Implementation Decisions</td>
<td>1426</td>
</tr>
<tr>
<td>H.3</td>
<td>Reviewable Object Code</td>
<td>1427</td>
</tr>
<tr>
<td>H.3.1</td>
<td>Pragma Reviewable</td>
<td>1427</td>
</tr>
<tr>
<td>H.3.2</td>
<td>Pragma Inspection_Point</td>
<td>1429</td>
</tr>
<tr>
<td>H.4</td>
<td>High Integrity Restrictions</td>
<td>1430</td>
</tr>
<tr>
<td>H.4.1</td>
<td>Aspect No_Controlled_Parts</td>
<td>1436</td>
</tr>
<tr>
<td>H.5</td>
<td>Pragma Detect_Blocking</td>
<td>1437</td>
</tr>
<tr>
<td>H.6</td>
<td>Pragma Partition_Elaboration_Policy</td>
<td>1437</td>
</tr>
<tr>
<td>H.7</td>
<td>Extensions to Global and Global'Class Aspects</td>
<td>1439</td>
</tr>
<tr>
<td>H.7.1</td>
<td>The Use_Formal and Dispatching Aspects</td>
<td>1440</td>
</tr>
</tbody>
</table>

**Obsolescent Features**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>J</td>
<td>Renamings of Library Units</td>
<td>1443</td>
</tr>
<tr>
<td>J.3</td>
<td>Reduced Accuracy Subtypes</td>
<td>1444</td>
</tr>
<tr>
<td>J.4</td>
<td>The Constrained Attribute</td>
<td>1446</td>
</tr>
<tr>
<td>J.5</td>
<td>ASCII</td>
<td>1446</td>
</tr>
<tr>
<td>J.6</td>
<td>Numeric_Error</td>
<td>1447</td>
</tr>
<tr>
<td>J.7</td>
<td>At Clauses</td>
<td>1447</td>
</tr>
<tr>
<td>J.7.1</td>
<td>Interrupt Entries</td>
<td>1447</td>
</tr>
<tr>
<td>J.8</td>
<td>Mod Clauses</td>
<td>1449</td>
</tr>
<tr>
<td>J.9</td>
<td>The Storage_Size Attribute</td>
<td>1450</td>
</tr>
<tr>
<td>J.10</td>
<td>Specific Suppression of Checks</td>
<td>1450</td>
</tr>
<tr>
<td>J.11</td>
<td>The Class Attribute of Untagged Incomplete Types</td>
<td>1451</td>
</tr>
<tr>
<td>J.12</td>
<td>Pragma Interface</td>
<td>1451</td>
</tr>
<tr>
<td>J.13</td>
<td>Dependence Restriction Identifiers</td>
<td>1452</td>
</tr>
<tr>
<td>J.14</td>
<td>Character and Wide_Character Conversion Functions</td>
<td>1452</td>
</tr>
<tr>
<td>J.15</td>
<td>Aspect-related Pragmas</td>
<td>1452</td>
</tr>
</tbody>
</table>

**Obsolescent Features**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>J.15.1</td>
<td>Pragma Inline</td>
<td>1454</td>
</tr>
<tr>
<td>J.15.2</td>
<td>Pragma No_Return</td>
<td>1455</td>
</tr>
<tr>
<td>J.15.3</td>
<td>Pragma Pack</td>
<td>1455</td>
</tr>
<tr>
<td>J.15.4</td>
<td>Pragma Storage_Size</td>
<td>1456</td>
</tr>
</tbody>
</table>

**High Integrity Systems**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.1</td>
<td>Pragma Normalize_Scalars</td>
<td>1425</td>
</tr>
<tr>
<td>H.2</td>
<td>Documentation of Implementation Decisions</td>
<td>1426</td>
</tr>
<tr>
<td>H.3</td>
<td>Reviewable Object Code</td>
<td>1427</td>
</tr>
<tr>
<td>H.3.1</td>
<td>Pragma Reviewable</td>
<td>1427</td>
</tr>
<tr>
<td>H.3.2</td>
<td>Pragma Inspection_Point</td>
<td>1429</td>
</tr>
<tr>
<td>H.4</td>
<td>High Integrity Restrictions</td>
<td>1430</td>
</tr>
<tr>
<td>H.4.1</td>
<td>Aspect No_Controlled_Parts</td>
<td>1436</td>
</tr>
<tr>
<td>H.5</td>
<td>Pragma Detect_Blocking</td>
<td>1437</td>
</tr>
<tr>
<td>H.6</td>
<td>Pragma Partition_Elaboration_Policy</td>
<td>1437</td>
</tr>
<tr>
<td>H.7</td>
<td>Extensions to Global and Global'Class Aspects</td>
<td>1439</td>
</tr>
<tr>
<td>H.7.1</td>
<td>The Use_Formal and Dispatching Aspects</td>
<td>1440</td>
</tr>
</tbody>
</table>
### J.15 Interfacing Pragmas
- J.15.5 Interfacing Pragmas ................................................................. 1456
- J.15.6 Pragma Unchecked_Union .......................................................... 1457
- J.15.7 Pragmas Interrupt_Handler and Attach_Handler ....................... 1458
- J.15.8 Shared Variable Pragmas ............................................................ 1459
- J.15.9 Pragma CPU ............................................................................... 1460
- J.15.10 Pragma Dispatching_Domain ................................................... 1460
- J.15.11 Pragmas Priority and Interrupt_Priority .................................... 1461
- J.15.12 Pragma Relative_Deadline ....................................................... 1462
- J.15.13 Pragma Asynchronous ............................................................. 1462
- J.15.14 Elaboration Control Pragmas .................................................... 1462
- J.15.15 Distribution Pragmas ............................................................... 1463

### Annex K (informative) Language-Defined Aspects and Attributes ......... 1465
- K.1 Language-Defined Aspects ............................................................. 1465
- K.2 Language-Defined Attributes ....................................................... 1469

### Annex L (informative) Language-Defined Pragmas ................................. 1489

### Annex M (informative) Summary of Documentation Requirements ............ 1493
- M.1 Specific Documentation Requirements ........................................... 1493
- M.2 Implementation-Defined Characteristics ....................................... 1495
- M.3 Implementation Advice ................................................................. 1503

### Annex N (informative) Glossary ............................................................ 1513

### Annex P (informative) Syntax Summary .................................................. 1515
- P.1 Syntax Rules .................................................................................. 1515
- P.2 Syntax Cross Reference ................................................................. 1538

### Annex Q (informative) Language-Defined Entities .................................... 1551
- Q.1 Language-Defined Packages ......................................................... 1551
- Q.2 Language-Defined Types and Subtypes ......................................... 1554
- Q.3 Language-Defined Subprograms .................................................. 1558
- Q.4 Language-Defined Exceptions ...................................................... 1571
- Q.5 Language-Defined Objects ............................................................ 1572

### Index .................................................................................................... 1577
Foreword

This document is the Annotated Ada Reference Manual. The International Standard for the programming language Ada is ISO/IEC 8652:2023/20121995(E). The International Standard is derived from the Ada Reference Manual, with various non-normative changes. In particular, the International Standard numbers clauses differently, omits the annotations and paragraph numbers, eliminates the Acknowledgements, and modifies various front matter such as the Title page and the Foreword.

Discussion: New ISO requirements necessitated changing the numbers of all of the numbered clauses and subclauses in the International Standard. The Ada Reference Manual retains its traditional numbering of clauses and subclauses as it is common for existing material (both printed and electronic) to refer to subclauses just by number.

The Ada Working Group ISO/IEC JTC 1/SC 22/WG 9 is tasked by ISO with the work item to interpret and maintain the International Standard and to produce Technical Corrigenda, as appropriate. The technical work on the International Standard is performed by the Ada Rapporteur Group (ARG) of WG 9.

AXE Consultants produces the Ada Reference Manual in consultation with the ARG, along with drafts of other documents as needed. ISO/IEC documents often list the individual changes that need to be made to the text of a Standard, rather than simply updating the document. As such, an International Standard is often found in several parts, while the Ada Reference Manual is always a single document.

In June 2015, September 2000, WG 9 approved and forwarded Technical Corrigendum 1 to SC 22 for ISO approval, which was granted in December 2015/February 2001. Technical Corrigendum 1 was published in February 2016/June 2001.

In June 2016, WG 9 approved a tentative schedule for the preparation of an Amendment or Revision to the International Standard, with a delivery no earlier than 2018. In July 2019, WG 9 approved an additional review and prototyping period for this revision, extending the delivery to no earlier than late 2020. The draft standard was delivered to WG 9 in July 2021, and the Standard was published as ISO/IEC 8652:2023 in May 2023.


Since the completion of Ada 2022, work has continued on Ada, both to correct errors and to add small enhancements. Currently, there has been no determination of when or in what form these changes will be issued. However, it is valuable to have all of the corrections available in one place. Thus, we've created this draft update, which for the purposes of this document, we'll call Ada 202y.

This Ada Reference Manual replaces the edition of 2012. It modifies the previous edition by making changes and additions that improve the capability of the language and the reliability of programs written in the language.

Significant changes in this edition are as follows:

- Improved support for parallel execution is provided via the introduction of parallel loops, parallel blocks, parallel container iteration, and parallel reduction.
- More precise specification of subprogram interfaces is supported via the new aspects Global, Global'Class, and Nonblocking. The Global aspects, in particular, help to determine whether two constructs can safely execute in parallel.
- Pre and Post aspects can now be specified for access-to-subprogram types and for generic formal subprograms; a postcondition for the default initialization of a type can be specified using the new Default Initial Condition aspect.
The behavior of many predefined container operations is now more precisely specified by using pre- and postcondition specifications instead of English descriptions; a restricted ("stable") view for most containers is introduced to support more efficient iteration.

More flexible uses of static expressions are supported via the introduction of static expression functions along with fewer restrictions on static strings.

The Image attribute is supported for nonscalar types, and a user-specifiable attribute Put_Image is provided, which determines the value of the Image attribute for a user-defined type.

The use of numeric and string literals is generalized to allow their use with other categories of types, via the new aspects Integer_Literal, Real_Literal, and String_Literal.

Array and record aggregates are made more flexible: index parameters are allowed in an array aggregate to define the components as a function of their array index; discriminants can be defined more flexibly within an aggregate for a variant record type.

New types of aggregates are provided: delta aggregates to allow the construction of a new object by incremental updates to an existing object; container aggregates to allow construction of an object of a container type by directly specifying its elements.

A shorthand is provided, using the token '@', to refer to the target of an assignment statement in the expression defining its new value.

Declare expressions are provided that permit the definition and use of local constants or renamings, to allow a large expression to be simplified by defining common parts as named entities.

Support for lightweight iteration is added via the introduction of procedural iterators.

Support for the map-reduce programming strategy is added via the introduction of reduction expressions.

For constructs that use iterators of any sort, a filter can be specified that restricts the elements produced by the iteration to those that satisfy the condition of the filter.

Predefined packages supporting arbitrary-precision integer and real arithmetic are provided.

The Jorvik profile is introduced to support hard real-time applications that want to go beyond the restrictions of the Ravenscar profile.
Introduction

This is the Annotated Ada Reference Manual.

**Discussion:** This document is the Annotated Ada Reference Manual (AARM). It contains the entire text of the Ada 202y standard (ISO/IEC 8652:202y), plus various annotations. It is intended primarily for compiler writers, validation test writers, and other language lawyers. The annotations include detailed rationale for individual rules and explanations of some of the more arcane interactions among the rules.

Other available Ada documents include:

- **{AI95-00387-01} {AI05-0245-1} Ada 2022 Overview/2012 Rationale.** This gives an introduction to the changes and new features in Ada 2022, and explains the rationale behind them. Programmers should read this overview/rationale before reading Reference Manual in depth. Rationales for Ada 83, Ada 95, and Ada 2005 are also available. Ada 95 Rationale. This Rationale for the Ada Programming Language — 1995 edition, which gives an introduction to the new features of Ada incorporated in the 1995 edition of this Reference Manual, and explains the rationale behind them. Programmers unfamiliar with Ada 95 should read this first.
  
  **Discussion:** As of this writing (December 2012), only five chapters of the Ada 2012 Rationale have been published. Additional chapters are in development and should be published during 2013.

- **{AI95-00387-01} {AI05-0245-1} Ada 2005 Rationale.** This gives an introduction to the changes and new features in Ada 2005 (compared with the 1995 edition), and explains the rationale behind them. Programmers should read this rationale before reading this Reference Manual in depth.

- **This paragraph was deleted.** Changes to Ada — 1987 to 1995. This document lists in detail the changes made to the 1987 edition of the standard.


**Design Goals**

**{AI95-00387-01} {AI12-0313-1} Ada was originally designed with three overriding concerns: program reliability and maintenance, programming as a human activity, and efficiency. The 1995 revision to the language was designed to provide greater flexibility and extensibility, additional control over storage management and synchronization, and standardized packages oriented toward supporting important application areas, while at the same time retaining the original emphasis on reliability, maintainability, and efficiency. Subsequent editions, including this fourth/third edition amended version, have provided further flexibility and added more standardized packages within the framework provided by the 1995 revision.**

The need for languages that promote reliability and simplify maintenance is well established. Hence emphasis was placed on program readability over ease of writing. For example, the rules of the language require that program variables be explicitly declared and that their type be specified. Since the type of a variable is invariant, compilers can ensure that operations on variables are compatible with the properties intended for objects of the type. Furthermore, error-prone notations have been avoided, and the syntax of the language avoids the use of encoded forms in favor of more English-like constructs. Finally, the
language offers support for separate compilation of program units in a way that facilitates program
development and maintenance, and which provides the same degree of checking between units as within a
unit.

Concern for the human programmer was also stressed during the design. Above all, an attempt was made
to keep to a relatively small number of underlying concepts integrated in a consistent and systematic way
while continuing to avoid the pitfalls of excessive involution. The design especially aims to provide
language constructs that correspond intuitively to the normal expectations of users.

Like many other human activities, the development of programs is becoming ever more decentralized and
distributed. Consequently, the ability to assemble a program from independently produced software
components continues to be a central idea in the design. The concepts of packages, of private types, and
of generic units are directly related to this idea, which has ramifications in many other aspects of the
language. An allied concern is the maintenance of programs to match changing requirements; type
extension and the hierarchical library enable a program to be modified while minimizing disturbance to
existing tested and trusted components.

No language can avoid the problem of efficiency. Languages that require over-elaborate
compilers, or that lead to the inefficient use of storage or execution time, force these inefficiencies on all
machines and on all programs. Every construct of the language was examined in the light of present
implementation techniques. Any proposed construct whose implementation was unclear or that required
excessive machine resources was rejected. Parallel constructs were introduced to simplify making safe
and efficient use of modern multicore architectures.

Language Summary

An Ada program is composed of one or more program units. Program
units can be subprograms (which define executable algorithms), packages (which define collections
of entities), task units (which define concurrent computations), protected units (which define operations
for the coordinated sharing of data between tasks), or generic units (which define parameterized forms of
packages and subprograms). Each program unit normally consists of two parts: a specification, containing
the information that must be visible to other units, and a body, containing the implementation details,
which are not be visible to other units. Most program units can be compiled separately.

This distinction of the specification and body, and the ability to compile units separately, allows a
program to be designed, written, and tested as a set of largely independent software components.

An Ada program will normally make use of a library of program units of general utility. The
language provides means whereby individual organizations can construct their own libraries. All
libraries are structured in a hierarchical manner; this enables the logical decomposition of a subsystem
into individual components. The text of a separately compiled program unit names the library
units it requires.

Program Units

A subprogram is the basic unit for expressing an algorithm. There are two kinds of
subprograms: procedures and functions. A procedure is the means of invoking a series of actions. For
example, it can read data, update variables, or produce some output. It can have parameters, to
provide a controlled means of passing information between the procedure and the point of call. A function
is the means of invoking the computation of a value. It is similar to a procedure, but in addition will
return a result.

A package is the basic unit for defining a collection of logically related entities. For example, a package
can be used to define a set of type declarations and associated operations. Portions of a package can be
hidden from the user, thus allowing access only to the logical properties expressed by the package specification.

\{AI12-0441-1\} Subprogram and package units \textit{can} may be compiled separately and arranged in hierarchies of parent and child units giving fine control over visibility of the logical properties and their detailed implementation.

\{AI12-0441-1\} A task unit is the basic unit for defining a task whose sequence of actions \textit{can} may be executed concurrently with those of other tasks. Such tasks \textit{can} may be implemented on multicomputers, multiprocessors, or with interleaved execution on a single processor. A task unit \textit{can} may define either a single executing task or a task type permitting the creation of any number of similar tasks.

\{AI95-00114-01\} \{AI12-0441-1\} \{AI12-0446-1\} A protected unit is the basic unit for defining protected operations for the coordinated use of data shared between tasks. Simple mutual exclusion is provided automatically, and more elaborate sharing protocols can be defined. A protected operation can either be a subprogram or an entry. A protected entry specifies a Boolean expression (an entry barrier) that \textit{blocks the execution of the body until it evaluates to True}, \textit{must be True} before the body of the entry is executed. A protected unit \textit{can} may define a single protected object or a protected type permitting the creation of several similar objects.

\textit{Declarations and Statements}

The body of a program unit generally contains two parts: a declarative part, which defines the logical entities to be used in the program unit, and a sequence of statements, which defines the execution of the program unit.

\{AI12-0441-1\} The declarative part associates names with declared entities. For example, a name \textit{can} may denote a type, a constant, a variable, or an exception. A declarative part also introduces the names and parameters of other nested subprograms, packages, task units, protected units, and generic units to be used in the program unit.

\{AI12-0454-1\} The sequence of statements describes a sequence of actions \textit{that are to be performed}. The statements are executed in succession (unless a transfer of control causes execution to continue from another place).

An assignment statement changes the value of a variable. A procedure call invokes execution of a procedure after associating any actual parameters provided at the call with the corresponding formal parameters.

Case statements and if statements allow the selection of an enclosed sequence of statements based on the value of an expression or on the value of a condition.

\{AI12-0446-1\} The loop statement provides the basic iterative mechanism in the language. A loop statement specifies \textit{that a sequence of statements that are to be executed repeatedly as directed by an iteration scheme, or until an exit statement is encountered.}

A block statement comprises a sequence of statements preceded by the declaration of local entities used by the statements.

\{AI12-0119-1\} Certain statements are associated with concurrent execution. A delay statement delays the execution of a task for a specified duration or until a specified time. An entry call statement is written as a procedure call statement; it requests an operation on a task or on a protected object, blocking the caller until the operation can be performed. A called task \textit{can} may accept an entry call by executing a corresponding accept statement, which specifies the actions then to be performed as part of the rendezvous with the calling task. An entry call on a protected object is processed when the corresponding entry barrier evaluates to true, whereupon the body of the entry is executed. The requeue statement
permits the provision of a service as a number of related activities with preference control. One form of the select statement allows a selective wait for one of several alternative rendezvous. Other forms of the select statement allow conditional or timed entry calls and the asynchronous transfer of control in response to some triggering event. Various parallel constructs, including parallel loops and parallel blocks, support the initiation of multiple logical threads of control designed to execute in parallel when multiple processors are available.

Execution of a program unit can encounter error situations in which normal program execution cannot continue. For example, an arithmetic computation may exceed the maximum allowed value of a number, or an attempt may be made to access an array component by using an incorrect index value. To deal with such error situations, the statements of a program unit can be textually followed by exception handlers that specify the actions to be taken when the error situation arises. Exceptions can be raised explicitly by a raise statement.

Data Types

Every object in the language has a type, which characterizes a set of values and a set of applicable operations. The main categories of types are elementary types (comprising enumeration, numeric, and access types) and composite types (including array and record types).

An enumeration type defines an ordered set of distinct enumeration literals, for example a list of states or an alphabet of characters. The enumeration types Boolean, Character, and Wide_Character, and Wide_Wide_Character are predefined.

Numeric types provide a means of performing exact or approximate numerical computations. Exact computations use integer types, which denote sets of consecutive integers. Approximate computations use either fixed point types, with absolute bounds on the error, or floating point types, with relative bounds on the error. The numeric types Integer, Float, and Duration are predefined.

Composite types allow definitions of structured objects with related components. The composite types in the language include arrays and records. An array is an object with indexed components of the same type. A record is an object with named components of possibly different types. Task and protected types are also forms of composite types. The array types String, and Wide_String, and Wide_Wide_String are predefined.

Record, task, and protected types have special components called discriminants which parameterize the type. Variant record structures that depend on the values of discriminants can be defined within a record type.

Access types allow the construction of linked data structures. A value of an access type represents a reference to an object declared as aliased or to an object created by the evaluation of an allocator. Several variables of an access type designate the same object, and components of one object designate the same or other objects. Both the elements in such linked data structures and their relation to other elements can be altered during program execution. Access types also permit references to subprograms to be stored, passed as parameters, and ultimately dereferenced as part of an indirect call.

Private types permit restricted views of a type. A private type can be defined in a package so that only the logically necessary properties are made visible to the users of the type. The full structural details that are externally irrelevant are then only available within the package and any child units.

From any type a new type can be defined by derivation. A type, together with its derivatives (both direct and indirect) form a derivation class. Class-wide operations can be defined that accept as a parameter an operand of any type in a derivation class. For record and private types, the derivatives can be extensions of the parent type. Types that support these object-
oriented capabilities of class-wide operations and type extension are tagged, so that the specific type of an operand within a derivation class can be identified at run time. When an operation of a tagged type is applied to an operand whose specific type is not known until run time, implicit dispatching is performed based on the tag of the operand.

\{AI95-00387-01\} \{AI12-0441-1\} Interface types provide abstract models from which other interfaces and types can be composed and derived. This provides a reliable form of multiple inheritance. Interface types can also be implemented by task types and protected types thereby enabling concurrent programming and inheritance to be merged.

The concept of a type is further refined by the concept of a subtype, whereby a user can constrain the set of allowed values of a type. Subtypes can be used to define subranges of scalar types, arrays with a limited set of index values, and records and private types with particular discriminant values.

**Other Facilities**

\{AI95-00387-01\} \{AI12-0438-1\} Aspect Representation clauses can be used to specify the mapping between types and features of an underlying machine. For example, the user can specify that objects of a given type are to be represented with a given number of bits, or that the components of a record are to be represented using a given storage layout. Other features allow the controlled use of low level, nonportable, or implementation-dependent aspects, including the direct insertion of machine code.

\{AI12-0313-1\} Aspect clauses can also be used to specify more abstract properties of program entities, such as the pre- and postconditions of a subprogram, or the invariant for a private type. Additional aspects are specifiable to allow user-defined types to use constructs of the language, such as literals, aggregates, or indexing, normally reserved for particular language-defined categories of types, such as numeric types, record types, or array types.

\{AI95-00387-01\} The predefined environment of the language provides for input-output and other capabilities (such as string manipulation and random number generation) by means of standard library packages. Input-output is supported for values of user-defined as well as of predefined types. Standard means of representing values in display form are also provided. Other standard library packages are defined in annexes of the standard to support systems with specialized requirements.

\{AI95-00387-01\} The predefined standard library packages provide facilities such as string manipulation, containers of various kinds (vectors, lists, maps, etc.), mathematical functions, random number generation, and access to the execution environment.

\{AI95-00387-01\} The specialized annexes define further predefined library packages and facilities with emphasis on areas such as real-time scheduling, interrupt handling, distributed systems, numerical computation, and high-integrity systems.

Finally, the language provides a powerful means of parameterization of program units, called generic program units. The generic parameters can be types and subprograms (as well as objects and packages) and so allow general algorithms and data structures to be defined that are applicable to all types of a given class.

**Language Changes**

*Paragraphs 44 through 57 have been replaced and moved to the Foreword removed as they described differences from the first edition of Ada (Ada 83).*

\{AI95-00387-01\} This amended International Standard updates the edition of 1995 which replaced the first edition of 1987. In the 1995 edition, the following major language changes were incorporated:
Support for standard 8-bit and 16-bit characters was added. See clauses 2.1, 3.5.2, 3.6.3, A.1, A.3, and A.4.

The type model was extended to include facilities for object-oriented programming with dynamic run-time polymorphism. See the discussions of classes, derived types, record extensions, and private extensions in clauses 3.4, 3.9, and 7.3. Additional types that are allowed as described in clauses 12.5.1 and 12.7, “Formal Private and Derived Types,” and 12.7, “Formal Packages.”

Access types were extended to allow an access value to designate a subprogram or an object declared by an object declaration (as opposed to just an object that is heap-allocated on a heap object). See clause 3.10.

The object-oriented model has been improved by the addition of an interface facility which provides multiple inheritance and additional flexibility for type extensions. See subclauses 3.4, 3.9, and 7.3. An alternative notation for calling operations more akin to that used in other languages has also been added. See subclause 4.1.3.

Access types have been further extended to unify properties such as the ability to access constants and to exclude null values. See clause 3.10. Anonymous access types are now permitted more freely and anonymous access to subprogram types are introduced. See subclauses 3.3, 3.6, 3.10, and 8.5.1.

The control of structure and visibility has been enhanced to permit mutually dependent references between units and finer control over access from the private part of a package. See subclauses 3.10.1 and 10.1.2. In addition, limited types have been made more useful by the provision of aggregates, constants, and constructor functions. See subclauses 4.3, 6.5, and 7.5.
The predefined environment has been extended to include additional time and calendar operations, improved string handling, a comprehensive container library, file and directory management, and access to environment variables. See subclauses 9.6.1, A.4, A.16, A.17, and A.18.

Two of the Specialized Needs Annexes have been considerably enhanced:

- The Real-Time Systems Annex now includes the Ravenscar profile for high-integrity systems, further dispatching policies such as Round Robin and Earliest Deadline First, support for timing events, and support for control of CPU time utilization. See subclauses D.2, D.13, D.14, and D.15.

- The Numerics Annex now includes support for real and complex vectors and matrices as previously defined in ISO/IEC 13813:1997 plus further basic operations for linear algebra. See subclause clause G.3.

The overall reliability of the language has been enhanced by a number of improvements. These include new syntax which detects accidental overloading, as well as pragmas for making assertions and giving better control over the suppression of checks. See subclauses 6.1, 11.4.2, and 11.5.

In addition, this third edition makes enhancements to address two important issues, namely, the particular problems of multiprocessor architectures, and the need to further increase the capabilities regarding assertions for correctness. It also makes additional changes and additions that improve the capability of the language and the reliability of programs written in the language.

The following significant changes with respect to the 1995 edition as amended by Amendment 1 are incorporated:

- New syntax (the aspect specification) is introduced to enable properties to be specified for various entities in a more structured manner than through pragmas. See subclause 13.1.1.

- The concept of assertions introduced in the 2005 edition is extended with the ability to specify preconditions and postconditions for subprograms, and invariants for private types and interfaces. The concept of constraints in defining subtypes is supplemented with subtype predicates that enable subsets to be specified other than as simple ranges. These properties are all indicated using aspect specifications. See subclauses 3.2.4, 6.1.1, and 7.3.2.

- New forms of expressions are introduced. These are if expressions, case expressions, quantified expressions, and expression functions, and raise expressions. As well as being useful for programming in general by avoiding the introduction of unnecessary assignments, they are especially valuable in conditions and invariants since they avoid the need to introduce auxiliary functions. See subclauses 4.5.7, 4.5.8, and 6.8. Membership tests are also made more flexible. See subclauses 4.4 and 4.5.2.

- A number of changes are made to subprogram parameters. Functions may now have parameters of all modes. In order to mitigate consequent (and indeed existing) problems of inadvertent order dependence, rules are introduced to reduce aliasing. A parameter may now be explicitly marked as aliased and the type of a parameter may be incomplete in certain circumstances. See subclauses 3.10.1, 6.1, and 6.4.1.

- The use of access types is now more flexible. The rules for accessibility and certain conversions are improved. See subclauses 3.10.2, 4.5.2, 4.6, and 8.6. Furthermore, better control of storage pools is provided. See subclause 13.11.4.
• `{AI12-0313-1}` The Real-Time Systems Annex now includes facilities for defining domains of processors and assigning tasks to them. Improvements are made to scheduling and budgeting facilities. See subclauses D.10.1, D.14, and D.16.

• `{AI12-0313-1}` A number of important improvements are made to the standard library. These include packages for conversions between strings and UTF encodings, and classification functions for wide and wide-wide characters. Internationalization is catered for by a package giving locale information. See subclauses A.3, A.4.11, and A.19. The container library is extended to include bounded forms of the existing containers and new containers for indefinite objects, multiway trees, and queues. See subclause A.18.

• `{AI12-0313-1}` Finally, certain features are added primarily to ease the use of containers, such as the ability to iterate over all elements in a container without having to encode the iteration. These can also be used for iteration over arrays, and within quantified expressions. See subclauses 4.1.5, 4.1.6, 5.5.1, and 5.5.2.

Instructions for Comment Submission

• `{AI12-0446-1}` Informal comments on this Reference Manual can be submitted in three ways:

  • via e-mail to: ada-comment@ada-auth.org
  • by filling out a web form at: https://arg.adaic.org/community-input
  • by creating a new “issue” on the ARG GitHub site: https://github.com/Ada-Rapporteur-Group/User-Community-Input

• `{AI12-0446-1}` Informal comments on this Reference Manual may be sent via e-mail to ada-comment@ada-auth.org or ada-comment@sw-eng.falls-church.va.us. If appropriate, the Project Editor will initiate the defect correction procedure.

Comments should use the following format:

```
!topic Title summarizing comment
!reference Ada 2022/2012/2005 RMRM95-ss.ss(pp)
!from Author Name yy-mm-dd
!keywords keywords related to topic
!discussion
text of discussion
```

where `ss.ss` is the section, clause or subclause number, `pp` is the paragraph number where applicable, and `yy-mm-dd` is the date the comment was sent. The date is optional, as is the `!keywords` line.

• `{AI12-0446-1}` Multiple comments per e-mail message are acceptable. Please use a descriptive “Subject” when sending an e-mail message, or title when creating a new issue, and limit each message to a single comment.

When correcting typographical errors or making minor wording suggestions, please put the correction directly as the topic of the comment; use square brackets `[ ]` to indicate text to be omitted and curly braces `{ }` to indicate text to be added, and provide enough context to make the nature of the suggestion self-evident or put additional information in the body of the comment, for example:

```
!topic [c]{C}haracter
!topic it[']s meaning is not defined
```
Formal requests for interpretations and for reporting defects in the International Standard may be made in accordance with the ISO/IEC JTC 1 Directives and the ISO/IEC JTC 1/SC 22 policy for interpretations. National Bodies may submit a Defect Report to ISO/IEC JTC 1/SC 22 for resolution under the JTC 1 procedures. A response will be provided and, if appropriate, a Technical Corrigendum will be issued in accordance with the procedures.

Acknowledgements for the Ada 83 edition

Ada is the result of a collective effort to design a common language for programming large scale and real-time systems.

The common high order language program began in 1974. The requirements of the United States Department of Defense were formalized in a series of documents which were extensively reviewed by the Services, industrial organizations, universities, and foreign military departments. The Ada language was designed in accordance with the final (1978) form of these requirements, embodied in the Steelman specification.

The Ada design team was led by Jean D. Ichbiah and has included Bernd Krieg-Brueckner, Brian A. Wichmann, Henry F. Ledgard, Jean-Claude Heliard, Jean-Loup Gailly, Jean-Raymond Abrial, John G.P. Barnes, Mike Woodger, Olivier Roubine, Paul N. Hilfinger, and Robert Firth.


Two parallel efforts that were started in the second phase of this design had a deep influence on the language. One was the development of a formal definition using denotational semantics, with the participation of V. Donzeau-Gouge, G. Kahn, and B. Lang. The other was the design of a test translator with the participation of K. Ripken, P. Boullier, P. Cadiou, J. Holden, J.F. Hueras, R.G. Lange, and D.T. Cornhill. The entire effort benefited from the dedicated assistance of Lyn Churchill and Marion Myers, and the effective technical support of B. Gravem, W.L. Heimerdinger, and P. Cleve. H.G. Schmitz served as program manager.

Over the five years spent on this project, several intense week-long design reviews were conducted, with the participation of P. Belmont, B. Broscol, P. Cohen, R. Dewar, A. Evans, G. Fisher, H. Harte, A.L. Hisgen, P. Knueven, M. Kronental, N. Lomuto, E. Plaedereader, G. Seegmueller, V. Stenning, D. Taffs, and also F. Belz, R. Converse, K. Correll, A.N. Habermann, J. Sammet, S. Squires, J. Teller, P. Wegner, and P.R. Wetherall.


These reviews and comments, the numerous evaluation reports received at the end of the first and second phase, the nine hundred language issue reports and test and evaluation reports received from fifteen different countries during the third phase of the project, the thousands of comments received during the ANSI Canvass, and the on-going work of the IFIP Working Group 2.4 on system implementation languages and that of the Purdue Europe LTPL-E committee, all had a substantial influence on the final definition of Ada.
The Military Departments and Agencies have provided a broad base of support including funding, extensive reviews, and countless individual contributions by the members of the High Order Language Working Group and other interested personnel. In particular, William A. Whitaker provided leadership for the program during the formative stages. David A. Fisher was responsible for the successful development and refinement of the language requirement documents that led to the Steelman specification.

The Ada 83 language definition was developed by Cii Honeywell Bull and later Alsys, and by Honeywell Systems and Research Center, under contract to the United States Department of Defense. William E. Carlson and later Larry E. Druffel served as the technical representatives of the United States Government and effectively coordinated the efforts of all participants in the Ada program.

Acknowledgements for the Ada 95 edition

This Reference Manual was prepared by the Ada 9X Mapping/Revision Team based at Intermetrics, Inc., which has included: W. Carlson, Program Manager; T. Taft, Technical Director; J. Barnes (consultant); B. Bros gol (consultant); R. Duff (Oak Tree Software); M. Edwards; C. Garrity; R. Hilliard; O. Pazy (consultant); D. Rosenfeld; L. Shafer; W. White; M. Woodger.

The following consultants to the Ada 9X Project contributed to the Specialized Needs Annexes: T. Baker (Real-Time/Systems Programming — SEI, FSU); K. Dritz (Numerics — Argonne National Laboratory); A. Gargaro (Distributed Systems — Computer Sciences); J. Goodenough (Real-Time/Systems Programming — SEI); J. McHugh (Secure Systems — consultant); B. Wichmann (Safety-Critical Systems — NPL: UK).

This work was regularly reviewed by the Ada 9X Distinguished Reviewers and the members of the Ada 9X Rapporteur Group (XRG): E. Ploedereder, Chairman of DRs and XRG (University of Stuttgart: Germany); B. Bardin (Hughes); J. Barnes (consultant: UK); B. Brett (DEC); B. Bros gol (consultant); R. Brukardt (RR Software); N. Cohen (IBM); R. Dewar (NYU); G. Dismukes (TeleSoft); A. Evans (consultant); A. Gargaro (Computer Sciences); M. Gerhardt (ESL); J. Goodenough (SEI); S. Heilbrunner (University of Salzburg: Austria); P. Hilfinger (UC/Berkeley); B. Källberg (CelsiusTech: Sweden); M. Kamrad II (Unisys); J. van Katwijk (Delft University of Technology: The Netherlands); V. Kaufman (Russia); P. Kruchten (Rational); R. Landwehr (CCI: Germany); C. Lester (Portsmouth Polytechnic: UK); L. Månsson (TELIA Research: Sweden); S. Michell (Multiprocessor Toolsmiths: Canada); M. Mills (US Air Force); D. Pogge (US Navy); K. Power (Boeing); O. Roubine (Veridix: France); A. Strohmeier (Swiss Fed Inst of Technology: Switzerland); W. Taylor (consultant: UK); J. Tokar (Tartan); E. Vasilescu (Grumman); J. Vladik (Prospek s s.r.o.: Czech Republic); S. Van Vlierberghe (OFFIS: Belgium).

Other valuable feedback influencing the revision process was provided by the Ada 9X Language Precision Team (Odyssey Research Associates), the Ada 9X User/Implementer Teams (AETECH, Tartan, TeleSoft), the Ada 9X Implementation Analysis Team (New York University) and the Ada community-at-large.


The Ada 9X Project was sponsored by the Ada Joint Program Office. Christine M. Anderson at the Air Force Phillips Laboratory (Kirtland AFB, NM) was the project manager.

Acknowledgements for the Corrigendum version

The editor [R. Brukardt (USA)] would like to thank the many people whose hard work and assistance has made this update revision possible.
Thanks go out to all of the members of the ISO/IEC JTC 1/SC 22/WG 9 Ada Rapporteur Group, whose work on creating and editing the wording corrections was critical to the entire process. Especially valuable contributions came from the chairman of the ARG, E. Ploedereder (Germany), who kept the process moving; J. Barnes (UK) and K. Ishihata (Japan), whose extremely detailed reviews kept the editor on his toes; G. Dismukes (USA), M. Kamrad (USA), P. Leroy (France), S. Michell (Canada), T. Taft (USA), J. Tokar (USA), and other members too numerous to mention.

Special thanks go to R. Duff (USA) for his explanations of the previous system of formatting of these documents during the tedious conversion to more modern formats. Special thanks also go to the convenor of ISO/IEC JTC 1/SC 22/WG 9, J. Moore (USA), without whose help and support the Corrigendum and this consolidated reference manual would not have been possible.

Acknowledgements for the Amendment 1 version

The editor [R. Brukardt (USA)] would like to thank the many people whose hard work and assistance has made this update/revision possible.

Thanks go out to all of the members of the ISO/IEC JTC 1/SC 22/WG 9 Ada Rapporteur Group, whose work on creating and editing the wording changes was critical to the entire process. Especially valuable contributions came from the chairman of the ARG, P. Leroy (France), who kept the process on schedule; J. Barnes (UK) whose careful reviews found many typographical errors; T. Taft (USA), who always seemed to have a suggestion when we were stuck, and who also was usually able to provide the valuable service of explaining why things were as they are; S. Baird (USA), who found many obscure problems with the proposals; and A. Burns (UK), who pushed many of the real-time proposals to completion. Other ARG members who contributed were: R. Dewar (USA), G. Dismukes (USA), R. Duff (USA), K. Ishihata (Japan), S. Michell (Canada), E. Ploedereder (Germany), J.P. Rosen (France), E. Schonberg (USA), J. Tokar (USA), and T. Vardanega (Italy).

Special thanks go to Ada-Europe and the Ada Resource Association, without whose help and support the Amendment and this consolidated reference manual would not have been possible. M. Heaney (USA) requires special thanks for his tireless work on the containers packages. Finally, special thanks go to the convenor of ISO/IEC JTC 1/SC 22/WG 9, J. Moore (USA), who guided the document through the standardization process.

Acknowledgements for the Ada 2012 edition

The editor [R. Brukardt (USA)] would like to thank the many people whose hard work and assistance has made this revision possible.

Thanks go out to all of the members of the ISO/IEC JTC 1/SC 22/WG 9 Ada Rapporteur Group, whose work on creating and editing the wording changes was critical to the entire process. Especially valuable contributions came from the chairman of the ARG, E. Schonberg (USA), who guided the work; T. Taft (USA), whose insights broke many logjams, both in design and wording; J. Barnes (UK) whose careful reviews uncovered many editorial errors; S. Baird (USA), who repeatedly found obscure interactions with the proposals that the rest of us missed. Other ARG members who substantially contributed were: A. Burns (UK), J. Cousins (UK), R. Dewar (USA), G. Dismukes (USA), R. Duff (USA), P. Leroy (France), B. Moore (Canada), E. Ploedereder (Germany), J.P. Rosen (France), B. Thomas (USA), and T. Vardanega (Italy).

Special thanks go to Ada-Europe and the Ada Resource Association, without whose help and support this third edition of the Ada Standard would not have been possible. A special mention has to go to A. Beneschan (USA) for his efforts in eliminating sloppiness in our wording. M. Heaney (USA) also deserves a mention for his efforts to improve the containers packages. Finally, special thanks go to the...
convenor of ISO/IEC JTC 1/SC 22/WG 9, J. Tokar (USA), who guided the document through the standardization process.

**Acknowledgements for the Ada 2012 Corrigendum 1 version**

The editor [R. Brukardt (USA)] would like to thank the many people whose hard work and assistance has made this update possible.

Thanks go out to all of the members of the ISO/IEC JTC 1/SC 22/WG 9 Ada Rapporteur Group, whose work on creating and editing the wording changes was critical to the entire process. Especially valuable contributions came from the chairman of the ARG, J. Cousins (UK), who guided the work; T. Taft (USA), who seems to have the ability to cut any Gordian knot we encounter in wording; J. Barnes (UK) who continues to be able to find editorial errors invisible to most; S. Baird (USA), who so frequently finds obscure interactions that we now have named such things for him. Other ARG members who substantially contributed were: A. Burns (UK), R. Dewar (USA), G. Dismukes (USA), R. Duff (USA), B. Moore (Canada), E. Ploedereder (Germany), J.P. Rosen (France), E. Schonberg (USA), and T. Vardanega (Italy).

Finally, special thanks go to the convenor of ISO/IEC JTC 1/SC 22/WG 9, J. Tokar (USA), who guided the document through the standardization process.

**Acknowledgements for the Ada 2022 version**

The editor [R. Brukardt] would like to thank the many people whose hard work and assistance has made this revision possible.

Thanks go out to all of the members of the ISO/IEC JTC 1/SC 22/WG 9 Ada Rapporteur Group, whose work in all steps of the process, from determining problems to address, reviewing feature designs, and creating and editing wording changes, was critical to the entire process. Especially valuable contributions came from the chairman of the ARG through June 2018, J. Cousins, who guided the work and ensured we followed defined procedures; his replacement as chairman, S. Baird, who ably powered through obstacles to complete the work while continuing to find obscure interactions; T. Taft, who often solved difficult problems that had stumped others; B. Moore, whose frequent suggestions for parallel constructs greatly improved the result. Other ARG members who substantially contributed were: R. Amiard, J. Barnes, A. Burns, A. Charlet, G. Dismukes, C. Dross, R. Duff, E. Fish, E. Ploedereder, J.P. Rosen, F. Schanda, E. Schonberg, J. Squirek, T. Vardanega, and R. Wai.

Finally, special thanks go to the convenor of ISO/IEC JTC 1/SC 22/WG 9, P. Rogers, who guided the document through the standardization process.

**Acknowledgements for the Ada 202y version**

The editor [R. Brukardt] would like to thank the many people whose hard work and assistance has made this update possible.

Thanks go out to all of the members of the ISO/IEC JTC 1/SC 22/WG 9 Ada Rapporteur Group, whose work in all steps of the process, from determining problems to address, reviewing feature designs, and creating and editing wording changes, was critical to the entire process.

**Using this version of the Ada Reference Manual**

This document has been revised with changes for Ada 202y: the corrections specified in Technical Corrigendum 1 for Ada 2012 (which corresponds to ISO/IEC 8652:2012/COR.1:2016) and other changes specifically for this fourth edition: the corrections specified in Technical Corrigendum 1 (which
corresponds to ISO/IEC 8652:1995/COR.1:2001) and Amendment 1 (which corresponds to ISO/IEC 8652/AMD 1:2007), along with changes specifically for this third edition. In addition, more additional annotations have been added and a variety of editorial errors have been corrected.

Changes to the original 1995 version of the Annotated Ada Reference Manual (AARM) can be identified by the version number /1 following the paragraph number. Paragraphs with a version number of /1 were changed by Technical Corrigendum 1 for Ada 95 or were editorial corrections at that time, while paragraphs with a version number of /2 were changed by Amendment 1 or were more recent editorial corrections, and paragraphs with a version number of /3 were changed by the 2012 edition of the AARM (including additional editorial corrections). Paragraphs with a version number of /4 were changed by Technical Corrigendum 1 for Ada 2012 or were editorial corrections at that time. Paragraphs with a version number of /5 were changed by the 2022 edition of the AARM (including additional editorial corrections). Paragraphs with a version number of /6 were changed for Ada 202y or are recent editorial corrections. Paragraphs not so marked are unchanged since the original 1995 edition of the Annotated Ada Reference Manual, and have the same paragraph numbers as in that edition. Inserted text is indicated by underlining, and deleted text is indicated by strikethroughs. Some versions also use color to indicate the version of the change. Where paragraphs are inserted, the paragraph numbers are of the form pp.nn, where pp is the number of the preceding paragraph, and nn is an insertion number. For instance, the first paragraph inserted after paragraph 8 is numbered 8.1, the second paragraph inserted is numbered 8.2, and so on. Deleted paragraphs are indicated by text such as This paragraph was deleted. Deleted paragraphs include empty paragraphs that were numbered in the 1995 edition of the original Ada Reference Manual. Similar markings and numbering are used for changes to annotations.

To be honest: For normative text, the paragraph number is considered part of the paragraph; when a paragraph is moved to a different paragraph number, it is marked as changed even if the contents have not changed. For non-normative text such as NOTES and Examples, paragraph numbers of unchanged context may change without indication. This may happen if additional normative content is added to a subclause.
1 General

Ada is a programming language designed to support the construction of long-lived, highly reliable software systems. The language includes facilities to define packages of related types, objects, and operations. The packages may be parameterized and the types may be extended to support the construction of libraries of reusable, adaptable software components. The operations may be implemented as subprograms using conventional sequential control structures, or as entries that include synchronization of concurrent threads of control as part of their invocation. The language treats modularity in the physical sense as well, with a facility to support separate compilation.

The language includes a complete facility for the support of real-time, concurrent programming. Errors can be signaled as exceptions and handled explicitly. The language also covers systems programming: this requires precise control over the representation of data and access to system dependent properties. Finally, a predefined environment of standard packages is provided, including facilities for, among others, input-output, string manipulation, numeric elementary functions, and random number generation.

Discussion: This Annotated Ada Reference Manual (AARM) contains the entire text of the fourth edition of the Ada Reference Manual as updated for Ada 2012; (referred to here as the Ada 2012 RM) plus certain annotations. The annotations give a more in-depth analysis of the language. They describe the reason for each nonobvious rule, and point out interesting ramifications of the rules and interactions among the rules (interesting to language lawyers, that is). Differences between Ada 83, Ada 95, and Ada 2005, Ada 2012, Ada 2022, and Ada 95 and Ada 2005 and Ada 2012 and Ada 95 are listed. (The text you are reading now is an annotation.)

The AARM stresses detailed correctness and uniformity over readability and understandability. We're not trying to make the language “appear” simple here; on the contrary, we're trying to expose hidden complexities, so we can more easily detect language bugs. The Ada 2012 RM, on the other hand, is intended to be a more readable document for programmers.

The annotations in the AARM are as follows:

- Text that is logically redundant is shown [in square brackets, like this]. Technically, such text could be written as a Note in the Ada 2012 RM (and the Ada 95 and 2005 RMs, that is). Differences between Ada 83, Ada 95, and Ada 2005, Ada 2012, Ada 2022, and Ada 95 and Ada 2005 and Ada 2012 and Ada 95 are listed. (The text you are reading now is an annotation.)

- The rules of the language (and some AARM-only text) are categorized, and placed under certain subheadings that indicate the category. For example, the distinction between Name Resolution Rules and Legality Rules is particularly important, as explained in 8.6.

- Text under the following sub-headings appears in both documents:
  - The unlabeled text at the beginning of each clause or subclause,
  - Syntax,
  - Name Resolution Rules,
  - Legality Rules,
  - Static Semantics,
  - Post-Compilation Rules,
  - Dynamic Semantics,
  - Bounded (Run-Time) Errors,
  - Erroneous Execution,
  - Implementation Requirements,
  - Documentation Requirements,
  - Metrics,
  - Implementation Permissions,
  - Implementation Advice,
  - Usage.
• NOTES,

• Examples.

• Text under the following sub-headings does not appear in the Ada 202y202220122005 RM95:

• Language Design Principles,

• Inconsistencies With Ada 83,

• Incompatibilities With Ada 83,

• Extensions to Ada 83,

• Wording Changes from Ada 83,

• Inconsistencies With Ada 95,

• Incompatibilities With Ada 95,

• Extensions to Ada 95,

• Wording Changes from Ada 95,

• Inconsistencies With Ada 2005,

• Incompatibilities With Ada 2005,

• Extensions to Ada 2005,

• Wording Changes from Ada 2005,

• Inconsistencies With Ada 2012,

• Incompatibilities With Ada 2012,

• Extensions to Ada 2012,

• Wording Changes from Ada 2012,

• Inconsistencies With Ada 2022,

• Incompatibilities With Ada 2022,

• Extensions to Ada 2022,

• Wording Changes from Ada 2022.

• The AARM also includes the following kinds of annotations. These do not necessarily annotate the immediately preceding rule, although they often do.

  2.u
  2.v
  2.w/3
  2.x
  2.y
  2.z
  2.aa
  2.bb/2
  2.bb.1/2
  2.bb.2/2
  2.bb.3/2
  2.bb.4/3
  2.bb.5/3
  2.bb.6/3
  2.bb.7/3
  2.bb.8/4
  2.bb.9/4
  2.bb.10/4
  2.bb.11/4
  2.bb.12/4
  2.bb.13/4
  2.bb.14/4
  2.bb.15/4
  2.bb.16/4
  2.cc
  2.dd
  2.ee
  2.ff
  2.gg
  2.hh
  2.ii
  2.jj
  2.jj.1/5
  2.kk/3
  2.ll
  2.mm

Reason: An explanation of why a certain rule is necessary, or why it is worded in a certain way.

Ramification: An obscure ramification of the rules that is of interest only to language lawyers. (If a ramification of the rules is of interest to programmers, then it appears under NOTES.)

Proof: An informal proof explaining how a given Note or [marked-as-redundant] piece of text follows from the other rules of the language.

Implementation Note: A hint about how to implement a feature, or a particular potential pitfall that an implementer needs to be aware of.

Change: Change annotations are not used in this version. Changes from previous versions have been removed. Changes in this version are marked with versioned paragraph numbers, as explained in the “Corrigendum Changes” clause of the “Introduction”.

Discussion: Other annotations not covered by the above.

To be honest: A rule that is considered logically necessary to the definition of the language, but which is so obscure or pedantic that only a language lawyer would care. These are the only annotations that could be considered part of the language definition.

Term entry: {AI12-0443-1} The text of a Term and Definition entry — this text will also appear in 1.3, “Terms and Definitions”.

Discussion: In general, the Ada 202y202220122005 RM95 text appears in the normal font, whereas AARM-only text appears in a smaller font. Ada examples are also usually printed in a smaller font. Notes also appear in the smaller font, as recommended by ISO/IEC style guidelines. Ada examples are also usually printed in a smaller font.

If you have trouble finding things, be sure to use the index. Each defined term appears there, and also in italics, like this. Syntactic categories defined in BNF are also indexed.

A definition marked “[distributed]” is the main definition for a term whose complete definition is given in pieces distributed throughout the document. The pieces are marked “[partial]” or with a phrase explaining what cases the partial definition applies to.
1.1 Scope

This Reference Manual specifies the form and meaning of programs written in Ada. Its purpose is to promote the portability of Ada programs to a variety of computing systems.

Ada is a programming language designed to support the construction of long-lived, highly reliable software systems. The language includes facilities to define packages of related types, objects, and operations. The packages may be parameterized and the types may be extended to support the construction of libraries of reusable, adaptable software components. The operations may be implemented as subprograms using conventional sequential control structures, or as entries that include synchronization of concurrent threads of control as part of their invocation. Ada supports object-oriented programming by providing classes and interfaces, inheritance, polymorphism of variables and methods, and generic units. The language treats modularity in the physical sense as well, with a facility to support separate compilation.

The language provides rich support for real-time, concurrent programming, and includes facilities for multicore and multiprocessor programming. Errors can be signaled as exceptions and handled explicitly. The language also covers systems programming; this requires precise control over the representation of data and access to system-dependent properties. Finally, a predefined environment of standard packages is provided, including facilities for, among others, input-output, string manipulation, numeric elementary functions, and random number generation, and definition and use of containers.

1.1.1 Extent

This Reference Manual specifies:

- The form of a program written in Ada;
- The effect of translating and executing such a program;
- The manner in which program units can be combined to form Ada programs;
- The language-defined library units that a conforming implementation is required to supply;
- The permissible variations in conformance to the rules of this document within the standard, and the manner in which they are to be documented;
- Those violations of the requirements of this document that a conforming implementation is required to detect, and the effect of attempting to translate or execute a program containing such violations;
- Those violations of the requirements of this document that a conforming implementation is not required to detect.

This Reference Manual does not specify:

- The means whereby a program written in Ada is transformed into object code executable by a processor;
- The means whereby translation or execution of programs is invoked and the executing units are controlled;
- The size or speed of the object code, or the relative execution speed of different language constructs;
- The form or contents of any listings produced by implementations; in particular, the form or contents of error or warning messages;
• {AI12-0425-1} The effect of unspecified execution;
• The size of a program or program unit that will exceed the capacity of a particular conforming implementation.

1.1.2 Structure

{AI05-0299-1} This document contains thirteen clauses sections, fifteen annexes, and an index.

Discussion: {AI05-0299-1} What Ada 83 called a “chapter” and Ada 95 (and Ada 2005) called a “section” is called a “clause” in this Reference Manual. Similarly, what Ada 83 called a “section” and Ada 95 (and Ada 2005) called a “clause” is called a “subclause” in this Reference Manual. Confused yet? This terminology is out of our hands; it is (and was) forced by ever-changing ISO rules for drafting Reference Manuals.

The core of the Ada language consists of:

• {AI05-0299-1} Clauses Sections 1 through 13
• Annex A, “Predefined Language Environment”
• Annex B, “Interface to Other Languages”
• Annex J, “Obsolescent Features”

Term entry: core language — clause or annex in which are defined language constructs or capabilities that are provided by all conforming implementations
Note: A construct is said to be part of the core language if it is defined in a core language clause or annex.

The following Specialized Needs Annexes define features that are needed by certain application areas:

• Annex C, “Systems Programming”
• Annex D, “Real-Time Systems”
• Annex E, “Distributed Systems”
• Annex F, “Information Systems”
• Annex G, “Numerics”
• Annex H, “High Integrity Systems”

Term entry: specialized needs annex — annex in which are defined language constructs or capabilities that are not necessarily provided by all conforming implementations

The core language and the Specialized Needs Annexes are normative, except that the material in each of the items listed below is informative:

• Text under a NOTES or Examples heading.

{AI05-0299-1} Each clause or subclause whose title starts with the word “Example” or “Examples”.

All implementations shall conform to the core language. In addition, an implementation may conform separately to one or more Specialized Needs Annexes.

The following Annexes are informative:

• Annex K, “Language-Defined Aspects and Attributes”
• Annex L, “Language-Defined Pragmas”


• Annex N, “Glossary”
• Annex P, “Syntax Summary”
• {AI05-0262-1} Annex Q, “Language-Defined Entities”

**Discussion:** The idea of the Specialized Needs Annexes is that implementations can choose to target certain application areas. For example, an implementation specifically targeted to embedded machines might support the application-specific features for Real-time Systems, but not the application-specific features for Information Systems.

The Specialized Needs Annexes extend the core language only in ways that users, implementations, and standards bodies are allowed to extend the language; for example, via additional library units, attributes, representation items (see 13.1), pragmas, and constraints on semantic details that are left unspecified by the core language. Many implementations already provide much of the functionality defined by Specialized Needs Annexes; our goal is to increase uniformity among implementations by defining standard ways of providing the functionality.

{AI95-00114-01} We recommend that the certification/validation procedures allow implementations to certify/validate the core language, plus any set of the Specialized Needs Annexes. We recommend that implementations not be allowed to certify/validate a portion of one of the Specialized Needs Annexes, although implementations can, of course, provide uncertified/unvalidated support for such portions. We have designed the Specialized Needs Annexes assuming that this recommendation is followed. Thus, our decisions about what to include and what not to include in those annexes are based on the assumption that each annex is certified/validated in an “all-or-nothing” manner.

An implementation may, of course, support extensions that are different from (but possibly related to) those defined by one of the Specialized Needs Annexes. We recommend that, where appropriate, implementations do this by adding library units that are children of existing language-defined library packages.

An implementation should not provide extensions that conflict with those defined in the Specialized Needs Annexes, in the following sense: Suppose an implementation supports a certain error-free program that uses only functionality defined in the core and in the Specialized Needs Annexes. The implementation should ensure that that program will still be error free in some possible full implementation of all of the Specialized Needs Annexes, and that the semantics of the program will not change. For example, an implementation should not provide a package with the same name as one defined in one of the Specialized Needs Annexes, but that behaves differently, even if that implementation does not claim conformance to that Annex.

Note that the Specialized Needs Annexes do not conflict with each other; it is the intent that a single implementation can conform to all of them.

{AI05-0299-1} {AI12-0056-1} Each clause section is divided into clauses and subclauses that have a common structure. Each section, clause, and subclause first introduces its subject. After the introductory text, text is labeled with the following headings:

**Language Design Principles**

These are not rules of the language, but guiding principles or goals used in defining the rules of the language. In some cases, the goal is only partially met; such cases are explained.

{AI05-0005-1} This is not part of the definition of the language, and does not appear in the Ada 2022/2012/2005 RM.

**Syntax**

Syntax rules (indented).

{AI05-0299-1} Compile-time rules that are used in name resolution, including overload resolution.

**Discussion:** These rules are observed at compile time. (We say “observed” rather than “checked”, because these rules are not individually checked. They are really just part of the Legality Rules in Clause Section 8 that require exactly one interpretation of each constituent of a complete context.) The only rules used in overload resolution are the Syntax Rules and the Name Resolution Rules.

When dealing with nonoverloadable declarations it sometimes makes no semantic difference whether a given rule is a Name Resolution Rule or a Legality Rule, and it is sometimes difficult to decide which it should be. We generally make a given rule a Name Resolution Rule only if it has to be. For example, “The name, if any, in a raise_statement shall be the name of an exception.” is under “Legality Rules.”
Legality Rules

Rules that are enforced at compile time. A construct is legal if it obeys all of the Legality Rules.

Discussion: These rules are not used in overload resolution.

Note that run-time errors are always attached to exceptions; for example, it is not “illegal” to divide by zero, it just raises an exception.

Static Semantics

A definition of the compile-time effect of each construct.

Discussion: The most important compile-time effects represent the effects on the symbol table associated with declarations (implicit or explicit). In addition, we use this heading as a bit of a grab bag for equivalences, package specifications, etc. For example, this is where we put statements like so-and-so is equivalent to such-and-such. (We ought to try to really mean it when we say such things!) Similarly, statements about magically-generated implicit declarations go here. These rules are generally written as statements of fact about the semantics, rather than as a you-shall-do-such-and-such sort of thing.

Post-Compilation Rules

Rules that are enforced before running a partition. A partition is legal if its compilation units are legal and it obeys all of the Post-Compilation Rules.

Discussion: It is not specified exactly when these rules are checked, so long as they are checked for any given partition before that partition starts running. An implementation may choose to check some such rules at compile time, and reject compilation units accordingly. Alternatively, an implementation may check such rules when the partition is created (usually known as “link time”), or when the partition is mapped to a particular piece of hardware (but before the partition starts running).

Dynamic Semantics

A definition of the run-time effect of each construct.

Discussion: This heading describes what happens at run time. Runtime checks, which raise exceptions upon failure, are described here. Each item that involves a runtime check is marked with the name of the check — these are the same check names that are used in a pragma Suppress. Principle: Every check should have a name, usable in a pragma Suppress.

Bounded (Run-Time) Errors

Situations that result in bounded (run-time) errors (see 1.1.5).

Discussion: The “bounds” of each such error are described here — that is, we characterize the set of all possible behaviors that can result from a bounded error occurring at run time.

Erroneous Execution

Situations that result in erroneous execution (see 1.1.5).

Implementation Requirements

Additional requirements for conforming implementations.

Discussion: ...as opposed to rules imposed on the programmer. An example might be, “The smallest representable duration, Duration'Small, shall not be greater than twenty milliseconds”.

It's really just an issue of how the rule is worded. We could write the same rule as “The smallest representable duration is an implementation-defined value less than or equal to 20 milliseconds” and then it would be under “Static Semantics”.

Documentation Requirements

Documentation requirements for conforming implementations.

Discussion: These requirements are beyond those that are implicitly specified by the phrase “implementation defined”. The latter require documentation as well, but we don't repeat these cases under this heading. Usually this heading is
used for when the description of the documentation requirement is longer and does not correspond directly to one, narrow normative sentence.

**Metrics**

Metrics that are specified for the time/space properties of the execution of certain language constructs.

**Implementation Permissions**

Additional permissions given to the implementer.

**Discussion:** For example, “The implementation is allowed to impose further restrictions on the record aggregates allowed in code statements.” When there are restrictions on the permission, those restrictions are given here also. For example, “An implementation is allowed to restrict the kinds of subprograms that are allowed to be main subprograms. However, it shall support at least parameterless procedures.” — we don’t split this up between here and “Implementation Requirements”.

**Implementation Advice**

Optional advice given to the implementer. The word “should” is used to indicate that the advice is a recommendation, not a requirement. It is implementation defined whether or not a given recommendation is obeyed.

**Implementation defined:** Whether or not each recommendation given in Implementation Advice is followed ___ see M.3 for a listing.

**Discussion:** The advice generally shows the intended implementation, but the implementer is free to ignore it. The implementer is the sole arbiter of whether or not the advice has been obeyed, if not, whether the reason is a good one, and whether the required documentation is sufficient. It would be wrong for the ACATS/ACVC to enforce any of this advice.

For example, “Whenever possible, the implementation should choose a value no greater than fifty microseconds for the smallest representable duration, Duration'Small.”

We use this heading, for example, when the rule is so low level or implementation-oriented as to be untestable. We also use this heading when we wish to encourage implementations to behave in a certain way in most cases, but we do not wish to burden implementations by requiring the behavior.

**Usage**

Advice and notes on the usage of Ada programming language. This material is informative.

**Discussion:** Traditionally, this information has been given in notes; however, the current ISO/IEC JTC1 drafting standard does not allow giving advice in notes. Therefore, this information has been moved to its own category in order to keep it separate from advice and notes intended for implementers.

**NOTE** Notes emphasize consequences of the rules described in the (sub)clause or elsewhere. This material is informative.

**Examples**

Examples illustrate the possible forms of the constructs described. This material is informative.

**Discussion:** [AI12-0386-1] Names used in examples refer either to language-defined entities or to entities declared in other Examples in this Reference Manual. In the latter case, if the reference is to a later example, we use a cross-reference (See <<some clause>>) to show the source of the declaration. In theory, one could combine all of the examples (excepting examples of fragments like identifiers or type definitions) in an appropriate unit and compile them all.

The next three headings list all language changes between Ada 83 and Ada 95. Language changes are any change that changes the set of text strings that are legal Ada programs, or changes the meaning of any legal program. Wording changes, such as changes in terminology, are not language changes. Each language change falls into one of the following three categories:
Inconsistencies With Ada 83

This heading lists all of the upward inconsistencies between Ada 83 and Ada 95. Upward inconsistencies are situations in which a legal Ada 83 program is a legal Ada 95 program with different semantics. This type of upward incompatibility is the worst type for users, so we only tolerate it in rare situations.

(Note that the semantics of a program is not the same thing as the behavior of the program. Because of Ada's indeterminacy, the “semantics” of a given feature describes a set of behaviors that can be exhibited by that feature. The set can contain more than one allowed behavior. Thus, when we ask whether the semantics changes, we are asking whether the set of behaviors changes.)

This is not part of the definition of the language, and does not appear in the Ada 95, or Ada 2005, Ada 2012, or Ada 2022, or Ada 2012 RM.

Incompatibilities With Ada 83

This heading lists all of the upward incompatibilities between Ada 83 and Ada 95, except for the ones listed under “Inconsistencies With Ada 83” above. These are the situations in which a legal Ada 83 program is illegal in Ada 95. We do not generally consider a change that turns erroneous execution into an exception, or into an illegality, to be upwardly incompatible.

This is not part of the definition of the language, and does not appear in the Ada 95, or Ada 2005, Ada 2012, or Ada 2022, or Ada 2012 RM.

Extensions to Ada 83

This heading is used to list all upward compatible language changes; that is, language extensions. These are the situations in which a legal Ada 95 program is not a legal Ada 83 program. The vast majority of language changes fall into this category.

This is not part of the definition of the language, and does not appear in the Ada 95, or Ada 2005, Ada 2012, or Ada 2022, or Ada 2012 RM.

As explained above, the next heading does not represent any language change:

Wording Changes from Ada 83

This heading lists some of the nonsemantic changes between the Ada 83 RM and the Ada 95 RM. It is incomplete; we have not attempted to list all wording changes, but only the “interesting” ones.

This is not part of the definition of the language, and does not appear in the Ada 95, or Ada 2005, Ada 2012, or Ada 2022, or Ada 2012 RM.

Discussion:

The next three headings list all language changes between Ada 95 and Ada 2005 (the language defined by the Ada 95 standard plus Technical Corrigendum 1 plus Amendment 1). Each language change falls into one of the following three categories:

Inconsistencies With Ada 95

This heading lists all of the upward inconsistencies between Ada 95 and Ada 2005. Upward inconsistencies are situations in which a legal Ada 95 program is a legal Ada 2005 program with different semantics.

Inconsistencies marked with Corrigendum: are corrections to the original Ada 95 definition introduced by Corrigendum 1. Inconsistencies marked with Amendment Correction: are corrections to the original Ada 95 definition added by Amendment 1. Formally, these are inconsistencies caused by Ada Issues classified as Binding Interpretations; implementations of Ada 95 are supposed to follow these corrections, not the original flawed language definition. Thus, these strictly speaking are not inconsistencies between Ada 95 and Ada 2005. Practically, however, they very well may be, as early Ada 95 implementations might not follow the recommendation. Inconsistencies so marked are not portable between Ada 95 implementations, while usually Ada 2005 will have more clearly defined behavior. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in the Ada 2005, Ada 2012, or Ada 2022 RM.

Incompatibilities With Ada 95

This heading lists all of the upward incompatibilities between Ada 95 and Ada 2005, except for the ones listed under “Inconsistencies With Ada 95” above. These are the situations in which a legal Ada 95 program is illegal in Ada 2005.
As with inconsistencies, incompatibilities marked with **Corrigendum:** are corrections to the original Ada 95 definition introduced by Corrigendum 1. Incompatibilities marked with **Amendment Correction:** are corrections to the original Ada 95 definition added by Amendment 1. Formally, these are incompatibilities caused by Ada Issues classified as Binding Interpretations; implementations of Ada 95 are supposed to follow these corrections, not the original flawed language definition. Thus, these strictly speaking are not incompatibilities between Ada 95 and Ada 2005. Practically, however, they very well may be, as early Ada 95 implementations might not follow the recommendation. Therefore, some Ada 95 implementations may be able to compile the examples, while others might not. In contrast, Ada 2005 compilers will have consistent behavior. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in the Ada 2005, Ada 2012, or Ada 2022 RM.

### Extensions to Ada 95

This heading is used to list all upward compatible language changes; that is, language extensions. These are the situations in which a legal Ada 2005 program is not a legal Ada 95 program. The vast majority of language changes fall into this category.

As with incompatibilities, extensions marked with **Corrigendum:** are corrections to the original Ada 95 definition introduced by Corrigendum 1. Extensions marked with **Amendment Correction:** are corrections to the original Ada 95 definition added by Amendment 1. Formally, these are extensions allowed by Ada Issues classified as Binding Interpretations. As corrections, implementations of Ada 95 are allowed to implement these extensions. Thus, these strictly speaking are not extensions of Ada 95; they're part of Ada 95. Practically, however, they very well may be extensions, as early Ada 95 implementations might not implement the extension. Therefore, some Ada 95 implementations may be able to compile the examples, while others might not. In contrast, Ada 2005 compilers will always support the extensions. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in the Ada 2005, Ada 2012, or Ada 2022 RM.

---

As explained above, the next heading does not represent any language change:

### Wording Changes from Ada 95

This heading lists some of the nonsemantic changes between the Ada 95 RM and the Ada 2005 RM. This heading lists only “interesting” changes (for instance, editorial corrections are not listed). Changes which come from Technical Corrigendum 1 are marked **Corrigendum:**; unmarked changes come from Amendment 1.

This is not part of the definition of the language, and does not appear in the Ada 2005, Ada 2012, or Ada 2022 RM.

### Discussion:

The next three headings list all language changes between Ada 2005 (the language defined by the Ada 95 standard plus Technical Corrigendum 1 plus Amendment 1) and Ada 2012 (the language defined by the third edition of the Reference Manual). Each language change falls into one of the following three categories:

#### Inconsistencies With Ada 2005

This heading lists all of the upward inconsistencies between Ada 2005 and Ada 2012. Upward inconsistencies are situations in which a legal Ada 2005 program is a legal Ada 2012 program with different semantics.

Inconsistencies marked with **Correction:** are corrections to the original Ada 2005 definition added by the third edition of the Reference Manual. Formally, these are inconsistencies caused by Ada Issues classified as Binding Interpretations; implementations of Ada 2005 are supposed to follow these corrections, not the original flawed language definition. Thus, these strictly speaking are not inconsistencies between Ada 2005 and Ada 2012. Practically, however, they very well may be, as early Ada 2005 implementations might not follow the recommendation. Inconsistencies so marked are not portable between Ada 2005 implementations, while usually Ada 2012 will have more clearly defined behavior. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in the Ada 2012 or Ada 2022 RM.

#### Incompatibilities With Ada 2005

This heading lists all of the upward incompatibilities between Ada 2005 and Ada 2012, except for the ones listed under “Inconsistencies With Ada 2005” above. These are the situations in which a legal Ada 2005 program is illegal in Ada 2012.
As with inconsistencies, incompatibilities marked with **Correction**: are corrections to the original Ada 2005 definition added by the third edition. Formally, these are incompatibilities caused by Ada Issues classified as Binding Interpretations; implementations of Ada 2005 are supposed to follow these corrections, not the original flawed language definition. Thus, these strictly speaking are not incompatibilities between Ada 2005 and Ada 2012. Practically, however, they very well may be, as early Ada 2005 implementations might not follow the recommendation. Therefore, some Ada 2005 implementations may be able to compile the examples, while others might not. In contrast, Ada 2012 compilers will have consistent behavior. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in the Ada 2012 or Ada 2022 RM.

---

**Extensions to Ada 2005**

This heading is used to list all upward compatible language changes; that is, language extensions. These are the situations in which a legal Ada 2012 program is not a legal Ada 2005 program. The vast majority of language changes fall into this category.

As with incompatibilities, extensions marked with **Correction**: are corrections to the original Ada 2005 definition added by the third edition. Formally, these are extensions allowed by Ada Issues classified as Binding Interpretations. As corrections, implementations of Ada 2005 (and sometimes Ada 95) are allowed to implement these extensions. Thus, these strictly speaking are not extensions of Ada 2005; they're part of Ada 2005. Practically, however, they very well may be extensions, as early Ada 2005 implementations might not implement the extensions. Therefore, some Ada 2005 implementations may be able to compile the examples, while others might not. In contrast, Ada 2012 compilers will always support the extensions. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in the Ada 2012 or Ada 2022 RM.

---

**Wording Changes from Ada 2005**

This heading lists some of the nonsemantic changes between the Ada 2005 RM and the Ada 2012 RM. This heading lists only “interesting” changes (for instance, editorial corrections are not listed). Items marked **Correction**: come from Ada Issues classified as Binding Interpretations and strictly speaking belong to Ada 2005; other items only belong to Ada 2012.

This is not part of the definition of the language, and does not appear in the Ada 2012 or Ada 2022 RM.

**Discussion:**

The next three headings list all language changes between Ada 2012 (the language defined by ISO/IEC 8652:2012(E)) and Ada 2022 (the language defined by unmodified ISO/IEC 8652:2012(E)) and current Ada 2012 (the language defined by ISO/IEC 8652:2012(E) as corrected by the Corrigendum ISO/IEC 8652:2012/Cor 1:2016). Each language change falls into one of the following three categories:

**Inconsistencies With Ada 2012**

This heading lists all of the upward inconsistencies between Ada 2012 and Ada 2022. Upward inconsistencies are situations in which a legal Ada 2012 program is a legal Ada 2022 program with different semantics.

Inconsistencies marked with **Corrigendum**: are corrections to the original Ada 2012 definition added by Technical Corrigendum 1 to Ada 2012. Inconsistencies marked with **Correction**: are corrections to the original Ada 2012 definition added by this edition of the Reference Manual. Formally, these are inconsistencies caused by Ada Issues classified as Binding Interpretations; implementations of Ada 2012 are supposed to follow these corrections, not the original flawed language definition. Thus, these strictly speaking are not inconsistencies between Ada 2012 and Ada 2022. Practically, however, they very well may be, as early Ada 2012 implementations might not follow the recommendation. Inconsistencies so marked are not portable between Ada 2012 implementations, while usually Ada 2022 will have more clearly defined behavior. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in any version of the Ada RM.

**Incompatibilities With Ada 2012**

This heading lists all of the upward incompatibilities between Ada 2012 and Ada 2022, except for the ones listed under “Inconsistencies With Ada 2012” above. These are the situations in which a legal Ada 2012 program is illegal in Ada 2022.
As with inconsistencies, incompatibilities marked with **Corrigendum:** are corrections to the original Ada 2012 definition added by Corrigendum 1 to Ada 2012, and incompatibilities marked with **Correction:** are corrections to the original Ada 2012 definition added by this edition. Formally, these are incompatibilities caused by Ada Issues classified as Binding Interpretations; implementations of Ada 2012 are supposed to follow these corrections, not the original flawed language definition. Thus, these strictly speaking are not incompatibilities between Ada 2012 and Ada 202y. Practically, however, they very well may be, as early Ada 2012 implementations might not follow the recommendation. Therefore, some Ada 2012 implementations may be able to compile the examples, while others might not. In contrast, Ada 2022 compilers will have consistent behavior. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in any version of the Ada RM.

**Extensions to Ada 2012**

This heading is used to list all upward compatible language changes; that is, language extensions. These are the situations in which a legal Ada 2022 program is not a legal Ada 2012 current Ada 2012 program is not a legal original Ada 2012 program. The vast majority of language changes fall into this category.

As with incompatibilities, extensions marked with **Corrigendum:** are corrections to the original Ada 2012 definition added by Corrigendum 1 to Ada 2012, and extensions marked with **Correction:** are corrections to the original Ada 2012 definition added by this edition. Formally, these are extensions allowed by Ada Issues classified as Binding Interpretations. As corrections, implementations of Ada 2012 (and sometimes Ada 95) are allowed to implement these extensions. Thus, these strictly speaking are not extensions of Ada 2012; they're part of Ada 2012. Practically, however, they very well may be extensions, as early Ada 2012 implementations might not implement the extension. Therefore, some Ada 2012 implementations may be able to compile the examples, while others might not. In contrast, Ada 2022 compilers will always support the extensions. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in any version of the Ada RM.

As explained above, the next heading does not represent any language change:

**Wording Changes from Ada 2012**

This heading lists some of the nonsemantic changes between the Ada 2012 RM and the Ada 2022 RM original and corrected Ada 2012 RM. This heading lists only “interesting” changes (for instance, editorial corrections are not listed). Items marked **Corrigendum:** are included in Corrigendum 1 to Ada 2012, and items marked with **Correction:** are added by this edition. In both cases, these items come from Ada Issues classified as Binding Interpretations and strictly speaking belong to Ada 2012; other items only belong to Ada 2022.

This is not part of the definition of the language, and does not appear in any version of the Ada RM.

**Discussion:**

The next three headings list all language changes between original Ada 2022 (the language defined by unmodified ISO/IEC 8652:2023(E)) and Ada 202y (the language defined by this draft). Each language change falls into one of the following three categories:

**Inconsistencies With Ada 2022**

This heading lists all of the upward inconsistencies between original Ada 2022 and current Ada 202y. Upward inconsistencies are situations in which a legal Ada 2022 program is a legal Ada 202y program with different semantics.

Inconsistencies marked with **Corrigendum:** are corrections to the original Ada 2022 definition added by this edition of the Reference Manual. Formally, these are inconsistencies caused by Ada Issues classified as Binding Interpretations; implementations of Ada 2022 are supposed to follow these corrections, not the original flawed language definition. Thus, these strictly speaking are not inconsistencies between Ada 2022 and Ada 202y. Practically, however, they very well may be, as early Ada 2022 implementations might not follow the recommendation. Inconsistencies so marked are not portable between Ada 2022 implementations, while usually Ada 202y will have more clearly defined behavior. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in any version of the Ada RM.

**Incompatibilities With Ada 2022**

This heading lists all of the upward incompatibilities between Ada 2022 and Ada 202y except for the ones listed under “Inconsistencies With Ada 2022” above. These are the situations in which a legal Ada 2022 program is illegal in Ada 202y.
As with inconsistencies, incompatibilities marked with Corrigendum: are corrections to the original Ada 2022 definition added by this edition. Formally, these are incompatibilities caused by Ada Issues classified as Binding Interpretations; implementations of Ada 2022 are supposed to follow these corrections, not the original flawed language definition. Thus, these strictly speaking are not incompatibilities between Ada 2022 and Ada 202y; Practically, however, they very well may be, as early Ada 2022 implementations might not follow the recommendation. Therefore, some Ada 2022 implementations may be able to compile the examples, while others might not. In contrast, Ada 202y compilers will have consistent behavior. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in any version of the Ada RM.

Extensions to Ada 2022

As with incompatibilities, extensions marked with Corrigendum: are corrections to the original Ada 2022 definition added by this edition. Formally, these are extensions allowed by Ada Issues classified as Binding Interpretations. As corrections, implementations of Ada 2022 (and sometimes previous versions) are allowed to implement these extensions. Thus, these strictly speaking are not extensions of Ada 2022; they're part of Ada 2022. Practically, however, they very well may be extensions, as early Ada 2022 implementations might not implement the extension. Therefore, some Ada 2022 implementations may be able to compile the examples, while others might not. In contrast, Ada 202y compilers will always support the extensions. Therefore, we document these for completeness.

This is not part of the definition of the language, and does not appear in any version of the Ada RM.

As explained above, the next heading does not represent any language change:

Wording Changes from Ada 2022

This heading lists some of the nonsensematic changes between the Ada 2022 RM and the Ada 202y RM. This heading lists only “interesting” changes (for instance, editorial corrections are not listed). Items marked Corrigendum: are added by this edition. These items come from Ada Issues classified as Binding Interpretations and strictly speaking belong to Ada 2022; other items only belong to Ada 202y.

This is not part of the definition of the language, and does not appear in any version of the Ada RM.

1.1.3 Conformity of an Implementation with the Standard

Implementation Requirements

A conforming implementation shall:

1. **Discussion:** The implementation is the software and hardware that implements the language. This includes compiler, linker, operating system, hardware, etc.

   We first define what it means to “conform” in general — basically, the implementation has to properly implement the normative rules given throughout the Reference Manual. Then we define what it means to conform to a Specialized Needs Annex — the implementation must support the core features plus the features of that Annex. Finally, we define what it means to “conform to the Reference Manual” — this requires support for the core language, and allows partial (but not conflicting) support for the Specialized Needs Annexes.

2. • Translate and correctly execute legal programs written in Ada, provided that they are not so large as to exceed the capacity of the implementation;

3. • Identify all programs or program units that are so large as to exceed the capacity of the implementation (or raise an appropriate exception at run time);

   **Implementation defined:** Capacity limitations of the implementation.

4. • Identify all programs or program units that contain errors whose detection is required by this Reference Manual;
Discussion: Note that we no longer use the term “rejection” of programs or program units. We require that programs or program units with errors or that exceed some capacity limit be “identified”. The way in which errors or capacity problems are reported is not specified.

An implementation is allowed to use standard error-recovery techniques. We do not disallow such techniques from being used across compilation_unit or compilation_unit boundaries.

See also the Implementation Requirements of 10.2, which disallow the execution of illegal partitions.

- Supply all language-defined library units required by this Reference Manual;

Implementation Note: An implementation cannot add to or modify the visible part of a language-defined library unit, except where such permission is explicitly granted, unless such modifications are semantically neutral with respect to the client compilation units of the library unit. An implementation defines the contents of the private part and body of language-defined library units.

An implementation can add with_clauses and use_clauses, since these modifications are semantically neutral to clients. (The implementation might need with_clauses in order to implement the private part, for example.) Similarly, an implementation can add a private part even in cases where a private part is not shown in the Reference Manual. Explicit declarations can be provided implicitly or by renaming, provided the changes are semantically neutral.

Wherever in the Reference Manual the text of a language-defined library unit contains an italicized phrase starting with “implementation-defined”, the implementation's version will replace that phrase with some implementation-defined text that is syntactically legal at that place, and follows any other applicable rules.

Note that modifications are permitted, even if there are other tools in the environment that can detect the changes (such as a program library browser), so long as the modifications make no difference with respect to the static or dynamic semantics of the resulting programs, as defined by the Reference Manual.

- Contain no variations except those explicitly permitted by this Reference Manual, or those that are impossible or impractical to avoid given the implementation's execution environment;

Implementation defined: Variations from the standard that are impractical to avoid given the implementation's execution environment.

Reason: The “impossible or impractical” wording comes from AI-325. It takes some judgement and common sense to interpret this. Restricting compilation units to less than 4 lines is probably unreasonable, whereas restricting them to less than 4 billion lines is probably reasonable (at least given today's technology). We do not know exactly where to draw the line, so we have to make the rule vague.

- Specify all such variations in the manner prescribed by this Reference Manual.

The external effect of the execution of an Ada program is defined in terms of its interactions with its external environment. The following are defined as external interactions:

- Any interaction with an external file (see A.7);

- The execution of certain code_statements (see 13.8); which code_statements cause external interactions is implementation defined.

Implementation defined: Which code_statements cause external interactions.

- Any call on an imported subprogram (see Annex B), including any parameters passed to it;

- Any result returned or exception propagated from a main subprogram (see 10.2) or an exported subprogram (see Annex B) to an external caller;

Discussion: By “result returned” we mean to include function results and values returned in [in] out parameters.

[8652/0094] [AI95-00119-01] The lack of a result from a program that does not terminate is also included here.

- [Any read or update of an atomic or volatile object (see C.6);]

- The values of imported and exported objects (see Annex B) at the time of any other interaction with the external environment.

To be honest: [AI05-0229-1] Also other uses of imported and exported entities, as defined by the implementation, if the implementation supports such importing or exporting pragmas.
A conforming implementation of this Reference Manual shall produce for the execution of a given Ada program a set of interactions with the external environment whose order and timing are consistent with the definitions and requirements of this Reference Manual for the semantics of the given program.

**Ramification:** There is no need to produce any of the “internal effects” defined for the semantics of the program — all of these can be optimized away — so long as an appropriate sequence of external interactions is produced.

**Discussion:** See also 11.6 which specifies various liberties associated with optimizations in the presence of language-defined checks, that could change the external effects that might be produced. These alternative external effects are still consistent with the standard, since 11.6 is part of the standard.

Note also that we only require “an appropriate sequence of external interactions” rather than “the same sequence...” An optimizer may cause a different sequence of external interactions to be produced than would be produced without the optimizer, so long as the new sequence still satisfies the requirements of the standard. For example, optimization might affect the relative rate of progress of two concurrent tasks, thereby altering the order in which two external interactions occur.

Note that the Ada 83 RM explicitly mentions the case of an “exact effect” of a program, but since so few programs have their effects defined that exactly, we don’t even mention this “special” case. In particular, almost any program that uses floating point or tasking has to have some level of inexactness in the specification of its effects. And if one includes aspects of the timing of the external interactions in the external effect of the program (as is appropriate for a real-time language), no “exact effect” can be specified. For example, if two external interactions initiated by a single task are separated by a “delay 1.0;” then the language rules imply that the two external interactions have to be separated in time by at least one second, as defined by the clock associated with the delay_relative_statement. This in turn implies that the time at which an external interaction occurs is part of the characterization of the external interaction, at least in some cases, again making the specification of the required “exact effect” impractical.

**AI112-0441-1** An implementation that conforms to this Reference Manual shall support each capability required by the core language as specified. In addition, an implementation that conforms to this Reference Manual may conform to one or more Specialized Needs Annexes (or to none). Conformance to a Specialized Needs Annex means that each capability required by the Annex shall be provided as specified.

**Discussion:** The last sentence defines what it means to say that an implementation conforms to a Specialized Needs Annex, namely, only by supporting all capabilities required by the Annex.

**AI05-0229-1** An implementation conforming to this Reference Manual may provide additional aspects, attributes, library units, and pragmas. However, it shall not provide any aspect, attribute, library unit, or pragma having the same name as an aspect, attribute, library unit, or pragma (respectively) specified in a Specialized Needs Annex unless the provided construct is either as specified in the Specialized Needs Annex or is more limited in capability than that required by the Annex. A program that attempts to use an unsupported capability of an Annex shall either be identified by the implementation before run time or shall raise an exception at run time.

**Discussion:** The last sentence of the preceding paragraph defines what an implementation is allowed to do when it does not "conform" to a Specialized Needs Annex. In particular, the sentence forbids implementations from providing a construct with the same name as a corresponding construct in a Specialized Needs Annex but with a different syntax (e.g., an extended syntax) or quite different semantics. The phrase concerning "more limited in capability" is intended to give permission to provide a partial implementation, such as not implementing a subprogram in a package or having a restriction not permitted by an implementation that conforms to the Annex. For example, a partial implementation of the package Ada.Decimal might have Decimal.Max_Decimal_Digits as 15 (rather than the required 18). This allows a partial implementation to grow to a fully conforming implementation.

A restricted implementation might be restricted by not providing some subprograms specified in one of the packages defined by an Annex. In this case, a program that tries to use the missing subprogram will usually fail to compile. Alternatively, the implementation might declare the subprogram as abstract, so it cannot be called. Alternatively, a subprogram body might be implemented just to raise Program_Error. The advantage of this approach is that a program to be run under a fully conforming Annex implementation can be checked syntactically and semantically under an implementation that only partially supports the Annex. Finally, an implementation might provide a package declaration without the corresponding body, so that programs can be compiled, but partitions cannot be built and executed.

To ensure against wrong answers being delivered by a partial implementation, implementers are required to raise an exception when a program attempts to use an unsupported capability and this can be detected only at run time. For example, a partial implementation of Ada.Decimal might require the length of the Currency string to be 1, and hence, an exception would be raised if a subprogram were called in the package Edited_Output with a length greater than 1.
For an implementation that conforms to this Reference Manual, the implementation of a language-defined unit shall abide by all postconditions, type invariants, and default initial conditions specified for the unit by this document (see 11.4.2).

Documentation Requirements

Certain aspects of the semantics are defined to be either implementation defined or unspecified. In such cases, the set of possible effects is specified, and the implementation may choose any effect in the set. Implementations shall document their behavior in implementation-defined situations, but documentation is not required for unspecified situations. The implementation-defined characteristics are summarized in M.2.

Discussion: We used to use the term “implementation dependent” instead of “unspecified”. However, that sounded too much like “implementation defined”. Furthermore, the term “unspecified” is used in the ANSI C and POSIX standards for this purpose, so that is another advantage. We also use “not specified” and “not specified by the language” as synonyms for “unspecified”. The documentation requirement is the only difference between implementation defined and unspecified.

Note that the “set of possible effects” can be “all imaginable effects”, as is the case with erroneous execution.

The implementation may choose to document implementation-defined behavior either by documenting what happens in general, or by providing some mechanism for the user to determine what happens in a particular case.

Discussion: For example, if the Reference Manual says that library unit elaboration order is implementation defined, the implementation might describe (in its user's manual) the algorithm it uses to determine the elaboration order. On the other hand, the implementation might provide a command that produces a description of the elaboration order for a partition upon request from the user. It is also acceptable to provide cross references to existing documentation (for example, a hardware manual), where appropriate.

Note that dependence of a program on implementation-defined or unspecified functionality is not defined to be an error; it might cause the program to be less portable, however.

Documentation Requirement: The behavior of implementations in implementation-defined situations shall be documented — see M.2 for a listing.

Implementation Advice

If an implementation detects the use of an unsupported Specialized Needs Annex feature at run time, it should raise Program_Error if feasible.

Implementation Advice: Program_Error should be raised when an unsupported Specialized Needs Annex feature is used at run time.

Reason: The reason we don't require Program_Error is that there are situations where other exceptions might make sense. For example, if the Real Time Systems Annex requires that the range of System.Priority include at least 30 values, an implementation could conform to the Reference Manual (but not to the Annex) if it supported only 12 values. Since the rules of the language require Constraint_Error to be raised for out-of-range values, we cannot require Program_Error to be raised instead.

If an implementation wishes to provide implementation-defined extensions to the functionality of a language-defined library unit, it should normally do so by adding children to the library unit.

Implementation Advice: Implementation-defined extensions to the functionality of a language-defined library unit should be provided by adding children to the library unit.

Implementation Note: If an implementation has support code (“run-time system code”) that is needed for the execution of user-defined code, it can put that support code in child packages of System. Otherwise, it has to use some trick to avoid polluting the user's namespace. It is important that such tricks not be available to user-defined code (not in the standard mode, at least) — that would defeat the purpose.

NOTE {AI12-0440-1} The above requirements imply that an implementation conforming to this Reference Manual cannot support some of the capabilities required by a Specialized Needs Annex without supporting all required capabilities.

Discussion: A conforming implementation can partially support a Specialized Needs Annex. Such an implementation does not conform to the Annex, but it does conform to the Reference Manual.
1.1.4 Method of Description and Syntax Notation

The form of an Ada program is described by means of a context-free syntax together with context-dependent requirements expressed by narrative rules.

The meaning of Ada programs is described by means of narrative rules defining both the effects of each construct and the composition rules for constructs.

The context-free syntax of the language is described using a simple variant of Backus-Naur Form. In particular:

- Lower case words in a sans-serif font, some containing embedded underlines, are used to denote syntactic categories, for example:
  
  \texttt{case\_statement}

- Boldface words are used to denote reserved words, for example:
  
  \texttt{array}

- Square brackets enclose optional items. Thus the two following rules are equivalent.
  
  $\{A195-00433-01\}$ \texttt{simple\_return\_statement} \texttt{return\_statement} ::= \texttt{return} [expression];
  
  $\{A195-00433-01\}$ \texttt{simple\_return\_statement} \texttt{return\_statement} ::= \texttt{return}; | \texttt{return expression};

- Curly brackets enclose a repeated item. The item may appear zero or more times; the repetitions occur from left to right as with an equivalent left-recursive rule. Thus the two following rules are equivalent.
  
  \texttt{term} ::= \texttt{factor} \{\texttt{multiplying\_operator factor}\}
  
  \texttt{term} ::= \texttt{factor} | \texttt{term multiplying\_operator factor}

- $\{AI12-0212-1\}$ A vertical line separates alternative items, for example unless it occurs immediately after an opening curly bracket, in which case it stands for itself:
  
  $\{AI12-0212-1\}$ \texttt{constraint} ::= \texttt{scalar\_constraint} | \texttt{composite\_constraint}
  
  $\{AI12-0212-1\}$ \texttt{discrete\_choice\_list} ::= \texttt{discrete\_choice} |\texttt{discrete\_choice}

- $\{AI12-0212-1\}$ For symbols used in this notation (square brackets, curly brackets, and the vertical line), the symbols when surrounded by ' represent themselves, for example:
  
  $\{AI12-0212-1\}$ \texttt{discrete\_choice\_list} ::= \texttt{discrete\_choice} |\texttt{discrete\_choice}
  
  $\{AI12-0212-1\}$ \texttt{named\_container\_aggregate} ::= \texttt{[ container\_element\_association\_list ]}

- If the name of any syntactic category starts with an italicized part, it is equivalent to the category name without the italicized part. The italicized part is intended to convey some semantic information. For example \texttt{subtype\_name} and \texttt{task\_name} are both equivalent to \texttt{name} alone.

Discussion: The grammar given in this document is not LR(1). In fact, it is ambiguous; the ambiguities are resolved by the overload resolution rules (see 8.6).

We often use “if” to mean “if and only if” in definitions. For example, if we define “photogenic” by saying, “A type is photogenic if it has the following properties...”, we mean that a type is photogenic if \textit{and only if} it has those properties. It is usually clear from the context, and adding the “and only if” seems too cumbersome.

When we say, for example, “a declarative\_item of a declarative\_part”, we are talking about a declarative\_item immediately within that declarative\_part. When we say “a declarative\_item in, or within, a declarative\_part”, we are talking about a declarative\_item anywhere in the declarative\_part, possibly deeply nested within other declarative\_parts. (This notation doesn't work very well for names, since the name “of” something also has another meaning.)

When we refer to the name of a language-defined entity (for example, Duration), we mean the language-defined entity even in programs where the declaration of the language-defined entity is hidden by another declaration. For example, when we say that the expected type for the expression of a delay\_relative\_statement is Duration, we mean the language-defined type Duration that is declared in Standard, not some type Duration the user might have declared.
The delimiters, compound delimiters, reserved words, and numeric literals are exclusively made of the characters whose code point positions are between 16#20# and 16#7E#, inclusively. The special characters for which names are defined in this document (see 2.1) belong to the same range. [For example, the character E in the definition of exponent is the character whose name is “LATIN CAPITAL LETTER E”, not “GREEK CAPITAL LETTER EPSILON”.

**Discussion:** This just means that programs can be written in plain ASCII characters; no characters outside of the 7-bit range are required.

When this document mentions the conversion of some character or sequence of characters to upper case, it means the character or sequence of characters obtained by using simple upper case mapping locale-independent full case folding, as defined by documents referenced in the note in Clause section 21 of ISO/IEC 10646:2020.

**Implementation Note:** The “documents referenced” means Unicode, Chapter 4 (specifically, section 4.2 — Case). Machine-readable versions of Simple Uppercase Mapping and Simple Lowercase Mapping can be found in http://www.unicode.org/Public/UCD/latest/ucd/UnicodeData.txt. Data for older Unicode versions can be found on this site as well; start at http://www.unicode.org/Public/ and find the appropriate version number. Simple Uppercase Mapping is the 12th field in this file (the 13th element of each line, since Unicode counts from 0); the Simple Lowercase Mapping is the 13th field in this file. In both cases, if no character is present in the field, the character maps to itself.

A syntactic category is a nonterminal in the grammar defined in BNF under “Syntax”. Names of syntactic categories are set in a different font, like this.

A construct is a piece of text (explicit or implicit) that is an instance of a syntactic category defined under “Syntax”.

**Term entry:** construct — piece of text (explicit or implicit) that is an instance of a syntactic category defined under Syntax

**Ramification:** For example, an expression is a construct. A declaration is a construct, whereas the thing declared by a declaration is an “entity”.

**Discussion:** “Explicit” and “implicit” don’t mean exactly what you might think they mean: The text of an instance of a generic is considered explicit, even though it does not appear explicitly (in the nontechnical sense) in the program text, and even though its meaning is not defined entirely in terms of that text.

A constituent of a construct is the construct itself, or any construct appearing within it.

Whenever the run-time semantics defines certain actions to happen in an arbitrary order, this means that the implementation shall arrange for these actions to occur in a way that is equivalent to some sequential order, following the rules that result from that sequential order. When evaluations are defined to happen in an arbitrary order, with conversion of the results to some subtypes, or with some runtime checks, the evaluations, conversions, and checks may be arbitrarily interspersed, so long as each expression is evaluated before converting or checking its value. [Note that the effect of a program can depend on the order chosen by the implementation. This can happen, for example, if two actual parameters of a given call have side effects.]

**Discussion:** Programs will be more portable if their external effect does not depend on the particular order chosen by an implementation.

**Ramification:** Additional reordering permissions are given in 11.6, “Exceptions and Optimization”. There is no requirement that the implementation always choose the same order in a given kind of situation. In fact, the implementation is allowed to choose a different order for two different executions of the same construct. However, we expect most implementations will behave in a relatively predictable manner in most situations.
18.d **Reason:** The “sequential order” wording is intended to allow the programmer to rely on “benign” side effects. For example, if \( F \) is a function that returns a unique integer by incrementing some global and returning the result, a call such as \( P(F, F) \) is OK if the programmer cares only that the two results of \( F \) are unique; the two calls of \( F \) cannot be executed in parallel, unless the compiler can prove that parallel execution is equivalent to some sequential order.

19 **NOTE 1** The syntax rules describing structured constructs are presented in a form that corresponds to the recommended paragraphing. For example, an if_statement is defined as:

```markdown
if_statement ::= if condition then sequence_of_statements
[elsif condition then sequence_of_statements]
else sequence_of_statements end if;
```

20 **NOTE 2** The line breaks and indentation in the syntax rules indicate the recommended line breaks and indentation in the corresponding constructs. The preferred places for other line breaks are after semicolons.

### Wording Changes from Ada 95

21.a/2 \{AI95-00285-01\} We now explicitly say that the lexical elements of the language (with a few exceptions) are made up of characters in the lower half of the Latin-1 character set. This is needed to avoid confusion given the new capability to use most ISO 10646 characters in identifiers and strings.

21.b/2 \{AI95-00395-01\} We now explicitly define what the Reference Manual means by upper case, as there are many possibilities for ISO 10646 characters.

21.c/2 \{AI95-00433-01\} The example for square brackets has been changed as there is no longer a return_statement syntax rule.

### Wording Changes from Ada 2005

21.d/3 \{AI05-0227-1\} **Correction:** Upper case is defined by "simple upper case mapping", because "full case folding" is a mapping (mostly) to lower case.

### Wording Changes from Ada 2012

21.e/5 \{AI12-0212-1\} Changed the syntax description to quote symbols used in the notation when they appear as themselves. We made this change to allow square brackets in Ada syntax, but the change also allowed us to get rid of an old hack which allowed vertical lines to stand for themselves in limited circumstances.

### 1.1.5 Classification of Errors

#### Language Design Principles

0.a/5 \{AI12-0204-1\} When the Reference Manual says that some construct \( C_1 \) has equivalent dynamic semantics to some other construct \( C_2 \), then there should be a language rule that says that \( C_1 \) is illegal if \( C_2 \) is illegal.

0.b/5 **Reason:** \{AI12-0204-1\} We do not want to infer Legality Rules from Dynamic Semantics rules.

0.c/5 \{AI12-0064-2\} When the value of an expression is needed to enforce a Legality Rule or Post-Compilation Rule, then there should be a language rule requiring the expression to be static (see 4.9).

0.d/5 **Discussion:** \{AI12-0064-2\} This most likely occurs when the expression specifies the value of an aspect.

#### Implementation Requirements

1 The language definition classifies errors into several different categories:

- Errors that are required to be detected prior to run time by every Ada implementation;

2 These errors correspond to any violation of a rule given in this document, other than those listed below. In particular, violation of any rule that uses the terms shall, allowed, permitted, legal, or illegal belongs to this category. Any program that contains such an error is not a legal Ada program; on the other hand, the fact that a program is legal does not mean, *per se*, that the program is free from other forms of error.
The rules are further classified as either compile time rules, or post compilation rules, depending on whether a violation has to be detected at the time a compilation unit is submitted to the compiler, or may be postponed until the time a compilation unit is incorporated into a partition of a program.

**Ramification:** See, for example, 10.1.3, “Subunits of Compilation Units”, for some errors that are detected only after compilation. Implementations are allowed, but not required, to detect post compilation rules at compile time when possible.

- **Errors that are required to be detected at run time by the execution of an Ada program;**
  
  The corresponding error situations are associated with the names of the predefined exceptions. Every Ada compiler is required to generate code that raises the corresponding exception if such an error situation arises during program execution. [If such an error situation is certain to arise in every execution of a construct, then an implementation is allowed (although not required) to report this fact at compilation time.]

- **Bounded errors;**
  
  \{AI12-0444-1\} The language rules define certain kinds of errors that are not expected to need not be detected either prior to or during run time, but if not detected, the range of possible effects shall be bounded. The errors of this category are called *bounded errors*. The possible effects of a given bounded error are specified for each such error, but in any case one possible effect of a bounded error is the raising of the exception `Program_Error`.

- **Erroneous execution.**
  
  \{AI12-0444-1\} In addition to bounded errors, the language rules define certain kinds of errors as leading to *erroneous execution*. Like bounded errors, the implementation is not expected to detect such errors either prior to or during run time. Unlike bounded errors, there is no language-specified bound on the possible effect of erroneous execution; the effect is in general not predictable.

  **Ramification:** Executions are erroneous, not programs or parts of programs. Once something erroneous happens, the execution of the entire program is erroneous from that point on, and potentially before given possible reorderings permitted by 11.6 and elsewhere. We cannot limit it to just one partition, since partitions are not required to live in separate address spaces. (But implementations are encouraged to limit it as much as possible.)

  Suppose a program contains a pair of things that will be executed “in an arbitrary order”. It is possible that one order will result in something sensible, whereas the other order will result in erroneous execution. If the implementation happens to choose the first order, then the execution is not erroneous. This may seem odd, but it is not harmful.

  Saying that something is erroneous is semantically equivalent to saying that the behavior is unspecified. However, “erroneous” has a slightly more disapproving flavor.

**Implementation Permissions**

[ An implementation may provide *nonstandard modes* of operation. Typically these modes would be selected by a *pragma* or by a command line switch when the compiler is invoked. When operating in a nonstandard mode, the implementation may reject *compilation_units* that do not conform to additional requirements associated with the mode, such as an excessive number of warnings or violation of coding style guidelines. Similarly, in a nonstandard mode, the implementation may apply special optimizations or alternative algorithms that are only meaningful for programs that satisfy certain criteria specified by the implementation. In any case, an implementation shall support a *standard* mode that conforms to the requirements of this Reference Manual; in particular, in the standard mode, all legal *compilation_units* shall be accepted.]

**Discussion:** These permissions are designed to authorize explicitly the support for alternative modes. Of course, nothing we say can prevent them anyway, but this (redundant) paragraph is designed to indicate that such alternative modes are in some sense “approved” and even encouraged where they serve the specialized needs of a given user community, so long as the standard mode, designed to foster maximum portability, is always available.
Implementation Advice

If an implementation detects a bounded error or erroneous execution, it should raise Program_Error.

Implementation Advice: If a bounded error or erroneous execution is detected, Program_Error should be raised.

Wording Changes from Ada 83

Some situations that are erroneous in Ada 83 are no longer errors at all. For example, depending on the parameter passing mechanism when unspecified is possibly nonportable, but not erroneous.

Other situations that are erroneous in Ada 83 are changed to be bounded errors. In particular, evaluating an uninitialized scalar variable is a bounded error. The possible results are to raise Program_Error (as always), or to produce a machine-representable value (which might not be in the subtype of the variable). Violating a Range_Check or Overflow_Check raises Constraint_Error, even if the value came from an uninitialized variable. This means that optimizers can no longer “assume” that all variables are initialized within their subtype’s range. Violating a check that is suppressed remains erroneous.

The “incorrect order dependences” category of errors is removed. All such situations are simply considered potential nonportabilities. This category was removed due to the difficulty of defining what it means for two executions to have a “different effect”. For example, if a function with a side effect is called twice in a single expression, it is not in principle possible for the compiler to decide whether the correctness of the resulting program depends on the order of execution of the two function calls. A compile time warning might be appropriate, but raising of Program_Error at run time would not be.

1.2 Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. Standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards. For other documents mentioned in this document, see 1.2.1, “Bibliography”.

Paragraphs 1 through 7 and 9 through 10 have been moved to the Bibliography.


Discussion: Unlike Fortran and COBOL, which added the Information technology prefix to the titles of their standard, C did not. This was confirmed in the list of standards titles on the ISO web site. No idea why ISO allowed that.

Discussion: This title is also missing the Information technology part. That was confirmed in the list of standards titles on the ISO web site.

Discussion: This title is also missing the Information technology part. That was confirmed in the list of standards titles on the ISO web site.

Wording Changes from Ada 95

Wording Changes from Ada 2005

Wording Changes from Ada 2012

1.2.1 Bibliography

The following documents are mentioned in this document as informative references.
1.3 Terms and Definitions

Definitions

Terms are defined throughout this document, indicated by italic type. Terms explicitly defined in this document are not to be presumed to refer implicitly to similar terms defined elsewhere. Mathematical terms not defined in this document are to be interpreted according to the CRC Concise Encyclopedia of Mathematics, Second Edition. Other terms not defined in this document are to be interpreted according to the Webster's Third New International Dictionary of the English Language. Informal descriptions of some terms are also given below in Annex N, “Glossary.”


The definitions found in this subclause are short, descriptive definitions. These are most useful for comprehension when an exact meaning is not needed. More formal, detailed definitions are found in the body of the Reference Manual; these are needed to determine the exact application of rules to constructs and entities.

To see the difference, consider “aliased view”. The descriptive definition is “a view of an object that can be designated by an access value”. The formal definition is a lengthy paragraph in 3.10 that defines 10 separate constructs as aliased views. In order to reason about a language rule that requires an aliased view in a particular context, one needs to look at the list of constructs in order to determine if the object in hand is actually an aliased view. The descriptive definition is no help in this case.

Term entry: Each term defined in this subclause is marked like this in the body of the AARM near its detailed formal definition.

Discussion: Here are some AARM-only definitions: The Ada Rapporteur Group (ARG) interprets the Ada Reference Manual RMR83. An Ada Issue (AI) is a numbered ruling from the ARG. Ada Issues created for Ada 83 are denoted as "AI83", while Ada Issues created for Ada 95 are denoted as "AI95" in this document. Similarly, Ada Issues created for Ada 2005 are denoted as "AI05", Ada Issues created for Ada 2012 are denoted as "AI12", and Ada Issues created for Ada 2022 are denoted as "AI22". The Ada Commentary Integration Document (ACID) is an edition of the Ada 83 RMR83 in which clearly marked insertions and deletions indicate the effect of integrating the approved AIs. The Uniformity Rapporteur Group (URG) issues recommendations intended to increase uniformity across Ada implementations. The functions of the URG have been assumed by the ARG. A Uniformity Issue (UI) was a numbered recommendation from the URG. A Defect Report and Response is an official query to WG9 about an error in the standard. Defect Reports are processed by the ARG, and are referenced here by their ISO numbers: 8652/nnnn. Most changes to the Ada 95 standard include reference(s) to the Defect Report(s) that prompted the change. The Ada Conformity Assessment Test Suite (ACATS) is a set of tests intended to check the conformity of Ada implementations to this standard. This set of tests was previously known as the Ada Compiler Validation Capability (ACVC).
1.3.1 Types, Objects, and their Properties

abstract type

tagged type intended for use as an ancestor of other types, but which is not allowed to have objects of its own

access type

type that has values that designate aliased objects

Note: Access types correspond to “pointer types” or “reference types” in some other languages.

accessibility level

representation of the lifetime of an entity in terms of the level of dynamic nesting within which the entity is known to exist

aliased view

view of an object that can be designated by an access value

Note: Objects allocated by allocators are aliased. Objects can also be explicitly declared as aliased with the reserved word aliased. The Access attribute can be used to create an access value designating an aliased object.

ancestor of a type

type itself or, in the case of a type derived from other types, its parent type or one of its progenitor types or one of their ancestors

Note: Ancestor and descendant are inverse relationships.

array type

composite type whose components are all of the same type

aspect

specifiable property of an entity

Note: An aspect can be specified by an aspect specification on the declaration of the entity. Some aspects can be queried via attributes.

attribute

characteristic or property of an entity that can be queried, and in some cases specified

category of types

set of types with one or more common properties, such as primitive operations

Note: A category of types that is closed under derivation is also known as a class.

character type

enumeration type whose values include characters

class of types

set of types that is closed under derivation, which means that if a given type is in the class, then all types derived from that type are also in the class

Note: The set of types of a class share common properties, such as their primitive operations.

composite type

type with components, such as an array or record

controlled type

type that supports user-defined assignment and finalization

Note: Objects are always finalized before being destroyed.

default initial condition

property that holds for every default-initialized object of a given type
1.3.1 Types, Objects, and their Properties

**derived type**

Type defined in terms of a parent type and zero or more progenitor types given in a derived type definition.

Note 1: A derived type inherits properties such as components and primitive operations from its parent and progenitors.

Note 2: A type together with the types derived from it (directly or indirectly) form a derivation class.

**descendant of a type**

Type itself or a type derived (directly or indirectly) from it.

Note: Descendant and ancestor are inverse relationships.

**discrete type**

Type that is either an integer type or an enumeration type.

**discriminant**

Parameter for a composite type, which can control, for example, the bounds of a component that is an array.

Note: A discriminant for a task type can be used to pass data to a task of the type upon its creation.

**elementary type**

Type that does not have components.

**enumeration type**

Type defined by an enumeration of its values, which can be denoted by identifiers or character literals.

**full type**

Type that defines a full view.

**full view**

View of a type that reveals all of its properties.

Note: There can be other views of the type that reveal fewer properties.

**incomplete type**

Type that defines an incomplete view.

Note: Incomplete types can be used for defining recursive data structures.

**incomplete view**

View of a type that reveals minimal properties.

Note: The remaining properties are defined by the full view given elsewhere.

**indexable container type**

Type that has user-defined behavior for indexing, via the Constant_Indexing or Variable_Indexing aspects.

**integer type**

Type that represents signed or modular integers.

Note: A signed integer type has a base range that includes both positive and negative numbers, and has operations that can raise an exception when the result is outside the base range. A modular type has a base range whose lower bound is zero, and has operations with “wraparound” semantics. Modular types subsume what are called “unsigned types” in some other languages.

**interface type**

Abstract tagged type that has no components or concrete operations except possibly null procedures.

Note: Interface types are used for composing other interfaces and tagged types and thereby provide multiple inheritance. Only an interface type can be used as a progenitor of another type.

**invariant**

Assertion that is expected to be True for all objects of a given private type when viewed from outside the defining package.
iterable container type
   type that has user-defined behavior for iteration, via the Default_Iterator and Iterator_Element aspects

limited type
   type for which copying (such as in an assignment statement) is not allowed
   Note: All types are either limited types or nonlimited types.

needed component
   component of a record type or record extension that is required to have its value specified within a given aggregate

nominal subtype
   subtype specified when a view of an object is defined

nonlimited type
   type for which copying is allowed

object
   entity that contains a value, and is either a constant or a variable
   Note: An object is created by an object declaration or by an allocator. A formal parameter is (a view of) an object. A subcomponent of an object is an object.

operational aspect
   aspect that indicates a logical property of an entity, such as the precondition of a subprogram, or the procedure used to write a given type of object to a stream

parent of a derived type
   first ancestor type given in the definition of the derived type
   Note: The parent can be almost any kind of type, including an interface type.

partial view
   view of a type that reveals only some of its properties
   Note: The remaining properties are defined by the full view given elsewhere.

primitive operations of a type
   operations (such as subprograms) declared together with the type declarations
   Note: Primitive operations are inherited by other types in the same derivation class of types.

private extension
   type that extends another type, with the additional properties hidden from its clients

private type
   type that defines a partial view
   Note: Private types can be used for defining abstractions that hide unnecessary details from their clients.

progenitor
   type given in the interface list, if any, of an interface, task, protected, or derived type definition
   Note: A progenitor is always an interface type.

protected type
   composite type whose components are accessible only through one of its protected operations, which synchronize concurrent access by multiple tasks

real type
   type that has values that are approximations of the real numbers
   Note: Floating point and fixed point types are real types.

record extension
   type that extends another type optionally with additional components
1.3.1 Types, Objects, and their Properties

**record type**
composite type consisting of zero or more named components, possibly of different types

**reference type**
type that has user-defined behavior for "all", defined by the Implicit Dereference aspect

**representation aspect**
aspect that indicates how an entity is mapped onto the underlying hardware, for example the size or alignment of an object

**scalar type**
either a discrete type or a real type

**stable property**
characteristic associated with objects of a given type that is preserved by many of the primitive operations of the type

**storage pool object**
object associated with one or more access types from which the storage for objects created by allocators of the access type(s) is obtained

Note: Some storage pools can be partitioned into subpools in order to support finer-grained storage management.

**stream**
sequence of elements that can be used, along with the stream-oriented attributes, to support marshalling and unmarshalling of values of most types

**subtype**
type together with optional constraints, null exclusions, and predicates, which constrain the values of the type to the subset that satisfies the implied conditions

**synchronized**
can be safely operated on by multiple tasks concurrently

Note: Synchronized is used to qualify entities, as in a synchronized interface.

**tagged type**
type whose objects each have a run-time type tag, which indicates the specific type for which the object was originally created

Note: Tagged types can be extended with additional components.

**task type**
composite type used to represent active entities which execute concurrently and that can communicate via queued task entries

Note: The top-level task of a partition is called the environment task.

**type**
defining characteristic of each object and expression of the language, with an associated set of values, and a set of primitive operations that implement the fundamental aspects of its semantics

Note: Types are grouped into categories. Most language-defined categories of types are also classes of types.

**view of an entity**
representation of an entity that reveals some or all of the properties of the entity

Note: A single entity can have multiple views.

1.3.2 Subprograms and their Properties

**function**
form of subprogram that returns a result and can be called as part of an expression
overriding operation
operation that replaces an inherited primitive operation

Note: Operations can be marked explicitly as overriding or not overriding.

postcondition
assertion that is expected to be True when a given subprogram returns normally

precondition
assertion that is expected to be True when a given subprogram is called

procedure
form of subprogram that does not return a result and can only be invoked by a statement

subprogram
unit of a program that can be brought into execution in various contexts, with the invocation being a
subprogram call that can parameterize the effect of the subprogram through the passing of operands

Note: There are two forms of subprograms: functions, which return values, and procedures, which do not.

1.3.3 Other Syntactic Constructs

aggregate
construct used to define a value of a composite type by specifying the values of the components of the
type

compilation unit
program unit that is separately compiled

Note: A compilation unit contains either the declaration, the body, or a renaming of a program unit.

construct
piece of text (explicit or implicit) that is an instance of a syntactic category defined under Syntax

container
structured object that represents a collection of elements all of the same (potentially class-wide) type,
such as a vector or a tree

Note: Several predefined container types are provided by the children of package Ada.Containers (see A.18.1).

container aggregate
construct used to define a value of a type that represents a collection of elements, by explicitly
specifying the elements in the collection

core language
clause or annex in which are defined language constructs or capabilities that are provided by all
conforming implementations

Note: A construct is said to be part of the core language if it is defined in a core language clause or annex.

declaration
language construct that associates a name with (a view of) an entity

Note: A declaration can appear explicitly in the program text (an explicit declaration), or can be supposed to occur at a
given place in the text as a consequence of the semantics of another construct (an implicit declaration).

generic instance
nongeneric unit created by the instantiation of a generic unit

generic unit
template for a (nongeneric) program unit

Note 1: The template can be parameterized by objects, types, subprograms, and packages.

Note 2: Generic units can be used to perform the role that macros sometimes play in other languages.
**iterator**

Construct that is used to loop over the elements of an array or container.

Note: Iterators can be user defined, and can perform arbitrary computations to access elements from a container.

**iterator filter**

Construct that is used to restrict the elements produced by an iteration to those for which a boolean condition evaluates to True.

**library unit**

Separately compiled program unit, which is a package, a subprogram, or a generic unit.

Note: Library units can have other (logically nested) library units as children, and can have other program units physically nested within them. A root library unit, together with its children and grandchildren and so on, form a subsystem.

**master construct**

One of certain executable constructs for which there can be objects or tasks whose lifetime ends when the construct completes.

Note: Execution of a master construct is a master, with which objects and tasks are associated for the purposes of waiting and finalization.

**needed compilation unit**

Compilation unit that is necessary to produce an executable partition, because some entity declared or defined within the unit is used elsewhere in the partition.

**package**

Program unit that defines the interface to a group of logically related entities, along with their implementation.

Note: Typically, a package contains the declaration of a type (often a private type or private extension) along with the declarations of primitive subprograms of the type, which can be called from outside the package, while their inner workings remain hidden from outside users.

**parallel construct**

Executable construct that defines multiple activities of a single task that can proceed in parallel, via the execution of multiple logical threads of control.

**partition**

Part of a program, which consists of a set of interdependent library units.

Note: Each partition can run in a separate address space, possibly on a separate computer. A program can contain just one partition, or it can be distributed across multiple partitions, which can execute concurrently.

**pragma**

Compiler directive to provide control over and above that provided by the other syntactic constructs of the language.

Note: There are language-defined pragmas that give instructions for optimization, listing control, etc. An implementation can support additional (implementation-defined) pragmas.

**program**

Set of partitions, each of which can execute in a separate address space, possibly on a separate computer.

**program unit**

Language construct that is a package, a task unit, a protected unit, a protected entry, a generic unit, or an explicitly declared subprogram other than an enumeration literal.

Note: Certain kinds of program units can be separately compiled. Alternatively, they can appear physically nested within other program units.

**reduction expression**

Expression that defines how to map or transform a collection of values into a new set of values, and then summarize the values by applying an operation to reduce the set to a single value.
renaming
declaration that does not define a new entity, but instead defines a new view of an existing entity

specialized needs annex
annex in which are defined language constructs or capabilities that are not necessarily provided by all conforming implementations

subunit
body of a program unit that can be compiled separately from its enclosing program unit

1.3.4 Runtime Actions

assertion
boolean expression that is expected to be True at run time at certain specified places
Note: Certain pragmas and aspects define various kinds of assertions.

elaboration
process by which a declaration achieves its run-time effect
Note: Elaboration is one of the forms of execution.

evaluation
process by which an expression achieves its run-time effect
Note: Evaluation is one of the forms of execution.

execution
process by which a construct achieves its run-time effect
Note: Execution of a declaration is also called elaboration. Execution of an expression is also called evaluation.

logical thread of control
activity within the execution of a program that can proceed in parallel with other activities of the same task, or of separate tasks

master
execution of a master construct
Note: Each object and task is associated with a master. When a master is left, associated tasks are awaited and associated objects are finalized.

1.3.5 Exceptional Situations

check
test made during execution to determine whether a language rule has been violated

exception
kind of exceptional situation

exception occurrence
run-time occurrence of an exceptional situation

handle an exception
perform some actions in response to the arising of an exception

raise an exception
abandon normal program execution so as to draw attention to the fact that the corresponding situation has arisen

suppress a check
assert that the check cannot fail, and request that the compiler optimize by disabling the check
Note: The compiler is not required to honor this request. Suppressing checks that can fail can cause a program to behave in arbitrary ways.
2 Lexical Elements

The text of a program consists of the texts of one or more compilations. The text of a compilation is a sequence of lexical elements, each composed of characters; the rules of composition are given in this clause section. Pragmas, which provide certain information for the compiler, are also described in this clause section.

2.1 Character Set

The character repertoire for the text of an Ada program consists of the collection of characters described by the ISO/IEC 10646:2020 Universal Multi-octet Coded Character Set, plus a set of format_effectors and, in comments only, a set of other_control_functions; the coded representation for these characters is implementation defined.

A character is defined by this Reference Manual for each cell in the coding space described by ISO/IEC 10646:2020, regardless of whether or not ISO/IEC 10646 allocates a character to that cell.

Syntax

character ::= graphic_character | format_effector | other_control_function

graphic_character ::= identifier_letter | digit | space_character | special_character

Discussion: It is our intent to follow the terminology of ISO/IEC 10646 ISO 10646 BMP where appropriate, and to remain compatible with the character classifications defined in A.3, “Character Handling”.

Static Semantics

The character repertoire for the text of an Ada program consists of the collection of characters described by the ISO/IEC 10646:2020 called the Basic Multilingual Plane (BMP) of the ISO 10646 Universal Multi-octet Coded Character Set, plus a set of format_effectors and, in comments only, a set of other_control_functions; the coded representation for these characters is implementation defined.

Implementation defined: The coded representation for the text of an Ada program.

Ramification: Note that this rule doesn't really have much force, since the implementation can represent characters in the source in any way it sees fit. For example, an implementation could simply define that what seems to be an other_private_use character is actually a representation of the space character.
The semantics of an Ada program whose text is not in Normalization Form CKC (as defined by Clause 221 section 24 of ISO/IEC 10646:2020) is implementation defined.

**Implementation defined:** The semantics of an Ada program whose text is not in Normalization Form CKC.

**Ramification:** In particular, an implementation can reject such program source. It is easy during lexical analysis to reject source that contains any code point not present in Normalization Form C. Portable programs should always be encoded in Normalization Form C.

**Reason:** Normalization Form C ensures that all source is in a unique format; it eliminates ambiguities and security issues potentially caused by source using unusual sequences of characters. Note that WC3 (the Internet standards group) recommends that all Internet content be in Normalization Form C. We don't require this as there is a potentially significant cost to checking this (just rejecting unallowed code points is not enough), and some implementations may need to be interoperable with tools that produce unnormalized text.

The description of the language definition in this document uses the character properties General Category, Simple Uppercase Mapping, Uppercase Mapping, and Special Case Condition of the documents referenced by the note in Clause section 24 of ISO/IEC 10646:2020; Basic Latin and Row 00: Latin-1 Supplement of the ISO 10646 BMP; these correspond to the graphic symbols of ISO 8859-1 (Latin 1); no graphic symbols are used in this document for characters outside of Row 00 of the BMP. The actual set of graphic symbols used by an implementation for the visual representation of the text of an Ada program is not specified.

**Discussion:** The “documents referenced” means Unicode, Chapter 4. See the Discussion after the character categorization definition for a source for machine-readable definitions of these properties.

The categories of characters are categorized as follows:

- **identifier_letter**
- **upper_case_identifier_letter**
- **lower_case_identifier_letter**

Our character classification considers that the cells not allocated in ISO/IEC 10646:2020 are graphic characters, except for those whose relative code point position in their plane is 16#FFFE# or 16#FFFF#. This seems to provide the best compatibility with future versions of ISO/IEC 10646, as future characters can be already be used in Ada character and string literals.

Any character whose General Category is defined to be “Letter, Uppercase” of Row 00 of ISO 10646 BMP whose name begins “Latin Capital Letter”.

Any character whose General Category is defined to be “Letter, Lowercase” of Row 00 of ISO 10646 BMP whose name begins “Latin Small Letter”.

Any character whose General Category is defined to be “Letter, Titlecase”.

Any character whose General Category is defined to be “Letter, Modifier”.

Any character whose General Category is defined to be “Letter, Other”.

Any character whose General Category is defined to be “Mark, Non-Spacing”.

To be honest: The above rules do not include the ligatures Æ and æ. However, the intent is to include these characters as identifier letters. This problem was pointed out by a comment from the Netherlands.
Any character whose General Category is defined to be “Mark, Spacing Combining”.

Any character whose General Category is defined to be “Number, Decimal”. One of the characters 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.

Any character whose General Category is defined to be “Number, Letter”.

Any character whose General Category is defined to be “Punctuation, Connector”.

Any character whose General Category is defined to be “Other, Format”.

Any character whose General Category is defined to be “Separator, Space”. The character of ISO 10646 BMP named “Space”.

Any character whose General Category is defined to be “Separator, Line”. of the ISO 10646 BMP that is not reserved for a control function, and is not the space_character, an identifier_letter, or a digit.

Ramification: Note that the no_break space and soft hyphen are special_characters, and therefore graphic_characters. They are not the same characters as space and hyphen-minus.

Any character whose General Category is defined to be “Separator, Paragraph”.

The characters whose code positions are 16#09# (CHARACTER TABULATION), 16#0A# (LINE FEED), 16#0B# (LINE TABULATION), 16#0C# (FORM FEED), 16#0D# (CARRIAGE RETURN), 16#85# (NEXT LINE), and the characters in categories separator_line and separator_paragraphcontrol functions of ISO 6429 called character tabulation (HT), line tabulation (VT), carriage return (CR), line feed (LF), and form feed (FF).

Discussion: ISO/IEC 10646:2003 does not define the names of control characters, but rather refers to the names defined by ISO/IEC 6429:1992. These are the names that we use here.

Any character whose General Category is defined to be “Other, Control”, and which is not defined to be a format_effector.

Any character whose General Category is defined to be “Other, Private Use”.

Any character whose General Category is defined to be “Other, Surrogate”.

Any character that is not in the categories other_control, other_private_use, other_surrogate, format_effector, and whose relative code positions in its plane is neither 16#FFFE# nor 16#FFFF#. Any control function, other than a format_effector, that is allowed in a comment, the set of other_control_functions allowed in comments is implementation defined.

This paragraph was deleted. Implementation defined: The control functions allowed in comments.

Discussion: [AI95-00285-01] We considered basing the definition of lexical elements on Annex A of ISO/IEC TR 10176 (4th edition), which lists the characters which should be supported in identifiers for all programming languages, but we finally decided against this option. Note that it is not our intent to diverge from ISO/IEC TR 10176, except to

the extent that ISO/IEC TR 10176 itself diverges from ISO/IEC 10646:2003 (which is the case at the time of this writing [January 2005]).

More precisely, we intend to align strictly with ISO/IEC 10646:2003. It must be noted that ISO/IEC TR 10176 is a Technical Report while ISO/IEC 10646:2003 is a Standard. If one has to make a choice, one should conform with the Standard rather than with the Technical Report. And, it turns out that one must make a choice because there are important differences between the two:

- ISO/IEC TR 10176 is still based on ISO/IEC 10646:2000 while ISO/IEC 10646:2003 has already been published for a year. We cannot afford to delay the adoption of our amendment until ISO/IEC TR 10176 has been revised.
- There are considerable differences between the two editions of ISO/IEC 10646, notably in supporting characters beyond the BMP (this might be significant for some languages, e.g. Korean).
- ISO/IEC TR 10176 does not define case conversion tables, which are essential for a case-insensitive language like Ada. To get case conversion tables, we would have to reference either ISO/IEC 10646:2003 or Unicode, or we would have to invent our own.

For the purpose of defining the lexical elements of the language, we need character properties like categorization, as well as case conversion tables. These are mentioned in ISO/IEC 10646:2003 as useful for implementations, with a reference to Unicode. Machine-readable tables are available on the web at URLs:

http://www.unicode.org/Public/UCD/latest/ucd/UnicodeData.txt
http://www.unicode.org/Public/UCD/latest/ucd/CaseFolding.txt
http://www.unicode.org/Public/4.0-Update/UnicodeData-4.0.0.txt
http://www.unicode.org/Public/4.0-Update/CaseFolding-4.0.0.txt

with an explanatory document found at URL:

http://www.unicode.org/reports/tr44/tr44-20.html

\{AI12-0263-1\} The actual text of the standard only makes specific references to the corresponding clauses of ISO/IEC 10646:2003, not to Unicode.
The following names are used when referring to certain characters (the first name is that given in ISO/IEC 10646:2003):

**Discussion:**

This table serves to show the correspondence between ISO/IEC 10646:2003 names and the graphic symbols (glyphs) used in this document. These are the characters that play a special role in the syntax of Ada 95, or in the syntax rules; we don't bother to define names for all characters. The first name given is the name from ISO 10646; the subsequent names, if any, are those used within the standard, depending on context.

<table>
<thead>
<tr>
<th>graphic symbol</th>
<th>name</th>
<th>graphic symbol</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;</td>
<td>quotation mark</td>
<td></td>
<td>colon</td>
</tr>
<tr>
<td>#</td>
<td>number sign</td>
<td>;</td>
<td>semicolon</td>
</tr>
<tr>
<td>&amp;</td>
<td>ampersand</td>
<td>&lt;</td>
<td>less-than sign</td>
</tr>
<tr>
<td>,</td>
<td>apostrophe, tick</td>
<td>=</td>
<td>equals sign</td>
</tr>
<tr>
<td>(</td>
<td>left parenthesis</td>
<td>&gt;</td>
<td>greater-than sign</td>
</tr>
<tr>
<td>)</td>
<td>right parenthesis</td>
<td>-</td>
<td>low line, underline</td>
</tr>
<tr>
<td>*</td>
<td>asterisk, multiply</td>
<td>|</td>
<td>vertical line</td>
</tr>
<tr>
<td>+</td>
<td>plus sign</td>
<td>|</td>
<td>solidus, divide</td>
</tr>
<tr>
<td>,</td>
<td>comma</td>
<td>|</td>
<td>left square bracket</td>
</tr>
<tr>
<td>–</td>
<td>hyphen-minus, minus</td>
<td>%|</td>
<td>exclamation point</td>
</tr>
<tr>
<td>.</td>
<td>full stop, dot, point</td>
<td>|</td>
<td>square bracket</td>
</tr>
<tr>
<td>@</td>
<td>commercial at, at sign</td>
<td>|</td>
<td>percent sign</td>
</tr>
<tr>
<td>/</td>
<td>solidus, divide</td>
<td>|</td>
<td>left curly bracket</td>
</tr>
<tr>
<td></td>
<td></td>
<td>|</td>
<td>right square bracket</td>
</tr>
<tr>
<td></td>
<td></td>
<td>|</td>
<td>right curly bracket</td>
</tr>
</tbody>
</table>

**Implementation Requirements**

An Ada implementation shall accept Ada source code in UTF-8 encoding, with or without a BOM (see A.4.11), where every character is represented by its code point. The character pair CARRIAGE RETURN/LINE FEED (code points 16#0D# 16#0A#) signifies a single end of line (see 2.2); every other occurrence of a format effector other than the character whose code point position is 16#09# (CHARACTER TABULATION) also signifies a single end of line.

**Reason:**

This is simply requiring that an Ada implementation be able to directly process the ACATS, which is provided in the described format. Note that files that only contain characters with code points in the first 128 (which is the majority of the ACATS) are represented in the same way in both UTF-8 and in "plain" string format. The ACATS includes a BOM in files that have any characters with code points greater than 127. Note that the BOM contains characters not legal in Ada source code, so an implementation can use that to automatically distinguish between files formatted as plain Latin-1 strings and UTF-8 with BOM.

We allow line endings to be both represented as the pair CR LF (as in Windows and the ACATS), and as single characters (usually LF, as in Linux), in order that files created by standard tools on most operating systems will meet the standard format. We specify how many line endings each represent so that compilers use the same line numbering for standard source files.

This requirement increases portability by having a format that is accepted by all Ada compilers. Note that implementations can support other source representations, including structured representations like a parse tree.

**Implementation Permissions**

The categories defined above, as well as case mapping and folding, may be based on an implementation-defined version of ISO/IEC 10646 (2003 edition or later). In a nonstandard mode, the implementation may support a different character repertoire; in particular, the set of characters that are considered identifier letters can be extended or changed to conform to local conventions.
Ramification: If an implementation supports other character sets, it defines which characters fall into each category, such as "identifier_letter", and what the corresponding rules of this section are, such as which characters are allowed in the text of a program.

The exact categories, case mapping, and case folding chosen affects identifiers, the result of "[[Wide_]]Image" and packages Wide_Characters.Handling and Wide_Wide_Characters.Handling.

Discussion: This permission allows implementations to upgrade to using a newer character set standard whenever that makes sense, rather than having to wait for the next Ada Standard. But the character set standard used cannot be older than ISO/IEC 10646:2003 (which is essentially similar to Unicode 4.0).

NOTE \{AI95-00285-01\} The characters in categories other_control, other_private_use, and other_surrogate are only allowed in comments. Every code position of ISO 10646 BMP that is not reserved for a control function is defined to be a graphic_character by this document. This includes all code positions other than 0000—001F, 007F—009F, and FFFE—FFFF.

NOTE \{AI05-0286-1\} The language does not specify the source representation of programs.

This paragraph was deleted. Discussion: \{AI05-0286-1\} Any source representation is valid so long as the implementer can produce an (information-preserving) algorithm for translating both directions between the representation and the standard character set. (For example, every character in the standard character set has to be representable, even if the output devices attached to a given computer cannot print all of those characters properly.) From a practical point of view, every implementer will have to provide some way to process the ACATS. It is the intent to allow source representations, such as parse trees, that are not even linear sequences of characters. It is also the intent to allow different fonts, reserved words might be in bold face, and that should be irrelevant to the semantics.

Extensions to Ada 83

Ada 95 allows 8-bit and 16-bit characters, as well as implementation-specified character sets.

Wording Changes from Ada 83

\{AI95-00285-01\} \{AI05-0299-1\} The syntax rules in this subclause are modified to remove the emphasis on basic characters vs. others. (In this day and age, there is no need to point out that you can write programs without using (for example) lower case letters.) In particular, character (representing all characters usable outside comments) is added, and basic_graphic_character, other_special_character, and basic_character are removed. Special_character is expanded to include Ada 83's other_special_character, as well as new 8-bit characters not present in Ada 83. Ada 2005 removes special_character altogether; we want to stick to ISO/IEC 10646:2003 character classifications. Note that the term "basic letter" is used in A.3, "Character Handling" to refer to letters without diacritical marks.


This paragraph was deleted. \{AI95-00285-01\} We use identifier_letter rather than letter since ISO-10646-BMP includes many "letters" that are not permitted in identifiers (in the standard mode).

Extensions to Ada 95

\{AI95-00285-01\} \{AI95-00395-01\} Program text can use most characters defined by ISO-10646:2003. This subclause has been rewritten to use the categories defined in that Standard. This should ease programming in languages other than English.

Inconsistencies With Ada 2005

\{AI05-0299-1\} \{AI05-0266-1\} An implementation is allowed (but not required) to use a newer character set standard to determine the categories, case mapping, and case folding. Doing so will change the results of attributes [[Wide_]]Image and the packages Wide_Characters.Handling in the case of a few rarely used characters. (This also could make some identifiers illegal, for characters that are not longer classified as letters.) This is unlikely to be a problem in practice. Moreover, truly portable Ada 2012 programs should avoid using in these contexts any characters that would have different classifications in any character set standards issued since 10646:2003 (since the compiler can use any such standard as the basis for its classifications).

Wording Changes from Ada 2005

\{AI05-0079-1\} Correction: Clarified that only characters in the categories defined here are allowed in the source of an Ada program. This was clear in Ada 95, but Amendment 1 dropped the wording instead of correcting it.

\{AI05-0286-1\} A standard source representation is defined that all compilers are expected to process. Since this is the same format as the ACATS, it seems unlikely that there are any implementations that don't meet this requirement. Moreover, other representations are still permitted, and the "impossible or impractical" loophole (see 1.1.3) can be invoked for any implementations that cannot directly process the ACATS.
Wording Changes from Ada 2012

Correction: The interpretation of Ada source that is in Normalization Form C but not in Normalization Form KC is no longer implementation-defined. This change could potentially change the meaning of a program for a compiler that normalized all program source to Normalization Form KC before processing it. We don't document this as an inconsistency as such handling was previously implementation defined (so any such code was already defined to be not portable), and we're not aware of any compiler that normalized source code (so we don't expect to see this problem in the real world).

2.2 Lexical Elements, Separators, and Delimiters

Static Semantics

The text of a program consists of the texts of one or more compilations. The text of each compilation is a sequence of separate lexical elements. Each lexical element is formed from a sequence of characters, and is either a delimiter, an identifier, a reserved word, a numeric_literal, a character_literal, a string_literal, or a comment. The meaning of a program depends only on the particular sequences of lexical elements that form its compilations, excluding comments.

The text of a compilation is divided into lines. In general, the representation for an end of line is implementation defined. However, a sequence of one or more format_effector other than the character whose code point position is 16#09# (CHARACTER TABULATION) signifies at least one end of line.

Implementation defined: The representation for an end of line.

A separator is any of a separator_space, a format_effector, or the end of a line, as follows:

Discussion: It might be useful to define “white space” and use it here.

• A separator_space is a separator except within a comment, a string_literal, or a character_literal.

• The end of a line is always a separator.

One or more separators are allowed between any two adjacent lexical elements, before the first of each compilation, or after the last. At least one separator is required between an identifier, a reserved word, or a numeric_literal and an adjacent identifier, reserved word, or numeric_literal.

One or more other_format characters are allowed anywhere that a separator is, any such characters have no effect on the meaning of an Ada program.

A delimiter is either one of the following special characters:

or one of the following compound delimiters each composed of two adjacent special characters

Each of the special characters listed for single character delimiters is a single delimiter except if this character is used as a character of a compound delimiter, or as a character of a comment, string_literal, character_literal, or numeric_literal.
The following names are used when referring to compound delimiters:

<table>
<thead>
<tr>
<th>delimiter</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>=&gt;</td>
<td>arrow</td>
</tr>
<tr>
<td>..</td>
<td>double dot</td>
</tr>
<tr>
<td>**</td>
<td>double star, exponentiate</td>
</tr>
<tr>
<td>:=</td>
<td>assignment (pronounced: “becomes”)</td>
</tr>
<tr>
<td>/=</td>
<td>inequality (pronounced: “not equal”)</td>
</tr>
<tr>
<td>&gt;=</td>
<td>greater than or equal</td>
</tr>
<tr>
<td>&lt;=</td>
<td>less than or equal</td>
</tr>
<tr>
<td>&lt;&lt;</td>
<td>left label bracket</td>
</tr>
<tr>
<td>&gt;&gt;</td>
<td>right label bracket</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>box</td>
</tr>
</tbody>
</table>

**Implementation Requirements**

An implementation shall support lines of at least 200 characters in length, not counting any characters used to signify the end of a line. An implementation shall support lexical elements of at least 200 characters in length. The maximum supported line length and lexical element length are implementation defined.

**Implementation defined:** Maximum supported line length and lexical element length.

**Discussion:** From URG recommendation.

**Wording Changes from Ada 95**

\{AI95-00285-01\} \{AI05-0299-1\} The wording was updated to use the new character categories defined in the preceding subclause.

**Extensions to Ada 2005**

\{AI05-0079-1\} **Correction:** Clarified that other_format characters are allowed anywhere that separators are allowed. This was intended in Ada 2005, but didn’t actually make it into the wording.

**Wording Changes from Ada 2012**

\{AI12-0125-3\} \{AI12-0212-1\} Added square brackets and the target_name symbol (see 5.2.1) to the list of delimiters.

### 2.3 Identifiers

Identifiers are used as names.

**Syntax**

\{AI95-00285-01\} \{AI95-00395-01\} \texttt{identifier ::=}

\begin{verbatim}
  identifier_start \{identifier_start | identifierExtend\} identifier_letter \{[underline] letter_or_digit\}
\end{verbatim}

\{AI95-00285-01\} \{AI95-00395-01\} \texttt{identifier_start | letter_or_digit ::=}

\begin{verbatim}
  letter_uppercase
  | letter_lowercase
  | letter_titlecase
\end{verbatim}
| letter modifier  
| letter other  
| number  
| letter_identifier_letter | digit

An identifier shall only contain characters that may be present in Normalization Form KC as defined by Clause 22 of ISO/IEC 10646:2020.

Implementation Note: An implementation can usually detect this during lexical processing. The code points not allowed are those for which Unicode property NFKC QC (Normalization Form KC Quick Check) has the value No. We say "may be present" so that characters for which the value is Maybe (really, one of the possible values is Maybe) are allowed (these are mainly combining marks). The necessary tables can be found in http://www.unicode.org/Public/UCD/latest/ucd/DerivedNormalizationProps.txt. Versions for older Unicode versions can be found on this site as well; start at http://www.unicode.org/Public/ and find the appropriate version number.

Static Semantics

Two identifiers are considered the same if they consist of the same sequence of characters after applying locale-independent simple case folding, as defined by documents referenced in the note in Clause 21 of ISO/IEC 10646:2020, the following transformations (in this order). All characters of an identifier are significant, including any underline character. Identifiers differing only in the use of corresponding upper and lower case letters are considered the same.

- The characters in category other_format are eliminated.
- The remaining sequence of characters is converted to upper case.

Discussion: Simple case folding is a mapping to lower case, so this is matching the defining (lower case) version of a reserved word. We could have mentioned case folding of the reserved words, but as that is an identity function, it would have no effect. Two of the letters of ISO 8859-1 appear only as lower case, “comma” and “/” with diaeresis”. These two letters have no corresponding upper case letter (in particular, they are not considered equivalent to one another).

The "documents referenced" means Unicode, Chapter 4 (specifically, section 4.2 — Case). Note that simple case folding is supposed to be compatible between Unicode versions, so the Unicode version used doesn’t matter. A machine-readable version of the needed mapping can be found at http://www.unicode.org/Public/UCD/latest/ucd/CaseFolding.txt.

After applying simple case folding these transformations, an identifier shall not be identical to a reserved word (in upper case).

Implementation Note: We match the reserved words after applying case folding doing these transformations so that the rules for identifiers and reserved words are the same. (This allows other_format characters, which usually don’t
Ramification: \{AI05-0227-1\} The rules for reserved words differ in one way: they define case conversion on letters rather than sequences. This means that it is possible that there exist some unusual sequences that are neither identifiers nor reserved words. We are not aware of any such sequences so long as we use simple case folding (as opposed to full case folding), but we have defined the rules in case any are introduced in future character set standards. This originally was a problem when converting to upper case: for instance, “İ” and “ACCESS” have upper case conversions of “İF” and “ACCESS” respectively. We would not want these to be treated as reserved words. But neither of these cases exist when using simple case folding. These are not identifiers, because the transformed values are identical to a reserved word. But they are not reserved words, either, because the original values do not match any reserved word as defined or with any number of characters of the reserved word in upper case. Thus, these odd constructions are just illegal, and should not appear in the source of a program.

Implementation Permissions

In a nonstandard mode, an implementation may support other upper/lower case equivalence rules for identifiers, to accommodate local conventions.

Discussion: \{AI95-00285-01\} \{AI05-0227-1\} For instance, in most languages, the simple case folded uppercase equivalent of LATIN CAPITAL SMALL LETTER I (an upper-lower case letter without a dot above) is LATIN SMALL CAPITAL LETTER I (a lower-upper case letter with a dot above). In Turkish, though, LATIN CAPITAL SMALL LETTER I and LATIN CAPITAL SMALL LETTER DOTLESS I WITH DOT ABOVE are two distinct letters, so the case folded uppercase equivalent of LATIN CAPITAL SMALL LETTER I is LATIN SMALL CAPITAL LETTER DOTLESS I WITH DOT ABOVE, and the case folded uppercase equivalent of LATIN SMALL CAPITAL LETTER DOTLESS I WITH DOT ABOVE is LATIN SMALL CAPITAL LETTER I. Take for instance the following identifier (which is the name of a city on the Tigris river in Eastern Anatolia):

```
dİYARBAKIR
```

--- The first i is dotted, the second isn’t.

A Turkish reader would expect that the above identifier is equivalent to locale-independent conversion to upper case results in:

```
dİYARBAKIR
```

--- Both i are dotted.

However, locale-independent simple case folding (and thus Ada) maps this to:

```
dİyARBAKIR
```

which is different from any of the following identifiers: This means that the four following sequences of characters represent the same identifier, even though for a locutor of Turkish they would probably be considered distinct words:

```
dİyARBAKIR
dİyARBAKIR
dİyARBAKIR
dİyARBAKIR
```

including the “correct” matching identifier for Turkish: Upper case conversion (used in ![Wide Image]) introduces additional problems.

An implementation targeting the Turkish market is allowed (in fact, expected) to provide a nonstandard mode where case folding is appropriate for Turkish. This would cause the original identifier to be converted to:

```
DİYARBAKIR
```

--- The first i is dotted, the second isn’t.

and the four sequences of characters shown above would represent four distinct identifiers.

Lithuanian and Azeri are two other languages that present similar idiosyncrasies.

NOTE \{AI95-00285-01\} Identifiers differing only in the use of corresponding upper and lower case letters are considered the same.

Examples

```
Examples of identifiers:
```

```
Count X Get_Symbol Ethelyn Marion
Snobol 4 X1 Page_Count Store_Next_Item
Platon -- Plato
Chaykovskij -- Tchaikovsky
θ φ -- Angles
```

Examples of identifiers:
We no longer include reserved words as identifiers. This is not a language change. In Ada 83, identifier included reserved words. However, this complicated several other rules (for example, regarding implementation-defined attributes and pragmas, etc.). We now explicitly allow certain reserved words for attribute designators, to make up for the loss.

**Ramification:** Because syntax rules are relevant to overload resolution, it means that if it looks like a reserved word, it is not an identifier. As a side effect, implementations cannot use reserved words as implementation-defined attributes or pragma names.

**Extensions to Ada 95**

{AI95-00285-01} An identifier can use any letter defined by ISO-10646:2003, along with several other categories. This should ease programming in languages other than English.

**Incompatibilities With Ada 2005**

{AI05-0091-1} Correction: Other format characters were removed from identifiers as the Unicode recommendations have changed. This change can only affect programs written for the original Ada 2005, so there should be few such programs.

{AI05-0227-1} Correction: We now specify simple case folding rather than full case folding. That potentially could change identifier equivalence, although it is more likely that identifiers that are considered the same in original Ada 2005 will now be considered different. This change was made because the original Ada 2005 definition was incompatible (and even inconsistent in unusual cases) with the Ada 95 identifier equivalence rules. As such, the Ada 2005 rules were rarely fully implemented, and in any case, only Ada 2005 identifiers containing wide characters could be affected.

**Incompatibilities With Ada 2012**

{AI12-0004-1} Correction: An identifier that contains any characters not permitted in Normalization Form KC is now illegal. Ada 2012 allowed such identifiers, but their interpretation was implementation-defined (so the use of such identifiers was not portable). Identifiers that may be interpreted differently by different compilers are a safety and security hazard, so we no longer allow them.

## 2.4 Numeric Literals

There are two kinds of numeric_literals, real literals and integer literals. A real literal is a numeric_literal that includes a point; an integer literal is a numeric_literal without a point.

**Syntax**

```
numeric_literal ::= decimal_literal | based_literal
```

**NOTE** The type of an integer literal is universal_integer. The type of a real literal is universal_real.

### 2.4.1 Decimal Literals

A decimal_literal is a numeric_literal in the conventional decimal notation (that is, the base is ten).

**Syntax**

```
decimal_literal ::= numeral [.numeral] [exponent]
numeral ::= digit {[underline] digit}
exponent ::= E [+] numeral | E − numeral
```

{AI95-00285-01} digit ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

An exponent for an integer literal shall not have a minus sign.

**Ramification:** Although this rule is in this subclause, it applies also to the next subclause.
Static Semantics

An underline character in a numeric_literal does not affect its meaning. The letter E of an exponent can be written either in lower case or in upper case, with the same meaning.

Ramification: Although these rules are in this subclause, they apply also to the next subclause.

An exponent indicates the power of ten by which the value of the decimal_literal without the exponent is to be multiplied to obtain the value of the decimal_literal with the exponent.

Examples

Examples of decimal literals:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>integer literals</td>
</tr>
<tr>
<td>0.0</td>
<td>real literals</td>
</tr>
<tr>
<td>12.0</td>
<td>real literals</td>
</tr>
<tr>
<td>0.456</td>
<td>real literals</td>
</tr>
<tr>
<td>3.14159_26</td>
<td>real literals</td>
</tr>
</tbody>
</table>

Wording Changes from Ada 83

We have changed the syntactic category name integer to be numeral. We got this idea from ACID. It avoids the confusion between this and integers. (Other places don't offer similar confusions. For example, a string_literal is different from a string.)

2.4.2 Based Literals

A based_literal is a numeric_literal expressed in a form that specifies the base explicitly.

Syntax

based_literal ::= base # based_numeral [based_numeral] # [exponent]

base ::= numeral

based_numeral ::= extended_digit [{underline} extended_digit]

extended_digit ::= digit | A | B | C | D | E | F

Legality Rules

The base (the numeric value of the decimal numeral preceding the first #) shall be at least two and at most sixteen. The extended_digits A through F represent the digits ten through fifteen, respectively. The value of each extended_digit of a based_literal shall be less than the base.

Static Semantics

The conventional meaning of based notation is assumed. An exponent indicates the power of the base by which the value of the based_literal without the exponent is to be multiplied to obtain the value of the based_literal with the exponent. The base and the exponent, if any, are in decimal notation.

The extended_digits A through F can be written either in lower case or in upper case, with the same meaning.

Examples

Examples of based literals:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>2#1111_1111# 16#FF#</td>
<td>integer literals of value 255</td>
</tr>
<tr>
<td>2#1110_0000# 16#E1</td>
<td>integer literals of value 224</td>
</tr>
<tr>
<td>2#1.1111_1111_1110#E11</td>
<td>real literals of value 4095.0</td>
</tr>
</tbody>
</table>
Wording Changes from Ada 83

The rule about which letters are allowed is now encoded in BNF, as suggested by Mike Woodger. This is clearly more readable.

2.5 Character Literals

[ A character_literal is formed by enclosing a graphic character between two apostrophe characters. ]

Syntax

character_literal ::= 'graphic_character'

NOTE A character_literal is an enumeration literal of a character type. See 3.5.2.

Examples

Examples of character literals:

{AI95-00433-01} 'A'     '*'     '''     ' '     'L'     'Л'     'Λ'    -- Various els.
      ∞     'א'     --            ' '     -- Big numbers - infinity and aleph

Wording Changes from Ada 83

{AI05-0299-1} The definitions of the values of literals are in ClausesSections 3 and 4, rather than here, since it requires knowledge of types.

2.6 String Literals

[ A string_literal is formed by a sequence of graphic characters (possibly none) enclosed between two quotation marks used as string brackets. They are used to represent operator_symbols (see 6.1), values of a string type (see 4.2), and array subaggregates (see 4.3.3). ]

Syntax

string_literal ::= "{string_element}"  
string_element ::= "" | non_quotation_mark_graphic_character

A string_element is either a pair of quotation marks (""), or a single graphic_character other than a quotation mark.

Static Semantics

The sequence of characters of a string_literal is formed from the sequence of string_elements between the bracketing quotation marks, in the given order, with a string_element that is "" becoming a single quotation mark in the sequence of characters, and any other string_element being reproduced in the sequence.

A null string_literal is a string_literal with no string_elements between the quotation marks.

NOTE 1 An end of line cannot appear in a string_literal.
NOTE 2 {AI95-00285-01} No transformation is performed on the sequence of characters of a string_literal.
Examples of string literals:

\{AI95-00433-01\} "Message of the day:"

" " -- a null string literal
"  "  "  "  " -- three string literals of length 1

"Characters such as $, %, and } are allowed in string literals"

Archimedes said "Εύρηκα"

"Volume of cylinder (πr²h) = "

Wording Changes from Ada 83

The wording has been changed to be strictly lexical. No mention is made of string or character values, since string_literals are also used to represent operator_symbols, which don't have a defined value.

Wording Changes from Ada 95

\{AI95-00285-01\} We explicitly say that the characters of a string literal should be used as is. In particular, no normalization or folding should be performed on a string literal.

2.7 Comments

A comment starts with two adjacent hyphens and extends up to the end of the line.

Syntax

comment ::= --{non_end_of_line_character}

A comment may appear on any line of a program.

Static Semantics

The presence or absence of comments has no influence on whether a program is legal or illegal. Furthermore, comments do not influence the meaning of a program; their sole purpose is the enlightenment of the human reader.

Examples

Examples of comments:

\{AI12-0440-1\} -- the last sentence above echoes the Algol 68 report

end; -- processing of Line is complete

-- a long comment comment be split onto
-- two or more consecutive lines

------------------ the first two hyphens start the comment

2.8 Pragmas

A pragma is a compiler directive. There are language-defined pragmas that give instructions for optimization, listing control, etc. An implementation may support additional (implementation-defined) pragmas.

Term entry: pragma — compiler directive to provide control over and above that provided by the other syntactic constructs of the language

Note: There are language-defined pragmas that give instructions for optimization, listing control, etc. An implementation can support additional (implementation-defined) pragmas.
Language Design Principles

AI05-0100-1 AI05-0163-1 In general, if all pragmas are treated as unrecognized pragmas, the program should remain both syntactically and semantically legal. There are a few exceptions to this general principle (for example, pragma Import can eliminate the need for a completion), but the principle remains, and is strictly true at the syntactic level. Certainly any implementation-defined pragmas should obey this principle both syntactically and semantically, so that if the pragmas are not recognized by some other implementation, the program will remain legal.

Syntax

pragma ::= 
    pragma identifier [(pragma_argument_association {, pragma_argument_association})];

AI05-0290-1 pragma_argument_association ::= 
    [pragma_argument_identifier =>] name 
    | [pragma_argument_identifier =>] expression 
    | pragma_argument_aspect_mark => name 
    | pragma_argument_aspect_mark => expression

AI05-0290-1 In a pragma, any pragma_argument_associations without a pragma_argument_identifier or pragma_argument_aspect_mark shall precede any associations with a pragma_argument_identifier or pragma_argument_aspect_mark.

Pragmas are only allowed at the following places in a program:

- AI12-0236-1 After a semicolon delimiter, but not within a formal_part or discriminant_part or declare_expression.
- AI05-0100-1 AI05-0163-1 At any place where the syntax rules allow a construct defined by a syntactic category whose name ends with “declaration”, “item”, “statement”, “clause”, or “alternative”, or one of the syntactic categories variant or exception_handler; but not in place of such a construct if the construct is required, or is part of a list that is required to have at least one such construct. Also at any place where a compilation_unit would be allowed.
- AI05-0163-1 In place of a statement in a sequence_of_statements.
- AI05-0100-1 At any place where a compilation_unit is allowed.

Additional syntax rules and placement restrictions exist for specific pragmas.

Discussion: The above rule is written in text, rather than in BNF; the syntactic category pragma is not used in any BNF syntax rule.

Discussion: The above rule is written in text, rather than in BNF; the syntactic category pragma is not used in any BNF syntax rule.

Ramification: A pragma is allowed where a generic_formal_parameter_declaration is allowed.

Discussion: The above rule is written in text, rather than in BNF; the syntactic category pragma is not used in any BNF syntax rule.

Discussion: The above rule is written in text, rather than in BNF; the syntactic category pragma is not used in any BNF syntax rule.

Ramification: A pragma is allowed where a generic_formal_parameter_declaration is allowed.

The name of a pragma is the identifier following the reserved word pragma. The name or expression of a pragma_argument_association is a pragma argument.

To be honest: AI95-00284-02 For compatibility with Ada 83, the name of a pragma may also be “interface”, which is not an identifier (because it is a reserved word). See J.12.

AI05-0272-1 An identifier specific to a pragma is an identifier or reserved_word that is used in a pragma argument with special meaning for that pragma.

To be honest: Whenever the syntax rules for a given pragma allow "identifier" as an argument of the pragma, that identifier is an identifier specific to that pragma.

AI05-0272-1 In a few cases, a reserved word is allowed as "an identifier specific to a pragma". Even in these cases, the syntax still is written as identifier (the reserved word(s) are not shown). For example, the restriction No_Use_Of_Attribute (see 13.12.1) allows the reserved words which can be attribute designators, but the syntax for a restriction does not include these reserved words.
**Static Semantics**

11 If an implementation does not recognize the name of a **pragma**, then it has no effect on the semantics of the program. Inside such a **pragma**, the only rules that apply are the Syntax Rules.

11.a **To be honest:** This rule takes precedence over any other rules that imply otherwise.

11.b **Ramification:** Note well: this rule applies only to **pragmas** whose name is not recognized. If anything else is wrong with a **pragma** (at compile time), the **pragma** is illegal. This is true whether the **pragma** is language defined or implementation defined.

11.c For example, an expression in an unrecognized **pragma** does not cause freezing, even though the rules in 13.14, “Freezing Rules” say it does; the above rule overrules those other rules. On the other hand, an expression in a recognized **pragma** causes freezing, even if this makes something illegal.

11.d For another example, an expression that would be ambiguous is not illegal if it is inside an unrecognized **pragma**.

11.e Note, however, that implementations have to recognize **pragma** Inline(Foo) and freeze things accordingly, even if they choose to never do inlining.

11.f Obviously, the contradiction needs to be resolved one way or the other. The reasons for resolving it this way are: The implementation is simple — the compiler can just ignore the **pragma** altogether. The interpretation of constructs appearing inside implementation-defined **pragmas** is implementation defined. For example: "**pragma** Mumble(X);". If the current implementation has never heard of Mumble, then it doesn't know whether X is a name, an expression, or an identifier specific to the **pragma** Mumble.

11.g **To be honest:** The syntax of individual pragmas overrides the general syntax for **pragma**.

11.h **Ramification:** Thus, an identifier specific to a **pragma** is not a name, syntactically; if it were, the visibility rules would be invoked, which is not what we want.

11.i The order given in the syntax rule for each individual **pragma** must be obeyed. However, it is generally possible to leave out earlier arguments when later ones are given; for example, this is allowed by the syntax rule for **pragma** Import (see J.15.5, “Interfacing Pragmas”)[1],[2],[3]. As for subprogram calls, positional notation precedes named notation.

11.j Note that Ada 83 had no pragmas for which the order of named associations mattered, since there was never more than one argument that allowed named associations.

11.k **To be honest:** The interpretation of the arguments of implementation-defined **pragmas** is implementation defined. However, the syntax rules have to be obeyed.

**Dynamic Semantics**

12 Any **pragma** that appears at the place of an executable construct is executed. Unless otherwise specified for a particular **pragma**, this execution consists of the evaluation of each evaluable **pragma** argument in an arbitrary order.

12.a **Ramification:** For a **pragma** that appears at the place of an elaborable construct, execution is elaboration.

12.b An identifier specific to a **pragma** is neither a name nor an expression — such identifiers are not evaluated (unless an implementation defines them to be evaluated in the case of an implementation-defined **pragma**).

12.c The “unless otherwise specified” part allows us (and implementations) to make exceptions, so a **pragma** can contain an expression that is not evaluated. Note that **pragmas** in **type_definition**s may contain expressions that depend on discriminants.

12.d When we wish to define a **pragma** with some run-time effect, we usually make sure that it appears in an executable context; otherwise, special rules are needed to define the run-time effect and when it happens.

**Implementation Requirements**

13 The implementation shall give a warning message for an unrecognized **pragma** name.

13.a **Ramification:** An implementation is also allowed to have modes in which a warning message is suppressed, or in which the presence of an unrecognized **pragma** is a compile-time error.

**Implementation Permissions**

14 An implementation may provide implementation-defined **pragmas**; the name of an implementation-defined **pragma** shall differ from those of the language-defined **pragmas**.
Implementation defined: Implementation-defined pragmas.

Ramification: The semantics of implementation-defined pragmas, and any associated rules (such as restrictions on their placement or arguments), are, of course, implementation defined. Implementation-defined pragmas may have run-time effects.

An implementation may ignore an unrecognized pragma even if it violates some of the Syntax Rules, if detecting the syntax error is too complex.

Reason: Many compilers use extra post-parsing checks to enforce the syntax rules, since the Ada syntax rules are not LR(k) (for any k). (The grammar is ambiguous, in fact.) This paragraph allows them to ignore an unrecognized pragma, without having to perform such post-parsing checks.

Implementation Advice

{AI05-0163-1} Normally, implementation-defined pragmas should have no semantic effect for error-free programs; that is, if the implementation-defined pragmas in a working program are replaced with unrecognized pragmas are removed from a working program, the program should still be legal, and should still have the same semantics.

Implementation Advice: Implementation-defined pragmas should have no semantic effect for error-free programs.

Ramification: Note that “semantics” is not the same as “effect;” as explained in 1.1.3, the semantics defines a set of possible effects.

Note that adding a pragma to a program might cause an error (either at compile time or at run time). On the other hand, if the language-specified semantics for a feature are in part implementation defined, it makes sense to support pragmas that control the feature, and that have real semantics; thus, this paragraph is merely a recommendation.

Normally, an implementation should not define pragmas that can make an illegal program legal, except as follows:

• {AI05-0229-1} A pragma used to complete a declaration, such as a pragma Import;

Discussion: {AI05-0229-1} There are no language-defined pragmas which can be completions; pragma Import was defined this way in Ada 95 and Ada 2005, but in Ada 2012 pragma Import just sets aspect Import which disallows having any completion.

• A pragma used to configure the environment by adding, removing, or replacing library items.

Implementation Advice: Implementation-defined pragmas should not make an illegal program legal, unless they complete a declaration or configure the library items in an environment.

Ramification: For example, it is OK to support Interface, System_Name, Storage_Unit, and Memory_Size pragmas for upward compatibility reasons, even though all of these pragmas can make an illegal program legal. (The latter three can affect legality in a rather subtle way: They affect the value of named numbers in System, and can therefore affect the legality in cases where static expressions are required.)

On the other hand, adding implementation-defined pragmas to a legal program can make it illegal. For example, a common kind of implementation-defined pragma is one that promises some property that allows more efficient code to be generated. If the promise is a lie, it is best if the user gets an error message.

Incompatibilities With Ada 83

In Ada 83, “bad” pragmas are ignored. In Ada 95, they are illegal, except in the case where the name of the pragma itself is not recognized by the implementation.

Extensions to Ada 83

Implementation-defined pragmas may affect the legality of a program.

Wording Changes from Ada 83

Implementation-defined pragmas may affect the run-time semantics of the program. This was always true in Ada 83 (since it was not explicitly forbidden by RM83), but it was not clear, because there was no definition of “executing” or “elaborating” a pragma.
### Extensions to Ada 2005

19.f/3  
\{AI05-0163-1\}  **Correction:** Allow pragmas in place of a statement, even if there are no other statements in a sequence of statements.

19.g/3  
\{AI05-0272-1\} Identifiers specific to a pragma can be reserved words.

19.h/3  
\{AI05-0290-1\} Pragma arguments can be identified with aspect marks; this allows identifier Class in this context. As usual, this is only allowed if specifically allowed by a particular pragma.

### Wording Changes from Ada 2005

19.i/3  
\{AI05-0100-1\}  **Correction:** Clarified where pragmas are (and are not) allowed.

### Wording Changes from Ada 2012

19.j/5  
\{AI12-0236-1\} Added wording to ensure that pragmas are not allowed in declare expressions. We don't allow this as the definition of most pragmas assume that they're given between entities. We also don't want to answer questions about conformance of pragmas, especially unrecognized pragmas and pragmas whose state can change between the specification and body.

### Syntax

The forms of List, Page, and Optimize pragmas are as follows:

```
pragma List(identifier);
pragma Page;
pragma Optimize(identifier);
```

[Other pragmas are defined throughout this Reference Manual, and are summarized in Annex L.]

### Static Semantics

A `pragma List` takes one of the identifiers `On` or `Off` as the single argument. This pragma is allowed anywhere a `pragma` is allowed. It specifies that listing of the compilation is to be continued or suspended until a List `pragma` with the opposite argument is given within the same compilation. The `pragma` itself is always listed if the compiler is producing a listing.

A `pragma Page` is allowed anywhere a `pragma` is allowed. It specifies that the program text which follows the `pragma` should start on a new page (if the compiler is currently producing a listing).

A `pragma Optimize` takes one of the identifiers `Time`, `Space`, or `Off` as the single argument. This `pragma` is allowed anywhere a `pragma` is allowed, and it applies until the end of the immediately enclosing declarative region, or for a `pragma` at the place of a `compilation_unit`, to the end of the compilation. It gives advice to the implementation as to whether time or space is the primary optimization criterion, or that optional optimizations should be turned off. [It is implementation defined how this advice is followed.]

### Implementation defined

Effect of `pragma Optimize`.

### Discussion

For example, a compiler might use Time vs. Space to control whether generic instantiations are implemented with a macro-expansion model, versus a shared-generic-body model.

We don't define what constitutes an “optimization” — in fact, it cannot be formally defined in the context of Ada. One compiler might call something an optional optimization, whereas another compiler might consider that same thing to be a normal part of code generation. Thus, the programmer cannot rely on this `pragma` having any particular portable effect on the generated code. Some compilers might even ignore the `pragma` altogether.
Examples

Examples of pragmas:

```
{AI95-00433-01} {AI05-0229-1} {AI12-0417-1} pragma List(Off); -- turn off listing generation
pragma Optimize(Off); -- turn off optional optimizations
pragma Assertion_Policy(Check); -- check assertions
pragma Pure(Rational_Numbers); -- set categorization for package
pragma Assert(Exists(File_Name), Message => "Nonexistent file"); -- assert file exists
pragma Inline(Set_Mask); -- generate code for Set_Mask inline
pragma Import(C, Put_Char, External_Name => "putchar"); -- import C putchar function
pragma Suppress(Range_Check, On => Index); -- turn off range checking on Index
```

Extensions to Ada 83

The Optimize pragma now allows the identifier Off to request that normal optimization be turned off.

An Optimize pragma may appear anywhere pragmas are allowed.

**Wording Changes from Ada 83**

We now describe the pragmas Page, List, and Optimize here, to act as examples, and to remove the normative material from Annex L, “Language-Defined Pragmas”, so it can be entirely an informative annex.

**Wording Changes from Ada 95**

```
{AI95-00433-01} Updated the example of named pragma parameters, because the second parameter of pragma Suppress is obsolescent.
```

**Wording Changes from Ada 2005**

```
{AI05-0229-1} Updated the example of pragmas, because both pragmas Inline and Import are obsolescent.
```

2.9 Reserved Words

**Syntax**

```
This paragraph was deleted.
```

```
{AI95-00284-02} {AI95-00395-01} {AI05-0091-1} The following are the reserved words. Within a program, some or all of the letters of a reserved word may be in upper case, and one or more characters in category other_format may be inserted within or at the end of the reserved word (ignoring upper/lower case distinctions):
```

Discussion: Reserved words have special meaning in the syntax. In addition, certain reserved words are used as attribute names.

The syntactic category identifier no longer allows reserved words. We have added the few reserved words that are legal explicitly to the syntax for attribute_reference. Allowing identifier to include reserved words has been a source of confusion for some users, and differs from the way they are treated in the C and Pascal language definitions.

```
{AI12-0005-1} Reserved words are sometimes called keywords in informal material.
```
The reserved words appear in lower case boldface in this document, except when used in the designator of an attribute (see 4.1.4). Lower case boldface is also used for a reserved word in a string literal used as an operator symbol. This is merely a convention — programs can be written in whatever typeface is desired and available.

Incompatibilities With Ada 83

The following words are not reserved in Ada 83, but are reserved in Ada 95: abstract, aliased, protected, requeue, tagged, until.

Wording Changes from Ada 83

The subclause entitled “Allowed Replacements of Characters” has been moved to Annex J, “Obsolescent Features”.

Incompatibilities With Ada 95

The following words are not reserved in Ada 95, but are reserved in Ada 2005: interface, overriding, synchronized. A special allowance is made for pragma Interface (see J.12). Uses of these words as identifiers will need to be changed, but we do not expect them to be common.

Wording Changes from Ada 95

The definition of upper case equivalence has been modified to allow identifiers using all of the characters of ISO 10646. This change has no effect on the character sequences that are reserved words, but does make some unusual sequences of characters illegal.

Incompatibilities With Ada 2005

Correction: Removed other format characters from reserved words in order to be compatible with the latest Unicode recommendations. This change can only affect programs written for original Ada 2005, and there is little reason to put other format characters into reserved words in the first place, so there should be very few such programs.

The following word is not reserved in Ada 2005, but is reserved in Ada 2012: some. Uses of this word as an identifier will need to be changed, but we do not expect them to be common.
Incompatibilities With Ada 2012

\{AI12-0119-1\} The following word is not reserved in Ada 2012, but is reserved in Ada 2022: parallel. Uses of this word as an identifier will need to be changed, but we do not expect them to be common.
3 Declarations and Types

This clause describes the types in the language and the rules for declaring constants, variables, and named numbers.

3.1 Declarations

The language defines several kinds of named entities that are declared by declarations. The entity's name is defined by the declaration, usually by a defining_identifier, but sometimes by a defining_character_literal or defining_operator_symbol. There are also entities that are not directly declared; some of these are elements of other entities, or are allocated dynamically. Such entities can be denoted using indexed_component, selected_component, or dereference names (see 4.1).

Discussion: Some entities are always anonymous. For instance, a type is never named (the name represents the first subtype). We don't mention those here as this paragraph is about named entities.

There are several forms of declaration. A basic_declaration is a form of declaration defined as follows.

\begin{verbatim}
basic_declaration ::= type_declaration | subtype_declaration | object_declaration | number_declaration | subprogram_declaration | abstract_subprogram_declaration | null_procedure_declaration | expression_function_declaration | package_declaration | renaming_declaration | exception_declaration | generic_declaration | generic_instantiation | defining_identifier ::= identifier
\end{verbatim}

A declaration is a language construct that associates a name with (a view of) an entity. A declaration may appear explicitly in the program text (an explicit declaration), or may be supposed to occur at a given place in the text as a consequence of the semantics of another construct (an implicit declaration).

Discussion: An implicit declaration generally declares a predefined or inherited operation associated with the definition of a type. This term is used primarily when allowing explicit declarations to override implicit declarations, as part of a type declaration.

Term entry: declaration — language construct that associates a name with (a view of) an entity

Note: A declaration can appear explicitly in the program text (an explicit declaration), or can be supposed to occur at a given place in the text as a consequence of the semantics of another construct (an implicit declaration).

Each of the following is defined to be a declaration: any basic_declaration; an enumeration_literal_specification; a discriminant_specification; a component_declaration; a defining_identifier of an iterated_component association; a loop_parameter_specification; a defining_identifier of a chunk_specification; an iterator_specification; a defining_identifier of an iterator parameter specification; a parameter_specification; a subprogram_body; an extended_return_object_declaration; an entry_declaration; an...
entry_index_specification; a choice_parameter_specification; a generic_formal_parameter_-declaration. In addition, an extended_return_statement is a declaration of its defining_identifier.

6.a  
Discussion: This list (when basic_declaration is expanded out) contains all syntactic categories that end in "/declaration" or "/specification", except for program_unit_specifications. Moreover, it contains subprogram_body. A subprogram_body is a declaration, whether or not it completes a previous declaration. This is a bit strange, subprogram_body is not part of the syntax of basic_declaration or library_unit_declaration. A renaming-as-body is considered a declaration. An accept_statement is not considered a declaration. Completions are sometimes declarations, and sometimes not.

7  
All declarations contain a definition for a view of an entity. A view consists of an identification of the entity (the entity of the view), plus view-specific characteristics that affect the use of the entity through that view (such as mode of access to an object, formal parameter names and defaults for a subprogram, or visibility to components of a type). In most cases, a declaration also contains the definition for the entity itself (a renaming_declaration is an example of a declaration that does not define a new entity, but instead defines a view of an existing entity (see 8.5)).

7.a.1/5  
Term entry: view of an entity — representation of an entity that reveals some or all of the properties of the entity. 
Note: A single entity can have multiple views.

7.a  
Discussion: Most declarations define a view (of some entity) whose view-specific characteristics are unchanging for the life of the view. However, subtypes are somewhat unusual in that they inherit characteristics from whatever view of their type is currently visible. Hence, a subtype is not a view of a type; it is more of an indirect reference. By contrast, a private type provides a single, unchanging (partial) view of its full type.

7.1/3  
\{AI05-0080-1\} When it is clear from context, the term object is used in place of view of an object. Similarly, the terms type and subtype are used in place of view of a type and view of a subtype, respectively.

7.b/3  
Discussion: Rules interpreted at compile time generally refer to views of entities, rather than the entities themselves. This is necessary to preserve privacy: characteristics that are not visible should not be used in compile-time rules. Thus, Static Semantics and Legality Rules generally implicitly have “view of”: Legality Rules that need to look into the private part are the exception to this interpretation.

7.c/3  
On the other hand, run-time rules can work either way, so “view of” should not be assumed in Dynamic Semantics rules.

7.d/5  
\{AI12-0191-1\} For example, a reference to the components of an object in a rule that is interpreted at compile time would not apply to components that are not visible. On the other hand, a reference to the components of an object in a dynamic semantics rule would apply to all components of the object, visible or not, including (for tagged objects) components which are not components of the nominal type of the object (see 3.9.1). Other terms, such as "subcomponent" and "part", are interpreted analogously.

8  
For each declaration, the language rules define a certain region of text called the scope of the declaration (see 8.2). Most declarations associate an identifier with a declared entity. Within its scope, and only there, there are places where it is possible to use the identifier to refer to the declaration, the view it defines, and the associated entity; these places are defined by the visibility rules (see 8.3). At such places the identifier is said to be a name of the entity (the direct_name or selector_name); the name is said to denote the declaration, the view, and the associated entity (see 8.6). The declaration is said to declare the name, the view, and in most cases, the entity itself.

9  
As an alternative to an identifier, an enumeration literal can be declared with a character_literal as its name (see 3.5.1), and a function can be declared with an operator_symbol as its name (see 6.1).

10  
The syntax rules use the terms defining_identifier, defining_character_literal, and defining_operator_symbol for the defining occurrence of a name; these are collectively called defining names. The terms direct_name and selector_name are used for usage occurrences of identifiers, character_literals, and operator_symbols. These are collectively called usage names.

To be honest: The terms identifier, character_literal, and operator_symbol are used directly in contexts where the normal visibility rules do not apply (such as the identifier that appears after the end of a task_body). Analogous conventions apply to the use of designator, which is the collective term for identifier and operator_symbol.
The process by which a construct achieves its run-time effect is called *execution*. This process is also called *elaboration* for declarations and *evaluation* for expressions. One of the terms execution, elaboration, or evaluation is defined by this Reference Manual for each construct that has a run-time effect.

**Term entry: execution** — process by which a construct achieves its run-time effect

Note: Execution of a declaration is also called elaboration. Execution of an expression is also called evaluation.

To be honest: The term elaboration is also used for the execution of certain constructs that are not declarations, and the term evaluation is used for the execution of certain constructs that are not expressions. For example, `subtype_indications` are elaborated, and `ranges` are evaluated.

For bodies, execution and elaboration are both explicitly defined. When we refer specifically to the execution of a body, we mean the explicit definition of execution for that kind of body, not its elaboration.

Discussion: Technically, "the execution of a declaration" and "the elaboration of a declaration" are synonymous. We use the term "elaboration" of a construct when we know the construct is elaborable; when we are talking about more arbitrary constructs, we use the term "execution". For example, we use the term "erroneous execution", to refer to any erroneous execution, including erroneous elaboration or evaluation.

When we explicitly define evaluation or elaboration for a construct, we are implicitly defining execution of that construct.

We also use the term "execution" for things like statements, which are executable, but neither elaborable nor evaluable. We considered using the term "execution" only for nonelaborable, nonevaluable constructs, and defining the term "action" to mean what we have defined "execution" to mean. We rejected this idea because we thought three terms that mean the same thing was enough — four would be overkill. Thus, the term "action" is used only informally in the standard (except where it is defined as part of a larger term, such as "protected action").

**Term entry: elaboration** — process by which a declaration achieves its run-time effect

Note: Elaboration is one of the forms of execution.

**Term entry: evaluation** — process by which an expression achieves its run-time effect

Note: Evaluation is one of the forms of execution.

To be honest: A construct is *elaborable* if elaboration is defined for it. A construct is *evaluable* if evaluation is defined for it. A construct is *executable* if execution is defined for it.

Discussion: Don't confuse “elaborable” with “preelaborable” (defined in 10.2.1).

The following are evaluable: `expression`; `name prefix`; `range`; `entry_index_specification` entry index iterator; and possibly `discrete_range`. The last one is curious — RM83 uses the term “evaluation of a discrete_range”, but never defines it. One might presume that the evaluation of a `discrete_range` consists of the evaluation of the `range` or the `subtype_indication`, depending on what it is. But `subtype_indications` are not evaluated; they are elaborated.

Intuitively, an executable construct is one that has a defined run-time effect (which may be null). Since execution includes elaboration and evaluation as special cases, all elaborable and all evaluable constructs are also executable. Hence, most constructs in Ada are executable. An important exception is that the constructs inside a generic unit are not executable directly, but rather are used as a template for (generally) executable constructs in instances of the generic.

NOTE At compile time, the declaration of an entity *declares* the entity. At run time, the elaboration of the declaration *creates* the entity.

**Ramification:** Syntactic categories for declarations are named either `entity_declaration` (if they include a trailing semicolon) or `entity_specification` (if not).

The various kinds of named entities that can be declared are as follows: an object (including components and parameters), a named number, a type (the name always refers to its first subtype), a subtype, a subprogram (including enumeration literals and operators), a single entry, an entry family, a package, a protected or task unit (which corresponds to either a type or a single object), an exception, a generic unit, a label, and the name of a statement.

Identifiers are also associated with names of pragmas, arguments to pragmas, and with attributes, but these are not user-definable.

**Wording Changes from Ada 83**

The syntax rule for `defining_identifier` is new. It is used for the defining occurrence of an identifier. Usage occurrences use the `direct_name` or `selector_name` syntactic categories. Each occurrence of an identifier (or `simple_name`), `character_literal`, or `operator_symbol` in the Ada 83 syntax rules is handled as follows in Ada 95:
12.e  • It becomes a defining_identifier, defining_character_literal, or defining_operator_symbol (or some syntactic
category composed of these), to indicate a defining occurrence;
12.f  • It becomes a direct_name, in usage occurrences where the usage is required (in Clause 8 to be directly
visible;
12.g  • It becomes a selector_name, in usage occurrences where the usage is required (in Clause 8) to be visible but
not necessarily directly visible;
12.h  • It remains an identifier, character_literal, or operator_symbol, in cases where the visibility rules do not
apply (such as the designator that appears after the end of a subprogram_body).
12.i  For declarations that come in “two parts” (program unit declaration plus body, private or incomplete type plus full
type, deferred constant plus full constant), we consider both to be defining occurrences. Thus, for example, the syntax
for package_body uses defining_identifier after the reserved word body, as opposed to direct_name.
12.j  The defining occurrence of a statement name is in its implicit declaration, not where it appears in the program text.
Considering the statement name itself to be the defining occurrence would complicate the visibility rules.
12.k  The phrase “visible by selection” is not used in Ada 95. It is subsumed by simply “visible” and the Name Resolution
Rules for selector_names.
{AI05-0299-1} (Note that in Ada 95, a declaration is visible at all places where one could have used a selector_name,
not just at places where a selector_name was actually used. Thus, the places where a declaration is directly visible are
a subset of the places where it is visible. See Clause 8 for details.)
12.l  We use the term “declaration” to cover _specifications that declare (views of) objects, such as
parameter_specifications. In Ada 83, these are referred to as a “form of declaration”, but it is not entirely clear that
they are considered simply “declarations”.
{AI05-0299-1} RM83 contains an incomplete definition of "elaborated" in this subclause: it defines "elaborated"
for declarations, declarative_parts, declarative_items and compilation_units, but "elaboration" is defined elsewhere
for various other constructs. To make matters worse, Ada 95 has a different set of elaborable constructs. Instead of
correcting the list, it is more maintainable to refer to the term "elaborable," which is defined in a distributed manner.
12.m  RM83 uses the term "has no other effect" to describe an elaboration that doesn't do anything except change the state
from not-yet-elaborated to elaborated. This was a confusing wording, because the answer to “other than what?” was to
be found many pages away. In Ada 95, we change this wording to “has no effect” (for things that truly do nothing at
run time), and "has no effect other than to establish that so-and-so can happen without failing the Elaboration_Check”
(for things where it matters).
12.n  We make it clearer that the term "execution" covers elaboration and evaluation as special cases. This was implied in
RM83. For example, "erroneous execution" can include any execution, and RM83-9.4(3) has, "The task designated by
any other task object depends on the master whose execution creates the task object;” the elaboration of the master's
declarative_part is doing the task creation.

Wording Changes from Ada 95

12.q  {AI95-00318-02} Added extended_return_statement to the list of declarations.
12.r  {AI95-00348-01} Added null procedures (see 6.7) to the syntax.

Wording Changes from Ada 2005

12.s  {AI05-0177-1} Added expression functions (see 6.8) to the syntax.

3.2 Types and Subtypes

Static Semantics

A type is characterized by a set of values, and a set of primitive operations which implement the
fundamental aspects of its semantics. An object of a given type is a run-time entity that contains (has) a
value of the type.

Term entry: type — defining characteristic of each object and expression of the language, with an associated set of
values, and a set of primitive operations that implement the fundamental aspects of its semantics.
Note: Types are grouped into categories. Most language-defined categories of types are also classes of types.

Term entry: subtype — type together with optional constraints, null exclusions, and predicates, which constrain the
values of the type to the subset that satisfies the implied conditions.
Types are grouped into categories of types, reflecting the similarity of their values and primitive operations. There exist several language-defined categories of types (summarized in the NOTE below), reflecting the similarity of their values and primitive operations. [Most categories of types form classes of types.] Elementary types are those whose values are logically indivisible; composite types are those whose values are composed of component values.

Proof: The formal definition of category and class is found in 3.4.

Term entry: class of types — set of types that is closed under derivation, which means that if a given type is in the class, then all types derived from that type are also in the class.

Note: The set of types of a class share common properties, such as their primitive operations.

Term entry: category of types — set of types with one or more common properties, such as primitive operations.

Note: A category of types that is closed under derivation is also known as a class.

Term entry: elementary type — type that does not have components.

Term entry: composite type — type with components, such as an array or record.

Term entry: scalar type — either a discrete type or a real type.

Term entry: access type — type that has values that designate aliased objects.

Note: Access types correspond to “pointer types” or “reference types” in some other languages.

Term entry: discrete type — type that is either an integer type or an enumeration type.

Note: Floating point and fixed point types are real types.

Term entry: integer type — type that represents signed or modular integers.

Note: A signed integer type has a base range that includes both positive and negative numbers, and has operations that can raise an exception when the result is outside the base range. A modular type has a base range whose lower bound is zero, and has operations with “wraparound” semantics. Modular types subsume what are called “unsigned types” in some other languages.

Term entry: enumeration type — type defined by an enumeration of its values, which can be denoted by identifiers or character literals.

Term entry: character type — enumeration type whose values include characters.

Term entry: record type — composite type consisting of zero or more named components, possibly of different types.

Term entry: record extension — type that extends another type optionally with additional components.

Term entry: array type — composite type whose components are all of the same type.

Term entry: task type — composite type used to represent active entities which execute concurrently and that can communicate via queued task entries.

Note: The top-level task of a partition is called the environment task.

Term entry: protected type — composite type whose components are accessible only through one of its protected operations, which synchronize concurrent access by multiple tasks.

Term entry: partial view — view of a type that reveals only some of its properties.

Note: The remaining properties are defined by the full view given elsewhere.

Term entry: full view — view of a type that reveals all of its properties.

Note: There can be other views of the type that reveal fewer properties.

Term entry: incomplete view — view of a type that reveals minimal properties.

Note: The remaining properties are defined by the full view given elsewhere.

Term entry: private type — type that defines a partial view.

Note: Private types can be used for defining abstractions that hide unnecessary details from their clients.

Term entry: private extension — type that extends another type, with the additional properties hidden from its clients.

Term entry: full type — type that defines a full view.

Term entry: incomplete type — type that defines an incomplete view.

Note: Incomplete types can be used for defining recursive data structures.
The elementary types are the scalar types (discrete and real) and the access types (whose values provide access to objects or subprograms). Discrete types are either integer types or are defined by enumeration of their values (enumeration types). Real types are either floating point types or fixed point types.

The composite types are the record types, record extensions, array types, interface types, task types, and protected types. A private type or private extension represents a partial view (see 7.3) of a type, providing support for data abstraction. A partial view is a composite type.

There can be multiple views of a type with varying sets of operations. An incomplete type represents an incomplete view (see 3.10.1) of a type with a very restricted usage, providing support for recursive data structures. A private type or private extension represents a partial view (see 7.3) of a type, providing support for data abstraction. The full view (see 3.2.1) of a type represents its complete definition. An incomplete or partial view is considered a composite type, even if the full view is not.

The term subcomponent is used in this Reference Manual in place of the term subfield. The intuitive meaning of “subfield” here is designed to simplify rules elsewhere. By design, the intuitive meaning of “subfield” will convey the correct result to the casual reader, while this formalistic definition will answer the concern of the compiler-writer.

We use the term “part” when talking about the parent part, ancestor part, or extension part of a type extension. In contexts such as these, the part might represent an empty set of subcomponents (e.g. in a null record extension, or a nonnull extension of a null record). We also use “part” when specifying rules such as those that apply to an object with a “controlled part” meaning that it applies if the object as a whole is controlled, or any subcomponent is.

The set of possible values for an object of a given type can be subjected to a condition that is called a constraint (the case of a null constraint that specifies no restriction is also included); the rules for which values satisfy a given kind of constraint are given in 3.5 for range constraints, 3.6.1 for index constraints, and 3.7.1 for discriminant constraints. The set of possible values for an object of an access type can also be subjected to a condition that excludes the null value (see 3.10).

A subtype of a given type is a combination of the type, a constraint on values of the type, and certain attributes specific to the subtype. The given type is called the type of the subtype of the subtype. Similarly, the associated constraint is called the constraint of the subtype of the subtype. The set of values of a subtype consists of the values of its type that satisfy its constraint and any exclusion of the null value. Such values belong to the subtype.

The other values of the type are outside the subtype.
A subtype is called an *unconstrained* subtype if its type has unknown discriminants, or if its type allows range, index, or discriminant constraints, but the subtype does not impose such a constraint; otherwise, the subtype is called a *constrained* subtype (since it has no unconstrained characteristics).

**Discussion:** In an earlier version of Ada 9X, "constrained" meant "has a nonnull constraint." However, we changed to this definition since we kept having to special case composite non-array/nondiscriminated types. It also corresponds better to the (now obsolete) attribute 'Constrained.

For scalar types, "constrained" means "has a nonnull constraint". For composite types, in implementation terms, "constrained" means that the size of all objects of the subtype is the same, assuming a typical implementation model.

Class-wide subtypes are always unconstrained.

**NOTE** Any set of types can be called a “category” of types, and any set of types that is closed under derivation (see 3.4) can be called a “class” of types. However, only certain categories and classes are used in the description of the rules of the language — generally those that have their own particular set of primitive operations (see 3.2.3), or that correspond to a set of types that are matched by a given kind of generic formal type (see 12.5). The following are examples of “interesting” language-defined classes: elementary, scalar, discrete, enumeration, character, boolean, integer, signed integer, modular, real, floating point, fixed point, decimal fixed point, numeric, access, access-to-object, access-to-subprogram, composite, array, string, (untagged) record, tagged, task, protected, nonlimited. Special syntax is provided to define types in each of these classes. In addition to these classes, the following are examples of “interesting” language-defined categories: abstract, incomplete, interface, limited, private, record.

**Discussion:** A value is a run-time entity with a given type which can be assigned to an object of an appropriate subtype of the type. An operation is a program entity that operates on zero or more operands to produce an effect, or yield a result, or both.

**Ramification:** Note that a type's category (and class) depends on the place of the reference — a private type is composite outside and possibly elementary inside. It's really the view that is elementary or composite. Note that although private types are composite, there are some properties that depend on the corresponding full view — for example, parameter passing modes, and the constraint checks that apply in various places.

**AI95-00442-01** Every property of types forms a category, but not every property of types represents a class. For example, the set of all abstract types does not form a class, because this set is not closed under derivation. Similarly, the set of all interface types does not form a class.

The set of limited types does not form a class (since nonlimited types can inherit from limited interfaces), but the set of nonlimited types does. The set of tagged record types and the set of tagged private types do not form a class (because each of them can be extended to create a type of the other category); that implies that the set of record types and the set of private types also do not form a class (even though untagged record types and untagged private types do form a class). In all of these cases, we can talk about the category of the type; for instance, we can talk about the “category of limited types” forms a class in the sense that it is closed under derivation, but the more interesting class, from the point of generic formal type matching, is the set of all types, limited and nonlimited, since that is what matches a generic formal “limited” private type. Note also that a limited type can "become nonlimited" under certain circumstances, which makes "limited" somewhat problematic as a class of types.

**AI95-00442-01** Normatively, the language-defined classes are those that are defined to be inherited on derivation by 3.4; other properties either aren't interesting or form categories, not classes.

These language-defined categories are organized like this:

- **AI95-00345-01** all types
  - **AI95-00442-01** elementary
    - **AI95-00442-01** scalar
There are other categories, such as the classes "numeric" and "discriminated nonlimited", which represent other classification dimensions, but and do not fit into the above strictly hierarchical picture.

Discussion: Note that this is also true for some categories mentioned in the chart. The category "task" includes both untagged tasks and tagged tasks. Similarly for "protected", "limited", and "nonlimited" (note that limited and nonlimited are not shown for untagged composite types).

Wording Changes from Ada 83

This subclause and its subclauses now precede the clause and subclauses on objects and named numbers, to cut down on the number of forward references.

We have dropped the term "base type" in favor of simply "type" (all types in Ada 83 were "base types" so it wasn't clear when it was appropriate/necessary to say "base type"). Given a subtype S of a type T, we call T the "type of the subtype S."

Wording Changes from Ada 95

Added a mention of null exclusions when we're talking about constraints (these are not constraints, but they are similar).

Defined an interface type to be a composite type.

Revised the wording so that it is clear that an incomplete view is similar to a partial view in terms of the language.

Added a definition of component of a type, subcomponent of a type, and part of a type. These are commonly used in the standard, but they were not previously defined.

Reworded most of this subclause to use category rather than class, since so many interesting properties are not, strictly speaking, classes. Moreover, there was no normative description of exactly which properties formed classes, and which did not. The real definition of class, along with a list of properties, is now in 3.4.
3.2.1 Type Declarations

A type_declaration declares a type and its first subtype.

Syntax

```
type_declaration ::= full_type_declaration |
                   incomplete_type_declaration |
                   private_type_declaration |
                   private_extension_declaration

{AI05-0183-1} full_type_declaration ::= type_defining_identifier [known_discriminant_part] is type_definition |
                                      [aspect_specification]; |
                                      task_type_declaration |
                                      protected_type_declaration

{AI95-00251-01} type_definition ::= enumeration_type_definition |
                                 integer_type_definition |
                                 real_type_definition |
                                 array_type_definition |
                                 record_type_definition |
                                 access_type_definition |
                                 derived_type_definition |
                                 interface_type_definition
```

Legality Rules

A given type shall not have a subcomponent whose type is the given type itself.

Static Semantics

{AI12-0449-1} The defining_identifier of a type_declaration denotes the first subtype of the type. The known_discriminant_part, if any, defines the discriminants of the type (see 3.7.3, “Discriminants”). The remainder of the type_declaration defines the remaining characteristics of (the view of) the type.

{AI95-00230-01} A type defined by a type_declaration is a named type; such a type has one or more nameable subtypes. Certain other forms of declaration also include type definitions as part of the declaration for an object (including a parameter or a discriminant). The type defined by such a declaration is anonymous — it has no nameable subtypes. For explanatory purposes, this document sometimes refers to an anonymous type by a pseudo-name, written in italics, and uses such pseudo-names at places where the syntax normally requires an identifier. For a named type whose first subtype is T, this document sometimes refers to the type of T as simply “the type T”.

Ramification: {AI95-00230-01} The only user-defined types that can be anonymous in the above sense are array, access, task, and protected types. An anonymous array, task, or protected type can be defined as part of an object_declaration. An anonymous access type can be defined as part of numerous other constructs as parameter or discriminant specification.

{AI95-00230-01} {AI95-00326-01} A named type that is declared by a full_type_declaration, or an anonymous type that is defined by an access_definition or as part of declaring an object of the type, is called a full type. The declaration of a full type also declares the full view of the type. The type_definition, task_definition, protected_definition, or access_definition that defines a full type is called a full type definition. [Types declared by other forms of type_declaration are not separate types; they are partial or incomplete views of some full type.]

To be honest: Class-wide, universal, and root numeric types are full types.

Reason: {AI95-00230-01} We need to mention access_definition separately, as it may occur in renames, which do not declare objects.
The definition of a type implicitly declares certain predefined operators that operate on the type, according to what classes the type belongs, as specified in 4.5.4.5, “Operators and Expression Evaluation”.

**Discussion:** We no longer talk about the implicit declaration of basic operations. These are treated like an if_statement — they don't need to be declared, but are still applicable to only certain classes of types.

The predefined types [(for example the types Boolean, Wide_Character, Integer, root_integer, and universal_integer)] are the types that are defined in [a predefined library package called] Standard; this package also includes the [(implicit)] declarations of their predefined operators. [The package Standard is described in A.1.]

**Ramification:** We use the term “predefined” to refer to entities declared in the visible part of Standard, to implicitly declared operators of a type whose semantics are defined by the language, to Standard itself, and to the "predefined environment". We do not use this term to refer to library packages other than Standard. For example Text_IO is a language-defined package, not a predefined package, and Text_IO.Put_Line is not a predefined operation.

**Dynamic Semantics**

The elaboration of a full_type_declaration consists of the elaboration of the full type definition. Each elaboration of a full type definition creates a distinct type and its first subtype.

**Reason:** The creation is associated with the type definition, rather than the type declaration, because there are types that are created by full type definitions that are not immediately contained within a type declaration (e.g. an array object declaration, a singleton task declaration, etc.).

**Ramification:** Any implicit declarations that occur immediately following the full type definition are elaborated where they (implicitly) occur.

**Examples**

**Examples of type definitions:**

(White, Red, Yellow, Green, Blue, Brown, Black)

range 1 .. 72

array(1 .. 10) of Integer

**Examples of type declarations:**

type Color is (White, Red, Yellow, Green, Blue, Brown, Black);
type Column is range 1 .. 72;
type Table is array(1 .. 10) of Integer;

**NOTE** Each of the above examples declares a named type. The identifier given denotes the first subtype of the type. Other named subtypes of the type can be declared with subtype_declarations (see 3.2.2). Although names do not directly denote types, a phrase like “the type Column” is sometimes used in this document to refer to the type of Column, where Column denotes the first subtype of the type. For an example of the definition of an anonymous type, see the declaration of the array Color_Table in 3.3.1; its type is anonymous — it has no nameable subtypes.

**Wording Changes from Ada 83**

The syntactic category full_type_declaration now includes task and protected type declarations.

**We have generalized the concept of first-named subtype (now called simply “first subtype”) to cover all kinds of types, for uniformity of description elsewhere. RM83 defined first-named subtype in Section 13. We define first subtype here, because it is now a more fundamental concept. We renamed the term, because in Ada 95 some first subtypes have no name.**

**AI95-00230-01** We no longer elaborate discriminant_parts, because there is nothing to do, and it was complex to say that you only wanted to elaborate it once for a private or incomplete type. This is also consistent with the fact that subprogram specifications are not elaborated (neither in Ada 83 nor in Ada 95). Note, however, that an access_definition appearing in a discriminant_part is elaborated at the full_type_declaration (for a nonlimited type) or when an object with such a discriminant is created (for a limited type).

**Wording Changes from Ada 95**

**AI95-00230-01** Added wording so that anonymous access types are always full types, even if they appear in renames.
3.2.2 Subtype Declarations

A subtype_declaration declares a subtype of some previously declared type, as defined by a subtype_indication.

Syntax

\[
\text{subtype} \text{ defining_identifier} \text{ is subtype} \text{ indication} \quad \text{[aspect} \text{ specification]};
\]

\[
\text{subtype} \text{ indication} ::= \quad \text{[null} \text{ exclusion]} \text{ subtype} \text{ mark} \text{ [constraint]}
\]

\[
\text{subtype} \text{ mark} ::= \text{ subtype} \text{ name}
\]

Ramification: Note that name includes attribute_reference; thus, S'Base can be used as a subtype_mark.

Reason: We considered changing subtype_mark to subtype_name. However, existing users are used to the word "mark," so we're keeping it.

constraint ::= scalar_constraint \text{ | composite} \text{ constraint}

scalar_constraint ::= \range_constraint \text{ | digits_constraint | delta} \text{ constraint}

composite_constraint ::= \index_constraint \text{ | discriminant} \text{ constraint}

Name Resolution Rules

A subtype_mark shall resolve to denote a subtype. The type determined by a subtype_mark is the type of the subtype denoted by the subtype_mark.

Ramification: Types are never directly named; all subtype_marks denote subtypes — possibly an unconstrained (base) subtype, but never the type. When we use the term anonymous type we really mean a type with no nameable subtypes.

Dynamic Semantics

The elaboration of a subtype_declaration consists of the elaboration of the subtype_indication. The elaboration of a subtype_indication creates a new subtype. If the subtype_indication does not include a constraint, the new subtype has the same (possibly null) constraint as that denoted by the subtype_mark. The elaboration of a subtype_indication that includes a constraint proceeds as follows:

• The constraint is first elaborated.

• A check is then made that the constraint is compatible with the subtype denoted by the subtype_mark.

Ramification: The checks associated with constraint compatibility are all Range_Checks. Discriminant_Checks and Index_Checks are associated only with checks that a value satisfies a constraint.

The condition imposed by a constraint is the condition obtained after elaboration of the constraint. The rules defining compatibility are given for each form of constraint in the appropriate subclause. These rules are such that if a constraint is compatible with a subtype, then the condition imposed by the
constraint cannot contradict any condition already imposed by the subtype on its values. The exception
Constraint_Error is raised if any check of compatibility fails.

To be honest: The condition imposed by a constraint is named after it — a range_constraint imposes a range
constraint, etc.

Ramification: A range_constraint causes freezing of its type. Other constraints do not.

NOTE {AI12-0440-1} A scalar_constraint can be applied to a subtype of an appropriate scalar type (see 3.5, 3.5.9,
and J.3), even if the subtype is already constrained. On the other hand, a composite_constraint can be applied to a
composite subtype (or an access-to-composite subtype) only if the composite subtype is unconstrained (see 3.6.1 and 3.7.1).

Examples

Examples of subtype declarations:

{AI95-00433-01} subtype Rainbow is Color range Red .. Blue; -- see 3.2.1
subtype Red_Blue is Rainbow;
subtype Int is Integer;
subtype Small_Int is Integer range -10 .. 10;
subtype Up_To_K is Column range 1 .. K; -- see 3.2.1
subtype Square is Matrix(1 .. 10, 1 .. 10); -- see 3.6
subtype Male is Person(Sex => M); -- see 3.10.1
subtype Binop_Ref is not null Binop_Ptr; -- see 3.10

Incompatibilities With Ada 83

In Ada 95, all range_constraints cause freezing of their type. Hence, a type-related representation item for a scalar
type has to precede any range_constraints whose type is the scalar type.

Wording Changes from Ada 83

Subtype_marks allow only subtype names now, since types are never directly named. There is no need for RM83-
3.3.2(3), which says a subtype_mark can denote both the type and the subtype; in Ada 95, you denote an
unconstrained (base) subtype if you want, but never the type.

The syntactic category type_mark is now called subtype_mark, since it always denotes a subtype.

Extensions to Ada 95

{AI95-00231-01} An optional null_exclusion can be used in a subtype_indication. This is described in 3.10.

Extensions to Ada 2005

{AI05-0183-1} An optional aspect_specification can be used in a subtype_declaration. This is described in 13.1.1.

3.2.3 Classification of Operations

Static Semantics

{AI95-00416-01} An operation operates on a type T if it yields a value of type T, if it has an operand
whose expected type (see 8.6) is T, or if it has an access parameter or access_result_type (see 6.1)
designating T. A predefined operator, or other language-defined operation such as assignment or a
membership test, that operates on a type, is called a predefined operation of the type. The primitive
operations of a type are the predefined operations of the type, plus any user-defined primitive
subprograms.

Term entry: primitive operations of a type — operations (such as subprograms) declared together with the type
declarations
Note: Primitive operations are inherited by other types in the same derivation class of types.

To be honest: Protected subprograms are not considered to be “primitive subprograms”, even though they are
subprograms, and they are inherited by derived types.

Discussion: We use the term “primitive subprogram” in most of the rest of the manual. The term “primitive operation”
is used mostly in conceptual discussions.

The primitive subprograms of a specific type are defined as follows:
• The predefined operators of the type (see 4.5);  
• For a derived type, the inherited (see 3.4) user-defined subprograms;  
• For an enumeration type, the enumeration literals (which are considered parameterless functions — see 3.5.1);  
• For a specific type declared immediately within a package_specification, any subprograms (in addition to the enumeration literals) that are explicitly declared immediately within the same package_specification and that operate on the type;  
• \{AI05-0128-1\} For a specific type with an explicitly declared primitive 
  \texttt{"\text{"}} operator whose result type is Boolean, the corresponding 
  \texttt{"\neq\text{"}} operator (see 6.6);  
• \{AI95-00200-01\} For a nonformal type, any subprograms not covered above [that are 
  explicitly declared immediately within the same declarative region as the type] and that 
  override (see 8.3) other implicitly declared primitive subprograms of the type.

Discussion: In Ada 83, only subprograms declared in the visible part were “primitive” (i.e. derivable). In Ada 95, mostly because of child library units, we include all operations declared in the private part as well, and all operations that override implicit declarations.

Ramification: It is possible for a subprogram to be primitive for more than one type, though it is illegal for a subprogram to be primitive for more than one tagged type. See 3.9.

Discussion: The order of the implicit declarations when there are both predefined operators and inherited subprograms is described in 3.4, “Derived Types and Classes”.

Ramification: \{AI95-00200-01\} Subprograms declared in a generic package specification are never primitive for a formal type, even if they happen to override an operation of the formal type. This includes formal subprograms, which are never primitive operations (that's true even for an abstract formal subprogram).

A primitive subprogram whose designator is an operator_symbol is called a primitive operator.

Incompatibilities With Ada 83

The attribute S'Base is no longer defined for nonscalar subtypes. Since this was only permitted as the prefix of another attribute, and there are no interesting nonscalar attributes defined for an unconstrained composite or access subtype, this should not affect any existing programs.

Extensions to Ada 83

The primitive subprograms (derivable subprograms) include subprograms declared in the private part of a package specification as well, and those that override implicitly declared subprograms, even if declared in a body.

Wording Changes from Ada 83

We have dropped the confusing term operation of a type in favor of the more useful primitive operation of a type and the phrase operates on a type.

The description of S'Base has been moved to 3.5, “Scalar Types” because it is now defined only for scalar types.

Wording Changes from Ada 95

\{AI95-00200-01\} Clarified that a formal subprogram that happens to override a primitive operation of a formal type is not a primitive operation (and thus not a dispatching operation) of the formal type.

\{AI95-00416-01\} Added wording to include access result types in the kinds of operations that operate on a type T.

Wording Changes from Ada 2005

\{AI05-0128-1\} Correction: The implicitly declared 
  \texttt{"\neq\text{"}} for a primitive 
  \texttt{"\text{"}} operator is also primitive; this makes it 
  eligible to be made visible by a use type clause.

3.2.4 Subtype Predicates

\{AI05-0153-3\} \{AI05-0269-1\} \{AI05-0299-1\} \{AI12-0396-1\} \{AI12-0419-1\} The language-defined predicate aspects Static_Predicate and Dynamic_Predicate may be used to define properties of subtypes.
A predicate specification is an aspect specification for one of the two predicate aspects. General rules for aspects and aspect specifications are found in Clause 13 (13.1 and 13.1.1 respectively). The predicate aspects are assertion aspects (see 11.4.2). [The predicate aspects are not inherited, but their effects are additive, as defined below.]

Aspect Description for Static Predicate: Condition that will must hold true for objects of a given subtype; the subtype may be static.

Aspect Description for Dynamic Predicate: Condition that will must hold true for objects of a given subtype; the subtype is not static.

Name Resolution Rules

The expected type for a predicate aspect expression is any boolean type.

Static Semantics

A predicate specification may be given on a type declaration or a subtype declaration, and applies to the declared subtype. In addition, predicate specifications apply to certain other subtypes:

- For a (first) subtype defined by a derived type declaration, any the predicates of the parent or subtype and the progenitor subtypes apply.
- For a subtype created by a subtype indication, the predicate of the subtype denoted by the subtype mark applies.

The predicate of a subtype consists of all predicate specifications that apply, and ed together; if no predicate specifications apply, the predicate is True [(in particular, the predicate of a base subtype is True)].

Predicate checks are defined to be enabled or disabled for a given subtype as follows:

- If a subtype is declared by a type declaration or subtype declaration that includes a predicate specification, then:
  - if performing checks is required by the Static Predicate assertion policy (see 11.4.2) and the declaration includes a Static Predicate specification, then predicate checks are enabled for the subtype;
  - if performing checks is required by the Dynamic Predicate assertion policy (see 11.4.2) and the declaration includes a Dynamic Predicate specification, then predicate checks are enabled for the subtype;
  - otherwise, predicate checks are disabled for the subtype[, regardless of whether predicate checking is enabled for any other subtypes mentioned in the declaration];

- If a subtype is defined by a derived type declaration that does not include a predicate specification, then predicate checks are enabled for the subtype if and only if any predicate checks are enabled for at least one of the parent or subtype and the progenitor subtypes;

- If a subtype is created by a subtype indication other than in one of the previous cases, then predicate checks are enabled for the subtype if and only if predicate checks are enabled for the subtype denoted by the subtype mark;

- Otherwise, predicate checks are disabled for the given subtype.

Discussion: In this case, no predicate specifications can apply to the subtype and so it doesn't typically matter whether predicate checks are enabled. This rule does make a difference, however, when determining whether predicate checks are enabled for another type when this type is one of multiple progenitors. See the "derived type declaration" wording above.

Even when predicate checks are disabled, a predicate can affect various Legality Rules, the results of membership tests, the items in a for loop, and the result of the Valid attribute.
For a subtype with a directly-specified predicate aspect, the following additional language-defined aspect may be specified with an aspect specification (see 13.1.1):

**Predicate Failure**

This aspect shall be specified by an expression, which determines the action to be performed when a predicate check fails because a directly-specified predicate aspect of the subtype evaluates to False, as explained below.

**Aspect Description for Predicate Failure:** Action to be performed when a predicate check fails.

**Name Resolution Rules**

The expected type for the Predicate Failure expression is String.

**Legality Rules**

The expression of a Static Predicate specification shall be predicate-static; that is, one of the following:

- a static expression;
- a membership test whose tested simple expressions is the current instance, and whose membership choice list meets the requirements for a static membership test (see 4.9);
- a case expression whose selecting expression is the current instance, and whose dependent expressions are static expressions;
- a call to a predefined equality or ordering operator, where one operand is the current instance, and the other is a static expression;
- a call to a predefined boolean logical operator and, or, xor, or not, where each operand is predicate-static;
- a short-circuit control form where both operands are predicate-static; or
- a parenthesized predicate-static expression.

A predicate shall not be specified for an incomplete subtype. The expression of such a predicate could not depend on the properties of the value of the type (since it doesn't have any), so it is useless and we don't want to require the added complexity needed to support it.

If a predicate applies to a subtype, then that predicate shall not mention any other subtype to which the same predicate applies.

Reason: This is intended to prevent recursive predicates, which cause definitional problems for static predicates. Inside of the predicate, the subtype name refers to the current instance of the subtype, which is an object, so a direct use of the subtype name cannot be recursive. But other subtypes naming the same type might:

```ada
type Really_Ugly is private;
private
    subtype Ugly is Really_Ugly;
    type Really_Ugly is new Integer
    with Static Predicate => Really_Ugly not in Ugly; -- Illegal!
```

An index subtype, discrete range of an index constraint or slice, or a discrete subtype definition of a constrained array definition, entry declaration, or entry index specification shall not denote a subtype to which predicate specifications apply.

The prefix of an attribute reference whose attribute_designator is First, Last, or Range shall not denote a scalar subtype to which predicate specifications apply.

Reason: This is to prevent confusion about whether the First value is the lowest value of the subtype (which does not depend on the predicate) or the lowest value of the subtype which meets the predicate. (For a dynamic predicate, determining this latter value is expensive as it would usually require a loop.) For a static subtype that has a static predicate, the First_Valid and Last_Valid attributes (see 3.5.5) can be used instead.
3.2.4 Subtype Predicates

The discrete subtype definition of a loop parameter specification shall not denote a nonstatic subtype to which predicate specifications apply or any subtype to which Dynamic Predicate specifications apply.

The discrete choice of a named_array_aggregate shall not denote a nonstatic subtype to which predicate specifications apply.

Reason: This rule prevents noncontiguous dynamically bounded array aggregates, which could be expensive to check for. (Array aggregates have rules to prevent problems with static subtypes.) We define this rule here so that the runtime generic body check applies.

In addition to the places where Legality Rules normally apply (see 12.3), these rules apply also in the private part of an instance of a generic unit.

Dynamic Semantics

If any of the above Legality Rules is violated in an instance of a generic unit, Program_Error is raised at the point of the violation.

Discussion: This is the usual way around the contract model; this applies even in instance bodies. Note that errors in instance specifications will be detected at compile time by the "recheck" of the specification; only errors in the body should raise Program_Error.

To determine whether a value satisfies the predicates of a subtype S, the following tests are performed in the following order, until one of the tests fails, in which case the predicates are not satisfied and no further tests are performed, or all of the tests succeed, in which case the predicates are satisfied:

• the value is first tested to determine whether it satisfies any constraints or any null exclusion of S;
• then:
  • if S is a first subtype, the value is tested to determine whether it satisfies the predicates of the parent and progenitor subtypes (if any) of S (in an arbitrary order), after a (view) conversion of the value to the corresponding parent or progenitor type;
  Ramification: This rule has an effect for derived types (which have a parent subtype and may have progenitors) and for task and protected types (which may have progenitors). Other kinds of type declarations can have neither, and no test is required for other first subtypes.
  • if S is defined by a subtype indication, the value is tested to determine whether it satisfies the predicates of the subtype denoted by the subtype mark of the subtype indication;
  • finally, if S is defined by a declaration to which one or more predicate specifications apply, the predicates are evaluated (in an arbitrary order) to test that all of them yield True for the given value.

Discussion: It is important to stop on the first of the above steps that fails, as later steps might presume that the earlier steps had succeeded.

If predicate checks are enabled for a given subtype, then:

On every subtype conversion, the predicate of the target subtype is evaluated, and a check is performed that the operand satisfies the predicates of the target subtype. The predicate is True, except for certain view conversions (see 4.6). This includes all parameter passing, except for certain parameters passed by reference, which are covered by the following rule: In addition, after normal completion and leaving of a subprogram, for each in out or out parameter that is passed by reference, a check is performed that the value of the parameter satisfies the predicates of the subtype of the actual value predicate is True. For an object created by an object declaration with no explicit initialization expression, or by an uninitialized allocator, if the types of any parts have specified Default Value or Default Component Value
aspects, or any subcomponents have default expressions, the predicate of the nominal subtype of the created object is evaluated, and a check is performed that the value of the created object satisfies the predicates of the nominal subtype. Predicate is True. Assertions.Assertion_Error is raised if any of these checks fail.

Ramification: \{AI12-0333-1\} Most parameter passing is covered by the subtype conversion rule: all inbound in and in out parameters are converted to the formal subtype, and the copy-back for by-copy out and in out parameters includes a conversion to the actual subtype. The remaining parameter-passing cases are covered by special rules: by-reference out and in out parameters by the rule given above, and we don’t want any predicate checks on inbound out parameters, accomplished in part by a special rule in 4.6.

\{AI12-0054-2\} If any of the predicate checks fail, Assertion_Error is raised, unless the subtype whose directly-specified predicate aspect evaluated to False also has a directly-specified Predicate_Failure aspect. In that case, the specified Predicate_Failure expression is evaluated; if the evaluation of the Predicate_Failure expression propagates an exception occurrence, then this occurrence is propagated for the failure of the predicate check; otherwise, Assertion_Error is raised, with an associated message string defined by the value of the Predicate_Failure expression. In the absence of such a Predicate_Failure aspect, an implementation-defined message string is associated with the Assertion_Error exception.

Ramification: Predicates are not evaluated at the point of the (sub)type declaration.  

Implementation Note: Static Predicate checks can be removed even in the presence of potentially invalid values, just as constraint checks can be removed.

Implementation defined: The message string associated with the Assertion_Error exception raised by the failure of a predicate check if there is no applicable Predicate_Failure aspect.

Paragraphs 32 and 33 were moved above

\{AI05-0262-1\} \{AI12-0071-1\} A value satisfies a predicate if the predicate is True for that value.

\{AI05-0153-3\} \{AI05-0276-1\} \{AI12-0071-1\} If any of the above Legality Rules is violated in an instance of a generic unit, Program_Error is raised at the point of the violation.

This paragraph was deleted Discussion: This is the usual way around the contract model; this applies even in instance bodies. Note that errors in instance specifications will be detected at compile time by the "re-check" of the specification, only errors in the body raise Program_Error.

NOTE 1 \{AI05-0153-3\} A predicate specification does not cause a subtype to be considered constrained.

NOTE 2 \{AI05-0153-3\} A Static.Predicate, like a constraint, always remains True for all objects of the subtype, except in the case of uninitialized variables and other invalid values. A Dynamic.Predicate, on the other hand, is checked as specified above, but can become False at other times. For example, the predicate of a record subtype is not checked when a subcomponent is modified.

NOTE 3 \{AI12-0071-1\} No predicates apply to the base subtype of a scalar type; every value of a scalar type \(T\) is considered to satisfy the predicates of \(T\)Base.

NOTE 4 \{AI12-0054-2\} Predicate Failure expressions are never evaluated during the evaluation of a membership test (see 4.5.2) or Valid attribute (see 13.9.2).

NOTE 5 \{AI12-0054-2\} A Predicate_Failure expression can be a raise_expression (see 11.3).

Examples

\{AI12-0429-1\} Examples of predicates applied to scalar types:

\{AI12-0054-2\} \texttt{subtype Basic Letter is Character -- See A.3.2 for "basic letter".} 
\hspace{1cm} \texttt{with Static Predicate => Basic Letter in 'A'..'Z' | 'a'..'z' | 'Æ' | 'æ' | 'Ð' | 'ð' | 'Þ' | 'þ' | 'ß';}

\{AI12-0054-2\} \texttt{subtype Even Integer is Integer} 
\hspace{1cm} \texttt{with Dynamic Predicate => Even Integer \mod 2 = 0,} 
\hspace{1cm} \texttt{Predicate_Failure => "Even Integer must be a multiple of 2";}
with Ada.IO_Exceptions;
package Ada.Text_IO is

  type File_Type is limited private;
  subtype Open_File_Type is File_Type;
    with Dynamic_Predicate => Is_Open (Open_File_Type),
        Predicate_Failure => raise Status_Error with "File not open";
  subtype Input_File_Type is Open_File_Type;
    with Dynamic_Predicate => Mode (Input_File_Type) = In_File,
        Predicate_Failure => raise Mode_Error
          with "Cannot read file: " & Name (Input_File_Type);
  subtype Output_File_Type is Open_File_Type;
    with Dynamic_Predicate => Mode (Output_File_Type) /= In_File,
        Predicate_Failure => raise Mode_Error
          with "Cannot write file: " & Name (Output_File_Type);

  function Mode (File : in Open_File_Type) return File_Mode;
  function Name (File : in Open_File_Type) return String;
  function Form (File : in Open_File_Type) return String;

  procedure Get (File : in Input_File_Type; Item : out Character);
  procedure Put (File : in Output_File_Type; Item : in Character);

  ... -- Similarly for all of the other input and output subprograms.

Discussion: We didn’t change the language-defined Text_IO this way for Ada 2022 as it would be incompatible in marginal cases; these subprogram specifications would not be subtype conformant with existing access-to-subprogram types, so Put_Line'Access (for instance) would become illegal in existing code. The gain would not be worth the disruption.

Extensions to Ada 2005

{AI05-0153-3} {AI05-0262-1} {AI05-0276-1} {AI05-0290-1} Predicate aspects are new in Ada 2012.

Inconsistencies With Ada 2012

{AI12-0301-1} Correction: Predicate checks are now performed on default-initialized objects with parts that have Default Value or Default Component Value specified. This is consistent with the handling of constraint checks for such objects; it is thought that the omission was unintended. However, a program that declares such an object and depends on there not being a predicate check in original Ada 2012 will fail in Ada 2022. As these attributes were new in Ada 2012, their use is uncommon, so we believe that this inconsistency will be rare and more likely to catch a bug than create one.

Extensions to Ada 2012

{AI12-0054-2} Corrigendum: The Predicate Failure aspect is new. We can consider this a correction as it is always possible for implementers to add implementation-defined aspects, so the same is true for language-defined aspects.

Wording Changes from Ada 2012

{AI12-0071-1} Corrigendum: Specified the order of evaluation of most predicates, by defining the new term "satisfies the predicates of the subtype". This is not inconsistent, as the order previously was unspecified, so any code depending on the order was incorrect. The change is necessary so that the Predicate Failure aspect has consistent results in cases where multiple predicates and aspects apply; see the Ada.Text_IO example above for such a case.

{AI12-0099-1} Corrigendum: Revised wording to ensure all kinds of types are covered, including the anonymous task associated with a single task declaration, and generalized it.

{AI12-0099-1} Corrigendum: Revised wording to list the boolean operators that can be predicate-static, to eliminate confusion about whether not is included.

{AI12-0333-1} {AI12-0432-1} Correction: Predicate checks are no longer made for any inbound out parameters nor for the target of an assignment_statement when it is a view conversion. The rule change for this is found in 4.6, so the inconsistency is documented there.
3.3 Objects and Named Numbers

[Objects are created at run time and contain a value of a given type. An object can be created and
initialized as part of elaborating a declaration, evaluating an allocator, aggregate, or function_call, or
passing a parameter by copy. Prior to reclaiming the storage for an object, it is finalized if necessary (see
7.6.1).]

Static Semantics

All of the following are objects:

- The entity declared by an object_declaration;
- A formal parameter of a subprogram, entry, or generic subprogram;
- A generic formal object;
- A loop parameter;
- {AI12-0061-1} the index parameter of an iterated_component_association;
- {AI12-0308-1} the chunk parameter of a chunk_specification;
- A choice parameter of an exception_handler;
- An entry index of an entry_body;
- The result of dereferencing an access-to-object value (see 4.1);
- {AI95-00416-01} {AI05-0015-1} the return object of a function created as the result of evaluating
  a function_call (or the equivalent operator invocation — see 6.6);
- The result of evaluating an aggregate;
- {AI12-0226-1} an qualified_expression whose operand denotes an object;
- A component, slice, or view conversion of another object.

{AI05-0054-2} An object is either a constant object or a variable object. The value of a constant object
cannot be changed between its initialization and its finalization, whereas the value of a variable object can
be changed. Similarly, a view of an object is either a constant or a variable. All views of a constant
elementary object are constant. All views of a constant composite object are constant, except for parts that
are of controlled or immutably limited types; variable views of those parts and their subcomponents may
exist. In this sense, objects of controlled and immutably limited types are inherently mutable. A constant
view of a variable object cannot be used to modify its value the value of the variable. The terms
constant and variable by themselves refer to constant and variable views of objects.

Ramification: {AI12-0222-1} If some part of an object has a variable view, then the object as a whole has a variable
view, and not all views of the object are constant. That's true even if only a subcomponent has a variable view.

{AI12-0222-1} A constant object is known to have no variable views if it does not have a part that is
immutably limited, or of a controlled type, private type, or private extension.

Reason: {AI12-0222-1} This definition can be used in Legality Rules as it respects privacy. It is an assume-the-worst
rule, as all private types and private extensions might have a controlled component.

The value of an object is read when the value of any part of the object is evaluated, or when the value of
an enclosing object is evaluated. The value of a variable is updated when an assignment is performed to
any part of the variable, or when an assignment is performed to an enclosing object.
Ramification: Reading and updating are intended to include read/write references of any kind, even if they are not associated with the evaluation of a particular construct. Consider, for example, the expression “X.all(F)”, where X is an access-to-array object, and F is a function. The implementation is allowed to first evaluate “X.all” and then F. Finally, a read is performed to get the value of the F'th component of the array. Note that the array is not necessarily read as part of the evaluation of “X.all”. This is important, because if F were to free X using Unchecked_Deallocation, we want the execution of the final read to be erroneous.

15/5 \AI12-0392-1\ Whether a view of an object is constant or variable is determined by the definition of the view. The following (and no others) represent variables:

16/5

- \AI12-0392-1\ an object declared by an object_declaration without the reserved word constant;
- \AI12-0392-1\ a formal parameter or generic formal object of mode in out or outin;
- \AI12-0392-1\ a generic formal object of mode in out;
- \AI12-0392-1\ a non-discriminant component of a variable discriminant;
- \AI12-0392-1\ a slice of a variable;
- \AI12-0392-1\ a loop parameter that is unless specified to be a variable for a generalized loop (see 5.5.2);
- \AI12-0392-1\ a view conversion of a variable loop parameter, choice parameter, or entry index;
- \AI12-0392-1\ the dereference of an access-to-variable value conversion to constant value;
- \AI12-0392-1\ the return object declared by an extended return statement without the reserved word constant;
- \AI12-0392-1\ the current instance of a type other than a protected type, if the current instance is an object and not a value (see 8.6) object denoted by result of evaluating a function_call or an aggregate;
- \AI05-0003-1\ The result of evaluating a qualified_expression;
- \AI12-0392-1\ the current instance of a protected unit except within the body of a protected function of that protected unit, or within (or a function declared immediately within the body of the protected_body), the current instance of the enclosing protected unit;
- \AI12-0392-1\ an attribute reference where the attribute is defined to denote a variable (for example, the Storage_Pool attribute – see 13.11) a selected_component, indexed_component, slice, or view conversion of a constant.

Ramification: \AI12-0392-1\ In particular, this implies that the following are not variables:

- \AI12-0226-1\ the result of evaluating a function_call, an aggregate, a value conversion, a qualified_expression, a conditional_expression, a raise_expression, or a parenthesized expression;
- \AI12-0125-3\ a target_name of an assignment_statement (see 5.2.1);
- \AI12-0061-1\ the index parameter of an iterated_component_association;
- \AI12-0392-1\ a choice parameter or entry index;
{AI12-0308-1} A chunk parameter of a chunk specification.

{AI12-0392-1} This list of constructs that yield constant views is not exhaustive.

To be honest: {AI95-00114-01} A noninvertible view conversion to a general access type is also defined to be a constant — see 4.6.

{AI05-0264-1} {AI12-0191-1} {AI12-0294-1} At the place where a view of an object is defined, a nominal subtype of the view. The object's actual subtype (that is, its subtype) can be more restrictive than the nominal subtype of the view; it always is more restrictive if the nominal subtype is an indefinite subtype. A subtype is an indefinite subtype if it is an unconstrained array subtype, or if it has unknown discriminants or unconstrained discriminants without defaults (see 3.7); otherwise, the subtype is a definite subtype [(all elementary subtypes are definite subtypes)]. [A class-wide subtype is defined to have unknown discriminants, and is therefore an indefinite subtype. An indefinite subtype does not by itself provide enough information to create an object; an additional constraint or explicit initialization expression is necessary (see 3.3.1). A component cannot have an indefinite nominal subtype.]

Term entry: nominal subtype — subtype specified when a view of an object is defined

{AI10-0008-1} A view of a composite object is known to be constrained if:

- {AI12-0401-1} its nominal subtype is constrained and, and is not an untagged partial view, and it is neither a value conversion nor a qualified expression, or
- its nominal subtype is indefinite; or
- {AI05-0008-1} {AI05-0093-1} its type is immutably limited (see 7.5); or
- it is part of a stand-alone constant (including a generic formal object of mode in); or
- it is part of a formal parameter of mode in; or
- it is part of the object denoted by a function_call or aggregate; or
- {AI12-0226-1} {AI12-0228-1} it is a value conversion or qualified expression where the operand denotes a view of a composite object that is known to be constrained; or
- {AI12-0228-1} it is part of a constant return object of an extended_return_statement; or
- {AI05-0008-1} {AI05-0041-1} {AI12-0228-1} it is a dereference of a pool-specific access type, and there is no ancestor of its type that has a constrained partial view.

Discussion: We do not include dereferences of general access types because they might denote stand-alone aliased unconstrained variables. That's true even for access-to-constant types (the denoted object does not have to be a constant).

{AI05-0005-1} {AI05-0008-1} {AI12-0228-1} We don't mention view conversions as there are no mutable tagged types (discriminant defaults are allowed only if the type is immutably limited), so all tagged view conversions are either of an indefinite type (if it has discriminants without defaults), an immutably limited type (if the discriminants do have defaults), or constrained (if there are no discriminants). This matches the first three bullets here, so all tagged view conversions are known to be constrained without needing to mention them explicitly. Untagged view conversions only can occur in parameter passing (as actuals to in_out or out parameters), and "known to be constrained" is not used there. There are other cases that could have been included in this definition (view conversions, the current instance of a type, objects of a formal discriminated private type), but these are not relevant to the places this term is used, so they were not included. If this term is used in additional places, the definition should be checked to see if any of these additional cases are relevant and appropriate wording added if necessary.

{AI12-0228-1} We don't need to mention the current instance of a (sub)type, either. If a current instance of a type or subtype appears in an aspect specification, it represents a value, so whether or not it is known to be constrained is irrelevant (the term is only defined for composite objects). Otherwise, the current instance of a type can only be used in an immutably limited type, so all such instances are known to be constrained by the third bullet.
For the purposes of determining within a generic body whether an object is known to be constrained:

- if a subtype is a descendant of an untagged generic formal private or derived type, and the subtype is not an unconstrained array subtype, it is not considered indefinite and is considered to have a constrained partial view;
- if a subtype is a descendant of a formal access type, it is not considered pool-specific.

A named number provides a name for a numeric value known at compile time. It is declared by a number_declaration.

NOTE 1 A constant cannot be the target of an assignment operation, nor be passed as an in out or out parameter, between its initialization and finalization, if any.

NOTE 2 The value of a constant object cannot be changed after its initialization, except in some cases where the object has a controlled or immutably limited part (see 7.5, 7.6, and 13.9.1).

NOTE 3 The nominal and actual subtypes of an elementary object are always the same. For a discriminated or array object, if the nominal subtype is constrained, then so is the actual subtype.

Extensions to Ada 83

There are additional kinds of objects (choice parameters and entry indices of entry bodies).

The result of a function and of evaluating an aggregate are considered (constant) objects. This is necessary to explain the action of finalization on such things. Because a function_call is also syntactically a name (see 4.1), the result of a function_call can be renamed, thereby allowing repeated use of the result without calling the function again.

Wording Changes from Ada 83

This subclause and its subclauses now follow the clause and subclauses on types and subtypes, to cut down on the number of forward references.

The term nominal subtype is new. It is used to distinguish what is known at compile time about an object's constraint, versus what its "true" run-time constraint is.

The terms definite and indefinite (which apply to subtypes) are new. They are used to aid in the description of generic formal type matching, and to specify when an explicit initial value is required in an object_declaration.

We have moved the syntax for object_declaration and number_declaration down into their respective subclauses, to keep the syntax close to the description of the associated semantics.

We talk about variables and constants here, since the discussion is not specific to object_declarations, and it seems better to have the list of the kinds of constants juxtaposed with the kinds of objects.

We no longer talk about indirect updating due to parameter passing. Parameter passing is handled in 6.2 and 6.4.1 in a way that there is no need to mention it here in the definition of read and update. Reading and updating now includes the case of evaluating or assigning to an enclosing object.

Wording Changes from Ada 95

Clarified that the return object is the object created by a function_call.

Extensions to Ada 2005

Added wording to allow return objects to be declared as constants, and corrected the definition of return objects as objects.

Wording Changes from Ada 2005

Correction: Added a definition of known to be constrained, for use in other rules.

Correction: We now recognize the fact that not all declared constant objects are immutable; for those that a variable view can be constructed, they can be changed via that view.

Correction: Added the current instance of a protected object to the list of constant views; since the list claims to include all possibilities, it had better include that one.
The result of a qualified_expression is defined to be a constant view and is defined to be an object if the operand of the qualified_expression is an object. These definitions, combined with some grammar changes, allow qualified_expressions to be used in more places. See 4.1 for details.

Incompatibilities With Ada 2012

Correction: Corrected the definition of “known to be constrained” so that the status of the operand of value conversions and qualified_expressions is always used to determine whether the property exists. As the rules are ordered together, a value conversion or qualified_expression with a constrained nominal subtype would have always met the requirements in Ada 2012, regardless of the operand. This change will mean that some conversions or qualifications (mostly of variables) will no longer be considered “known to be constrained” and therefore Access and renaming of such prefixes will now be illegal. This is necessary to meet the design goal that subsequent execution cannot cause a renaming or 'Access to cause erroneous execution.

Extensions to Ada 2012

Correction: A qualified_expression of an object that is known to be constrained is now also known to be constrained. This allows qualification to be used to disambiguate a function call used as a prefix in a renaming_declaration without making the renaming_declaration illegal.

Correction: A value conversion of an object is an object; this makes value conversions consistent with qualified expressions.

Wording Changes from Ada 2012

Correction: Changed from a list of constants to a list of variables. This makes the default to be a constant, which is the more common case, and eliminates issues caused by omissions from the list (such as parenthesized expressions).

Added the term “known to have no variable views” in order to have a definition that can be used in Legality Rules without breaking privacy.

### 3.3.1 Object Declarations

An object_declaration declares a stand-alone object with a given nominal subtype and, optionally, an explicit initial value given by an initialization expression. For an array, access, task, or protected object, the object_declaration may include the definition of the (anonymous) type of the object.

**Syntax**

```ada
object_declaration ::= 
  defining_identifier_list : [aliased] [constant] subtype_indication [:= expression] 
  | [aspect_specification];
| defining_identifier_list : [aliased] [constant] access_definition [:= expression] 
  | [aspect_specification];
| defining_identifier_list : [aliased] [constant] array_type_definition [:= expression] 
  | [aspect_specification];
| single_task_declaration
| single_protected_declaration

defining_identifier_list ::= 
  defining_identifier {, defining_identifier}
```

**Name Resolution Rules**

For an object_declaration with an expression following the compound delimiter :=, the type expected for the expression is that of the object. This expression is called the initialization expression.

**Legality Rules**

An object_declaration without the reserved word constant declares a variable object. If it has a subtype_indication or an array_type_definition that defines an indefinite subtype, then there
shall be an initialization expression. An initialization expression shall not be given if the object is of a limited type.

Static Semantics

6/5 \{AI05-0264-1\} \{AI05-0299-1\} \{AI12-0449-1\} An object_declaration with the reserved word constant declares a constant object. If it has an initialization expression, then it is called a full constant declaration. Otherwise, it is called a deferred constant declaration. The rules for deferred constant declarations are given in subclause 7.4. The rules for full constant declarations are given in this subclause.

7 Any declaration that includes a defining_identifier_list with more than one defining_identifier is equivalent to a series of declarations each containing one defining_identifier from the list, with the rest of the text of the declaration copied for each declaration in the series, in the same order as the list. The remainder of this Reference Manual relies on this equivalence; explanations are given for declarations with a single defining_identifier.

8/2 \{AI95-00385-01\} The subtype_indication_access_definition or full type definition of an object_declaration defines the nominal subtype of the object. The object_declaration declares an object of the type of the nominal subtype.

8.a/2 Discussion: \{AI95-00385-01\} The phrase “full type definition” here includes the case of an anonymous array, access, task, or protected type.

8.1/5 \{AI95-00373-01\} \{AI12-0192-1\} A component of an object is said to require late initialization if: it has an access_discriminant value constrained by a per-object expression, or if it has an initialization expression that includes a name denoting the current instance of the type or denoting an access_discriminant.

8.2/5 \{AI12-0192-1\} \{AI12-0404-1\} it has an access_discriminant value constrained by a per-object expression; or

8.3/5 \{AI12-0192-1\} it has an initialization expression that includes a name denoting an access_discriminant; or

8.4/5 \{AI12-0192-1\} it has an initialization expression that includes a reference to the current instance of the type either by name or implicitly as the target object of a call.

8.b/2 Reason: Such components can depend on the values of other components of the object. We want to initialize them as late and as reproducibly as possible.

Dynamic Semantics

9/2 \{AI95-00363-01\} If a composite object declared by an object_declaration has an unconstrained nominal subtype, then if this subtype is indefinite or the object is constant or aliased (see 3.10) the actual subtype of this object is constrained. The constraint is determined by the bounds or discriminants (if any) of its initial value; the object is said to be constrained by its initial value. [In the case of an aliased object, this initial value may be either explicit or implicit; in the other cases, an explicit initial value is required.]

When not constrained by its initial value, the actual and nominal subtypes of the object are the same. If its actual subtype is constrained, the object is called a constrained object.

For an object_declaration without an initialization expression, any initial values for the object or its subcomponents are determined by the implicit initial values defined for its nominal subtype, as follows:

11 The implicit initial value for an access subtype is the null value of the access type.

11.1/5 \{AI05-0228-1\} \{AI12-0439-1\} The implicit initial value for a scalar subtype that has the Default_Value aspect specified is the value of that aspect converted to the nominal subtype (which cannot raise Constraint_Error — see 4.6, “Type Conversions”).
Ramification: This is a Dynamic Semantics rule, so the visibility of the aspect_specification is not relevant — if the full type for a private type has the Default_Value aspect specified, partial views of the type also have this implicit initial value.

- The implicit initial (and only) value for each discriminant of a constrained discriminated subtype is defined by the subtype.

- \{AI05-0228-1\} \{AI12-0439-1\} For a (definite) composite subtype, the implicit initial value of each component with a default_expression is obtained by evaluation of this expression and conversion to the component's nominal subtype (which cannot raise Constraint_Error — see 4.6, “Type Conversions”), unless the component is a discriminant of a constrained subtype (the previous case), or is in an excluded variant (see 3.8.1). For each component that does not have a default_expression, if the composite subtype has the Default_Component_Value aspect specified, the implicit initial value is the value of that aspect converted to the component's nominal subtype; otherwise, any implicit initial values are those determined by the component's nominal subtype.

- For a protected or task subtype, there is an implicit component (an entry queue) corresponding to each entry, with its implicit initial value being an empty queue.

Implementation Note: The implementation may add implicit components for its own use, which might have implicit initial values. For a task subtype, such components might represent the state of the associated thread of control. For a type with dynamic-sized components, such implicit components might be used to hold the offset to some explicit component.

The elaboration of an object_declaration proceeds in the following sequence of steps:

1. \{AI95-00385-01\} The subtype_indication, access_definition, array_type_definition, single_task_declaration, or single_protected_declaration is first elaborated. This creates the nominal subtype (and the anonymous type in the last four latter three cases).

2. \{AI12-0439-1\} If the object_declaration includes an initialization expression, the (explicit) initial value is obtained by evaluating the expression and converting it to the nominal subtype (which cannot raise Constraint_Error — see 4.6).

3. \{8652/0002\} \{AI95-00171-01\} \{AI95-00373-01\} The object is created, and, if there is not an initialization expression, the object is initialized by default. When an object is initialized by default, any per-object constraintexpressions (see 3.8) are evaluated and any implicit initial values for the object or for its subcomponents are obtained as determined by the nominal subtype. Any initial values (whether explicit or implicit) are assigned to the object or to the corresponding subcomponents. As described in 5.2 and 7.6, Initialize and Adjust procedures can be called.

Discussion: For a per-object constraint that contains some per-object expressions and some non-per-object expressions, the values used for the constraint consist of the values of the non-per-object expressions evaluated at the point of the type_declaration, and the values of the per-object expressions evaluated at the point of the creation of the object.

The elaboration of per-object constraints was presumably performed as part of the dependent compatibility check in Ada 83. If the object is of a limited type with an access discriminant, the access_definition is elaborated at this time (see 3.7).

Reason: The reason we say that evaluating an explicit initialization expression happens before creating the object is that in some cases it is impossible to know the size of the object being created until its initial value is known, as in “X: String := Func_Call(...);”. The implementation can create the object early in the common case where the size can be known early, since this optimization is semantically neutral.

This paragraph was deleted.

\{AI95-00373-01\} Any initial values (whether explicit or implicit) are assigned to the object or to the corresponding subcomponents. As described in 5.2 and 7.6, Initialize and Adjust procedures can be called.
Ramification: Since the initial values have already been converted to the appropriate nominal subtype, the only Constraint_Errors that might occur as part of these assignments are for values outside their base range that are used to initialize unconstrained numeric subcomponents. See 3.5.

For the third step above, the object creation and any elaborations and evaluations and assignments are performed in an arbitrary order subject to the following restrictions: except that if the default_expression for a discriminant is evaluated to obtain its initial value, then this evaluation is performed before that of the default_expression for any component that depends on the discriminant, and also before that of any default_expression that includes the name of the discriminant. The evaluations of the third step and the assignments of the fourth step are performed in an arbitrary order, except that each evaluation is performed before the resulting value is assigned.

Assignment to any part of the object is preceded by the evaluation of the value that is to be assigned.

Reason: Duh. But we ought to say it. Note that, like any rule in the Reference Manual, it doesn't prevent an “as-if” optimization; as long as the semantics as observed from the program are correct, the compiler can generate any code it wants.

The evaluation of a default_expression that includes the name of a discriminant is preceded by the assignment to that discriminant.

Reason: Duh again. But we have to say this, too. It's odd that Ada 95 only required the default expressions to be evaluated before the discriminant is used, it says nothing about discriminant values that come from subtype_indications.

The evaluation of the default_expression for any component that depends on a discriminant is preceded by the assignment to that discriminant.

Reason: For example:

```ada
type R(D : Integer := F) is
  record
    S : String(1..D) := (others => G);
  end record;
X : R;
```

For the elaboration of the declaration of X, it is important that F be evaluated before the aggregate.

The assignments to any components, including implicit components, not requiring late initialization must precede the initial value evaluations for any components requiring late initialization; if two components both require late initialization, then assignments to parts of the component occurring earlier in the order of the component declarations must precede the initial value evaluations of the component occurring later.

Reason: Components that require late initialization can refer to the entire object during their initialization. We want them to be initialized as late as possible to reduce the chance that their initialization depends on uninitialized components. For instance:

```ada
type T (D : Natural) is
  limited record
    C1 : T1 (T'Access);
    C2 : Natural := F (D);
    C3 : String (1..D) := (others => ' ');
  end record;
```

Component C1 requires late initialization. The initialization could depend on the values of any component of T, including D, C2, or C3. Therefore, we want to it to be initialized last. Note that C2 and C3 do not require late initialization; they only have to be initialized after D.

It is possible for there to be more than one component that requires late initialization. In this case, the language can't prevent problems, because all of the components can't be the last one initialized. In this case, we specify the order of initialization for components requiring late initialization; by doing so, programmers can arrange their code to avoid accessing uninitialized components, and such arrangements are portable. Note that if the program accesses an uninitialized component, 13.9.1 defines the execution to be erroneous.

There is no implicit initial value defined for a scalar subtype unless the Default_Value aspect has been specified for the type. In the absence of an explicit initialization or the
specification of the Default Value aspect, a newly created scalar object can have a value that does not belong to its subtype (see 13.9.1 and H.1).

To be honest: It could even be represented by a bit pattern that doesn't actually represent any value of the type at all, such as an invalid internal code for an enumeration type, or a NaN for a floating point type. It is generally a bounded error to reference scalar objects with such “invalid representations”, as explained in 13.9.1, “Data Validity”.

Ramification: There is no requirement that two objects of the same scalar subtype have the same implicit initial “value” (or representation). It might even be the case that two elaborations of the same object_declaration produce two different initial values. However, any particular uninitialized object is default-initialized to a single value (or invalid representation). Thus, multiple reads of such an uninitialized object will produce the same value each time (if the implementation chooses not to detect the error).

NOTE 1 Implicit initial values are not defined for an indefinite subtype, because if an object's nominal subtype is indefinite, an explicit initial value is required.

NOTE 2 As indicated above, a stand-alone object is an object declared by an object_declaration. Similar definitions apply to “stand-alone constant” and “stand-alone variable”. A subcomponent of an object is not a stand-alone object, nor is an object that is created by an allocator. An object declared by a loop_parameter_specification, iterator_specification, generalized_component_specification, parameter_specification, entry_index_specification, choice_parameter_specification, extended_return_statement, or a formal_object_declaration of mode in out is not considered called a stand-alone object.

NOTE 3 The type of a stand-alone object cannot be abstract (see 3.9.3).

Examples of variable declarations:

Example of a multiple object declaration:

```ada
-- the multiple object declaration

{AI95-00433-01} John, Paul : not null Person_Name := new Person(Sex => M); -- see 3.10.1
-- is equivalent to the two single object declarations in the order given

{AI95-00433-01} John : not null Person_Name := new Person(Sex => M);
Paul : not null Person_Name := new Person(Sex => M);
```

Examples of variable declarations:

```ada
{AI95-00433-01} {AI2-0430-1} Count, Sum : Integer;
Size : Integer range 0 .. 10_000 := 0;
Sorted : Boolean := False;
Color_Table : array (1 .. Max) of Color;
Option : Bit_Vector (1 .. 10) := (others => True); -- see 3.6
Hello : aliased constant String := "Hi, world.";
θ, φ : Float range -π .. +π;
```

Examples of constant declarations:

```ada
{AI95-00433-01} {AI2-0425-1} Limit : constant Integer := 10_000;
Low_Limit : constant Integer := Limit/10;
Tolerance : constant Real := Dispersion(1.15);
A_String : constant String := "A";
Hello_Msg : constant access String := Hello'Access; -- see 3.10.2
```

Extensions to Ada 83
The syntax rule for object_declaration is modified to allow the aliased reserved word.

A variable declared by an object_declaration can be constrained by its initial value; that is, a variable of a nominally unconstrained array subtype, or discriminated type without defaults, can be declared so long as it has an explicit initial value. In Ada 83, this was permitted for constants, and for variables created by allocators, but not for variables declared by object_declarations. This is particularly important for tagged class-wide types, since there is no way to constrain them explicitly, and so an initial value is the only way to provide a constraint. It is also important for generic formal private types with unknown discriminators.

We now allow an unconstrained_array_definition in an object_declaration. This allows an object of an anonymous array type to have its bounds determined by its initial value. This is for uniformity: If one can write “X: constant array(Integer range 1 .. 10) of Integer := ...”, then it makes sense to also allow “X: constant array(Integer range <>) of Integer := ...”. (Note that if anonymous array types are ever sensible, a common situation is for a table implemented
as an array. Tables are often constant, and for constants, there's usually no point in forcing the user to count the number of elements in the value.)

Wording Changes from Ada 83

33.d We have moved the syntax for object_declarations into this subclause.

33.e Deferred constants no longer have a separate syntax rule, but rather are incorporated in object_declaration as constants declared without an initialization expression.

Inconsistencies With Ada 95

33.f/2 {AI95-00363-01} Unconstrained aliased objects of types with discriminants with defaults are no longer constrained by their initial values. This means that a program that raised Constraint_Error from an attempt to change the discriminants will no longer do so. The change only affects programs that depended on the raising of Constraint_Error in this case, so the inconsistency is unlikely to occur outside of the ACATS. This change may however cause compilers to implement these objects differently, possibly taking additional memory or time. This is unlikely to be worse than the differences caused by any major compiler upgrade.

Extensions to Ada 95

33.g/2 {AI95-00287-01} A constant may have a limited type; the initialization expression has to be built-in-place (see 7.5).

33.h/2 {AI95-00385-01} {AI95-00406-01} A stand-alone object may have an anonymous access type.

Wording Changes from Ada 95

33.i/2 {8652/0002} {AI95-00171-01} Corrigendum: Corrected wording to say that per-object constraints are elaborated (not evaluated).

33.j/2 {AI95-00373-01} The rules for evaluating default initialization have been tightened. In particular, components whose default initialization can refer to the rest of the object are required to be initialized last.

33.k/2 {AI95-00433-01} Added examples of various new constructs.

Extensions to Ada 2005

33.l/3 {AI05-0183-1} An optional aspect_specification can be used in an object_declaration. This is described in 13.1.1.

Wording Changes from Ada 2005

33.m/3 {AI05-0228-1} Implicit initial values can now be given for scalar types and for scalar array components, using the Default_Value (see 3.5) and Default_Component_Value (see 3.6) aspects; the extension is documented there.

Inconsistencies With Ada 2012

33.n/5 {AI12-0192-1} Correction: Components of a protected type require late initialization if their initialization includes (implicitly) the current instance of the type. This means that the components could end up being initialized in a different order. In most cases, this will have no visible effect, or will even fix bugs. Most code for which this is an issue depends on the (unspecified) order of initialization, so it is at risk of failing with a new compiler version regardless of Ada rule changes. However, there do exist very unlikely cases where legal, portable Ada 2012 code would become erroneous. (See the discussion section of AI12-0192-1 for an example.) These are so unlikely that it is expected that they only exist in the minds of Ada lawyers.

3.3.2 Number Declarations

A number_declaration declares a named number.

Discussion: {AI05-0299-1} {AI12-0449-1} If a value or other property of a construct is required to be static that means it is required to be determined prior to execution. A static expression is an expression whose value is computed at compile time and is usable in contexts where the actual value might affect the legality of the construct. This is fully defined in subclause clause 4.9.

Syntax

number_declaration ::= defining_identifier_list : constant := static_expression;
Name Resolution Rules

The static_expression given for a number_declaration is expected to be of any numeric type.

\{AI12-0394-1\} A name that denotes a number_declaration is interpreted as a value of a universal type, unless the expected type for the name is a non-numeric type with an Integer_Literal or Real_Literal aspect, in which case it is interpreted to be of its expected type.

**To be honest:** This is only a Name Resolution Rule; all named numbers are values of a universal type (see the Static Semantics below). We need this rule so that named numbers can match types with user-defined literals; we need the other rules so the value of the named number is well-defined in all cases.

Legality Rules

\{AI05-0299-1\} \{AI12-0449-1\} The static_expression given for a number declaration shall be a static expression, as defined by subclause clause 4.9.

Static Semantics

The named number denotes a value of type universal_integer if the type of the static_expression is an integer type. The named number denotes a value of type universal_real if the type of the static_expression is a real type.

The value denoted by the named number is the value of the static_expression, converted to the corresponding universal type.

Dynamic Semantics

The elaboration of a number_declaration has no effect.

**Proof:** Since the static_expression was evaluated at compile time.

Examples of number declarations:

Two_Pi : constant := 2.0*Ada.Numerics.Pi;

-- a real number (see A.5)

\{AI95-00433-01\} Max : constant := 500;

-- an integer number

Max_Line_Size : constant := Max/6;

-- the integer 83

Power_16 : constant := 2**16;

-- the integer 65_536

One, Un, Eins : constant := 1;

-- three different names for 1

Extensions to Ada 83

We now allow a static expression of any numeric type to initialize a named number. For integer types, it was possible in Ada 83 to use 'Pos to define a named number, but there was no way to use a static expression of some nonuniversal real type to define a named number. This change is upward compatible because of the preference rule for the operators of the root numeric types.

Wording Changes from Ada 83

We have moved the syntax rule into this subclause.

AI83-00263 describes the elaboration of a number declaration in words similar to that of an object_declaration. However, since there is no expression to be evaluated and no object to be created, it seems simpler to say that the elaboration has no effect.

Extensions to Ada 2012

\{AI12-0394-1\} Named numbers now can be used with (non-numeric) types that define user-defined literals (see 4.2.1).
3.4 Derived Types and Classes

A derived_type_definition defines a derived type (and its first subtype) whose characteristics are derived from those of a parent type, and possibly from progenitor types.

Term entry: derived type — type defined in terms of a parent type and zero or more progenitor types given in a derived type definition

Note 1: A derived type inherits properties such as components and primitive operations from its parent and progenitors.

Note 2: A type together with the types derived from it (directly or indirectly) form a derivation class.

A class of types is a set of types that is closed under derivation; that is, if the parent or a progenitor type of a derived type belongs to a class, then so does the derived type. By saying that a particular group of types forms a class, we are saying that all derivatives of a type in the set inherit the characteristics that define that set. The more general term category of types is used for a set of types whose defining characteristics are not necessarily inherited by derivatives; for example, limited, abstract, and interface are all categories of types, but not classes of types.

Ramification: A class of types is also a category of types.

Syntax

Syntax

Legality Rules

A derived type has one parent type and zero or more progenitor types.

Term entry: parent of a derived type — first ancestor type given in the definition of the derived type

Note: The parent can be almost any kind of type, including an interface type.

A type shall be completely defined (see 3.11.1) prior to being specified as the parent type in a derived_type_definition — [the full_type_declarations for the parent type and any of its subcomponents have to precede the derived_type_definition.]

Discussion: This restriction does not apply to the ancestor type of a private extension — see 7.3; such a type need not be completely defined prior to the private_extension_declaration. However, the restriction does apply to record extensions, so the ancestor type will have to be completely defined prior to the full_type_declaration corresponding to the private_extension_declaration.

Reason: We originally hoped we could relax this restriction. However, we found it too complex to specify the rules for a type derived from an incompletely defined limited type that subsequently became nonlimited.

Proof: The syntax only allows an interface_list to appear with a record_extension_part, and a record_extension_part can only be provided if the parent type is a tagged type. We give the last sentence anyway for completeness.

Implementation Note: We allow a record extension to inherit discriminants; an early version of Ada 9X did not. If the parent subtype is unconstrained, it can be implemented as though its discriminants were repeated in a new known_discriminant_part and then used to constrain the old ones one-for-one. However, in an extension aggregate, the discriminants in this case do not appear in the component association list.

Ramification: This rule needs to be rechecked in the visible part of an instance of a generic unit because of the "only if" part of the rule. For example:
generic
  type T is private;
package P is
  type Der is new T;
end P;
package I is new P (Some_Tagged_Type);    -- illegal

{AI95-00114-01} The instantiation is illegal because a tagged type is being extended in the visible part without a
record_extension_part. Note that this is legal in the private part or body of an instance, both to avoid a contract model
violation, and because no code that can see that the type is actually tagged can also see the derived type declaration.

No recheck is needed for derived types with a record_extension_part, as that has to be derived from something that is
known to be tagged (otherwise the template is illegal).

{AI95-00419-01} {AI05-0096-1} If the reserved word limited appears in a derived_type_definition, the
parent type shall be a limited type. If the parent type is a tagged formal type, then in addition to the places
where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of
a generic unit.

Reason: We allow limited because we don't inherit limitedness from interfaces, so we must have a way to derive a
limited type from interfaces. The word limited has to be legal when the parent could be an interface, and that includes
generic formal abstract types. Since we have to allow it in this case, we might as well allow it everywhere as
documentation, to make it explicit that the type is limited.

However, we do not want to allow limited when the parent is nonlimited: limitedness cannot change in a derivation
tree.

If the parent type is an untagged limited formal type with an actual type that is nonlimited, we allow derivation as a
limited type in the private part or body as no place could have visibility on the resulting type where it was known to be
nonlimited (outside of the instance). (See the previous paragraph's annotations for an explanation of this.) However, if
the parent type is a tagged limited formal type with an actual type that is nonlimited, it would be possible to pass a
value of the limited type extension to a class-wide type of the parent, which would be nonlimited. That's too weird to
allow (even though all of the extension components would have to be nonlimited because the rules of 3.9.1 are
rechecked), so we have a special rule to prevent that in the private part (type extension from a formal type is illegal in a
generic package body).

Static Semantics

The first subtype of the derived type is unconstrained if a known_discriminant_part is provided in the
declaration of the derived type, or if the parent subtype is unconstrained. Otherwise, the constraint of the
first subtype corresponds to that of the parent subtype in the following sense: it is the same as that of the
parent subtype except that for a range constraint (implicit or explicit), the value of each bound of its range
is replaced by the corresponding value of the derived type.

Discussion: A digits_constraint in a subtype_indication for a decimal fixed point subtype always imposes a range
constraint, implicitly if there is no explicit one given. See 3.5.9, "Fixed Point Types".

{AI95-00231-01} The first subtype of the derived type excludes null (see 3.10) if and only if the parent
subtype excludes null.

{AI05-0110-1} The characteristics and implicitly declared primitive subprograms characteristics of the
derived type are defined as follows:

Ramification: {AI05-0110-1} The characteristics of a type do not include its primitive subprograms (primitive
subprograms include predefined operators). The rules governing availability/visibility and inheritance of characteristics
are separate from those for primitive subprograms.

• {AI95-00251-01} {AI95-00401-01} {AI95-00442-01} If the parent type or a progenitor type
belongs to a class of types, then the derived type also belongs to that class.] The following sets of
types, as well as any higher-level sets composed from them, are classes in this sense, and hence
the characteristics defining these classes are inherited by derived types from their parent or
progenitor types]: signed integer, modular integer, ordinary fixed, decimal fixed, floating point,
enumeration, boolean, character, access-to-constant, general access-to-variable, pool-specific
access-to-variable, access-to-subprogram, array, string, non-array composite, nonlimited,
Derived Types and Classes

8. A class of types that includes the parent type also includes the derived type.

Discussion: This is inherent in our notion of a “class” of types. It is not mentioned in the initial definition of “class” since at that point type derivation has not been defined. In any case, this rule ensures that every class of types is closed under derivation.

9. If the parent type is an elementary type or an array type, then the set of possible values of the derived type is a copy of the set of possible values of the parent type. For a scalar type, the base range of the derived type is the same as that of the parent type.

Discussion: The base range of a type defined by an integer_type_definition or a real_type_definition is determined by the _definition, and is not necessarily the same as that of the corresponding root numeric type from which the newly defined type is implicitly derived. Treating numerics types as implicitly derived from one of the two root numeric types is simply to link them into a type hierarchy; such an implicit derivation does not follow all the rules given here for an explicit derived_type_definition.

9.a If the parent type is a composite type other than an array type, then the components, protected subprograms, and entries that are declared for the derived type are as follows:

- The discriminants specified by a new known_discriminant_part, if there is one; otherwise, each discriminant of the parent type (implicitly declared in the same order with the same specifications) — in the latter case, the discriminants are said to be inherited, or if unknown in the parent, are also unknown in the derived type;
- Each nondiscriminant component, entry, and protected subprogram of the parent type, implicitly declared in the same order with the same declarations; these components, entries, and protected subprograms are said to be inherited;

Ramification: The profiles of entries and protected subprograms do not change upon type derivation, although the type of the “implicit” parameter identified by the prefix of the name in a call does.

To be honest: Any name in the parent type_declaration that denotes the current instance of the type is replaced with a name denoting the current instance of the derived type, converted to the parent type.

Each component declared in a record_extension_part, if any.

10. Declarations of components, protected subprograms, and entries, whether implicit or explicit, occur immediately within the declarative region of the type, in the order indicated above, following the parent subtype_indication.

Discussion: The order of declarations within the region matters for record_aggregates and extension_aggregates.

Ramification: In most cases, these things are implicitly declared immediately following the parent subtype_indication. However, 7.3.1, “Private Operations” defines some cases in which they are implicitly declared later, and some cases in which the are not declared at all.

Discussion: The place of the implicit declarations of inherited components matters for visibility — they are not visible in the known_discriminant_part nor in the parent subtype_indication, but are usually visible within the record_extension_part, if any (although there are restrictions on their use). Note that a discriminant specified in a new known_discriminant_part is not considered “inherited” even if it has the same name and subtype as a discriminant of the parent type.

16.a The derived type is limited if and only if the parent type is limited.

To be honest: The derived type can become nonlimited if the derivation takes place in the visible part of a child package, and the parent type is nonlimited as viewed from the private part of the child package — see 7.5.

16.b [For each predefined operator of the parent type, there is a corresponding predefined operator of the derived type.]

Proof: This is a ramification of the fact that each class that includes the parent type also includes the derived type, and the fact that the set of predefined operators that is defined for a type, as described in 4.5, is determined by the classes to which it belongs.

Reason: Predefined operators are handled separately because they follow a slightly different rule than user-defined primitive subprograms. In particular the systematic replacement described below does not apply fully to the relational
operators for Boolean and the exponentiation operator for Integer. The relational operators for a type derived from Boolean still return Standard.Boolean. The exponentiation operator for a type derived from Integer still expects Standard.Integer for the right operand. In addition, predefined operators "reemerge" when a type is the actual type corresponding to a generic formal type, so they need to be well defined even if hidden by user-defined primitive subprograms.

{AI95-00401-01} For each user-defined primitive subprogram (other than a user-defined equality operator — see below) of the parent type or of a progenitor type that already exists at the place of the derived_type_definition, there exists a corresponding inherited primitive subprogram of the derived type with the same defining name. Primitive user-defined equality operators of the parent type and any progenitor types are also inherited by the derived type, except when the derived type is a nonlimited record extension, and the inherited operator would have a profile that is type conformant with the profile of the corresponding predefined equality operator; in this case, the user-defined equality operator is not inherited, but is rather incorporated into the implementation of the predefined equality operator of the record extension (see 4.5.2).

**Ramification:** We say "...already exists..." rather than "is visible" or "has been declared" because there are certain operations that are declared later, but still exist at the place of the derived_type_definition, and there are operations that are never declared, but still exist. These cases are explained in 7.3.1. Note that nonprivate extensions can appear only after the last primitive subprogram of the parent — the freezing rules ensure this.

**Reason:** A special case is made for the equality operators on nonlimited record extensions because their predefined equality operators are already defined in terms of the primitive equality operator of their parent type (and of the tagged components of the extension part). Inheriting the parent's equality operator as is would be undesirable, because it would ignore any components of the extension part. On the other hand, if the parent type is limited, then any user-defined equality operator is inherited as is, since there is no predefined equality operator to take its place.

**Ramification:** {AI95-00114-01} Because user-defined equality operators are not inherited by nonlimited record extensions, the formal parameter names of = and /= revert to Left and Right, even if different formal parameter names were used in the user-defined equality operators of the parent type.

**Discussion:** {AI95-00401-01} This rule only describes what operations are inherited; the rules that describe what happens when there are conflicting inherited subprograms are found in 8.3.

{AI95-00401-01} {AI05-0164-1} {AI05-0240-1} The profile of an inherited subprogram (including an inherited enumeration literal) is obtained from the profile of the corresponding (user-defined) primitive subprogram of the parent or progenitor type, after systematic replacement of each subtype of its profile (see 6.1) that is of the parent or progenitor type, other than those subtypes found in the designated profile of an access_definition, with a corresponding subtype of the derived type. For a given subtype of the parent or progenitor type, the corresponding subtype of the derived type is defined as follows:

- If the declaration of the derived type has neither a known_discriminant_part nor a record_extension_part, then the corresponding subtype has a constraint that corresponds (as defined above for the first subtype of the derived type) to that of the given subtype.
- If the derived type is a record extension, then the corresponding subtype is the first subtype of the derived type.
- If the derived type has a new known_discriminant_part but is not a record extension, then the corresponding subtype is constrained to those values that when converted to the parent type belong to the given subtype (see 4.6).

**Reason:** An inherited subprogram of an untagged type has an Intrinsic calling convention, which precludes the use of the Access attribute. We preclude Access because correctly performing all required constraint checks on an indirect call to such an inherited subprogram was felt to impose an undesirable implementation burden.

{AI05-0164-1} Note that the exception to substitution of the parent or progenitor type applies only in the profiles of anonymous access-to-subprogram types. The exception is necessary to avoid calling an access-to-subprogram with types and/or constraints different than expected by the actual routine.

{AI95-00401-01} The same formal parameters have default_expressions in the profile of the inherited subprogram. [Any type mismatch due to the systematic replacement of the parent or...
progenitor type by the derived type is handled as part of the normal type conversion associated
with parameter passing — see 6.4.1.]

Reason: {AI95-00401-01} We don't introduce the type conversion explicitly here since conversions to record
extensions or on access parameters are not generally legal. Furthermore, any type conversion would just be "undone"
since the parent's subprogram of the parent or progenitor is ultimately being called anyway. (Null procedures can be
inherited from a progenitor without being overridden, so it is possible to call subprograms of an interface.)

{AI95-00401-01} If a primitive subprogram of the parent or progenitor type is visible at the place of the
derived_type_definition, then the corresponding inherited subprogram is implicitly declared immediately
after the derived_type_definition. Otherwise, the inherited subprogram is implicitly declared later or not
at all, as explained in 7.3.1.

A derived type can also be defined by a private_extension_declaration (see 7.3) or a formal_derived_-type_definition (see 12.5.1). Such a derived type is a partial view of the corresponding full or actual type.

All numeric types are derived types, in that they are implicitly derived from a corresponding root numeric
type (see 3.5.4 and 3.5.6).

Dynamic Semantics

The elaboration of a derived_type_definition creates the derived type and its first subtype, and consists of the
elaboration of the subtype_indication and the record_extension_part, if any. If the subtype_indication
depends on a discriminant, then only those expressions that do not depend on a discriminant are evaluated.

Discussion: {AI95-00251-01} We don't mention the interface_list, because it does not need elaboration (see 3.9.4).
This is consistent with the handling of discriminant_parts, which aren't elaborated either.

{AI95-00391-01} {AI95-00401-01} For the execution of a call on an inherited subprogram, a call on the
corresponding primitive subprogram of the parent or progenitor type is performed; the normal conversion
of each actual parameter to the subtype of the corresponding formal parameter (see 6.4.1) performs any
necessary type conversion as well. If the result type of the inherited subprogram is the derived type, the
result of calling the parent's subprogram of the parent or progenitor is converted to the derived type, or in
the case of a null extension, extended to the derived type using the equivalent of an extension_aggregate
with the original result as the ancestor_part and null record as the record_component_association_list.

Discussion: {AI95-00391-01} If an inherited function returns the derived type, and the type is a nonnull record
extension, then the inherited function shall be overridden, unless the type is abstract (in which case the function
is abstract, and (unless overridden) cannot be called except via a dispatching call). See 3.9.3.

NOTE 1 Classes are closed under derivation — any class that contains a type also contains its derivatives. Operations
available for a given class of types are available for the derived types in that class.

NOTE 2 Evaluating an inherited enumeration literal is equivalent to evaluating the corresponding enumeration literal of
the parent type, and then converting the result to the derived type. This follows from their equivalence to parameterless
functions.

NOTE 3 A generic subprogram is not a subprogram, and hence cannot be a primitive subprogram and cannot be inherited
by a derived type. On the other hand, an instance of a generic subprogram can be a primitive subprogram, and hence can be
inherited.

NOTE 4 If the parent type is an access type, then the parent and the derived type share the same storage pool; there is a
null access value for the derived type and it is the implicit initial value for the type. See 3.10.

NOTE 5 If the parent type is a boolean type, the predefined relational operators of the derived type deliver a result of the
predefined type Boolean (see 4.5.2). If the parent type is an integer type, the right operand of the predefined exponentiation
operator is of the predefined type Integer (see 4.5.6).

NOTE 6 Any discriminants of the parent type are either all inherited, or completely replaced with a new set of
discriminants.

NOTE 7 {AI12-0442-1} For an inherited subprogram, the subtype of a formal parameter of the derived type can be such
that it has noneed not have any value in common with the first subtype of the derived type.
Proof: This happens when the parent subtype is constrained to a range that does not overlap with the range of a subtype of the parent type that appears in the profile of some primitive subprogram of the parent type. For example:

```plaintext
type T1 is range 1..100;
subtype S1 is T1 range 1..10;
procedure P(X : in S1); -- P is a primitive subprogram

type T2 is new T1 range 11..20;
-- implicitly declared:
-- procedure P(X : in T2'Base range 1..10);
-- X cannot be in T2'First..T2'Last
```

NOTE 8 If the reserved word `abstract` is given in the declaration of a type, the type is abstract (see 3.9.3).

NOTE 9 `{AI95-00251-01}` `{AI95-00401-01}` An interface type that has a progenitor type “is derived from” that type. A `derived_type_definition`, however, never defines an interface type.

NOTE 10 `{AI95-00345-01}` It is illegal for the parent type of a `derived_type_definition` to be a synchronized tagged type.

Proof: `{AI05-0299-1}` 3.9.1 prohibits record extensions whose parent type is a synchronized tagged type, and this subclause requires tagged types to have a record extension. Thus there are no legal derivations. Note that a synchronized interface can be used as a progenitor in an `interface_type_definition` as well as in task and protected types, but we do not allow concrete extensions of any synchronized tagged type.

Examples of derived type declarations:

```plaintext
type Local_Coordinate is new Coordinate; -- two different types
type Midweek is new Day range Tue..Thu; -- see 3.5.1
type Counter is new Positive; -- same range as Positive

type Special_Key is new Key_Manager.Key; -- see 7.3.1
-- the inherited subprograms have the following specifications:
-- procedure Get_Key(K : out Special_Key);
-- function "<(X,Y : Special_Key) return Boolean;
```

Inconsistencies With Ada 83

When deriving from a (nonprivate, nonderived) type in the same visible part in which it is defined, if a predefined operator had been overridden prior to the derivation, the derived type will inherit the user-defined operator rather than the predefined operator. The work-around (if the new behavior is not the desired behavior) is to move the definition of the derived type prior to the overriding of any predefined operators.

Incompatibilities With Ada 83

When deriving from a (nonprivate, nonderived) type in the same visible part in which it is defined, a primitive subprogram of the parent type declared before the derived type will be inherited by the derived type. This can cause upward incompatibilities in cases like this:

```plaintext
package P is
  type T is (A, B, C, D);
  function P(X : T := A) return Integer;
  type NT is new T;
  -- inherits F as
  -- function F(X : NT := A) return Integer;
  -- in Ada 95 only
  ...
end P;
...
use P; -- Only one declaration of F from P is use-visible in
  -- Ada 83: two declarations of F are use-visible in
  -- Ada 95.
begin
  ...
  if F > 1 then ... -- legal in Ada 83, ambiguous in Ada 95
```

Extensions to Ada 83

The syntax for a `derived_type_definition` is amended to include an optional `record_extension_part` (see 3.9.1).

A derived type may override the discriminants of the parent by giving a new `discriminant_part`.

The parent type in a `derived_type_definition` may be a derived type defined in the same visible part.

When deriving from a type in the same visible part in which it is defined, the primitive subprograms declared prior to the derivation are inherited as primitive subprograms of the derived type. See 3.2.3.
Wording Changes from Ada 83

AI05-0190-1 As explained in Section 13, the concept of "storage pool" replaces the Ada 83 concept of "collection." These concepts are similar, but not the same.

Extensions to Ada 95

AI95-00251-01, AI95-00401-01 A derived type may inherit from multiple (interface) progenitors, as well as the parent type — see 3.9.4, "Interface Types".

AI95-00419-01 A derived type may specify that it is a limited type. This is required for interface ancestors (from which limitedness is not inherited), but it is generally useful as documentation of limitedness.

Wording Changes from Ada 95

AI95-00391-01 Defined the result of functions for null extensions (which we no longer require to be overridden - see 3.9.3).

AI95-00442-01 Defined the term "category of types" and used it in wording elsewhere; also specified the language-defined categories that form classes of types (this was never normatively specified in Ada 95).

Incompatibilities With Ada 2005

AI05-0096-1 Correction: Added a (re)check that limited type extensions never are derived from nonlimited types in generic private parts. This is disallowed as it would make it possible to pass a limited object to a nonlimited class-wide type, which could then be copied. This is only possible using Ada 2005 syntax, so examples in existing programs should be rare.

Wording Changes from Ada 2005

AI05-0110-1 Correction: Added wording to clarify that the characteristics of derived types are formally defined here. (This is the only place in the Reference Manual that actually spells out what sorts of things are actually characteristics, which is rather important.)

AI05-0164-1 Correction: Added wording to ensure that anonymous access-to-subprogram types don't get modified on derivation.

3.4.1 Derivation Classes

In addition to the various language-defined classes of types, types can be grouped into derivation classes.

Static Semantics

AI95-00251-01, AI95-00401-01 A derived type is derived from its parent type directly; it is derived indirectly from any type from which its parent type is derived. A derived type, interface type, type extension, task type, protected type, or formal derived type is also derived from every ancestor of each of its progenitor types, if any. The derivation class of types for a type \( T \) (also called the class rooted at \( T \)) is the set consisting of \( T \) (the root type of the class) and all types derived from \( T \) (directly or indirectly) plus any associated universal or class-wide types (defined below).

Discussion: Note that the definition of "derived from" is a recursive definition. We don't define a root type for all interesting language-defined classes, though presumably we could.

To be honest: By the class-wide type “associated” with a type \( T \), we mean the type \( T \) Class. Similarly, the universal type associated with root integer, root real, and root fixed are universal integer, universal real, and universal fixed, respectively.

AI95-00230-01, AI12-0437-1 Every type is one of either a specific type, a class-wide type, or a universal type. A specific type is one defined by a type declaration, a formal type declaration, or a full type definition embedded in another construct, a declaration for an object. Class-wide and universal types are implicitly defined, to act as representatives for an entire class of types, as follows:

To be honest: The root types root integer, root real, and root fixed are also specific types. They are declared in the specification of package Standard.
Class-wide types

Class-wide types are defined for [(and belong to)] each derivation class rooted at a tagged type (see 3.9). Given a subtype S of a tagged type T, S'Class is the subtype_mark for a corresponding subtype of the tagged class-wide type T'Class. Such types are called “class-wide” because when a formal parameter is defined to be of a class-wide type T'Class, an actual parameter of any type in the derivation class rooted at T is acceptable (see 8.6).

The set of values for a class-wide type T'Class is the discriminated union of the set of values of each specific type in the derivation class rooted at T (the tag acts as the implicit discriminant — see 3.9). Class-wide types have no primitive subprograms of their own. However, as explained in 3.9.2, operands of a class-wide type T'Class can be used as part of a dispatching call on a primitive subprogram of the type T. The only components [(including discriminants)] of T'Class that are visible are those of T. If S is a first subtype, then S'Class is a first subtype.

Reason: We want S'Class to be a first subtype when S is, so that an attribute_definition_clause like “for S'Class use ...,” will be legal.

Universal types

Universal types are defined for [(and belong to)] the integer, real, and fixed point, and access classes, and are referred to in this document as standard as respectively, universal integer, universal_real, and universal fixed, and universal access. These are analogous to class-wide types for these language-defined elementary numeric classes. As with class-wide types, if a formal parameter is of a universal type, then an actual parameter of any type in the corresponding class is acceptable. In addition, a value of a universal type (including an integer or real numeric literal, or the literal null) is “universal” in that it is acceptable where some particular type in the class is expected (see 8.6).

The set of values of a universal type is the undiscriminated union of the set of values possible for any definable type in the associated class. Like class-wide types, universal types have no primitive subprograms of their own. However, their “universality” allows them to be used as operands with the primitive subprograms of any type in the corresponding class.

Discussion: A class-wide type is only class-wide in one direction, from specific to class-wide, whereas a universal type is class-wide (universal) in both directions, from specific to universal and back.

We considered defining standard names for the universal numeric types so they could be used in formal parameter specifications. However, this was felt to impose an undue implementation burden for some implementations.

To be honest: Formally, the set of values of a universal type is actually a copy of the undiscriminated union of the values of the types in its class. This is because we want each value to have exactly one type, with explicit or implicit conversion needed to go between types. An alternative, consistent model would be to associate a class, rather than a particular type, with a value, even though any given expression would have a particular type. In that case, implicit type conversions would not generally need to change the value, although an associated subtype conversion might need to.

The integer and real numeric classes each have a specific root type in addition to their universal type, named respectively root_integer and root_real.

A class-wide or universal type is said to cover all of the types in its class. In addition, universal integer covers a type that has a specified Integer_Literal aspect, while universal real covers a type that has a specified Real_Literal aspect (see 4.2.1). A specific type covers only itself.

A specific type T2 is defined to be a descendant of a type T1 if T2 is the same as T1, or if T2 is derived (directly or indirectly) from T1. A class-wide type T2'Class is defined to be a descendant of type T1 if T2 is a descendant of T1. Similarly, the numeric universal types are defined to be descendants of the root types of their classes. If a type T2 is a descendant of a type T1, then...
3.4.1 Derivation Classes

1

Scalar types comprise enumeration types, integer types, and real types. Enumeration types and integer types are called discrete types; each value of a discrete type has a position number which is an integer value. Integer types and real types are called numeric types. [All scalar types are ordered, that is, all relational operators are predefined for their values.]

Syntax

2

range_constraint ::= range range
range ::= range_attribute_reference  
  | simple_expression .. simple_expression

**Discussion:** These need to be simple_expressions rather than more general expressions because ranges appear in membership tests and other contexts where expression .. expression would be ambiguous.

A range has a lower bound and an upper bound and specifies a subset of the values of some scalar type (the type of the range). A range with lower bound L and upper bound R is described by “L .. R”. If R is less than L, then the range is a null range, and specifies an empty set of values. Otherwise, the range specifies the values of the type from the lower bound to the upper bound, inclusive. A value belongs to a range if it is of the type of the range, and is in the subset of values specified by the range. A value satisfies a range constraint if it belongs to the associated range. One range is included in another if all values that belong to the first range also belong to the second.

**Name Resolution Rules**

For a subtype_indication containing a range_constraint, either directly or as part of some other scalar_constraint, the type of the range shall resolve to that of the type determined by the subtype_mark of the subtype_indication. For a range of a given type, the simple_expressions of the range (likewise, the simple_expressions of the equivalent range for a range_attribute_reference) are expected to be of the type of the range.

**Discussion:** In Ada 95, constraints only appear within subtype_indications; things that look like constraints that appear in type declarations are called something else like real_range_specifications.

\{AI05-0299-1\} \{AI12-0449-1\} We say ”the expected type is ..." or ”the type is expected to be ..." depending on which reads better. They are fundamentally equivalent, and both feed into the type resolution rules of subclause clause 8.6.

In some cases, it doesn't work to use expected types. For example, in the above rule, we say that the ’type of the range shall resolve to ..." rather than ”the expected type for the range is ..." We then use ”expected type” for the bounds. If we used “expected” at both points, there would be an ambiguity, since one could apply the rules of 8.6 either on determining the type of the range, or on determining the types of the individual bounds. It is clearly important to allow one bound to be of a universal type, and the other of a specific type, so we need to use ”expected type” for the bounds. Hence, we used ”shall resolve to” for the type of the range as a whole. There are other situations where ”expected type” is not quite right, and we use ”shall resolve to” instead.

**Static Semantics**

The base range of a scalar type is the range of finite values of the type that can be represented in every unconstrained object of the type; it is also the range supported at a minimum for intermediate values during the evaluation of expressions involving predefined operators of the type.

**Implementation Note:** Note that in some machine architectures intermediates in an expression (particularly if static), and register-resident variables might accommodate a wider range. The base range does not include the values of this wider range that are not assignable without overflow to memory-resident objects.

**Ramification:** The base range of an enumeration type is the range of values of the enumeration type.

**Reason:** If the representation supports infinities, the base range is nevertheless restricted to include only the representable finite values, so that 'Base'First and 'Base'Last are always guaranteed to be finite.

**To be honest:** By a ”value that can be assigned without overflow” we don't mean to restrict ourselves to values that can be represented exactly. Values between machine representable values can be assigned, but on subsequent reading, a slightly different value might be retrieved, as (partially) determined by the number of digits of precision of the type.

[A constrained scalar subtype is one to which a range constraint applies.] The range of a constrained scalar subtype is the range associated with the range constraint of the subtype. The range of an unconstrained scalar subtype is the base range of its type.
Dynamic Semantics

A range is *compatible* with a scalar subtype if and only if it is either a null range or each bound of the range belongs to the range of the subtype. A *range_constraint* is *compatible* with a scalar subtype if and only if its range is compatible with the subtype.

**Ramification:** Only *range_constraints* (explicit or implicit) impose conditions on the values of a scalar subtype. The other *scalar_constraints*, *digits_constraints* and *delta_constraints* impose conditions on the subtype denoted by the *subtype_mark* in a *subtype_indication*, but don't impose a condition on the values of the subtype being defined. Therefore, a scalar subtype is not called constrained if all that applies to it is a *digits_constraint*. Decimal subtypes are subtle, because a *digits_constraint* without a range_constraint nevertheless includes an implicit range_constraint.

The elaboration of a *range_constraint* consists of the evaluation of the *range*. The evaluation of a *range* determines a lower bound and an upper bound. If *simple_expressions* are given to specify bounds, the evaluation of the *range* evaluates these *simple_expressions* in an arbitrary order, and converts them to the type of the *range*. If a *range_attribute_reference* is given, the evaluation of the *range* consists of the evaluation of the *range_attribute_reference*.

**Attributes**

For every scalar subtype *S*, the following attributes are defined:

- **S'First**
  - *S'First* denotes the lower bound of the range of *S*. The value of this attribute is of the type of *S*.
  - **Ramification:** Evaluating *S'First* never raises *Constraint_Error*.

- **S'Last**
  - *S'Last* denotes the upper bound of the range of *S*. The value of this attribute is of the type of *S*.
  - **Ramification:** Evaluating *S'Last* never raises *Constraint_Error*.

- **S'Range**
  - *S'Range* is equivalent to the *range* *S'First* .. *S'Last*.

- **S'Base**
  - *S'Base* denotes an unconstrained subtype of the type of *S*. This unconstrained subtype is called the *base subtype* of the type.

- **S'Min**
  - *S'Min* denotes a function with the following specification:
    
    ```
    function S'Min(Left, Right : S'Base) return S'Base
    ```
    
    The function returns the lesser of the values of the two parameters.

- **S'Max**
  - *S'Max* denotes a function with the following specification:
    
    ```
    function S'Max(Left, Right : S'Base) return S'Base
    ```
    
    The function returns the greater of the values of the two parameters.

- **S'Succ**
  - *S'Succ* denotes a function with the following specification:
    
    ```
    function S'Succ(Arg : S'Base) return S'Base
    ```
    
    For an enumeration type, the function returns the value whose position number is one more than that of the value of *Arg*; *Constraint_Error* is raised if there is no such value of the type. For an integer type, the function returns the result of adding one to the value of *Arg*. For a fixed point type, the function returns the result of adding *small* to the value of *Arg*. For a floating point type, the function returns the machine number (as defined in 3.5.7) immediately above the value of *Arg*; *Constraint_Error* is raised if there is no such machine number.
Ramification: S'Succ for a modular integer subtype wraps around if the value of Arg is S'Base'Last. S'Succ for a signed integer subtype might raise Constraint_Error if the value of Arg is S'Base'Last, or it might return the out-of-base-range value S'Base'Last+1, as is permitted for all predefined numeric operations.

S'Pred

S'Pred denotes a function with the following specification:

``` ada
function S'Pred (Arg : S'Base) return S'Base
```

For an enumeration type, the function returns the value whose position number is one less than that of the value of Arg; Constraint_Error is raised if there is no such value of the type. For an integer type, the function returns the result of subtracting one from the value of Arg. For a fixed point type, the function returns the result of subtracting small from the value of Arg. For a floating point type, the function returns the machine number (as defined in 3.5.7) immediately below the value of Arg; Constraint_Error is raised if there is no such machine number.

Ramification: S'Pred for a modular integer subtype wraps around if the value of Arg is S'Base'First. S'Pred for a signed integer subtype might raise Constraint_Error if the value of Arg is S'Base'First, or it might return the out-of-base-range value S'Base'First–1, as is permitted for all predefined numeric operations.

S'Wide_Wide_Image

{AI12-0020-1} S'Wide_Wide_Image denotes a function with the following specification:

``` ada
function S'Wide_Wide_Image (Arg : S'Base) return Wide_Wide_String
```

{AI12-0020-1} The function returns an image of the value of Arg, that is, a sequence of characters representing the value in display form. The lower bound of the result is one.

The image of an integer value is the corresponding decimal literal, without underlines, leading zeros, exponent, or trailing spaces, but with a single leading character that is either a minus sign or a space.

Implementation Note: If the machine supports negative zeros for signed integer types, it is not specified whether "0" or "–0" should be returned for negative zero. We don't have enough experience with such machines to know what is appropriate, and what other languages do. In any case, the implementation should be consistent.

The image of an enumeration value is either the corresponding identifier in upper case or the corresponding character literal (including the two apostrophes); neither leading nor trailing spaces are included. For a nongraphic character (a value of a character type that has no enumeration literal associated with it), the result is a corresponding language-defined name in upper case (for example, the image of the nongraphic character identified as nul is “NUL”—the quotes are not part of the image).

Implementation Note: For an enumeration type T that has "holes" (caused by an enumeration_representation_clause), T'Wide_Image should raise Program_Error if the value is one of the holes (which is a bounded error anyway, since holes can be generated only via uninitialized variables and similar things).

The image of a floating point value is a decimal real literal best approximating the value (rounded away from zero if halfway between) with a single leading character that is either a minus sign or a space, a single digit (that is nonzero unless the value is zero), a decimal point, S'Digits–1 (see 3.5.8) digits after the decimal point (but one if S'Digits is one), an upper case E, the sign of the exponent (either + or –), and two or more digits (with leading zeros if necessary) representing the exponent. If S'Signed_Zeros is True, then the leading character is a minus sign for a negatively signed zero.

To be honest: Leading zeros are present in the exponent only if necessary to make the exponent at least two digits.

Reason: This image is intended to conform to that produced by Text_IO.Float_IO.Put in its default format.

Implementation Note: The rounding direction is specified here to ensure portability of output results.

The image of a fixed point value is a decimal real literal best approximating the value (rounded away from zero if halfway between) with a single leading character that is either a
minus sign or a space, one or more digits before the decimal point (with no redundant leading zeros), a decimal point, and S'Aft (see 3.5.10) digits after the decimal point.

Reason: This image is intended to conform to that produced by Text_IO.Fixed_IO.Put.

Implementation Note: The rounding direction is specified here to ensure portability of output results.

Implementation Note: For a machine that supports negative zeros, it is not specified whether " -0.000" or " 0.000" is returned. See corresponding comment above about integer types with signed zeros.

\[ S'Wide_{Image} \]

\{AI12-0020-1\} \( S'Wide_{Image} \) denotes a function with the following specification:

\[
function\ S'Wide_{Image}(Arg: S'Base)\ return\ Wide_{String}
\]

\{AI95-00285-01\} \( S'Wide_{Wide_{Image}} \) denotes a function with the following specification:

\[
function\ S'Wide_{Wide_{Image}}(Arg: S'Base)\ return\ Wide_{String}
\]

\{AI12-0020-1\} The function returns an image of the value of Arg as a Wide_String, that is, a sequence of characters representing the value in display form. The lower bound of the result is one. The image has the same sequence of graphic characters character as defined for S'Wide_{Wide_{Image}} if all the graphic characters are defined in Wide_Character; otherwise, the sequence of characters is implementation defined (but no shorter than that of S'Wide_{Wide_{Image}} for the same value of Arg).

Implementation defined: The sequence of characters of the value returned by S'Image when some of the graphic characters of S'Wide_{Wide_{Image}} are not defined in Character.

Paragraphs 2834 through 3734 were moved to 4.10, "Image Attributes"Wide_{Wide_{Image}}.

\{AI95-00285-01\} The image of an integer value is the corresponding decimal literal, without underlines, leading zeros, exponent, or trailing spaces, but with a single leading character that is either a minus sign or a space.

Implementation Note: If the machine supports negative zeros for signed integer types, it is not specified whether " -0" or " 0" should be returned for negative zero. We don't have enough experience with such machines to know what is appropriate, and what other languages do. In any case, the implementation should be consistent.

\{AI95-00285-01\} The image of an enumeration value is either the corresponding identifier in upper case or the corresponding character literal (including the two apostrophes); neither leading nor trailing spaces are included. For a nongraphic character (a value of a character type that has no enumeration literal associated with it), the result is a corresponding language-defined or implementation-defined name in upper case (for example, the image of the nongraphic character identified as \texttt{nul} is “NUL” – the quotes are not part of the image).

Implementation Note: For an enumeration type \( T \) that has “holes” (caused by an enumeration_representation_clause), \( T'Wide_{Image} \) should raise Program_Error if the value is one of the holes (which is a bounded error anyway, since holes can be generated only via uninitialized variables and similar things).

\{AI95-00285-01\} The image of a floating-point value is a decimal real literal best approximating the value (rounded away from zero if halfway between) with a single leading character that is either a minus sign or a space, a single digit (that is nonzero unless the value is zero), a decimal point, S'Digits - 1 (see 3.5.8) digits after the decimal point (but one if S'Digits is one), an upper case \( E \), the sign of the exponent (either + or –), and two or more digits (with leading zeros if necessary) representing the exponent. If S'Signed_Zeros is True, then the leading character is a minus sign for a negatively signed zero.

To be honest: Leading zeros are present in the exponent only if necessary to make the exponent at least two digits.

Reason: This image is intended to conform to that produced by Text_IO.Float_IO.Put in its default format.

Implementation Note: The rounding direction is specified here to ensure portability of output results.

\{AI95-00285-01\} The image of a fixed-point value is a decimal real literal best approximating the value (rounded away from zero if halfway between) with a single leading character that is either a minus sign or a space, one or more digits before the decimal point (with no redundant leading zeros), a decimal point, and S'Aft (see 3.5.10) digits after the decimal point.
Reason: This image is intended to conform to that produced by Text_IO.Fixed_IO.Put.

Implementation Note: The rounding direction is specified here to ensure portability of output results.

Implementation Note: For a machine that supports negative zeros, it is not specified whether "0.000" or "-0.000" is returned. See corresponding comment above about integer types with signed zeros.

\[ S'Image \]

\{AI12-0020-1\} \( S'Image \) denotes a function with the following specification:

\[
\begin{align*}
function S'Image(Arg : S'Base) \\
return String
\end{align*}
\]

\{AI95-00285-01\} \{AI05-0264-1\} \{AI12-0020-1\} The function returns an image of the value of \( Arg \) as a String. The lower bound of the result is one. The image has the same sequence of graphic characters as that defined for \( S'Wide_Wide_Image \) if all the graphic characters are defined in Character, otherwise, the sequence of characters is implementation defined (but no shorter than that of \( S'Wide_Wide_Image \) for the same value of \( Arg \)).

Implementation defined: The sequence of characters of the value returned by \( S'Image \) when some of the graphic characters of \( S'Wide_Wide_Image \) are not defined in Character.

\[ S'Wide_Wide_Width \]

\{AI95-00285-01\} \{AI12-0020-1\} \( S'Wide_Wide_Width \) denotes the maximum length of a \( Wide_Wide_String \) returned by \( S'Wide_Wide_Image \) over all values of the subtype \( S \), assuming a default implementation of \( S'Put_Image \). It denotes zero for a subtype that has a null range. Its type is \( universal_integer \).

\[ S'Wide_Width \]

\{AI12-0020-1\} \( S'Wide_Width \) denotes the maximum length of a \( Wide_String \) returned by \( S'Wide_Image \) over all values of the subtype \( S \), assuming a default implementation of \( S'Put_Image \). It denotes zero for a subtype that has a null range. Its type is \( universal_integer \).

\[ S'Width \]

\{AI12-0020-1\} \( S'Width \) denotes the maximum length of a String returned by \( S'Image \) over all values of the subtype \( S \), assuming a default implementation of \( S'Put_Image \). It denotes zero for a subtype that has a null range. Its type is \( universal_integer \).

\[ S'Wide_Wide_Value \]

\{AI95-00285-01\} \( S'Wide_Wide_Value \) denotes a function with the following specification:

\[
\begin{align*}
function S'Wide_Wide_Value(Arg : Wide_Wide_String) \\
return S'Base
\end{align*}
\]

This function returns a value given an image of the value as a \( Wide_Wide_String \), ignoring any leading or trailing spaces.

\{AI05-0264-1\} For the evaluation of a call on \( S'Wide_Wide_Value \) for an enumeration subtype \( S \), if the sequence of characters of the parameter (ignoring leading and trailing spaces) has the syntax of an enumeration literal and if it corresponds to a literal of the type of \( S \) (or corresponds to the result of \( S'Wide_Wide_Image \) for a nongraphic character of the type), the result is the corresponding enumeration value; otherwise, Constraint_Error is raised.

Discussion: It's not crystal clear that Range_Check is appropriate here, but it doesn't seem worthwhile to invent a whole new check name just for this weird case, so we decided to lump it in with Range_Check.

To be honest: \{8652/0096\} \{AI95-00053-01\} A sequence of characters corresponds to the result of \( S'Wide_Wide_Image \) if it is the same ignoring case. Thus, the case of an image of a nongraphic character does not matter. For example, \( Character'Wide_Wide_Value("nul") \) does not raise \( Constraint_Error \), even though \( Character'Wide_Wide_Image \) returns "NUL" for the nul character.

\{AI05-0264-1\} For the evaluation of a call on \( S'Wide_Wide_Value \) for an integer subtype \( S \), if the sequence of characters of the parameter (ignoring leading and trailing spaces) has the syntax of an integer literal, with an optional leading sign character (plus or minus for a signed
type; only plus for a modular type), and the corresponding numeric value belongs to the base
range of the type of \( S \), then that value is the result; otherwise, Constraint_Error is raised.

Discussion: We considered allowing \( S \)Value to return a representable but out-of-range value without a
Constraint_Error. However, we currently require (see 4.9) in an assignment_statement like \( X := <\text{numeric literal}>; \) that the value of the numeric-literal be in \( X \)'s base range (at compile time), so it seems unfriendly and confusing to have a different range allowed for \( S \)Value. Furthermore, for modular types, without the requirement for being in the
base range, \( S \)Value would have to handle arbitrarily long literals (since overflow never occurs for modular types).

For the evaluation of a call on \( S \Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wide\Wid
minus for a signed type; only plus for a modular type), and the corresponding numeric value belongs to the base range of the type of S, then that value is the result; otherwise Constraint_Error is raised.

Discussion: We considered allowing 'Value to return a representable but out-of-range value without a Constraint_Error. However, we currently require (see 4.9) in an assignment statement like “X := <numeric_literal>;” that the value of the numeric literal be in X's base range (at compile time), so it seems unfriendly and confusing to have a different range allowed for 'Value. Furthermore, for modular types, without the requirement for being in the base range, 'Value would have to handle arbitrarily long literals (since overflow never occurs for modular types).

For the evaluation of a call on S'Wide_Value (or S'Value) for a real subtype S, if the sequence of characters of the parameter (ignoring leading and trailing spaces) has the syntax of one of the following:

- numeric_literal
- numeral[[exponent]]
- .numeral[[exponent]]
- base#based_numeral.[[exponent]]
- base#.based_numeral[[exponent]]

with an optional leading sign character (plus or minus), and if the corresponding numeric value belongs to the base range of the type of S, then that value is the result; otherwise Constraint_Error is raised. The sign of a zero value is preserved (positive if none has been specified) if S'Signed_Zeros is True.

S'Value S'Value denotes a function with the following specification:

```ada
function S'Value(Arg : String) return S'Base
```

This function returns a value given an image of the value as a String, ignoring any leading or trailing spaces.

### 44.a/2 45/2

For the evaluation of a call on S'Value for an enumeration subtype S, if the sequence of characters of the parameter (ignoring leading and trailing spaces) has the syntax of an enumeration literal and if it corresponds to a literal of the type of S (or corresponds to the result of S'Image for a value of the type, assuming a default implementation of S'Put_Image), the result is the corresponding enumeration value; otherwise Constraint_Error is raised. For a numeric subtype S, the evaluation of a call on S'Value with Arg of type String is equivalent to a call on S'Wide_Wide_Value for a corresponding Arg of type Wide_Wide_String.

### 44.a/2 45/2

Reason: {AI95-00285-01} S'Value is subtly different from S'Wide_Wide_Value for enumeration subtypes; see the discussion under S'Wide_Value since S'Image might produce a different sequence of characters than S'Wide_Image if the enumeration literal uses characters outside of the predefined type Character. That is why we don't just define S'Value in terms of S'Wide_Value

For a prefix X that denotes an object of a scalar type (after any implicit dereference), the following attributes are defined:

### X'Wide_Wide_Image

- {AI12-0124-1} {AI12-0020-1} {AI12-0225-1} For a prefix X that denotes an object of a scalar type (after any implicit dereference), the following attributes are defined:

- {AI12-0124-1} {AI12-0020-1} X'Wide_Wide_Image denotes the result of calling function S'Wide_Wide_Image with Arg being X, where S is the nominal subtype of X.

### X'Wide_Image

- {AI12-0124-1} {AI12-0020-1} X'Wide_Image denotes the result of calling function S'Wide_Image with Arg being X, where S is the nominal subtype of X.
X'Image denotes the result of calling function S'Image with Arg being X, where S is the nominal subtype of X.

Implementation Permissions

An implementation may extend the Wide_Wide_Value, Wide_Value, [Wide_Value, Value, Wide_Wide_Image, Wide_Image, and Image] attributes of a floating point type to support special values such as infinities and NaNs.

Proof: The permission is really only necessary for Wide_Wide_Value, because Value and Wide_Value are defined in terms of Wide_Wide_Value, and because the behavior of Wide_Wide_Image, Wide_Image, and Image is already unspecified for things like infinities and NaNs.

Reason: This is to allow implementations to define full support for IEEE arithmetic. See also the similar permission for Get in A.10.9.

An implementation may extend the Wide_Wide_Value, Wide_Value, and Value attributes of a character type to accept strings of the form “Hex hhhhhhhh” (ignoring case) for any character (not just the ones for which Wide_Wide_Image would produce that form — see 3.5.2), as well as three-character strings of the form “'X'”, where X is any character, including nongraphic characters.

Static Semantics

For a scalar type, the following language-defined representation aspect may be specified with an aspect_specification (see 13.1.1):

Default_Value

This aspect shall be specified by a static expression, and that expression shall be explicit, even if the aspect has a boolean type. Default_Value shall be specified only on a full_type_declaration.

Reason: The part about requiring an explicit expression is to disallow omitting the value for this aspect, which would otherwise be allowed by the rules of 13.1.1.

This is a representation aspect in order to disallow specifying it on a derived type that has inherited primitive subprograms; that is necessary as the sizes of out parameters could be different whether or not a Default_Value is specified (see 6.4.1).

Aspect Description for Default_Value: Default value for a scalar subtype.

If a derived type with no primitive subprograms inherits a boolean Default_Value aspect, the aspect may be specified to have any value for the derived type. If a derived type T does not inherit a Default_Value aspect, it shall not specify such an aspect if it inherits a primitive subprogram that has a parameter of type T of mode out.

Reason: This overrides the 13.1.1 rule that says that a boolean aspect with a value True cannot be changed.

The second sentence is to avoid violating the rules specified in 6.4.1 about view conversions of out parameters with a specified Default_Value aspect.

Name Resolution Rules

The expected type for the expression specified for the Default_Value aspect is the type defined by the full_type_declaration on which it appears.

NOTE 1 The evaluation of S'First or S'Last never raises an exception. If a scalar subtype S has a nonnull range, S'First and S'Last belong to this range. These values can, for example, always be assigned to a variable of subtype S.

Discussion: This paragraph addresses an issue that came up with Ada 83, where for fixed point types, the end points of the range specified in the type definition were not necessarily within the base range of the type. However, it was later clarified (and we reconfirm it in 3.5.9, “Fixed Point Types”) that the First and Last attributes reflect the true bounds chosen for the type, not the bounds specified in the type definition (which might be outside the ultimately chosen base range).
NOTE 2  {AI12-0442-1} For a subtype of a scalar type, the result delivered by the attributes Succ, Pred, and Value can be outside the subtype; similarly, the actual parameters of the attributes Succ, Pred, and Image need not belong to the subtype.

NOTE 3  {AI95-00285-01} {AI12-0020-1} For any value V (including any nongraphic character) of an enumeration subtype S without a specified Put_Named_Image (see 4.10), S'Value(S'Image(V)) equals V, as does S'Wide_Value(S'Wide_Named_Image(V)) and S'Wide_Wide_Value(S'Wide_Wide_Named_Image(V)). None of these expressions ever raise Constraint_Error.

Examples

Examples of ranges:

-10 .. 10
X .. X + 1
0.0 .. 2.0 * Pi
Red .. Green  -- see 3.5.1
1 .. 0  -- a null range
Table'Range  -- a range attribute reference (see 3.6)

Examples of range constraints:

range -999.0 .. +999.0
range S'First+1 .. S'Last-1

Incompatibilities With Ada 83

S'Base is no longer defined for nonscalar types. One conceivable existing use of S'Base for nonscalar types is S'Base'Size where S is a generic formal private type. However, that is not generally useful because the actual subtype corresponding to S might be a constrained array or discriminated type, which would mean that S'Base'Size might very well overflow (for example, S'Base'Size where S is a constrained subtype of String will generally be 8 * (Integer'Last + 1)). For derived discriminated types that are packed, S'Base'Size might not even be well defined if the first subtype is constrained, thereby allowing some amount of normally required “dope” to have been squeezed out in the packing. Hence our conclusion is that S'Base'Size is not generally useful in a generic, and does not justify keeping the attribute S'Base for nonscalar types just so it can be used as a prefix.

Extensions to Ada 83

The attribute S'Base for a scalar subtype is now permitted anywhere a subtype_mark is permitted. S'Base'First .. S'Base'Last is the base range of the type. Using an attribute_definition_clause, one cannot specify any subtype-specific attributes for the subtype denoted by S'Base (the base subtype).

The attribute S'Range is now allowed for scalar subtypes.

The attributes S'Min and S'Max are now defined, and made available for all scalar types.

The attributes S'Succ, S'Pred, S'Image, S'Value, and S'Width are now defined for real types as well as discrete types.

Wide_String versions of S'Image and S'Value are defined. These are called S'Wide_Named_Image and S'Wide_Named_Value to avoid introducing ambiguities involving uses of these attributes with string literals.

Wording Changes from Ada 83

We now use the syntactic category range_attribute_reference since it is now syntactically distinguished from other attribute references.

The definition of S'Base has been moved here from 3.3.3 since it now applies only to scalar types.

More explicit rules are provided for nongraphic characters.

Extensions to Ada 95

{AI95-00285-01} The attributes S'Wide_Named_Image, S'Wide_Named_Value, and S'Wide_Width are new. Note that S'Wide_Named_Image and S'Wide_Named_Value are now defined in terms of S'Wide_Named_Named_Image and S'Wide_Named_Named_Value, but the image of types other than characters have not changed.

Wording Changes from Ada 95

{AI95-00285-01} The S'Wide_Named_Image and S'Wide_Named_Value attributes are now defined in terms of S'Wide_Named_Named_Image and S'Wide_Named_Named_Value, but the images of numeric types have not changed.
3.5.1 Enumeration Types

[An enumeration_type_definition defines an enumeration type.]

Syntax

```
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>enumeration_type_definition ::=</td>
</tr>
<tr>
<td>3</td>
<td>(enumeration_literal_specification {, enumeration_literal_specification})</td>
</tr>
<tr>
<td>4</td>
<td>defining_identifier</td>
</tr>
</tbody>
</table>
```

Legality Rules

```
5/3  {AI05-0227-1}  {AI05-0299-1}  The defining_identifiers in upper case and the |
|    | defining_character_literals] listed in an enumeration_type_definition shall be distinct. |
5.a/3  Proof: {AI05-0227-1}  For character literals, this is a ramification of the normal disallowance of homographs |
|      | explicitly declared immediately in the same declarative region. |
5.b/3  Reason: {AI05-0227-1}  To ease implementation of the attribute Wide_Wide_Value, we require that all enumeration |
|      | literals have distinct images. |

Static Semantics

```
6/3  {AI05-0006-1}  Each enumeration_literal_specification is the explicit declaration of the corresponding |
|     | enumeration_literal: it declares a parameterless function, whose defining name is the defining_identifier |
|     | or defining_character_literal, and whose result subtype is the base subtype of type is the enumeration |
|     | type. |
6.a  Reason: This rule defines the profile of the enumeration literal, which is used in the various types of conformance. |
6.b  Ramification: The parameterless function associated with an enumeration literal is fully defined by the |
|     | enumeration_type_definition; a body is not permitted for it, and it never fails the Elaboration_Check when called. |
6.c/3 Discussion: {AI05-0006-1}  The result subtype is primarily a concern when an enumeration literal is used as the |
|     | expression of a case statement, due to the full coverage requirement based on the nominal subtype. |
```
Each enumeration literal corresponds to a distinct value of the enumeration type, and to a distinct position number. The position number of the value of the first listed enumeration literal is zero; the position number of the value of each subsequent enumeration literal is one more than that of its predecessor in the list.

[The predefined order relations between values of the enumeration type follow the order of corresponding position numbers.]

[If the same defining_identifier or defining_character_literal is specified in more than one enumeration_type_definition, the corresponding enumeration literals are said to be overloaded. At any place where an overloaded enumeration literal occurs in the text of a program, the type of the enumeration literal has to be determinable from the context (see 8.6).]

Dynamic Semantics

The elaboration of an enumeration_type_definition creates the enumeration type and its first subtype, which is constrained to the base range of the type.

Ramification: The first subtype of a discrete type is always constrained, except in the case of a derived type whose parent subtype is Whatever'Base.

When called, the parameterless function associated with an enumeration literal returns the corresponding value of the enumeration type.

NOTE If an enumeration literal occurs in a context that does not otherwise suffice to determine the type of the literal, then qualification by the name of the enumeration type is one way to resolve the ambiguity (see 4.7).

Examples of enumeration types and subtypes:

Examples

{AI12-0386-1} type Day is (Mon, Tue, Wed, Thu, Fri, Sat, Sun);
    type Month_Name is (January, February, March, April, May, June, July, 
                            August, September, October, November, December);
    type Suit is (Clubs, Diamonds, Hearts, Spades);
    type Gender is (M, F);
    type Level is (Low, Medium, Urgent);
    type Color is (White, Red, Yellow, Green, Blue, Brown, Black);
    type Light is (Red, Amber, Green); -- Red and Green are overloaded
    type Hexa is ('A', 'B', 'C', 'D', 'E', 'F');
    type Mixed is ('A', 'B', '*', 'B', None, '?', '%');

subtype Weekday is Day range Mon .. Fri;
subtype Major is Suit range Hearts .. Spades;
subtype Rainbow is Color range Red .. Blue;  
    -- the Color Red, not the Light

Wording Changes from Ada 83

The syntax rule for defining_character_literal is new. It is used for the defining occurrence of a character_literal, analogously to defining_identifier. Usage occurrences use the name or selector_name syntactic categories.

We emphasize the fact that an enumeration literal denotes a function, which is called to produce a value.

Incompatibilities With Ada 2005

{AI05-0227-1} Correction: Required that all enumeration literals in a type have distinct images; this might not be the case since upper case conversion can map distinct characters to the same upper case character. This can only happen for identifiers using Unicode characters first allowed by Ada 2005; moreover, the original definition of Ada 2005 was confused and appeared to require inconsistent results from the Image attribute, so implementations that allowed problematic cases are rare; the problematic cases are very rare; so it is expected that this change would only affect test programs.

Wording Changes from Ada 2005

{AI05-0006-1} Correction: Defined the result subtype of an enumeration literal to close a minor language hole.
3.5.2 Character Types

Static Semantics

An enumeration type is said to be a character type if at least one of its enumeration literals is a character literal.

The predefined type Character is a character type whose values correspond to the 256 code points of Row 00 (also known as Latin-1) of the ISO/IEC 10646:2020 Basic Multilingual Plane (BMP). Each of the graphic characters of Row 00 of the BMP has a corresponding character literal in Character. Each of the nongraphic characters of Row 00 (0000-001F and 007F-009F) has a corresponding language-defined name, which is not usable as an enumeration literal, but which is usable with the attributes Image, Wide_Image, Wide_Wide_Image, Value, Wide_Value, and Wide_Wide_Value; these names are given in the definition of type Character in A.1, “The Package Standard”, but are set in italics.

Discussion: The predefined type Wide_Character is a character type whose values correspond to the 65536 code points of the ISO/IEC 10646:2020 Basic Multilingual Plane (BMP). Each of the graphic characters of the BMP has a corresponding character literal in Wide_Character. The first 256 values of Wide_Character have the same character literal or language-defined name as defined for Character. Each of the graphic characters has.The last 2 values of Wide_Character correspond to the nongraphic positions FFFE and FFFF of the BMP, and are assigned the language-defined names FFFE and FFFF. As with the other language-defined names for nongraphic characters, the names FFFE and FFFF are usable only with the attributes (Wide_)Image and (Wide_)Value; they are not usable as enumeration literals. All other values of Wide_Character are considered graphic characters, and have a corresponding character literal.

The characters whose code position is larger than 16#FF# and which are not graphic characters have language-defined names which are formed by appending to the string "Hex " the representation of their code position in hexadecimal as eight extended digits. As with other language-defined names, these names are usable only with the attributes (Wide )Wide_Image and (Wide )Wide_Value; they are not usable as enumeration literals.

Reason: The language-defined names are not usable as enumeration literals to avoid "polluting" the name space. Since Wide_Character and Wide_Wide_Character are defined in Standard, if the language-defined names FFFE and FFFF were usable as enumeration literals, they would hide other nonoverloadable declarations with the same names in use-d packages.

Implementation Permissions

In a nonstandard mode, an implementation may provide other interpretations for the predefined types Character and Wide_Character[... to conform to local conventions].
Original Paragraphs 4 and 5 were deleted.

**Implementation Advice**

\{AI95-00285-01\} If an implementation supports a mode with alternative interpretations for Character and Wide_Character, the set of graphic characters of Character should nevertheless remain a proper subset of the set of graphic characters of Wide_Character. Any character set “localizations” should be reflected in the results of the subprograms defined in the language-defined package Characters.Handling (see A.3) available in such a mode. In a mode with an alternative interpretation of Character, the implementation should also support a corresponding change in what is a legal identifier_letter.

**NOTE 1** The language-defined library package Characters.Latin_1 (see A.3.3) includes the declaration of constants denoting control characters, lower case characters, and special characters of the predefined type Character.

To be honest: The package ASCII does the same, but only for the first 128 characters of Character. Hence, it is an obsolescent package, and we no longer mention it here.

**NOTE 2** \{AI05-0299-1\} \{AI12-0449-1\} A conventional character set such as EBCDIC can be declared as a character type; the internal codes of the characters can be specified by an enumeration_representation_clause as explained in subclause 13.4.

**Examples**

**Example of a character type:**

```ada
type Roman_Digit is ('I', 'V', 'X', 'L', 'C', 'D', 'M');
```

**Inconsistencies With Ada 83**

The declaration of Wide_Character in package Standard hides use-visible declarations with the same defining identifier. In the unlikely event that an Ada 83 program had depended on such a use-visible declaration, and the program remains legal after the substitution of Standard.Wide_Character, the meaning of the program will be different.

**Incompatibilities With Ada 95**

\{AI95-00285-01\} Ada 95 defined most characters in Wide_Character to be graphic characters, while Ada 2005 uses the categorizations from ISO-10646:2003. It also provides language-defined names for all nongraphic characters. That means that in Ada 2005, Wide_Character.Wide_Value will raise Constraint_Error for a string representing a character literal of a nongraphic character, while Ada 95 would have accepted it. Similarly, the result of Wide_Character.Wide_Image will change for such nongraphic characters.

\{AI95-000395-01\} \{AI05-00005-1\} \{AI05-0262-1\} The language-defined names FFFE and FFFF were replaced by a consistent set of language-defined names for all nongraphic characters with code point positions greater than 16#FF#. That means that in Ada 2005, Wide_Character.Wide_Value("FFFE") will raise Constraint_Error while Ada 95 would have accepted it. Similarly, the result of Wide_Character.Wide_Image will change for the position numbers 16#FFFE# and 16#FFFF#. It is very unlikely that this will matter in practice, as these names do not represent usable characters.

\{AI95-00285-01\} \{AI95-00395-01\} Because of the previously mentioned changes to the Wide_Character.Wide_Image of various character values, the value of attribute Wide_Width will change for some subtypes of Wide_Character,
However, the new language-defined names were chosen so that the value of Wide_Character'Wide_Width itself does not change.

{AI95-00285-01} The declaration of Wide_Character in package Standard hides use-visible declarations with the same defining identifier. In the (very) unlikely event that an Ada 95 program had depended on such a use-visible declaration, and the program remains legal after the substitution of Standard.Wide_Character, the meaning of the program will be different.

**Extensions to Ada 95**

{AI95-00285-01} The type Wide_Character is new.

**Wording Changes from Ada 95**

{AI95-00285-01} Characters are now defined in terms of the entire ISO/IEC 10646:2003 character set.

{AI95-00285-01} {AI05-0248-1} We dropped the Implementation Advice for nonstandard interpretation of character sets; an implementation can do what it wants in a nonstandard mode, so there isn't much point to any advice.

**Wording Changes from Ada 2005**

{AI05-0181-1} Correction: Removed the position numbers of nongraphic characters from the text, as it is wrong and thus misleading.

{AI05-0262-1} Changed "code position" to "code point" consistently throughout the standard, as ISO/IEC 10646:2011 prefers "code point" and we are referring to the definition in that Standard. This change also reduces confusion between "code point" and "position number"; while these have the same values for the predefined character types, there is no required relationship for other character types.

### 3.5.3 Boolean Types

**Static Semantics**

There is a predefined enumeration type named Boolean, [declared in the visible part of package Standard]. It has the two enumeration literals False and True ordered with the relation False < True. Any descendant of the predefined type Boolean is called a **boolean** type.

**Implementation Note:** An implementation is not required to support enumeration representation clauses on boolean types that impose an unacceptable implementation burden. See 13.4, “Enumeration Representation Clauses”. However, it is generally straightforward to support representations where False is zero and True is 2**n – 1 for some n.

### 3.5.4 Integer Types

An **integer_type_definition** defines an integer type; it defines either a **signed** integer type, or a **modular** integer type. The base range of a signed integer type includes at least the values of the specified range. A modular type is an integer type with all arithmetic modulo a specified positive **modulus**; such a type corresponds to an unsigned type with wrap-around semantics.

**Syntax**


general_integer_type_definition ::=  
signed_integer_type_definition | modular_type_definition

signed_integer_type_definition ::=  
range static_simple_expression .. static_simple_expression

**Discussion:** We don't call this a range_constraint, because it is rather different — not only is it required to be static, but the associated overload resolution rules are different than for normal range constraints. A similar comment applies to real_range_specification. This used to be integer_range_specification but when we added support for modular types, it seemed overkill to have three levels of syntax rules, and just calling these signed_integer_range_specification and modular_range_specification loses the fact that they are defining different classes of types, which is important for the generic type matching rules.
modular_type_definition ::= \texttt{mod} \ static_expression

\textbf{Name Resolution Rules}

\texttt{\{AI12-0444-1\}} Each \texttt{simple_expression} in a \texttt{signed_integer_type_definition} is expected to be of any integer type; they \texttt{can be of different integer types}, \texttt{need not be of the same type}. The expression in a modular_type_definition is likewise expected to be of any integer type.

\textbf{Legality Rules}

The \texttt{simple_expressions} of a \texttt{signed_integer_type_definition} shall be static, and their values shall be in the range System.Min_Int .. System.Max_Int.

The expression of a modular_type_definition shall be static, and its value (the \texttt{modulus}) shall be positive, and shall be no greater than System.Max_Binary_Modulus if a power of 2, or no greater than System.Max_Nonbinary_Modulus if not.

\textbf{Reason}: For a 2's-complement machine, supporting nonbinary moduli greater than System.Max_Int can be quite difficult, whereas essentially any binary moduli are straightforward to support, up to $2 \times \text{System.Max_Int} + 2$, so this justifies having two separate limits.

\textbf{Static Semantics}

The set of values for a signed integer type is the (infinite) set of mathematical integers[, though only values of the base range of the type are fully supported for run-time operations]. The set of values for a modular integer type are the values from 0 to one less than the modulus, inclusive.

A \texttt{signed_integer_type_definition} defines an integer type whose base range includes at least the values of the \texttt{simple_expressions} and is symmetric about zero, excepting possibly an extra negative value. A \texttt{signed_integer_type_definition} also defines a constrained first subtype of the type, with a range whose bounds are given by the values of the \texttt{simple_expressions}, converted to the type being defined.

\textbf{Implementation Note}: \texttt{\{AI95-00114-01\}} The base range of a signed integer type might be much larger than is necessary to satisfy the above requirements.

\textbf{To be honest}: The conversion mentioned above is not an \texttt{implicit subtype conversion} (which is something that happens at overload resolution, see 4.6), although it happens implicitly. Therefore, the freezing rules are not invoked on the type (which is important so that representation items can be given for the type).

A \texttt{modular_type_definition} defines a modular type whose base range is from zero to one less than the given modulus. A \texttt{modular_type_definition} also defines a constrained first subtype of the type with a range that is the same as the base range of the type.

There is a predefined signed integer subtype named Integer[, declared in the visible part of package Standard]. It is constrained to the base range of its type.

\textbf{Reason}: Integer is a constrained subtype, rather than an unconstrained subtype. This means that on assignment to an object of subtype Integer, a range check is required. On the other hand, an object of subtype Integer'Base is unconstrained, and no range check (only overflow check) is required on assignment. For example, if the object is held in an extended-length register, its value might be outside of Integer'First .. Integer'Last. All parameter and result subtypes of the predefined integer operators are of such unconstrained subtypes, allowing extended-length registers to be used as operands or for the result. In an earlier version of Ada 95, Integer was unconstrained. However, the fact that certain Constraint Errors might be omitted or appear elsewhere was felt to be an undesirable upward inconsistency in this case. Note that for Float, the opposite conclusion was reached, partly because of the high cost of performing range checks when not actually necessary. Objects of subtype Float are unconstrained, and no range checks, only overflow checks, are performed for them.

Integer has two predefined subtypes, [declared in the visible part of package Standard:]  

\begin{verbatim}
subtype Natural is Integer range 0 .. Integer'Last;
subtype Positive is Integer range 1 .. Integer'Last;
\end{verbatim}
A type defined by an integer_type_definition is implicitly derived from root_integer, an anonymous predefined (specific) integer type, whose base range is System.Min_Int .. System.Max_Int. However, the base range of the new type is not inherited from root_integer, but is instead determined by the range or modulus specified by the integer_type_definition. [Integer literals are all of the type universal_integer, the universal type (see 3.4.1) for the class rooted at root_integer, allowing their use with the operations of any integer type.]

Discussion: This implicit derivation is not considered exactly equivalent to explicit derivation via a derived_type_definition. In particular, integer types defined via a derived_type_definition inherit their base range from their parent type. A type defined by an integer_type_definition does not necessarily inherit its base range from root_integer. It is not specified whether the implicit derivation from root_integer is direct or indirect, not that it really matters. All we want is for all integer types to be descendants of root_integer.

Note that this derivation does not imply any inheritance of subprograms. Subprograms are inherited only for types derived by a derived_type_definition (see 3.4), or a private_extension_declaration (see 7.3, 7.3.1, and 12.5.1).

Implementation Note: It is the intent that even nonstandard integer types (see below) will be descendants of root_integer, even though they might have a base range that exceeds that of root_integer. This causes no problem for static calculations, which are performed without range restrictions (see 4.9). However for run-time calculations, it is possible that Constraint_Error might be raised when using an operator of root_integer on the result of 'Val applied to a value of a nonstandard integer type.

The position number of an integer value is equal to the value.

For every modular subtype S, the following attributes are defined:

\[ S'Mod \]

\[ S'Mod denotes a function with the following specification: \]

\[ \text{function } S'Mod (Arg : universal_integer) \]

\[ \text{return } S'Base \]

This function returns Arg mod S'Modulus, as a value of the type of S.

S'Modulus S'Modulus yields the modulus of the type of S, as a value of the type universal_integer.

Dynamic Semantics

The elaboration of an integer_type_definition creates the integer type and its first subtype.

For a modular type, if the result of the execution of a predefined operator (see 4.5) is outside the base range of the type, the result is reduced modulo the modulus of the type to a value that is within the base range of the type.

For a signed integer type, the exception Constraint_Error is raised by the execution of an operation that cannot deliver the correct result because it is outside the base range of the type. [ For any integer type, Constraint_Error is raised by the operators "/", "rem", and "mod" if the right operand is zero.]

Implementation Requirements

In an implementation, the range of Integer shall include the range \(-2**15+1 .. +2**15-1\).

If Long_Integer is predefined for an implementation, then its range shall include the range \(-2**31+1 .. +2**31-1\).

System.Max_Binary_Modulus shall be at least \(2**16\).

Implementation Permissions

For the execution of a predefined operation of a signed integer type, it is optional to the implementation need not raise Constraint_Error if the result is outside the base range of the type, so long as the correct result is produced.
Discussion: Constraint_Error is never raised for operations on modular types, except for divide-by-zero (and \texttt{rem/\texttt{mod}-by-zero}).

An implementation may provide additional predefined signed integer types[, declared in the visible part of Standard], whose first subtypes have names of the form \texttt{Short_Integer}, \texttt{Long_Integer}, \texttt{Short_Short_Integer}, \texttt{Long_Long_Integer}, etc. Different predefined integer types are allowed to have the same base range. However, the range of \texttt{Integer} should be no wider than that of \texttt{Long_Integer}. Similarly, the range of \texttt{Short_Integer} (if provided) should be no wider than \texttt{Integer}. Corresponding recommendations apply to any other predefined integer types. An implementation may support there need not be a named integer type corresponding to each distinct base ranges for which there is no corresponding named integer type range supported by an implementation. The range of each first subtype should be the base range of its type.

\{\textit{AI12-0444-1}\} An implementation may provide nonstandard integer types, descendants of \texttt{root_integer} that are declared outside of the specification of package Standard, which may have different need not have all the standard characteristics than of a type defined by an \texttt{integer_type_definition}. For example, a nonstandard integer type \texttt{can} might have an asymmetric base range or it can be disallowed might not be allowed as an array or loop index (a very long integer). Any type descended from a nonstandard integer type is also nonstandard. An implementation may place arbitrary restrictions on the use of such types; it is implementation defined whether operators that are predefined for “any integer type” are defined for a particular nonstandard integer type. [In any case, such types are not permitted as \texttt{explicit_generic_actual_parameters} for formal scalar types — see 12.5.2.]

Implementation defined: Any nonstandard integer types and the operators defined for them.

For a one's complement machine, the high bound of the base range of a modular type whose modulus is one less than a power of 2 may be equal to the modulus, rather than one less than the modulus. It is implementation defined for which powers of 2, if any, this permission is exercised.

\{\textit{8652/0003}\} \{\textit{AI95-00095-01}\} For a one's complement machine, implementations may support nonbinary modulus values greater than \texttt{System.Max_Nonbinary_Modulus}. It is implementation defined which specific values greater than \texttt{System.Max_Nonbinary_Modulus}, if any, are supported.

Reason: On a one's complement machine, the natural full word type would have a modulus of \(2^{\text{Word Size}}\)–1. However, we would want to allow the all-ones bit pattern (which represents negative zero as a number) in logical operations. These permissions are intended to allow that and the natural modulus value without burdening implementations with supporting expensive modulus values.

Implementation Advice

An implementation should support Long_Integer in addition to Integer if the target machine supports 32-bit (or longer) arithmetic. No other named integer subtypes are recommended for package Standard. Instead, appropriate named integer subtypes should be provided in the library package Interfaces (see B.2).

\textbf{Implementation Advice:} Long_Integer should be declared in Standard if the target supports 32-bit arithmetic. No other named integer subtypes should be declared in Standard.

\textbf{Implementation Note:} To promote portability, implementations should explicitly declare the integer (sub)types Integer and Long_Integer in Standard, and leave other predefined integer types anonymous. For implementations that already support Byte_Integer, etc., upward compatibility argues for keeping such declarations in Standard during the transition period, but perhaps generating a warning on use. A separate package Interfaces in the predefined environment is available for pre-declaring types such as \texttt{Integer_8}, \texttt{Integer_16}, etc. See B.2. In any case, if the user declares a subtype (first or not) whose range fits in, for example, a byte, the implementation can store variables of the subtype in a single byte, even if the base range of the type is wider.

An implementation for a two's complement machine should support modular types with a binary modulus up to \texttt{System.Max_Int*2+2}. An implementation should support a nonbinary modulus up to Integer'Last.
Implementation Advice: For a two's complement target, modular types with a binary modulus up to
System.Max_Int*2+2 should be supported. A nonbinary modulus up to Integer'Last should be supported.

Reason: Modular types provide bit-wise "and", "or", "xor", and "not" operations. It is important for systems
programming that these be available for all integer types of the target hardware.

Ramification: Note that on a one's complement machine, the largest supported modular type would normally have
a nonbinary modulus. On a two's complement machine, the largest supported modular type would normally have
a binary modulus.

Implementation Note: Supporting a nonbinary modulus greater than Integer'Last can impose an undesirable
implementation burden on some machines.

NOTE 1 Integer literals are of the anonymous predefined integer type universal_integer. Other integer types have no
literals. However, the overload resolution rules (see 8.6, “The Context of Overload Resolution”) allow expressions of the
type universal_integer whenever an integer type is expected.

NOTE 2 The same arithmetic operators are predefined for all signed integer types defined by a
signed_integer_type_definition (see 4.5, “Operators and Expression Evaluation”). For modular types, these same operators
are predefined, plus bit-wise logical operators (and, or, xor, and not). In addition, for the unsigned types declared in the
language-defined package Interfaces (see B.2), functions are defined that provide bit-wise shifting and rotating.

NOTE 3 Modular types match a generic_formal_parameter_declaration of the form "type T is mod <>;"; signed integer
types match "type T is range <>;" (see 12.5.2).

Examples

Examples of integer types and subtypes:

```ada
type Page_Num is range 1 .. 2_000;
type Line_Size is range 1 .. Max_Line_Size;
subtype Small_Int is Integer range -10 .. 10;
subtype Column_Ptr is Line_Size range 1 .. 10;
subtype Buffer_Size is Integer range 0 .. Max;
type Byte is mod 256; -- an unsigned byte
type Hash_Index is mod 97; -- modulus is prime
```

Extensions to Ada 83

An implementation is allowed to support any number of distinct base ranges for integer types, even if fewer integer
types are explicitly declared in Standard.

Modular (unsigned, wrap-around) types are new.

Wording Changes from Ada 83

Ada 83's integer types are now called "signed" integer types, to contrast them with "modular" integer types.

Standard.Integer, Standard.Long_Integer, etc., denote constrained subtypes of predefined integer types, consistent with
the Ada 95 model that only subtypes have names.

We now impose minimum requirements on the base range of Integer and Long_Integer.

We no longer explain integer type definition in terms of an equivalence to a normal type derivation, except to say that
all integer types are by definition implicitly derived from root_integer. This is for various reasons.

First of all, the equivalence with a type derivation and a subtype declaration was not perfect, and was the source of
various AIs (for example, is the conversion of the bounds static? Is a numeric type a derived type with respect to other
rules of the language?)

Secondly, we don't want to require that every integer size supported shall have a corresponding named type in
Standard. Adding named types to Standard creates nonportabilities.

Thirdly, we don't want the set of types that match a formal derived type "type T is New Integer:" to depend on the
particular underlying integer representation chosen to implement a given user-defined integer type. Hence, we would
have needed anonymous integer types as parent types for the implicit derivation anyway. We have simply chosen to
identify only one anonymous integer type — root_integer, and stated that every integer type is derived from it.

Finally, the “fiction” that there were distinct preexisting predefined types for every supported representation breaks
down for fixed point with arbitrary smalls, and was never exploited for enumeration types, array types, etc. Hence,
there seems little benefit to pushing an explicit equivalence between integer type definition and normal type derivation.
Extensions to Ada 95

{AI95-00340-01} The Mod attribute is new. It eases mixing of signed and unsigned values in an expression, which can be difficult as there may be no type which can contain all of the values of both of the types involved.

Wording Changes from Ada 95

{8652/0003} {AI95-00095-01} Corrigendum: Added additional permissions for modular types on one's complement machines.

3.5.5 Operations of Discrete Types

Static Semantics

For every discrete subtype S, the following attributes are defined:

S'Pos S'Pos denotes a function with the following specification:

```ada
function S'Pos (Arg : S'Base) return universal_integer
```

This function returns the position number of the value of Arg, as a value of type universal_integer.

S'Val S'Val denotes a function with the following specification:

```ada
function S'Val (Arg : universal_integer) return S'Base
```

This function returns a value of the type of S whose position number equals the value of Arg. For the evaluation of a call on S'Val, if there is no value in the base range of its type with the given position number, Constraint_Error is raised.

Ramification: By the overload resolution rules, a formal parameter of type universal_integer allows an actual parameter of any integer type.

Reason: We considered allowing S'Val for a signed integer subtype S to return an out-of-range value, but since checks were required for enumeration and modular types anyway, the allowance didn't seem worth the complexity of the rule.

{AI05-0297-1} {AI12-0071-1} For every static discrete subtype S for which there exists at least one value belonging to S that satisfies the predicate of S, the following attributes are defined:

S'First_Valid

{AI05-0297-1} {AI12-0071-1} S'First_Valid denotes the smallest value that belongs to S and satisfies the predicate of S. The value of this attribute is of the type of S.

S'Last_Valid

{AI05-0297-1} {AI12-0071-1} S'Last_Valid denotes the largest value that belongs to S and satisfies the predicate of S. The value of this attribute is of the type of S.

{AI05-0297-1} [First_Valid and Last_Valid attribute references are always static expressions. Any explicit predicate of S can only have been specified by a Static_Predicate aspect.]

Proof: An attribute reference is static if the prefix is a static subtype (see 4.9), (true by definition) and any arguments are static (there are none). Similarly, a dynamic predicate always makes a subtype nonstatic. QED.

Reason: We require there to be at least one value so that these are always values of the subtype. (This sidesteps the question of what to return for a subtype with no values.)

Discussion: These attributes are intended primarily for use in the case where the Static_Predicate aspect of S has been specified; First and Last are equivalent if these are allowed and there is no predicate.

Implementation Advice

For the evaluation of a call on S'Pos for an enumeration subtype, if the value of the operand does not correspond to the internal code for any enumeration literal of its type [(perhaps due to an uninitialized variable)], then the implementation should raise Program_Error. This is particularly important for
enumeration types with noncontiguous internal codes specified by an \texttt{enumeration_representation\_} clause.

\textbf{Implementation Advice:} Program Error should be raised for the evaluation of S'Pos for an enumeration type, if the value of the operand does not correspond to the internal code for any enumeration literal of the type.

\textbf{Reason:} We say Program Error here, rather than Constraint Error, because the main reason for such values is uninitialized variables, and the normal way to indicate such a use (if detected) is to raise Program Error. (Other reasons would involve the misuse of low-level features such as Unchecked_Conversion.)

\textbf{NOTE 1} Indexing and loop iteration use values of discrete types.

\textbf{NOTE 2} The predefined operations of a discrete type include the assignment operation, qualification, the membership tests, and the relational operators; for a boolean type they include the short-circuit control forms and the logical operators; for an integer type they include type conversion to and from other numeric types, as well as the binary and unary adding operators – and +, the multiplying operators, the unary operator abs, and the exponentiation operator. The assignment operation is described in 5.2. The other predefined operations are described in Clause 4.

\textbf{NOTE 3} As for all types, objects of a discrete type have Size and Address attributes (see 13.3).

\textbf{NOTE 4} \{AI12-0442-1\} For a subtype of a discrete type, the result delivered by the attribute Val can be outside might not belong to the subtype; similarly, the actual parameter of the attribute Pos can also be outside need not belong to the subtype.

The following relations are satisfied (in the absence of an exception) by these attributes:

\[
S'\text{Val}(S'\text{Pos}(X)) = X \\
S'\text{Pos}(S'\text{Val}(N)) = N
\]

\textbf{Examples of attributes of discrete subtypes:}

\{AI12-0449-1\} -- For the types and subtypes declared in subclause 3.5.1 the following hold:

\begin{itemize}
  \item \texttt{Color’First} = White, \texttt{Color’Last} = Black
  \item \texttt{Rainbow’First} = Red, \texttt{Rainbow’Last} = Blue
  \item \texttt{Color’Succ(Blue)} = Rainbow’Succ(Blue) = Brown
  \item \texttt{Color’Pos(Blue)} = Rainbow’Pos(Blue) = 4
  \item \texttt{Color’Val(0)} = Rainbow’Val(0) = White
\end{itemize}

\textbf{Extensions to Ada 83}

The attributes S’Succ, S’Pred, S’Width, S’Image, and S’Value have been generalized to apply to real types as well (see 3.5, “Scalar Types”).

\textbf{Extensions to Ada 2005}

\{AI05-0297-1\} \textbf{The attributes S’First\_Valid and S’Last\_Valid are new.}

\textbf{Wording Changes from Ada 2012}

\{AI12-0071-1\} \textbf{Corrigendum: Updated wording of the attributes S’First\_Valid and S’Last\_Valid to use the new term "satisfies the predicates" (see 3.2.4).}

\section*{3.5.6 Real Types}

Real types provide approximations to the real numbers, with relative bounds on errors for floating point types, and with absolute bounds for fixed point types.

\textbf{Syntax}

\[
\text{real\_type\_definition ::=} \\
\quad \text{floating\_point\_definition | fixed\_point\_definition}
\]

\textbf{Static Semantics}

A type defined by a \texttt{real\_type\_definition} is implicitly derived from \texttt{root\_real}, an anonymous predefined (specific) real type. [Hence, all real types, whether floating point or fixed point, are in the derivation class rooted at \texttt{root\_real}.]
Ramification: It is not specified whether the derivation from root_real is direct or indirect, not that it really matters. All we want is for all real types to be descendants of root_real.

Note that this derivation does not imply any inheritance of subprograms. Subprograms are inherited only for types derived by a derived_type_definition (see 3.4), or a private_extension_declaration (see 7.3, 7.3.1, and 12.5.1).

Real literals are all of the type universal_real, the universal type (see 3.4.1) for the class rooted at root_real, allowing their use with the operations of any real type. Certain multiplying operators have a result type of universal_fixed (see 4.5.5), the universal type for the class of fixed point types, allowing the result of the multiplication or division to be used where any specific fixed point type is expected.

Dynamic Semantics

The elaboration of a real_type_definition consists of the elaboration of the floating_point_definition or the fixed_point_definition.

Implementation Requirements

An implementation shall perform the run-time evaluation of a use of a predefined operator of root_real with an accuracy at least as great as that of any floating point type definable by a floating_point_definition.

Ramification: Static calculations using the operators of root_real are exact, as for all static calculations. See 4.9.

Implementation Note: The Digits attribute of the type used to represent root_real at run time is at least as great as that of any other floating point type defined by a floating_point_definition, and its safe range includes that of any such floating point type with the same Digits attribute. On some machines, there might be real types with less accuracy but a wider range, and hence run-time calculations with root_real might not be able to accommodate all values that can be represented at run time in such floating point or fixed point types.

Implementation Permissions

For the execution of a predefined operation of a real type, it is optional to the implementation need not raise Constraint_Error if the result is outside the base range of the type, so long as the correct result is produced, or the Machine_Overflows attribute of the type is False (see G.2.1).

An implementation may provide nonstandard real types, descendants of root_real that are declared outside of the specification of package Standard, which may have different characteristics than of a type defined by a real_type_definition. For example, a nonstandard real type can have an asymmetric or unsigned base range, or its predefined operations can wrap around or “saturate” rather than overflow (modular or saturating arithmetic), or it can have a different accuracy model than is standard (see G.2.1G.2). Any type descended from a nonstandard real type is also nonstandard. An implementation may place arbitrary restrictions on the use of such types; it is implementation defined whether operators that are predefined for “any real type” are defined for a particular nonstandard real type. [In any case, such types are not permitted as explicit_generic_actual_parameters for formal scalar types — see 12.5.2.]

Implementation defined: Any nonstandard real types and the operators defined for them.

As stated, real literals are of the anonymous predefined real type universal_real. Other real types have no literals. However, the overload resolution rules (see 8.6) allow expressions of the type universal_real whenever a real type is expected.

Wording Changes from Ada 83

The syntax rule for real_type_definition is modified to use the new syntactic categories floating_point_definition and fixed_point_definition, instead of floating_point_constraint and fixed_point_constraint, because the semantics of a type definition are significantly different than the semantics of a constraint.
All discussion of model numbers, safe ranges, and machine numbers is moved to 3.5.7, 3.5.8, and G.2. Values of a fixed point type are now described as being multiples of the small of the fixed point type, and we have no need for model numbers, safe ranges, etc. for fixed point types.

### 3.5.7 Floating Point Types

For floating point types, the error bound is specified as a relative precision by giving the required minimum number of significant decimal digits.

#### Syntax

```
floating_point_definition ::= digits static_expression [real_range_specification]
real_range_specification ::= range static_simple_expression .. static_simple_expression
```

#### Name Resolution Rules

The requested decimal precision, which is the minimum number of significant decimal digits required for the floating point type, is specified by the value of the expression given after the reserved word `digits`. This expression is expected to be of any integer type.

Each `simple_expression` of a `real_range_specification` is expected to be of any real type; the types can need not be different.

#### Legality Rules

The requested decimal precision shall be specified by a static expression whose value is positive and no greater than System.Max_Base_Digits. Each `simple_expression` of a `real_range_specification` shall also be static. If the `real_range_specification` is omitted, the requested decimal precision shall be no greater than System.Max_Digits.

**Reason:** We have added Max_Base_Digits to package System. It corresponds to the requested decimal precision of root_real. System.Max_Digits corresponds to the maximum value for Digits that may be specified in the absence of a `real_range_specification`, for upward compatibility. These might not be the same if root_real has a base range that does not include ± 10.0**(4*Max_Base_Digits).

A `floating_point_definition` is illegal if the implementation does not support a floating point type that satisfies the requested decimal precision and range.

**Implementation defined:** What combinations of requested decimal precision and range are supported for floating point types.

#### Static Semantics

The set of values for a floating point type is the (infinite) set of rational numbers. The machine numbers of a floating point type are the values of the type that can be represented exactly in every unconstrained variable of the type. The base range (see 3.5) of a floating point type is symmetric around zero, except that it can include some extra negative values in some implementations.

**Implementation Note:** For example, if a 2's complement representation is used for the mantissa rather than a sign-mantissa or 1's complement representation, then there is usually one extra negative machine number.

**To be honest:** If the Signed_Zeros attribute is True, then minus zero could in a sense be considered a value of the type. However, for most purposes, minus zero behaves the same as plus zero.

The base decimal precision of a floating point type is the number of decimal digits of precision representable in objects of the type. The safe range of a floating point type is that part of its base range for which the accuracy corresponding to the base decimal precision is preserved by all predefined operations.
Implementation Note: In most cases, the safe range and base range are the same. However, for some hardware, values near the boundaries of the base range might result in excessive inaccuracies or spurious overflows when used with certain predefined operations. For such hardware, the safe range would omit such values.

\{AI12-0439-1\} A floating_point_definition defines a floating point type whose base decimal precision is no less than the requested decimal precision. If a real_range_specification is given, the safe range of the floating point type (and hence, also its base range) includes at least the values of the simple expressions given in the real_range_specification. If a real_range_specification is not given, the safe (and base) range of the type includes at least the values of the range \(-10.0^{*(4*D)} \ldots +10.0^{*(4*D)}\) where D is the requested decimal precision. [The safe range could include other values as well. The attributes Safe_First and Safe_Last give the actual bounds of the safe range.]

A floating_point_definition also defines a first subtype of the type. If a real_range_specification is given, then the subtype is constrained to a range whose bounds are given by a conversion of the values of the simple_expressions of the real_range_specification to the type being defined. Otherwise, the subtype is unconstrained.

To be honest: The conversion mentioned above is not an implicit subtype conversion (which is something that happens at overload resolution, see 4.6), although it happens implicitly. Therefore, the freezing rules are not invoked on the type (which is important so that representation items can be given for the type).

There is a predefined, unconstrained, floating point subtype named Float[, declared in the visible part of package Standard].

Dynamic Semantics

[The elaboration of a floating_point_definition creates the floating point type and its first subtype.]

Implementation Requirements

In an implementation that supports floating point types with 6 or more digits of precision, the requested decimal precision for Float shall be at least 6.

If Long_Float is predefined for an implementation, then its requested decimal precision shall be at least 11.

Implementation Permissions

\{AI12-0444-1\} An implementation is allowed to provide additional predefined floating point types[, declared in the visible part of Standard], whose (unconstrained) first subtypes have names of the form Short_Float, Long_Float, Short_Short_Float, Long_Long_Float, etc. Different predefined floating point types are allowed to have the same base decimal precision. However, the precision of Float should be no greater than that of Long_Float. Similarly, the precision of Short_Float (if provided) should be no greater than Float. Corresponding recommendations apply to any other predefined floating point types. An implementation may support there need not be a named floating point type corresponding to each distinct base decimal precisions for which there is no corresponding named floating point type supported by an implementation.

Implementation defined: The predefined floating point types declared in Standard.

Implementation Advice

An implementation should support Long_Float in addition to Float if the target machine supports 11 or more digits of precision. No other named floating point subtypes are recommended for package Standard. Instead, appropriate named floating point subtypes should be provided in the library package Interfaces (see B.2).

Implementation Advice: Long_Float should be declared in Standard if the target supports 11 or more digits of precision. No other named float subtypes should be declared in Standard.
Implementation Note: To promote portability, implementations should explicitly declare the floating point (sub)types Float and Long_Float in Standard, and leave other predefined float types anonymous. For implementations that already support Short_Float, etc., upward compatibility argues for keeping such declarations in Standard during the transition period, but perhaps generating a warning on use. A separate package Interfaces in the predefined environment is available for pre-declaring types such as Float_32, IEEE_Float_64, etc. See B.2.

NOTE If a floating point subtype is unconstrained, then assignments to variables of the subtype involve only Overflow_Checks, never Range_Checks.

Examples of floating point types and subtypes:

```ada
type Coefficient is digits 10 range -1.0 .. 1.0;
type Real is digits 8;
type Mass is digits 7 range 0.0 .. 1.0E35;
subtype Probability is Real range 0.0 .. 1.0;
-- a subtype with a smaller range
```

Inconsistencies With Ada 83

No Range_Checks, only Overflow_Checks, are performed on variables (or parameters) of an unconstrained floating point subtype. This is upward compatible for programs that do not raise Constraint_Error. For those that do raise Constraint_Error, it is possible that the exception will be raised at a later point, or not at all, if extended range floating point registers are used to hold the value of the variable (or parameter).

Reason: This change was felt to be justified by the possibility of improved performance on machines with extended-range floating point registers. An implementation need not take advantage of this relaxation in the range checking; it can hide completely the use of extended range registers if desired, presumably at some run-time expense.

Wording Changes from Ada 83

The syntax rules for floating_point_constraint and floating_accuracy_definition are removed. The syntax rules for floating_point_definition and real_range_specification are new.

A syntax rule for digits_constraint is given in 3.5.9, “Fixed Point Types”. In J.3 we indicate that a digits_constraint may be applied to a floating point subtype_mark as well (to be compatible with Ada 83's floating_point_constraint).

Discussion of model numbers is postponed to 3.5.8 and G.2. The concept of safe numbers has been replaced by the concept of the safe range of values. The bounds of the safe range are given by T'Safe_First .. T'Safe_Last, rather than -T'Safe_Large .. T'Safe_Large, since on some machines the safe range is not perfectly symmetric. The concept of machine numbers is new, and is relevant to the definition of Succ and Pred for floating point numbers.

3.5.8 Operations of Floating Point Types

Static Semantics

The following attribute is defined for every floating point subtype S:

S'Digits {8652/0004} {AI95-00203-01} S'Digits denotes the requested decimal precision for the subtype S. The value of this attribute is of the type universal_integer. The requested decimal precision of the base subtype of a floating point type T is defined to be the largest value of d for which

\[
\text{ceiling}(d \times \log(10) / \log(T'Machine_Radix)) + g \leq T'Model_Mantissa}
\]

where g is 0 if Machine_Radix is a positive power of 10 and 1 otherwise.

NOTE 1 The predefined operations of a floating point type include the assignment operation, qualification, the membership tests, and explicit conversion to and from other numeric types. They also include the relational operators and the following predefined arithmetic operators: the binary and unary adding operators – and +, certain multiplying operators, the unary operator abs, and the exponentiation operator.

NOTE 2 As for all types, objects of a floating point type have Size and Address attributes (see 13.3). Other attributes of floating point types are defined in A.5.3.
3.5.9 Fixed Point Types

A fixed point type is either an ordinary fixed point type, or a decimal fixed point type. The error bound of a fixed point type is specified as an absolute value, called the *delta* of the fixed point type.

**Syntax**

```plaintext
fixed_point_definition ::= 
  ordinary_fixed_point_definition | decimal_fixed_point_definition

ordinary_fixed_point_definition ::= 
  delta static_expression real_range_specification

decimal_fixed_point_definition ::= 
  delta static_expression digits static_expression [real_range_specification]

{AI12-0152-1} digits_constraint ::= 
  digits static_simple_expression expression [range_constraint]
```

**Name Resolution Rules**

For a type defined by a *fixed_point_definition*, the *delta* of the type is specified by the value of the expression given after the reserved word *delta*; this expression is expected to be of any real type. For a type defined by a *decimal_fixed_point_definition* (a decimal fixed point type), the number of significant decimal digits for its first subtype (the *digits* of the first subtype) is specified by the expression given after the reserved word *digits*; this expression is expected to be of any integer type.

{AI12-0159-1} The *simple_expression* of a *digits_constraint* is expected to be of any integer type.

**Legality Rules**

In a *fixed_point_definition* or *digits_constraint*, the expressions given after the reserved words *delta* and *digits* shall be static; their values shall be positive.

{AI95-00100-01} The set of values of a fixed point type comprise the integral multiples of a number called the *small* of the type. The *machine numbers of a fixed point type are the values of the type that can be represented exactly in every unconstrained variable of the type.* For a type defined by an *ordinary_fixed_point_definition* (an ordinary fixed point type), the *small* may be specified by an *attribute_definition_clause* (see 13.3); if so specified, it shall be no greater than the *delta* of the type. If not specified, the *small* of an ordinary fixed point type is an implementation-defined power of two less than or equal to the *delta*.

**Implementation defined:** The *small* of an ordinary fixed point type.

For a decimal fixed point type, the *small* equals the *delta*; the *delta* shall be a power of 10. If a *real_range_specification* is given, both bounds of the range shall be in the range −(10**≥digits−1)*delta .. +(10**≥digits−1)*delta.

A *fixed_point_definition* is illegal if the implementation does not support a fixed point type with the given *small* and specified range or *digits*.

**Implementation defined:** What combinations of *small*, range, and *digits* are supported for fixed point types.

For a *subtype_indication* with a *digits_constraint*, the *subtype_mark* shall denote a decimal fixed point subtype.
To be honest: Or, as an obsolescent feature, a floating point subtype is permitted — see J.3.

Static Semantics

The base range (see 3.5) of a fixed point type is symmetric around zero, except possibly for an extra negative value in some implementations.

An ordinary_fixed_point_definition defines an ordinary fixed point type whose base range includes at least all multiples of small that are between the bounds specified in the real_range Specification. The base range of the type does not necessarily include the specified bounds themselves. An ordinary_fixed_point_definition also defines a constrained first subtype of the type, with each bound of its range given by the closer to zero of:

- the value of the conversion to the fixed point type of the corresponding expression of the real_range Specification;
- the corresponding bound of the base range.

A decimal_fixed_point_definition defines a decimal fixed point type whose base range includes at least the range \((-10^{**\text{digits}–1})\delta .. +(10^{**\text{digits}–1})\delta\). A decimal_fixed_point_definition also defines a constrained first subtype of the type. If a real_range Specification is given, the bounds of the first subtype are given by a conversion of the values of the expressions of the real_range Specification. Otherwise, the range of the first subtype is \((-10^{**\text{digits}–1})\delta .. +(10^{**\text{digits}–1})\delta\).

To be honest: The conversion mentioned above is not an implicit subtype conversion (which is something that happens at overload resolution, see 4.6), although it happens implicitly. Therefore, the freezing rules are not invoked on the type (which is important so that representation items can be given for the type).

The elaboration of a fixed_point_definition creates the fixed point type and its first subtype.

For a digits_constraint on a decimal fixed point subtype with a given \(\delta\), if it does not have a range_constraint, then it specifies an implicit range \((-10^{**D–1})\delta .. +(10^{**D–1})\delta\), where \(D\) is the value of the simple_expression

\(\text{simple_expression} \delta\). A digits_constraint is compatible with a decimal fixed point subtype if the value of the simple_expression

\(\text{simple_expression} \delta\) is no greater than the digits of the subtype, and if it specifies (explicitly or implicitly) a range that is compatible with the subtype.

Discussion: Except for the requirement that the digits specified be no greater than the digits of the subtype being constrained, a digits_constraint is essentially equivalent to a range_constraint.

Consider the following example:

```ada
type D is delta 0.01 digits 7 range -0.00 .. 9999.99;
```

The compatibility rule implies that the digits_constraint "digits 6" specifies an implicit range of "-.9999.9999999 .. 9999.9999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
(10**D–1)*delta .. +(10**D–1)*delta, where D is the value of the (static) simple_expression given after the reserved word digits. If this check fails, Constraint_Error is raised.

Implementation Requirements

The implementation shall support at least 24 bits of precision (including the sign bit) for fixed point types.

Reason: This is sufficient to represent Standard.Duration with a small no more than 50 milliseconds.

Implementation Permissions

Implementations are permitted to support only smalls that are a power of two. In particular, all decimal fixed point type declarations can be disallowed. Note however that conformance with the Information Systems Annex requires support for decimal smalls, and decimal fixed point type declarations with digits up to at least 18.

Implementation Note: The accuracy requirements for multiplication, division, and conversion (see G.2.1, “Model of Floating Point Arithmetic”) are such that support for arbitrary smalls should be practical without undue implementation effort. Therefore, implementations should support fixed point types with arbitrary values for small (within reason). One reasonable limitation would be to limit support to fixed point types that can be converted to the most precise floating point type without loss of precision (so that Fixed_IO is implementable in terms of Float_IO).

NOTE {AI12-0442-1} The specified bounds themselves can be outside the base range of an ordinary fixed point type need not include the specified bounds themselves so that the range specification can be given in a natural way, such as:

```
type Fraction is delta 2.0**(–15) range -1.0 .. 1.0;
```

{AI12-0442-1} With 2’s complement hardware, such a type would typically have a signed 16-bit representation, using 1 bit for the sign and 15 bits for fraction, resulting in a base range of –1.0 .. 1.0–2.0**(–15).

Examples

Examples of fixed point types and subtypes:

```
type Volt is delta 0.125 range 0.0 .. 255.0;
-- A pure fraction which requires all the available
-- space in a word can be declared as the type Fraction:
type Fraction is delta System.Fine_Delta range -1.0 .. 1.0;
-- Fraction'Last = 1.0 – System.Fine_Delta
```

```
type Money is delta 0.01 digits 15;  -- decimal fixed point
subtype Salary is Money digits 10;
-- Money'Last = 10.0**13 – 0.01, Salary'Last = 10.0**8 – 0.01
```

Inconsistencies With Ada 83

In Ada 95, S'Small always equals S'Base'Small, so if an implementation chooses a small for a fixed point type smaller than required by the delta, the value of S'Small in Ada 95 might not be the same as it was in Ada 83.

Extensions to Ada 83

{AI05-0005-1} Decimal fixed point types are new, though their capabilities are essentially similar to that available in Ada 83 with a fixed point type whose small equals its delta and both are smalls that are a power of 10. However, in the Information Systems Annex, additional requirements are placed on the support of decimal fixed point types (e.g. a minimum of 18 digits of precision).

Wording Changes from Ada 83

The syntax rules for fixed_point_constraint and fixed_accuracy_definition are removed. The syntax rule for fixed_point_definition is new. A syntax rule for delta_constraint is included in the Obsolescent features (to be compatible with Ada 83's fixed_point_constraint).

Wording Changes from Ada 95

{AI95-00100-01} Added wording to define the machine numbers of fixed point types; this is needed by the static evaluation rules.
Incompatibilities With Ada 2012

{AI12-0152-1} Corrigendum: Changed the syntax so that the value following digits in a digits_constraint is a simple_expression. This is compatible with one very unlikely exception: if the digits expression is a static expression of a modular type using an unparenthesized logical operator (like and or or). Parenthesizing the expression will make it legal in that case. The change is necessary to eliminate syntax ambiguities in derived_type_definitions.

Wording Changes from Ada 2012

{AI12-0159-1} Corrigendum: Added wording to define the expected type for a digits_constraint. This was missing since Ada 95, but as it is obvious and unchanged from Ada 83, we don't consider it an incompatibility.

3.5.10 Operations of Fixed Point Types

Static Semantics

The following attributes are defined for every fixed point subtype S:

S'Small

{8652/0005} {AI95-00054-01} {AI12-0367-1} S'Small denotes the small of the type of S. The value of this attribute is of the type universal_real. Small may be specified for nonderived ordinary fixed point types via an attribute_definition_clause (see 13.3); the expression of such a clause shall be static and positive.

2.a/3

Aspect Description for Small: Scale factor for a fixed point type.

S'Delta

S'Delta denotes the delta of the fixed point subtype S. The value of this attribute is of the type universal_real.

3.a

Reason: The delta is associated with the subtype as opposed to the type, because of the possibility of an (obsolescent) delta_constraint.

S'Fore

S'Fore yields the minimum number of characters needed before the decimal point for the decimal representation of any value of the subtype S, assuming that the representation does not include an exponent, but includes a one-character prefix that is either a minus sign or a space. (This minimum number does not include superfluous zeros or underlines, and is at least 2.) The value of this attribute is of the type universal_integer.

S'Aft

S'Aft yields the number of decimal digits needed after the decimal point to accommodate the delta of the subtype S, unless the delta of the subtype S is greater than 0.1, in which case the attribute yields the value one. ([S'Aft is the smallest positive integer N for which (10**N)*S'Delta is greater than or equal to one.] The value of this attribute is of the type universal_integer.

The following additional attributes are defined for every decimal fixed point subtype S:

S'Digits

S'Digits denotes the digits of the decimal fixed point subtype S, which corresponds to the number of decimal digits that are representable in objects of the subtype. The value of this attribute is of the type universal_integer. Its value is determined as follows:

• For a first subtype or a subtype defined by a subtype_indication with a digits_constraint, the digits is the value of the expression given after the reserved word digits;

• {AI12-0426-1} For a subtype defined by a subtype_indication without a digits_constraint, the digits of the subtype is the same as that of the subtype denoted by the subtype_mark in the subtype_indication.

Implementation Note: Although a decimal subtype can be both range-constrained and digits-constrained, the digits constraint is intended to control the Size attribute of the subtype. For decimal types, Size can be important because input/output of decimal types is so common.

• The digits of a base subtype is the largest integer D such that the range –(10**D–1)*delta .. +(10**D–1)*delta is included in the base range of the type.
S'Scale  S'Scale denotes the *scale* of the subtype S, defined as the value N such that S'Delta = 10.0**(–N). [The scale indicates the position of the point relative to the rightmost significant digits of values of subtype S.] The value of this attribute is of the type *universal_integer*.

**Ramification:** S'Scale is negative if S'Delta is greater than one. By contrast, S'Aft is always positive.

S'Round  S'Round denotes a function with the following specification:

```plaintext
function S'Round (X : universal_real) return S'Base
```

The function returns the value obtained by rounding X (away from 0, if X is midway between two values of the type of S).

**NOTE 1** All subtypes of a fixed point type will have the same value for the Delta attribute, in the absence of *delta_constraints* (see J.3).

**NOTE 2** S'Scale is not always the same as S'Aft for a decimal subtype; for example, if S'Delta = 1.0 then S'Aft is 1 while S'Scale is 0.

**NOTE 3** The predefined operations of a fixed point type include the assignment operation, qualification, the membership tests, and explicit conversion to and from other numeric types. They also include the relational operators and the following predefined arithmetic operators: the binary and unary adding operators – and +, multiplying operators, and the unary operator abs.

**NOTE 4** As for all types, objects of a fixed point type have Size and Address attributes (see 13.3). Other attributes of fixed point types are defined in A.5.4.

---

**Wording Changes from Ada 95**

{8652/0005} {AI95-00054-01} **Corrigendum:** Clarified that small may be specified only for ordinary fixed point types.

**Wording Changes from Ada 2012**

{AI12-0367-1} **Correction:** Clarified that small may be specified only with positive values.

---

### 3.6 Array Types

An *array* object is a composite object consisting of components which all have the same subtype. The name for a component of an array uses one or more index values belonging to specified discrete types. The value of an array object is a composite value consisting of the values of the components.

**Syntax**

```plaintext
array_type_definition ::=  
  unconstrained_array_definition | constrained_array_definition
unconstrained_array_definition ::=  
  array (index_subtype_definition {, index_subtype_definition}) of component_definition
index_subtype_definition ::= subtype_mark range <>
constrained_array_definition ::=  
  array (discrete_subtype_definition {, discrete_subtype_definition}) of component_definition
discrete_subtype_definition ::= discrete_subtype_indication | range

{AI95-00230-01} {AI95-00406-01} component_definition ::=  
  [aliased] subtype_indication | [aliased] access_definition
```
Name Resolution Rules

For a `discrete_subtype_definition` that is a range, the range shall resolve to be of some specific discrete type; which discrete type shall be determined without using any context other than the bounds of the range itself (plus the preference for `root_integer` — see 8.6).

Legality Rules

Each `index_subtype_definition` or `discrete_subtype_definition` in an `array_type_definition` defines an index subtype; its type (the index type) shall be discrete.

Discussion: An index is a discrete quantity used to select along a given dimension of an array. A component is selected by specifying corresponding values for each of the indices.

The subtype defined by the `subtype_indication` of a `component_definition` (the component subtype) shall be a definite subtype.

Ramification: This applies to all uses of `component_definition`, including in `record_type_definitions` and `protected_definition`s.

This paragraph was deleted. {AI95-00363-01} Within the definition of a nonlimited composite type (or a limited composite type that later in its immediate scope becomes nonlimited — see 7.3.1 and 7.5), if a `component_definition` contains the reserved word aliased and the type of the component is discriminated, then the nominal subtype of the component shall be constrained.

Reason: If we allowed the subtype to be unconstrained, then the discriminants might change because of an assignment to the containing (nonlimited) object, thus causing a potential violation of an access subtype constraint of an access value designating the aliased component.

Note that the rule elsewhere defining all aliased discriminated objects to be constrained does not help — that rule prevents assignments to the component itself from doing any harm, but not assignments to the containing object.

We allow this for components within limited types since assignment to the enclosing object is not a problem. Furthermore, it is important to be able to use a default expression for a discriminant in arrays of limited components, since that is the only way to give the components different values for their discriminants. For example:

```ada
protected type Counter_Type(Initial_Value : Integer := 1) is
  procedure Get_Next(Next_Value : out Integer);
  -- Returns the next value on each call, bumping Count
  -- before returning.
  private
  -- Count : Integer := Initial_Value;
  end Counter_Type;
protected body Counter_Type is
  function Next_Id(Counter : access Counter_Type) return Integer is
    Result : Integer;
  begin
    Counter.Get_Next(Result);
    return Result;
  end Next_Id;

  C : aliased Counter_Type;
  task type T(Who_Am_I : Integer := Next_Id(C'Access)) is
  -- Array of task elements, each with its own unique ID.
  -- We specify "aliased" so we can use Task_Array(I)'Access.
  -- This is safe because Task_Array is of a limited type.
  -- so there is no way an assignment to it could change
  -- the discriminants of one of its components.

  Ramification: Note that this rule applies to array components and record components, but not to protected type components (since they are always limited).
```

Static Semantics

An array is characterized by the number of indices (the dimensionality of the array), the type and position of each index, the lower and upper bounds for each index, and the subtype of the components. The order of the indices is significant.
A one-dimensional array has a distinct component for each possible index value. A multidimensional array has a distinct component for each possible sequence of index values that can be formed by selecting one value for each index position (in the given order). The possible values for a given index are all the values between the lower and upper bounds, inclusive; this range of values is called the index range. The bounds of an array are the bounds of its index ranges. The length of a dimension of an array is the number of values of the index range of the dimension (zero for a null range). The length of a one-dimensional array is the length of its only dimension.

An array_type_definition defines an array type and its first subtype. For each object of this array type, the number of indices, the type and position of each index, and the subtype of the components are as in the type definition[; the values of the lower and upper bounds for each index belong to the corresponding index subtype of its type, except for null arrays (see 3.6.1)].

{AI12-0444-1} An unconstrained_array_definition defines an array type with an unconstrained first subtype. Each index_subtype_definition defines the corresponding index subtype to be the subtype denoted by the subtype_mark. [ The compound delimiter <> (called a box) of an index_subtype_definition stands for an undefined range (different objects of the type cannot have different bounds).]

A constrained_array_definition defines an array type with a constrained first subtype. Each discrete_subtype_definition defines the corresponding index subtype, as well as the corresponding index range for the constrained first subtype. The constraint of the first subtype consists of the bounds of the index ranges.

Discussion: {AI05-0005-1} Although there is no nameable unconstrained array subtype in this case, the predefined slicing and concatenation operations can operate on and yield values that do not necessarily belong to the first array subtype. This is also true for Ada 83.

The discrete subtype defined by a discrete_subtype_definition is either that defined by the subtype_indication, or a subtype determined by the range as follows:

• If the type of the range resolves to root_integer, then the discrete_subtype_definition defines a subtype of the predefined type Integer with bounds given by a conversion to Integer of the bounds of the range;
  
  Reason: This ensures that indexing over the discrete subtype can be performed with regular Integers, rather than only universal_integers.
  
  Discussion: We considered doing this by simply creating a “preference” for Integer when resolving the range. However, this can introduce Beaujolais effects when the simple_expressions involve calls on functions visible due to use clauses.

• Otherwise, the discrete_subtype_definition defines a subtype of the type of the range, with the bounds given by the range.

The component_definition of an array_type_definition defines the nominal subtype of the components. If the reserved word aliased appears in the component_definition, then each component of the array is aliased (see 3.10).

Ramification: {AI95-00363-01} In this case, the nominal subtype cannot be an unconstrained discriminated subtype. See 3.8.

Dynamic Semantics

The elaboration of an array_type_definition creates the array type and its first subtype, and consists of the elaboration of any discrete_subtype_definitions and the component_definition.

{8652/0002} {AI95-00171-01} {AI95-00230-01} The elaboration of a discrete_subtype_definition that does not contain any per-object expressions creates the discrete subtype, and consists of the elaboration of the subtype_indication or the evaluation of the range. The elaboration of a discrete_subtype_definition...
that contains one or more per-object expressions is defined in 3.8. The elaboration of a component definition in an array_type_definition consists of the elaboration of the subtype_indication or access_definition. The elaboration of any discrete_subtype_definitions and the elaboration of the component_definition are performed in an arbitrary order.

Static Semantics

{AI05-0228-1} For an array type with a scalar component type, the following language-defined representation aspect may be specified with an aspect specification (see 13.1.1):

22.2/3 Default_Component_Value

This aspect shall be specified by a static expression, and that expression shall be explicit, even if the aspect has a boolean type. Default_Component_Value shall be specified only on a full_type_declaration.

Reason: The part about requiring an explicit expression is to disallow omitting the value for this aspect, which would otherwise be allowed by the rules of 13.1.1.

This is a representation attribute in order to disallow specifying it on a derived type that has inherited primitive subprograms; that is necessary as the sizes of out parameters could be different whether or not a Default_Value is specified (see 6.4.1).

Aspect Description for Default_Component_Value: Default value for the components of an array-of-scalar subtype.

{AI05-0228-1} {AI12-0427-1} If a derived type with no primitive subprograms inherits a boolean Default_Component_Value aspect, the aspect may be specified to have any value for the derived type.

Reason: This overrides the 13.1.1 rule that says that a boolean aspect with a value True cannot be changed.

Name Resolution Rules

{AI05-0228-1} The expected type for the expression specified for the Default_Component_Value aspect is the component type of the array type defined by the full_type_declaration on which it appears.

23 NOTE 1 All components of an array have the same subtype. In particular, for an array of components that are one-dimensional arrays, this means that all components have the same bounds and hence the same length.

24 NOTE 2 Each elaboration of an array_type_definition creates a distinct array type. A consequence of this is that each object whose object_declaration contains an array_type_definition is of its own unique type.

Examples

Examples of type declarations with unconstrained array definitions:

26 type Vector is array(Integer range <>) of Real;
27 type Matrix is array(Integer range <=, Integer range <=) of Real;
28 type Bit_Vector is array(Integer range <=) of Boolean;
29 type Roman is array(Positive range <=) of Roman_Digit; -- see 3.5.2

Examples of type declarations with constrained array definitions:

30 type Table is array(1 .. 10) of Integer;
31 type Schedule is array(Day) of Boolean;
32 type Line is array(1 .. Max_Line_Size) of Character;

Examples of object declarations with array type definitions:

30/2 {AI95-00433-01} Grid : array(1 .. 80, 1 .. 100) of Boolean;
31 Mix : array(Color range Red .. Green) of Boolean;
32 Msg_Table : constant array(Error Code) of access constant String :=
33 (Too_Big => new String'("Result too big"), Too_Small => ...);  
34 Page : array(Positive range <=) of Line := -- an array of arrays
35                (1 .. 50 => Line'(1 | Line'Last => '+', others => ' - ')), -- see 4.3.3
36                2 .. 49 => Line'(1 | Line'Last => '|', others => ' '),
37                -- Page is constrained by its initial value to (1..50)
Extensions to Ada 83

The syntax rule for component_definition is modified to allow the reserved word aliased.
The syntax rules for unconstrained_array_definition and constrained_array_definition are modified to use component_definition (instead of component_subtype_indication). The effect of this change is to allow the reserved word aliased before the component_subtype_indication.

A range in a discrete_subtype_definition may use arbitrary universal expressions for each bound (e.g. \(-1 \ldots 3+5\)), rather than strictly "implicitly convertible" operands. The subtype defined will still be a subtype of Integer.

Wording Changes from Ada 83

We introduce a new syntactic category, discrete_subtype_definition, as distinct from discrete_range. These two constructs have the same syntax, but their semantics are quite different (one defines a subtype, with a preference for Integer subtypes, while the other just selects a subrange of an existing subtype). We use this new syntactic category in for loops and entry families.

The syntax for index_constraint and discrete_range have been moved to their own subclause, since they are no longer used here.

The syntax rule for component_definition (formerly component_subtype_definition) is moved here from RM83-3.7.

Extensions to Ada 95

\{AI95-00230-01\} \{AI95-00406-01\} Array components can have an anonymous access type.

\{AI95-00363-01\} The prohibition against unconstrained discriminated aliased components has been lifted. It has been replaced by a prohibition against the actual troublemakers: general access discriminant constraints (see 3.7.1).

Wording Changes from Ada 95

\{8652/0002\} \{AI95-00171-01\} Corrigendum: Added wording to allow the elaboration of per-object constraints for constrained arrays.

Extensions to Ada 2005

\{AI05-0228-1\} The new aspect Default_Component_Value allows defining implicit initial values (see 3.3.1) for arrays of scalar types.

3.6.1 Index Constraints and Discrete Ranges

An index_constraint determines the range of possible values for every index of an array subtype, and thereby the corresponding array bounds.

Syntax

\[
\text{index\_constraint ::= (discrete\_range \{, discrete\_range\})} \\
\text{discrete\_range ::= discrete\_subtype\_indication | range}
\]

Name Resolution Rules

The type of a discrete_range is the type of the subtype defined by the subtype_indication, or the type of the range. For an index_constraint, each discrete_range shall resolve to be of the type of the corresponding index.

Discussion: In Ada 95, index_constraints only appear in a subtype_indication; they no longer appear in constrained_array_definitions.

Legality Rules

An index_constraint shall appear only in a subtype_indication whose subtype_mark denotes either an unconstrained array subtype, or an unconstrained access subtype whose designated subtype is an unconstrained array subtype; in either case, the index_constraint shall provide a discrete_range for each index of the array type.
Static Semantics

A discrete_range defines a range whose bounds are given by the range, or by the range of the subtype defined by the subtype_indication.

Dynamic Semantics

An index_constraint is compatible with an unconstrained array subtype if and only if the index range defined by each discrete_range is compatible (see 3.5) with the corresponding index subtype. If any of the discrete_ranges defines a null range, any array thus constrained is a null array, having no components. An array value satisfies an index_constraint if at each index position the array value and the index_constraint have the same index bounds.

Ramification: There is no need to define compatibility with a constrained array subtype, because one is not allowed to constrain it again.

The elaboration of an index_constraint consists of the evaluation of the discrete_range(s), in an arbitrary order. The evaluation of a discrete_range consists of the elaboration of the subtype_indication or the evaluation of the range.

NOTE 1  The elaboration of a subtype_indication consisting of a subtype_mark followed by an index_constraint checks the compatibility of the index_constraint with the subtype_mark (see 3.2.2).

NOTE 2  Even if an array value does not satisfy the index constraint of an array subtype, Constraint_Error is not raised on conversion to the array subtype, so long as the length of each dimension of the array value and the array subtype match. See 4.6.

Examples

Examples of array declarations including an index constraint:

{AI12-0442-1} Board : Matrix(1 .. 8, 1 .. 8); -- see 3.6
Rectangle : Matrix(1 .. 20, 1 .. 30);
Inverse : Matrix(1 .. N, 1 .. N); -- N can be nonstatic
{AI125-0430-1} Filter : Bit_Vector(0 .. 31); -- see 3.6

Example of array declaration with a constrained array subtype:

My_Schedule : Schedule; -- all arrays of type Schedule have the same bounds

Example of record type with a component that is an array:

type Var_Line(Length : Natural) is
  record
    Image : String(1 .. Length);
  end record;

Null_Line : Var_Line(0); -- Null_Line.Image is a null array

Extensions to Ada 83

We allow the declaration of a variable with a nominally unconstrained array subtype, so long as it has an initialization expression to determine its bounds.

Wording Changes from Ada 83

We have moved the syntax for index_constraint and discrete_range here since they are no longer used in constrained_array_definitions. We therefore also no longer have to describe the (special) semantics of index_constraints and discrete_ranges that appear in constrained_array_definitions.

The rules given in RM83-3.6.1(5,7-10), which define the bounds of an array object, are redundant with rules given elsewhere, and so are not repeated here. RM83-3.6.1(6), which requires that the (nominal) subtype of an array variable be constrained, no longer applies, so long as the variable is explicitly initialized.
3.6.2 Operations of Array Types

Legality Rules

[The argument N used in the attribute_designators for the N-th dimension of an array shall be a static expression of some integer type.] The value of N shall be positive (nonzero) and no greater than the dimensionality of the array.

Static Semantics

{8652/0006} {AI95-00030-01} The following attributes are defined for a prefix A that is of an array type [(after any implicit dereference)], or denotes a constrained array subtype:

Ramification: These attributes are not defined if A is a subtype-mark for an access-to-array subtype. They are defined (by implicit dereference) for access-to-array values.

A'First
A'First denotes the lower bound of the first index range; its type is the corresponding index type.

A'First(N)
A'First(N) denotes the lower bound of the N-th index range; its type is the corresponding index type.

A'Last
A'Last denotes the upper bound of the first index range; its type is the corresponding index type.

A'Last(N)
A'Last(N) denotes the upper bound of the N-th index range; its type is the corresponding index type.

A'Range
A'Range is equivalent to the range A'First .. A'Last, except that the prefix A is only evaluated once.

A'Range(N)
A'Range(N) is equivalent to the range A'First(N) .. A'Last(N), except that the prefix A is only evaluated once.

A'Length
A'Length denotes the number of values of the first index range (zero for a null range); its type is universal_integer.

A'Length(N)
A'Length(N) denotes the number of values of the N-th index range (zero for a null range); its type is universal_integer.

Implementation Advice

{AI05-0229-1} An implementation should normally represent multidimensional arrays in row-major order, consistent with the notation used for multidimensional array aggregates (see 4.3.3). However, if convention a pragma Convention(Fortran is specified for ...), applies to a multidimensional array type, then column-major order should be used instead (see B.5, “Interfacing with Fortran”).

Implementation Advice: Multidimensional arrays should be represented in row-major order, unless the array has

NOTE 1 The attribute_references A'First and A'First(1) denote the same value. A similar relation exists for the attribute_references A'Last, A'Range, and A'Length. The following relation is satisfied (except for a null array) by the above attributes if the index type is an integer type:

A'Length(N) = A'Last(N) - A'First(N) + 1

NOTE 2 An array type is limited if its component type is limited (see 7.5).

NOTE 3 The predefined operations of an array type include the membership tests, qualification, and explicit conversion. If the array type is not limited, they also include assignment and the predefined equality operators. For a one-dimensional
array type, they include the predefined concatenation operators (if nonlimited) and, if the component type is discrete, the predefined relational operators; if the component type is boolean, the predefined logical operators are also included.

NOTE 4  {AI95-00287-01} A component of an array can be named with an indexed_component. A value of an array type can be specified with an array_aggregate, unless the array type is limited. For a one-dimensional array type, a slice of the array can be named; also, string literals are defined if the component type is a character type.

Examples

Examples (using arrays declared in the examples of subclause 3.6.1):

```ada
-- Filter'First   = 0   Filter'Last    = 31   Filter'Length  = 32
-- Rectangle'Last (1) = 20   Rectangle'Last (2) = 30
```

3.6.3 String Types

**Static Semantics**

A one-dimensional array type whose component type is a character type is called a string type.

[AI95-00285-01] [There are three predefined string types, String, and Wide_String, and Wide_Wide_String, each indexed by values of the predefined subtype Positive; these are declared in the visible part of package Standard:]

```ada
subtype Positive is Integer range 1 .. Integer'Last;
type String is array (Positive range <>) of Character;
type Wide_String is array (Positive range <>) of Wide_Character;
type Wide_Wide_String is array (Positive range <>) of Wide_Wide_Character;
```

NOTE  String literals (see 2.6 and 4.2) are defined for all string types. The concatenation operator & is predefined for string types, as for all nonlimited one-dimensional array types. The ordering operators <, <=, >, and >= are predefined for string types, as for all one-dimensional discrete array types; these ordering operators correspond to lexicographic order (see 4.5.2).

Examples of string objects:

```ada
Stars      : String (1 .. 120) := (1 .. 120 => '*');
Question   : constant String  := "How many characters?";
             -- Question'First = 1, Question'Last = 20
             -- Question'Length = 20 (the number of characters)
Ask_Twice  : String  := Question & Question;  -- constrained to (1..40)
Ninety_Six : constant Roman := "XCVI";       -- see 3.5.2 and 3.6
```

Inconsistencies With Ada 83

8.a The declaration of Wide_String in Standard hides a use-visible declaration with the same defining_identifier. In rare cases, this might result in an inconsistency between Ada 83 and Ada 95.

Incompatibilities With Ada 83

8.b Because both String and Wide_String are always directly visible, an expression like

```
a" < "bc"
```

is now ambiguous, whereas in Ada 83 both string literals could be resolved to type String.

Extensions to Ada 83

8.e The type Wide_String is new (though it was approved by ARG for Ada 83 compilers as well).

Wording Changes from Ada 83

8.f We define the term string type as a natural analogy to the term character type.
Inconsistencies With Ada 95

\{AI95-00285-01\} The declaration of Wide_Wide_String in Standard hides a use-visible declaration with the same defining_identifier. In the (very) unlikely event that an Ada 95 program had depended on such a use-visible declaration, and the program remains legal after the substitution of Standard.Wide_Wide_String, the meaning of the program will be different.

Extensions to Ada 95

\{AI95-00285-01\} The type Wide_Wide_String is new.

3.7 Discriminants

\{AI95-00251-01\} \{AI95-00326-01\} A composite type (other than an array or interface type) can have discriminants, which parameterize the type. A known_discriminant_part specifies the discriminants of a composite type. A discriminant of an object is a component of the object, and is either of a discrete type or an access type. An unknown_discriminant_part in the declaration of a partial view of a type specifies that the discriminants of the type are unknown for the given view; all subtypes of such a partial view are indefinite subtypes.

Term entry: discriminant — parameter for a composite type, which can control, for example, the bounds of a component that is an array

Note: A discriminant for a task type can be used to pass data to a task of the type upon its creation.

Discussion: \{AI95-00114-01\} A view of a type, and all of its subtypes of the view, have unknown discriminants when the number or names of the discriminants, if any, are unknown at the point of the type declaration for the view. A discriminant_part of (<> is used to indicate unknown discriminants.

Language Design Principles

\{AI95-00402-01\} When an access discriminant is initialized at the time of object creation with an allocator of an anonymous type, the allocated object and the object with the discriminant are tied together for their lifetime. They should be allocated out of the same storage pool, and then at the end of the lifetime of the enclosing object, finalized and reclaimed together. In this case, the allocated object is called a coextension (see 3.10.2).

Discussion: The above principle when applied to a nonlimited type implies that such an object may be copied only to a shorter-lived object, because attempting to assign it to a longer-lived object would fail because the access discriminants would not match. In a copy, the lifetime connection between the enclosing object and the allocated object does not exist. The allocated object is tied in the above sense only to the original object. Other copies have only secondary references to it.

Note that when an allocator appears as a constraint on an access discriminant in a subtype_indication that is elaborated independently from object creation, no such connection exists. For example, if a named constrained subtype is declared via "subtype Constr is Rec(Acc_Discrim => new T);", or if such an allocator appears in the subtype_indication for a component, the allocator is evaluated when the subtype_indication is elaborated, and hence its lifetime is typically longer than the objects or components that will later be subject to the constraint. In these cases, the allocated object should not be reclaimed until the subtype_indication goes out of scope.

Syntax

discriminant_part ::= unknown_discriminant_part | known_discriminant_part

unknown_discriminant_part ::= (<>)

known_discriminant_part ::= (discriminant_specification {; discriminant_specification})

\{AI95-00231-01\} \{AI12-0398-1\} discriminant_specification ::= defining_identifier_list : [null_exclusion] subtype_mark [:= default_expression] [aspect_specification] defining_identifier_list : access_definition [:= default_expression] [aspect_specification]
Discriminants

5.a/5

Discussion: [AI12-0398-1] Only implementation-defined aspects are allowed on discriminants in Ada 2022. Implementers are cautioned that any aspect allowed on a discriminant will need conformance rules. If, for instance, an aspect changed the representation of a discriminant, rules would be needed to ensure that the representation is the same for all views of the type (partial and full).

6

default_expression ::= expression

Name Resolution Rules

7

The expected type for the default_expression of a discriminant_specification is that of the corresponding discriminant.

Legality Rules

8/2 {8652/0007} {AI95-00098-01} {AI95-00251-01} A discriminant_part_known_discriminant_part is only permitted in a declaration for a composite type that is not an array or interface type (this includes generic formal types). A type declared with a known_discriminant_part is called a discriminated type, as is a type that inherits (known) discriminants.

8.a

Implementation Note: Discriminants on array types were considered, but were omitted to ease (existing) implementations.

8.b

Discussion: Note that the above definition for “discriminated type” does not include types declared with an unknown_discriminant_part. This seems consistent with Ada 83, where such types (in a generic formal part) would not be considered discriminated types. Furthermore, the full type for a type with unknown discriminants need not even be composite, much less have any discriminants.

8.b.1/1 {8652/0007} {AI95-00098-01} On the other hand, unknown_discriminant_parts cannot be applied to type declarations that cannot have a known_discriminant_part. There is no point in having unknown discriminants on a type that can never have discriminants (for instance, a formal modular type), even when these are allowed syntactically.

9/2 {AI95-00231-01} {AI95-00254-01} The subtype of a discriminant may be defined by an optional null exclusion and a subtype_mark, in which case the subtype_mark shall denote a discrete or access subtype, or it may be defined by an access_definition [(in which case the subtype_mark of the access_definition may denote any kind of subtype)]. A discriminant that is defined by an access_definition is called an access_discriminant and is of an anonymous access_general_access_variable_type whose designated subtype is denoted by the subtype_mark of the access_definition.

9.a/2

This paragraph was deleted

Reason: {AI95-00230-01} In an early version of Ada 9X, we allowed access discriminants on nonlimited types, but this created unpleasant complexities. It turned out to be simpler and more uniform to allow discriminants of a named access type on any discriminated type, and keep access discriminants just for limited types.

9.b

Note that discriminants of a named access type are not considered “access discriminants”. Similarly, “access parameter” only refers to a formal parameter defined by an access_definition.

9.1/3 {AI95-00402-01} {AI05-0214-1} Default_expressions shall be provided either for all or for none of the discriminants of a known_discriminant_part. No default_expressions are permitted in a known_discriminant_part in a declaration of a nonlimited tagged type [or a generic formal type].

9.0/2

Reason: The all-or-none rule is related to the rule that a discriminant constraint shall specify values for all discriminants. One could imagine a different rule that allowed a constraint to specify only some of the discriminants, with the others provided by default. Having defaults for discriminants has a special significance — it allows objects of the type to be unconstrained, with the discriminants alterable as part of assigning to the object.

9.0/3 {AI05-0214-1} Defaults for discriminants of tagged types are disallowed so that every object of a nonlimited tagged type is constrained, either by an explicit constraint, or by its initial discriminant values. This substantially simplifies the semantic rules and the implementation of inherited dispatching operations. We don’t need this rule for limited tagged types, as the discriminants of such objects cannot be changed after the object is created in any case — no full-object assignment is supported, and that is required to change discriminant values. For generic formal types, the restriction simplifies the type matching rules. If one simply wants a "default" value for the discriminants, a constrained subtype can be declared for future use.

10/3 {AI95-00230-01} {AI95-00402-01} {AI95-00419-01} {AI05-0063-1} A discriminant_specification for an access discriminant may have a default_expression shall appear only in the declaration for an immutably limited type (see 7.5) a task or protected type, or for a type that is a descendant of an explicitly
limited record type with the reserved word limited in its [(full) definition or in that of one of its ancestors. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

Discussion: This rule implies that a type can have a default for an access discriminant if the type is limited, but not if the only reason it's limited is because of a limited component. Compare with the definition of limited type and immutably limited type in 7.5. Also, recall that a “descendant” includes the type itself, so an explicitly limited record type can have defaults.

Ramification: It is a consequence of this rule that only a return by reference type can have an access discriminant (see 6.5). This is important to avoid dangling references to local variables. A (nonformal) limited private type can always have a default for an access discriminant, because having the default itself makes the type immutably limited. Such a private type must necessarily have a full type with the same access discriminant with a default, and thus the full type will always be immutably limited (if legal).

Reason: [A95-00230-01] We also considered the following rules for access discriminants:

- If a type has an access discriminant, this automatically makes it limited, just like having a limited component automatically makes a type limited. This was rejected because it decreases program readability, and because it seemed error prone (two bugs in a previous version of the RM9X were attributable to this rule).
- A type with an access discriminant shall be limited. This is equivalent to the rule we actually chose for Ada 95, except that it allows a type to have an access discriminant if it is limited just because of a limited component. For example, any record containing a task would be allowed to have an access discriminant, whereas the actual rule requires “limited record”. This rule was also rejected due to readability concerns, and because would interact badly with the rules for limited types that “become nonlimited”.
- [A105-0063-1] A type may have an access discriminant if it is an immutably limited partial view, or a task, protected, or explicitly limited record type. This was the rule chosen for Ada 95.
- Any type may have an access discriminant. For nonlimited type, there is no special accessibility for access discriminants; they’re the same as any other anonymous access component. For a limited type, they have the special accessibility of Ada 95. However, this doesn’t work because a limited partial view can have a nonlimited full view -- giving the two views different accessibility.
- [A105-0063-1] Any type may have an access discriminant, as above. However, special accessibility rules only apply to types that are immutably limited (task, protected, and explicitly limited records). However, this breaks privacy; worse, Legality Rules depend on the definition of accessibility.
- [A105-0063-1] Any type may have an access discriminant, as above. Limited types have special accessibility, while nonlimited types have normal accessibility. However, a limited partial view with an access discriminant can only be completed by an immutably limited partial view, or a task, protected, or explicitly limited record type. That prevents accessibility from changing. A runtime accessibility check is required on generic formal types with access discriminants. However, changing between limited and nonlimited types would have far-reaching consequences for access discriminants — which is uncomfortable.
- Any type may have an access discriminant. All types have special accessibility. This was considered early during the Ada 9X process, but was dropped for “unpleasant complexities”, which unfortunately aren’t recorded. It does seem that an accessibility check would be needed on assignment of such a type, to avoid copying an object with a discriminant pointing to a local object into a more global object (and thus creating a dangling pointer).
- Any type may have an access discriminant, but access discriminants cannot have defaults. All types have special accessibility. This gets rid of the problems on assignment (you couldn’t change such a discriminant), but it would be horribly incompatible with Ada 95.
- [A105-0063-1] Any type may have an access discriminant, but access discriminants may have defaults only if they are of an immutably limited type. This is the rule chosen for Ada 2005, as it is not incompatible, and it doesn’t require weird accessibility checks.

This paragraph was deleted. [A95-00402-01] Default_expression shall be provided either for all or for none of the discriminants of a known Discriminant_part. No default_expression are permitted in a known_discriminant_part in a declaration of a tagged type [or a generic formal type].

Reason: The all-or-none rule is related to the rule that a discriminant constraint shall specify values for all discriminants. One could imagine a different rule that allowed a constraint to specify only some of the discriminants, with the others provided by default. Having defaults for discriminants has a special significance — it allows objects of the type to be unconstrained, with the discriminants alterable as part of assigning to the object.

Defaults for discriminants of tagged types are disallowed so that every object of a tagged type is constrained, either by an explicit constraint, or by its initial discriminant values. This substantially simplifies the semantic rules and the implementation of inherited dispatching operations. For generic formal types, the restriction simplifies the type
For a type defined by a derived_type_definition, if a known_discriminant_part is provided in its declaration, then:

- The parent subtype shall be constrained;
- If the parent type is not a tagged type, then each discriminant of the derived type shall be used in the constraint defining the parent subtype;

**Implementation Note:** This ensures that the new discriminant can share storage with an existing discriminant.

- If a discriminant is used in the constraint defining the parent subtype, the subtype of the discriminant shall be statically compatible (see 4.9.1) with the subtype of the corresponding parent discriminant.

**Reason:** This ensures that on conversion (or extension via an extension aggregate) to a distantly related type, if the discriminants satisfy the target type's requirements they satisfy all the intermediate types' requirements as well.

**Ramification:** There is no requirement that the new discriminant have the same (or any) default_expression as the parent's discriminant.

This paragraph was deleted. 

**This paragraph was deleted.**

Ramification: This requires convertibility of the designated subtypes.

**Static Semantics**

A discriminant_specification declares a discriminant; the subtype_mark denotes its subtype unless it is an access discriminant, in which case the discriminant's subtype is the anonymous access-to-variable subtype defined by the access_definition.

[For a type defined by a derived_type_definition, each discriminant of the parent type is either inherited, constrained to equal some new discriminant of the derived type, or constrained to the value of an expression.] When inherited or constrained to equal some new discriminant, the parent discriminant and the discriminant of the derived type are said to correspond. Two discriminants also correspond if there is some common discriminant to which they both correspond. A discriminant corresponds to itself as well. If a discriminant of a parent type is constrained to a specific value by a derived_type_definition, then that discriminant is said to be specified by that derived_type_definition.

**Ramification:** The correspondence relationship is transitive, symmetric, and reflexive. That is, if A corresponds to B, and B corresponds to C, then A, B, and C each corresponds to A, B, and C in all combinations.

A constraint that appears within the definition of a discriminated type depends on a discriminant of the type if it names the discriminant as a bound or discriminant value. A component_definition depends on a discriminant if its constraint depends on the discriminant, or on a discriminant that corresponds to it.

**Ramification:** A constraint in a task_body is not considered to depend on a discriminant of the task type, even if it names it. It is only the constraints in the type definition itself that are considered dependents. Similarly for protected types.

A component depends on a discriminant if:

- Its component_definition depends on the discriminant; or

  **Ramification:** A component does not depend on a discriminant just because its default_expression refers to the discriminant.

- It is declared in a variant_part that is governed by the discriminant; or

- It is a component inherited as part of a derived_type_definition, and the constraint of the parent_subtype_indication depends on the discriminant; or

  **Reason:** When the parent subtype depends on a discriminant, the parent part of the derived type is treated like a discriminant-dependent component.
Ramification: Because of this rule, we don't really need to worry about "corresponding" discriminants, since all the inherited components will be discriminant-dependent if there is a new known_discriminant_part whose discriminants are used to constrain the old discriminants.

- It is a subcomponent of a component that depends on the discriminant.

Reason: The concept of discriminant-dependent (sub)components is primarily used in various rules that disallow renaming or 'Access, or specify that certain discriminant-changing assignments are erroneous. The goal is to allow implementations to move around or change the size of discriminant-dependent subcomponents upon a discriminant-changing assignment to an enclosing object. The above definition specifies that all subcomponents of a discriminant-dependent component or parent part are themselves discriminant-dependent, even though their presence or size does not in fact depend on a discriminant. This is because it is likely that they will move in a discriminant-changing assignment if they are a component of one of several discriminant-dependent parts of the same record.

Each value of a discriminated type includes a value for each component of the type that does not depend on a discriminant; this includes the discriminants themselves. The values of discriminants determine which other component values are present in the value of the discriminated type.

To be honest: Which values are present might depend on discriminants of some ancestor type that are constrained in an intervening derived_type_definition. That's why we say "values of discriminants" instead of "values of the discriminants" — a subtle point.

A type declared with a known_discriminant_part is said to have known discriminants; its first subtype is unconstrained. A type declared with an unknown_discriminant_part is said to have unknown discriminants. A type declared without a discriminant_part has no discriminants, unless it is a derived type; if derived, such a type has the same sort of discriminants (known, unknown, or none) as its parent (or ancestor) type. A tagged class-wide type also has unknown discriminants. [Any subtype of a type with unknown discriminants is an unconstrained and indefinite subtype (see 3.2 and 3.3.).]

Discussion: [AI95-00114-01] An unknown_discriminant_part "(<>)") is only permitted in the declaration of a (generic or nongeneric) private type, private extension, incomplete_type, or formal derived type. Hence, only such types, descendants thereof, and class-wide types can have unknown discriminants. An unknown_discriminant_part is used to indicate that the corresponding actual or full type might have discriminants without defaults, or be an unconstrained array subtype. Tagged class-wide types are also considered to have unknown discriminants because discriminants can be added by type extensions, so the total number of discriminants of any given value of a tagged class-wide type is not known at compile time.

{AI95-00287-01} A subtype with unknown discriminants is indefinite, and hence an object of such a subtype needs explicit initialization. If the subtype is limited, no (stand alone) objects can be declared since initialization is not permitted (though formal parameters are permitted, and objects of the actual/full type will generally be declarable). A limited private type with unknown discriminants is "extremely" limited; objects of such a type can be initialized only by subprograms (either procedures with a parameter of the type, or a function returning the type) declared in the package. Subprograms declared elsewhere can operate on and even return the type, but they can only initialize the object by calling (ultimately) a subprogram in the package declaring the type. Such a type is useful for keeping complete control over object creation within the package declaring the type.

A partial view of a type might have unknown discriminants, while the full view of the same type might have known, unknown, or no discriminants.

Dynamic Semantics

{AI95-00230-01} {AI95-00416-01} For an access discriminant, its corresponding access_definition is elaborated when the value of the corresponding access discriminant is defined; either by evaluation of its default_expression, or by elaboration of a discriminant_constraint, or by an assignment that initializes the enclosing object. [The elaboration of an access_definition creates the anonymous access type. When the expression defining the access discriminant is evaluated, it is converted to this anonymous access type (see 4.6).]

Ramification: [AI95-00231-01] {AI95-00416-01} The conversion of the expression defining the access discriminant to the anonymous access type raises Program_ErrorConstraint_Error if the initial value is null, or, for an object created by an allocator of an access type T, if the initial value is an access parameter that designates a view whose accessibility level is deeper than that of T.

NOTE 1 If a discriminated type has default_expressions for its discriminants, then unconstrained variables of the type are permitted, and the values of the discriminants can be changed by an assignment to such a variable. If defaults are not
provided for the discriminants, then all variables of the type are constrained, either by explicit constraint or by their initial value; the values of the discriminants of such a variable cannot be changed after initialization.

**Discussion:** This connection between discriminant defaults and unconstrained variables can be a source of confusion. For Ada 95, we considered various ways to break the connection between defaults and unconstrainedness, but ultimately gave up for lack of a sufficiently simple and intuitive alternative.

An unconstrained discriminated subtype with defaults is called a mutable subtype, and a variable of such a subtype is called a mutable variable, because the discriminants of such a variable can change. There are no mutable arrays (that is, the bounds of an array object can never change), because there is no way in the language to define default values for the bounds. Similarly, there are no mutable class-wide subtypes, because there is no way to define the default tag, and defaults for discriminants are not allowed in the tagged case. Mutable tags would also require a way for the maximum possible size of such a class-wide subtype to be known. (In some implementations, all mutable variables are allocated with the maximum possible size. This approach is appropriate for real-time applications where implicit use of the heap is inappropriate.)

**NOTE 2** The default_expression for a discriminant of a type is evaluated when an object of an unconstrained subtype of the type is created.

**NOTE 3** Assignment to a discriminant of an object (after its initialization) is not allowed, since the name of a discriminant is a constant; neither assignment_statements nor assignments inherent in passing as an in out or out parameter are allowed. Note however that the value of a discriminant can be changed by assigning to the enclosing object, presuming it is an unconstrained variable.

**Discussion:** {AI95-00114-01} An unknown_discriminant_part is permitted only in the declaration of a private type (including generic formal private), private extension, incomplete type, or generic formal derived type. These are the things that will have a corresponding completion or generic actual, which will either define the discriminants, or say there are none. The (<>) indicates that the actual/full subtype might be an indefinite subtype. An unknown_discriminant_part is not permitted in a normal untagged derived type declaration, because there is no separate full type declaration for such a type. Note that (<>) allows unconstrained array bounds; those are somewhat like undefaulted discriminants.

For a derived type, either the discriminants are inherited as is, or completely respecified in a new discriminant_part. In this latter case, each discriminant of the parent type shall be constrained, either to a specific value, or to equal one of the new discriminants. Constraining a parent type's discriminant to equal one of the new discriminants is like a renaming of the discriminant, except that the subtype of the new discriminant can be more restrictive than that of the parent's one. In any case, the new discriminant can share storage with the parent's discriminant.

**NOTE 4** A discriminant that is of a named access type is not called an access discriminant; that term is used only for discriminants defined by an access_definition.

**Examples**

**Examples of discriminated types:**

```ada
33 type Buffer(Size : Buffer_Size := 100) is
     record
       Pos   : Buffer_Size := 0;
       Value : String(1 .. Size);
     end record;

34 type Matrix_Rec(Rows, Columns : Integer) is
     record
       Mat : Matrix(1 .. Rows, 1 .. Columns);
     end record;

35 type Square(Side : Integer) is new
     Matrix_Rec(Rows => Side, Columns => Side);

36 type Double_Square(Number : Integer) is
     record
       Left  : Square(Number);
       Right : Square(Number);
     end record;
```
task type Worker(Prio : System.Priority; Buf : access Buffer)
  with Priority => Prio is -- see D.1
  pragma Priority(Prio); -- see D.1
  entry Fill;
  entry Drain;
end Worker;

type Item(Number : Positive) is
  record
    Content : Integer;
  end record;

Discriminants

Discriminants are allowed on all composite types other than array and interface types. Discriminants may be of an access type.

Wording Changes from Ada 83

Discriminant_parts are not elaborated, though an access_definition is elaborated when the discriminant is initialized.

Extensions to Ada 95

Access discriminants (anonymous access types used as a discriminant) can be used on any type allowing discriminants. Defaults aren't allowed on discriminants of nonlimited types, however, so that accessibility problems don't happen on assignment.

null_exclusion can be used in the declaration of a discriminant.

Wording Changes from Ada 95

Corrigendum: The wording was clarified so that types that cannot have discriminants cannot have an unknown_discriminant_part.

Added wording to prevent interfaces from having discriminants. We don't want interfaces to have any components.

Removed wording which implied or required an access discriminant to have an access-to-object type (anonymous access types can now be access-to-subprogram types as well).

Fixed the wording of the introduction to this subclause to reflect that both incomplete and partial views can have unknown discriminants. That was always true, but for some reason this wording specified partial views.

Changed the wording to use the new term "explicitly limited record", which makes the intent much clearer (and eliminates confusion with derived types that happen to contain the reserved word limited).

Incompatibilities With Ada 2005

Correction: Changed the rules for when access discriminants can have defaults to depend on the new definition for immutably limited types; this will help ensure that unusual corner cases are properly handled. Note that the Ada 2005 rule was unintentionally incompatible with the Ada 95 rule (as enforced by the ACATS); this change brings it back into alignment with actual practice. So there should be no practical incompatibility.

A limited tagged type may now have defaults for its discriminants.

Correction: Moved implicit conversion Legality Rule to 8.6.

Discriminants now can have an aspect_specification, allowing the specification of (implementation-defined) aspects for individual discriminants.
3.7.1 Discriminant Constraints

A discriminant_constraint specifies the values of the discriminants for a given discriminated type.

**Language Design Principles**

The rules in this clause are intentionally parallel to those given in 4.3.1, “Record Aggregates”.

**Syntax**

`discriminant_constraint ::= (discriminant_association {, discriminant_association})`

`{AI12-0212-1}`

`discriminant_association ::= [discriminant_selector_name { '|' discriminant_selector_name } =>] expression`

A discriminant_association is said to be named if it has one or more discriminant_selector_names; it is otherwise said to be positional. In a discriminant_constraint, any positional associations shall precede any named associations.

**Name Resolution Rules**

Each selector_name of a named discriminant_association shall resolve to denote a discriminant of the subtype being constrained; the discriminants so named are the associated discriminants of the named association. For a positional association, the associated discriminant is the one whose discriminant_specification occurred in the corresponding position in the known_discriminant_part that defined the discriminants of the subtype being constrained.

The expected type for the expression in a discriminant_association is that of the associated discriminant(s).

**Legality Rules**

A discriminant_constraint is only allowed in a subtype_indication whose subtype_mark denotes either an unconstrained discriminated subtype, or an unconstrained access subtype whose designated subtype is an unconstrained discriminated subtype. However, in the case of a general access subtype, a discriminant_constraint is legal only if any dereference of a value of the access type is known to be constrained (see 3.3); illegal if the designated type has a partial view that is constrained or, for a general access subtype, has default_expressions for its discriminants.

This paragraph was deleted. **Reason:** The second rule is necessary to prevent assignments that change the discriminant of a constrained object. See the defect report for examples.

**Discussion:** The second rule will only use the indefinite or dereference bullets in the definition of “known to be constrained”. The rule is worded in terms of “known to be constrained” in order to capture the special rules that apply in generic bodies (rather than repeating them and getting them subtly wrong).
A named discriminant_association with more than one selector_name is allowed only if the named discriminants are all of the same type. A discriminant_constraint shall provide exactly one value for each discriminant of the subtype being constrained.

This paragraph was deleted.\[^{AI05-0102-1}\] The expression associated with an access discriminant shall be of a type convertible to the anonymous access type.

**Ramification:** In addition, 8.6 requires that the expression associated with an access discriminant is convertible (see 4.6) to the anonymous access type. This implies both convertibility of designated types, and static accessibility. This implies that if an object of type T with an access discriminant is created by an allocator for an access type A, then it requires that the type of the expression associated with the access discriminant have an accessibility level that is not statically deeper than that of A. This is to avoid dangling references.

**Dynamic Semantics**

A discriminant_constraint is compatible with an unconstrained discriminated subtype if each discriminant value belongs to the subtype of the corresponding discriminant.

**Ramification:** The "dependent compatibility check" has been eliminated in Ada 95. Any checking on subcomponents is performed when (and if) an object is created.

**Discussion:** There is no need to define compatibility with a constrained discriminated subtype, because one is not allowed to constrain it again.

A composite value satisfies a discriminant constraint if and only if each discriminant of the composite value has the value imposed by the discriminant constraint.

\[^{AI12-0439-1}\] For the elaboration of a discriminant_constraint, the expressions in the discriminant_associations are evaluated in an arbitrary order and converted to the type of the associated discriminant (which **cannot** raise Constraint_Error — see 4.6); the expression of a named association is evaluated (and converted) once for each associated discriminant. The result of each evaluation and conversion is the value imposed by the constraint for the associated discriminant.

**Reason:** We convert to the type, not the subtype, so that the definition of compatibility of discriminant constraints is not vacuous.

**Note** The rules of the language ensure that a discriminant of an object always has a value, either from explicit or implicit initialization.

**Discussion:** Although it is illegal to constrain a class-wide tagged subtype, it is possible to have a partially constrained class-wide subtype: If the subtype S is defined by T(A => B), then S'Class is partially constrained in the sense that objects of subtype S'Class have to have discriminants corresponding to A equal to B, but there can be other discriminants defined in extensions that are not constrained to any particular value.

**Examples**

\[^{AI05-0299-1}\] \[^{AI12-0449-1}\] Examples (using types declared above in subclause clause-3.7):

```
Large   : Buffer(200);  -- constrained, always 200 characters
Message : Buffer;       -- unconstrained, initially 100 characters
    -- (default discriminant value)
Basis   : Square(5);    -- constrained, always 5 by 5
Illegal : Square;       -- illegal, a Square has to be constrained
```

**Inconsistencies With Ada 83**

Dependent compatibility checks are no longer performed on subtype declaration. Instead they are deferred until object creation (see 3.3.1). This is upward compatible for a program that does not raise Constraint_Error.

**Wording Changes from Ada 83**

Everything in RM83-3.7.2(7-12), which specifies the initial values for discriminants, is now redundant with 3.3.1, 6.4.1, 8.5.1, and 12.4. Therefore, we don't repeat it here. Since the material is largely intuitive, but nevertheless complicated to state formally, it doesn't seem worth putting it in a "Note".
Incompatibilities With Ada 95

The Corrigendum added a restriction on discriminant_constraints for general access subtypes. Such constraints are prohibited if the designated type can be treated as constrained somewhere in the program. Ada 2005 goes further and prohibits such discriminant_constraints if the designated type has (or might have, in the case of a formal type) defaults for its discriminants. The use of general access subtypes is rare, and this eliminates a boatload of problems that required many restrictions on the use of aliased objects and components (now lifted). Similarly, Ada 2005 prohibits discriminant_constraints on any access type whose designated type has a partial view that is constrained. Such a type will not be constrained in the heap to avoid privacy problems. Again, the use of such subtypes is rare (they can only happen within the package and its child units).

Wording Changes from Ada 2005

Correction: Revised the rules on access subtypes having discriminant constraints to depend on the “known to be constrained” rules. This centralizes the rules so that future fixes need to be made in only one place, as well as fixing bugs in obscure cases.

Correction: Moved implicit conversion Legality Rule to 8.6.

3.7.2 Operations of Discriminated Types

If a discriminated type has default_expressions for its discriminants, then unconstrained variables of the type are permitted, and the discriminants of such a variable can be changed by assignment to the variable. For a formal parameter of such a type, an attribute is provided to determine whether the corresponding actual parameter is constrained or unconstrained.

Static Semantics

For a prefix A that is of a discriminated type [(after any implicit dereference)], the following attribute is defined:

\[ \text{A'Constrained} \]

Yields the value True if A denotes a constant, a value, a tagged object, or a constrained variable, and False otherwise. The value of this attribute is of the predefined type Boolean.

Implementation Note: This attribute is primarily used on parameters, to determine whether the discriminants can be changed as part of an assignment. The Constrained attribute is statically True for in parameters. For in out and out parameters of a discriminated type, the value of this attribute needs to be passed as an implicit parameter, in general. However, if the type is tagged or does not have defaults for its discriminants, the attribute is statically True, so no implicit parameter is needed. Parameters of a limited untagged type with defaulted discriminants need this implicit parameter, unless there are no nonlimited views, because they might be passed to a subprogram whose body has visibility on a nonlimited view of the type, and hence might be able to assign to the object and change its discriminants.

Reason: All tagged objects are known to be constrained (as nonlimited tagged types cannot have discriminant defaults, and limited tagged objects are immutably limited), and are always considered constrained by this attribute to avoid distributed overhead for parameters of limited class-wide classwide types, as limited tagged objects may technically be unconstrained if they use defaulted discriminants. Such objects still cannot have their discriminants changed, as assignment is not supported for them, so there is no use for this attribute that would justify the overhead of passing it with all class-wide classwide parameters.

Discussion: If the type of A is a type derived from an untagged partial view of a tagged type such that it is not a tagged type, then A is not considered a tagged object, and A'Constrained can return either True or False depending on the nature of the object.

Erroneous Execution

The execution of a construct is erroneous if the construct has a constituent that is a name denoting a subcomponent that depends on discriminants, and the value of any of these discriminants is changed by this execution between evaluating the name and the last use (within this execution) of the subcomponent denoted by the name.
Ramification: This rule applies to assignment statements, calls (except when the discriminant-dependent subcomponent is an in parameter passed by copy), indexed components, and slices. Ada 83 only covered the first two cases. A183-00585 pointed out the situation with the last two cases. The cases of object_renaming_declarations and generic formal in out objects are handled differently, by disallowing the situation at compile time.

Extensions to Ada 83

For consistency with other attributes, we are allowing the prefix of Constrained to be a value as well as an object of a discriminated type, and also an implicit dereference. These extensions are not important capabilities, but there seems no reason to make this attribute different from other similar attributes. We are curious what most Ada 83 compilers do with F(1).X’Constrained.

We now handle in a general way the cases of erroneousness identified by A183-00585, where the prefix of an indexed_component or slice is discriminant-dependent, and the evaluation of the index or discrete range changes the value of a discriminant.

Wording Changes from Ada 83

We have moved all discussion of erroneous use of names that denote discriminant-dependent subcomponents to this subclause. In Ada 83, it used to appear separately under assignment statements and subprogram calls.

Wording Changes from Ada 2005

{AI05-0214-1} A’Constrained is now defined to return True for any A that is a tagged object. This doesn’t change the result for any A allowed by previous versions of Ada; the change is necessary to avoid unnecessary overhead for limited tagged parameters.

3.8 Record Types

A record object is a composite object consisting of named components. The value of a record object is a composite value consisting of the values of the components.

Syntax

record_type_definition ::= [[abstract] tagged] [limited] record_definition

{AI12-0213-1} record_definition ::= record
  component_list
  end record [record_identifier]
| null record

component_list ::= component_item {component_item}
| {component_item} variant_part
| null;

{8652/0009} {AI95-00137-01} component_item ::= component_declaration | aspect_clause representation_clause

{AI05-0183-1} component_declaration ::= defining_identifier_list : component_definition [:= default_expression] [aspect_specification];

{AI12-0213-1} If a record_identifier appears at the end of the record_definition, it shall repeat the defining_identifier of the enclosing full_type_declaration.

Name Resolution Rules

The expected type for the default_expression, if any, in a component_declaration is the type of the component.
This paragraph was deleted. **AI95-00287-01** A default_expression is not permitted if the component is of a limited type.

**AI95-00366-01** Each component_declaration declares a component of the record type. Besides components declared by component_declarations, the components of a record type include any components declared by discriminant_specifications of the record type declaration. [The identifiers of all components of a record type shall be distinct.]

**Proof:** **AI05-0299-1** **AI12-0449-1** The identifiers of all components of a record type have to be distinct because they are all declared immediately within the same declarative region. See Clause 8 Clause Section 8.

Within a type_declaration, a name that denotes a component, protected subprogram, or entry of the type is allowed only in the following cases:

- **AI05-0004-1** **AI05-0295-1** A name that denotes any component, protected subprogram, or entry is allowed within an aspect_specification, an operational item, or a representation item that occurs within the declaration of the composite type.
- **AI05-0264-1** A name that denotes a noninherited discriminant is allowed within the declaration of the type, but not within the discriminant_part. If the discriminant is used to define the constraint of a component, the bounds of an entry family, or the constraint of the parent subtype in a derived_type_definition, then its name shall appear alone as a direct_name (not as part of a larger expression or expanded name). A discriminant shall not be used to define the constraint of a scalar component.

**Reason:** The penultimate restriction simplifies implementation, and allows the outer discriminant and the inner discriminant or bound to possibly share storage.

**Ramification:** Other rules prevent such a discriminant from being an inherited one.

**Reason:** The last restriction is inherited from Ada 83. The restriction is not really necessary from a language design point of view, but we did not remove it, in order to avoid unnecessary changes to existing compilers.

**Discussion:** Note that a discriminant can be used to define the constraint for a component that is of an access-to-composite type.

**Reason:** **AI95-00373-01** The above rules, and a similar one in 6.1 for formal parameters, are intended to allow initializations of components or parameters to occur in a (nearly) arbitrary order — whatever order is most efficient (subject to the restrictions of 3.3.1), since one default_expression cannot depend on the value of another one. They also prevent circularities.

**Ramification:** **AI05-0295-1** Inherited discriminants are not allowed to be denoted, except within aspect_specifications and representation items. However, the discriminant_selector_name of the parent subtype_indication is allowed to denote a discriminant of the parent.

If the name of the current instance of a type (see 8.6) is used to define the constraint of a component, then it shall appear as a direct_name that is the prefix of an attribute_reference whose result is of an access type, and the attribute_reference shall appear alone.

**Reason:** This rule allows T'Access or T'Unchecked_Access, but disallows, for example, a range constraint (1..T'Size). Allowing things like (1..T'Size) would mean that a per-object constraint could affect the size of the object, which would be bad.

**Static Semantics**

**AI95-00318-02** **AI05-0004-1** If a record_type_definition includes the reserved word limited, the type is called an explicitly limited record type.

The component_definition of a component_declaration defines the (nominal) subtype of the component. If the reserved word aliased appears in the component_definition, then the component is aliased (see 3.10).

**Ramification:** **AI95-00363-01** In this case, the nominal subtype cannot be an unconstrained discriminated subtype. See 3.6.
If the component_list of a record type is defined by the reserved word null and there are no
discriminants, then the record type has no components and all records of the type are null records. A
record_definition of null record is equivalent to record null; end record.

Ramification: {AI12-0426-1} This shorthand is available both for declaring a record type and a record
extension — see 3.9.1.

Dynamic Semantics

The elaboration of a record_type_definition creates the record type and its first subtype, and consists of
the elaboration of the record_definition. The elaboration of a record_definition consists of the elaboration
of its component_list, if any.

The elaboration of a component_list consists of the elaboration of the component_items and
variant_part, if any, in the order in which they appear. The elaboration of a component_declaration
consists of the elaboration of the component_definition.

Discussion: If the defining_identifier_list has more than one defining_identifier, we presume here that the
transformation explained in 3.3.1 has already taken place. Alternatively, we could say that the component_definition is
elaborated once for each defining_identifier in the list.

Within the definition of a composite type, if a
component_definition or discrete_subtype_definition (see 9.5.2) includes a name that denotes a
discriminant of the type, or that is an attribute_reference whose prefix denotes the current instance of the
type, the expression containing the name is called a per-object expression, and the constraint or
range being defined is called a per-object constraint. For the elaboration of a
component_definition of a component_declaration or the discrete_subtype_definition of an entry -
declaration for an entry family (see 9.5.2), if the component_subtype is defined by an access_definition
or if the constraint or range of the subtype_indication or discrete_subtype_definition is not a per-object
constraint, then the access_definition, subtype_indication, or discrete_subtype_definition is elaborated.
On the other hand, if the constraint or range is a per-object constraint, then the elaboration consists of the
evaluation of any included expression that is not part of a per-object expression. Each such expression is
evaluated once unless it is part of a named association in a discriminant constraint, in which case it is
evaluated once for each associated discriminant.

When a per-object constraint is elaborated [(as part of creating an
object)], each per-object expression of the constraint is evaluated. For other expressions, the values
determined during the elaboration of the component_definition or entry_declaration are used. Any
checks associated with the enclosing subtype_indication or discrete_subtype_definition are performed,
including the subtype compatibility check (see 3.2.2),] and the associated subtype is created.

Discussion: The evaluation of other expressions that appear in component_definitions and
discrete_subtype_definitions is performed when the type definition is elaborated. The evaluation of expressions that
appear as default_expressions is postponed until an object is created. Expressions in representation items that appear
within a composite type definition are evaluated according to the rules of the particular representation item.

NOTE 1 A component_declaration with several identifiers is equivalent to a sequence of single component_declarations,
as explained in 3.3.1.

NOTE 2 The default_expression of a record component is only evaluated upon the creation of a default-initialized object
of the record type (presuming the object has the component, if it is in a variant_part — see 3.3.1).

NOTE 3 The subtype defined by a component_definition (see 3.6) has to be a definite subtype.

NOTE 4 If a record type does not have a variant_part, then the same components are present in all values of the type.

NOTE 5 A record type is limited if it has the reserved word limited in its definition, or if any of its components are limited
(see 7.5).

NOTE 6 The predefined operations of a record type include membership tests, qualification, and explicit conversion. If the
record type is nonlimited, they also include assignment and the predefined equality operators.
NOTE 7  \{AI95-00287-01\} A component of a record can be named with a selected_component. A value of a record can be specified with a record_aggregate, unless the record type is limited.

Examples of record type declarations:

```ada
27/5  \{AI12-0430-1\} type Date is
case record
  Day   : Integer range 1 .. 31;
  Month : Month_Name;                  -- see 3.5.1
  Year  : Integer range 0 .. 4000;
end record;
28/5  \{AI12-0213-1\} type Complex is
  record
    Re : Real := 0.0;
    Im : Real := 0.0;
  end record Complex;
```

Examples of record variables:

```ada
29  Tomorrow, Yesterday : Date;
    A, B, C : Complex;
    -- both components of A, B, and C are implicitly initialized to zero
```

Extensions to Ada 83

31.a The syntax rule for component_declaration is modified to use component_definition (instead of component_subtype_definition). The effect of this change is to allow the reserved word aliased before the component_subtype_definition.

31.b A short-hand is provided for defining a null record type (and a null record extension), as these will be more common for abstract root types (and derived types without additional components).

31.c The syntax rule for record_type_definition is modified to allow the reserved words tagged and limited. Tagging is new. Limitedness is now orthogonal to privateness. In Ada 83 the syntax implied that limited private was sort of more private than private. However, limitedness really has nothing to do with privateness; limitedness simply indicates the lack of assignment capabilities, and makes perfect sense for nonprivate types such as record types.

Wording Changes from Ada 83

31.d/1  \{8652/0009\}  \{AI95-00137-01\} The syntax rules now allow aspect_clause, representation_clauses to appear in a record_definition. This is not a language extension, because Legality Rules prevent all language-defined representation clauses from appearing there. However, an implementation-defined attribute_definition_clause could appear there. The reason for this change is to allow the rules for aspect_clause, representation_clauses, and representation pragmas to be as similar as possible.

Extensions to Ada 95

31.e/2  \{AI95-00287-01\} Record components can have an anonymous access type.

31.f/2  \{AI95-00287-01\} Limited components can be initialized, so long as the expression is one that allows building the object in place (such as an aggregate or function_call).

Wording Changes from Ada 95

31.g/2  \{8652/0002\}  \{AI95-00171-01\} Corrigendum: Improved the description of the elaboration of per-object constraints.

31.h/2  \{8652/0009\}  \{AI95-00137-01\} Corrigendum: Changed representation clauses to aspect clauses to reflect that they are used for more than just representation.

31.i/2  \{AI95-00318-02\} Defined explicitly limited record type to use in other rules.

Extensions to Ada 2005

31.j/3  \{AI05-0183-1\} An optional aspect_specification can be used in a component_declaration. This is described in 13.1.1.

Extensions to Ada 2012

31.k/5  \{AI12-0213-1\} The record_identifier following end_record is new.
3.8.1 Variant Parts and Discrete Choices

A record type with a variant_part specifies alternative lists of components. Each variant defines the components for the value or values of the discriminant covered by its discrete_choice_list.

Discussion: Discrete_choice_lists and discrete_choices are said to cover values as defined below; which discrete_choice_list covers a value determines which of various alternatives is chosen. These are used in variant_parts, array_aggregates, and case_statements.

Language Design Principles
The definition of “cover” in this subclause and the rules about discrete choices are designed so that they are also appropriate for array aggregates and case statements.
The rules of this subclause intentionally parallel those for case statements.

Syntax

variant_part ::= case discriminant_direct_name is
variant {variant}
end case;

variant ::= when discrete_choice_list =>
component_list

{AI12-0212-1} discrete_choice_list ::= discrete_choice {""} discrete_choice

{AI05-0153-3} {AI05-0158-1} discrete_choice ::= choice_expressionexpression | discrete_subtype_indication | rangediscrete_range | others

Name Resolution Rules

The discriminant_direct_name shall resolve to denote a discriminant (called the discriminant of the variant_part) specified in the known_discriminant_part of the full_type_declaration that contains the variant_part. The expected type for each discrete_choice in a variant is the type of the discriminant of the variant_part.

Ramification: A full_type_declaration with a variant_part has to have a (new) known_discriminant_part; the discriminant of the variant_part cannot be an inherited discriminant.

Legality Rules

The discriminant of the variant_part shall be of a discrete type.

Ramification: It shall not be of an access type, named or anonymous.

{AI05-0153-3} The choice_expressions, subtype_indications, and ranges given as discrete_choices in a variant_part shall be static. The discrete_choice others shall appear alone in a discrete_choice_list, and such a discrete_choice_list, if it appears, shall be the last one in the enclosing construct.

A discrete_choice is defined to cover a value in the following cases:

- {AI05-0262-1} A discrete_choice that is a choice_expressionexpression covers a value if the value equals the value of the choice_expressionexpression converted to the expected type.
- {AI05-0153-3} {AI05-0262-1} {AI12-0071-1} A discrete_choice that is a subtype indication covers all values (possibly none) that belong to the subtype and that satisfy the static predicates of the subtype (see 3.2.4).
Ramification: {AI05-0262-1} A dynamic predicate is never allowed in this case (for variants, case statements, and case expressions, a subtype with a dynamic predicate isn’t static and thus isn’t allowed in a discrete choice, and for a choice in an array aggregate, a dynamic predicate is explicitly disallowed — see 3.2.4).

11/3
• {AI05-0153-3} A discrete_choice that is a ranged_discrete_range covers all values (possibly none) that belong to the range.

12
• The discrete_choice others covers all values of its expected type that are not covered by previous discrete_choice_lists of the same construct.

Ramification: For case statements, this includes values outside the range of the static subtype (if any) to be covered by the choices. It even includes values outside the base range of the case expression’s type, since values of numeric types (and undefined values of any scalar type?) can be outside their base range.

A discrete_choice_list covers a value if one of its discrete_choices covers the value.

The possible values of the discriminant of a variant_part shall be covered as follows:

15/4
• {AI05-0153-3} {AI05-0188-1} {AI05-0262-1} {AI12-0071-1} If the discriminant is of a static constrained scalar subtype, then, except within an instance of a generic unit, each non-others discrete_choice shall cover only values in that subtype that satisfy its predicate, and each value of that subtype that satisfies its predicate shall be covered by some discrete_choice [(either explicitly or by others)].

Reason: {AI05-0188-1} The exemption for a discriminated type declared in an instance allows the following example:

```ada
generic
type T is new Integer;
package G is
    type Rec (Discrim : T) is record
        case Discrim is
            when -10 .. -1 =>
                Foo : Float;
                null;
            when others =>
                null;
        end case;
    end record;
end G;
```

package I is new G (Natural); -- Legal

15/3
• {AI05-0264-1} If the type of the discriminant is a descendant of a generic formal scalar type, then the variant_part shall have an others discrete_choice;

Reason: The base range is not known statically in this case.

16.a
• Otherwise, each value of the base range of the type of the discriminant shall be covered [(either explicitly or by others)].

Two distinct discrete_choices of a variant_part shall not cover the same value.

Static Semantics

If the component_list of a variant is specified by null, the variant has no components.

The discriminant of a variant_part is said to govern the variant_part and its variants. In addition, the discriminant of a derived type governs a variant_part and its variants if it corresponds (see 3.7) to the discriminant of the variant_part.

Dynamic Semantics

A record value contains the values of the components of a particular variant only if the value of the discriminant governing the variant is covered by the discrete_choice_list of the variant. This rule applies in turn to any further variant that is, itself, included in the component_list of the given variant.

16.a
• {AI05-0290-1} When an object of a discriminated type T is initialized by default, Constraint_Error is raised if no discrete_choice_list of any variant of a variant_part of T covers the value of the discriminant that governs the variant_part. When a variant_part appears in the component_list of another variant V,
this test is only applied if the value of the discriminant governing $V$ is covered by the
discrete_choice_list of $V$.

**Implementation Note:** This is not a “check”; it cannot be suppressed. However, in most cases it is not necessary to
generate any code to raise this exception. A test is needed (and can fail) in the case where the discriminant subtype has
a Static Predicate specified, it also has predicate checking disabled, and the discriminant governs a variant_part which
lacks a when others choice.

The test also could fail for a static discriminant subtype with range checking suppressed and the discriminant governs a
variant_part which lacks a when others choice. But execution is erroneous if a range check that would have failed is
suppressed (see 11.5), so an implementation does not have to generate code to check this case. (An unchecked failed
predicate does not cause erroneous execution, so the test is required in that case.)

Like the checks associated with a per-object constraint, this test is not made during the elaboration of a
subtype_indication.

The elaboration of a variant_part consists of the elaboration of the component_list of each variant in the
order in which they appear.

**Examples**

**Example of record type with a variant part:**

```ada
type Device is (Printer, Disk, Drum);
type State is (Open, Closed);
type Peripheral (Unit : Device := Disk) is record
  Status : State;
case Unit is
  when Printer =>
    Line_Count : Integer range 1 .. Page_Size;
  when others =>
    Cylinder : Cylinder_Index;
    Track : Track_Number;
  end case;
end record;
```

**Examples of record subtypes:**

```ada
subtype Drum_Unit is Peripheral (Dum);
sstype Disk_Unit is Peripheral (Disk);
```

**Examples of constrained record variables:**

```ada
Writer : Peripheral (Unit  => Printer);
Archive : Disk_Unit;
```

**Extensions to Ada 83**

In Ada 83, the discriminant of a variant_part is not allowed to be of a generic formal type. This restriction is removed
in Ada 95; an others discrete_choice is required in this case.

**Wording Changes from Ada 83**

The syntactic category choice is removed. The syntax rules for variant, array_aggregate, and case_statement now
use discrete_choice_list or discrete_choice instead. The syntax rule for record_aggregate now defines its own syntax
for named associations.

{AI05-0299-1} We have added the term Discrete Choice to the title since this is where they are talked about. This is
analogous to the name of the subclause "Index Constraints and Discrete Ranges" in the subclause of Array
Types.

The rule requiring that the discriminant denote a discriminant of the type being defined seems to have been left implicit
in RM83.
Incompatibilities With Ada 2005

29.e/3  
{AI05-0158-1} Membership tests are no longer allowed as a discrete_choice, in order that those tests can be expanded to allow multiple tests in a single expression without ambiguity. Since a membership test has a boolean type, they are very unlikely to be used as a discrete_choice.

Extensions to Ada 2005

29.f/3  
{AI05-0153-3} Subtypes with static predicates can be used in discrete_choices, and the coverage rules are modified to respect the predicates.

29.g/3  
{AI05-0188-1} Variants in generic specifications are no longer rejected if the subtype of the actual type does not include all of the case choices. This probably isn't useful, but it is consistent with the treatment of case_expressions.

Wording Changes from Ada 2005

29.h/3  
{AI05-0290-1} Added a test that some variant covers the value of a discriminant that governs a variant_part. This is similar to the test that some case limb covers the value of the Selecting_expression of a case_statement. This test cannot change the behavior of any nonerroneous Ada 2005 program, so it is not an inconsistency.

Wording Changes from Ada 2012

29.i/4  
{AI12-0071-1} Corrigendum: Updated wording of the coverage rules to use the new term "satisfies the predicates" (see 3.2.4).

3.9 Tagged Types and Type Extensions

1  [ Tagged types and type extensions support object-oriented programming, based on inheritance with extension and run-time polymorphism via dispatching operations. ]

Language Design Principles

1.a/2  
{AI95-00251-01} The intended implementation model is for the static portion of a tag to be represented as a pointer to a statically allocated and link-time initialized type descriptor. The type descriptor contains the address of the code for each primitive operation of the type. It probably also contains other information, such as might make membership tests convenient and efficient. Tags for nested type extensions must also have a dynamic part that identifies the particular elaboration of the type.

1.b  
The primitive operations of a tagged type are known at its first freezing point; the type descriptor is laid out at that point. It contains linker symbols for each primitive operation; the linker fills in the actual addresses.

1.b.1/2  
{AI95-00251-01} Primitive operations of type extensions that are declared at a level deeper than the level of the ultimate ancestor from which they are derived can be represented by wrappers that use the dynamic part of the tag to call the actual primitive operation. The dynamic part would generally be some way to represent the static link or display necessary for making a nested call. One implementation strategy would be to store that information in the extension part of such nested type extensions, and use the dynamic part of the tag to point at it. (That way, the "dynamic" part of the tag could be static, at the cost of indirect access.)

1.b.2/2  
{AI95-00251-01} If the tagged type is descended from any interface types, it also will need to include “subtags” (one for each interface) that describe the mapping of the primitive operations of the interface to the primitives of the type. These subtags could directly reference the primitive operations (for faster performance), or simply provide the tag “slot” numbers for the primitive operations (for easier derivation). In either case, the subtags would be used for calls that dispatch through a class-wide type of the interface.

1.c  
The rules ensure that “dangling dispatching” is impossible; that is, when a dispatching call is made, there is always a body to execute. This is different from some other object-oriented languages, such as Smalltalk, where it is possible to get a run-time error from a missing method.

1.d  
Other implementation models are possible.

1.e/2  
{AI95-00251-01} Dispatching calls should be efficient, and should have a bounded worst-case execution time. This is important in a language intended for real-time applications. In the intended implementation model, a dispatching call involves calling indirect through the appropriate slot in the dispatch table. No complicated "method lookup" is involved although a call which is dispatching on an interface may require a lookup of the appropriate interface subtag.

1.f  
The programmer should have the choice at each call site of a dispatching operation whether to do a dispatching call or a statically determined call (i.e. whether the body executed should be determined at run time or at compile time).
When deriving from a tagged type, as an alternative to using a view of a derived type for any derived type, additional primitive subprograms may be defined, and inherited from the parent or progenitor of some other tagged type. A record extension is defined by a derived_type_definition with a record_extension_part. A private extension, which is a partial view of a record extension, can be declared in the visible part of a package (see 7.3) or in a generic formal part (see 12.5.1).

The visibility rules determine what is legal at compile time; they have nothing to do with what bodies can be executed at run time. Thus, it is possible to dispatch to a subprogram whose declaration is not visible at the call site. In fact, this is one of the primary facts that gives object-oriented programming its power. The subprogram that ends up being dispatched to by a given call might even be designed long after the call site has been coded and compiled.

Given that Ada has overloading, determining whether a given subprogram overrides another is based on both the types and the names of the operations.

{AI95-00401-01} When a type extension is declared, if there is any place within its immediate scope where a certain subprogram of the parent or progenitor is visible, then a matching subprogram should override. If there is no such place, then a matching subprogram should be totally unrelated, and occupy a different slot in the type descriptor. This is important to preserve the privacy of private parts; when an operation declared in a private part is inherited, the inherited version can be overridden only in that private part, in the package body, and in any children of the package.

If an implementation shares code for instances of generic bodies, it should be allowed to share type descriptors of tagged types declared in the generic body, so long as they are not extensions of types declared in the specification of the generic unit.

**Static Semantics**

{AI95-00345-01} A record type or private type that has the reserved word tagged in its declaration is called a tagged type. In addition, an interface type is a tagged type, as is a task or protected type derived from an interface (see 3.9.4). [When deriving from a tagged type, additional components may be defined. As for any derived type, additional primitive subprograms may be defined, and inherited primitive subprograms may be overridden.] The derived type is called an extension of its ancestor type, or simply a type extension. Every type extension is also a tagged type, and is either a record extension or a private extension of some other tagged type. A record extension is defined by a derived_type_definition with a record_extension_part. A private extension, which is a partial view of a record extension, can be declared in the visible part of a package (see 7.3) or in a generic formal part (see 12.5.1).

{AI95-00345-01} Every type extension is also a tagged type, and is a record extension or a private extension of some other tagged type, or a noninterface synchronized tagged type (see 3.9.4). A record extension is defined by a derived_type_definition with a record_extension_part (see 3.9.1), which may include the definition of additional components. A private extension, which is a partial view of a record extension or of a synchronized tagged type, can be declared in the visible part of a package (see 7.3) or in a generic formal part (see 12.5.1).

**Term entry: tagged type** — type whose objects each have a run-time type tag, which indicates the specific type for which the object was originally created.

**Note:** Tagged types can be extended with additional components.

**Ramification:** {AI95-00218-03} If a tagged type is declared other than in a package_specification, it is impossible to add new primitive subprograms for that type, although it can inherit primitive subprograms, and those can be overridden. If the user incorrectly thinks a certain subprogram is primitive when it is not, and tries to call it with a dispatching call, an error message will be given at the call site. Similarly, by using an overriding_indicator (see 6.1), the user can declare that a subprogram is intended to be overriding, and get an error message when they made a mistake. The use of overriding indicators is highly recommended in new code that does not need to be compatible with Ada 95.

{AI95-00344-01} Note that the accessibility rules imply that a tagged type declared in a library package_specification cannot be extended in a nested subprogram or task body.

An object of a tagged type has an associated (run-time) tag that identifies the specific tagged type used to create the object originally. [The tag of an operand of a class-wide tagged type TClass controls which subprogram body is to be executed when a primitive subprogram of type T is applied to the operand (see 3.9.2); using a tag to control which body to execute is called dispatching.]
The tag of a specific tagged type identifies the full_type_declaration of the type, and for a type extension, is sufficient to uniquely identify the type among all descendants of the same ancestor. If a declaration for a tagged type occurs within a generic_package_declaration, then the corresponding type declarations in distinct instances of the generic package are associated with distinct tags. For a tagged type that is local to a generic package body and with all of its ancestors (if any) also local to the generic body, the language does not specify whether repeated instantiations of the generic body result in distinct tags.

Implementation Note: In most cases, a tag need only identify a particular tagged type declaration, and can therefore be a simple link-time-known address. However, for tag checks (see 3.9.2) it is essential that each descendant (that currently exists) of a given type have a unique tag. Hence, for types declared in shared generic bodies where an ancestor comes from outside the generic, or for types declared at a deeper level than an ancestor, the tag needs to be augmented with some kind of dynamic descriptor (which may be a static link, global display, instance descriptor pointer, or combination). This implies that type Tag may need to be two words, the second of which is normally null, but in these identified special cases needs to include a static link or equivalent. Within an object of one of these types with a two-word tag, the two parts of the tag would typically be separated, one part as the first word of the object, the second placed in the first extension part that corresponds to a type declared more nested than its parent or declared in a shared generic body when the parent is declared outside. Alternatively, by using an extra level of indirection, the type Tag could remain a single-word.

To be honest: The wording “is sufficient to uniquely identify the type among all descendants of the same ancestor” only applies to types that currently exist. It is not necessary to distinguish between descendants that currently exist, and descendants of the same type that no longer exist. For instance, the address of the stack frame of the object, the second placed in the first extension part that corresponds to a type declared more nested than its parent or declared in a shared generic body when the parent is declared outside. Alternatively, by using an extra level of indirection, the type Tag could remain a single-word.

The following language-defined library package exists:

```ada
package Ada.Tags is
  type Tag is private,
    withpragma Preelaborate, Nonblocking, Global => in out synchronized is(Tag);

  No_Tag : constant Tag;

  function Expanded_Name(T : Tag) return String;
  function Wide_Expanded_Name(T : Tag) return Wide_String;
  function Internal_Tag(T : Tag) return String;
  function External_Tag(External : String; T : Tag) return Tag;

  function Descendant_Tag(External : String; Ancestor : Tag) return Tag;
  function Is_Descendant_At_Same_Level(Descendant, Ancestor : Tag) return Boolean;
  function Parent_Tag (T : Tag) return Tag;
  function Tag_Array is array (Positive range <>) of Tag;
  function Interface_Ancestor_Tags (T : Tag) return Tag_Array;
  function Is_Abstract (T : Tag) return Boolean;

  Tag_Error : exception;
private
  ... -- not specified by the language
end Ada.Tags;
```

3.9 Tagged Types and Type Extensions
Reason: Tag is a nonlimited, definite subtype, because it needs the equality operators, so that tag checking makes sense. Also, equality, assignment, and object declaration are all useful capabilities for this subtype.

For an object X and a type T, “X'Tag = T'Tag” is not needed, because a membership test can be used. However, comparing the tags of two objects cannot be done via membership. This is one reason to allow equality for type Tag.

{AI95-00260-02} No_Tag is the default initial value of type Tag.

Reason: {AI95-00260-02} This is similar to the requirement that all access values be initialized to null.

{AI95-00400-01} The function Wide_Wide_Expanded_Name returns the full expanded name of the first subtype of the specific type identified by the tag, in upper case, starting with a root library unit. The result is implementation defined if the type is declared within an unnamed block_statement.

To be honest: This name, as well as each prefix of it, does not denote a renaming_declaration.

Implementation defined: The result of Tags.Wide_Wide_Expanded_Name for types declared within an unnamed block_statement.

{AI95-00400-01} The function Expanded_Name (respectively, Wide_Expanded_Name) returns the same sequence of graphic characters as that defined for Wide_Wide_Expanded_Name, if all the graphic characters are defined in Character (respectively, Wide_Character); otherwise, the sequence of characters is implementation defined, but no shorter than that returned by Wide_Wide_Expanded_Name for the same value of the argument.

Implementation defined: The sequence of characters of the value returned by Tags.Expanded_Name (respectively, Tags.Wide_Expanded_Name) when some of the graphic characters of Tags.Wide_Wide_Expanded_Name are not defined in Character (respectively, Wide_Character).

The function External_Tag returns a string to be used in an external representation for the given tag. The call External_Tag(S’Tag) is equivalent to the attribute_reference of External_Tag (see 13.3).

Reason: It might seem redundant to provide both the function External_Tag and the attribute External_Tag. The function is needed because the attribute can't be applied to values of type Tag. The attribute is needed so that it can be specified via an attribute_definition_clause.

{AI95-00417-01} The string returned by the functions Expanded_Name, Wide_Expanded_Name, Wide_Wide_Expanded_Name, and External_Tag has lower bound 1.

{AI95-00279-01} The function Internal_Tag returns the (internal) tag for the type that corresponds to the given external tag, or raises Tag_Error if the given string is not the external tag for any specific type of the partition. Tag_Error is also raised if the specific type identified is a library-level type whose tag has not yet been created (see 13.14).

Reason: {AI95-00279-01} {AI05-0005-1} The check for uncreated library-level types prevents a reference to the type before execution reaches the freezing point of the type. This is important so that TClass'Input or an instance of Tags.Generic_Dispatching_Constructor do not try to create an object of a type that hasn't been frozen (which might not have yet elaborated its constraints). We don't require this behavior for non-library-level types as the tag can be created multiple times and possibly multiple copies can exist at the same time, making the check complex.

{AI95-00344-01} {AI05-0113-1} The function Descendant_Tag returns the (internal) tag for the type that corresponds to the given external tag and is both a descendant of the type identified by the Ancestor tag and has the same accessibility level as the identified ancestor. Tag_Error is raised if External is not the external tag for such a type. Tag_Error is also raised if the specific type identified is a library-level type whose tag has not yet been created, or if the given external tag identifies more than one type that has the appropriate Ancestor and accessibility level.

Reason: Descendant_Tag is used by TClass'Input to identify the type identified by an external tag. Because there can be multiple elaborations of a given type declaration, Internal_Tag does not have enough information to choose a unique such type. Descendant_Tag does not return the tag for types declared at deeper accessibility levels than the ancestor because there could be ambiguity in the presence of recursion or multiple tasks. Descendant_Tag can be used in constructing a user-defined replacement for TClass’Input.
Rules for specifying external tags will usually prevent an external tag from identifying more than one type. However, an external tag can identify multiple types if a generic body contains a derivation of a tagged type declared outside of the generic, and there are multiple instances at the same accessibility level as the type. (The Reference Manual allows default external tags to not be unique in this case.)

The function Is_Descendant_At_Same_Level returns True if the Descendant tag identifies a type that is both a descendant of the type identified by Ancestor and at the same accessibility level. If not, it returns False.

Reason: Is_Descendant_At_Same_Level (or something similar to it) is used by T'Class'Output to determine whether the item being written is at the same accessibility level as T. It may be used to determine prior to using T'Class'Output whether Tag_Error will be raised, and also can be used in constructing a user-defined replacement for T'Class'Output.

For the purposes of the dynamic semantics of functions Descendant_Tag and Is_Descendant_At_Same_Level, a tagged type T2 is a descendant of a type T1 if it is the same as T1, or if its parent type or one of its progenitor types is a descendant of type T1 by this rule, even if at the point of the declaration of T2, one of the derivations in the chain is not visible.

Discussion: In other contexts, “descendant” is dependent on visibility, and the particular view a derived type has of its parent type. See 7.3.1.

The function Parent_Tag returns the tag of the parent type of the type whose tag is T. If the type does not have a parent type (that is, it was not defined by a derived_type_definition), then No_Tag is returned.

Ramification: The parent type is always the parent of the full type; a private extension appears to define a parent type, but it does not (only the various forms of derivation do that). As this is a run-time operation, ignoring privateness is OK.

The function Interface_Ancestor_Tags returns an array containing the tag of each interface ancestor type of the type whose tag is T, other than T itself. The lower bound of the returned array is 1, and the order of the returned tags is unspecified. Each tag appears in the result exactly once. If the type whose tag is T has no interface ancestors, a null array is returned.

Ramification: The result of Interface_Ancestor_Tags includes the tag of the parent type, if the parent is an interface.

Indirect interface ancestors are included in the result of Interface_Ancestor_Tags. That's because where an interface appears in the derivation tree has no effect on the semantics of the type; the only interesting property is whether the type has an interface as an ancestor.

The function Is_Abstract returns True if the type whose tag is T is abstract, and False otherwise.

For every subtype S of a tagged type T (specific or class-wide), the following attributes are defined:

S'Class denotes a subtype of the class-wide type (called TClass in this document) for the class rooted at T (or if S already denotes a class-wide subtype, then S'Class is the same as S).

S'Class is unconstrained. However, if S is constrained, then the values of S'Class are only those that when converted to the type T belong to S.

Ramification: This attribute is defined for both specific and class-wide subtypes. The definition is such that S'Class is the same as S'Class.

Note that if S is constrained, S'Class is only partially constrained, since there might be additional discriminants added in descendants of T which are not constrained.

Reason: The Class attribute is not defined for untagged subtypes (except for incomplete types and private types whose full view is tagged — see 11.2 and 7.3.1) so as to preclude implicit conversion in the absence of run-time type information. If it were defined for untagged subtypes, it would correspond to the concept of universal types provided for the predefined numeric classes.

S'Tag denotes the tag of the type T (or if T is class-wide, the tag of the root type of the corresponding class). The value of this attribute is of type Tag.

Reason: S'Class'Tag equals S'Tag, to avoid generic contract model problems when S'Class is the actual type associated with a generic formal derived type.
Given a prefix \(X\) that is of a class-wide tagged type \((\text{after any implicit dereference})\), the following attribute is defined:

\[X'\text{Tag}\]

\(X'\text{Tag}\) denotes the tag of \(X\). The value of this attribute is of type Tag.

**Reason:** \(X'\text{Tag}\) is not defined if \(X\) is of a specific type. This is primarily to avoid confusion that might result about whether the \(Tag\) attribute should reflect the tag of the type of \(X\), or the tag of \(X\). No such confusion is possible if \(X\) is of a class-wide type.

\{AI95-00260-02\} \{AI95-00441-01\} The following language-defined generic function exists:

\begin{verbatim}
generic
  type \(T\) (<>)
    is abstract tagged limited private;
  type Parameters (<>)
    is limited private;
  with function Constructor (Params : not null access Parameters)
    return \(T\)
    is abstract;

function Ada.Tags.Generic_Dispatching_Constructor
  (The_Tag : Tag;
   Params : not null access Parameters) return \(T'\text{Class}\)
  with Preelaborate, Convention => Intrinsic,
      Nonblocking, Global => in out synchronized;
pragma Preelaborate(Generic_Dispatching_Constructor);
pragma Convention(Intrinsic, Generic_Dispatching_Constructor);
\end{verbatim}

\{AI95-00260-02\} Tags.Generic_Dispatching_Constructor provides a mechanism to create an object of an appropriate type from just a tag value. The function Constructor is expected to create the object given a reference to an object of type Parameters.

**Discussion:** This specification is designed to make it easy to create dispatching constructors for streams; in particular, this can be used to construct overridings for \(T'\text{Class}'\text{Input}\).

\{AI12-0005-1\} Note that almost any tagged type can be used in an instance of Generic_Dispatching_Constructor. Using a tagged incomplete view or a tagged partial view before the completion of the type in such an instance would be illegal; all other tagged types can be used in an instance of Generic_Dispatching_Constructor will match \(T\) (see 12.5.1).

**Dynamic Semantics**

The tag associated with an object of a tagged type is determined as follows:

- The tag of a stand-alone object, a component, or an aggregate of a specific tagged type \(T\) identifies \(T\).

  **Discussion:** The tag of a formal parameter of type \(T\) is not necessarily the tag of \(T\), if, for example, the actual was a type conversion.

- \{AI12-0437-1\} The tag of an object created by an allocator for an access type with a specific designated tagged type \(T\) identifies \(T\).

  **Discussion:** The tag of an object designated by a value of such an access type might not be \(T\), if, for example, the access value is the result of a type conversion.

- The tag of an object of a class-wide tagged type is that of its initialization expression.

  **Ramification:** The tag of an object (even a class-wide one) cannot be changed after it is initialized, since a “class-wide” assignment statement raises Constraint_Error if the tags don't match, and a “specific” assignment statement does not affect the tag.

- The tag of the result returned by a function whose result type is a specific tagged type \(T\) identifies \(T\).

  **Implementation Note:** \{AI95-00318-02\} For a limited tagged type, the return object is “built in place” in the ultimate result object with the appropriate tag. This requires a runtime check for limited tagged types, since they are returned “by-reference”. For a nonlimited type, a new anonymous object with the appropriate tag is created as part of the function return, and then assigned the value of the return expression. See 6.5, “Return Statements”.

- \{AI95-00318-02\} The tag of the result returned by a function with a class-wide result type is that of the return object expression.
The tag is preserved by type conversion and by parameter passing. The tag of a value is the tag of the associated object (see 26.2).

An instance of Tags.Generic_Dispatching_Constructor raises Tag_Error if The_Tag does not represent a concrete descendant of T or if the innermost master (see 7.6.1) of this descendant is not also a master of the instance. Otherwise, it dispatches to the primitive function denoted by the formal Constructor for the type identified by The_Tag, passing Params, and returns the result. Any exception raised by the function is propagated.

Ramification: The tag check checks both that The_Tag is in T'Class, and that it is not abstract. These checks are similar to the ones required by streams for T'Class'Input (see 13.13.2). In addition, there is a check that the tag identifies a type declared on the current dynamic call chain, and not a more nested type or a type declared by another task. This check is not necessary for streams, because the stream attributes are declared at the same dynamic level as the type used.

Erroneous Execution

If an internal tag provided to an instance of Tags.Generic_Dispatching_Constructor or to any subprogram declared in package Tags identifies either a type that is not library-level and whose tag has not been created (see 13.14), or a type that does not exist in the partition at the time of the call, then execution is erroneous.

Ramification: One reason that a type might not exist in the partition is that the tag refers to a type whose declaration was elaborated as part of an execution of a subprogram_body which has been left (see 7.6.1).

We exclude tags of library-level types from the current execution of the partition, because misuse of such tags should always be detected. T'Tag freezes the type (and thus creates the tag), and Internal_Tag and Descendant_Tag cannot return the tag of a library-level type that has not been created. All ancestors of a tagged type must be frozen no later than the (full) declaration of a type that uses them, so Parent_Tag and Interface_Ancestor_Tags cannot return a tag that has not been created. Finally, library-level types never cease to exist while the partition is executing. Thus, if the tag comes from a library-level type, there cannot be erroneous execution (the use of Descendant_Tag rather than Internal_Tag can help ensure that the tag is of a library-level type). This is also similar to the rules for T'Class'Input (see 13.13.2).

Discussion: Ada 95 allowed Tag_Error in this case, or expected the functions to work. This worked because most implementations used tags constructed at link-time, and each elaboration of the same type declaration produced the same tag. However, Ada 2005 requires at least part of the tags to be dynamically constructed for a type derived from a type at a shallower level. For dynamically constructed tags, detecting the error can be expensive and unreliable. To see this, consider a program containing two tasks. Task A creates a nested tagged type, passes the tag to task B (which saves it), and then terminates. The nested tag (if dynamic) probably will need to refer in some way to the stack frame for task A. If task B later tries to use the tag created by task A, the tag's reference to the stack frame of A probably is a dangling pointer. Avoiding this would require some sort of protected tag manager, which would be a bottleneck in a program's performance. Moreover, we'd still have a race condition: if task A terminated after the tag check, but before the tag was used, we'd still have a problem. That means that all of these operations would have to be serialized. That could be a significant performance drain, whether or not nested tagged types are ever used. Therefore, we allow execution to become erroneous as we do for other dangling pointers. If the implementation can detect the error, we recommend that Tag_Error be raised.

Implementation Permissions

The implementation of Internal_Tag and Descendant_Tag may raise Tag_Error if no specific type corresponding to the string External_Tag passed as a parameter exists in the partition at the time the function is called, or if there is no such type whose innermost master is a master of the point of the function call.

Reason: Locking would be required to ensure that the mapping of strings to tags never returned tags of types which no longer exist, because types can cease to exist (because they
In most implementations, repeated elaborations of the same objects of a class-wide type are illegal unless they belong to another task, as described above) during the execution of these operations. Moreover, even if these functions did use locking, that would not prevent the type from ceasing to exist at the instant that the function returned. Thus, we do not require the overhead of locking. In most implementations, repeated elaborations of the same type_declaration will all produce the same tag. In such an implementation, Tag_Error will be raised in cases where the internal or external tag was passed from a different partition. However, some implementations might create a new tag value at runtime for each elaboration of a type_declaration. In that case, Tag_Error could also be raised if the created type no longer exists because the subprogram containing it has returned, for example. We don't require the latter behavior, hence the word “may” in this rule.

**Implementation Advice**

{AI95-00260-02} {AI05-0113-1} Internal Tag should return the tag of a type, if one exists, whose innermost master is the master of the point of the function call.

**Implementation Advice:** Tags.Internal_Tag should return the tag of a type, if one exists, whose innermost master is the master of the point of the function call.

**Reason:** {AI95-00260-02} {AI95-00344-01} It's not helpful if Internal_Tag returns the tag of some type in another task when one is available in the task that made the call. We don't require this behavior (because it requires the same implementation techniques we decided not to insist on previously), but encourage it.

**Discussion:** {AI05-0113-1} There is no Advice for the result of Internal_Tag if no such type exists. In most cases, the Implementation Permission can be used to raise Tag_Error, but some other tag can be returned as well.

**NOTE 1** {AI12-0442-1} A type declared with the reserved word tagged is normally declared in a package_specification, so that new primitive subprograms can be declared for it.

**NOTE 2** Once an object has been created, its tag never changes.

**NOTE 3** {AI12-0447-1} Class-wide types are defined to have unknown discriminants (see 3.7). This means that, by the rules in 3.7 for objects with unknown discriminants, objects of a class-wide type are illegal unless they are explicitly initialized (whether created by an object_declaration or an allocator), and that aggregates are illegal unless they are explicitly qualified with a specific type when their expected type is class-wide.

**NOTE 4** {AI95-00260-02} {AI95-00326-01} The capability provided by Tags.GenericDispatchingConstructor is sometimes known as a factory. If S denotes an untagged private type whose full type is tagged, then S.Class is also allowed before the full type definition, but only in the private part of the package in which the type is declared (see 7.3.1). Similarly, the Class attribute is defined for incomplete types whose full type is tagged, but only within the library unit in which the incomplete type is declared (see 3.10.1).

**Examples**

**Examples of tagged record types:**

```ada
package_specification

type Point is tagged record
  X, Y : Real := 0.0;
end record;

type Expression is tagged null record;
-- Components will be added by each extension
```

**Extensions to Ada 83**

Tagged types are a new concept.

**Inconsistencies With Ada 95**

{AI95-00279-01} **Amendment Correction:** Added wording specifying that Internal_Tag must raise Tag_Error if the tag of a library-level type has not yet been created. Ada 95 gave an Implementation Permission to do this; we require it to avoid erroneous execution when streaming in an object of a library-level type that has not yet been elaborated. This is technically inconsistent; a program that used Internal_Tag outside of streaming and used a compiler that didn't take advantage of the Implementation Permission would not have raised Tag_Error, and may have returned a useful tag. (If the tag was used in streaming, the program would have been erroneous.) Since such a program would not have been portable to a compiler that did take advantage of the Implementation Permission, this is not a significant inconsistency.

{AI95-00417-01} We now define the lower bound of the string returned from [[Wide]]Wide_Expanded_Name and External_Name. This makes working with the returned string easier, and is consistent with many other string-returning functions in Ada. This is technically an inconsistency; if a program depended on some other lower bound for the string returned from one of these functions, it could fail when compiled with Ada 2005. Such code is not portable even between Ada 95 implementations, so it should be very rare.
3.9 Tagged Types and Type Extensions

Incompatibilities With Ada 95

Constant No_Tag, and functions Parent_Tag, Interface_Ancestor_Tags, Descendant_Tag, Is_Descendant_At_Same_Level, Wide_Expanded_Name, and Wide_Wide_Expanded_Name are newly added to Ada.Tags. If Ada.Tags is referenced in a use_clause, and an entity \( E \) with the same defining_identifier as a new entity in Ada.Tags is defined in a package that is also referenced in a use_clause, the entity \( E \) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 95

Ada.Tags is now defined to be preelaborated.

Generic function Tags.Generic_Dispatching_Constructor is new.

Wording Changes from Ada 95

We talk about return objects rather than return expressions, as functions can return using an extended_return_statement.

Inconsistencies With Ada 2005

Correction: Added wording specifying that Dependent_Tag must raise Tag_Error if there is more than one type which matches the requirements. If an implementation had returned a random tag of the matching types, a program may have worked properly. However, such a program would not be portable (another implementation may return a different tag) and the conditions that would cause the problem are unlikely (most likely, a tagged type extension declared in a generic body with multiple instances in the same scope).

Incompatibilities With Ada 2005

Function Is_Abstract is added to Ada.Tags. If Ada.Tags is referenced in a use_clause, and an entity \( E \) with the defining_identifier Is_Abstract is defined in a package that is also referenced in a use_clause, the entity \( E \) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Wording Changes from Ada 2005

We explicitly define the meaning of "descendant" at runtime, so that it does not depend on visibility as does the usual meaning.

3.9.1 Type Extensions

Every type extension is a tagged type, and is either a record extension or a private extension of some other tagged type, or a noninterface synchronized tagged type.

Language Design Principles

We want to make sure that we can extend a generic formal tagged type, without knowing its discriminants.

We don't want to allow components in an extension aggregate to depend on discriminants inherited from the parent value, since such dependence requires staticness in aggregates, at least for variants.

Syntax

record_extension_part ::= with record_definition

Legality Rules

The parent type of a record extension shall not be a class-wide type nor shall it be a synchronized tagged type (see 3.9.4). If the parent type or any progenitor is nonlimited, then each of the components of the record_extension_part shall be nonlimited. The accessibility level (see 3.10.2) of a record extension shall not be statically deeper than that of its parent.
**type**. In addition to the places where Legality Rules normally apply (see 12.3), these rules apply also in the private part of an instance of a generic unit.

**Reason:** If the parent is a limited formal type, then the actual might be nonlimited.

{AI95-00344-01} Ada 95 required the record extensions to be the same level as the parent type. Now we use accessibility checks on class-wide allocators and return statements to prevent objects from living longer than their type. A similar accessibility rule is not needed for private extensions, because in a package, the rule will apply to the full_type_declaration, and for a generic private formal extension, the actual is all that matters.

{AI95-00345-01} Synchronized tagged types cannot be extended. We have this limitation so that all of the data of a task or protected type is defined within the type. Data defined outside of the type wouldn't be subject to the mutual exclusion properties of a protected type, and couldn't be used by a task, and thus doesn't seem to be worth the potential impact on implementations.

{AI95-00344-01} Within the body of a generic unit, or the body of any of its descendant library units, a tagged type—A type extension shall not be declared as a descendant of a formal type declared within the formal part of the generic unit in a generic body if the parent type is declared outside that body.

**Reason:** This paragraph ensures that a dispatching call will never attempt to execute an inaccessible subprogram body.

{AI95-00344-01} The convoluted wording (“formal type declared within the formal part”) is necessary to include tagged types that are formal parameters of formal packages of the generic unit, as well as formal tagged and tagged formal derived types of the generic unit.

{AI95-00344-01} This rule is necessary in order to preserve the contract model.

{AI95-0005-1} [AI95-00344-01] If an ancestor of a generic unit can be instantiated at a deeper accessibility level than the generic unit, it is necessary to prevent type extensions whose parent is declared outside the generic unit. The same is true if the parent is a formal of the generic unit, we have a problem. If the parent is declared in the generic_declaration (but is not a formal), we don't run afoul of the accessibility rules, because we know that the instance declaration and body will be at the same accessibility level. However, we still have a problem in that case, because it might have an unknown number of abstract subprograms that require overriding, as in the following example:

```ada
define a package P is
type T is tagged null record;
function F return T; -- Inherited versions will require overriding be abstract.
end P;

generic
  type TT is tagged private;
package Gp is
  type NT is abstract new TT with null record;
  procedure Q(X : in NT) is abstract;
end Gp;

package body Gp is
  type NT2 is new NT with null record; -- Illegal!
  procedure Q(X : in NT2) is begin null; end Q;
  -- Is this legal or not? Can't decide because
  -- we don't know whether TT had any functions that require abstract
  -- overriding on extension.
end Gp;

package I is new Gp(TT => P.T);
```

I. NT is an abstract type with two abstract subprograms: F (inherited as abstract) and Q (explicitly declared as abstract). But the generic body doesn't know about F, so we don't know that it needs to be overridden to make a nonabstract extension of NT. Furthermore, a formal tagged limited private type can be extended with limited components, but the actual might not be limited, which would allow assignment of limited types, which is bad. Hence, we have to disallow this case as well.

Similarly, since the actual type for a formal tagged limited private type can be a nonlimited type, we would have a problem if a type extension of a limited formal private type could be declared in a generic body. Such an extension could have a task component, for example, and an object of that type could be passed to a dispatching operation of a nonlimited ancestor type. That operation could try to copy the object with the task component. That would be bad. So we disallow this as well.

If TT were declared as abstract, then we could have the same problem with abstract procedures.

We considered disallowing all tagged types in a generic body, for simplicity. We decided not to go that far, in order to avoid unnecessary restrictions.
We also considered trying make the accessibility level part of the contract; i.e. invent some way of saying (in the generic_declaration) “all instances of this generic unit will have the same accessibility level as the generic_declaration”. Unfortunately, that doesn't solve the part of the problem having to do with abstract types.

**Ramification:** {AI95-00391-01} This rule applies to types with ancestors (directly or indirectly) of formal interface types (see 12.5.1), formal tagged private types (see 12.5.1), and formal derived private types whose ancestor type is tagged (see 12.5.1).

**Static Semantics**

### 4.1/2

**AI95-00391-01** A record extension is a null extension if its declaration has no known_discriminant_part and its record_extension_part includes no component_declarations.

### 4.2/5

**AI12-0191-1** In the case where (the compile-time) view of an object X is of a tagged type T1 or T1'Class and the (run-time) tag of X is T2'Tag, only the components (if any) of X that are components of T1 (or that are discriminants which correspond to a discriminant of T1) are said to be components of the nominal type of X. Similarly, only parts (respectively, subcomponents) of T1 are parts (respectively, subcomponents) of the nominal type of X.

**Ramification:** {AI12-0191-1} For example, if T2 is an undiscriminated extension of T1 which declares a component named Comp, then X.Comp is not a component of the nominal type of X.

**Discussion:** {AI12-0191-1} For example, there is a Dynamic Semantics rule that finalization of an object includes finalization of its components (see 7.6.1). In the following case:

```
type T1 is tagged null record;
type T2 is new T1 with record;
end record;
function Func return T1'Class is (T2'others => <>);
X: T1'Class := Func;
```

the rule that “every component of the object is finalized” (as opposed to something like “every component of the nominal type of the object is finalized”) means that the finalization of X will include finalization of X.Comp. For another example, see the rule about accessibility checking of access discriminants of parts of function results in 6.5. In contrast, the rules in 7.3.2 explicitly state that type invariant checks are only performed for parts which are of the type-invariant bearing type and which are parts of the nominal type of the object (as opposed to for all parts, whether part of the nominal type or not, which are of the invariant-bearing type). Similarly, the rule in 13.13.2 governing which components of a composite value are read and written by the default implementations of Read and Write for a composite type states that only the components of the object which are components of the nominal type of the object are read or written.

**Dynamic Semantics**

The elaboration of a record_extension_part consists of the elaboration of the record_definition.

**NOTE 1** The term “type extension” refers to a type as a whole. The term “extension part” refers to the piece of text that defines the additional components (if any) the type extension has relative to its specified ancestor type.

Discussion: We considered other terminology, such as “extended type”. However, the terms “private extended type” and “record extended type” did not convey the proper meaning. Hence, we have chosen to uniformly use the term “extension” as the type resulting from extending a type, with “private extension” being one produced by privately extending the type, and “record extension” being one produced by extending the type with an additional record-like set of components. Note also that the term “type extension” refers to the result of extending a type in the language Oberon as well (though there the term “extended type” is also used, interchangeably, perhaps because Oberon doesn't have the concept of a “private extension”).

**NOTE 2** {AI95-00344-01} The accessibility rules imply that a tagged type declared in a library package_specification can be extended only at library level or as a generic formal. When an extension is declared immediately within a body/package_body, primitive subprograms are inherited and are overridable, but new primitive subprograms cannot be added.

**NOTE 3** {AI12-0447-1} By the rules given in 3.8, a name that denotes a component (including a discriminant) of the parent type is illegal if it is allowed within the record_extension_part. Similarly, a name that denotes a component defined within the record_extension_part is illegal if it is allowed within the record_extension_part. All is permissible to use a name that denotes a discriminant of the record extension is legal, providing that it refers to a discriminant defined in there is a new known_discriminant_part in the enclosing type declaration. (The full rule is given in 3.8.)
Reason: The restriction against depending on discriminants of the parent is to simplify the definition of extension aggregates. The restriction against using parent components in other ways is methodological; it presumably simplifies implementation as well.

NOTE 4 {AI12-0447-1} By the rules given in 8.3, each visible component of a record extension will have a unique name, whether the component is (visibly) inherited from the parent type or declared in the record_extension_part (see 8.3).

Examples of record extensions (of types defined above in 3.9):

```ada
type Painted_Point is new Point with record
  Paint : Color := White;
end record;
-- Components X and Y are inherited
Origin : constant Painted_Point := (X | Y => 0.0, Paint => Black);
type Literal is new Expression with record
  Value : Real;
end record;

{AI12-0404-1} type Expr_Ptr is access all Expression'Class;
-- see 3.9.4.10

type Binary_Operation is new Expression with record
  -- an internal node in an Expression tree
  Left, Right : Expr_Ptr;
end record;
type Addition is new Binary_Operation with null record;
type Subtraction is new Binary_Operation with null record;
-- No additional components needed for these extensions

Tree : Expr_Ptr := -- A tree representation of "5.0 + (13.0–7.0)"
  new Addition'(
    Left => new Literal'(Value => 5.0),
    Right => new Subtraction'(
      Left => new Literal'(Value => 13.0),
      Right => new Literal'(Value => 7.0)));
```

Extensions to Ada 83

Type extension is a new concept.

Extensions to Ada 95

{AI95-00344-01} Type extensions now can be declared in more nested scopes than their parent types. Additional accessibility checks on allocators and return statements prevent objects from outliving their type.

Wording Changes from Ada 95

{AI95-00345-01} Added wording to prevent extending synchronized tagged types.
{AI95-00391-01} Defined null extension for use elsewhere.

Wording Changes from Ada 2012

{AI12-0191-1} Defined the term “components of the nominal type” to remove a confusion as to how components are described in Dynamic Semantics rules.

3.9.2 Dispatching Operations of Tagged Types

{AI95-00260-02} {AI95-00335-01} {AI12-0342-1} {AI12-0419-1} The primitive subprograms of a tagged type, the subprograms declared by formal abstract subprogram declarations, the Put_Image attribute (see 4.10) of a specific tagged type, and the stream attributes of a specific tagged type that are available (see 13.13.2) at the end of the declaration list where the type is declared are called dispatching...
operations. [A dispatching operation can be called using a statically determined controlling tag, in which case the body to be executed is determined at compile time. Alternatively, the controlling tag can be dynamically determined, in which case the call dispatches to a body that is determined at run time:] such a call is termed a dispatching call. [As explained below, the properties of the operands and the context of a particular call on a dispatching operation determine how the controlling tag is determined, and hence whether or not the call is a dispatching call. Run-time polymorphism is achieved when a dispatching operation is called by a dispatching call.]

**Reason:** {AI95-00335-01} For the stream attributes of a type declared immediately within a package specification that has a partial view, the declaration list to consider is the visible part of the package. Stream attributes that are not available in the same declaration list are not dispatching as there is no guarantee that descendants of the type have available attributes (there is such a guarantee for visibly available attributes). If we allowed dispatching for any available attribute, then for attributes defined in the private part we could end up executing a nonexistent body.

**Language Design Principles**

1.a

The controlling tag determination rules are analogous to the overload resolution rules, except they deal with run-time type identification (tags) rather than compile-time type resolution. As with overload resolution, controlling tag determination may depend on operands or result context.

**Static Semantics**

{AI95-00260-02} {AI95-00416-01} {AI05-0076-1} A call on a dispatching operation is a call whose name or prefix denotes the declaration of a primitive subprogram of a tagged type, that is, a dispatching operation. A controlling operand in a call on a dispatching operation of a tagged type T is one whose corresponding formal parameter is of type T or is of an anonymous access type with designated type T; the corresponding formal parameter is called a controlling formal parameter. If the controlling formal parameter is an access parameter, the controlling operand is the object designated by the actual parameter, rather than the actual parameter itself. If the call is to a (primitive) function with result type T (a function with a controlling result), then the call has a controlling result — the context of the call can control the dispatching. Similarly, if the call is to a function with an access result type designating T (a function with a controlling access result), then the call has a controlling access result, and the context can similarly control dispatching.

**Ramification:** This definition implies that a call through the dereference of an access-to-subprogram value is never considered a call on a dispatching operation. Note also that if the prefix denotes a renaming declaration, the place where the renaming occurs determines whether it is primitive; the thing being renamed is irrelevant.

{AI12-0236-1} A name or expression of a tagged type is either statically tagged, dynamically tagged, or tag indeterminate, according to whether, when used as a controlling operand, the tag that controls dispatching is determined statically by the operand's (specific) type, dynamically by its tag at run time, or from context. A qualified expression or parenthesized expression is statically, dynamically, or indeterminately tagged according to its operand. A conditional expression is statically, dynamically, or indeterminately tagged according to rules given in 4.5.7. A declare expression is statically, dynamically, or indeterminately tagged according to its body expression. For other kinds of names and expressions, this is determined as follows:

- {AI95-00416-01} The name or expression is statically tagged if it is of a specific tagged type and, if it is a call with a controlling result or controlling access result, it has at least one statically tagged controlling operand;

  **Discussion:** It is illegal to have both statically tagged and dynamically tagged controlling operands in the same call -- see below.

- {AI95-00416-01} The name or expression is dynamically tagged if it is of a class-wide type, or it is a call with a controlling result or controlling access result and at least one dynamically tagged controlling operand;
• \{AI95-00416-01\} The name or expression is tag indeterminate if it is a call with a controlling result or controlling access result, all of whose controlling operands (if any) are tag indeterminate.

\{8652/0010\} \{AI95-00127-01\} [A type_conversion is statically or dynamically tagged according to whether the type determined by the subtype_mark is specific or class-wide, respectively.] For an object that is designated by an expression whose expected type is an anonymous access-to-specific tagged type, the object is dynamically tagged if the expression, ignoring enclosing parentheses, is of the form X'Access, where X is of a class-wide type, or is of the form new T'(...), where T denotes a class-wide subtype. Otherwise, the object is statically or dynamically tagged according to whether the designated type of the expression of the actual parameter is specific or class-wide, respectively.

Ramification: A type_conversion is never tag indeterminate, even if its operand is. A designated object is never tag indeterminate.

\{8652/0010\} \{AI95-00127-01\} Allocators and access attributes of class-wide types can be used as the controlling parameters of dispatching calls.

Legality Rules

A call on a dispatching operation shall not have both dynamically tagged and statically tagged controlling operands.

Reason: This restriction is intended to minimize confusion between whether the dynamically tagged operands are implicitly converted to, or tag checked against the specific type of the statically tagged operand(s).

\{8652/0010\} \{AI95-00127-01\} If the expected type for an expression or name is some specific tagged type, then the expression or name shall not be dynamically tagged unless it is a controlling operand in a call on a dispatching operation. Similarly, if the expected type for an expression is an anonymous access-to-specific tagged type, then the object designated by the expression shall not be dynamically tagged unless it is expression shall not be of an access-to-class-wide type unless it designates a controlling operand in a call on a dispatching operation.

Reason: This prevents implicit "truncation" of a dynamically-tagged value to the specific type of the target object/formal. An explicit conversion is required to request this truncation.

Ramification: \{AI95-00252-01\} \{AI12-0039-1\} This rule applies to all expressions or names with a specific expected type, not just those that are actual parameters to a dispatching call. This rule does not apply to a membership test whose tested simple_expression expression is class-wide, since any type that covers the tested type is explicitly allowed. See 4.5.2. This rule also doesn't apply to a selected_component whose selector_name is a subprogram, since the rules explicitly say that the prefix may be class-wide (see 4.1.3).

\{8652/0011\} \{AI95-00117-01\} \{AI95-00430-01\} In the declaration of a dispatching operation of a tagged type, everywhere a subtype of the tagged type appears as a subtype of the profile (see 6.1), it shall statically match the first subtype of the tagged type. If the dispatching operation overrides an inherited subprogram, it shall be subtype conformant with the inherited subprogram. The convention of an inherited or overriding dispatching operation is the convention of the corresponding primitive operation of the parent or progenitor type. The default convention of a dispatching operation that overrides an inherited primitive operation is the convention of the inherited operation; if the operation overrides multiple inherited operations, then they shall all have the same convention. An explicitly declared dispatching operation shall not be of convention Intrinsic. If a dispatching operation overrides the predefined equals operator, then it shall be of convention Ada [(either explicitly or by default — see 6.3.1)].

Reason: These rules ensure that constraint checks can be performed by the caller in a dispatching call, and parameter passing conventions match up properly. A special rule on aggregates prevents values of a tagged type from being created that are outside of its first subtype.
3.9.2 Dispatching Operations of Tagged Types

The default_expression for a controlling formal parameter of a dispatching operation shall be tag indeterminate. A controlling formal parameter that is an access parameter shall not have a default_expression.

Reason: The first part ensures that the default_expression always produces the "correct" tag when called with or without dispatching, or when inherited by a descendant. If it were statically tagged, the default would be useless for a dispatching call; if it were dynamically tagged, the default would be useless for a nondispatching call.

The second part is consistent with the first part, since designated objects are never tag indeterminate.

If a dispatching operation is defined by a subprogram_renaming_declaration or the instantiation of a generic subprogram, any access parameter of the renamed subprogram or the generic subprogram that corresponds to a controlling access parameter of the dispatching operation, shall have a subtype that excludes null.

A given subprogram shall not be a dispatching operation of two or more distinct tagged types.

Reason: This restriction minimizes confusion since multiple dispatching is not provided. The normal solution is to replace all but one of the tagged types with their class-wide types.

The explicit declaration of a primitive subprogram of a tagged type shall occur before the type is frozen (see 13.14). [For example, new dispatching operations cannot be added after objects or values of the type exist, nor after deriving a record extension from it, nor after a body.]

Reason: This rule is needed because (1) we don't want people dispatching to things that haven't been declared yet, and (2) we want to allow the static part of tagged type descriptors to be static (allocated statically, and initialized to link-time-known symbols). Suppose T2 inherits primitive P from T1, and then overrides P. Suppose P is called before the declaration of the overriding P. What should it dispatch to? If the answer is the new P, we've violated the first principle above. If the answer is the old P, we've violated the second principle. (A call to the new one necessarily raises Program_Error, but that's beside the point.)

Note that a call upon a dispatching operation of type T will freeze T.

We considered applying this rule to all derived types, for uniformity. However, that would be upward incompatible, so we rejected the idea. As in Ada 83, for an untagged type, the above call upon P will call the old P (which is arguably confusing).

Implementation Note: Because of this rule, the type descriptor can be created (presumably containing linker symbols pointing at the not-yet-compiled bodies) at the first freezing point of the type. It also prevents, for a (nonincomplete) tagged type declared in a package_specification, overriding in the body or by a child subprogram.

Ramification: A consequence is that for a tagged type declaration in a declarative_part, only the last (overriding) last primitive subprogram can be declared by a subprogram_body. Other overridings must be provided by subprogram_declarations.

To be honest: This rule applies only to "original" declarations and not to the completion of a primitive subprogram, even though a completion is technically an explicit declaration, and it may declare a primitive subprogram.

For the execution of a call on a dispatching operation of a type T, the controlling tag value determines which subprogram body is executed. The controlling tag value is defined as follows:

- If one or more controlling operands are statically tagged, then the controlling tag value is statically determined to be the tag of T.

- If one or more controlling operands are dynamically tagged, then the controlling tag value is not statically determined, but is rather determined by the tags of the controlling operands. If there is more than one dynamically tagged controlling operand, a check is made that they all have the same tag. If this check fails, Constraint_Error is raised unless the call is a function_call whose...
name denotes the declaration of an equality operator (predefined or user defined) that returns
Boolean, in which case the result of the call is defined to indicate inequality, and no
subprogram_body is executed. This check is performed prior to evaluating any tag-indeterminate
controlling operands.

**Reason:** Tag mismatch is considered an error (except for "=" and "/=") since the corresponding primitive subprograms
in each specific type expect all controlling operands to be of the same type. For tag mismatch with an equality
operator, rather than raising an exception, ",=" returns False and "/=" returns True. No equality operator is actually
invoked, since there is no common tag value to control the dispatch. Equality is a special case to be consistent with the
existing Ada 83 principle that equality comparisons, even between objects with different constraints, never raise
Constraint_Error.

- **{AI95-00196-01}** If all of the controlling operands (if any) are tag-indeterminate, then:
  - **{AI95-00239-01}** **{AI95-00416-01}** If the call has a controlling result or controlling access
    result and is itself, or designates, a (possibly parenthesized or qualified) controlling operand
    of an enclosing call on a dispatching operation of a descendant of type \( T \), then its controlling
tag value is determined by the controlling tag value of this enclosing call;

**Discussion:** **{AI95-00239-01}** For code that a user can write explicitly, the only contexts that can control dispatching
of a function with a controlling result of type \( T \) are those that involve controlling operands of the same type \( T \): if the
two types differ there is an illegality and the dynamic semantics are irrelevant.

In the case of an inherited subprogram however, if a default expression is a function call, it may be of type \( T \) while the
parameter is of a type derived from \( T \). To cover this case, we talk about "a descendant of \( T \)" above. This is safe,
because if the type of the parameter is descended from the type of the function result, it is guaranteed to inherit or
override the function, and this ensures that there will be an appropriate body to dispatch to. Note that abstract functions
are not an issue here because the call to the function is a dispatching call, so it is guaranteed to always land on a
concrete body.

- **{AI95-00196-01}** **{AI95-00416-01}** If the call has a controlling result or controlling access
    result and (possibly parenthesized, qualified, or dereferenced) is the expression of an
    assignment_statement whose target is of a class-wide type, then its controlling tag value is
determined by the target;

- Otherwise, the controlling tag value is statically determined to be the tag of type \( T \).

**Ramification:** This includes the cases of a tag-indeterminate procedure call, and a tag-indeterminate function_call that
is used to initialize a class-wide formal parameter or class-wide object.

**{AI95-00345-01}** **{AI05-0126-1}** For the execution of a call on a dispatching operation, the action
performed is determined by the properties of the corresponding dispatching operation. Body executed is the
one for the corresponding primitive subprogram of the specific type identified by the controlling tag
value. If the corresponding operation is The body for an explicitly declared for this type, [even if the
declaration occurs in a private part], then the action comprises an invocation of the dispatching operation
is the corresponding explicit body for the operation. If the corresponding operation is implicitly declared
for this type subprogram. The body for an implicitly declared dispatching operation that is overridden is
the body for the overriding subprogram, [even if the overriding occurs in a private part.] The body for an
inherited dispatching operation that is not overridden is the body of the corresponding subprogram of the
parent or ancestor type.

- **{AI05-0126-1}** if the corresponding operation is explicitly declared for this type, [even if the
declaration occurs in a private part], then the action comprises an invocation of the explicit body
for the operation;

- **{AI95-00345-01}** **{AI05-0126-1}** if the corresponding operation is implicitly declared for this
type and is implemented by an entry or protected subprogram (see 9.1 and 9.4), then the action
comprises a call on this entry or protected subprogram, with the target object being given by the
first actual parameter of the call, and the actual parameters of the entry or protected subprogram
being given by the remaining actual parameters of the call, if any;

- **{AI05-0197-1}** if the corresponding operation is a predefined operator then the action comprises
an invocation of that operator;
20.4.3 • \{AI05-0045-01\} \{AI05-0126-1\} \{AI05-0197-1\} \{AI05-0250-1\} \{AI05-0254-1\} otherwise, the action is the same as the action for the corresponding operation of the parent type or progenitor type from which the operation was inherited except that additional invariant checks (see 7.3.2) and class-wide postcondition checks (see 6.1.1) may apply. If there is more than one such corresponding operation, the action is that for the operation that is not a null procedure, if any; otherwise, the action is that of an arbitrary one of the operations.

20.a/3

\begin{itemize}
\item \{AI05-0126-1\} \{AI05-0197-1\} \{AI05-0250-1\} \{AI05-0254-1\} \{AI05-0005-1\}\{AI05-0126-1\} \{AI05-0197-1\} “Corresponding dispatching operation” refers to the inheritance relationship between subprograms. Primitive operations are always inherited for a type T, but they might not be declared if the primitive operation is never visible within the immediate scope of the type T. If no corresponding operation is declared, the last bullet is used and the corresponding operation of the parent type is executed (an explicit body that happens to have the same name and profile is not called in that case).
\item \{AI05-0005-1\} \{AI05-0126-1\} We have to talk about progenitors in the last bullet in case the corresponding operation is a null procedure inherited from an interface. In that case, the parent type might not even have the operation in question.
\item \{AI05-0197-1\} For the last bullet, if there are multiple corresponding operations for the parent and progenitors, all but one of them have to be a null procedure. (If the progenitors declared abstract routines, there would have to be an explicit overriding of the operation, and then the first bullet would apply.) We call the nonnull routine if one exists.
\item \{AI05-0126-1\} Any explicit declaration for an inherited corresponding operation has to be an overriding routine. These rules mean that a dispatching call executes the overriding routine (if any) for the specific type.
\end{itemize}

20.a/1

\begin{itemize}
\item \{AI05-0005-1\} The wording of the above rules is intended to ensure that the same body is executed for a given tag, whether that tag is determined statically or dynamically. For a type declared in a package, it doesn't matter whether a given subprogram is overridden in the visible part or the private part, and it doesn't matter whether the call is inside or outside the package. For example:
\end{itemize}

\begin{verbatim}
20.c

package P1 is
  type T1 is tagged null record;
  procedure Op_A(Param : in T1);
  procedure Op_B(Param : in T1);
end P1;

20.d

with P1; use P1;

package P2 is
  type T2 is new T1 with null record;
  procedure Op_A(Param : in T2);
  private
    procedure Op_B(Param : in T2);
end P2;

20.e/1

with P1; with P2;

procedure Main is
  X : P2.T2;
  Y : P1.T1'TClass := X;
begin
  P2.Op_A(Param => X); -- Nondispatching call to a dispatching operation.
  P1.Op_A(Param => Y); -- Dispatching call.
  P2.Op_B(Param => X); -- Nondispatching call to a dispatching operation.
  P1.Op_B(Param => Y); -- Dispatching call.
end Main;

20.f

The two calls to Op_A both execute the body of Op_A that has to occur in the body of package P2. Similarly, the two calls to Op_B both execute the body of Op_B that has to occur in the body of package P2, even though Op_B is overridden in the private part of P2. Note, however, that the formal parameter names are different for P2.Op_A versus P2.Op_B. The overriding declaration for P2.Op_B is not visible in Main, so the name in the call actually denotes the implicit declaration of Op_B inherited from T1.

20.g

If a call occurs in the program text before an overriding, which can happen only if the call is part of a default expression, the overriding will still take effect for that call.

20.h

Implementation Note: Even when a tag is not \textit{statically determined}, a compiler might still be able to figure it out and thereby avoid the overhead of run-time dispatching.

NOTE 1 The body to be executed for a call on a dispatching operation is determined by the tag; it does not matter whether that tag is determined statically or dynamically, and it does not matter whether the subprogram's declaration is visible at the place of the call.
NOTE 2 {AI95-00260-02} This subclause covers calls on dispatching primitive subprograms of a tagged type. Rules for tagged type membership tests are described in 4.5.2. Controlling tag determination for an assignment_statement is described in 5.2.

NOTE 3 A dispatching call can dispatch to a body whose declaration is not visible at the place of the call.

NOTE 4 A call through an access-to-subprogram value is never a dispatching call, even if the access value designates a dispatching operation. Similarly a call whose prefix denotes a subprogram_renaming_declaration cannot be a dispatching call unless the renaming itself is the declaration of a primitive subprogram.

Extensions to Ada 83

The concept of dispatching operations is new.

Incompatibilities With Ada 95

{AI95-00404-01} If a dispatching operation is defined by a subprogram_renaming_declaration, and it has a controlling access parameter, Ada 2005 requires the subtype of the parameter to exclude null. The same applies to instantiations. This is required so that all calls to the subprogram operate the same way (controlling access parameters have to exclude null so that dispatching calls will work). Since Ada 95 didn't have the notion of access subtypes that exclude null, and all access parameters excluded null, it had no such rules. These rules will require the addition of an explicit not null on nondispatching operations that are later renamed to be dispatching, or on a generic that is used to define a dispatching operation.

Extensions to Ada 95

{AI95-00416-01} Functions that have an access result type can be dispatching in the same way as a function that returns a tagged object directly.

Wording Changes from Ada 95

{8652/0010} {AI95-00127-01} {AI05-0299-1} **Corrigendum:** Allocators and access attributes of objects of class-wide types can be used as the controlling parameter in a dispatching calls. This was an oversight in the definition of Ada 95. (See 3.10.2 and 4.8).

{8652/0011} {AI95-00117-01} {AI95-00430-01} **Corrigendum:** Corrected the conventions of dispatching operations. This is extended in Ada 2005 to cover operations inherited from progenitors, and to ensure that the conventions of all inherited operations are the same.

{AI95-00196-01} Clarified the wording to ensure that functions with no controlling operands are tag-indeterminate, and to describe that the controlling tag can come from the target of an assignment_statement.

{AI95-00239-01} Fixed the wording to cover default expressions inherited by derived subprograms. A literal reading of the old wording would have implied that operations would be called with objects of the wrong type.

{AI95-00260-02} **An abstract formal subprogram is a dispatching operation, even though it is not a primitive operation. See 12.6, "Formal Subprograms"**.

{AI95-00345-01} Dispatching calls include operations implemented by entries and protected operations, so we have to update the wording to reflect that.

{AI95-00355-01} **A stream attribute of a tagged type is usually a dispatching operation, even though it is not a primitive operation. If they weren't dispatching, T'Class'Input and T'Class'Output wouldn't work.**

Wording Changes from Ada 2005

{AI05-0076-1} **Correction:** Defined “function with a controlling result”, as it is used in 3.9.3.

{AI05-0126-1} {AI05-0197-1} **Correction:** Corrected holes in the definition of dynamic dispatching: the behavior for operations that are never declared and/or inherited from a progenitor were not specified.

Wording Changes from Ada 2012

{AI12-0236-1} Added a special rule for taggedness of declare_expressions, and added a pointer to the existing special rules for conditional_expressions, as the list of exceptions to the usual rules appear to be exhaustive.

{AI12-0419-1} **Added wording to clarify that the Put Image attribute is a dispatching operation. Put Image follows the model of stream-oriented attributes, and thus need to be mentioned in the same place.**
3.9.3 Abstract Types and Subprograms

An abstract type is a tagged type intended for use as an ancestor of other types, but which is not allowed to have objects of its own. An abstract subprogram is a subprogram that has no body, but is intended to be overridden at some point when inherited. Because objects of an abstract type cannot be created, a dispatching call to an abstract subprogram always dispatches to some overriding body.

Syntax

```
abstract_subprogram_declaration ::= 
[overriding_indicator]
subprogram_specification is abstract
[aspect_specification];
```

Static Semantics

Interface types (see 3.9.4) are abstract types. In addition, a tagged type that has the reserved word abstract in its declaration is an abstract type. The class-wide type (see 3.4.1) rooted at an abstract type is not itself an abstract type.

Legality Rules

Only a tagged type shall have an abstract type is a specific type that has the reserved word abstract in its declaration. Only a tagged type is allowed to be declared abstract.

Ramification: Untagged types are never abstract, even though they can have primitive abstract subprograms. Such subprograms cannot be called, unless they also happen to be dispatching operations of some tagged type, and then only via a dispatching call.

Class-wide types are never abstract. If T is abstract, then it is illegal to declare a stand-alone object of type T, but it is OK to declare a stand-alone object of type T'Class; the latter will get a tag from its initial value, and this tag will necessarily be different from T'Tag.

A subprogram declared by an abstract_subprogram_declaration or a formal abstract_subprogram_declaration (see 12.6)(see 6.1) is an abstract subprogram. If it is a primitive subprogram of a tagged type, then the tagged type shall be abstract.

Ramification: Note that for a private type, this applies to both views. The following is illegal:

```
package P is
  type T is abstract tagged private;
  function Foo (X : T) return Boolean is abstract; -- Illegal!
private
  type T is tagged null record; -- Illegal!
  X : T;
  Y : Boolean := Foo (T'Class (X));
end P;
```

The full view of T is not abstract, but has an abstract operation Foo, which is illegal. The two lines marked "-- Illegal!" are illegal when taken together.
Reason: \{AI95-00310-01\} We considered disallowing untagged types from having abstract primitive subprograms. However, we rejected that plan, because it introduced some silly anomalies, and because such subprograms are harmless (if not terribly useful). For example:

```
package P is
  type Field_Size is range 0..100;
  type T is abstract tagged null record;
  procedure Print(X : in T; F : in Field_Size := 0) is abstract abstract;
  . . .
package Q is
  type My_Field_Size is new Field_Size;
  -- implicit declaration of Print(X : T; F : My_Field_Size := 0) is abstract abstract;
end Q;
```

It seemed silly to make the derivative of My_Field_Size illegal, just because there was an implicitly declared abstract subprogram that was not primitive on some tagged type. Other rules could be formulated to solve this problem, but the current ones seem like the simplest.

\{AI95-00310-01\} In Ada 2005, abstract primitive subprograms of an untagged type may be used to “undefine” an operation.

Ramification: \{AI95-00260-02\} Note that the second sentence does not apply to abstract formal subprograms, as they are never primitive operations of a type.

\{AI95-00251-01\} \{AI95-00334-01\} \{AI95-00391-01\} \{AI05-0097-1\} \{AI05-0198-1\} If a type has an implicitly declared primitive subprogram that is inherited or is the predefined equality-operator, and the corresponding primitive subprogram of a derived type, if the parent or ancestor type is abstract or is a function with a controlling access result, or if a type other than a nonabstract null extension inherits an abstract primitive subprogram, or a primitive function with a controlling result, then:

Ramification: \{AI95-0068-1\} These rules apply to each view of the type individually. That is necessary to preserve privacy. For instance, in the following example:

```
package P is
  -- type I is interface;
  procedure Op (X : I) is abstract;
end P;
with P;
package Q is
  -- type T is abstract new P.I with private;
  -- Op inherited here.
  private
  -- type T is abstract new P.I with null record;
  procedure Op (X : T) is null;
end Q;
with Q;
package R is
  -- type T2 is new Q.T with null record;
  -- illegal. Op inherited here, but requires overriding.
end R;
```

If this did not depend on the view, this would be legal. But in that case, the fact that Op is overridden in the private part would be visible; package R would have to be illegal if no overriding was in the private part.

Note that this means that whether an inherited subprogram is abstract or concrete depends on where it inherited. In the case of Q, Q.Op in the visible part is abstract, while Q.Op in the private part is concrete. That is, R is illegal since it is an unrelated unit (and thus it cannot see the private part), but if R had been a private child of Q, it would have been legal.

- \{AI95-00251-01\} \{AI95-00334-01\} If the derived type is abstract or untagged, the implicitly declared inherited subprogram is abstract.

Ramification: Note that it is possible to override a concrete subprogram with an abstract one.

- \{AI95-00391-01\} \{AI12-0080-1\} \{AI12-0444-1\} Otherwise, the subprogram shall be overridden with a nonabstract subprogram or, in the case of a private extension inheriting a nonabstract function with a controlling result, have a full type that is a null extension; for a type declared in the visible part of a package, the overriding may be either in the visible or the private part. Such a subprogram is said to require overriding. However, if the type is a generic formal type, the subprogram is allowed to be inherited as is, without being needed to be overridden for the formal type itself; a nonabstract version will necessarily be provided by the actual type.]
Reason: {AI95-00228-01} {AI95-00391-01} A function that returns the parent type requires overriding because abstract for an abstract type extension (or becomes abstract for an abstract type) if not overridden, because conversion from a parent type to a type extension is not defined, and function return semantics is defined in terms of conversion (other than for a null extension; see below). (Note that parameters of mode in or out do not have this problem, because the tag of the actual is not changed.)

Note that the overriding required above can be in the private part, which allows the following:

package Pack1 is
  type Ancestor is abstract ...;
  procedure Do_Something(X : in Ancestor) is abstract;
end Pack1;

with Pack1; use Pack1;
package Pack2 is
  type T1 is new Ancestor with record ...;
  -- A concrete type.
  procedure Do_Something(X : in T1); -- Have to override.
end Pack2;

with Pack1; use Pack1;
with Pack2; use Pack2;
package Pack3 is
  type T2 is new Ancestor with private;
  -- A concrete type.
  private
    type T2 is new T1 with -- Parent different from ancestor.
    record ... end record;
    -- Here, we inherit Pack2.Do_Something.
  end T2;
end Pack3;

T2 inherits an abstract Do_Something, but T2 is not abstract, so Do_Something has to be overridden. However, it is OK to override it in the private part. In this case, we override it by inheriting a concrete version from a different type. Nondispatching calls to Pack3.Do_Something are allowed both inside and outside package Pack3, as the client "knows" that the subprogram was necessarily overridden somewhere.

For a null extension, the result of a function with a controlling result is defined in terms of an extension_aggregate with a null record extension part (see 3.4). This means that these restrictions on functions with a controlling result do not have to apply to null extensions.

However, functions with controlling access results still require overriding. Changing the tag in place might clobber a preexisting object, and allocating new memory would possibly change the pool of the object, leading to storage leaks. Moreover, copying the object isn't possible for limited types. We don't need to restrict functions that have an access return type of an untagged type, as derived types with primitive subprograms have to have the same representation as their parent type.

A call on an abstract subprogram shall be a dispatching call; nondispatching calls to an abstract subprogram are not allowed. In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

Ramification: {AI95-00310-01} {AI92-0413-1} If an abstract subprogram is not a dispatching operation of some tagged type, then it cannot be called at all. In Ada 2005, such subprograms are not even considered by name resolution (see 6.4). However, this rule is still needed for cases that can arise in the instance of a generic specification where Name Resolution Rules are not reapplied, but Legality Rules are, when the equality operator for an untagged record type is abstract, while the operator for the formal type is not abstract (see 12.5).

If the name or prefix given in an iterator_procedure_call (see 5.5.3) denotes an abstract subprogram, the subprogram shall be a dispatching subprogram.

The type of an aggregate, or of an object created by an object_declaration or an allocator, or of a generic formal object of mode in, shall not be abstract. The type of the target of an assignment operation (see 5.2) shall not be abstract. The type of a component shall not be abstract. If the result type of a function is abstract, then the function shall be abstract. If a function has an access result type designating an abstract type, then the function shall be abstract. The type denoted by a return_subtype_indication (see 6.5) shall not be abstract. A generic function shall not have an abstract result type or an access result type designating an abstract type.

Reason: This ensures that values of an abstract type cannot be created, which ensures that a dispatching call to an abstract subprogram will not try to execute the nonexistent body.
Generic formal objects of mode \texttt{in} are like constants; therefore they should be forbidden for abstract types. Generic formal objects of mode \texttt{in out} are like renamings; therefore, abstract types are OK for them, though probably not terribly useful.

\{AI05-0073-1\} Generic functions returning a formal abstract type are illegal because any instance would have to be instantiated with a nonabstract type in order to avoid violating the function rule (generic functions cannot be declared abstract). But that would be an implied contract; it would be better for the contract to be explicit by the formal type not being declared abstract. Moreover, the implied contract does not add any capability.

If a partial view is not abstract, the corresponding full view shall not be abstract. If a generic formal type is abstract, then for each primitive subprogram of the formal that is not abstract, the corresponding primitive subprogram of the actual shall not be abstract.

\textbf{Discussion:} By contrast, we allow the actual type to be nonabstract even if the formal type is declared abstract. Hence, the most general formal tagged type possible is "\texttt{type T(<>)} is abstract tagged limited private;".

For an abstract private extension declared in the visible part of a package, it is only possible for the full type to be nonabstract if the private extension has no abstract dispatching operations.

\textbf{To be honest:} \{AI95-00294-01\} In the sentence about primitive subprograms above, there is some ambiguity as to what is meant by “corresponding” in the case where an inherited operation is overridden. This is best explained by an example, where the implicit declarations are shown as comments:

```ada
package P1 is
    type T1 is abstract tagged null record;
    procedure P (X : T1);  -- (1)
end P1;

package P2 is
    type T2 is abstract new P1.T1 with null record;
    -- procedure P(X : T2);  -- (2)
    procedure P (X : T2) is abstract;  -- (3)
end P2;

generic
type D is abstract new P1.T1 with private;
    procedure G (X : D);  -- (4)
procedure I is new G (P2.T2);  -- Illegal.
```

Type T2 inherits a nonabstract procedure P (2) from the primitive procedure P (1) of T1. P (2) is overridden by the explicitly declared abstract procedure P (3). Type D inherits a nonabstract procedure P (4) from P (1). In instantiation I, the operation corresponding to P (4) is the one which is not overridden, that is, P (3); the overridden operation P (2) does not “reemerge”. Therefore, the instantiation is illegal.

\{AI05-0073-1\} For an abstract type declared in a visible part, an abstract primitive subprogram shall not be declared in the private part, unless it is overriding an abstract subprogram implicitly declared in the visible part. For a tagged type declared in a visible part, a primitive function with a controlling result or a controlling access result shall not be declared in the private part, unless it is overriding a function implicitly declared in the visible part.

\textbf{Reason:} The “visible part” could be that of a package or a generic package. This rule is needed because a nonabstract type extension declared outside the package would not know about any abstract primitive subprograms or primitive functions with controlling results declared in the private part, and wouldn't know that they need to be overridden with nonabstract subprograms. The rule applies to a tagged record type or record extension declared in a visible part, just as to a tagged private type or private extension. The rule applies to explicitly and implicitly declared abstract subprograms:

```ada
package Pack is
    type T is abstract new T1 with private;
    private
        type T is abstract new T2 with record ... end record;
    ...
end Pack;
```

The above example would be illegal if T1 has a nonabstract primitive procedure P, but T2 overides P with an abstract one; the private part should override P with a nonabstract version. On the other hand, if the P were abstract for both T1 and T2, the example would be legal as is.

\{AI95-00260-02\} A generic actual subprogram shall not be an abstract subprogram unless the generic formal subprogram is declared by a formal abstract subprogram declaration. The prefix of an
attribute_reference for the Access, Unchecked_Access, or Address attributes shall not denote an abstract subprogram.

**Ramification:** An abstract_subprogram_declaration is not syntactically a subprogram_declaration. Nonetheless, an abstract subprogram is a subprogram, and an abstract_subprogram_declaration is a declaration of a subprogram.

\{AI95-00260-02\} The part about generic actual subprograms includes those given by default. Of course, an abstract formal subprogram’s actual subprogram can be abstract.

**Dynamic Semantics**

\{AI95-00348-01\} The elaboration of an abstract_subprogram_declaration has no effect.

**NOTE 1** \{AI12-0447-1\} Abstractness is not inherited; a type is abstract only if to declare an abstract type, the reserved word abstract has to be used in the declaration of the type extension.

**Ramification:** A derived type can be abstract even if its parent is not. Similarly, an inherited concrete subprogram can be overridden with an abstract subprogram.

**NOTE 2** A class-wide type is never abstract. Even if a class is rooted at an abstract type, the class-wide type for the class is not abstract, and an object of the class-wide type can be created; the tag of such an object will identify some nonabstract type in the class.

**Examples**

Example of an abstract type representing a set of natural numbers:

```ada
package Sets is
  subtype Element_Type is Natural;
type Set is abstract tagged null record;
function Empty return Set is abstract;
function Union(Left, Right : Set) return Set is abstract;
function Intersection(Left, Right : Set) return Set is abstract;
function Unit_Set(Element : Element_Type) return Set is abstract;
procedure Take(Element : out Element_Type;
  From : in out Set) is abstract;
end Sets;
```

\{AI12-0442-1\} \{AI12-0452-1\} Given the above abstract type, one can derive various (nonabstract) extensions of the type, representing alternative implementations of a set. One possibility is to use a bit vector, but impose an upper bound on the largest element representable, while another possible implementation is a hash table, trading off space for flexibility.

**NOTE 3** \{AI12-0452-1\} Notes on the example: Given the above abstract type, one could then derive various (nonabstract) extensions of the type, representing alternative implementations of a set. One might use a bit vector, but impose an upper bound on the largest element representable, while another might use a hash table, trading off space for flexibility.

**Discussion:** One way to export a type from a package with some components visible and some components private is as follows:

```ada
package P is
  type Public_Part is abstract tagged
    record ...
  end record;
  type T is new Public_Part with private;
private
  type T is new Public_Part with
    record ...
  end record;
end P;
```

The fact that Public_Part is abstract tells clients they have to create objects of type T instead of Public_Part. Note that the public part has to come first; it would be illegal to declare a private type Private_Part, and then a record extension T of it, unless T were in the private part after the full declaration of Private_Part, but then clients of the package would not have visibility to T.
Extensions to Ada 95

\{AI95-00391-01\} It is not necessary to override functions with a controlling result for a null extension. This makes it easier to derive a tagged type to complete a private type.

Wording Changes from Ada 95

\{AI95-00251-01\} \{AI95-00345-01\} Updated the wording to reflect the addition of interface types (see 3.9.4).
\{AI95-00260-02\} Updated the wording to reflect the addition of abstract formal subprograms (see 12.6).
\{AI95-00334-01\} The wording of shall-be-overridden was clarified so that it clearly applies to abstract predefined equality.
\{AI95-00348-01\} Moved the syntax and elaboration rule for \texttt{abstract_subprogram_declaration} here, so the syntax and most of the semantics are together (which is consistent with null procedures).
\{AI95-00391-01\} We define the term \texttt{require overriding} to make other wording easier to understand.

Incompatibilities With Ada 2005

\{AI05-0073-1\} \textbf{Correction:} Added rules to eliminate holes with controlling access results and generic functions that return abstract types. While these changes are technically incompatible, it is unlikely that they could be used in a program without violating some other rule of the use of abstract types.

\{AI05-0097-1\} \textbf{Correction:} Corrected a minor glitch having to do with abstract null extensions. The Ada 2005 rule allowed such extensions to inherit concrete operations in some rare cases. It is unlikely that these cases exist in user code.

Extensions to Ada 2005

\{AI05-0183-1\} An optional \texttt{aspect_specification} can be used in an \texttt{abstract_subprogram_declaration}. This is described in 13.1.1.

Wording Changes from Ada 2005

\{AI05-0198-1\} \textbf{Correction:} Clarified that the predefined operator corresponding to an inherited abstract operator is also abstract. The Ada 2005 rules caused the predefined operator and the inherited operator to override each other, which is weird. But the effect is the same either way (the operator is not considered for resolution).

\{AI05-0203-1\} \textbf{Correction:} Added wording to disallow abstract return objects. These were illegal in Ada 2005 by other rules; the extension to support class-wide type better opened a hole which has now been plugged.

Incompatibilities With Ada 2012

\{AI12-0413-1\} \textbf{Correction:} Clarified that a recheck is needed in the case of an actual that is a record type with an abstract equality. This is an incompatibility as the generic boilerplate was previously omitted, meaning that such a recheck should not have been performed in the private part of an instance. Usually, this would just change an elaboration time raise of \texttt{Program_Error} into an error (a good thing, as the instance will never be useful), but could break a working instance if the equality usage is in a default expression that appears in the private part of the generic unit and it is never used in a call. In that case, Ada 2022 will reject the instance while it would have worked in Ada 2012. As a practical matter, it’s more likely that a compiler already does the recheck in the entire instance spec, or does not do it at all; thus for many implementations there will be no practical incompatibility.

3.9.4 Interface Types

\{AI95-00251-01\} \{AI95-00345-01\} [An interface type is an abstract tagged type that provides a restricted form of multiple inheritance. A tagged type, task type, or protected type may have one or more interface types as ancestors.]

Term entry: interface type — abstract tagged type that has no components or concrete operations except possibly null procedures.

Note: Interface types are used for composing other interfaces and tagged types and thereby provide multiple inheritance. Only an interface type can be used as a progenitor of another type.
Language Design Principles

The rules are designed so that an interface can be used as either a parent type or a progenitor type without changing the meaning. That's important so that the order that interfaces are specified in a derived_type_definition is not significant. In particular, we want:

```ada
type Con1 is new Int1 and Int2 with null record;
type Con2 is new Int2 and Int1 with null record;
```

to mean exactly the same thing.

Syntax

```ada
interface_type_definition ::= [limited | task | protected | synchronized] interface [and interface_list]

interface_list ::= interface_subtype_mark {and interface_subtype_mark}
```

Static Semantics

An interface type (also called an interface) is a specific abstract tagged type that is defined by an interface_type_definition.

An interface with the reserved word limited, task, protected, or synchronized in its definition is termed, respectively, a limited interface, a task interface, a protected interface, or a synchronized interface. In addition, all task and protected interfaces are synchronized interfaces, and all synchronized interfaces are limited interfaces.

Term entry: synchronized — can be safely operated on by multiple tasks concurrently

Note: Synchronized is used to qualify entities, as in a synchronized interface.

A task or protected type derived from an interface is a tagged type. Such a tagged type is called a synchronized tagged type, as are synchronized interfaces and private extensions whose declaration includes the reserved word synchronized.

Proof: The full definition of tagged types given in 3.9 includes task and protected types derived from interfaces.

Ramification: The class-wide type associated with a tagged task type (including a task interface type) is a task type, because “task” is one of the language-defined classes of types (see 3.2). However, the class-wide type associated with an interface is not an interface type, as “interface” is not one of the language-defined classes (as it is not closed under derivation). In this sense, “interface” is similar to “abstract”. The class-wide type associated with an interface is a concrete (nonabstract) indefinite tagged composite type.

“Private extension” includes generic formal private extensions, as explained in 12.5.1.

A task interface is an [abstract] task type. A protected interface is an [abstract] protected type.

Proof: The “abstract” follows from the definition of an interface type.

Reason: This ensures that task operations (like abort and the Terminated attribute) can be applied to a task interface type and the associated class-wide type. While there are no protected type operations, we apply the same rule to protected interfaces for consistency.

An interface subtype mark in an interface list names a progenitor subtype; its type is the progenitor type. An interface type inherits user-defined primitive subprograms from each progenitor type in the same way that a derived type inherits user-defined primitive subprograms from its progenitor types (see 3.4).

Term entry: progenitor — type given in the interface list, if any, of an interface, task, protected, or derived type definition

Note: A progenitor is always an interface type.
### Legality Rules

**{AI95-00251-01}** All user-defined primitive subprograms of an interface type shall be abstract subprograms or null procedures.

**{AI95-00251-01}** The type of a subtype named in an interface_list shall be an interface type.

**{AI95-00251-01} {AI95-00345-01}** A type derived from a nonlimited interface shall be nonlimited.

**{AI95-00345-01}** An interface derived from a task interface shall include the reserved word `task` in its definition; any other type derived from a task interface shall be a private extension or a task type declared by a task declaration (see 9.1).

**{AI95-00345-01}** An interface derived from a protected interface shall include the reserved word `protected` in its definition; any other type derived from a protected interface shall be a private extension or a protected type declared by a protected declaration (see 9.4).

**{AI95-00345-01}** An interface derived from a synchronized interface shall include one of the reserved words `task`, `protected`, or `synchronized` in its definition; any other type derived from a synchronized interface shall be a private extension, a task type declared by a task declaration, or a protected type declared by a protected declaration.

**Reason:** We require that an interface descendant of a task, protected, or synchronized interface repeat the explicit kind of interface it will be, rather than simply inheriting it, so that a reader is always aware of whether the interface provides synchronization and whether it may be implemented only by a task or protected type. The only place where inheritance of the kind of interface might be useful would be in a generic if you didn't know the kind of the actual interface. However, the value of that is low because you cannot implement an interface properly if you don't know whether it is a task, protected, or synchronized interface. Hence, we require the kind of the actual interface to match the kind of the formal interface (see 12.5.5).

**{AI95-00345-01}** No type shall be derived from both a task interface and a protected interface.

**Reason:** This prevents a single private extension from inheriting from both a task and a protected interface. For a private type, there can be no legal completion. For a generic formal derived type, there can be no possible matching type (so no instantiation could be legal). This rule provides early detection of the errors.

**{AI95-00251-01}** In addition to the places where Legality Rules normally apply (see 12.3), these rules apply also in the private part of an instance of a generic unit.

**Ramification:** {AI05-0299-1} This paragraph is intended to apply to all of the Legality Rules in this subclause. We cannot allow interface types which do not obey these rules, anywhere. Luckily, deriving from a formal type (which might be an interface) is not allowed for any tagged types in a generic body. So checking in the private part of a generic covers all of the cases.

### Dynamic Semantics

**{AI95-00251-01} {AI05-0070-1}** The elaboration of an interface_type_definition creates the interface type and its first subtype has no effect.

**Discussion:** There is no other effect. An interface list is made up of subtype marks, which do not need to be elaborated, so the interface_list does not either. This is consistent with the handling of discriminant_parts.

**NOTE** {AI95-00411-01} {AI12-0440-1} Nonlimited interface types have predefined nonabstract equality operators. These cannot be overridden with user-defined abstract equality operators. Such operators will then require an explicit overriding for any nonabstract descendant of the interface.

### Examples

**{AI95-00433-01}** Example of a limited interface and a synchronized interface extending it:
type Queue is limited interface;
procedure Append(Q: in out Queue; Person: in Person_Name) is abstract;
procedure Remove_First(Q: in out Queue; Person: out Person_Name) is abstract;
function Cur_Count(Q: in Queue) return Natural is abstract;
function Max_Count(Q: in Queue) return Natural is abstract;
-- See 3.10.1 for Person_Name.
exception
  Queue_Error;
... 
procedure Transfer(From: in out Queue'Class; 
                    To: in out Queue'Class; 
                    Number: in Natural := 1) is 
  Person: Person_Name;
begin
  for I in 1..Number loop
    Remove_First(From, Person);
    Append(To, Person);
  end loop;
end Transfer;

This defines a Queue interface defining a queue of people. (A similar design *could be created* to define any kind of queue simply by replacing Person_Name by an appropriate type.) The Queue interface has four dispatching operations, Append, Remove First, Cur Count, and Max Count. The body of a class-wide operation, Transfer is also shown. Every nonabstract extension of Queue *must* provide implementations for at least its four dispatching operations, as they are abstract. Any object of a type derived from Queue *can* be passed to Transfer as either the From or the To operand. The two operands can be of different types in need not be of the same type in any given call.

The Synchronized Queue interface inherits the four dispatching operations from Queue and adds two additional dispatching operations, which wait if necessary rather than raising the Queue_Error exception. This synchronized interface *can* only be implemented by a task or protected type, and as such ensures safe concurrent access.

Example use of the interface:

type Fast_Food_Queue is new Queue with record ...;
procedure Append(Q: in out Fast_Food_Queue; Person: in Person_Name);
procedure Remove_First(Q: in out Fast_Food_Queue; 
                       Person: out in Person_Name);
function Cur_Count(Q: in Fast_Food_Queue) return Natural;
function Max_Count(Q: in Fast_Food_Queue) return Natural;
... 
Cashier, Counter: Fast_Food_Queue;

-- Add CaseyGeorge (see 3.10.1) to the cashier’s queue:
Append (Cashier, CaseyGeorge);
-- After payment, move CaseyGeorge to the sandwich counter queue:
Transfer (Cashier, Counter);
... 

An interface such as Queue can be used directly as the parent of a new type (as shown here), or can be used as a progenitor when a type is derived. In either case, the primitive operations of the interface are inherited. For Queue, the implementation of the four inherited routines *will necessarily*...
be provided. Inside the call of Transfer, calls will dispatch to the implementations of Append and Remove First for type Fast_Food_Queue.

Example of a task interface:

```ada
package Serial_Device is task interface; -- see 9.1
procedure Read (Dev : in Serial_Device; C : out Character) is abstract;
procedure Write (Dev : in Serial_Device; C : in Character) is abstract;
```

The Serial_Device interface has two dispatching operations which are intended to be implemented by task entries (see 9.1).

Extensions to Ada 95

Interface types are new. They provide multiple inheritance of interfaces, similar to the facility provided in Java and other recent language designs.

Wording Changes from Ada 2005

Correction: Corrected the definition of elaboration for an interface_type_definition to match that of other type definitions.

3.10 Access Types

A value of an access type (an access value) provides indirect access to the object or subprogram it designates. Depending on its type, an access value can designate either subprograms, objects created by allocators (see 4.8), or more generally aliased objects of an appropriate type.

Discussion: A name denotes an entity; an access value designates an entity. The “dereference” of an access value X, written “X.all”, is a name that denotes the entity designated by X.

Language Design Principles

Access values should always be well defined (barring uses of certain unchecked features of Clause 13ClauseSection 13). In particular, uninitialized access variables should be prevented by compile-time rules.

Syntax

```ada
access_type_definition ::= 
 null_exclusion access_to_object_definition 
 | null_exclusion access_to_subprogram_definition
access_to_object_definition ::= 
 access [general_access_modifier] subtype_indication
general_access_modifier ::= all | constant
access_to_subprogram_definition ::= 
 access [protected] procedure parameter_profile 
 | access [protected] function parameter_and_result_profile
null_exclusion ::= not null
access_definition ::= 
 null_exclusion access [constant] subtype_mark 
 | null_exclusion access [protected] procedure parameter_profile 
 | null_exclusion access [protected] function parameter_and_result_profile access subtype_mark
```
There are two kinds of access types, access-to-object types, whose values designate objects, and access-to-subprogram types, whose values designate subprograms. Associated with an access-to-object type is a storage pool; several access types may share the same storage pool. All descendants of an access type share the same storage pool. A storage pool is an area of storage used to hold dynamically allocated objects (called pool elements) created by allocators; storage pools are described further in 13.11, “Storage Management”.

Access-to-object types are further subdivided into pool-specific access types, whose values can designate only the elements of their associated storage pool, and general access types, whose values can designate the elements of any storage pool, as well as aliased objects created by declarations rather than allocators, and aliased subcomponents of other objects.

Implementation Note: The value of an access type will typically be a machine address. However, a value of a pool-specific access type can be represented as an offset (or index) relative to its storage pool, since it can point only to the elements of that pool.

A view of an object is defined to be aliased if it is defined by an object_declaration, component definition, parameter specification, or extended return object declaration with the reserved word aliased, or by a renaming of an aliased view. In addition, the dereference of an access-to-object value denotes an aliased view, as does a view conversion (see 4.6) of an aliased view. A qualified_expression denotes an aliased view when the operand denotes an aliased view. The current instance of an immutably limited type (see 7.5) isa limited tagged type, a protected type, a task type, or a type that has the reserved word limited in its full definition is also defined to be aliased.

Term entry: aliased view — view of an object that can be designated by an access value

Note: Objects allocated by allocators are aliased. Objects can also be explicitly declared as aliased with the reserved word aliased. The Access attribute can be used to create an access value designating an aliased object.

Ramification: The current instance of a nonlimited type is not aliased.

The object created by an allocator is aliased, but not its subcomponents, except of course for those that themselves have aliased in their component definition.

The renaming of an aliased object is aliased.

Slices are never aliased. See 4.1.2 for more discussion.

Reason: The current instance of a limited type is defined to be aliased so that an access discriminant of a component can be initialized with T'Access inside the definition of T. Note that we don’t want this to apply to a type that could become nonlimited later within its immediate scope, so we require the full definition to be limited.

A formal parameter of a tagged type is defined to be aliased so that a (tagged) parameter X may be passed to an access parameter P by using P => X’Access. Access parameters are most important for tagged types because of dispatching-on-access-parameters (see 3.9.2). By restricting this to formal parameters, we minimize problems associated with allowing components that are not declared aliased to be pointed-to from within the same record.

A view conversion of an aliased view is aliased so that the type of an access parameter can be changed without first converting to a named access type. For example:

```ada
type T1 is tagged ...;
procedure P(X : access T1);
```
type T2 is new T1 with ...;
procedure P(X : access T2) is begin
  P(T1(X.all)'Access); -- hand off to T1's P
  .. -- now do extra T2-specific processing
end P;

This paragraph was deleted. [AI95-00363-01] The rule about objects with discriminants is necessary because values of a constrained access subtype can designate an object whose nominal subtype is unconstrained: without this rule, a check on every use of such values would be required to ensure that the discriminants of the object had not changed. With this rule (among others), we ensure that if there might exist aliased views of a discriminated object, then the object is necessarily constrained. Note that this rule is necessary only for untagged types, since a discriminant of a tagged type can't have a default, so all tagged discriminated objects are always constrained anyway.

We considered making more kinds of objects aliased by default. In particular, any object of a by-reference type will pretty much have to be allocated at an addressable location, so it can be passed by reference without using bit-field pointers. Therefore, one might wish to allow the Access and Unchecked_Access attributes for such objects. However, private parts are transparent to the definition of “by-reference type”, so if we made all objects of a by-reference type aliased, we would be violating the privacy of private parts. Instead, we would have to define a concept of “visibly by-reference” and base the rule on that. This seemed to complicate the rules more than it was worth, especially since there is no way to declare an untagged limited private type to be by-reference, since the full type might by nonlimited.

Discussion: Note that we do not use the term “aliased” to refer to formal parameters that are referenced through multiple access paths (see 3.2).

An access_to_object_definition defines an access-to-object type and its first subtype; the subtype_indication defines the designated subtype of the access type. If a general_access_modifier appears, then the access type is a general access type. If the modifier is the reserved word constant, then the type is an access-to-constant type; a designated object cannot be updated through a value of such a type. If the modifier is the reserved word all, then the type is an access-to-variable type; a designated object can be both read and updated through a value of such a type. If no general_access_modifier appears in the access_to_object_definition, the access type is a pool-specific access-to-variable type.

To be honest: The type of the designated subtype is called the designated type.

Reason: The modifier all was picked to suggest that values of a general access type could point into “all” storage pools, as well as to objects declared aliased, and that “all” access (both read and update) to the designated object was provided. We couldn't think of any use for pool-specific access-to-constant types, so any access type defined with the modifier constant is considered a general access type, and can point into any storage pool or at other (appropriate) aliased objects.

Implementation Note: The predefined generic Unchecked_Deallocation can be instantiated for any named access-to-variable type. There is no (language-defined) support for deallocating objects designated by a value of an access-to-constant type. Because of this, an allocator for an access-to-constant type can allocate out of a storage pool with no support for deallocation. Frequently, the allocation can be done at link-time, if the size and initial value are known then.

Discussion: For the purpose of generic formal type matching, the relevant subclasses of access types are access-to-subprogram types, access-to-constant types, and (named) access-to-variable types, with its subclass (named) general access-to-variable types. Pool-specific access-to-variable types are not a separately matchable subclass of types, since they don't have any “extra” operations relative to all (named) access-to-variable types.

An access_to_subprogram_definition defines an access-to-subprogram type and its first subtype; the parameter_profile or parameter_and_result_profile defines the designated profile of the access type. There is a calling_convention associated with the designated profile; only subprograms with this calling convention can be designated by values of the access type.] By default, the calling convention is “protected” if the reserved word protected appears, and “Ada” otherwise. [See Annex B for how to override this default.]

Ramification: The calling convention protected is in italics to emphasize that it cannot be specified explicitly by the user. This is a consequence of it being a reserved word.

Implementation Note: [AI95-00254-01] For a named access-to-subprogram type, the representation of an access value might include implementation-defined information needed to support up-level references — for example, a static link. The accessibility rules (see 3.10.2) ensure that if there is a “global-display-based” implementation model (as opposed to a static-link-based model), a named access-to-(unprotected)-subprogram value need consist only of the address of the
subprogram. The global display is guaranteed to be properly set up any time the designated subprogram is called. Even in a static-link-based model, the only time a static link is definitely required is for an access-to-subprogram type declared in a scope nested at least two levels deep within subprogram or task bodies, since values of such a type might designate subprograms nested a smaller number of levels. For the normal case of an access-to-subprogram type declared at the outermost (library) level, a code address by itself should be sufficient to represent the access value in many implementations.

11.e For access-to-protected-subprogram, the access values will necessarily include both an address (or other identification) of the code of the subprogram, as well as the address of the associated protected object. This could be thought of as a static link, but it will be needed even for global-display-based implementation models. It corresponds to the value of the implicit parameter that is passed into every call of a protected operation, to identify the current instance of the protected type on which they are to operate.

11.d Any Elaboration_Check is performed when a call is made through an access value, rather than when the access value is first “created” via a 'Access. For implementation models that normally put that check at the call-site, an access value will have to point to a separate entry point that does the check. Alternatively, the access value could point to a "subprogram descriptor" that consisted of two words (or perhaps more), the first being the address of the code, the second being the elaboration bit. Or perhaps more efficiently, just the address of the code, but using the trick that the descriptor is initialized to point to a Raise-Program-Error routine initially, and then set to point to the "real" code when the body is elaborated.

11.f/2 This paragraph was deleted. Essentially the same implementation issues arise for calls on dispatching operations of tagged types, except that the static link is always known “statically.”

11,g/2 Note that access parameters of an anonymous access-to-subprogram type are not permitted. Such if there were such parameters represent, full “downward” closures would be required, meaning that in an implementation that uses a per-task (global) display, the display will have to be passed as a hidden parameter, and reconstructed at the point of call. This was felt to be an undue implementation burden, given that an equivalent (actually, more general) capability is available via formal subprogram parameters to a generic.

12/3 An access_definition defines an anonymous general access type or an anonymous access-to-subprogram type. For a general access type access-to-variable type, the subtype_mark denotes its designated subtype; if the general access modifier constant appears, the type is an access-to-constant type; otherwise, it is an access-to-variable type. For an access-to-subprogram type, the parameter_profile or parameter_and_result_profile denotes its designated profile. (An access_definition is used in the specification of an access discriminant (see 3.7) or an access parameter (see 6.1)).

13/2 For each (named) access type, there is a literal null which has a null access value designating no entity at all, which can be obtained by (implicitly) converting the literal null to the access type. (The null value of a named access type is the default initial value of the type.) Nonnull Other values of an access-to-object type are obtained by evaluating an attribute_reference for the Access or Unchecked_Access attribute of an aliased view of an object or nonintrinsic subprogram, or, in the case of a named access-to-object type, an allocator, which returns an access value designating a newly created object (see 3.10.2), or in the case of a general access-to-object type, evaluating an attribute_reference for the Access or Unchecked_Access attribute of an aliased view of an object. Nonnull values of an access-to-subprogram type are obtained by evaluating an attribute_reference for the Access attribute of a nonintrinsic subprogram.

This paragraph was deleted. A value of an anonymous access type (that is, the value of an access parameter or access discriminant) cannot be null.

This paragraph was deleted. Reason: Access parameters allow dispatching on the tag of the object designated by the actual parameter (which gets converted to the anonymous access type as part of the call). In order for dispatching to work properly, there had better be such an object. Hence, the type conversion will raise Constraint_Error if the value of the actual parameter is null.
An access value satisfies an exclusion of the null value if it does not equal the null value of its type. An access value does not exclude null.

To be honest: [AI95-00231-01] This means “directly allowed in”; we are not talking about a null exclusion that occurs in an access definition in one of these constructs (for an access definition, the subtype mark in such an access definition is not restricted).

Reason: [AI95-00231-01] This is similar to doubly constraining a composite subtype, which we also don’t allow.

Dynamic Semantics

A composite constraint is compatible with an unconstrained access subtype if it is compatible with the designated subtype. A null exclusion is compatible with any access subtype that does not exclude null. An access value satisfies a composite constraint of an access subtype if it equals the null value of its type or if it designates an object whose value satisfies the constraint. An access value satisfies an exclusion of the null value if it does not equal the null value of its type.

The elaboration of an access_type_definition creates the access type and its first subtype. For an access-to-object type, this elaboration includes the elaboration of the subtype_indication, which creates the designated subtype.
The elaboration of an access_definition creates an anonymous general access-to-variable type [this happens as part of the initialization of an access parameter or access discriminant].

NOTE 1 Access values are called “pointers” or “references” in some other languages.

NOTE 2 Each access-to-object type has an associated storage pool; several access types can share the same pool. An object can be created in the storage pool of an access type by an allocator (see 4.8) for the access type. A storage pool (roughly) corresponds to what some other languages call a “heap”. See 13.11 for a discussion of pools.

NOTE 3 Only index_constraints and discriminant_constraints can be applied to access types (see 3.6.1 and 3.7.1).

Examples of access-to-object types:

- type Frame is access Matrix; -- see 3.6
- type Peripheral_Ref is not null access Peripheral; -- see 3.8.1
- type Binop_Ptr is access all Binary_Operation'Class; -- general access-to-class-wide, see 3.9.1

Example of an access subtype:

- subtype Drum_Ref is Peripheral_Ref(Drum); -- see 3.8.1

Example of an access-to-subprogram type:

- type Message_Procedure is access procedure (M : in String := "Error!");
- procedure Default_Message_Procedure(M : in String);
- ...
- procedure Other_Procedure(M : in String);
- ...
- Give_Message := Other_Procedure'Access;
- ...
- Give_Message("File not found.");
- -- call with parameter (all is optional)
- Give_Message.all; -- call with no parameters

Extensions to Ada 83

The syntax for access_type_definition is changed to support general access types (including access-to-constants) and access-to-subprograms. The syntax rules for general_access_modifier and access_definition are new.

Wording Changes from Ada 83

Amendment Correction:

The rule defining when a current instance of a limited type is considered to be aliased has been tightened to apply only to types that cannot become nonlimited. A program which attempted to take 'Access of the current instance of a limited type that can become nonlimited will be illegal in Ada 2005. While original
Ada 95 allowed the current instance of any limited type to be treated as aliased, this was inconsistently implemented in compilers, and was likely to not work as expected for types that are ultimately nonlimited.

Correction: Static matching (see 4.9.1) requires that both anonymous access types exclude null; and full conformance requires statically matching subtypes. Because of the definition of “excludes null” given in this subclause, an access parameter that designates an untagged private type P (which does not exclude null) does not match its completion if P is completed with a tagged type (in that case, the parameter is controlling and thus excludes null, regardless of whether there is an explicit null exclusion on the body). Similar considerations apply in contexts where mode conformance and subtype conformance are required (for instance, subprogram renaming).

Extensions to Ada 95

The null_exclusion is new. It can be used in both anonymous and named access type definitions. It is most useful to declare that parameters cannot be null, thus eliminating the need for checks on use.

The kinds of anonymous access types allowed were increased by adding anonymous access-to-constant and anonymous access-to-subprogram types. Anonymous access-to-subprogram types used as parameters allow passing of subprograms at any level.

Wording Changes from Ada 95

Corrigendum: Added accidentally-omitted wording that says that a derived access type shares its storage pool with its parent type. This was clearly intended, both because of a note in 3.4, and because anything else would have been incompatible with Ada 83.

Corrigendum: Fixed typographical errors in the description of when access types are constrained.

The wording was fixed to allow allocators and the literal null for anonymous access types. The former was clearly intended by Ada 95; see the Implementation Advice in 13.11.

The rules about aliased objects being constrained by their initial values now apply only to allocated objects, and thus have been moved to 4.8, “Allocators”.

Wording Changes from Ada 2005

Correction: The rule about a current instance being aliased now is worded in terms of immutably limited types. Wording was also added to make extended return object declarations that have the keyword aliased be considered aliased. This latter was a significant oversight in Ada 2005 — technically, the keyword aliased had no effect. But of course implementations followed the intent, not the letter of the Reference Manual.

Explicitly aliased parameters (see 6.1) are defined to be aliased.

Extensions to Ada 2012

Correction: A qualified_expression of an aliased object is now also aliased.

3.10.1 Incomplete Type Declarations

There are no particular limitations on the designated type of an access type. In particular, the type of a component of the designated type can be another access type, or even the same access type. This permits mutually dependent and recursive access types. An incomplete_type_declaration can be used to introduce a type to be used as a designated type, while deferring its full definition to a subsequent full_type_declaration.

Syntax

 incomplete_type_declaration ::= type defining_identifier [discriminant_part] [is tagged];

Static Semantics

An incomplete_type_declaration declares an incomplete view of a type and its first subtype; the first subtype is unconstrained if a discriminant_part appears. If the incomplete_type_declaration includes the reserved word tagged, it declares a tagged incomplete view. If T denotes a
tagged incomplete view, then \textit{T}'Class denotes a tagged incomplete view. [An incomplete view of a type is a limited view of the type (see 7.5).]

\{AI95-00326-01\} Given an access type \textit{A} whose designated type \textit{T} is an incomplete view, a dereference of a value of type \textit{A} also has this incomplete view except when:

\textbf{Discussion}: \{AI05-0208-1\} Whether the designated type is an incomplete view (and thus whether this set of rules applies) is determined by the view of the type at the declaration of the access type; it does not change during the life of the type.

\begin{itemize}
  \item it occurs within the immediate scope of the completion of \textit{T}, or
  \item \{AI05-0208-1\} it occurs within the scope of a nonlimited \texttt{with} clause that mentions a library package in whose visible part the completion of \textit{T} is declared, or
  \item \{AI05-0208-1\} it occurs within the scope of the completion of \textit{T} and \textit{T} is an incomplete view declared by an \texttt{incomplete_type_declaration}.
\end{itemize}

\{AI05-0162-1\} In these cases, the dereference has the full view of \textit{T} visible at the point of the dereference.

\textbf{Discussion}: We need the “in whose visible part” rule so that the second rule doesn’t trigger in the body of a package with a \texttt{with} of a child unit:

{\small
\begin{verbatim}
package P is
  private
    type T;    -- T is access T;
  end P;
private package P.C is
  type PtrT is access T;
  end P.C;
\end{verbatim}
}

\{AI05-0005-1\} \texttt{with} \texttt{P.C};
{\small
\begin{verbatim}
package body P is
  -- P.all'Size is not legal here, but we are within scope of the completion of T.
  -- of a nonlimited with clause for P.
  type T is ... -- P.all'Size is legal here.
  end P;
\end{verbatim}
}

\{AI95-00412-01\} \{AI05-0162-1\} \{AI05-0208-1\} Similarly, if a \texttt{subtype_mark} denotes a \texttt{subtype_declaration} defining a subtype of an incomplete view \textit{T}, the \texttt{subtype_mark} denotes an incomplete view except under the same three circumstances given above, in which case it denotes the full view of \textit{T} visible at the point of the \texttt{subtype_mark}.

\textbf{Legality Rules}

\{AI05-0162-1\} An \texttt{incomplete_type_declaration} requires a completion, which shall be a \texttt{type_declaration} other than an \texttt{incomplete_type_declaration} \texttt{full_type_declaration}. [If the \texttt{incomplete_type_declaration} occurs immediately within either the visible part of a \texttt{package_specification} or a \texttt{declarative_part}, then the \texttt{type_declaration} \texttt{full_type_declaration} shall occur later and immediately within this visible part or \texttt{declarative_part}. If the \texttt{incomplete_type_declaration} occurs immediately within the private part of a given \texttt{package_specification}, then the \texttt{type_declaration} \texttt{full_type_declaration} shall occur later and immediately within either the private part itself, or the \texttt{declarative_part} of the corresponding \texttt{package_body}.]

\textbf{Proof}: This is implied by the next AARM-only rule, plus the rules in 3.11.1, “Completions of Declarations” which require a completion to appear later and immediately within the same declarative region.

\textbf{To be honest}: If the \texttt{incomplete_type_declaration} occurs immediately within the visible part of a \texttt{package_specification}, then the \texttt{completing_type_declaration} \texttt{full_type_declaration} shall occur immediately within this visible part.

\textbf{To be honest}: If the implementation supports it, an \texttt{incomplete_type_declaration} can be imported (using \texttt{aspect Import}, see B.1), in which case no explicit completion is allowed completed by a \texttt{pragma Import}.
If an incomplete_type_declaration includes the reserved word tagged, then a type declaration full_type_declaration that completes it shall declare a tagged type. If an incomplete_type_declaration has a known_discriminant_part, then a type_declaration full_type_declaration that completes it shall have a fully conforming (explicit) known_discriminant_part (see 6.3.1). If an incomplete_type_declaration has no discriminant_part (or an unknown_discriminant_part), then a corresponding type_declaration full_type_declaration is nevertheless allowed to have discriminants, either explicitly, or inherited via derivation.

The only allowed uses of a name that denotes an incomplete_view of a type may be used incomplete_type_declaration are as follows:

- **AI95-00326-01** as the subtype_mark in the subtype_indication of an access_to_object_definition; [the only form of constraint allowed in this subtype_indication is a discriminant_constraint [[a null exclusion is not allowed]];]

  Implementation Note: We now allow discriminant_constraints even if the full type is deferred to the package body. However, there is no particular implementation burden because we have dropped the concept of the dependent compatibility check. In other words, we have effectively repealed AI83-00007.

- **AI95-00326-01** as the subtype_mark in the subtype_indication of a subtype declaration; the subtype_indication shall not have a null exclusion or a constraint defining the subtype of a parameter or result of an access_to_subprogram_definition;

  Reason: [AI95-00326-01] This allows, for example, a record to have a component designating a subprogram that takes that same record type as a parameter.

- **AI95-00326-01** as the subtype_mark defining the subtype of a parameter or result in a profile occurring within a basic_declaration;

  Ramification: But not in the profile for a body or entry.

- **AI95-00326-01** as a generic actual parameter whose corresponding generic formal parameter is a formal incomplete_type (see 12.5.1).

If such a name denotes a tagged incomplete view, it may also be used:

- **AI95-00326-01** as the subtype_mark defining the subtype of a parameter in the profile for a subprogram_body, entry_body, or accept_statement_formal_part;

- **AI95-00326-01** as the prefix of an attribute_reference whose attribute_designator is Class; such an attribute_reference is similarly restricted to the uses allowed here; it denotes a tagged incomplete_view when used in this way, the corresponding full_type_declaration shall declare a tagged type, and the attribute_reference shall occur in the same library unit as the incomplete_type_declaration.

This paragraph was deleted. Reason: [AI95-00326-01] This is to prevent children from imposing requirements on their ancestor library units for deferred incomplete types.

If such a name occurs within the declaration list containing the completion of the incomplete view, it may also be used:

- This paragraph was deleted. [AI95-00326-01] **AI95-0151-1** as the subtype_mark defining the subtype of a parameter or result of an access_to_subprogram_definition.
This paragraph was deleted. Reason: This allows, for example, a record to have a component designating a subprogram that takes that same record type as a parameter.

{AI95-00326-01} If any of the above uses occurs as part of the declaration of a primitive subprogram of the incomplete view, and the declaration occurs immediately within the private part of a package, then the completion of the incomplete view shall also occur immediately within the private part; it shall not be deferred to the package body.

Reason: This fixes a hole in Ada 95 where a dispatching operation with an access parameter could be declared in a private part and a dispatching call on it could occur in a child even though there is no visibility on the full type, requiring access to the controlling tag without access to the representation of the type.

{AI95-00326-01} No other uses of a name that denotes an incomplete view of a type are allowed.

{AI95-00326-01} {AI05-0151-1} A prefix that denotes an object. A dereference (whether implicit or explicit—see 4.1) shall not be of an incomplete view type. An actual parameter in a call shall not be of an untagged incomplete view. The result object of a function call shall not be of an incomplete view. A prefix shall not denote a subprogram having a formal parameter of an untagged incomplete view, nor a return type that is an incomplete view.

Reason: We used to disallow all dereferences of an incomplete type. Now we only disallow such dereferences when used as a prefix. Dereferences used in other contexts do not pose a problem since normal type matching will preclude their use except when the full type is “nearby” as context (for example, as the expected type).

This also disallows prefixes that are directly of an incomplete view. For instance, a parameter P can be declared of a tagged incomplete type, but we don’t want to allow P.Size, P.Alignment, or the like, as representation values aren’t known for an incomplete view.

We say “denotes an object” so that prefixes that directly name an incomplete view are not covered; the previous rules cover such cases, and we certainly don’t want to ban Incomp’Class.

{AI05-0151-1} As subprogram profiles now may include any kind of incomplete type, we also disallow passing objects of untagged incomplete types in subprogram calls (as the parameter passing method is not known as it is for tagged types) and disallow returning any sort of incomplete objects (since we don’t know how big they are).

{AI12-0155-1} The controlling operand or controlling result of a dispatching call shall not be of an incomplete view if the operand or result is dynamically tagged.

Reason: This rule is needed to prevent the following case:

```ada
package Pack is
  type T is tagged;
  function F return access T'Class;
  function G (X : access T) return Integer;
  I : Integer := G (F); -- Illegal by above rule.
end Pack;
```

If this was not illegal, the compiler would have to generate a dispatching call on G without necessarily knowing where the tag of type T is stored (the completion of T might not be until the body of Pack). The fact that any such call will raise Program_Error does not absolve us of detecting the problem; see the Language Design Principles in 13.14.

Static Semantics

{AI95-00326-01} An incomplete_type_declaration declares an incomplete type and its first subtype; the first subtype is unconstrained if a known_discriminant_part appears.

Reason: If an unknown_discriminant_part or no_discriminant_part appears, then the constrainedness of the first subtype doesn’t matter for any other rules or semantics, so we don’t bother defining it. The case with a known_discriminant_part is the only case in which a constraint could later be given in a subtype_indication naming the incomplete type.

Paragraph 11 was deleted.

Dynamic Semantics

The elaboration of an incomplete_type_declaration has no effect.
Reason: An incomplete type has no real existence, so it doesn't need to be "created" in the usual sense we do for other types. It is roughly equivalent to a "forward," declaration in Pascal. Private types are different, because they have a different set of characteristics from their full type.

NOTE 1 {AI12-0447-1} Within a declarative_part, an incomplete_type_declaration and a corresponding full_type_declaration cannot be separated by an intervening body. This is because, by the rules given in 13.14, a type is illegal if it is not to be completely defined before it is frozen, and a body freezes all types declared prior to it in the same declarative_part (see 13.14).

NOTE 2 {AI05-0151-1} {AI05-0269-1} A name that denotes an object of an incomplete view is defined to be of a limited type. Hence, the target of an assignment statement cannot be of an incomplete view.

Examples

Example of a recursive type:

```ada
type Cell;  -- incomplete type declaration
type Link is access Cell;
type Cell is
record
  Value  : Integer;
  Succ   : Link;
  Pred   : Link;
end record;
Head : Link := new Cell'(0, null, null);
Next : Link := Head.Succ;
```

Examples of mutually dependent access types:

```ada
{AI95-00433-01} type Person(<>);    -- incomplete type declaration
type Car is tagged;                -- incomplete type declaration
{AI95-00433-01} type Person_Name is access Person;
type Car_Name is access all Car'Class;
{AI95-00433-01} type Car is tagged
record
  Number  : Integer;
  Owner   : Person_Name;
end record;
type Person(Sex : Gender) is
record
  Name     : String(1 .. 20);
  Birth    : Date;
  Age      : Integer range 0 .. 130;
  Vehicle  : Car_Name;
  case Sex is
    when M => Wife           : Person_Name(Sex => F);
    when F => Husband        : Person_Name(Sex => M);
  end case;
end record;
{AI12-0312-1} My_Car, Your_Car, Next_Car : Car_Name := new Car;  -- see 4.8
CaseyGeorge : Person_Name := new Person(M);
...        
CaseyGeorge.Vehicle := Your_Car;
```

Extensions to Ada 83

The full_type_declaration that completes an incomplete_type_declaration may have a known_discriminant_part even if the incomplete_type_declaration does not.

A discriminant_constraint may be applied to an incomplete type, even if its completion is deferred to the package body, because there is no “dependent compatibility check” required any more. Of course, the constraint can be specified only if a known_discriminant_part was given in the incomplete_type_declaration. As mentioned in the previous paragraph, that is no longer required even when the full type has discriminants.
Dereferences producing incomplete types were not explicitly disallowed in RM83, though AI83-00039 indicated that it was not strictly necessary since troublesome cases would result in Constraint_Error at run time, since the access value would necessarily be null. However, this introduces an undesirable implementation burden, as illustrated by Example 4 of AI83-00039:

```ada
package Pack is
  type Pri is private;
  private
    type Sep;
    type Pri is access Sep;
    X : Pri;
  end Pack;
package body Pack is -- Could be separately compiled!
  type Sep is ...;
  X := new Sep;
end Pack;
pragma Elaborate(Pack);
private package Pack.Child is
  I : Integer := X.all Size; -- Legal, by AI-00039.
end Pack.Child;
```

Generating code for the above example could be a serious implementation burden, since it would require all aliased objects to store size dope, and for that dope to be in the same format for all kinds of types (or some other equivalently inefficient implementation). On the contrary, most implementations allocate dope differently (or not at all) for different designated subtypes.

### Incompatibilities With Ada 95

- **{AI95-00326-01}** It is now illegal to use an incomplete view (type) as the parameter or result of an access-to-subprogram type unless the incomplete view is completed in the same declaration list as the use. This was allowed in Ada 95 for incomplete types where the completion was deferred to the body. By disallowing this rare use of incomplete views, we can allow the use of incomplete views in many more places, which is especially valuable for limited views.

- **{AI95-00326-01}** It is now illegal to use an incomplete view (type) in a primitive subprogram of the type unless the incomplete view is completed in the package specification. This was allowed in Ada 95 for incomplete types where the completion was deferred to the body (the use would have to be in an access parameter). This incompatibility was caused by the fix for the hole noted in Legality Rules above.

### Extensions to Ada 95

- **{AI95-00412-01}** A `subtype_declaration` can be used to give a new name to an incomplete view of a type. This is valuable to give shorter names to entities imported with a limited_with_clause.

### Wording Changes from Ada 95

- **{AI95-00326-01}** The description of incomplete types as incomplete views is new. Ada 95 defined these as separate types, but neglected to give any rules for matching them with other types. Luckily, implementers did the right thing anyway. This change also makes it easier to describe the meaning of a limited view.

### Extensions to Ada 2005

- **{AI05-0098-1}** Correction: Fixed the definition so that an anonymous access-to-subprogram type can use an incomplete view in the same way that a named access-to-subprogram type can.

- **{AI05-0151-1}** Incomplete types now can be used in subprogram declarations. The type has to be complete before any calls or the body is declared. This reduces the places where access types are required for types imported from limited views of packages.

- **{AI05-0162-1}** Incomplete types now can be completed by private types and private extensions. Since this can already happen for limited views, there is no remaining reason to disallow it for explicitly declared incomplete types.

### Wording Changes from Ada 2005

- **{AI05-0208-1}** Correction: Changed the rules of uses of dereferences of incomplete views such that it does not introduce an unintentional incompatibility with Ada 83 and Ada 95.
Incomplete types now can be used as actuals to formal incomplete types (see 12.5.1).

Wording Changes from Ada 2012

Corrigendum: Changed the wording to clarify that the class-wide type associated with a specific tagged type that has an incomplete view is also an incomplete view. While this was previously undefined, an interpretation where it is not an incomplete view leads to semantic nonsense, and thus we don't consider this a potential incompatibility, as compilers most likely are doing the right thing.

Correction: Added a rule preventing a dispatching call on an incomplete type before the completion. This is not an incompatibility as previously this was prevented by the freezing rules. However, that violated the intended design of the freezing rules, so we've now changed to an explicit Legality Rule here, and eliminated the associated freezing rules.

3.10.2 Operations of Access Types

[The attribute Access is used to create access values designating aliased objects and nonintrinsic subprograms. The “accessibility” rules prevent dangling references (in the absence of uses of certain unchecked features — see Clause 13).]

Language Design Principles

It should be possible for an access value to designate an object declared by an object declaration, or a subcomponent thereof. In implementation terms, this means pointing at stack-allocated and statically allocated data structures. However, dangling references should be prevented, primarily via compile-time rules, so long as features like Unchecked_Access and Unchecked_Deallocation are not used.

In order to create such access values, we require that the access type be a general access type, that the designated object be aliased, and that the accessibility rules be obeyed.

Name Resolution Rules

For an attribute_reference with attribute_designator Access (or Unchecked_Access — see 13.10), the expected type shall be a single access type _A such that_; the prefix of such an attribute_reference is never interpreted as an implicit_dereference. If the expected type is an access-to-subprogram type, then the expected profile of the prefix is the designated profile of the access type:

- _A is an access-to-object type with designated type _D and the type of the prefix is _D'Class or is covered by _D, or
- _A is an access-to-subprogram type whose designated profile is type conformant with that of the prefix.

The prefix of such an attribute_reference is never interpreted as an implicit_dereference or a parameterless function_call (see 4.1.4.) The designated type or profile of the expected type of the attribute_reference is the expected type or profile for the prefix.

Discussion: Saying that the expected type shall be a "single access type" is our "new" way of saying that the type has to be determinable from context using only the fact that it is an access type. See 4.2 and 8.6. Specifying the expected profile only implies type conformance. The more stringent subtype conformance is required by a Legality Rule. This is the only Resolution Rule that applies to the name in a prefix of an attribute_reference. In all other cases, the name has to be resolved without using context. See 4.1.4.

Saying “single access type” is a bit of a fudge. Both the context and the prefix may provide both multiple types; “single” only means that a single, specific interpretation must remain after resolution. We say “single” here to trigger the Legality Rules of 8.6. The resolution of an access attribute is similar to that of an assignment_statement. For example:

```ada
type Int_Ptr is access all Integer;
type Char_Ptr is access all Character;
type Float_Ptr is access all Float;

function Zap (Val : Int_Ptr) return Float; -- (1)
function Zap (Val : Float_Ptr) return Float; -- (2)
function Zop return Int_Ptr; -- (3)
function Zop return Char_Ptr; -- (4)
```
3.10.2 Operations of Access Types

The accessibility rules, which prevent dangling references, are written in terms of accessibility levels, which reflect the run-time nesting of masters. As explained in 7.6.1, a master is the execution of a certain construct (called a master construct), such as task body, a block_statement, a subprogram_body, an entry_body, or an accept_statement. An accessibility level is deeper than another if it is more deeply nested at run time. For example, an object declared local to a called subprogram has a deeper accessibility level than an object declared local to the calling subprogram.

The accessibility rules for access types require that the accessibility level of an object designated by an access value be no deeper than that of the access type. This ensures that the object will live at least as long as the access type, which in turn ensures that the access value cannot later designate an object that no longer exists. The Unchecked_Access attribute may be used to circumvent the accessibility rules.

AI95-00162-01 Each master, and each entity and view created by it, has an accessibility level; when two levels are defined to be the same, the accessibility levels of the two associated entities are said to be tied to each other. Accessibility levels are defined as follows:

- The accessibility level of a given master is deeper than that of each dynamically enclosing master, and deeper than that of each master upon which the task executing the given master directly depends (see 9.3).
- An entity or view defined created by a declaration and created as part of its elaboration has the same accessibility level as the innermost enclosing-master of the declaration except in the cases of renaming and derived access types described below. A formal parameter of a function or generic function, a formal parameter of a callable entity, has the same accessibility level as the master representing the invocation of the entity.

AI95-00162-01 This rule defines the “normal” accessibility of entities. In the absence of special rules below, we intend for this rule to apply.

AI95-00162-01 This rule defines the accessibility of all named access types, as well as the accessibility level of all anonymous access types defined by a component_definition other than those for access parameters and access discriminants. Special rules exist for the accessibility level of other such anonymous types. Components, stand-alone objects, and function results whose (anonymous) type is defined by an access_definition have accessibility levels corresponding to named access types defined at the same point.

AI95-00162-01 Because accessibility level is determined by where the access definition is elaborated, for a type extension, the anonymous access types of components (other than access discriminants) inherited from the parent have the same accessibility as they did in the parent; those in the extension part have the accessibility determined by the scope where the type extension is declared. Similarly, the types of the nondiscriminant access components of a derived untagged type have the same accessibility as they did in the parent.

AI95-00162-01 We use “invocation of” in the parameter case as a master is formally an execution of something. But we mean this to be interpreted statically (for instance, as the body of the subprogram) for the purposes of computing “statically deeper than” (see below).
Similarly, an execution of the called function returns a result object is the same as that of the master that elaborated the function body. For any other function, the accessibility level of an aggregate or the result of a function call that is used (in its entirety) to directly initialize part of an object is that of the object being initialized. In other contexts, the accessibility level of an aggregate or the result of a function call is that of the innermost master that evaluates the aggregate or function call/expression of the called function. Corresponding rules apply to a value conversion (see 4.6).

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** Note that accessibility can differ depending on the view of an object (for both static and dynamic accessibility). For instance, the accessibility level of a formal parameter may be different than the accessibility level of the corresponding actual parameter. This occurs in other cases as well.

- **AI95-00318-02** The accessibility level of a view conversion, qualified_expression, or parenthesized_expression is the same as that of the operand.

- **AI05-0188-1** The accessibility level of a conditional_expression (see 4.5.7) is the accessibility level of the evaluated dependent_expression.

- **AI12-0236-1** The accessibility level of a declare_expression (see 4.5.9) is the accessibility level of the body_expression.

- **AI95-00318-02** The accessibility level of a view conversion, qualified_expression, or parenthesized_expression is the same as that of the renamed view, unless the renaming is of a formal subprogram, in which case the accessibility level is that of the instance.

- **Reason:** We restrict the above rule to apply only if the function result is declared to be of a composite type. This makes sense since only results of a composite type (or of an anonymous access type, which are handled separately below) are potentially affected by the master of the function call. Note that a private type is considered composite, so this result assumes the worst for a function returning a private type. We could have made the rule more complex, depending on whether the result might be built in place, or might have an access discriminant, but we chose to keep the rule simpler. The wording says “the result type at the point of function declaration is a composite type”, to make it clear that this depends on the properties at the point of the declaration of the function, rather than properties that might be known at the point of call or inside the function body.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Ramification:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.

- **Reason:** We define the (dynamic) accessibility of formal parameters in order that it does not depend on the parameter passing model (by-reference or by-copy) as that is implementation defined. Otherwise, there would be a portability issue.
This paragraph was deleted. If the result is of an anonymous access type and defines an access discriminant, the master is the same as that for an object created by an anonymous allocator that defines an access discriminant (even if the access result is of an access to subprogram type).

If the call itself defines the result of a function to which one of the above rules applies, or has an accessibility level that is tied to the result of such a function \( F \), then the master of the call is that of the master of the call invoking \( F \) these rules are applied recursively.

In other cases, the master of the call is that of the innermost master that evaluates the function call.

Ramification: The “innermost master which evaluated the function call” does not include the function call itself (which might be a master).

We really mean the innermost master here, which could be a very short lifetime. Consider a function call used as a parameter of a procedure call. In this case the innermost master which evaluated the function call is the procedure call.

These rules do not mention whether the result object is built-in-place (see 7.6). In particular, in the case where building in place is optional, the choice whether or not to build-in-place has no effect on masters, lifetimes, or accessibility.

There are several cases where the implementation may have to pass in the accessibility level of the result object on a call, to support later rules where the accessibility level comes from the master of the call:

- when the function result may have a part with access discriminants;
- when the function result type is an anonymous access type;
- when the function result is built-in-place;
- when the function has an explicitly aliased parameter.

In particular, this implies passing a level parameter when the result type is class-wide, since descendants may add access discriminants. For most implementations this will mean that functions with controlling results will also need a level parameter.

In the case of a call to a function whose result type is an anonymous access type, the accessibility level of the type of the result of the function call is also determined by the point of call as described above.

Within a return statement, the accessibility level of the return object is that of the execution of the return statement. If the return statement completes normally by returning from the function, then prior to leaving the function, the accessibility level of the return object changes to be a level determined by the point of call, as does the level of any coextensions (see below) of the return object.

We define the accessibility level of the return object during the return statement to be that of the return statement itself so that the object may be designated by objects local to the return statement, but not by objects outside the return statement. In addition, the intent is that the return object gets finalized if the return statement ends without actually returning (for example, due to propagating an exception, or a goto). For a normal return, of course, no finalization is done before returning.

The accessibility level of a derived access type is the same as that of its ultimate ancestor.

The accessibility level of the anonymous access type defined by an access definition of an object renaming declaration is the same as that of the renamed view.

The accessibility level of the anonymous access type defined by an access definition of a loop parameter subtype indication is that of the loop parameter.

The accessibility level of the anonymous access type of an access discriminant in the subtype indication or qualified expression of an allocator, or in the expression or return subtype indication of a return statement is determined as follows: is the same as that of the containing object or associated constrained subtype.
• If the value of the access discriminant is determined by a discriminant association in a 
  subtype indication, the accessibility level of the object or subprogram designated by the
  associated value (or library level if the value is null);

  **Discussion:** This deals with the following cases, when they occur in the context of an allocator or return statement:
  • An extension aggregate where the ancestor part is a subtype mark denoting a constrained subtype;
  • An uninitialized allocator where the subtype indication defines a constrained subtype;
  • A discriminant of an object with a constrained nominal subtype, including constrained components, the result
    of calling a function with a constrained result subtype, the dereference of an access-to-constrained subtype,
    etc.

  **Ramification:** {AI05-0281-1} The subtype indication mentioned in this bullet is not necessarily the one given in the
  allocator or return statement that is determining the accessibility level; the constrained subtype might have been
  defined in an earlier declaration (as a named subtype).

  {AI05-0005-1} If the value for this rule and the next one is derived from an Unchecked Access attribute, the
  accessibility is library-level no matter what the accessibility level of the object is (see 13.10).

• {AI05-0234-1} If the value of the access discriminant is determined by a default expression
  in the declaration of the discriminant, the level of the object or subprogram designated by the
  associated value (or library level if null);

  **Discussion:** This covers the case of an unconstrained subcomponent of a limited type with defaulted access
  discriminants.

• {AI05-0004-1} If the value of the access discriminant is determined by a
  record_component_association in an aggregate, the accessibility level of the object or subprogram designated by the
  associated value (or library level if the value is null);

  **Discussion:** In this bullet, the aggregate has to occur in the context of an allocator or return statement, while the
  subtype indication of the previous bullet can occur anywhere (it doesn't have to be directly given in the allocator or
  return statement).

• In other cases, where the value of the access discriminant is determined by an object with an
  unconstrained nominal subtype, the accessibility level of the object.

  **Discussion:** {AI95-00416-01} In other words, if you know the value of the discriminant for an allocator or return
  statement from a discriminant constraint or an aggregate component association, then that determines the accessibility
  level; if you don't know it, then it is based on the object itself.

• {AI95-00416-01} The accessibility level of the anonymous access type of an access discriminant
  in any other context is that of the enclosing object.

• {AI95-00162-01} {AI95-00254-01} {AI05-0270-1} The accessibility level of the anonymous access type of an access parameter specifying an access-to-object type
  is the same as that of the view designated by the actual (or library-level if the actual is null). If the actual is an allocator,
  this is the accessibility level of the execution of the called subprogram.

  **Ramification:** {AI05-0005-1} If the value of the actual is derived from an Unchecked Access attribute, the
  accessibility is always library-level (see 13.10).

• {AI95-00254-01} The accessibility level of the anonymous access type of an access parameter
  specifying an access-to-subprogram type is deeper than that of any master; all such anonymous
  access types have this same level.

  **Reason:** These represent “downward closures” and thus require passing of static links or global display information
  (along with generic sharing information if the implementation does sharing) along with the address of the subprogram.
  We must prevent conversions of these to types with “normal” accessibility, as those typically don't include the extra
  information needed to make a call.

• {AI12-0070-1} The accessibility level of the anonymous access subtype defined by a
  return_subtype_indication that is an access_definition (see 6.5) is that of the result subtype of
  the enclosing function.
The accessibility level of the type of a stand-alone object of an anonymous access-to-object type is the same as the accessibility level of the type of the access value most recently assigned to the object; accessibility checks ensure that this is never deeper than that of the declaration of the stand-alone object.

**Proof:** The accessibility level of an object created by an allocator is the same as that of the access type, except for an allocator of an anonymous access type (an anonymous allocator) in certain contexts, as follows: For an anonymous allocator that defines the result of a function with an access result, the accessibility level is determined as though the allocator were in place of the call of the function; in the special case of a call that is the operand of a type conversion, the level is that of the target access type of the conversion that defines the value of an access parameter or an access discriminant. For an anonymous allocator defining the value of an access parameter, the accessibility level is that of the innermost master of the call. For an anonymous allocator whose type is that of a stand-alone object of an anonymous access-to-object type, the accessibility level is that of the declaration of the stand-alone object.

**Ramification:** The rules of access discriminants are such that when the space for an object with a coextension is reclaimed, the space for the coextensions can be reclaimed. Hence, there is implementation advice (see 13.11) that an object and its coextensions all be allocated from the same storage pool (or stack frame, in the case of a declared object).

Within a return statement, the accessibility level of the anonymous access type of an access result is that of the master of the call.

The accessibility level of a view of an object or subprogram designated by a dereference of an access value is the same as that of the access type.

This rule applies even when no dereference exists, for example when an access value is passed as an access parameter. This rule ensures that implementations are not required to include dynamic accessibility values with all access values.

The accessibility level of a component, protected subprogram, or entry of (a view of) a composite object is the same as that of (the view of) the composite object.
One accessibility level is defined to be **statically deeper** than another in the following cases:

- **[AI12-0406-1]** For a master **construct** that is statically nested within another master **construct**, the accessibility level of the inner master **construct** is statically deeper than that of the outer master **construct**.

  *This paragraph was deleted.*

**To be honest**: **[AI12-0406-1]** Strictly speaking, this should talk about the constructs (such as **subprogram bodies**) being statically nested within one another; the masters are really the **executions** of those constructs.

**To be honest**: If a given accessibility level is statically deeper than another, then each level defined to be the same as the given level is statically deeper than each level defined to be the same as the other level.

- **[AI95-00254-01]** The accessibility level of the anonymous access type of an access parameter specifying an access-to-subprogram type is statically deeper than that of any master; all such anonymous access types have this same level.

  **Ramification**: This rule means that it is illegal to convert an access parameter specifying an access to subprogram to a named access to subprogram type, but it is allowed to pass such an access parameter to another access parameter (the implicit conversion's accessibility will succeed).

- **[AI95-00254-01] [AI05-0082-1] [AI12-0406-1]** The statically deeper relationship does not apply to the accessibility level of the **following**: anonymous access type of an access parameter specifying an access-to-object type nor does it apply to a descendant of a generic formal type; that is, such an accessibility level is not considered to be statically deeper, nor statically shallower, than any other.

  - **[AI12-0406-1]** the anonymous type of an access parameter specifying an access-to-object type;
  - **[AI12-0406-1]** the type of a stand-alone object of an anonymous access-to-object type;
  - **[AI12-0392-1] [AI12-0406-1]** a **raise expression**;
  - **[AI12-0406-1]** a descendant of a generic formal type;
  - **[AI12-0406-1]** a descendant of a type declared in a generic formal package.

  **[AI05-0148-1] [AI12-0406-1]** When the statically deeper relationship does not apply, the **The statically deeper relationship does not apply to the accessibility level of the type of a stand-alone object of an anonymous access-to-object type; that is, such an accessibility level is not considered to be statically deeper, nor statically shallower, than any other.**

  **Ramification**: **[AI12-0005-1]** In these cases, no static accessibility checks are made, and we use dynamic accessibility checks to prevent problems.

- **This paragraph was deleted.** **[AI05-0142-4] [AI05-0235-1] [AI12-0089-1] [AI12-0157-1] [AI12-0277-1] [AI12-0324-1] [AI12-0392-1]** Inside a return statement that applies to a function or generic function $F$, or inside the return expression of an expression function $F$, when determining whether the accessibility level of an explicitly aliased parameter of $F$ is statically deeper than the level of the return object of $F$, the level of the return object is considered to be the same as that of the level of the explicitly aliased parameter, for statically comparing with the level of other...
entities, an explicitly aliased parameter of \( F \) is considered to have the accessibility level of a parameter of \( F \) that is not explicitly aliased the body of \( F \).

- \{AI05-0051-1\} \{AI05-0234-1\} \{AI05-0235-1\} \{AI12-0089-1\} \{AI12-0157-1\} \{AI12-0372-1\}

When within a function body or the return expression of an expression function, the accessibility level of the master representing an execution of the function, for determining whether a level is statically deeper than that of the master of the function call invoking that execution, independent of how the master of the function call is determined (see above), the level of the anonymous access type of an access result of a function or generic function \( F \), when within a return statement that applies to \( F \) or the return expression of expression function \( F \), the level of the master of the call is presumed to be the same as that of the level of the master that elaborated the function body of \( F \).

This paragraph was deleted.

- \{AI05-0051-1\} \{AI12-0345-1\} This rule has no effect if the previous bullet also applies (that is, the “a level” is of an explicitly aliased parameter).

\{AI12-0005-1\} “Function body” includes bodies of generic functions.

- \{AI12-0445-1\} [For determining whether one level is statically deeper than another when within a generic package body, the generic package is presumed to be instantiated at the same level as where it was declared; runtime checks are required in the case of more deeply nested instantiations.]

- **Proof:** \{AI05-0082-1\} A generic package does not introduce a new master, so it has the static level of its declaration; the rest follows from the other “statically deeper” rules.

- **Ramification:** In other words, the rules are checked at compile time of the type_declaration, in an assume-the-worst manner.

\{AI12-0345-1\} Notwithstanding other rules given above, the accessibility level of an entity that is tied to that of an explicitly aliased formal parameter of an enclosing function is considered (both statically and dynamically) to be the same as that of an entity whose accessibility level is tied to that of the return object of that function.

- **Ramification:** This rule only applies when the level of an explicitly aliased parameter of a function is compared to that of the return object of the function. If a value designating the explicitly aliased parameter is created and stored in a stand-alone object or passed as a parameter, this special property is lost (even for the dynamic accessibility of anonymous access types in these contexts).

\{AI12-0345-1\} Implementation Note: When this rule applies, no dynamic accessibility check should be made, even when one would normally be part of the execution of the construct. All places where this rule applies are known at compile-time.

The accessibility level of all library units is called the library level; a library-level declaration or entity is one whose accessibility level is the library level.

- **Ramification:** Library_unit_declarations are library level. Nested declarations are library level if they are nested only within packages (possibly more than one), and not within subprograms, tasks, etc.

- **To be honest:** The definition of the accessibility level of the anonymous type of an access parameter specifying an access-to-object type cheats a bit, since it refers to the view designated by the actual, but access values designate objects, not views of objects. What we really mean is the view that “would be” denoted by an expression “\( X.all \)”, where \( X \) is the actual, even though such an expression is a figment of our imagination. The definition is intended to be equivalent to the following more verbose version: The accessibility level of the anonymous type of an access parameter is as follows:

  - if the actual is an expression of a named access type — the accessibility level of that type;
  - if the actual is an allocator — the accessibility level of the execution of the called subprogram;
  - if the actual is a reference to the Access attribute — the accessibility level of the view denoted by the prefix \( \text{prefix} \);
  - if the actual is a reference to the Unchecked_Access attribute — library accessibility level;
• if the actual is an access parameter — the accessibility level of its type.

Note that the allocator case is explicitly mentioned in the RM95, because otherwise the definition would be circular: the level of the anonymous type is that of the view designated by the actual, which is that of the access type.

**Discussion:** A deeper accessibility level implies a shorter maximum lifetime. Hence, when a rule requires X to have a level that is “not deeper than” Y’s level, this requires that X has a lifetime at least as long as Y. (We say “maximum lifetime” here, because the accessibility level really represents an upper bound on the lifetime; an object created by an allocator can have its lifetime prematurely ended by an instance of Unchecked_Deallocation.)

Package elaborations are not masters, and are therefore invisible to the accessibility rules: an object declared immediately within a package has the same accessibility level as an object declared immediately within the declarative region containing the package. This is true even in the body of a package; it jibes with the fact that objects declared in a package_body live as long as objects declared outside the package, even though the body objects are not visible outside the package.

Note that the level of the view denoted by X.all can be different from the level of the object denoted by X.all. The former is determined by the type of X; the latter is determined either by the type of the allocator, or by the master in which the object was declared. The former is used in several Legality Rules and runtime checks; the latter is used to define when X.all gets finalized. The level of a view reflects what we can conservatively “know” about the object of that view; for example, due to type conversions, an access value might designate an object that was allocated by an allocator for a different access type.

Similarly, the level of the view denoted by X.all.Comp can be different from the level of the object denoted by X.all.Comp. If Y is statically deeper than X, this implies that Y will be (dynamically) deeper than X in all possible executions.

Most accessibility checking is done at compile time; the rules are stated in terms of “statically deeper than”. The exceptions are:

• Checks involving access parameters of an access-to-object type. The fact that “statically deeper than” is not defined for the anonymous access type of an access parameter implies that any rule saying “shall not be statically deeper than” does not apply to such a type, nor to anything defined to have “the same” level as such a type.

• \[\text{AI05-0082-1}\] Checks involving generic formal types and their descendants. This is because the actual type can be more or less deeply nested than the generic unit. Note that this only applies to the generic unit itself, and not to the instance. Any static checks needed in the instance will be performed. Any other checks (such as those in the generic body) will require a run-time check of some sort (although implementations that macro-expand generics can determine the result of the check when the generic is expanded).

• \[\text{AI05-0082-1}\] Checks involving other entities and views within generic packages. This is because an instantiation can be at a level that is more deeply nested than the generic package itself. In implementations that use a macro-expansion model of generics, these violations can be detected at macro-expansion time. For implementations that share generics, run-time code is needed to detect the error.

• \[\text{AI95-00318-02}\] \{AI95-00344-01\} \{AI95-00416-01\} Checks during function return and allocators, for nested type extensions and access discriminants.

\[\text{AI05-0005-1}\] Note that runtime checks are not required for access discriminants (except during function returns and allocators), because their accessibility is determined statically by the accessibility level of the enclosing object.

*This-The accessibility level of the result object of a function reflects the time when that object will be finalized; we don’t allow pointers to the object to survive beyond that time.

We sometimes use the terms “accessible” and “inaccessible” to mean that something has an accessibility level that is not deeper, or deeper, respectively, than something else.

**Implementation Note:** \[\text{AI95-00318-02}\] \{AI95-00344-01\} \{AI95-00416-01\} If an accessibility Legality Rule is satisfied, then the corresponding runtime check (if any) cannot fail (and a reasonable implementation will not generate any checking code) unless one of the cases requiring runtime checks mentioned previously is access parameters or shared generic bodies are involved.

Accessibility levels are defined in terms of the relations “the same as” and “deeper than”. To make the discussion more concrete, we can assign actual numbers to each level. Here, we assume that library-level accessibility is level 0, and each level defined as “deeper than” is one level deeper. Thus, a subprogram directly called from the environment task (such as the main subprogram) would be at level 1, and so on.

Accessibility is not enforced at compile time for access parameters of an access-to-object type. The “obvious” implementation of the runtime checks would be inefficient, and would involve distributed overhead; therefore, an efficient method is given below. The “obvious” implementation would be to pass the level of the caller at each subprogram call, task creation, etc. This level would be incremented by 1 for each dynamically nested master. An Accessibility Check would be implemented as a simple comparison — checking that X is not deeper than Y would involve checking that \(X \leq Y\).
A more efficient method is based on passing static nesting levels (within constructs that correspond at run time to masters — packages don't count). Whenever an access parameter is passed, an implicit extra parameter is passed with it. The extra parameter represents (in an indirect way) the accessibility level of the anonymous access type, and, therefore, the level of the view denoted by a dereference of the access parameter. This is analogous to the implicit “Constrained” bit associated with certain formal parameters of an unconstrained but definite composite subtype. In this method, we avoid distributed overhead: it is not necessary to pass any extra information to subprograms that have no access parameters. For anything other than an access parameter and its anonymous type, the static nesting level is known at compile time, and is defined analogously to the RM95 definition of accessibility level (e.g. derived access types get their nesting level from their parent). Checking “not deeper than” is a "<=" test on the levels.

For each access parameter of an access-to-object type, the static depth passed depends on the actual, as follows:

- If the actual is an expression of a named access type, pass the static nesting level of that type.
- If the actual is an allocator, pass the static nesting level of the caller, plus one.
- If the actual is a reference to the Access attribute, pass the level of the view denoted by the prefix.
- If the actual is a reference to the Unchecked_Access attribute, pass 0 (the library accessibility level).
- If the actual is an access parameter of an access-to-object type, usually just pass along the level passed in. However, if the static nesting level of the formal (access) parameter is greater than the static nesting level of the actual (access) parameter, the level to be passed is the minimum of the static nesting level of the access parameter and the actual level passed in.

For the Accessibility_Check associated with a type_conversion of an access parameter of an access-to-object type of a given subprogram to a named access type, if the target type is statically nested within the subprogram, do nothing; the check can't fail in this case. Otherwise, check that the value passed in is <= the static nesting depth of the target type. The other Accessibility_Checks are handled in a similar manner.

This method, using statically known values most of the time, is efficient, and, more importantly, avoids distributed overhead.

Examples of accessibility:

```ada
|{AI05-0005-1} package body Lib_Unit is
|  type T is tagged ...;
|  type A0 is access all T;
|  A1 is access all T;
|  A0 := Global; -- OK
|  A1 := X'Access; -- OK
|begin
|  P := A0(P1); -- Illegal type conversion!
|  P := A0(P1); -- Illegal reference to Access attribute!
|  P := A0(P1); -- Illegal reference to Access attribute!
|end P;
|end Lib_Unit;
```

The above illegal statements are illegal because the accessibility level of X and Y are statically deeper than the accessibility level of A0. In every possible execution of any program including this library unit, if P is called, the accessibility level of X will be (dynamically) deeper than that of A0. Note that the accessibility levels of X and Y are the same.
Here's an example involving access parameters of an access-to-object type:

```ada
procedure Main is
  type Level_1_Type is access all Integer;
  procedure P(X: access Integer) is
    type Nested_Type is access all Integer;
  begin
    ... Nested_Type(X) ... -- (1)
    ... Level_1_Type(X) ... -- (2)
  end P;
  procedure Q(X: access Integer) is
    procedure Nested(X: access Integer) is
      begin
        P(X);
      end Nested;
  begin
    Nested(X);
  end Q;
  procedure R is
    Level_2: aliased Integer;
  begin
    Q(Level_2'Access); --(3)
  end R;
  end Main;
```

The run-time Accessibility_Check at (1) can never fail, and no code should be generated to check it. The check at (2) will fail when called from (3), but not when called from (4).

Within a type_declaration, the rules are checked in an assume-the-worst manner. For example:

```ada
{AI05-0298-1} package P is
  type Int_Ptr is access all Integer;
  type Rec(D: access Integer) is limited private;
  private
    type Rec_Ptr is access all Rec;
    function F(X: Rec_Ptr) return Boolean;
    function G(X: access Rec) return Boolean;
    type Rec(D: access Integer) is limited record
      C1: Int_Ptr := Int_Ptr(D); -- Illegal!
      C2: Rec_Ptr := Rec'Access; -- Illegal!
      C3: Boolean := F(Rec'Access); -- Illegal!
      C4: Boolean := G(Rec'Access);
    end record;
  end P;
```

C1, C2, and C3 are all illegal, because one might declare an object of type Rec at a more deeply nested place than the declaration of the type. C4 is legal, but the accessibility level of the object will be passed to function G, and constraint checks within G will prevent it from doing any evil deeds.

Note that we cannot defer the checks on C1, C2, and C3 until compile-time of the object creation, because that would cause violation of the privacy of private parts. Furthermore, the problems might occur within a task or protected body, which the compiler can't see while compiling an object creation.

The following attribute is defined for a prefix X that denotes an aliased view of an object:

**X'Access**

```ada
{8652/00100} {AI95-00127-01} X'Access yields an access value that designates the object denoted by X. The type of X'Access is an access-to-object type, as determined by the expected type. The expected type shall be a general access type. X shall denote an aliased view of an object[, including possibly the current instance (see 8.6) of a limited type within its definition, or a formal parameter or generic formal object of a tagged type]. The view denoted by the prefix X shall satisfy the following additional requirements, presuming the expected type for X'Access is the general access type A with designated type D:
```
• If \( A \) is an access-to-variable type, then the view shall be a variable; [on the other hand, if \( A \) is an access-to-constant type, the view may be either a constant or a variable.]

**Discussion:** The current instance of a limited type is considered a variable.

• {AI95-00363-01} {AI05-0008-1} {AI05-0041-1} The view shall not be a subcomponent that depends on discriminants of an object unless the object is known to be constrained, a variable whose nominal subtype is unconstrained, unless this subtype is indefinite, or the variable is constrained by its initial value aliased.

**Discussion:** This restriction is intended to be similar to the restriction on renaming discriminant-dependent subcomponents.

**Reason:** This prevents references to subcomponents that might disappear or move or change constraints after creating the reference.

**Implementation Note:** There was some thought to making this restriction more stringent, roughly: "\( X \) shall not denote a subcomponent of a variable with discriminant-dependent subcomponents, if the nominal subtype of the variable is an unconstrained definite subtype.” This was because in some implementations, it is not just the discriminant-dependent subcomponents that might move as the result of an assignment that changed the discriminants of the enclosing object. However, it was decided not to make this change because a reasonable implementation strategy was identified to avoid such problems, as follows:

- Place nondiscriminant-dependent components with any aliased parts at offsets preceding any discriminant-dependent components in a discriminated record type with defaulted discriminants.
- Preallocate the maximum space for unconstrained discriminated variables with aliased subcomponents, rather than allocating the initial size and moving them to a larger (heap-resident) place if they grow as the result of an assignment.

Note that for objects of a by-reference type, it is not an error for a programmer to take advantage of the fact that such objects are passed by reference. Therefore, the above approach is also necessary for discriminated record types with components of a by-reference type.

To make the above strategy work, it is important that a component of a derived type is defined to be discriminant-dependent if it is inherited and the parent subtype constraint is defined in terms of a discriminant of the derived type (see 3.7).

• {8652/0010} {AI95-00127-01} {AI95-00363-01} If \( A \) is a named access type and \( D \) is a tagged type, the designated type of \( A \) is tagged, then the type of the view shall be covered by \( D \); the designated type of \( A \) is tagged, then the type of the view shall be either \( D’ \) class or a type covered by \( D \); if \( D \) is untagged, \( D’ \) is not tagged, then the type of the view shall be \( D \); the same, and either: either \( D’ \)’s designated subtype shall either statically match the nominal subtype of the view or be, or the designated subtype shall be discriminated and unconstrained.

- {AI95-00363-01} the designated subtype of \( A \) shall statically match the nominal subtype of the view; or

- {AI95-00363-01} {AI05-0041-1} {AI12-0095-1} \( D \) shall be discriminated in its full view and unconstrained in any partial view, and the designated subtype of \( A \) shall be unconstrained. For the purposes of determining within a generic body whether \( D \) is unconstrained in any partial view, a discriminated subtype is considered to have a constrained partial view if it is a descendant of an untagged generic formal private or derived type.

**Implementation Note:** This ensures that the dope for an aliased array object can always be stored contiguous with it, but need not be if its nominal subtype is constrained.

**Ramification:** {8652/0010} {AI95-00127-01} An access attribute can be used as the controlling operand in a dispatching call; see 3.9.2.

{AI95-00363-01} This does not require that types have a partial view in order to allow an access attribute of an unconstrained discriminated object, only that any partial view that does exist is unconstrained.

**Discussion:** {AI12-0095-1} We assume the worst in a generic body whether or not a formal subtype has a constrained partial view; specifically, in a generic body a discriminated subtype is considered to have a constrained partial view if
it is a descendant of an untagged generic formal private or derived type (see 12.5.1 for the formal definition of this rule).

- **{AI05-0041-1}** The accessibility level of the view shall not be statically deeper than that of the access type \( A \). In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

**Ramification:** In an instance body, a runtime check applies.

{AI95-00230-01} If \( A \) is an anonymous access-to-object type of an access parameter, access type, then the view can never have a deeper accessibility level than \( A \). The same is true for an anonymous access-to-object type of an access discriminant, except when X'Access is used to initialize an access discriminant of an object created by an allocator. The latter case is illegal if the accessibility level of X is statically deeper than that of the access type of the allocator; a runtime check is needed in the case where the initial value comes from an access parameter. Other anonymous access-to-object types have "normal" accessibility checks.

**Discussion:** {AI12-0363-1} Additional restrictions exist in the specialized needs annexes. For instance, C.6 includes additional restrictions on atomic and volatile prefixes of the Access attribute.

**{AI05-0041-1}** In addition to the places where Legality Rules normally apply (see 12.3), these requirements apply also in the private part of an instance of a generic unit.

A check is made that the accessibility level of X is not deeper than that of the access type \( A \). If this check fails, Program_Error is raised.

**Ramification:** The check is needed for access parameters of an access-to-object type and in instance bodies.

**{AI05-0024-1}** Because there are no access parameters permitted for task entries, the accessibility levels are always comparable. We would have to switch to the terminology used in 4.8 and 6.5 based on inclusion within masters if we relax this restriction. That might introduce unacceptable distributed overhead.

**Implementation Note:** {AI05-0148-1} This check requires that some indication of lifetime is passed as an implicit parameter along with access parameters of an access-to-object type. A similar indication is required for stand-alone objects of anonymous access-to-object types. No such requirement applies to other anonymous access types, since the checks associated with them are all compile-time checks.

**{AI12-0439-1}** If the nominal subtype of X does not statically match the designated subtype of \( A \), a view conversion of X to the designated subtype is evaluated (which can raise Constraint_Error — see 4.6) and the value of X'Access designates that view.

The following attribute is defined for a prefix P that denotes a subprogram:

**P'Access**

**{AI95-00229-01}** \{AI95-00254-01\} \{AI05-0239-1\} \{AI12-0064-2\} P'Access yields an access value that designates the subprogram denoted by P. The type of P'Access is an access-to-subprogram type \( S \), as determined by the expected type. The accessibility level of P shall not be statically deeper than that of \( S \). If \( S \) is nonblocking, P shall be nonblocking. In addition to the places where Legality Rules normally apply (see 12.3), these rules apply also in the private part of an instance of a generic unit. The profile of P shall be subtype_conformant with the designated profile of \( S \), and shall not be intrinsic. If the subprogram denoted by P is declared within a generic unit, and the expression P'Access occurs within the body of that generic unit or within the body of a generic unit declared within the declarative region of the generic unit, then the ultimate ancestor of \( S \) shall be either a nonformal type declared within the generic unit or an anonymous access type of an access parameter body, \( S \) shall be declared within the generic body.

**Discussion:** {AI95-00229-01} The part about generic bodies is worded in terms of the denoted subprogram, not the denoted view; this implies that renaming is invisible to this part of the rule. "Declared within the declarative region of the generic" is referring to child and nested generic units. This rule is partly to prevent contract model problems with respect to the accessibility rules, and partly to ease shared-generic-body implementations, in which a subprogram declared in an instance needs to have a different calling convention from other subprograms with the same profile.

Overload resolution ensures only that the profile is type_conformant. This rule specifies that subtype conformance is required (which also requires matching calling conventions). P cannot denote an entry because access-
to-subprogram types never have the entry calling convention. P cannot denote an enumeration literal or an attribute function because these have intrinsic calling conventions.

**Legality Rules**

32.1/3  
\{AI05-0188-1\}  
An expression is said to have distributed accessibility if it is

32.2/3  
- a conditional expression (see 4.5.7); or

32.3/5  
- \{AI12-0236-I\} a declare expression (see 4.5.9) whose body expression has distributed accessibility; or

32.4/5  
- a view conversion, qualified expression, or parenthesized expression whose operand has distributed accessibility.

32.5/5  
\{AI05-0188-1\} The statically deeper relationship does not apply to the accessibility level of an expression having distributed accessibility; that is, such an accessibility level is not considered to be statically deeper, nor statically shallower, than any other.

32.6/5  
\{AI05-0188-1\} Any static accessibility requirement that is imposed on an expression that has distributed accessibility (or on its type) is instead imposed on the dependent expressions of the underlying conditional expression. This rule is applied recursively if a dependent expression also has distributed accessibility.

**Discussion:** This means that any Legality Rule requiring that the accessibility level of an expression (or that of the type of an expression) shall or shall not be statically deeper than some other level also applies, in the case where the expression has distributed accessibility, to each dependent expression of the underlying conditional expression.

33  
NOTE 1 The Unchecked_Access attribute yields the same result as the Access attribute for objects, but has fewer restrictions (see 13.10). There are other predefined operations that yield access values; an allocator can be used to create an object, and return an access value that designates it (see 4.8); evaluating the literal null yields a null access value that designates no entity at all (see 4.2).

34/2  
NOTE 2 \{AI95-00230-01\} The predefined operations of an access type also include the assignment operation, qualification, and membership tests. Explicit conversion is allowed between general access types with matching designated subtypes; explicit conversion is allowed between access-to-subprogram types with subtype conformant profiles (see 4.6). Named access types have predefined equality operators; anonymous access types do not but they can use the predefined equality operators for universal access (see 4.5.2).

34.a/2  
Reason: \{AI95-00230-01\} Anonymous access types can use the universal access equality operators declared in Standard, while named access types cannot for compatibility reasons. By not having equality operators for anonymous access types, we eliminate the need to specify exactly where the predefined operators for anonymous access types would be defined, as well as the need for an implementer to insert an implicit declaration for "=", etc. at the appropriate place in their symbol table. Note that ".=". "Access" and ".all" are defined, and ".null" is defined though useless since all instances are constant. The literal null is also defined for the purposes of overload resolution, but is disallowed by a Legality Rule of this subclause.

35  
NOTE 3 The object or subprogram designated by an access value can be named with a dereference, either an explicit_dereference or an implicit_dereference. See 4.1.

36  
NOTE 4 A call through the dereference of an access-to-subprogram value is never a dispatching call.

36.a  
Proof: See 3.9.2.

36/5  
NOTE 5 \{AI95-00254-01\} \{AI12-0440-I\} \{AI12-0451-I\} The accessibility rules imply that it is not possible to use the Access attribute for subprograms and parameters of an anonymous access-to-subprogram type can be used together to implement “downward closures” — that is, to pass a more-nested subprogram as a parameter to a less-nested subprogram, as can be appropriate for example for an iterator abstraction or numerical integration. Downward closure can also be implemented using generic formal subprograms (see 12.6). Unlike for objects, there is no Note that Unchecked_Access is not allowed for subprograms.

38/5  
NOTE 6 \{AI12-0451-I\} Using an access-to-class-wide tagged type with a dispatching operation is a potentially more structured alternative to using an access-to-subprogram type.

39/5  
NOTE 7 \{AI12-0442-I\} An implementation can consider two access-to-subprogram values to be unequal, even though they designate the same subprogram. For instance, this can happen if two values point to a special prologue that performs an Elaboration_Check and then jumps to the subprogram.
**Ramification:** If equality of access-to-subprogram values is important to the logic of a program, a reference to the Access attribute of a subprogram should be evaluated only once and stored in a global constant for subsequent use and equality comparison.

**Examples**

**Example of use of the Access attribute:**

```
{AI12-0312-1} BeckyMartha : Person_Name := new Person(F);  -- see 3.10.1
Cars       : array (1..2) of aliased Car;
          ...
BeckyMartha.Vehicle := Cars(1)'Access;
CaseyGeorge.Vehicle := Cars(2)'Access;
```

**Examples**

**Extensions to Ada 83**

We no longer make things like "Last and "component" (basic) operations of an access type that need to be "declared" somewhere. Instead, implicit dereference in a prefix takes care of them all. This means that there should never be a case when X.all.Last is legal while X'Last is not. See A183-00154.

**Incompatibilities With Ada 95**

```
{AI95-00363-01} Aliased variables are not necessarily constrained in Ada 2005 (see 3.6). Therefore, a subcomponent of an aliased variable may disappear or change shape, and taking 'Access of such a subcomponent thus is illegal, while the same operation would have been legal in Ada 95. Note that most allocated objects are still constrained by their initial value (see 4.8), and thus legality of 'Access didn't change for them. For example:

```ada
type T1 (D1 : Boolean := False) is
  record
    case D1 is
      when False =>
        C1 : aliased Integer;
      when True =>
        null;
    end case;
  end record;

type Acc_Int is access all Integer;

A_T : aliased T1;
Ptr : Acc_Int := A_T.C1'Access; -- Illegal in Ada 2005, legal in Ada 95
A_T := (D1 => True); -- Raised Constraint_Error in Ada 95, but does not
  -- is assigned (thus Ptr is illegal).
```

```
{AI95-00229-01} {AI95-00254-01} Amendment Correction: Taking 'Access of a subprogram declared in a generic unit in the body of that generic is no longer allowed. Such references can easily be used to create dangling pointers, as Legality Rules are not rechecked in instance bodies. At the same time, the rules were loosened a bit where that is harmless, and also to allow any runtime to be passed to an access parameter of an access-to-subprogram type. The now illegal uses of 'Access can almost always be moved to the private part of the generic unit, where they are still legal (and rechecked upon instantiation for possibly dangling pointers).
```

**Extensions to Ada 95**

```
{8652/0010} {AI95-00127-01} Corrigendum: Access attributes of objects of class-wide types can be used as the controlling parameter in a dispatching calls (see 3.9.2). This was an oversight in Ada 95.

{AI95-00235-01} Amendment Correction: The type of the prefix can now be used in resolving Access attributes. This allows more uses of the Access attribute to resolve. For example:
```
```
This change is upward compatible; any expression that does not resolve by the new rules would have failed a Legality Rule.

Wording Changes from Ada 95

Adjusted the wording to reflect the fact that expressions and function calls are masters.

Defined the accessibility of the various new kinds and uses of anonymous access types.

Incompatibilities With Ada 2005

Correction: Simplified the description of when a discriminant-dependent component is allowed as the prefix of ‘Access to when the object is known to be constrained. This fixes a confusion as to whether a subcomponent of an object that is not certain to be constrained can be used as a prefix of ‘Access. The fix introduces an incompatibility, as the rule did not apply in Ada 95 if the prefix was a constant; but it now applies no matter what kind of object is involved. The incompatibility is not too bad, since most kinds of constants are known to be constrained.

Correction: Corrected the checks for the constrainedness of the prefix of the Access attribute so that assume-the-worst is used in generic bodies. This may make some programs illegal, but those programs were at risk having objects disappear while valid access values still pointed at them.

Extensions to Ada 2005

Correction: Eliminated the static accessibility definition for generic formal types, as the actual can be more or less nested than the generic itself. This allows programs that were illegal for Ada 95 and for Ada 2005.

Eliminate the static accessibility definition for stand-alone objects of anonymous access-to-object types. This allows such objects to be used as temporaries without causing accessibility problems.

Wording Changes from Ada 2005

Correction: Corrected the rules so that the accessibility of the object designated by an access object is that of the access type, even when no dereference is given. The accessibility was not specified in the past. This correction applies to both Ada 95 and Ada 2005.

Correction: Corrected accessibility rules for access discriminants so that no cases are omitted.

Correction: Corrected accessibility rules for anonymous access return types and access discriminants in return statements.

Correction: Changed coextension rules so that coextensions that belong to an anonymous object are transferred to the ultimate object.

Defined the accessibility of explicitly aliased parameters (see 6.1) and conditional expressions (see 4.3.7).

Defined the term “master of the call” to simplify other wording, especially that for the accessibility checks associated with return statements and explicitly aliased parameters.

Correction: Defined the (omitted) accessibility level of null values when those are passed as the actual of an access-to-object parameter.

Inconsistencies With Ada 2012

Correction: Defined that the accessibility of a function that returns an anonymous access type is the same for implicit and explicit conversions. This could cause code involving implicit conversions to named access types that is legal and does not raise an exception in original Ada 2012 to become illegal or raise Program Error because of an accessibility failure in Ada 2022. This is more likely to prevent a dangling pointer bug than to prevent something useful.

Correction: Tightened the cases where an explicitly aliased parameter has special accessibility, to avoid needing to pass the required dynamic accessibility to functions that have explicitly aliased parameters. The changes affects programs that use the dynamic accessibility of an explicitly aliased parameter within a return statement of a function (typically using anonymous access types). This can mean that a program that would have been legal and worked in Ada 2012 as defined would raise Program Error or be rejected in Ada 2022. One such example is:

```ada
type Rec is record
  Comp : aliased Integer;
  ...
end record;
```

41.m/2
At (2), there is a check that the dynamic accessibility level of B is not deeper than the master of the call for F2 (which is defined to be the master of the call for F1). In Ada 2012, since the reference is inside of a return statement, the dynamic accessibility of A.Comp'Access is the master of the call for F1 - meaning the check at (2) should pass. In Ada 2022, the dynamic accessibility of A.Comp'Access is local for F1 - meaning the check at (2) should fail and raise Program_Error.

We're not aware of any Ada 2012 compilers that correctly implemented the rule as written (because of the overhead that is implied), so the practical effect of this change is to make the rules more consistent with actual practice.

\{AI12-0345-1\} \textbf{Correction:} Adjusted the rules so that using a part of a return object in a return expression does not break the connection between the inner and outer function calls. This means that some cases that (unnecessarily) failed an accessibility check in Ada 2012 will not do so in Ada 2022. This change will mostly remove latent problems from Ada code; very little code depends on an accessibility check failing.

### Incompatibilities With Ada 2012

\{AI12-0027-1\} \textbf{Corrigendum:} Defined the accessibility of a value conversion, so that it is treated like an aggregate built at the point of the conversion. This was previously unspecified, so this change might be incompatible if an Ada implementation treated the accessibility of such conversions as that of the operand type; in that case, previous legal conversions probably will become illegal as the lifetime of the conversion is very short. However, code that could tell this difference is fairly rare (taking 'Access of a component of a result of a type conversion), code depending on this accessibility was not portable, and such code could have created an immediately dangling pointer if the conversion actually made a copy (which is necessary in some instances).

\{AI12-0371-1\} \textbf{Correction:} The accessibility of a renaming of a formal subprogram in a generic package specification has changed to reflect the fact that a wrapper may be needed for the formal subprogram. Thus, 'Access of such a renaming found in an instance that is not library-level may become illegal. We think this case is unlikely to occur in practice, and a simple workaround is available (rename the actual at the point of the instance, use that rename as the prefix of 'Access).

### Extensions to Ada 2012

\{AI12-0402-1\} \textbf{Adjusted} the special accessibility for functions initializing objects to only apply to composite types. This makes some function calls of functions that return elementary types and have aliased parameters legal that otherwise would be illegal. Such a function cannot return a part of a parameter, and thus one does not need parameter checks to make that possible.

### Wording Changes from Ada 2012

\{AI12-0067-1\} \textbf{Corrigendum:} Corrected so that it is clear that explicitly aliased parameters in procedures have the same accessibility as other parameters. Only explicitly aliased parameters in functions are special.

\{AI12-0070-1\} \textbf{Corrigendum:} The accessibility of an anonymous access type of an extended return statement is defined here rather than in 6.5 so that all accessibility rules are here.

\{AI12-0089-1\} \textbf{Corrigendum:} Corrected a number of rules so that they clearly apply to generic functions as well as functions. (Remember, a generic function is not a function.)

\{AI12-0095-1\} \textbf{Corrigendum:} Moved the assume the worst rule about constrainedness of the prefix of attribute Access to 12.5.1, as a number of places in the Reference Manual need this rule.

\{AI12-0157-1\} \textbf{Corrigendum:} Ensured that the statically deeper relationship applies within the return expression of an expression function. (Dynamic properties apply by equivalence, but static properties are handled separately.)

\{AI12-0064-2\} \textbf{Added} Nonblocking (see 9.5) matching to P'Access.

\{AI12-0156-1\} \textbf{Added} text to define the accessibility of anonymous access types declaring a loop parameter.

\{AI12-0236-1\} \textbf{Added} declare_expression to the accessibility rules.

\{AI12-0277-1\} \textbf{Correction:} Clarified the static level of explicitly aliased parameters.

\{AI12-0372-1\} \textbf{Correction:} Redefined the statically deeper relationship for the master of a function call and locals of that call. This might cause programs to be rejected that were previously legal, but any such program should have failed a dynamic accessibility check. Thus this is not an incompatibility as it is changing the detection of an error from runtime to compile-time.
3.11 Declarative Parts

[A declarative_part contains declarative_items (possibly none).]

Syntax

declarative_part ::= \{declarative_item\}
declarative_item ::= basic_declarative_item | body

Static Semantics

The list of declarative_items of a declarative_part is called the declaration list of the declarative_part.

Dynamic Semantics

The elaboration of a declarative_part consists of the elaboration of the declarative_items, if any, in the order in which they are given in the declarative_part.

An elaborable construct is in the elaborated state after the normal completion of its elaboration. Prior to that, it is not yet elaborated.

8.a Ramification: The elaborated state is only important for bodies; certain uses of a body raise an exception if the body is not yet elaborated.

8.b Note that "prior" implies before the start of elaboration, as well as during elaboration.

8.c The use of the term "normal completion" implies that if the elaboration propagates an exception or is aborted, the declaration is not elaborated. RM83 missed the aborted case.

For a construct that attempts to use a body, a check (Elaboration_Check) is performed, as follows:

10/1 • \{AI95-0064-01\} For a call to a (non-protected) subprogram that has an explicit body, a check is made that the subprogram_body is already elaborated. This check and the evaluations of any actual parameters of the call are done in an arbitrary order.

10.a Discussion: AI83-00180 specifies that there is no elaboration check for a subprogram defined by a pragma Interface (or equivalently, pragma Import), AI83-00430 specifies that there is no elaboration check for an enumeration literal, AI83-00406 specifies that the evaluation of parameters and the elaboration check occur in an arbitrary order. AI83-00406 applies to generic instantiation as well (see below).

10.a.1/3 • \{AI95-0064-01\} A subprogram can be completed by a renaming-as-body, a null_procedure_declaration, or an expression_function_declaration, and we need to make an elaboration check on such a body, so we use "body" rather than subprogram_body above.

11/3 • \{AI05-0229-1\} For a call to a protected operation of a protected type (that has a body — no check is performed if a pragma Import applies to the protected type is imported — see B.1), a check is
made that the protected_body is already elaborated. This check and the evaluations of any actual parameters of the call are done in an arbitrary order.

Discussion: A protected type has only one elaboration “bit”, rather than one for each operation, because one call may result in evaluating the barriers of other entries, and because there are no elaborable declarations between the bodies of the operations. In fact, the elaboration of a protected_body does not elaborate the enclosed bodies, since they are not considered independently elaborable.

Note that there is no elaboration check when calling a task entry. Task entry calls are permitted even before the associated task_body has been seen. Such calls are simply queued until the task is activated and reaches a corresponding accept_statement. We considered a similar rule for protected entries — simply queuing all calls until the protected_body was seen, but felt it was not worth the possible implementation overhead, particularly given that there might be multiple instances of the protected type.

- For the activation of a task, a check is made by the activator that the task_body is already elaborated. If two or more tasks are being activated together (see 9.2), as the result of the elaboration of a declarative_part or the initialization for the object created by an allocator, this check is done for all of them before activating any of them.

  Reason: As specified by AI83-00149, the check is done by the activator, rather than by the task itself. If it were done by the task itself, it would be turned into a Tasking_Error in the activator, and the other tasks would still be activated.

- For the instantiation of a generic unit that has a body, a check is made that this body is already elaborated. This check and the evaluation of any explicit_generic_actual_parameters of the instantiation are done in an arbitrary order.

The exception Program_Error is raised if any of these checks fails.

Extensions to Ada 83

{AI95-00114-01} The syntax for declarative_part is modified to remove the ordering restrictions of Ada 83; that is, the distinction between basic_declarative_items and later_declarative_items within declarative_parts is removed. This means that things like use_clauses and object_declarations,variable_declarations, can be freely intermixed with things like bodies.

The syntax rule for proper_body now allows a protected_body, and the rules for elaboration checks now cover calls on protected operations.

Wording Changes from Ada 83

The syntax rule for later_declarative_item is removed; the syntax rule for declarative_item is new.

RM83 defines “elaborated” and “not yet elaborated” for declarative_items here, and for other things in 3.1, “Declarations”. That's no longer necessary, since these terms are fully defined in 3.1.

In RM83, all uses of declarative_part are optional (except for the one in block_statement with a declare) which is sort of strange, since a declarative_part can be empty, according to the syntax. That is, declarative_parts are sort of “doubly optional”. In Ada 95, these declarative_parts are always required (but can still be empty). To simplify description, we go further and say (see 5.6, “Block Statements”) that a block_statement without an explicit declarative_part is equivalent to one with an empty one.

Wording Changes from Ada 95

{8652/0009} {AI95-00137-01} Corrigendum: Changed representation clauses to aspect clauses to reflect that they are used for more than just representation.

{8652/0014} {AI95-00064-01} Corrigendum: Clarified that the elaboration check applies to all kinds of subprogram bodies.

{AI95-00420-01} Defined “declaration list” to avoid confusion for various rules. Other kinds of declaration list are defined elsewhere.

3.11.1 Completions of Declarations

{8652/0014} {AI95-00064-01} {AI05-0177-1} Declarations sometimes come in two parts. A declaration that requires a second part is said to require completion. The second part is called the completion of the declaration (and of the entity declared), and is either another declaration, a body, or a pragma. A body is
a body, an entry_body, a null procedure declaration or an expression function declaration that completes another declaration, or a renaming-as-body (see 8.5.4).

Discussion: Throughout the RM95, there are rules about completions that define the following:

1.a Which declarations require a corresponding completion.
1.b Which constructs can only serve as the completion of a declaration.
1.c Where the completion of a declaration is allowed to be.
1.d What kinds of completions are allowed to correspond to each kind of declaration that allows one.

Don't confuse this compile-time concept with the run-time concept of completion defined in 7.6.1.

Note that the declaration of a private type (if limited) can be completed with the declaration of a task type, which is then completed with a body. Thus, a declaration can actually come in three parts.

1.v{AI95-00217-06} A incomplete type (whether declared in the limited view of a package or not) may be completed by a private type declaration. In Ada 2005 the limited view of the package contains an incomplete view of the private type, so we can in fact have four parts now.

1.i{AI05-0229-1} In Ada 2012, there are no language-defined pragmas that act as completions.Pragma Import (which is obsolescent) has the effect of setting aspect Import to True; such an aspect makes giving a completion illegal. The wording that allows pragmas as completions was left as it is harmless and appears in many places in this Reference Manual.

Name Resolution Rules

A construct that can be a completion is interpreted as the completion of a prior declaration only if:

2. The declaration and the completion occur immediately within the same declarative region;
3. The defining name or defining_program_unit_name in the completion is the same as in the declaration, or in the case of a pragma, the pragma applies to the declaration;
4. If the declaration is overloadable, then the completion either has a type-conformant profile, or is a pragma.

Legality Rules

An implicit declaration shall not have a completion. For any explicit declaration that is specified to require completion, there shall be a corresponding explicit completion, unless the declared entity is imported (see B.1).

To be honest: {AI95-00217-06} The implicit declarations occurring in a limited view do have a completion (the explicit declaration occurring in the full view) but that's a special case, since the implicit declarations are actually built from the explicit ones. So they do not require a completion, they have one by fiat.

Discussion: The implicit declarations of predefined operators are not allowed to have a completion. Enumeration literals, although they are subprograms, are not allowed to have a corresponding subprogram_body. That's because the completion rules are described in terms of constructs (subprogram_declarations) and not entities (subprograms). When a completion is required, it has to be explicit; the implicit null package_body that Clause 7 talks about cannot serve as the completion of a package_declaration if a completion is required.

At most one completion is allowed for a given declaration. Additional requirements on completions appear where each kind of completion is defined.

Rationale: A subunit is not a completion; the stub is.

If the completion of a declaration is also a declaration, then that declaration might have a completion, too. For example, a limited private type can be completed with a task type, which can then be completed with a task body. This is not a violation of the “at most one completion” rule.

A type is completely defined at a place that is after its full type definition (if it has one) and after all of its subcomponent types are completely defined. A type shall be completely defined before it is frozen (see 13.14 and 7.3).
NOTE 1  {AI05-0229-1} Completions are in principle allowed for any kind of explicit declaration. However, for some kinds of declaration, the only allowed completion is an implementation-defined pragma pragma Import, and implementations are not required to have any such pragma support pragma Import for every kind of entity. This paragraph was deleted. Discussion: {AI05-0229-1} In fact, we expect that implementations will not support pragma Import of things like types — it's hard to even define the semantics of what it would mean. Therefore, in practice, not every explicit declaration can have a completion. In any case, if an implementation chooses to support pragma Import for, say, types, it can place whatever restrictions on the feature it wants to. For example, it might want the pragma to be a freezing point for the type.

NOTE 2  {AI12-0449-1} There are rules that prevent premature uses of declarations that have a corresponding completion. The Elaboration_Checks of 3.11 prevent such uses at run time for subprograms, protected operations, tasks, and generic units. The freezing rules (see 13.14) of “Freezing Rules” prevent, at compile time, premature uses of other entities such as private types and deferred constants.

Wording Changes from Ada 83

This subclause is new. It is intended to cover all kinds of completions of declarations, be they a body for a spec, a full type for an incomplete or private type, a full constant declaration for a deferred constant declaration, or a pragma Import for any kind of entity.

Wording Changes from Ada 95

{8652/0014} {AI95-00064-01} Corrigendum: Added a definition of body, which is different than body or body.

Wording Changes from Ada 2005

{AI95-0177-1} Added null procedures and expression functions that are completions to the definition of body.
4 Names and Expressions

{AI05-0299-1} [The rules applicable to the different forms of name and expression, and to their evaluation, are given in this clause section.]

4.1 Names

[Names can denote declared entities, whether declared explicitly or implicitly (see 3.1). Names can also denote objects or subprograms designated by access values; the results of type conversions or function calls; subcomponents and slices of objects and values; protected subprograms, single entries, entry families, and entries in families of entries. Finally, names can denote attributes of any of the foregoing.]

Syntax

{name ::= direct_name | explicit_dereference | indexed_component | slice | selected_component | attribute_reference | type_conversion | function_call | character_literal | qualified_expression | generalized_reference | generalized_indexing | target_name}

direct_name ::= identifier | operator_symbol

Discussion: {AI95-00114-01} character_literal is no longer a direct_name. character_literals are usable even when the corresponding enumeration_type_declaration is not visible. See 4.2.

prefix ::= name | implicit_dereference

explicit_dereference ::= name.all

implicit_dereference ::= name

{AI05-0004-1} [Certain forms of name (indexed_components, selected_components, slices, and attribute_references) include a prefix that is either itself a name that denotes some related entity, or an implicit_dereference of an access value that designates some related entity.]

Name Resolution Rules

The name in a dereference (either an implicit_dereference or an explicit_dereference) is expected to be of any access type.

Static Semantics

{AI05-0008-1} If the type of the name in a dereference is some access-to-object type T, then the dereference denotes a view of an object, the nominal subtype of the view being the designated subtype of T. If the designated subtype has unconstrained discriminants, the (actual) subtype of the view is constrained by the values of the discriminants of the designated object, except when there is a partial view of the type of the designated subtype that does not have discriminants, in which case the dereference is not constrained by its discriminant values.

Ramification: If the value of the name is the result of an access type conversion, the dereference denotes a view created as part of the conversion. The nominal subtype of the view is not necessarily the same as that used to create the designated object. See 4.6.
To be honest: We sometimes refer to the nominal subtype of a particular kind of name rather than the nominal subtype of the view denoted by the name (presuming the name denotes a view of an object). These two uses of nominal subtype are intended to mean the same thing.

Reason: [AI05-0008-1] The last sentence was not present in Ada 95; it is necessary in Ada 2005 because general access types can designate unconstrained objects, which was not possible in Ada 95. Thus, the rules that had this effect in Ada 95 (the object being constrained by its initial value) don't work in Ada 2005 and we have to say this explicitly.

[AI05-0008-1] The "except" part of the last sentence prevents privacy "breaking", so that if a private type has discriminants only in the full view, they don't interfere with freely interassigning values between objects of the type, even when the objects live in the heap.

Implementation Note: [AI05-0008-1] Since we don't depend on whether the designated object is constrained, it is not necessary to include a constrained bit in every object that could be designated by a general access type.

If the type of the name in a dereference is some access-to-subprogram type $S$, then the dereference denotes a view of a subprogram, the profile of the view being the designated profile of $S$.

Ramification: This means that the formal parameter names and default expressions to be used in a call whose name or prefix is a dereference are those of the designated profile, which need not be the same as those of the subprogram designated by the access value, since 'Access requires only subtype conformance, not full conformance.

Dynamic Semantics

The evaluation of a name determines the entity denoted by the name. This evaluation has no other effect for a name that is a direct_name or a character_literal.

[The evaluation of a name that has a prefix includes the evaluation of the prefix.] The evaluation of a prefix consists of the evaluation of the name or the implicit_dereference. The prefix denotes the entity denoted by the name or the implicit_dereference.

The evaluation of a dereference consists of the evaluation of the name and the determination of the object or subprogram that is designated by the value of the name. A check is made that the value of the name is not the null access value. Constraint_Error is raised if this check fails. The dereference denotes the object or subprogram designated by the value of the name.

Examples of direct names:

- Pi -- the direct name of a number (see 3.3.2)
- Limit -- the direct name of a constant (see 3.3.1)
- Count -- the direct name of a scalar variable (see 3.3.1)
- Board -- the direct name of an array variable (see 3.6.1)
- Matrix -- the direct name of a type (see 3.6)
- Random -- the direct name of a function (see 6.1)
- Error -- the direct name of an exception (see 11.1)

Examples of dereferences:

- Next_Car.all -- explicit dereference denoting the object designated
- by the access variable Next_Car (see 3.10.1)
- Next_Car.Owner -- selected component with implicit dereference;
- same as Next_Car.all.Owner

Extensions to Ada 83

Type conversions and function calls are now considered names that denote the result of the operation. In the case of a type conversion used as an actual parameter or that is of a tagged type, the type conversion is considered a variable if the operand is a variable. This simplifies the description of "parameters of the form of a type conversion" as well as better supporting an important OOP paradigm that requires the combination of a conversion from a class-wide type to some specific type followed immediately by component selection. Function calls are considered names so that a type conversion of a function call and the function call itself are treated equivalently in the grammar. A function call is considered the name of a constant, and can be used anywhere such a name is permitted. See 6.5.
Type conversions of a tagged type are permitted anywhere their operand is permitted. That is, if the operand is a variable, then the type conversion can appear on the left-hand side of an assignment statement. If the operand is an object, then the type conversion can appear in an object renaming or as a `prefix(...)`. See 4.6.

Wording Changes from Ada 83

{AI95-00114-01} Everything of the general syntactic form `name(...)` is now syntactically a name. In any realistic parser, this would be a necessity since distinguishing among the various `name(...)` constructs inevitably requires name resolution. In cases where the construct yields a value rather than an object, the name denotes the value rather than an object. Names already denote values in Ada 83 with named numbers, components of the result of a function call, etc. This is partly just a wording change, and partly an extension of functionality (see Extensions heading above).

The syntax rule for `direct_name` is new. It is used in places where direct visibility is required. It's kind of like Ada 83's `simple_name`, but `simple_name` applied to both direct visibility and visibility by selection, and furthermore, it didn't work right for `operator_symbols`. The syntax rule for `simple_name` is removed, since its use is covered by a combination of `direct_name` and `selector_name`. The syntactic categories `direct_name` and `selector_name` are similar; it's mainly the visibility rules that distinguish the two. The introduction of `direct_name` requires the insertion of one new explicit textual rule: to forbid `statement_identifiers` from being `operator_symbols`. This is the only case where the explicit rule is needed, because this is the only case where the declaration of the entity is implicit. For example, there is no need to syntactically forbid (say) "X: "Rem"",", because it is impossible to declare a type whose name is an `operator_symbol` in the first place.

{AI12-0005-1} The syntax rules for `explicit_dereference` and `implicit_dereference` are new; this makes other rules simpler, since dereferencing an access value has substantially different semantics from `selected_components`. We also use `name` instead of `prefix` in the `explicit_dereference` rule since that seems clearer. Note that these rules rely on the fact that function calls are now names, so we don't need to use `prefix` to allow `function_calls` in front of `.all`. 

Discussion: Actually, it would be reasonable to allow any `primary` in front of `.all`, since only the value is needed, but that would be a bit radical.

We no longer use the term `appropriate for a type` since we now describe the semantics of a `prefix` in terms of implicit dereference.

Extensions to Ada 2005

{AI05-0003-1} A qualified expression is now a name denoting a constant view; this allows them to be used as a `prefix` and to be renamed as an object. They are often used to remove ambiguity from function calls, and there may be no other way to do that. Interestingly, a type conversion of a qualified expression is already legal in these contexts, so this change mainly reduces clutter by eliminating an otherwise unneeded type conversion from some expressions.

Wording Changes from Ada 2005

{AI05-0008-1} Correction: Added a missing rule so that most dereferences are assumed constrained (without determining whether the designated object is). This is just confirming the Ada 95 rules; Ada 2005 failed to ensure that this property was unchanged.

{AI05-0139-2} {AI05-0299-1} Added `generalized_reference` and `generalized_indexing` as types of `name`; these are documented as extensions in the appropriate subclauses.

Wording Changes from Ada 2012

{AI12-0125-3} Added a `target_name` (see 5.2.1) to the syntax of `name`.

4.1.1 Indexed Components

[An indexed_component denotes either a component of an array or an entry in a family of entries.]

Syntax

\[
\text{indexed_component ::= prefix(expression \{, expression\})}
\]

Name Resolution Rules

The `prefix` of an `indexed_component` with a given number of expressions shall resolve to denote an array (after any implicit dereference) with the corresponding number of index positions, or shall resolve to denote an entry family of a task or protected object (in which case there shall be only one expression).
The expected type for each expression is the corresponding index type.

Static Semantics

When the prefix denotes an array, the indexed_component denotes the component of the array with the specified index value(s). The nominal subtype of the indexed_component is the component subtype of the array type.

Ramifications: *AI95-00363-01* In the case of an array whose components are aliased, and of an unconstrained discriminated subtype, the components are constrained even though their nominal subtype is unconstrained. (This is because all aliased discriminated objects are constrained. See 3.10.2.) In all other cases, an array_component is constrained if and only if its nominal subtype is constrained.

When the prefix denotes an entry family, the indexed_component denotes the individual entry of the entry family with the specified index value.

Dynamic Semantics

For the evaluation of an indexed_component, the prefix and the expressions are evaluated in an arbitrary order. The value of each expression is converted to the corresponding index type. A check is made that each index value belongs to the corresponding index range of the array or entry family denoted by the prefix. Constraint_Error is raised if this check fails.

Examples

Examples of indexed components:

- `My_Schedule(Sat)` -- a component of a one-dimensional array (see 3.6.1)
- `Page(10)` -- a component of a one-dimensional array (see 3.6)
- `Board(M, J + 1)` -- a component of a two-dimensional array (see 3.6.1)
- `Page(10)(20)` -- a component of a component (see 3.6)
- `Request(Medium)` -- an entry in a family of entries (see 9.1)
- `Next_Frame(L)(M, N)` -- a component of a function call (see 6.1)

Distinct notations are used for components of multidimensional arrays (such as `Board`) and arrays of arrays (such as `Page`). The components of an array of arrays are arrays and can therefore be indexed. Thus `Page(10)(20)` denotes the 20th component of `Page(10)`. In the last example `Next_Frame(L)` is a function call returning an access value that designates a two-dimensional array.

4.1.2 Slices

[A slice denotes a one-dimensional array formed by a sequence of consecutive components of a one-dimensional array. A slice of a variable is a variable; a slice of a constant is a constant;] a slice of a value is a value.

Syntax

```
slice ::= prefix(discrete_range)
```

Name Resolution Rules

The prefix of a slice shall resolve to denote a one-dimensional array (after any implicit dereference).

The expected type for the discrete_range of a slice is the index type of the array type.
Static Semantics

A slice denotes a one-dimensional array formed by the sequence of consecutive components of the array denoted by the prefix, corresponding to the range of values of the index given by the discrete_range.

The type of the slice is that of the prefix. Its bounds are those defined by the discrete_range.

Dynamic Semantics

For the evaluation of a slice, the prefix and the discrete_range are evaluated in an arbitrary order. If the slice is not a null slice (a slice where the discrete_range is a null range), then a check is made that the bounds of the discrete_range belong to the index range of the array denoted by the prefix. Constraint_Error is raised if this check fails.

Examples of slices:

Stars(1 .. 15)        -- a slice of 15 characters     (see 3.6.3)
Page(10 .. 10 + Size) -- a slice of 1 + Size components (see 3.6)
Page(L) (A .. B)      -- a slice of the array Page(L) (see 3.6)
Stars(1 .. 0)         -- a null slice                  (see 3.6.3)
My_Schedule(Weekday)  -- bounds given by subtype     (see 3.6.1 and 3.5.1)
Stars(5 .. 15)(K)     -- same as Stars(K)             (see 3.6.3)
-- provided that K is in 5 .. 15

4.1.3 Selected Components

[Selected_components are used to denote components (including discriminants), entries, entry families, and protected subprograms; they are also used as expanded names as described below.]

Syntax

selected_component ::= prefix . selector_name

selector_name ::= identifier | character_literal | operator_symbol

Name Resolution Rules

A selected_component is called an expanded name if, according to the visibility rules, at least one possible interpretation of its prefix denotes a package or an enclosing named construct (directly, not through a subprogram_renaming_declaration or generic_renaming_declaration).

Discussion: See AI83-00187.

A selected_component that is not an expanded name shall resolve to denote one of the following:

Ramification: If the prefix of a selected_component denotes an enclosing named construct, then the selected_component is interpreted only as an expanded name, even if the named construct is a function that could be called without parameters.

- A component [(including a discriminant)]:

NOTE 1 {AI12-0447-1} By the rules given in 3.10.2, a slice is illegal not permitted as the prefix of an Access attribute_reference, even if the components or the array as a whole are aliased. See 3.10.2.

Proof: Slices are not aliased, by 3.10, “Access Types”.

Reason: This is to ease implementation of general-access-to-array. If slices were aliased, implementations would need to store array dope with the access values, which is not always desirable given access-to-incomplete types completed in a package body.

NOTE 2 For a one-dimensional array A, the slice A(N .. N) denotes an array that has only one component; its type is the type of A. On the other hand, A(N) denotes a component of the array A and has the corresponding component type.
The prefix shall resolve to denote an object or value of some non-array composite type (after any implicit dereference). The selector_name shall resolve to denote a discriminant specification of the type, or, unless the type is a protected type, a component declaration of the type. The selected_component denotes the corresponding component of the object or value.

Reason: The components of a protected object cannot be named except by an expanded name, even from within the corresponding protected body. The protected body cannot reference the private components of some arbitrary object of the protected type; the protected body may reference components of the current instance only (by an expanded name or a direct name).

Ramification: Only the discriminants and components visible at the place of the selected_component can be selected, since a selector_name can only denote declarations that are visible (see 8.3).

- A single entry, an entry family, or a protected subprogram:

The prefix shall resolve to denote an object or value of some task or protected type (after any implicit dereference). The selector_name shall resolve to denote an entry_declaration or subprogram_declaration occurring (implicitly or explicitly) within the visible part of that type. The selected_component denotes the corresponding entry, entry family, or protected subprogram.

Reason: This explicitly says “visible part” because even though the body has visibility on the private part, it cannot call the private operations of some arbitrary object of the task or protected type, only those of the current instance (and expanded name notation has to be used for that).

A view of a subprogram whose first formal parameter is of a tagged type or is an access parameter whose designated type is tagged:

A view of a subprogram whose first formal parameter is of a tagged type or is an access parameter whose designated type is tagged.

The prefix (after any implicit dereference) shall resolve to denote an object or value of a specific tagged type \( T \) or class-wide type \( TClass \). The selector_name shall resolve to denote a view of a subprogram declared immediately within the declarative region in which an ancestor of the type \( T \) is declared. The first formal parameter of the subprogram shall be of type \( T \), or a class-wide type that covers \( T \), or an access parameter designating one of these types. The designator of the subprogram shall not be the same as that of a component of the tagged type visible at the point of the selected_component. The subprogram shall not be an implicitly declared primitive operation of type \( T \) that overrides an inherited subprogram implemented by an entry or protected subprogram visible at the point of the selected_component. The selected_component denotes a view of this subprogram that omits the first formal parameter. This view is called a prefixed view of the subprogram, and the prefix of the selected_component (after any implicit dereference) is called the prefix of the prefixed view.

Discussion: The part of the rule that excludes a primitive overriding subprogram as a selector applies only to the wrapper subprogram that is implicitly declared to override a subprogram inherited from a synchronized interface that is implemented by an operation of a task or protected type (see 9.1 and 9.4). We don't want calls that use a prefixed view to be ambiguous between the wrapper subprogram and the implementing entry or protected operation. Note that it is illegal to declare an explicit primitive that has a prefixed view that is homographic with one of the type's operations, so in normal cases it isn't possible to have an ambiguity in a prefix call. However, a class-wide operation of an ancestor type that is declared in the same declaration list with the ancestor type is also considered, and that can still make a call ambiguous.

An expanded name shall resolve to denote a declaration that occurs immediately within a named declarative region, as follows:

- The prefix shall resolve to denote either a package [(including the current instance of a generic package, or a rename of a package)], or an enclosing named construct.

- The selector_name shall resolve to denote a declaration that occurs immediately within the declarative region of the package or enclosing construct [(the declaration shall be visible at the place of the expanded name — see 8.3)]. The expanded name denotes that declaration.

Ramification: Hence, a library unit or subunit can use an expanded name to refer to the declarations within the private part of its parent unit, as well as to other children that have been mentioned in with_clauses.
• If the prefix does not denote a package, then it shall be a direct_name or an expanded name, and it shall resolve to denote a program unit (other than a package), the current instance of a type, a block_statement, a loop_statement, or an accept_statement (in the case of an accept_statement or entry_body, no family index is allowed); the expanded name shall occur within the declarative region of this construct. Further, if this construct is a callable construct and the prefix denotes more than one such enclosing callable construct, then the expanded name is ambiguous, independently of the selector_name.

Legality Rules

\{AI95-00252-01\} \{AI95-00407-01\} \{AI12-0204-1\} \{AI12-0427-1\} For a prefixed view of a subprogram whose first formal parameter is an access parameter, the prefix of any prefixed view shall be legal as the prefix of an attribute_reference with attribute_designator Access appearing as the first actual parameter in a call on the unprefixed view of the subprogram denote an aliased view of an object.

Ramification: \{AI12-0204-1\} This rule prevents, for instance, using a nonaliased prefix in such a prefixed view. It also prevents using discriminant-dependent components as the prefix of such a prefixed view if those components would not be allowed to be renamed.

\{AI95-00407-01\} For a subprogram whose first parameter is of mode in out or out, or of an anonymous access-to-variable type, the prefix of any prefixed view shall denote a variable.

Reason: We want calls through a prefixed view and through a normal view to have the same legality. Thus, the implicit 'Access in this new notation needs the same legality check that an explicit 'Access would have. Similarly, we need to prohibit the object from being constant if the first parameter of the subprogram is in out, because that is (obviously) prohibited for passing a normal parameter.

Dynamic Semantics

The evaluation of a selected_component includes the evaluation of the prefix.

For a selected_component that denotes a component of a variant, a check is made that the values of the discriminants are such that the value or object denoted by the prefix has this component. The exception Constraint_Error is raised if this check fails.

Examples of selected components:

\{AI95-00252-01\} \{AI95-00407-01\} \{AI12-0178\} Tomorrow.Month -- a record component (see 3.8)

Next.Car.Owner -- a record component (see 3.10.1)
Next.Car.Owner.Age -- a record component (see 3.10.1)
-- the previous two lines involve implicit dereferences
Writer.Unit -- a record component (a discriminant) (see 3.8.1)
Min.Cell(H).Value -- a record component of the result (see 6.1)
-- of the function call Min_Cell(H)
Cashier.Append -- a prefixed view of a procedure (see 3.9.4)
Control.Seize -- an entry of a protected object (see 9.4)
Pool(K).Write -- an entry of the task Pool(K) (see 9.4-4)

Examples of expanded names:

Key_Manager."<" -- an operator of the visible part of a package (see 7.3.1)
Dot_Product.Sum -- a variable declared in a function body (see 6.1)
Buffer.Pool -- a variable declared in a protected unit (see 9.11)
Buffer.Read -- an entry of a protected unit (see 9.11)
Swap.Temp -- a variable declared in a block statement (see 5.6)
Standard.Boolean -- the name of a predefined type (see A.1)

Extensions to Ada 83

We now allow an expanded name to use a prefix that denotes a rename of a package, even if the selector is for an entity local to the body or private part of the package, so long as the entity is visible at the place of the reference. This
eliminates a preexisting anomaly where references in a package body may refer to declarations of its visible part but not those of its private part or body when the prefix is a rename of the package.

Wording Changes from Ada 83

The syntax rule for selector_name is new. It is used in places where visibility, but not necessarily direct visibility, is required. See 4.1, “Names” for more information.

The description of dereferencing an access type has been moved to 4.1, “Names”; name.all is no longer considered a selected_component.

The rules have been restated to be consistent with our new terminology, to accommodate class-wide types, etc.

Extensions to Ada 95

{[AI95-00252-01] The prefixed view notation for tagged objects is new. This provides a similar notation to that used in other popular languages, and also reduces the need for use clauses. This is sometimes known as “distinguished receiver notation”.

Given the following definitions for a tagged type T:

procedure Do_Something (Obj : in out T; Count : in Natural);
procedure Do_Something_Else (Obj : access T; Flag : in Boolean);
My_Object : aliased T;

the following calls are equivalent:
Do_Something (My_Object, Count => 10);
My_Object.Do_Something (Count => 10);

as are the following calls:
Do_Something_Else (My_Object'Access, Flag => True);
My_Object.Do_Something_Else (Flag => True);

Wording Changes from Ada 2005

{[AI05-0090-1] Correction: Corrected the definition of a prefixed view to ignore the implicit subprograms declared for “implemented by” entries and protected subprograms.

Incompatibilities With Ada 2012

{[AI12-0204-1] Correction: Added a rule to ensure that all reasons that the prefix of an Access attribute can be illegal are covered by the rule for the implicit Access attribute of a prefixed view. If the object is a subcomponent that depends on discriminants or fails a static accessibility check, Ada 2012 would have allowed the prefix while Ada 2022 would not. This violated the principle that a prefixed view and a normal call have the same semantics; practically, the code may not have worked anyway if a compiler implemented generalized indexing by code expansion into the canonical form. Thus, such code wasn't practically portable.

4.1.4 Attributes

[An attribute is a characteristic of an entity that can be queried via an attribute_reference or a range_attribute_reference.]

Term entry: attribute — characteristic or property of an entity that can be queried, and in some cases specified

Syntax

attribute_reference ::= __prefix'attribute_designator
| reduction_attribute_reference

attribute_designator ::= identifier[(static_expression)]
| Access | Delta | Digits | Mod

range_attribute_reference ::= prefix'range_attribute_designator

range_attribute_designator ::= Range[(static_expression)]
Name Resolution Rules

\{AI12-0242-1\} \{AI12-0262-1\} In an attribute_reference that is not a reduction_attribute_reference, if the attribute_designator is for an attribute defined for (at least some) objects of an access type, then the prefix is never interpreted as an implicit_dereference; otherwise (and for all range_attribute_references and reduction_attribute_references), if there is a prefix and the type of the name within the prefix is of an access type, the prefix is interpreted as an implicit_dereference. Similarly, if the attribute_designator is for an attribute defined for (at least some) functions, then the prefix is never interpreted as a parameterless function_call; otherwise (and for all range_attribute_references and reduction_attribute_references), if there is a prefix and the prefix consists of a name that denotes a function, it is interpreted as a parameterless function_call.

Discussion: The first part of this rule is essentially a "preference" against implicit dereference, so that it is possible to ask for, say, 'Size of an access object, without automatically getting the size of the object designated by the access object. This rule applies to 'Access, 'Unchecked_Access, 'Size, and 'Address, and any other attributes that are defined for at least some access objects.

The second part of this rule implies that, for a parameterless function F, F'Address is the address of F, whereas F'Size is the size of the anonymous constant returned by F.

We normally talk in terms of expected type or profile for name resolution rules, but we don't do this for attributes because certain attributes are legal independent of the type or the profile of the prefix.

\{AI95-00114-01\} Other than the rules given above, the Name Resolution Rules for the prefix of each attribute are defined as Name Resolution Rules for that attribute. If no such rules are defined, then no context at all should be used when resolving the prefix. In particular, any knowledge about the kind of entities required must not be used for resolution unless that is required by Name Resolution Rules. This matters in obscure cases; for instance, given the following declarations:

\begin{verbatim}
function Get_It return Integer is ... -- (1)
function Get_It return Some_Record_Type is ... -- (2)
\end{verbatim}

the following attribute_reference cannot be resolved and is illegal:

\begin{verbatim}
if Get_It'Valid then
\end{verbatim}

\{AI05-0005-1\} even though the Valid attribute is only defined for objects of scalar types, and thus cannot be applied to the result of function (2). That information cannot be used to resolve the prefix. The same would be true if (2) had been a procedure; even though the procedure does not denote an object, the attribute_reference is still illegal.

The expression, if any, in an attribute_designator or range_attribute_designator is expected to be of any integer type.

Legality Rules

The expression, if any, in an attribute_designator or range_attribute_designator shall be static.

Static Semantics

\{AI05-0006-1\} \{AI12-0032-1\} \{AI12-0159-1\} An attribute_reference denotes a value, an object, a subprogram, or some other kind of program entity. Unless explicitly specified otherwise, for an attribute_reference that denotes a value or an object, if its type is scalar, then its nominal subtype is the base subtype of the type; if its type is tagged, its nominal subtype is the first subtype of the type; otherwise, its nominal subtype is a subtype of the type without any constraint, or predicate. Similarly, unless explicitly specified otherwise, for an attribute_reference that denotes a function, when its result type is scalar, its result subtype is the base subtype of the type, when its result type is tagged, the result subtype is the first subtype of the type, and when the result type is some other type, the result subtype is a subtype of the type without any constraint, or predicate.

Discussion: The attributes defined by the language are summarized in K.2. Implementations can define additional attributes.
nominal subtype. For nondiscrete cases, we define the nominal subtype mainly for completeness. Implementations may specify otherwise for implementation-defined attribute functions.

The rule is written to match the meaning of the italicized $T$ in the definition of attributes such as Input; see 4.5.1.

To be honest: \[AI05-0006-1\] We don't worry about the fact that “base subtype” is not explicitly defined for the universal types. Since it is not possible to constrain a universal numeric type, all subtypes are unconstrained, and hence can be considered base subtypes. The wording above could be altered to bypass this issue, but it doesn't seem necessary, since universal integer is handled specially in the rules for case expression full coverage, and we don't allow user-defined functions for attribute functions whose result type is universal.

[A range_attribute_reference X'Range(N) is equivalent to the range X'First(N) .. X'Last(N), except that the prefix is only evaluated once. Similarly, X'Range is equivalent to X'First .. X'Last, except that the prefix is only evaluated once.]

Dynamic Semantics

\[AI12-0262-1\] The evaluation of an attribute_reference (or range_attribute_reference or an attribute_reference that is not a reduction_attribute_reference) consists of the evaluation of the prefix.\[The evaluation of a reduction_attribute_reference is defined in 4.5.10.\]

Implementation Permissions

\[AI95-00093-01\] An implementation may provide implementation-defined attributes; the identifier for such an implementation-defined attribute shall differ from those of the language-defined attributes unless supplied for compatibility with a previous edition of this Reference Manual.

**Implementation defined:** Implementation-defined attributes.

**Ramification:** They cannot be reserved words because reserved words are not legal identifiers.

For example, the implementation defines whether a given implementation-defined attribute can be used in a static expression.

\[AI12-0362-2\] An implementation may extend the definition of a language-defined attribute by accepting uses of that attribute that would otherwise be illegal in the following cases:

- in order to support compatibility with a previous edition of this Reference Manual; or

**Ramification:** \[AI95-00093-01\] Implementations are allowed to support the Small attribute for floating types, as this was defined in Ada 83, even though the name would conflict with a language-defined attribute.

- in the case of a language-defined attribute whose prefix is required by this document to be a floating point subtype, an implementation may accept an attribute_reference whose prefix is a fixed point subtype; the semantics of such an attribute_reference are implementation defined.]

**NOTE 1** Attributes are defined throughout this document, and are summarized in K.2.

**NOTE 2** \[AI95-00235\] By the general rules given above, there is no expected type or profile for the name in a prefix of an attribute_reference (or a range_attribute_reference), which means that no context can be used to resolve the name has to be resolved without using any context. However, by the rules given in 3.10.2 for the case of the Access attribute, the expected type for the attribute_reference is the first single access type, and if it is an access-to-subprogram_type (see 3.10.2) then the resolution of the name can make use of the designated type or profile of this use the fact that the type of the object or the profile of the callable entity denoted by the name has to match the designated type or be type conformant with the designated profile of the access type.

**Proof:** \[AI95-00235\] In the general case, there is no “expected type” for the prefix of an attribute_reference. In the special case of ‘Access, there is an “expected type” or “expected profile” for the prefix.

**Reason:** ‘Access is a special case, because without it, it would be very difficult to take ’Access of an overloaded subprogram.
Examples of attributes:

- Color’First        -- minimum value of the enumeration type Color (see 3.5.1)
- Rainbow’Base’First -- same as Color’First (see 3.5.1)
- Real’Digits        -- precision of the type Real (see 3.5.7)
- Board’Last(2)      -- upper bound of the second dimension of Board (see 3.6.1)
- Board’Range(1)     -- index range of the first dimension of Board (see 3.6.1)
- Pool(K)’Terminated -- True if task Pool(K) is terminated (see 9.1)
- Date’Size          -- number of bits for records of type Date (see 3.8)
- Message’Address    -- address of the record variable Message

Extensions to Ada 83

We now uniformly treat X’Range as X’First..X’Last, allowing its use with scalar subtypes.
We allow any integer type in the static_expression of an attribute designator, not just a value of universal_integer. The preference rules ensure upward compatibility.

Wording Changes from Ada 83

We use the syntactic category attribute_reference rather than simply "attribute" to avoid confusing the name of something with the thing itself.
The syntax rule for attribute_reference now uses identifier instead of simple_name, because attribute identifiers are not required to follow the normal visibility rules.
We now separate attribute_reference from range_attribute_reference, and enumerate the reserved words that are legal attribute or range attribute designators. We do this because identifier no longer includes reserved words.
The Ada 95 name resolution rules are a bit more explicit than in Ada 83. The Ada 83 rule said that the "meaning of the prefix of an attribute must be determinable independently of the attribute designator and independently of the fact that it is the prefix of an attribute". That isn't quite right since the meaning even in Ada 83 embodies whether or not the prefix is interpreted as a parameterless function call, and in Ada 95, it also embodies whether or not the prefix is interpreted as an implicit dereference. So the attribute designator does make a difference — just not much.
Note however that if the attribute designator is Access, it makes a big difference in the interpretation of the prefix (see 3.10.2).

Wording Changes from Ada 95

{8652/0015}  {AI95-00093-01}  Corrigendum: The wording was changed to allow implementations to continue to implement the Ada 83 Small attribute. This was always intended to be allowed.
{AI95-00235-01} The note about resolving prefixes of attributes was updated to reflect that the prefix of an Access attribute now has an expected type (see 3.10.2).

Wording Changes from Ada 2005

{AI05-0006-1} Correction: Defined the nominal subtype of an attribute_reference to close a minor language hole.

Wording Changes from Ada 2012

{AI12-0032-1} Corrigendum: Allowed overriding the nominal subtype of an attribute_reference for an object; that is used elsewhere in this standard.
{AI12-0159-1} Corrigendum: Added wording so it is clear that predicates don’t apply to the result of an attribute.
{AI12-0242-1} {AI12-0262-1} Added reduction_attribute_reference and cleaned up the rules here to avoid trampling the definition of those in 4.5.10.
{AI12-0362-2} Added a permission to support fixed point versions of float attributes, such as the rounding attributes found in A.5.3.
4.1.5 User-Defined References

Static Semantics

{AI05-0139-2} Given a discriminated type $T$, the following type-related operational aspect may be specified:

Implicit Dereference

This aspect is specified by a name that denotes an access discriminant declared for the type $T$.

Aspect Description for Implicit Dereference: Mechanism for user-defined implicit .

{AI05-0139-2} A (view of a) type with a specified Implicit Dereference aspect is a reference type. A reference object is an object of a reference type. The discriminant named by the Implicit Dereference aspect is the reference discriminant of the reference type or reference object. [A generalized reference is a name that identifies a reference object, and denotes the object or subprogram designated by the reference discriminant of the reference object.]

Term entry: reference type — type that has user-defined behavior for “.all”, defined by the Implicit Dereference aspect

Syntax

{AI05-0139-2} generalized_reference ::= reference_object_name

Name Resolution Rules

{AI05-0139-2} {AI05-0269-1} The expected type for the reference_object_name in a generalized_reference is any reference type.

Static Semantics

{AI12-0138-1} The Implicit Dereference aspect is nonoverridable (see 13.1.1).

Reason: This ensures that all descendants of a reference type have the same reference discriminant. This prevents generic contract problems with formal derived types.

{AI05-0139-2} A generalized_reference denotes a view equivalent to that of a dereference of the reference discriminant of the reference object.

{AI05-0139-2} {AI12-0203-1} Given a reference type $T$, the Implicit Dereference aspect is inherited by descendants of type $T$ if not overridden [(which is only permitted if confirming)]. If a descendant type constrains the value of the reference discriminant of $T$ by a new discriminant, that new discriminant is the reference discriminant of the descendant. [If the descendant type constrains the value of the reference discriminant of $T$ by an expression other than the name of a new discriminant, a generalized_reference that identifies an object of the descendant type denotes the object or subprogram designated by the value of this constraining expression.]

Dynamic Semantics

{AI05-0139-2} The evaluation of a generalized_reference consists of the evaluation of the reference_object_name and a determination of the object or subprogram designated by the reference discriminant of the named reference object. A check is made that the value of the reference discriminant is not the null access value. Constraint Error is raised if this check fails. The generalized_reference denotes the object or subprogram designated by the value of the reference discriminant of the named reference object.
Examples

{AI12-0429-1} Examples of the specification and use of generalized references:

{AI05-0268-1} type Barrel is tagged ... -- holds objects of type Element
{AI05-0139-2} [AI05-0299-1] type Ref_Element(Data : access Element) is limited
private
    with Implicit_Dereference => Data;
    -- This Ref_Element type is a "reference" type.
    -- "Data" is its reference discriminant.
{AI05-0139-2} {AI05-0268-1} function Find (B : aliased in out Barrel; Key : String)
    return Ref_Element;
    -- Returns a reference to an element of a barrel.
{AI05-0268-1} {AI05-0299-1} B : aliased Barrel;
{AI05-0139-2} ... {AI05-0268-1} Find (B, "grape") := Element'(...); -- Assign through a reference.
{AI05-0139-2} ... {AI05-0268-1} Find (B, "grape").Data.all := Element'(...); -- This is equivalent to:

Extensions to Ada 2005

{AI05-0139-2} The aspect Implicit_Dereference and the generalized_reference are new.

Incompatibilities With Ada 2012

{AI12-0138-1} Corrigendum: Defined Implicit_Dereference to be nonoverridable, which makes redefinitions and hiding of the aspect illegal. It's possible that some program could violate one of these new restrictions, but this is not very likely as reference types are not likely to be used in a hierarchy.

4.1.6 User-Defined Indexing

Static Semantics

{AI05-0139-2} Given a tagged type T, the following type-related, operational aspects may be specified:

{AI12-0428-1} Constant_Indexing
This aspect shall be specified by a name that denotes one or more functions declared immediately within the same declaration list in which T, or the declaration completed by T, is declared. All such functions shall have at least two parameters, the first of which is of type T or T'Class, or is an access-to-constant parameter with designated type T or T'Class.

Aspect Description for Constant_Indexing: Defines function(s) to implement user-defined indexed components.

{AI12-0428-1} Variable_Indexing
This aspect shall be specified by a name that denotes one or more functions declared immediately within the same declaration list in which T, or the declaration completed by T, is declared. All such functions shall have at least two parameters, the first of which is of type T or T'Class, or is an access parameter with designated type T or T'Class. All such functions shall have a return type that is a reference type (see 4.1.5), whose reference discriminant is of an access-to-variable type.

Reason: We require these functions to return a reference type so that the object returned from the function can act like a variable. We need no similar rule for Constant_Indexing, since all functions return constant objects.

Aspect Description for Variable_Indexing: Defines function(s) to implement user-defined indexed components.

Reason: {AI22-0002-1} {AI22-0005-1} For a function that has a parameter of T or access T, a blanket rule in 13.1.1 requires the function to be a primitive operation of T, the wording about the same declaration list is redundant in that case. That 13.1.1 rule does not apply to functions that have parameters of T'Class or access T'Class (which is good, as those can never be primitive); the wording about the declaration list is necessary in that case.
These aspects are inherited by descendants of T (including the class-wide type TClass). [The aspects shall not be overridden, but the functions they denote may be.]

**Ramification:** Indexing can be provided for multiple index types by overloading routines with different parameter profiles. For instance, the map containers provide indexing on both cursors and keys by providing pairs of overloaded routines to the Constant_Indexing and Variable_Indexing aspects.

An indexable container type is (a view of) a tagged type with at least one of the aspects Constant_Indexing or Variable_Indexing specified. An indexable container object is an object of an indexable container type. [A generalized indexing is a name that denotes the result of calling a function named by a Constant_Indexing or Variable_Indexing aspect.]

**Term entry:** indexable container type — type that has user-defined behavior for indexing, via the Constant_Indexing or Variable_Indexing aspects

The Constant_Indexing and Variable_Indexing aspects are nonoverridable (see 13.1.1).

**Reason:** This (and the following Legality Rules) ensures that all descendants of an indexable container type have aspects with the same properties. This prevents generic contract problems with formal derived types.

A nonoverridable aspect allows the replacement of the implementation of an indexing function and the addition of a new indexing function for a derived type, but not the removal of an indexing function. This is necessary so that indexing can be used on objects of TClass. So long as the tag of O is that of its normal subtype, we do not want TClass(O)(I) to mean something different than O(I). Thus we cannot allow a change in the function identified. As TClass(O)(I) expands into a dispatching call, we need to ensure that there is a body for each such function — but it is OK for that body to be changed from the original body (that’s just normal dispatching).

Paragraphs 6 through 9 were deleted.

**Legality Rules**

The Constant_Indexing or Variable_Indexing aspect shall not be specified:

- If an ancestor of a type T is an indexable container type, then any explicit specification of the Constant_Indexing or Variable_Indexing aspects shall be confirming; that is, the specified name shall match the inherited aspect (see 13.1.1).

- on a derived type if the parent type has the corresponding aspect specified or inherited; or

- on a full_type_declaration if the type has a tagged partial view.

Paragraphs 7 through 8 were deleted.

In addition to the places where Legality Rules normally apply (see 12.3), these rules apply also in the private part of an instance of a generic unit. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

Ramification: In order to enforce these rules without breaking privacy, we cannot allow a tagged private type to have hidden indexing aspects. There is no problem if the private type is not tagged (as the indexing aspects cannot be specified on descendants in that case).

We don’t need an assume-the-worst rule as deriving from formal tagged types is not allowed in generic bodies.

A generalized indexing is illegal if the equivalent prefixed view (see below) is illegal.

**Syntax**

genrated indexing ::= indexable_container_object_prefix actual_parameter_part

**Name Resolution Rules**

The expected type for the indexable_container_object_prefix of a generalized_indexing is any indexable container type.
Ramification: A prefix can be an implicit dereference (see 4.1), so an access-to-indexable container object can be the prefix (English meaning!) of a generalized indexing.

If the Constant_Indexing aspect is specified for the type of the indexable container object prefix of a generalized indexing, then the generalized indexing is interpreted as a constant indexing under the following circumstances:

- when the Variable_Indexing aspect is not specified for the type of the indexable container object prefix;
- when the indexable container object prefix denotes a constant;
- when the generalized indexing is used within a primary where a name denoting a constant is permitted.

Ramification: This means it is not interpreted as a constant indexing for the variable name in the LHS of an assignment (not inside a primary), nor for the name used for an out or in out parameter (not allowed to be a constant), nor for the name in an object renaming (not inside a primary), unless there is no Variable_Indexing aspect defined.

Otherwise, the generalized indexing is interpreted as a variable indexing.

When a generalized indexing is interpreted as a constant (or variable) indexing, it is equivalent to a call on a prefixed view of one of the functions named by the Constant_Indexing (or Variable_Indexing) aspect of the type of the indexable container object prefix with the given actual_parameter_part, and with the indexable container object prefix as the prefix of the prefixed view.

Ramification: In other words, the generalized indexing is equivalent to:

\[ \text{indexable container object prefix}.\text{Indexing}\text{actual parameter part} \]

where Indexing is the name specified for the Constant_Indexing or Variable_Indexing aspect. This equivalence is then resolved in the normal way; the aspect specifies a name, it does not denote declarations.

NOTE The Constant_Indexing and Variable_Indexing aspects cannot be redefined when inherited for a derived type, but the functions that they denote can be modified by overriding or overloading.

Examples

\{A112-0429-1\} Examples of the specification and use of generalized indexing:

\{A105-0268-1\} \{A105-0292-1\} `type Indexed_Barrel is tagged ...` with Variable_Indexing => Find;

- `-- Indexed_Barrel is an indexable container type.`
- `-- Find is the generalized indexing operation.`

\{A105-0268-1\} `function Find (B : aliased in out Indexed_Barrel; Key : String) return Ref_Element;` `-- Return a reference to an element of a barrel (see 4.1.5).`

\{A105-0268-1\} `IB : aliased Indexed_Barrel;` `-- IB : aliased Indexed_Barrel;`

\{A105-0268-1\} `-- All of the following calls are then equivalent:`

\{A105-0268-1\} `Find (IB,"pear").Data.all := Element'(...);` `-- Traditional call`
\{A105-0268-1\} `IB.Find ("pear").Data.all := Element'(...);` `-- Call of prefixed view`
\{A105-0268-1\} `IB."pear" := Element'(...);` `-- Implicit dereference (see 4.1.5)`
\{A105-0268-1\} `IB ("pear") := Element'(...);` `-- Implicit indexing and dereference`
\{A105-0268-1\} `IB ("pear").Data.all := Element'(...);` `-- Implicit indexing only`

Extensions to Ada 2005

\{A105-0139-2\} Aspects Constant_Indexing and Variable_Indexing, and the generalized_indexing syntax are new.

Incompatibilities With Ada 2012

\{A112-0160-1\} Correction: Prevented a derived type from specifying Constant_Indexing if the ancestor specified Variable_Indexing (and vice versa). This is necessary to preserve the intent that for an object Obj whose tag is that of its nominal subtype, TClass(Obj)(I) always has the same meaning as Obj(I). Situations like this should be rare in practice; most types will either define both aspects or neither.

\{A112-0204-1\} Correction: Added a rule that a generalized indexing is illegal if the equivalent prefixed view would be illegal. If the prefixed view would be illegal for any reason, Ada 2012 would have allowed the generalized indexing
while Ada 2022 does not. This violated the principle that a generalized indexing and the equivalent prefixed view have the same semantics; practically, the code may not have worked anyway if a compiler implemented generalized indexing by code expansion into the canonical form. Thus, such code wasn’t practically portable.

Wording Changes from Ada 2012

{AI12-0104-1} Corrigendum: Converted confusing and unnecessary normative wording about "overriding an aspect" into a note.

{AI12-0138-1} Corrigendum: Defined Constant_Indexing and Variable_Indexing to be nonoveridable. This is merely a new description for Legality Rules which already applied to these aspects.

{AI12-0428-1} Correction: Allowed the completion of a private type to use declarations from either the visible part or the private part.

4.2 Literals

[A literal represents a value literally, that is, by means of notation suited to its kind.] A literal is either a numeric_literal, a character_literal, the literal null, or a string_literal.

Discussion: An enumeration literal that is an identifier rather than a character_literal is not considered a literal in the above sense, because it involves no special notation “suited to its kind”. It might more properly be called an enumeration_identifier, except for historical reasons.

Name Resolution Rules

This paragraph was deleted.{AI95-00230-01} The expected type for a literal null shall be a single access type.

Discussion: This new wording ("expected type ... shall be a single ... type") replaces the old "shall be determinable" stuff. It reflects an attempt to simplify and unify the description of the rules for resolving aggregates, literals, type conversions, etc. See 8.6, “The Context of Overload Resolution” for the details.

For a name that consists of a character_literal, either its expected type shall be a single character type, in which case it is interpreted as a parameterless function_call that yields the corresponding value of the character type, or its expected profile shall correspond to a parameterless function with a character result type, in which case it is interpreted as the name of the corresponding parameterless function declared as part of the character type's definition (see 3.5.1). In either case, the character_literal denotes the enumeration_literal_specification.

Discussion: See 4.1.3 for the resolution rules for a selector_name that is a character_literal.

Legality Rules

A character_literal that is a name shall correspond to a defining_character_literal of the expected type, or of the result type of the expected profile.

If the expected type for a string_literal is a string type, then for each character of the string_literal with a given expected string type, there shall be a corresponding defining_character_literal of the component type of the expected string type.

A literal null shall not be of an anonymous access type[, since such types do not have a null value (see 3.10)].
**Reason:** This is a legality rule rather than an overloading rule, to simplify implementations.

**Static Semantics**

\{AI95-00230-01\} \{AI12-0373-1\} An integer literal is of type `universal_integer`. A real literal is of type `universal_real`. The literal `null` is of type `universal_access`.

**Dynamic Semantics**

\{AI12-0249-1\} If its expected type is a numeric type, the evaluation of a numeric literal, or the literal `null`, yields the represented value. [In other cases, the effect of evaluating a numeric literal is determined by the Integer_Literal or Real_Literal aspect that applies (see 4.2.1).]

\{AI12-0249-1\} The evaluation of the literal `null` yields the null value of the expected type.

\{AI12-0295-1\} \{AI12-0325-1\} The evaluation of a string literal that is a primary and has an expected type that is a string type, yields an array value containing the value of each character of the sequence of characters of the string literal, as defined in 2.6. The bounds of this array value are determined according to the rules for positional_array_aggregates (see 4.3.3), except that for a null string literal, the upper bound is the predecessor of the lower bound. [In other cases, the effect of evaluating a string literal is determined by the String_Literal aspect that applies (see 4.2.1).]

\{AI12-0295-1\} \{AI12-0325-1\} For the evaluation of a string literal of a string type `T`, a check is made that the value of each character of the string literal belongs to the component subtype of `T`. For the evaluation of a null string literal of a string type, a check is made that its lower bound is greater than the lower bound of the base range of the index type. The exception Constraint_Error is raised if either of these checks fails.

**Ramification:** \{AI12-0005-1\} If no predicates apply to the component subtype, the checks on the characters need not involve more than two checks altogether, since one need only check the characters of the string with the lowest and highest position numbers against the range of the component subtype.


**Examples of literals:**

```
3.14159_26536  --  a real literal
1_345           --  an integer literal
'A'             --  a character literal
"Some Text"     --  a string literal
```

**Incompatibilities With Ada 83**

Because character literals are now treated like other literals, in that they are resolved using context rather than depending on direct visibility, additional qualification might be necessary when passing a character literal to an overloaded subprogram.

**Extensions to Ada 83**

Character literals are now treated analogously to `null` and string literals, in that they are resolved using context, rather than their content; the declaration of the corresponding defining_character_l literal need not be directly visible.

**Wording Changes from Ada 83**

Name Resolution rules for enumeration literals that are not character literals are not included anymore, since they are neither syntactically nor semantically "literals" but are rather names of parameterless functions.
Null now has type universal access, which is similar to other literals. Null can be used with anonymous access types.

The rules in this subclause are adjusted to allow for the possibility of user-defined literals. These are fully documented in the next subclause.

4.2.1 User-Defined Literals

Using one or more of the aspects defined below, a type may be specified to allow the use of one or more kinds of literals as values of the type.

Static Semantics

The following type-related operational aspects (collectively known as user-defined literal aspects) may be specified for a type T:

This aspect is specified by a function name that statically denotes a function with a result type of T and one in parameter that is of type String and is not explicitly aliased.

Aspect Description for Integer_Literal: Defines a function to implement user-defined integer literals.

This aspect is specified by a function name that statically denotes a function with a result type of T and one in parameter that is of type String and is not explicitly aliased, and optionally a second function (overloading the first) with a result type of T and two in parameters of type String that are not explicitly aliased.

Aspect Description for Real_Literal: Defines a function or functions to implement user-defined real literals.

Aspect Description for String_Literal: Defines a function to implement user-defined string literals.

Ramification: The following example is legal because the resolution of an aspect definition for an aspect that is defined to be a subprogram is based on the profile required for that aspect (see 13.1.1):

package Pkg1 is
  type T is record
    X, Y : Integer;
  end record
  with Integer_Literal => Int_Lit;
  function Int_Lit (X, Y : T) return Duration;    -- Wrong profile.
  function Int_Lit (Lit_Image : String) return T;  -- Right profile.
end Pkg1;

User-defined literal aspects are nonoverridable (see 13.1.1).

Discussion: This means that in this example

package Pkg2 is
  type T1 is record
    X, Y : Integer;
  end record with Integer_Literal => I_L;
  function I_L (S : String) return T1 is ((0, 0));
  type T2 is new T1;
  function I_L (Lit_Image : String) return T2 is ((1, 1));
  X : T2 := 123;
end Pkg2;

the initial value of Pkg2.X is (1,1), not (0,0).

When a numeric literal is interpreted as a value of a non-numeric type T or a string literal is interpreted as a value of a type T that is not a string type (see 4.2), it is equivalent to a
call to the subprogram denoted by the corresponding aspect of \(T\): the Integer_Literal aspect for an integer literal, the Real_Literal aspect for a real literal, and the String_Literal aspect for a string literal. The actual parameter of this notional call is a string literal representing a sequence of characters that is the same as the sequence of characters in the original numeric literal, or the sequence represented by the original string literal.

**Discussion:** This equivalence defines, for example, the nominal type, the nominal subtype, and the accessibility level of a user-defined literal. It also has the consequence that a user-defined literal shall not be of an abstract type (because that would be equivalent to a nondispatching call to an abstract function). This equivalence also defines the Dynamic Semantics of evaluating a user-defined literal.

The (sub)type of the actual parameter to this call is determined by the profile of the appropriate aspect, and the bounds of the string literal are defined by the usual rules for the bounds of a string literal.

\{AI12-0342-1\} Such a literal is said to be a user-defined literal.

\{AI12-0394-1\} When a named number that denotes a value of type universal_integer is interpreted as a value of a non-numeric type \(T\), it is equivalent to a call to the function denoted by the Integer_Literal aspect of \(T\). The actual parameter of this notional call is a String having a textual representation of a decimal integer literal optionally preceded by a minus sign, representing the same value as the named number.

\{AI12-0394-1\} When a named number that denotes a value of type universal_real is interpreted as a value of a non-numeric type \(T\), it is equivalent to a call to the two-parameter function denoted by the Real_Literal aspect of \(T\), if any. The actual parameters of this notional call are each a String with the textual representation of a decimal integer literal, with the first optionally preceded by a minus sign, where the first String represents the same value as the numerator, and the second the same value as the denominator, of the named number when represented as a rational number in lowest terms, with a positive denominator.

**Legality Rules**

\{AI12-0249-1\} \{AI12-0295-1\} \{AI12-0325-1\} \{AI12-0342-1\} The Integer_Literal or Real_Literal aspect shall not be specified for a type \(T\) if the full view of \(T\) is a numeric type. The String_Literal aspect shall not be specified for a type \(T\) if the full view of \(T\) is a string type.

\{AI12-0342-1\} For a nonabstract type, the function directly specified for a user-defined literal aspect shall not be abstract.

\{AI12-0342-1\} For a tagged type with a partial view, a user-defined literal aspect shall not be directly specified on the full type.

This paragraph was deleted:

\{AI12-0342-1\} \{AI12-0394-1\} \{AI22-0003-1\} If a nonabstract tagged type inherits any user-defined literal aspect, then each inherited aspect shall be directly specified as a nonabstract function for the type unless the inherited aspect denotes a nonabstract function, or functions, and the type is a null extension.

\{AI12-0394-1\} If a named number that denotes a value of type universal_integer is interpreted as a value of a non-numeric type \(T\), \(T\) shall have an Integer_Literal aspect. If a named number that denotes a value of type universal_real is interpreted as a value of a non-numeric type \(T\), \(T\) shall have a Real_Literal aspect, and the aspect shall denote a function that has two in parameters, both of type String, with result of type \(T\).

\{AI12-0249-1\} \{AI12-0342-1\} In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.
Bounded (Run-Time) Errors

It is a bounded error if the evaluation of a literal or named number that has an expected type with a specified user-defined literal aspect propagates an exception. Either Program_Error or the exception propagated by the evaluation is raised at the point of use of the value of the literal or named number. If it is recognized prior to run time that evaluation of such a literal or named number will inevitably (if executed) result in such a bounded error, then this may be reported as an error prior to run time.

Implementation Note: As always, an implementation may apply "as-if" optimizations (those that result in the same external effects in the absence of erroneous execution) to the function calls associated with user-defined literals. In particular, if the function associated with a user-defined literal aspect has a Global aspect that indicates no references to global variables, then a number of optimizations are available to the implementation:

- The implementation can evaluate a user-defined literal function at compile-time if it has access to the body of the function (for example, if it is inlined), and that body doesn't reference anything evaluated at runtime. If the compile-time evaluation results in an exception, this bounded error allows the compilation unit to be rejected.

- Implementations can use existing permissions (see 6.1.2) to avoid evaluating the function associated with a user-defined literal more than once for a particular literal value. This evaluation can be "hoisted" (done once per compilation unit during the elaboration of the unit) if the compiler can prove that the function doesn't depend on any constants or locals with a runtime value not yet elaborated.

- If the literal value is not needed by the execution of the program, the function call can be omitted even if it might have side-effects (again, see 6.1.2).

Examples

Examples of the specification and use of user-defined literals:

```
subtype Roman_Character is Wide_Wide_Character
  with Static_Predicate =>
  Roman_Character in 'I' | 'V' | 'X' | 'L' | 'C' | 'D' | 'M';
```

```
Max_Roman_Number : constant := 3_999; -- MMMCMXCIX
```

```
type Roman_Number is range 1 .. Max_Roman_Number
  with String_Literal => To_Roman_Number;
```

```
function To_Roman_Number (S : Wide_Wide_String) return Roman_Number
  with Pre => S'Length > 0
             and then
                 (for all Char of S => Char in Roman_Character);
```

```
function To_Roman_Number (S : Wide_Wide_String) return Roman_Number
  is
    declare
      R : constant array (Integer range <>) of Roman_Number :=
        (for D in S'Range => Roman_Digit'Enum_Rep
         (Roman_Digit'Wide_Wide_Value (''' & S(D) & ''')));
    begin
      for I in R'Range =>
        if I < R'Last then R(I) < R(I + 1) then -1 else 1 end if * R(I)
        'Reduce(12, 0);
    end;
```

```
X : Roman_Number := "III" * "IV" * "XII"; -- 144 (that is, CXLIV)
```

Extensions to Ada 2012

The user-defined literal aspects Integer Literal, Real Literal, and String Literal are new.

Wording Changes from Ada 2022

Corrigendum: Removed a vestigial Legality Rule that conflicted with the blanket rules for nonoverridable aspects.
4.3 Aggregates

[ An aggregate combines component values into a composite value of an array type, record type, or record extension.]

Term entry: aggregate — construct used to define a value of a composite type by specifying the values of the components of the type

Syntax

\{AI12-0127-1\} \{AI12-0212-1\} aggregate ::= _record_aggregate | extension_aggregate | array_aggregate 
| delta_aggregate | container_aggregate

Name Resolution Rules

\{AI95-00287-01\} \{AI12-0127-1\} \{AI12-0212-1\} \{AI12-0307-1\} The expected type for an aggregate shall be a single nonlimited array type, a single type with the Aggregate aspect specified, or a single descendant of a record type, or of a record extension.

Discussion: See 8.6, “The Context of Overload Resolution” for the meaning of “shall be a single ... type”.

Ramification: \{AI05-0005-1\} There are additional rules for each kind of aggregate. These aggregate rules are additive; a legal expression needs to satisfy all of the applicable rules. That means the rule given here must be satisfied even when it is syntactically possible to tell which specific kind of aggregate is being used.

Reason: \{AI12-0005-1\} \{AI12-0127-1\} \{AI12-0212-1\} \{AI12-0307-1\} Generally, we don't want to look in aggregates to resolve them. For instance, Ada 95 allowed array types to match extension aggregates, even though those have to be record types. Thus, we allow any record type with any visible (nondiscriminant) components to match an aggregate, even though only delta aggregates allow private types or private extensions. Similarly, we allow any container type to match an aggregate, even though only container aggregates allow container types.

Legality Rules

\{AI12-0127-1\} \{AI12-0212-1\} A record_aggregate, extension_aggregate, or container_aggregate is an aggregate shall not be of a class-wide type.

Ramification: When the expected type in some context is class-wide, an aggregate has to be explicitly qualified by the specific type of value to be created, so that the expected type for the aggregate itself is specific.

Discussion: We used to disallow aggregates of a type with unknown discriminants. However, that was unnecessarily restrictive in the case of an extension aggregate, and irrelevant to a record aggregate (since a type that is legal for a record aggregate could not possibly have unknown discriminants) and to an array aggregate (the only specific types that can have unknown discriminants are private types, private extensions, and types derived from them).

Reason: \{AI12-0127-1\} We don't mention delta aggregates, as those can get the specific type from the object represented by the base_expression (possibly at run time). We don't mention array aggregates, as those cannot even be of a tagged type, so being class-wide is impossible.

Dynamic Semantics

For the evaluation of an aggregate, an anonymous object is created and values for the components or ancestor part are obtained (as described in the subsequent subclause for each kind of the aggregate) and assigned into the corresponding components or ancestor part of the anonymous object. Obtaining the values and the assignments occur in an arbitrary order. The value of the aggregate is the value of this object.

Discussion: The ancestor part is the set of components inherited from the ancestor type. The syntactic category ancestor_part is the expression or subtype_mark that specifies how the ancestor part of the anonymous object should be initialized.

Ramification: The assignment operations do the necessary value adjustment, as described in 7.6. Note that the value as a whole is not adjusted — just the subcomponents (and ancestor part, if any). 7.6 also describes when this anonymous object is finalized.
If the `ancestor_part` is a `subtype_mark` the `Initialize` procedure for the ancestor type is applied to the ancestor part after default-initializing it, unless the procedure is abstract, as described in 7.6. The `Adjust` procedure for the ancestor type is not called in this case, since there is no assignment to the ancestor part as a whole.

If an `aggregate` is of a tagged type, a check is made that its value belongs to the first subtype of the type. Constraint_Error is raised if this check fails. Any discriminant check is performed before the initialization of any nondiscriminant component of the aggregate object.

The order of checks and initializations is generally unspecified. However, we need to do discriminant checks before initializing any discriminant-dependent components, in order to avoid creating components that the ultimate subtype does not have. Most such problems are prevented by the rules about needed components for an `aggregate` (see 4.3.1), but not those that result from deriving from a constrained subtype.

We now allow `extension_aggregates`.

We have adopted new wording for expressing the rule that the type of an aggregate shall be determinable from the outside, though using the fact that it is nonlimited record (extension) or array.

An `aggregate` now creates an anonymous object. This is necessary so that controlled types will work (see 7.6).

In Ada 95, a limited type is not considered when resolving an `aggregate`. Since Ada 2005 now allows limited aggregates, we can have incompatibilities. For example:

```ada
type Lim is limited
  record
    Comp: Integer;
  end record;

type Not_Lim is
  record
    Comp: Integer;
  end record;

procedure P(X: Lim);
procedure P(X: Not_Lim);
P((Comp => 123)); -- Illegal in Ada 2005, legal in Ada 95
```

The call to `P` is ambiguous in Ada 2005, while it would not be ambiguous in Ada 95 as the `aggregate` could not have a limited type. Qualifying the `aggregate` will eliminate any ambiguity. This construction would be rather confusing to a maintenance programmer, so it should be avoided, and thus we expect it to be rare.

Aggregates can be of a limited type.

We now allow types with the `Aggregate` aspect specified ("container types"), as well as private types and extensions descended from a record type or extension, to match all forms of `aggregate`. These types are only allowed for new types of `aggregate` (container, `aggregates` for the `Aggregate` aspect, and `delta_aggregates` for private types), but, consistent with other forms of `aggregate`, we do not look at the form of the `aggregate` to determine resolution. This can be incompatible in usually unlikely cases, where overloading of a container or private type with a type that was previously allowed in `aggregates` makes an existing call ambiguous. Unfortunately, `Ada.Containers.Vectors` has a number of such overloading for `Insert`, `Append`, `Prepend`, and "+".

This can easily be fixed by qualifying the `aggregate` with the correct type.
Wording Changes from Ada 2022

\{AI22-0007-1\} Corrigendum: Clarified that discriminant always occur before creating any non-discriminant components (in particular, discriminant-dependent components). This is specifying unspecified behavior, so it does not represent an inconsistency, but the possibility exists that an unusual program where initialization (or lack thereof) of some component has a side-effect that affects later execution would change behavior.

\{AI22-0032-1\} Corrigendum: Corrected the omission of container aggregates from the list of aggregates that cannot be class-wide. This could be considered an incompatibility, but since no static or dynamic semantics are defined for such an aggregate, it is unlikely that any implementation would usefully allow such a thing. As such, it is highly unlikely to occur in any code.

4.3.1 Record Aggregates

[In a record_aggregate, a value is specified for each component of the record or record extension value, using either a named or a positional association.]

Syntax

```plaintext
record_aggregate ::= (record_component_association_list)
record_component_association_list ::= record_component_association {, record_component_association}
| null record
```

\{AI95-00287-01\} record_component_association ::= [component_choice_list =>] expression
| component_choice_list => <>

\{AI12-0212-1\} component_choice_list ::= component_selector_name {"|" component_selector_name}
| others

A record_component_association is a named component association if it has a component_choice_list; otherwise, it is a positional component association. Any positional component associations shall precede any named component associations. If there is a named association with a component_choice_list of others, it shall come last.

Discussion: These rules were implied by the BNF in an early version of the RM9X, but it made the grammar harder to read, and was inconsistent with how we handle discriminant constraints. Note that for array aggregates we still express some of the rules in the grammar, but array aggregates are significantly different because an array aggregate is either all positional (with a possible others at the end), or all named.

In the record_component_association_list for a record_aggregate, if there is only one association, it shall be a named association.

Reason: \{AI95-0264-1\} Otherwise, the construct would be interpreted as a parenthesized expression. This is considered a syntax rule, since it is relevant to overload resolution. We choose not to express it with BNF so we can share the definition of record_component_association_list in both record_aggregate and extension_aggregate.

Ramification: The record_component_association_list of an extension_aggregate does not have such a restriction.

Name Resolution Rules

\{AI95-00287-01\} The expected type for a record_aggregate shall be a single nonlimited record type or record extension.

Ramification: This rule is used to resolve whether an aggregate is an array_aggregate or a record_aggregate. The presence of a with is used to resolve between a record_aggregate and an extension_aggregate.

\{AI12-0127-1\} For the record_component_association_list of a record_aggregate, all components of the composite value defined by the aggregate are needed; for the association list of an extension_aggregate, only those components not determined by the ancestor expression or subtype are
needed (see 4.3.2). Each \texttt{component_selector_name} in a \texttt{record_component_association} of a \texttt{record_aggregate} or \texttt{extension_aggregate} shall denote a needed component [(including possibly a discriminant)]. Each \texttt{component_selector_name} in a \texttt{record_component_association} of a \texttt{record_delta_aggregate} (see 4.3.4) shall denote a nondiscriminant component of the type of the aggregate.

\begin{align*}
9.a \quad \textbf{Ramification:} \text{ For the association list of a record_aggregate, “needed components” includes every component of the composite value, but does not include those in unchosen variants (see AI83-309). If there are variants, then the value specified for the discriminant that governs them determines which variant is chosen, and hence which components are needed.}

9.b \quad \text{If an extension defines a new known_discriminant_part, then all of its discriminants are needed in the component association list of an extension aggregate for that type, even if the discriminants have the same names and types as discriminants of the type of the ancestor expression. This is necessary to ensure that the positions in the \texttt{record_component_association_list} are well defined, and that discriminants that govern variant_parts can be given by static expressions.}

9.c/5 \quad \textbf{Reason:} We don’t define “needed” for \texttt{record_delta_aggregates} so that there is no completeness requirement. But that means that we need to ensure that the rules using “needed” doesn’t appear to apply to \texttt{record_delta_aggregates}, and we also need Legality Rules to prevent giving the same component twice and giving components from two different variants.

9.d/5 \quad \textbf{Term entry: needed component — component of a record type or record extension that is required to have its value specified within a given aggregate.}

The expected type for the expression of a \texttt{record_component_association} is the type of the \texttt{associated} component(s); the associated component(s) are as follows:

\begin{itemize}
\item For a positional association, the component [(including possibly a discriminant)] in the corresponding relative position (in the declarative region of the type), counting only the needed components;
\item For a positional association, the component [(including possibly a discriminant)] in the corresponding relative position (in the declarative region of the type), counting only the needed components;
\item For a named association with one or more \texttt{component_selector_names}, the named component(s);
\item For a named association with the reserved word \texttt{others}, all needed components that are not associated with some previous association.
\end{itemize}

\textbf{Legality Rules}

If the type of a \texttt{record_aggregate} is a record extension, then it shall be a descendant of a record type, through one or more record extensions (and no private extensions).

\begin{align*}
15/5 \quad \textit{AI05-0016-1} \quad \textit{AI12-0127-1} \quad \textbf{A record_component_association_list shall be}\textit{The reserved words \texttt{null record} only if the list occurs in a \texttt{record_aggregate} or \texttt{extension_aggregate}, and only if} \textit{there are no components needed for that list}\textit{a given record_component_association_list, then the reserved words \texttt{null record} shall appear rather than a list of record_component_associations.}

15.a \quad \textbf{Ramification:} \text{For example, "(null record)" is a record_aggregate for a null record type. Similarly, "(T(A) with null record)" is an extension_aggregate for a type defined as a null record extension of T.}

15.b/3 \quad \textit{AI05-0016-1} \quad \textit{If no components are needed and \texttt{null record} is not used, the record_component_association must necessarily be \texttt{others => <>}, as that is the only record_component_association that does not require an associated component.}

16/5 \quad \textit{AI95-00287-01} \quad \textit{AI05-0199-1} \quad \textit{AI12-0046-1} \quad \textit{AI12-0127-1} \quad \textbf{For a record_aggregate or extension_aggregate, each record_component_association other than an \texttt{others} choice with a \texttt{<>} shall have at least one associated component, and each needed component shall be associated with exactly one record_component_association. For a record_delta_aggregate, each component_selector_name}
of each component_choice list shall denote a distinct nondiscriminant component of the type of the aggregate. If a record_component_association with an expression has two or more associated components, all of them shall be of the same type, or all of them shall be of anonymous access types whose subtypes statically match. In addition, Legality Rules are enforced separately for each associated component.

**Ramification:** [AI95-00287-01] These rules apply to an association with an others choice, with an expression. An others choice with a <> can match zero components or several components with different types.

**Reason:** [AI95-00287-01] Without these rules, there would be no way to know what was the expected type for the expression of the association. Note that some of the rules do not apply to <> associations, as we do not need to resolve anything. We allow others => <> to match no components as this is similar to array aggregates. That means that (others => <>) always represents a default-initialized record or array value.

This paragraph was deleted. **Discussion:** [AI12-0046-1] AI83-00244 also requires that the expression shall be legal for each associated component. This is because even though two components have the same type, they might have different subtypes. Therefore, the legality of the expression, particularly if it is an array aggregate, might differ depending on the associated component's subtype. However, we have relaxed the rules on array aggregates slightly for Ada 95, so the staticness of an applicable index constraint has no effect on the legality of the array aggregate to which it applies. See 4.3.3. This was the only case (that we know of) where a subtype provided by context affected the legality of an expression.

**Ramification:** The rule that requires at least one associated component for each record_component_association implies that there can be no extra associations for components that don't exist in the composite value, or that are already determined by the ancestor expression or subtype of an extension_aggregate.

The second part of the first sentence ensures that no needed components are left out, nor specified twice.

**{AI12-0046-1} {AI12-0127-1}** If a record_component_association with an expression has two or more associated components, all of them shall be of the same type, or all of them shall be of anonymous access types whose subtypes statically match. In addition, Legality Rules are enforced separately for each associated component.

**Discussion:** [AI12-0046-1] AI83-00244 also requires that the expression shall be legal for each associated component. Ada 95 omitted this wording, as it was thought that all cases of difference had been eliminated. That probably was true, but Ada 2005 reintroduced cases where the types match but the legality differs. For example:

```ada
type Rec (D : access Integer) is record
   F : access Integer;
end record;
begin
   declare
      X : aliased Integer;
      R : Rec := (D | F => X'Access); -- Legal for D, illegal for F
end;
```

There are additional ways for this to happen; because of cases like the above we require that the Legality Rules are checked individually for each associated component.

**{AI05-0220-1} {AI12-0086-1} {AI12-0127-1}** For a record_aggregate or extension_aggregate, if a variant_part P is nested within a variant V that is not selected by the discriminant value governing the variant_part enclosing V, then there is no restriction on the discriminant governing P. Otherwise, the value of the field the components of a variant_part are needed, then the value of a discriminant that governs the variant_part P shall be given by a static expression, or by a nonstatic expression having a constrained static nominal subtype. In this latter case of a nonstatic expression, there shall be exactly one discrete_choice list of P that covers each value that belongs to the nominal subtype and satisfies the predicates of the subtype, and there shall be at least one such value unless P is nested within a variant V that is not selected by the discriminant value governing the variant_part enclosing V.

**Ramification:** This expression might either be given within the aggregate itself, or in a constraint on the parent subtype in a derived_type_definition for some ancestor of the type of the aggregate.

**{AI12-0086-1}** This means that in the nonstatic value case, the (static) subtype cannot have a null range.

**{AI95-00287-01}** A record_component_association for a discriminant without a default_expression shall have an expression rather than <>.
Reason: A discriminant must always have a defined value, but <> means uninitialized for a discrete type unless the component has a default value.

{AI12-0127-1} A record_component_association of the record_component_association_list of a record_delta_aggregate shall not:

17.2/5  
• {AI12-0418-1} use the box compound delimiter <> rather than an expression;
• have an expression of a limited type;
• omit the component_choice_list; or

Ramification: {AI12-0127-1} A record_delta_aggregate cannot use positional notation; all choices shall be named choices.

17.6/5  
• have a component_choice_list that is an others choice.

{AI12-0127-1} For a record_delta_aggregate, no two component_selector_names shall denote components declared within different variants of the same variant_part.

Dynamic Semantics

The evaluation of a record_aggregate consists of the evaluation of the record_component_association_list.

19/5  
{AI12-0086-1} {AI12-0451-1} For the evaluation of a record_component_association_list, any per-object constraints (see 3.8) for components specified in the association list are elaborated and any expressions are evaluated and converted to the subtype of the associated component. Any constraint elaborations and expression evaluations (and conversions) occur in an arbitrary order, except that the expression for a discriminant is evaluated (and converted) prior to the elaboration of any per-object constraint that depends on it, which in turn occurs prior to the evaluation and conversion of the expression for the component with the per-object constraint. If the value of a discriminant that governs a selected variant_part is given by a nonstatic expression, and the evaluation of that expression yields a value that does not belong to the nominal subtype of the expression, then Constraint_Error is raised.

Ramification: The conversion in the first rule might raise Constraint_Error.

Discussion: This check in the first rule presumably happened as part of the dependent compatibility check in Ada 83.

Ramification: {AI12-0086-1} The test on the value of the discriminant can only fail if the value is outside the base range of its type, does not satisfy the (static) predicates of the subtype (possible when the predicate is disabled), or is an invalid representation. This is a rule similar to that used for case statements. As with case statements, this is not a “check”; it cannot be Suppressed.

For a record_component_association with an expression, the expression defines the value for the associated component(s). For a record_component_association with <>, if the component declaration has a default expression, that default expression defines the value for the associated component(s); otherwise, the associated component(s) are initialized by default as for a stand-alone object of the component subtype (see 3.3.1).

The expression of a record_component_association is evaluated (and converted) once for each associated component.

Ramification: {AI05-0005-1} We don't need similar language for <>, as we're considering the value of <> for each individual component. Each component has its own default expression or its own default initialization (they can be different for each component; the components even could have different types), and each one has to be evaluated. So there is no need to repeat that.

NOTE {AI12-0447-1} By the rules given above, for {AI12-0447-1} a record_aggregate with positional associations, expressions specifying discriminant values appear first and in the same order as their corresponding discriminant specifications, since the known_discriminant_part occurs given first in the declaration of the type, they have to be in the same order as in the known_discriminant_part.
Examples

Example of a record aggregate with positional associations:

(4, July, 1776)                      -- see 3.8

Examples of record aggregates with named associations:

(Day => 4, Month => July, Year => 1776)
(Month => July, Day => 4, Year => 1776)

(Disk, Closed, Track => 5, Cylinder => 12)          -- see 3.8.1
(Unit => Disk, Status => Closed, Cylinder => 9, Track => 1)

{AI95-00287-01} Example of component associations with several choices:

(Value => 0, Succ|Pred => new Cell'(0, null, null)) -- see 3.10.1
                          -- The allocator is evaluated twice:
                          -- Succ and Pred designate different cells
                          (Value => 0, Succ|Pred => <>)                      -- see 3.10.1
                          -- Succ and Pred will be set to null

Examples of record aggregates for tagged types (see 3.9 and 3.9.1):

Expression'(null record)
Literal'(Value => 0.0)
Painted_Point'(0.0, Pi/2.0, Paint => Red)

Extensions to Ada 83

Null record aggregates may now be specified, via "(null record)". However, this syntax is more useful for null record extensions in extension aggregates.

Wording Changes from Ada 83

Various AIs have been incorporated (AI83-00189, AI83-00244, and AI83-00309). In particular, Ada 83 did not explicitly disallow extra values in a record aggregate. Now we do.

Extensions to Ada 95

{AI95-00287-01} <> can be used in place of an expression in a record aggregate, default initializing the component.

Wording Changes from Ada 95

{AI95-00287-01} Limited record aggregates are allowed (since all kinds of aggregates can now be limited, see 4.3).

Incompatibilities With Ada 2005

{AI05-0220-1} Correction: Corrected wording so that the rule for discriminants governing variant parts was not effectively circular. The change makes a few aggregates where a nonstatic discriminant governs an empty variant part illegal. However, most Ada implementations already enforce some version of the new rule and already reject these aggregates. So it is unlikely that any incompatibility will be noticed in practice.

Extensions to Ada 2005

{AI05-0016-1} Correction: Fixed the wording so that others => <> can be used in place of null record. This is needed to avoid a generic contract issue for generic bodies: we do not want to have to assume the worst to disallow others => <> if the record type might be a null record.

{AI05-0199-1} Correction: We now allow multiple components with anonymous access types to be specified with a single component association. This is to be consistent with the capabilities of a named access type.

Extensions to Ada 2012

{AI12-0086-1} The value of a discriminant that governs a variant part in an aggregate can be nonstatic if the nominal subtype of the discriminant expression is static and all possible values select a single variant.
4.3.2 Extension Aggregates

[An extension_aggregate specifies a value for a type that is a record extension by specifying a value or subtype for an ancestor of the type, followed by associations for any components not determined by the ancestor_part.]

Language Design Principles

The model underlying this syntax is that a record extension can also be viewed as a regular record type with an ancestor "prefix". The record_component_association_list corresponds to exactly what would be needed if there were no ancestor/prefix type. The ancestor_part determines the value of the ancestor/prefix.

Syntax

extension_aggregate ::= (ancestor_part with record_component_association_list)

ancestor_part ::= expression | subtype_mark

Name Resolution Rules

The expected type for an extension_aggregate shall be a single nonlimited type that is a record extension. If the ancestor_part is an expression, it is expected to be of any nonlimited tagged type.

Reason: We could have made the expected type T'Class where T is the ultimate ancestor of the type of the aggregate, or we could have made it even more specific than that. However, if the overload resolution rules get too complicated, the implementation gets more difficult and it becomes harder to produce good error messages.

Ramification: This rule is additive with the rule given in 4.3. That means the 4.3 rule must be satisfied even though it is always syntactically possible to tell that something is an extension aggregate rather than another kind of aggregate. Specifically, that means that an extension aggregate is ambiguous if the context is overloaded on array and/or untagged record types, even though those are never legal contexts for an extension aggregate. Thus, this rule acts more like a Legality Rule than a Name Resolution Rule.

Legality Rules

If the ancestor_part is a subtype_mark, it shall denote a specific tagged subtype. If the ancestor_part is an expression, it shall not be dynamically tagged. The type of the extension_aggregate shall be a descendant of derived from the type of the ancestor_part (the ancestor type), through one or more record extensions (and no private extensions). If the ancestor_part is a subtype_mark, the view of the ancestor type from which the type is descended (see 7.3.1) shall not have unknown discriminants.

Reason: The expression cannot be dynamically tagged to prevent implicit "truncation" of a dynamically-tagged value to the specific ancestor type. This is similar to the rules in 3.9.2.

If the type of the ancestor_part is limited and at least one component is needed in the record_component_association_list, then the ancestor_part shall not have an operative constituent expression (see 4.4) that is a call to a function with an unconstrained result subtype be:

- a call to a function with an unconstrained result subtype; nor
• \{AI12-0317-1\} a parenthesized or qualified expression whose operand would violate this rule; nor
• \{AI12-0317-1\} a conditional expression (see 4.5.7) having at least one dependent expression that would violate this rule.

Reason: \{AI05-0067-1\} \{AI05-0244-1\} This restriction simplifies implementation, because it ensures that either the caller or the callee knows the size to allocate for the aggregate. Without this restriction, information from both caller and callee would have to be combined to determine the appropriate size.

\{AI05-0067-1\} The \(F(\ldots)\) with null record) case is exempt from this rule, because such extension aggregates are created internally for inherited functions returning null-extension types — we can't very well make those illegal. Moreover, we don't need the rule for null extensions, as the result can simply use the space returned by the function call.

\{AI12-0317-1\} The mention of “operative constituents” means that constructs like parenthesized expressions, qualified expressions, and conditional expressions are ignored when enforcing this rule.

Static Semantics
For the record_component_association_list of an extension_aggregate, the only components needed are those of the composite value defined by the aggregate that are not inherited from the type of the ancestor_part, plus any inherited discriminants if the ancestor_part is a subtype_mark that denotes an unconstrained subtype.

Dynamic Semantics
For the evaluation of an extension_aggregate, the record_component_association_list is evaluated. If the ancestor_part is an expression, it is also evaluated; if the ancestor_part is a subtype_mark, the components of the value of the aggregate not given by the record_component_association_list are initialized by default as for an object of the ancestor type. Any implicit initializations or evaluations are performed in an arbitrary order, except that the expression for a discriminant is evaluated prior to any other evaluation or initialization that depends on it.

\{AI05-0282-1\} If the type of the ancestor_part has discriminants and that are not inherited by the type of the extension_aggregate, then, unless the ancestor_part is not a subtype_mark that denotes an unconstrained subtype, then a check is made that each discriminant determined by the ancestor_part of the ancestor has the value specified for a corresponding discriminant, if any, either in the record_component_association_list, or in the derived_type_definition for some ancestor of the type of the extension_aggregate. Constraint_Error is raised if this check fails.

Ramification: Corresponding and specified discriminants are defined in 3.7. The rules requiring static compatibility between new discriminants of a derived type and the parent discriminant(s) they constrain ensure that at most one check is required per discriminant of the ancestor expression.

\{AI05-0282-1\} The check needs to be made any time that the ancestor is constrained; the source of the discriminants or the constraints is irrelevant.

NOTE 1 \{AI12-0447-1\} By the rules given in 4.3.1, if all components of the value of the extension_aggregate are determined by the ancestor_part, then the record_component_association_list will be required to be simply null_record.

NOTE 2 If the ancestor_part is a subtype_mark, then its type can be abstract. If its type is controlled, then as the last step of evaluating the aggregate, the Initialize procedure of the ancestor type is called, unless the Initialize procedure is abstract (see 7.6).

Examples
Examples of extension aggregates (for types defined in 3.9.1):

Painted_Point’(Point with Red) (Point’(P) with Paint => Black)
{AI12-0178-1} (Expression with Left => new Literal'(Value => 1.2), Right => new Literal'(Value => 3.4])
Addition'(Binop with null record)
-- presuming Binop is of type Binary_Operation

Extensions to Ada 83

Incompatibilities With Ada 95

{AI95-00306-01} Amendment Correction: Eliminated implicit “truncation” of a dynamically tagged value when it is used as an ancestor_expression. If an aggregate includes such an expression, it is illegal in Ada 2005. Such aggregates are thought to be rare; the problem can be fixed with a type conversion to the appropriate specific type if it occurs.

Wording Changes from Ada 95

{AI95-00287-01} Limited extension_aggregates are allowed (since all kinds of aggregates can now be limited, see 4.3).

Inconsistencies With Ada 2005

{AI05-00328-1} Correction: An extension_aggregate with an ancestor_part whose discriminants are constrained and inherited might now raise Constraint_Error if the aggregate’s type is constrained, while it was OK in Ada 2005. In almost all cases, this will make no difference as the constraint will be checked by the immediately following use of the aggregate, but it is possible to compare such an aggregate for equality; in this case, no exception would be raised by Ada 2005, while Ada 2012 will raise Constraint_Error. This should be very rare, and having the possibility means that the representation of the aggregate type has to be able to support unconstrained values of the type, even if the first subtype is constrained and no such objects can be created any other way.

Wording Changes from Ada 2012

{AI12-0317-1} Rewrote a Legality Rule to use the new term “operative constituent” in order to reduce duplication of text about ignoring parenthesized expressions and similar constructs.

4.3.3 Array Aggregates

In an array_aggregate, a value is specified for each component of an array, either positionally or by its index. For a positional_array_aggregate, the components are given in increasing-index order, with a final others, if any, representing any remaining components. For a named_array_aggregate, the components are identified by the values covered by the discrete_choices.

Language Design Principles

The rules in this subclause are based on terms and rules for discrete_choice_lists defined in 3.8.1, “Variant Parts and Discrete Choices”: For example, the requirements that others come last and stand alone are found there.

Syntax

{AI12-0306-1} array_aggregate ::= positional_array_aggregate | null_array_aggregate | named_array_aggregate

{AI95-00287-01} {AI12-0212-1} {AI12-0306-1} positional_array_aggregate ::=
An n-dimensional array_aggregate is one that is written as n levels of nested array_aggregates (or at the bottom level, equivalent string_literals). For the multidimensional case (n >= 2) the array_aggregates (or equivalent string_literals) at the n–1 lower levels are called subaggregates of the enclosing n-dimensional array_aggregate. The expressions of the bottom level subaggregates (or of the array_aggregate itself if one-dimensional) are called the array component expressions of the enclosing n-dimensional array_aggregate.

Ramification: Subaggregates do not have a type. They correspond to part of an array. For example, with a matrix, a subaggregate would correspond to a single row of the matrix. The definition of "n-dimensional" array_aggregate applies to subaggregates as well as aggregates that have a type.

To be honest: An others choice is the reserved word others as it appears in a positional_array_aggregate or as the discrete_choice of the discrete_choice_list in an array_component_association.

Name Resolution Rules

The expected type for an array_aggregate (that is not a subaggregate) shall be a single nonlimited array type. The component type of this array type is the expected type for each array component expression of the array_aggregate.

Ramification: The above rule requiring a single nonlimited array type (and similar ones for record and extension aggregates) resolves which kind of aggregate you have.

The expected type for each discrete_choice in any discrete_choice_list of a named_array_aggregate is the type of the corresponding index; the corresponding index for an array_aggregate that is not a subaggregate is the first index of its type; for an (n–m)-dimensional subaggregate within an array_aggregate of an n-dimensional type, the corresponding index is the index in position m+1.
The applicable index constraint applies to an array_aggregate that appears in such a context, as well as to any subaggregates thereof. In the case of an explicit_actual_parameter (or default_expression) for a call on a generic formal subprogram, no applicable index constraint is defined.

Reason: This avoids generic contract model problems, because only mode conformance is required when matching actual subprograms with generic formal subprograms.

}] The discrete_choice_list of an array_component_association (including an iterated_component_association) is allowed to have a discrete_choice that is a nonstatic choice_expression or that is a subtype_indication or ranged_discrete_range that defines a nonstatic or null range, only if it is the single discrete_choice of its discrete_choice_list, and either there is only one array_component_association in the enclosing

### 4.3.3 Array Aggregates

16 October 2023 236
array_component_association_list or the enclosing aggregate is an array_delta_aggregate, not an array_aggregate.

Discussion: We now allow a nonstatic others choice even if there are other array component expressions as well.

Ramification: {AI12-0127-1} We allow multiple dynamic choices in array_delta_aggregates, but only one dynamic choice per association even in that case.

{AI12-0212-1} Either all or none of the array_component_association_list shall be iterated_component_associations with an iterator_specification.

{AI05-0262-1} In a named_array_aggregate where all discrete_choices are static with more than one discrete_choice, no two discrete_choices are allowed to cover the same value (see 3.8.1); if there is no others choice, the discrete_choices taken together shall exactly cover a contiguous sequence of values of the corresponding index type.

Ramification: This implies that each component must be specified exactly once. See AI83-309.

Reason: {AI05-0262-1} This has to apply even if there is only one static discrete_choice; a single choice has to represent a contiguous range (a subtype_mark with a static predicate might represent a discontiguous set of values). If the (single) choice is a dynamic subtype, we don't need to make this check as no predicates are allowed (see 3.2.4) and thus the range has to be contiguous.

A bottom level subaggregate of a multidimensional array_aggregate of a given array type is allowed to be a string_literal only if the component type of the array type is a character type; each character of such a string_literal shall correspond to a defining_character_literal of the component type.

Static Semantics

A subaggregate that is a string_literal is equivalent to one that is a positional_array_aggregate of the same length, with each expression being the character_literal for the corresponding character of the string_literal.

To be honest: {AI12-0306-1} This is true even in cases where there is no corresponding legal positional_array_aggregate.

{AI12-0061-1} The subtype (and nominal subtype) of an index parameter is the corresponding index subtype.

Dynamic Semantics

{AI12-0212-1} For an array_aggregate that contains only array_component_associations that are iterated_component_associations with iterator_specifications, evaluation proceeds in two steps:

1. {AI12-0212-1} {AI12-0250-1} {AI22-0006-1} Each iterator_specification is elaborated (in an arbitrary order) and an iteration is performed solely to determine a maximum count for the number of values conditionally produced by the iteration (see 5.5 and 5.5.2); all of these counts are combined to determine the overall length of the array, and ultimately the limits on the bounds of the array (defined below);

2. {AI12-0212-1} {AI12-0250-1} {AI12-0327-1} {AI22-0006-1} A second iteration is performed for each of the iterator_specifications, in the order given in the aggregate, and for each value conditionally produced by the iteration (see 5.5 and 5.5.2), the associated expression is evaluated, its value is converted to the component subtype of the array type, and used to define the value of the next component of the array starting at the low bound and proceeding sequentially toward the high bound. As part of this second iteration, aA check is made that the second iteration results in the same number of elements as an array_length no greater than the maximum determined by the first iteration; Constraint_Error is raised if this check fails. This check is performed before any attempt to access any nonexistent element of the array object.
To be honest: {AI12-0212-1} {AI12-0250-1} {AI22-0006-1} Constraint_Error should be raised no later than when the iterations exceed the maximum array length; memory that doesn't belong to the aggregate temporary should not be overwritten.

Reason: {AI12-0006-1} The last sentence ensures that Constraint_Error is raised no later than when the iterations exceed the maximum array length; memory that doesn't belong to the aggregate temporary should not be overwritten.

{AI112-0212-1} The evaluation of any other array_aggregate of a given array type proceeds in two steps:

1. Any discrete_choices of this aggregate and of its subaggregates are evaluated in an arbitrary order, and converted to the corresponding index type;

2. The array component expressions of the aggregate are evaluated in an arbitrary order and their values are converted to the component subtype of the array type; an array component expression is evaluated once for each associated component.

Ramification: Subaggregates are not separately evaluated. The conversion of the value of the component expressions to the component subtype might raise Constraint_Error.

{AI05-0005-1} We don't need to say that <> is evaluated once for each component, as <> means that each component is initialized by default. That means that the actions defined for default initialization are applied to each component individually. Initializing one component by default and copying that to the others would be an incorrect implementation in general (although it might be OK if the default initialization is known to be constant).

Each expression in an array_component_association defines the value for the associated component(s). For an array_component_association with <>, the associated component(s) are initialized to the Default_Component_Value of the array type if this aspect has been specified for the array type; otherwise, they are initialized by default as for a stand-alone object of the component subtype (see 3.3.1).

During an evaluation of the expression of an iterated_component_association with a discrete_choice_list, the value of the corresponding index parameter is that of the corresponding index of the corresponding array component. During an evaluation of the expression of an iterated_component_association with an iterator_specification, the value of the loop parameter of the iterator_specification is the value produced by the iteration (as described in 5.5.2).

Ramification: Taken together with the preceding rule that “The array component expressions of the aggregate are evaluated in an arbitrary order”, this implies that an index parameter of an iterated_component_association can take on its values in an arbitrary order. This is different from other constructs, such as a loop_statement. In contrast, a loop parameter of an iterated_component_association takes its values in the order defined by the iteration, the same as a loop_statement.

The bounds of the index range of an array_aggregate [(including a subaggregate)] are determined as follows:

- For an array_aggregate with an others choice, the bounds are those of the corresponding index range from the applicable index constraint;
- For a positional_array_aggregate [(or equivalent string_literal)] without an others choice, the lower bound is that of the corresponding index range in the applicable index constraint, if defined, or that of the corresponding index subtype, if not; in either case, the upper bound is determined from the lower bound and the number of expressions [(or the length of the string_literal)];
- For a null_array_aggregate, bounds for each dimension are determined as for a positional_array_aggregate without an others choice that has no expressions for each dimension;
- For a named_array_aggregate containing only iterated_component_associations with an iterator_specification, the lower bound is determined...
as for a positional array aggregate without an others choice, and the upper bound is determined from the lower bound and the total number of values produced by the second set of iterations;

- \{AI12-0212-1\} For any others named array aggregate without an others choice, the bounds are determined by the smallest and largest index values covered by any discrete choice list.

  **Reason:** We don't need to say that each index value has to be covered exactly once, since that is a ramification of the general rule on aggregates that each component's value has to be specified exactly once.

For an array aggregate, a check is made that the index range defined by its bounds is compatible with the corresponding index subtype.

  **Discussion:** In RM83, this was phrased more explicitly, but once we define "compatibility" between a range and a subtype, it seems to make sense to take advantage of that definition.

  **Ramification:** The definition of compatibility handles the special case of a null range, which is always compatible with a subtype. See AI83-00313.

- \{AI05-0037-1\} For an array aggregate with an others choice, a check is made that no expression or \(<\) is specified for an index value outside the bounds determined by the applicable index constraint.

  **Discussion:** RM83 omitted this case, apparently through an oversight. AI83-00309 defines this as a dynamic check, even though other Ada 83 rules ensured that this check could be performed statically. We now allow an others choice to be dynamic, even if it is not the only choice, so this check now needs to be dynamic, in some cases. Also, within a generic unit, this would be a nonstatic check in some cases.

For a multidimensional array aggregate, a check is made that all subaggregates that correspond to the same index have the same bounds.

  **Ramification:** No array bounds “sliding” is performed on subaggregates.

  **Reason:** If sliding were performed, it would not be obvious which subaggregate would determine the bounds of the corresponding index.

The exception Constraint_Error is raised if any of the above checks fail.

**Implementation Permissions**

- \{AI12-0212-1\} \{AI12-0250-1\} When evaluating iterated component associations for an array aggregate that contains only iterated component associations with iterator specifications, the first step of evaluating an iterated component association can be omitted if the implementation can determine the maximum number of values by some other means.

  **Discussion:** For instance, if the type of the aggregate is constrained, the implementation can (but does not have to) calculate the expected length from the constraint.

**Examples of array aggregates with positional associations:**

- \((7, 9, 5, 1, 3, 2, 4, 8, 6, 0)\)
- `Table'(5, 8, 4, 1, others => 0) -- see 3.6`
Examples of two-dimensional array aggregates:

```
{AI12-0306-1} ((1.1, 1.2, 1.3), (2.1, 2.2, 2.3))
(1 => (1 => 1.1, 2 => 1.2, 3 => 1.3),
2 => (1 => 2.1, 2 => 2.2, 3 => 2.3))
```

Examples of aggregates as initial values:

```
A : Table := (7, 9, 5, 1, 3, 2, 4, 8, 6, 0);        -- A(1)=7, A(10)=0
B : Table := (2 | 4 | 10 => 1, others => 0);        -- B(1)=0, B(10)=1
C : constant Matrix := (1 .. 5 => (1 .. 8 => 0.0)); -- C'Last(1)=5, C'Last(2)=8
D : Bit_Vector(M .. N) := (M .. N => True);        -- see 3.6
E : Bit_Vector(M .. N) := (others => True);
F : String(1 .. 1) := (1 => 'F');  -- a one component aggregate: same as "F"
```

Example of an array aggregate with defaulted others choice and with an applicable index constraint provided by an enclosing record aggregate:

```
{AI12-0061-1} G : constant Matrix :=
  (for I in 1 .. 4 =>
   (for J in 1 .. 4 =>
    (if I=J then 1.0 else 0.0))); -- Identity matrix
```

```
{AI12-0312-1} Empty_Matrix : constant Matrix := []; -- A matrix without elements
```

```
{AI95-00433-01} Example of an array aggregate with defaulted others choice and with an applicable index constraint provided by an enclosing record aggregate:
```

```
{AI12-0178-1} Buffer'(Size => 50, Pos => 1, Value => String'('x', others => <>)) -- see 3.7
```

In Ada 95, no applicable index constraint is defined for a parameter in a call to a generic formal subprogram; thus, some aggregates that are legal in Ada 83 are illegal in Ada 95. For example:

```
subtype S3 is String (1 .. 3);
...
generic
  with function F (The_S3 : in S3) return Integer;
package Gp is
  I : constant Integer := F ((1 => '!', others => '?'));
  -- The aggregate is legal in Ada 83, illegal in Ada 95.
end Gp;
```

This change eliminates generic contract model problems.

Extensions to Ada 83

We now allow "named with others" aggregates in all contexts where there is an applicable index constraint, effectively eliminating what was RM83-4.3.2(6). Sliding never occurs on an aggregate with others, because its bounds come from the applicable index constraint, and therefore already match the bounds of the target.

The legality of an others choice is no longer affected by the staticness of the applicable index constraint. This substantially simplifies several rules, while being slightly more flexible for the user. It obviates the rulings of AI83-00244 and AI83-00310, while taking advantage of the dynamic nature of the "extra values" check required by AI83-00309.

Named array aggregates are permitted even if the index type is descended from a formal scalar type. See 4.9 and AI83-00190.

Wording Changes from Ada 83

We now separate named and positional array aggregate syntax, since, unlike other aggregates, named and positional associations cannot be mixed in array aggregates (except that an others choice is allowed in a positional array aggregate).
We have also reorganized the presentation to handle multidimensional and one-dimensional aggregates more uniformly, and to incorporate the rulings of AI83-00019, AI83-00309, etc.

**Extensions to Ada 95**

{AI95-00287-01} <> can be used in place of an expression in an array_aggregate, default-initializing the component.

**Wording Changes from Ada 95**

{AI95-00287-01} Limited array_aggregates are allowed (since all kinds of aggregates can now be limited, see 4.3).

{AI95-00318-02} Fixed aggregates to use the subtype of the return object of a function, rather than the result subtype, because they can be different for an extended_return_statement, and we want to use the subtype that's explicitly in the code at the point of the expression.

**Inconsistencies With Ada 2005**

{AI05-0037-1} **Correction:** Fixed so the check for components outside of the array applies to both expressions and <>s. As <> was a new feature in Ada 2005, there should be little existing code that depends on a <> component that is specified outside of the array (and that is nonsense anyway, that a compiler is likely to detect even without an explicit language rule disallowing it).

**Wording Changes from Ada 2005**

{AI05-0147-1} Added a definition of the applicable index constraint for conditional_expressions (which are new).

**Inconsistencies With Ada 2012**

{AI05-0084-1} **Corrigendum:** Fixed so that the Default_Component_Value (if any) is used to initialize components specified with <> . This is what users would expect, and all Ada 2012 implementation known at the time of this writing initialize with the Default_Component_Value, so it is unlikely that anyone will be affected by this inconsistency.

**Extensions to Ada 2012**

{AI12-0061-1} {AI12-0212-1} {AI12-0250-1} The iterated_component_association is new (more than 25 years after it was originally proposed). It has been extended to allow container iterators as well as the basic index iterators.

{AI12-0212-1} An array_aggregate can be surrounded by brackets rather than parentheses. This allows consistent writing of zero- and one-component positional array aggregates, and is consistent with the syntax for writing container aggregates.

{AI12-0212-1} {AI12-0306-1} A null_array_aggregate is new.

**Wording Changes from Ada 2012**

{AI05-0157-1} **Corrigendum:** Added expression functions to the contexts that provide an applicable index constraint, because expression functions are handled separately in static semantics and legality rules.

{AI12-0212-1} **Corrigendum:** Made syntax and wording changes for delta_aggregates.

{AI12-0236-1} **Corrigendum:** Eliminated the dependence on the nominal subtype from the wording defining the applicable index constraint for the body_expression of a delta_aggregate. The nominal subtype of a delta_aggregate wasn't defined at all in original Ada 2022, and for Ada 202y it is defined in terms of the subtype of the body_expression (which would make the definition circular without this rewording).
4.3.4 Delta Aggregates

Evaluating a (record or array) delta aggregate yields a composite value that starts with a copy of another value of the same type and then assigns to some (but typically not all) components of the copy.

Syntax

\[
delta\text{-}aggregate ::= \text{record}\_\text{delta}\_\text{aggregate} | \text{array}\_\text{delta}\_\text{aggregate}
\]

\[
\text{record}\_\text{delta}\_\text{aggregate} ::= (\text{base}\_\text{expression} \text{with} \text{delta}\text{record}\_\text{component}\_\text{association}\_\text{list})
\]

\[
\text{array}\_\text{delta}\_\text{aggregate} ::= (\text{base}\_\text{expression} \text{with} \text{delta}\text{array}\_\text{component}\_\text{association}\_\text{list}) | [' base\_expression with delta\text{array}\_\text{component}\_\text{association}\_\text{list']}
\]

Name Resolution Rules

The expected type for a record\_delta\_aggregate shall be a single descendant of a record type or record extension.

The expected type for an array\_delta\_aggregate shall be a single array type.

The expected type for the base\_expression of any delta\_aggregate is the type of the enclosing delta\_aggregate.

[The Name Resolution Rules and Legality Rules for each record\_component\_association of a record\_delta\_aggregate are as defined in 4.3.1.]

For an array\_delta\_aggregate, the expected type for each discrete choice in an array\_component\_association is the index type of the type of the delta\_aggregate.

For an array\_delta\_aggregate, the expected type of the expression in an array\_component\_association occurring within an array\_aggregate of the type of the delta\_aggregate.

Legality Rules

For an array\_delta\_aggregate, the array\_component\_association shall not use the box symbol <>, and the discrete\_choice shall not be others.

For an array\_delta\_aggregate, the dimensionality of the type of the delta\_aggregate shall be 1.

For an array\_delta\_aggregate, the base\_expression and each expression in every array\_component\_association shall be of a nonlimited type.

Ramification: The base\_expression of a record\_delta\_aggregate may be of a limited type (for example a record with limited components), as it is not restricted. A rule in 4.3.1 ensures that we do not assign to a limited component. We do not allow any part of an array\_delta\_aggregate to be of a limited type, even the base\_expression, as this is a useless construct (you would not be able to update anything because the components necessarily are also limited except in pathological cases).

Dynamic Semantics

The evaluation of a delta\_aggregate begins with the evaluation of the base\_expression of the delta\_aggregate; then that value is used to create and initialize the anonymous object of the aggregate. The bounds of the anonymous object of an
array delta aggregate and the discriminants (if any) of the anonymous object of a record delta aggregate are those of the base expression. If a record delta aggregate is of a specific tagged type, its tag is that of the specific type; if it is of a class-wide type, its tag is that of the base expression.

Ramification: This is the same anonymous object as described in 7.6, “Assignment and Finalization”; in particular, it might be required to be built in place.

For a specific tagged type, any extension components that the actual object underlying the base expression might have are not used to initialize the anonymous object, which is critical if the aggregate is required to be built-in-place.

To be honest: The anonymous object associated with the evaluation of a delta aggregate begins its life as a variable, not a constant (3.3 notwithstanding). This must be the case because the object is initialized and then subsequently modified. After evaluation of the delta aggregate is complete, the object is a constant object. This is similar to the way that an extended return statement can provide a variable view of an object that will eventually be a constant object after the function returns its result.

{AI12-0127-1} For a record delta aggregate, for each component associated with each record component association (in an unspecified order):

- if the associated component belongs to a variant, a check is made that the values of the discriminants are such that the anonymous object has this component. The exception Constraint_Error is raised if this check fails.
- the expression of the record component association is evaluated, converted to the nominal subtype of the associated component, and assigned to the component of the anonymous object.

{AI12-0127-1} For an array delta aggregate, for each discrete choice of each array component association (in the order given in the enclosing discrete choice list and array component association list, respectively) the discrete choice is evaluated; for each represented index value (in ascending order, if the discrete choice represents a range):

- the index value is converted to the index type of the array type.
- a check is made that the index value belongs to the index range of the anonymous object of the aggregate; Constraint_Error is raised if this check fails.
- the component expression is evaluated, converted to the array component subtype, and assigned to the component of the anonymous object identified by the index value.

Reason: Unlike other aggregates, an array delta aggregate is evaluated in the order that it is written. This is necessary to get deterministic behavior, as (unlike other aggregates, including record delta aggregates) there is no requirement that the specified components be distinct. As such, the order requirement ensures that every array delta aggregate has a well-defined result, even if the same component is specified multiple times.

Examples

{AI12-0127-1} {AI12-0429-1} Examples of use of delta aggregates in a postcondition:

```ada
procedure Twelfth (D : in out Date) -- see 3.8 for type Date
  with Post => D = (D'Old with delta Day => 12);

procedure The Answer (V : in out Vector; A, B : in Integer) -- see 3.6 for type Vector
  with Post => V = (V'Old with delta A .. B => 42.0, V'First => 0.0);
```

{AI12-0127-1} {AI12-0324-1} {AI12-0379-1} {AI12-0386-1} {AI12-0429-1} Examples where the base expression is nontrivial:

```ada
New Cell : Cell := (Min Cell (Head) with delta Value => 42);
-- see 3.10.1 for Cell and Head; 6.1 for Min Cell
A1 : Vector := ((0 => 1.0, 1 => 2.0, 2 => 3.0)
  with delta Integer(Random * 2.0) => 14.2);
-- see 3.6 for declaration of type Vector
-- see 6.1 for declaration of Random
```
Tomorrow := ((Yesterday with delta Day => 12) with delta Month => April); -- see 3.8

{AI12-0127-1} {AI12-0379-1} {AI12-0429-1} Example where the base expression is class-wide:

function Translate (P : Point'Class; X, Y : Real) return Point'Class is
  (P with delta X => P.X + X, Y => P.Y + Y); -- see 3.9 for declaration of type Point

Extensions to Ada 2012

4.3.5 Container Aggregates

{AI12-0212-1} In a container aggregate, values are specified for elements of a container; for a positional container aggregate, the elements are given sequentially; for a named container aggregate, the elements are specified by a sequence of key/value pairs, or using an iterator. The Aggregate aspect of the type of the aggregate determines how the elements are combined to form the container.

Term entry: container aggregate — construct used to define a value of a type that represents a collection of elements, by explicitly specifying the elements in the collection

{AI12-0212-1} For a type other than an array type, the following type-related operational aspect may be specified:

Aggregate

This aspect is an aggregate of the form:

Aspect Description for Aggregate: Mechanism to define user-defined aggregates.

(Empty => name[,  
  Add Named => procedure name[]],  
  Add Unnamed => procedure name[]],  
  New Indexed => function name,  
  Assign Indexed => procedure name])

Ramification: {AI22-0020-1} As this aspect is described with syntax, it has to be given exactly as specified here. That means it cannot be given as a positional aggregate, nor can the order of the elements be changed. For instance, New_Indexed always has to occur before Assign_Indexed, and Empty always has to be first.

{AI12-0212-1} The type for which this aspect is specified is known as the container type of the Aggregate aspect. A procedure name shall be specified for at least one of Add_Named, Add_Unnamed, or Assign_Indexed. If Add_Named is specified, neither Add_Unnamed nor Assign_Indexed shall be specified. Either both or neither of New_Indexed and Assign_Indexed shall be specified.

Name Resolution Rules

{AI12-0212-1} {AI22-0002-1} The name specified for Empty for an Aggregate aspect shall denote a constant of the container type, or denote exactly one function with a result type of the container type that has no parameters, or that has one in parameter of a signed integer type.

Reason: The parameter of In the function case, the parameter, if present, may be used to specify an initial size for the container, in anticipation of adding elements to it. For a positional aggregate, or a named aggregate that doesn't use an iterator, it will be initialized with the number of elements. For a named aggregate that uses an iterator, the implementation is permitted to estimate the number of elements that the iterator will produce, but it is not required to do so.

{AI12-0212-1} {AI12-0437-1} {AI22-0021-1} The procedure name specified for Add_Unnamed for an Aggregate aspect shall denote exactly one procedure that has two parameters, the first an in out parameter
of the container type, and the second an in parameter whose type is of some nonlimited type, called the element type of the container type.

The function name specified for New_Indexed for an Aggregate aspect shall denote exactly one function with a result type of the container type, and two parameters of the same discrete type, called with that type being the key type of the container type.

Reason: The New_Indexed function is used instead of Empty as the first step of creating an aggregate that is initializing using the Assign_Indexed procedure.

The procedure name specified for Add_Named or Assign_Indexed for an Aggregate aspect shall denote exactly one procedure that has three parameters, the first an in out parameter of the container type, the second an in parameter whose of a nonlimited type is called (the key type of the container type), and the third, an in parameter whose of a nonlimited type is called the element type of the container type.

Legality Rules

If the container type of an Aggregate aspect is a private type, the full type of the container type shall not be an array type. If the container type is limited, the name specified for Empty shall denote a function rather than a constant object.

For an Aggregate aspect, neither the element type nor the key type (if any) of the container type shall be a limited type. Additionally, the key type of Assign_Indexed shall be the same type as that of the parameters of New_Indexed, and that type shall be a discrete type. If additionally, if both Add_Unnamed and Assign_Indexed are specified, the final parameters shall be of the same type — the element type of the container type.

None of the subprograms specified for an Aggregate aspect shall have a formal access parameter, nor an explicitly aliased formal parameter.

Reason: Both access parameters and explicitly aliased parameters add additional requirements on the corresponding actual parameter. These complicate the description and implementation of container aggregates with little benefit. Thus we make them illegal. This means neither the element type nor the key type (if any) of the container type can be an anonymous access type.

If the container type T is not abstract, then none of the subprograms specified in the Aggregate aspect for T shall be abstract.

Ramification: Since the Aggregate aspect is nonoverridable, this rule is rechecked on any derived type that inherits an Aggregate aspect.

In addition to the places where Legality Rules normally apply (see 12.3), these rules apply also in the private part of an instance of a generic unit.

Ramification: The first Legality Rule has to be rechecked in instances, if a type with an Aggregate aspect is derived from a formal private type, in case the actual type for the private type is an array type. The last Legality Rule has to be rechecked in instances, in case an actual type for an abstract formal type is not abstract.

Static Semantics

The Aggregate aspect is nonoverridable (see 13.1.1).

Syntax

container_aggregate ::= null_container_aggregate
                      | positional_container_aggregate
                      | named_container_aggregate
null_container_aggregate ::= "[" "]"
4.3.5 Container Aggregates

{AI12-0212-1} positional_container_aggregate ::= '[' expression {, expression} ']

{AI12-0212-1} named_container_aggregate ::= '[' container_element_association_list ']

Reason: {AI12-0212-1} Unlike other aggregates, container aggregates have to be surrounded with brackets rather than parentheses. Using brackets allows writing zero- and one-element positional aggregates. (Were we to use parentheses, a one-element positional aggregate would look the same as and would always be interpreted as a parenthesized expression.) Unlike the case for arrays, where it is always possible to give bounds to work around this gap, such an aggregate could not be written at all for a sequence type (such as a list) where there is no index or key to use.

{AI12-0212-1} container_element_association_list ::= 
  container_element_association {, container_element_association}

{AI12-0212-1} container_element_association ::= 
  key_choice_list => expression 
  | key_choice_list => <> 
  | iterated_element_association

{AI12-0212-1} key_choice_list ::= key_choice { '|' key_choice }

{AI12-0212-1} key_choice ::= key_expression | discrete_range

{AI12-0212-1} iterated_element_association ::= 
  for loop_parameter_specification[ use key_expression ] => expression 
  | for iterator_specification[ use key_expression ] => expression

Name Resolution Rules

{AI12-0212-1} {AI12-0437-1} The expected type for a container_aggregate shall be a single type for which the Aggregate aspect has been specified. The expected type for each expression of a container_aggregate is the element type of the expected type.

{AI12-0212-1} The expected type for a key_expression, or a discrete_range of a key_choice, is the key type of the expected type of the aggregate.

Legality Rules

{AI12-0212-1} {AI22-0018-1} The expected type for a positional_container_aggregate shall have an Aggregate aspect that includes a specification for an AddUnnamed procedure or an AssignIndexed procedure. The expected type for a named_container_aggregate that contains one or more iterated_element_associations with a key_expression shall have an Aggregate aspect that includes a specification for the AddNamed procedure. The expected type for a named_container_aggregate that contains one or more key_choice_lists shall have an Aggregate aspect that includes a specification for the AddNamed or AssignIndexed procedure. [For other kinds of named_container_agggregates, there are no additional restrictions on the Aggregate aspect of the expected type. A null_container_aggregate can be of any type with an Aggregate aspect.]

{AI12-0212-1} A non-null container aggregate is called an indexed aggregate if the expected type T of the aggregate specifies an AssignIndexed procedure in its Aggregate aspect, and either there is no AddUnnamed procedure specified for the type, or the aggregate is a named_container_aggregate with a container_element_association that contains a key_choice_list or a loop_parameter_specification. The key type of an indexed aggregate is also called the index type of the aggregate.

{AI12-0212-1} A container_element_association with a <> rather than an expression, or with a key_choice that is a discrete_range, is permitted only in an indexed aggregate.

Reason: Only an element of an indexed aggregate can be left uninitialized, because the compiler can simply omit producing an AssignIndexed operation for the given index. For other kinds of aggregates, there are no operations that
add an element without giving it a value. We could have defined such (optional) operations, but they would have added
significant complication to an already complex feature without adding much additional expressive power. Note that, to
be consistent with array aggregates, we do not support specifying <> in an iterated_element_association.

\{AI12-0212-1\} For an iterated_element_association without a key_expression, if the aggregate is an
indexed aggregate or the expected type of the aggregate specifies an Add_Named procedure in its
Aggregate aspect, then the type of the loop parameter of the iterated_element_association shall be the
same as the key type of the aggregate.

Ramification: If there is a key_expression in an iterated_element_association, it determines the key of each added
key/value pair, rather than the loop parameter. But if there is no key_expression, the loop parameter itself is used as
the key.

\{AI12-0212-1\} \{AI12-0250-1\} For a named_container_aggregate that is an indexed aggregate, all
container_element_associations shall contain either a key_choice_list, or a
loop_parameter_specification without a key_expression or iterator filter. Furthermore, for such an
aggregate, either:

- all key choices shall be static expressions or static ranges, and every
  loop_parameter_specification shall have a discrete_subtype_definition that defines a non-null
  static range, and the set of values of the index type covered by the key choices and the
  discrete_subtype_definitions shall form a contiguous range of values with no duplications; or
- there shall be exactly one container_element_association, and if it has a key_choice_list, the
  list shall have exactly one key_choice.

Reason: The above is trying to mimic the rules for named_array_aggregates, without others.

Dynamic Semantics

\{AI12-0212-1\} The evaluation of a container_aggregate starts by creating an anonymous object A of the
expected type T, initialized as follows:

- if the aggregate is an indexed aggregate, from the result of a call on the New_Indexed function;
  the actual parameters in this call represent the lower and upper bound of the aggregate, and are
determined as follows:
  - if the aggregate is a positional_container_aggregate, the lower bound is the low bound of
    the subtype of the key parameter of the Add_Indexed procedure, and the upper bound has a
    position number that is the sum of the position number of the lower bound and one less than
    the number of expressions in the aggregate;
  - if the aggregate is a named_container_aggregate, the lower bound is the lowest value
    covered by a key_choice_list or is the low bound of a range defined by a
    discrete_subtype_definition of a loop_parameter_specification; the upper bound is the
    highest value covered by a key_choice_list or is the high bound of a range defined by a
    discrete_subtype_definition of a loop_parameter_specification.
  - \{AI22-0002-1\} if the aggregate is not an indexed aggregate, by assignment from the Empty
    constant, or from a call on the Empty function specified in the Aggregate aspect. In the case of an
    Empty function with a formal parameter, the actual parameter has the following value:
    - for a null_container_aggregate, the value zero;
    - for a positional_container_aggregate, the number of expressions;
    - This paragraph was deleted.\{AI22-0018-1\} for a named_container_aggregate without an
      iterated_element_association, the number of key_expressions;
    - \{AI22-0018-1\} for a named_container_aggregate where every
      iterated_element_association, if any, contains a loop_parameter_specification, the total
      number of elements specified by all of the container_element_associations;
    - otherwise, to an implementation-defined value.
Implementation Note: This value ought to be an estimate for the number of elements in the aggregate, if one is available. If not, it is suggested to use the default value for the parameter if one exists, and zero otherwise.

Implementation defined: The value of the parameter to Empty for some container aggregates.

{AI12-0212-1} The evaluation then proceeds as follows:

• for a null_container_aggregate, the anonymous object A is the result;

• for a positional_container_aggregate of a type with a specified AddUnnamed procedure, each expression is evaluated in an arbitrary order, and the AddUnnamed procedure is invoked in sequence with the anonymous object A as the first parameter and the result of evaluating each expression as the second parameter, in the order of the expressions;

{AI22-0031-1} for a positional_container_aggregate that is an indexed aggregate, each expression is evaluated in an arbitrary order, and the AssignIndexed procedure is invoked once for each expression of the aggregate in sequence with the anonymous object A as the first parameter, the key value as the second parameter, computed by starting with the low bound of the subtype of the key formal parameter of the AssignIndexed procedure and taking the successor of this value for each successive expression of the aggregate, and the result of evaluating each expression as the third parameter;

• for a named_container_aggregate for a type with an AddNamed procedure in its Aggregate aspect, the container_element_associations are evaluated in an arbitrary order:

{AI22-0031-1} for a container_element_association with a key_choice_list, for each key_choice of the list in an arbitrary order, the key_choice is evaluated as is the expression of the container_element_association (in an arbitrary order), and the AddNamed procedure is invoked once for each value covered by the key_choice (in an arbitrary order), with the anonymous object A as the first parameter, the value from the key_choice as the second parameter, and the result of evaluating the expression of the container_element_association as the third parameter;

{AI12-0212-1} {AI12-0327-1} for a container_element_association with an iterated_element_association, first the iterated_element_association is elaborated, then an iteration is performed, and for each value conditionally produced by the iteration (see 5.5 and 5.5.2) the AddNamed procedure is invoked with the anonymous object A as the first parameter, the result of evaluating the expression as the third parameter, and:

if there is a key_expression, the result of evaluating the key_expression as the second parameter;

otherwise, with the loop parameter as the second parameter;

• for a named_container_aggregate that is an indexed aggregate, the evaluation proceeds as above for the case of AddNamed, but with the AssignIndexed procedure being invoked instead of AddNamed, in the case of a container_element_association with a <> rather than an expression, the corresponding call on AssignIndexed is not performed, leaving the component as it was upon return from the NewIndexed function;

• for any other named_container_aggregate, the container_element_associations (which are necessarily iterated_element_associations) are evaluated in the order given; each such evaluation comprises two steps:

1. the iterated_element_association is elaborated;

2. {AI12-0212-1} {AI12-0327-1} an iteration is performed, and for each value conditionally produced by the iteration (see 5.5 and 5.5.2) the AddUnnamed procedure is invoked, with the anonymous object A as the first parameter and the result of evaluating the expression as the second parameter.

Ramification: In this case, the value of the loop parameter is not directly relevant, though presumably it appears within the expression of the iterated_element_association.
When the above wording says that a subprogram is invoked or called, this is a
subprogram call as defined in 6.4, with parameter associations as specified in the wording evaluated as
defined 6.4.1. [In particular, this means that the parameters are converted to the subtype of the formal
parameter (which can raise an exception — see 4.6).]

Examples

Examples of specifying the Aggregate aspect for a Set_Type, a Map_Type,
and a Vector_Type:

-- Set_Type is a set-like container type.

type Set_Type is private
with Aggregate => (Empty     => Empty_Set,
                    Add Unnamed => Include);

function Empty_Set return Set_Type;

subtype Small_Int is Integer range -1000..1000;

procedure Include (S : in out Set_Type; N : in Small_Int);

-- Map_Type is a map-like container type.

type Map_Type is private
with Aggregate =>  (Empty     => Empty_Map,
                   Add Named => Add_To_Map);

procedure Add_To_Map (M     : in out Map_Type;
                      Key   : in Integer;
                      Value : in String);

Empty_Map : constant Map_Type;

-- Vector_Type is an extensible array-like container type.

type Vector_Type is private
with Aggregate => (Empty          => Empty_Vector,
                   Add Unnamed    => Append_One,
                   New_Indexed    => New_Vector,
                   Assign_Indexed => Assign_Element);

function Empty_Vector (Capacity : Integer := 0) return Vector_Type;

procedure Append_One (V : in out Vector_Type; New_Item : in String);

procedure Assign_Element (V     : in out Vector_Type;
                          Index : in Positive;
                          Item  : in String);

function New_Vector (First, Last : Positive) return Vector_Type
with Pre => First = Positive'First;

-- Vectors are always indexed starting at the
-- lower bound of their index subtype.

-- Private part not shown.

Examples of container aggregates for Set_Type, Map_Type, and
Vector_Type:

-- Example aggregates using Set_Type.
S : Set_Type;

-- Assign the empty set to S:
S := [];

-- Is equivalent to:
S := Empty_Set;

-- A positional set aggregate:
S := [1, 2];

-- Is equivalent to:
S := Empty_Set;
Include (S, 1);
Include (S, 2);
-- A set aggregate with an iterated_element_association:
S := [for Item in 1 .. 5 => Item * 2];

-- Is equivalent to:
S := Empty_Set;
for Item in 1 .. 5 loop
   Include (S, Item * 2);
end loop;

-- A set aggregate consisting of two iterated_element_associations:
S := [for Item in 1 .. 5 => Item, for Item in 1 .. 5 => -Item];

{AI12-0379-1} -- Is equivalent (assuming set semantics) to:
S := Empty_Set;
for Item in 1 .. 5 loop
   Include (S, Item);
end loop;
for Item in -5 .. -1 loop
   Include (S, Item);
end loop;

-- Example aggregates using Map_Type.
M : Map_Type;

-- A simple named map aggregate:
M := [12 => "house", 14 => "beige"];

-- Is equivalent to:
M := Empty_Map;
Add_To_Map (M, 12, "house");
Add_To_Map (M, 14, "beige");

-- Define a table of pairs:
type Pair is record
   Key : Integer;
   Value : Access constant String;
end record;

Table : constant array (Positive range <>) of Pair :=

[(Key => 33, Value => new String'("a nice string")),
 (Key => 44, Value => new String'("an even better string"))];

-- A map aggregate using an iterated_element_association
-- and a key_expression, built from a table of key/value pairs:
M := [for P of Table use P.Key => P.Value.all];

-- Is equivalent to:
M := Empty_Map;
for P of Table loop
   Add_To_Map (M, P.Key, P.Value.all);
end loop;

-- Create an image table for an array of integers:
Keys : constant array (Positive range <>) of Integer := [2, 3, 5, 7, 11];

-- A map aggregate where the values produced by the
-- iterated_element_association are of the same type as the key
-- (hence a separate key_expression is unnecessary):
M := [for Key of Keys => Integer'Image (Key)];

-- Is equivalent to:
M := Empty_Map;
for Key of Keys loop
   Add_To_Map (M, Key, Integer'Image (Key));
end loop;

-- Example aggregates using Vector_Type.
V : Vector_Type;

-- A positional vector aggregate:
V := ["abc", "def"];
-- Is equivalent to:
V := Empty_Vector (2);
Append_One (V, "abc");
Append_One (V, "def");

-- An indexed vector aggregate:
V := [1 => "this", 2 => "is", 3 => "a", 4 => "test"];

-- Is equivalent to:
V := New_Vector (1, 4);
Assign_Element (V, 1, "this");
Assign_Element (V, 2, "is");
Assign_Element (V, 3, "a");
Assign_Element (V, 4, "test");

Extensions to Ada 2012

{AI12-0212-1} Container aggregates are new.

Inconsistencies With Ada 2022

{AI22-0031-1} Corrigendum: Expressions in a named container_aggregate are evaluated once for each key value. This is consistent with other kinds of aggregate. Original Ada 2022 evaluated the expressions once per association. If a program depends on the number of times the expressions are evaluated, the behavior could change. This sort of program is unusual, and most depend on each component having a separate evaluation, so this change is more likely to fix a bug than cause one.

Incompatibilities With Ada 2022

{AI22-0002-1} Corrigendum: Unlike original Ada 2022, Empty can only be given by a function, not by a constant, as a constant does not make sense when the associated type is derived. As a new Ada 2022 feature, the specification of container aggregates should be rare, and the fix is easy: just replace the constant by an expression function returning the constant.

{AI22-0021-1} Corrigendum: Adjusted the rules about resolution of subprograms to avoid depending upon properties like limitedness of the parameter types (we do not do this elsewhere in the language). Also, some rules were added to make some unusual cases illegal that could have caused the aggregate implementation to be illegal. In both of these cases, unusual programs that were legal in original Ada 2022 are illegal in Ada 202y. As this is a new Ada 2022 feature, and the situations involved are unlikely, it is not expected that this will affect any existing code.

{AI22-0032-1} Corrigendum: The subprograms specified for an Aggregate aspect cannot be abstract unless the associated type is abstract; abstract subprograms were allowed in original Ada 2022. It is highly unlikely that any code using abstract subprograms in an Aggregate aspect exists, as such subprograms have no body but will be called when an aggregate is used for the type (usually causing internal errors in compilers).

Extensions to Ada 2022

{AI22-0018-1} Corrigendum: A named container_aggregate with a key_choice with a discrete range no longer has to be an indexed aggregate. There was no reason for this restriction.

Wording Changes from Ada 2022

{AI22-0031-1} Corrigendum: Added wording to clarify that calls defined in this subclause are evaluated as calls are defined in 6.4. While this could cause a program to raise an exception where it previously did not, this is just specifying otherwise unspecified behavior and does so as an Ada programmer would expect.

{AI22-0031-1} Corrigendum: Increased flexibility by removing an order requirement on the calls to Add_Indexed. This does not require any change to an existing implementation or program.

4.4 Expressions

{AI05-0147-1} {AI05-0158-1} {AI05-0176-1} An expression is a formula that defines the computation or retrieval of a value. In this Reference Manual, the term “expression” refers to a construct of the syntactic category expression or of any of the following categories: choice_expression, choice_relation, relation, simple_expression, term, factor, primary, conditional_expression, quantified_expression; the five syntactic categories defined below.
Syntax

expression ::= relation { and relation} | relation { and then relation}
| relation { or relation} | relation { or else relation}
| relation { xor relation}

{AI05-0158-1} choice_expression ::= 
| choice_relation { and choice_relation}
| choice_relation { or choice_relation}
| choice_relation { xor choice_relation}
| choice_relation { and then choice_relation}
| choice_relation { or else choice_relation}

{AI05-0158-1} choice_relation ::= 
| simple_expression [ relational_operator simple_expression]

{AI12-0022-1} {AI12-0039-1} relation ::= 
| simple_expression [ relational_operator simple_expression]
| upper simple_expression simple_expression [ not] in membership_choice_list
| raise_expression

range ::= simple_expression [ not] in subtype_mark

{AI05-0158-1} {AI12-0022-1} {AI12-0039-1} membership_choice_list ::= 
| membership_choice [" membership_choice]

{AI05-0158-1} {AI12-0022-1} membership_choice ::= 
| range | subtype_mark

simple_expression ::= 
| unary_adding_operator  term {binary_adding_operator term}

term ::= factor {multiplying_operator factor}

factor ::= primary [** primary] | abs primary | not primary

{AI05-0003-1} {AI05-0147-1} {AI05-0176-1} {AI12-0236-1} primary ::= 
| numeric_literal | null | string_literal | aggregate
| name | qualified_expression | allocator | expression
| (conditional_expression) | (quantified_expression)
| (declare_expression)

Name Resolution Rules

A name used as a primary shall resolve to denote an object or a value.

Discussion: This replaces RM83-4.4(3). We don't need to mention named numbers explicitly, because the name of a named number denotes a value. We don't need to mention attributes explicitly, because attributes now denote (rather than yield) values in general. Also, the new wording allows attributes that denote objects, which should always have been allowed (in case the implementation chose to have such a thing).

Reason: It might seem odd that this is an overload resolution rule, but it is relevant during overload resolution. For example, it helps ensure that a primary that consists of only the identifier of a parameterless function is interpreted as a function_call rather than directly as a direct_name.

Static Semantics

Each expression has a type; it specifies the computation or retrieval of a value of that type.
A primary that is an expression surrounded by ( and ) is known as a parenthesized expression.

Every name or expression consists of one or more operative constituent names or expressions, only one of which is evaluated as part of evaluating the name or expression (the evaluated operative constituent). The operative constituents are determined as follows, according to the form of the expression (or name):

- if the expression is a conditional expression, the operative constituents of its dependent expressions;
- if the expression (or name) is a parenthesized expression, a qualified expression, or a view conversion, the operative constituent(s) of its operand;
- if the expression is a declare expression, the operative constituent(s) of its body expression;
- otherwise, the expression (or name) itself.

In certain contexts, we specify that an operative constituent shall (or shall not) be newly constructed. This means the operative constituent shall (or shall not) be an aggregate or a function call; in either case, a raise_expression is permitted.

To be honest: If an if_expression does not have an else clause, "True" is an operative constituent of the expression and it can be the evaluated operative constituent.

Dynamic Semantics

The value of a primary that is a name denoting an object is the value of the object.

An expression of a numeric universal type is evaluated as if it has type root_integer (for universal_integer) or root_real (otherwise) unless the context identifies a specific type (in which case that type is used).

Ramification: This has no effect for a static expression; its value may be arbitrarily small or large since no specific type is expected for any expression for which this rule specifies one of the root types. The only effect of this rule is to allow Constraint_Error to be raised if the value is outside of the base range of root_integer or root_real when the expression is not static.

Reason: This rule means that implementations don't have to support unlimited range math at run time for universal expressions. Note that universal expressions for which the context doesn't specify a specific type are quite rare; attribute prefixes and results are the only known cases. (For operators, 8.6 already specifies that the operator of a root type be used, which provides a specific type.)

Implementation Permissions

For the evaluation of a primary that is a name denoting an object of an unconstrained numeric subtype, if the value of the object is outside the base range of its type, the implementation may either raise Constraint_Error or return the value of the object.

Ramification: This means that extra-range intermediates are used to hold the value of an object of an unconstrained numeric subtype, a Constraint_Error can be raised on a read of the object, rather than only on an assignment to it. Similarly, it means that computing the value of an object of such a subtype can be deferred until the first read of the object (presuming no side effects other than failing an Overflow_Check are possible). This permission is over and above that provided by subclause 11.6, since this allows the Constraint_Error to move to a different handler.

Reason: This permission is intended to allow extra-range registers to be used efficiently to hold parameters and local variables, even if they might need to be transferred into smaller registers for performing certain predefined operations.

Discussion: There is no need to mention other kinds of primaries, since any Constraint_Error to be raised can be “charged” to the evaluation of the particular kind of primary.
Examples of primaries:

4.0                -- real literal
Pi                 -- named number
(1 .. 10 => 0)     -- array aggregate
Sum                -- variable
Integer'Last       -- attribute
Sine(X)            -- function call
Color'(Blue)       -- qualified expression
Real(M*N)          -- conversion
(Line_Count + 10)  -- parenthesized expression

Examples of expressions:

{AI95-00433-01} Volume                      -- primary
not Destroyed               -- factor
2*Line_Count                -- term
-4.0                        -- simple expression
-4.0 + A                    -- simple expression
B**2 - 4.0*A*C              -- simple expression
R*Sin(θ)*Cos(φ)             -- simple expression
Password(1 .. 3) = "Bwv"    -- relation
Count in Small_Int          -- relation
Count not in Small_Int      -- relation
Index = 0 or Item_Hit       -- expression
(Cold and Sunny) or Warm    -- expression (parentheses are required)
A**(B**C)                   -- expression (parentheses are required)

Extensions to Ada 83

In Ada 83, out parameters and their nondiscriminant subcomponents are not allowed as primaries. These restrictions are eliminated in Ada 95.

In various contexts throughout the language where Ada 83 syntax rules had simple_expression, the corresponding Ada 95 syntax rule has expression instead. This reflects the inclusion of modular integer types, which makes the logical operators "and", "or", and "xor" more useful in expressions of an integer type. Requiring parentheses to use these operators in such contexts seemed unnecessary and potentially confusing. Note that the bounds of a range still have to be specified by simple_expressions, since otherwise expressions involving membership tests might be ambiguous. Essentially, the operation ".." is of higher precedence than the logical operators, and hence uses of logical operators still have to be parenthesized when used in a bound of a range.

Wording Changes from Ada 2005

Moved qualified_expression from primary to name (see 4.1). This allows the use of qualified_expressions in more places.

Added conditional_expression and quantified_expression to primary.

Expanded membership test syntax (see 4.5.2).

Inconsistencies With Ada 2012

Revised membership syntax to eliminate ambiguities. In some cases, previously ambiguous membership expressions will now have an unambiguous meaning. If an Ada 2012 implementation chose the "wrong" meaning, the expression could silently change meaning. Virtually all such expressions will become illegal because of type mismatches (and thus be incompatible, not inconsistent). However, if the choices are all of a Boolean type, resolution might succeed. For instance, A in B | C and D now always means (A in B | C) and D, but the original Ada 2012 syntax would have allowed it to mean A in B | (C and D). If a compiler allowed the expression and interpreted it as the latter, the meaning of the expression would silently change. We expect this to be extremely rare as membership operations on Boolean types are unlikely (and this can happen only in code written for Ada 2012).

Incompatibilities With Ada 2012

The revised membership syntax will require parentheses in membership_choice_lists in some cases where the Ada 2012 grammar did not require them. For instance, A in B in C | D is now illegal. However, such expressions can be interpreted in multiple ways (either A in (B in C) | D or A in (B in C | D).
for this example), so using such expressions is likely to be dangerous (another compiler might interpret the expression differently). In addition, all such expressions occur only in Ada 2012 syntax; so they should be rare.

Wording Changes from Ada 2012

{AI12-0227-1} Correction: Added wording so that universal expressions evaluated at run time can raise Constraint_Error if the value is outside of the range of root_integer or root_real. We don't document this as an inconsistency because the rule requires no implementation to change (as Constraint_Error is not required); it just allows implementations that already raise Constraint_Error (which is all of them surveyed) to be considered correct.

{AI12-0236-1} Added declare_expression to primary. It shares the rules about parentheses with conditional_expressions.

{AI12-0317-1} Added the definitions of “operative constituent” and “newly constructed” to centralize definitions that are needed for various rules and definitions across the Reference Manual. In particular, operative constituent is often used when we want the semantics or legality to be unchanged by the presence of parens, qualification, or view conversions. Examples are found in 4.3.2, 6.2, and 7.5.

4.5 Operators and Expression Evaluation

[ The language defines the following six categories of operators (given in order of increasing precedence). The corresponding operator_symbols, and only those, can be used as designators in declarations of functions for user-defined operators. See 6.6, “Overloading of Operators”.]

Syntax

logical_operator ::= and | or | xor
relational_operator ::= = | /= | < | <= | > | >=
binary_adding_operator ::= + | – | &
unary_adding_operator ::= + | –
multiplying_operator ::= * | / | mod | rem
highest_precedence_operator ::= ** | abs | not

Discussion: Some of the above syntactic categories are not used in other syntax rules. They are just used for classification. The others are used for both classification and parsing.

Static Semantics

For a sequence of operators of the same precedence level, the operators are associated with their operands in textual order from left to right. Parentheses can be used to impose specific associations.

Discussion: The left-associativity is not directly inherent in the grammar of 4.4, though in 1.1.4 the definition of the metasymbols { } implies left associativity. So this could be seen as redundant, depending on how literally one interprets the definition of the { } metasymbols.

See the Implementation Permissions below regarding flexibility in reassociating operators of the same precedence.

For each form of type definition, certain of the above operators are predefined; that is, they are implicitly declared immediately after the type definition. For each such implicit operator declaration, the parameters are called Left and Right for binary operators; the single parameter is called Right for unary operators. [An expression of the form X op Y, where op is a binary operator, is equivalent to a function_call of the form "op"(X, Y). An expression of the form op Y, where op is a unary operator, is equivalent to a function_call of the form "op"(Y). The predefined operators and their effects are described in subclauses 4.5.1 through 4.5.6.]

Dynamic Semantics

[ The predefined operations on integer types either yield the mathematically correct result or raise the exception Constraint_Error. For implementations that support the Numerics Annex, the predefined
operations on real types yield results whose accuracy is defined in Annex G, or raise the exception Constraint_Error. ]

To be honest: Predefined operations on real types can “silently” give wrong results when the Machine_Overflows attribute is false, and the computation overflows.

Proof: For integer types, this is normatively stated in the Dynamic Semantics of 3.5.4. For floating point types, this is normatively stated at the end of the Implementation Requirements of G.2.1. For fixed point types, this is normatively stated at the end of the Implementation Requirements of G.2.3.

Implementation Requirements

The implementation of a predefined operator that delivers a result of an integer or fixed point type may raise Constraint_Error only if the result is outside the base range of the result type.

The implementation of a predefined operator that delivers a result of a floating point type may raise Constraint_Error only if the result is outside the safe range of the result type.

To be honest: An exception is made for exponentiation by a negative exponent in 4.5.6.

Implementation Permissions

For a sequence of predefined operators of the same precedence level (and in the absence of parentheses imposing a specific association), an implementation may impose any association of the operators with operands so long as the result produced is an allowed result for the left-to-right association, but ignoring the potential for failure of language-defined checks in either the left-to-right or chosen order of association.

Discussion: Note that the permission to reassociate the operands in any way subject to producing a result allowed for the left-to-right association is not much help for most floating point operators, since reassociation may introduce significantly different round-off errors, delivering a result that is outside the model interval for the left-to-right association. Similar problems arise for division with integer or fixed point operands.

Note that this permission does not apply to user-defined operators.

NOTE: The two operands of an expression of the form X op Y, where op is a binary operator, are evaluated in an arbitrary order, as for any function_call (see 6.4).

Examples

Examples of precedence:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Equivalent Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>not Sunny or Warm</td>
<td>same as (not Sunny) or Warm</td>
</tr>
<tr>
<td>X &gt; 4.0 and Y &gt; 0.0</td>
<td>same as (X &gt; 4.0) and (Y &gt; 0.0)</td>
</tr>
<tr>
<td>-4.0*A**2</td>
<td>same as -(4.0 * (A**2))</td>
</tr>
<tr>
<td>abs(1 + A) + B</td>
<td>same as (abs (1 + A)) + B</td>
</tr>
<tr>
<td>Y**(-3)</td>
<td>parentheses are necessary</td>
</tr>
<tr>
<td>A / B * C</td>
<td>same as (A/B)*C</td>
</tr>
<tr>
<td>A + (B + C)</td>
<td>evaluate B + C before adding it to A</td>
</tr>
</tbody>
</table>

Wording Changes from Ada 83

We don't give a detailed definition of precedence, since it is all implicit in the syntax rules anyway.

The permission to reassociate is moved here from RM83-11.6(5), so it is closer to the rules defining operator association.

4.5.1 Logical Operators and Short-circuit Control Forms

Name Resolution Rules

An expression consisting of two relations connected by and then or or else (a short-circuit control form) shall resolve to be of some boolean type; the expected type for both relations is that same boolean type.
Reason: This rule is written this way so that overload resolution treats the two operands symmetrically; the resolution of overloading present in either one can benefit from the resolution of the other. Furthermore, the type expected by context can help.

Static Semantics

The following logical operators are predefined for every boolean type \( T \), for every modular type \( T \), and for every one-dimensional array type \( T \) whose component type is a boolean type:

\[
\begin{align*}
\text{function } & "\text{and}" (\text{Left, Right} : T) \text{ return } T \\
\text{function } & "\text{or}" (\text{Left, Right} : T) \text{ return } T \\
\text{function } & "\text{xor}" (\text{Left, Right} : T) \text{ return } T
\end{align*}
\]

This paragraph was deleted. To be honest: For predefined operators, the parameter and result subtypes shown as \( T \) are actually the unconstrained subtype of the type.

Ramification: For these operators, we are talking about the type without any (interesting) subtype, and not some subtype with a constraint or exclusion. Since it's possible that there is no name for the "uninteresting" subtype, we denote the type with an italicized \( T \). This applies to the italicized \( T \) in many other predefined operators and attributes as well.

\{AI95-00145-01\} In many cases, there is a subtype with the correct properties available. The italicized \( T \) means:

- \( T\text{'Base} \), for scalars;
- the first subtype of \( T \), for tagged types;
- a subtype of the type \( T \) without any constraint or null exclusion, in other cases.

Note that "without a constraint" is not the same as unconstrained. For instance, a record type with no discriminant part is considered constrained; no subtype of it has a constraint, but the subtype is still constrained.

Thus, the last case often is the same as the first subtype of \( T \), but that isn't the case for constrained array types (where the correct subtype is unconstrained) and for access types with a null exclusion (where the correct subtype does not exclude null).

This italicized \( T \) is used for defining operators and attributes of the language. The meaning is intended to be as described here.

For boolean types, the predefined logical operators \textbf{and}, \textbf{or}, and \textbf{xor} perform the conventional operations of conjunction, inclusive disjunction, and exclusive disjunction, respectively.

For modular types, the predefined logical operators are defined on a bit-by-bit basis, using the binary representation of the value of the operands to yield a binary representation for the result, where zero represents False and one represents True. If this result is outside the base range of the type, a final subtraction by the modulus is performed to bring the result into the base range of the type.

The logical operators on arrays are performed on a component-by-component basis on matching components (as for equality — see 4.5.2), using the predefined logical operator for the component type. The bounds of the resulting array are those of the left operand.

Dynamic Semantics

The short-circuit control forms \textbf{and then} and \textbf{or else} deliver the same result as the corresponding predefined \textbf{and} and \textbf{or} operators for boolean types, except that the left operand is always evaluated first, and the right operand is not evaluated if the value of the left operand determines the result.

For the logical operators on arrays, a check is made that for each component of the left operand there is a matching component of the right operand, and vice versa. Also, a check is made that each component of the result belongs to the component subtype. The exception Constraint_Error is raised if either of the above checks fails.

Discussion: The check against the component subtype is per AI83-00535.

NOTE The conventional meaning of the logical operators is given by the following truth table:

\[
\begin{array}{cccc}
A & B & (A \text{ and } B) & (A \text{ or } B) & (A \text{ xor } B) \\
\hline
\text{True} & \text{True} & \text{True} & \text{True} & \text{False}
\end{array}
\]
4.5.1 Logical Operators and Short-circuit Control Forms

Examples

Examples of logical operators:

- Sunny or Warm
- Filter(1..10) and Filter(15..24) -- see 3.6.1

Examples of short-circuit control forms:

- Next_Car.Owner /= null and then Next_Car.Owner.Age > 25 -- see 3.10.1
- N = 0 or else A(N) = Hit_Value

4.5.2 Relational Operators and Membership Tests

[ The equality operators = (equals) and /= (not equals) are predefined for nonlimited types. The other relational operators are the ordering operators < (less than), <= (less than or equal), > (greater than), and >= (greater than or equal). The ordering operators are predefined for scalar types, and for discrete array types, that is, one-dimensional array types whose components are of a discrete type.

Ramification: The equality operators are not defined for every nonlimited type — see below for the exact rule.

\{AI05-0262-1\} \{AI05-0269-1\} A membership test, using in or not in, determines whether or not a value belongs to any given subtype or range, is equal to any given value, or has a tag that identifies a type that is covered by a given type, or is convertible to and has an accessibility level appropriate for a given access type. Membership tests are allowed for all types.]

The tested type of a membership test is the type of the range or the type determined by the membership choices of the membership choice list. Either all membership choices of the membership choice list shall resolve to the same type, which is the tested type; or each membership choice shall be of an elementary type, and the tested type shall be covered by each of these elementary types.

If the tested type is tagged, then the simple expression shall resolve to be of a type that is convertible (see 4.6) to covers or is covered by the tested type; if untagged, the expected type for the simple expression is the tested type.

If the tested type is tagged, then the tested simple expression shall resolve to be of a type that is convertible (see 4.6) to covers or is covered by the tested type; if untagged, the expected type for the choice expression is the tested type.

\{AI95-00251-01\} \{AI05-0158-1\} The tested simple expression of a range in a membership choice, and of a simple expression of a range in a membership choice, is the tested type of the membership operation.

Reason: \{AI95-00230-01\} The part of the rule for untagged types is stated in a way that ensures that operands like a string literal null are still legal as operands of a membership test.

\{AI95-00251-01\} \{AI12-0039-1\} The significance of “is convertible to covers or is covered by” is that we allow the tested simple expression to be of any class-wide type that could be converted to covers the tested type, not just the one rooted at the tested type. This includes any class-wide type that covers the tested type, along with class-wide interfaces in some cases.

\{AI05-0158-1\} The special rule for determining the tested type for elementary types is to allow numeric literals in membership choice lists. Without the rule, A in B | 1 would be illegal as B and 1 have different types (the literal having type universal integer).
Legality Rules

{AI12-0039-1} For a membership test, if the tested simple_expression is of a tagged class-wide type, then the tested type shall be (visibly) tagged.

\[\text{Ramification: Untagged types covered by the tagged class-wide type are not permitted. Such types can exist if they are descendants of a private type whose full type is tagged. This rule is intended to avoid confusion since such derivatives don't have their “own” tag, and hence are indistinguishable from one another at run time once converted to a covering class-wide type.}\]

{AI05-0158-1} {AI12-0039-1} {AI12-0328-1} If a membership test includes one or more choice simple_expression and the tested type of the membership test is limited, then the tested type of the membership test shall have a visible primitive equality operator; if the tested type of the membership test is nonlimited with a user-defined primitive equality operator that is defined at a point where the type is limited, the tested type shall be a record type or record extension.

\[\text{Reason: A visible equality operator is required in order to avoid breaking privacy; that is, we don't want to depend on a hidden equality operator.}\]

\[\text{We make the membership test on the nonlimited view of a type illegal if it would use a different equality operator than what would be used for a limited view of the same type (and such a limited view is known to exist).}\]

Static Semantics

The result type of a membership test is the predefined type Boolean.

The equality operators are predefined for every specific type \(T\) that is not limited, and not an anonymous access type, with the following specifications:

\[
\begin{align*}
\text{function } &= (\text{Left, Right : } T) \text{ return Boolean} \\
\text{function } /= (\text{Left, Right : } T) \text{ return Boolean}
\end{align*}
\]

{AI95-00230-01} The following additional equality operators for the universal_access type are declared in package Standard for use with anonymous access types:

\[
\begin{align*}
\text{function } &= (\text{Left, Right : universal_access}) \text{ return Boolean} \\
\text{function } /= (\text{Left, Right : universal_access}) \text{ return Boolean}
\end{align*}
\]

The ordering operators are predefined for every specific scalar type \(T\), and for every discrete array type \(T\), with the following specifications:

\[
\begin{align*}
\text{function } < (\text{Left, Right : } T) \text{ return Boolean} \\
\text{function } <= (\text{Left, Right : } T) \text{ return Boolean} \\
\text{function } > (\text{Left, Right : } T) \text{ return Boolean} \\
\text{function } >= (\text{Left, Right : } T) \text{ return Boolean}
\end{align*}
\]

Name Resolution Rules

{AI95-00230-01} {AI95-00420-01} At least one of the operands of an equality operator for universal_access shall be of a specific anonymous access type. Unless the predefined equality operator is identified using an expanded name with prefix denoting the package Standard, neither operand shall be of an access-to-object type whose designated type is \(D\) or \(D\)Class, where \(D\) has a user-defined primitive equality operator such that:

- its result type is Boolean;
- \{AI05-0020-1\} it is declared immediately within the same declaration list as \(D\) or any partial or incomplete view of \(D\); and
- at least one of its operands is an access parameter with designated type \(D\).

\[\text{Reason: The first sentence prevents compatibility problems by ensuring that these operators are not used for named access types. Also, universal access types do not count for the purposes of this rule. Otherwise, equality expressions like (X = null) would be ambiguous for normal access types.}\]
The rest of the rule makes it possible to call (including a dispatching call) user-defined "=" operators for anonymous access-to-object types (they’d be hidden otherwise), and to write user-defined "=" operations for anonymous access types (by making it possible to see the universal operator using the Standard prefix).

**Ramification:** We don’t need a similar rule for anonymous access-to-subprogram types because they can’t be primitive for any type. Note that any nonprimitive user-defined equality operators still are hidden by the universal operators; they’ll have to be called with a package prefix, but they are likely to be very uncommon.

**Legality Rules**

**{AI95-00230-01}** At least one of the operands of the equality operators for universal access shall be of type universal access, or both shall be of access-to-object types, or both shall be of access-to-subprogram types. Further:

- When both are of access-to-object types, the designated types shall be the same or one shall cover the other, and if the designated types are elementary or array types, then the designated subtypes shall statically match;
- When both are of access-to-subprogram types, the designated profiles shall be subtype conformant.

**Reason:** We don’t want to allow completely arbitrary comparisons, as we don’t want to insist that all access types are represented in ways that are convertible to one another. For instance, a compiler could use completely separate address spaces or incompatible representations. Instead, we allow compares if there exists an access parameter to which both operands could be converted. Since the user could write such an subprogram, and any reasonable meaning for "=" would allow using it in such a subprogram, this doesn’t impose any further restrictions on Ada implementations.

**{AI05-0123-1} {AI12-0101-1} {AI12-0352-1}** If the profile of an explicitly declared primitive equality operator of an untagged record type is type conformant with that of the corresponding predefined equality operator, the declaration shall occur before the type is frozen. In addition, if the untagged record type has a nonlimited partial view, then the declaration shall occur in the visible part of the enclosing package. In addition, no type shall have been derived from the untagged record type before the declaration of the primitive equality operator. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

**Dynamic Semantics**

For discrete types, the predefined relational operators are defined in terms of corresponding mathematical operations on the position numbers of the values of the operands.

For real types, the predefined relational operators are defined in terms of the corresponding mathematical operations on the values of the operands, subject to the accuracy of the type.

**Ramification:** For floating point types, the results of comparing nearly equal values depends on the accuracy of the implementation (see G.2.1, “Model of Floating Point Arithmetic” for implementations that support the Numerics Annex).

**Implementation Note:** On a machine with signed zeros, if the generated code generates both plus zero and minus zero, plus and minus zero must be equal by the predefined equality operators.

Two access-to-object values are equal if they designate the same object, or if both are equal to the null value of the access type.

Two access-to-subprogram values are equal if they are the result of the same evaluation of an Access attribute_reference, or if both are equal to the null value of the access type. Two access-to-subprogram values are unequal if they designate different subprograms. [It is unspecified whether two access values that designate the same subprogram but are the result of distinct evaluations of Access attribute_references are equal or unequal.]

**Reason:** This allows each Access attribute_reference for a subprogram to designate a distinct “wrapper” subprogram if necessary to support an indirect call.
For a type extension, predefined equality is defined in terms of the primitive [possibly user-defined] equals operator of the parent type and any tagged components that have a record type in the extension part, and predefined equality for any other components not inherited from the parent type.

**Ramification:** Two values of a type extension are not equal if there is a variant part in the extension part and the two values have different variants present. This is a ramification of the requirement that a discriminant governing such a variant part has to be a “new” discriminant, and so has to be equal in the two values for the values to be equal. Note that variant parts in the parent part need not match if the primitive equals operator for the parent type considers them equal.

The full type extension's operation is used for a private extension. This follows as only full types have parent types; the type specified in a private extension is an ancestor, but not necessarily the parent type. For instance, in:

```ada
with Pak1;
package Pak2 is
  type Typ3 is new Pak1.Typ1 with private;
  private
    type Typ3 is new Pak1.Typ2 with null record;
end Pak2;
```

the parent type is Pak1.Typ2, not Pak1.Typ1, and the equality operator of Pak1.Typ2 is used to create predefined equality for Typ3.

For a derived type whose parent is an untagged record type, predefined equality is defined in terms of the primitive (possibly user-defined) equals operator of the parent type.

**Reason:** This prevents predefined equality from reemerging in generic units for untagged record types. For other uses the primitive equality is inherited and the inherited routine is primitive.

For a private type, if its full type is a record type or a record extension tagged, predefined equality is defined in terms of the primitive equals operator of the full type; otherwise, predefined equality for the private type is that of its full type.

For other composite types, the predefined equality operators [(and certain other predefined operations on composite types — see 4.5.1 and 4.6)] are defined in terms of the corresponding operation on matching components, defined as follows:

- For two composite objects or values of the same non-array type, matching components are those that correspond to the same component declaration or discriminant specification;
- For two one-dimensional arrays of the same type, matching components are those (if any) whose index values match in the following sense: the lower bounds of the index ranges are defined to match, and the successors of matching indices are defined to match;
- For two multidimensional arrays of the same type, matching components are those whose index values match in successive index positions.

The analogous definitions apply if the types of the two objects or values are convertible, rather than being the same.

**Discussion:** Ada 83 seems to omit this part of the definition, though it is used in array type conversions. See 4.6.

Given the above definition of matching components, the result of the predefined equals operator for composite types (other than for those composite types covered earlier) is defined as follows:

- If there are no components, the result is defined to be True;
- If there are unmatched components, the result is defined to be False;
- Otherwise, the result is defined in terms of the primitive equals operator for any matching tagged components that are records, and the predefined equals for any other matching untagged components.
Reason: [AI05-0123-1] This asymmetry between tagged and untagged components with and without a record type is necessary to preserve most upward compatibility and corresponds with the corresponding situation with generics, where the predefined operations “reemerge” in a generic for non-record tagged types, but do not for record tagged types. Also, only tagged types support user-defined assignment (see 7.6), so only tagged types can fully handle levels of indirection in the implementation of the type. For untagged types, one reason for a user-defined equals operator might be to allow values with different bounds or discriminants to compare equal in certain cases. When such values are matching components, the bounds or discriminants will necessarily match anyway if the discriminants of the enclosing values match.

Ramification: Two null arrays of the same type are always equal; two null records of the same type are always equal.

Note that if a composite object has a component of a floating point type, and the floating point type has both a plus and minus zero, which are considered equal by the predefined equality, then a block compare cannot be used for the predefined composite equality. Of course, with user-defined equals operators for tagged components that are records, a block compare breaks down anyway, so this is not the only special case that requires component-by-component comparisons. On a one’s complement machine, a similar situation might occur for integer types, since one’s complement machines typically have both a plus and minus (integer) zero.

To be honest: [AI95-00230-01] For a component with an anonymous access type, “predefined equality” is that defined for the universal access type (anonymous access types have no equality operators of their own).

For a component with a record tagged type T, “the primitive equals operator” is the one with two parameters of T which returns Boolean. We’re not talking about some random other primitive function named “=”. The predefined “/=” operator gives the complementary result to the predefined “=” operator.

If the primitive equals operator for an untagged record type is abstract, then Program_Error is raised at the point of any (implicit) call to that abstract subprogram, implicitly as part of an equality operation on an enclosing composite object, or in an instance of a generic with a formal private type where the actual type is a record type with an abstract “=”.

Reason: [AI12-0413-1] An explicit call to an abstract subprogram is generally illegal. This rule is needed in order to define the effect of a call in an instance of a generic body, or an implicit call such as a call that is part of the predefined equality operation for an enclosing composite type that has a component of an untagged record type that has an abstract primitive equals operator. For tagged types, an abstract primitive equals operator is only allowed for an abstract type, and abstract types cannot be components, so this case does not occur.

For any composite type, the order in which “=” is called for components is unspecified. Furthermore, if the result can be determined before calling “=” on some components, it is unspecified whether “=” is called on those components.

The predefined “/=” operator gives the complementary result to the predefined “=” operator.

Ramification: Furthermore, if the user defines an “=” operator that returns Boolean, then a “/=” operator is implicitly declared in terms of the user-defined “=” operator so as to give the complementary result. See 6.6.

For a discrete array type, the predefined ordering operators correspond to lexicographic order using the predefined order relation of the component type: A null array is lexicographically less than any array having at least one component. In the case of nonnull arrays, the left operand is lexicographically less than the right operand if the first component of the left operand is less than that of the right; otherwise, the left operand is lexicographically less than the right operand only if their first components are equal and the tail of the left operand is lexicographically less than that of the right (the tail consists of the remaining components beyond the first and can be null).

An individual membership test is the membership test of a single membership choice.

For the evaluation of a membership test using in whose membership_choice_list has a single membership choice, the tested simple expression and the membership_choice range (if any) are evaluated in an arbitrary order; the result is the result of the individual membership test for the membership_choice.
the operation is equivalent to that of a sequence consisting of an individual membership test on each membership_choice combined with the short-circuit control form or else.

Ramification: [AI05-0158-1] This equivalence includes the evaluation of the membership_choices; evaluation stops as soon as an individual choice evaluates to True.

{AI05-0158-1} {AI05-0269-1} A membership test using in yields the result True if:

• {AI05-0158-1} {AI05-0264-1} {AI12-0039-1} {AI12-0328-1} The membership choice is a
  choice simple_expression choice_expression, and the tested_simple_expression is equal to the value of the membership_choice.
  If the tested type is a record type or a record extension, or is limited at the point where the membership test occurs
  type, the test uses the primitive equality for the type; otherwise, the test uses predefined equality.

  Reason: We use the predefined equality operator if the membership test occurs where the type is nonlimited if the type
  is not a record type or record extension. However, to avoid confusion, cases where a membership test could use
  different equality operators based on the view are illegal.

• {AI05-0153-3} {AI05-0158-1} {AI12-0039-1} The membership choice is a range and the value
  of the tested_simple_expression belongs to the given range.

• {AI05-0153-3} {AI05-0158-1} {AI12-0039-1} {AI12-0071-1} The membership choice is a
  subtype_mark, the tested type is scalar, and the value of the tested_simple_expression belongs to the
given range, or the range of the named subtype, and the value satisfies the predicate of the named subtype evaluates to
True, or

  Ramification: [AI05-0153-3] The scalar membership test only does a range check and a predicate check. It does not
  perform any other check, such as whether a value falls in a “hole” of a “holey” enumeration type. The Pos attribute
  function can be used for that purpose.

  Even though Standard.Float is an unconstrained subtype, the test “X in Float” will still return False (presuming the
  evaluation of X does not raise Constraint_Error) when X is outside Float'Range.

• {AI95-00231-01} {AI05-0153-3} {AI05-0158-1} {AI12-0039-1} {AI12-0071-1} The
  membership choice is a subtype_mark, the tested type is not scalar, and the value of the tested_simple_expression
  satisfies any constraints of the named subtype, the value satisfies the predicate of the named subtype evaluates to
True, and:

  if the type of the simple_expression is class-wide, the value has a tag that identifies a type covered by the
tested type.

• {AI95-00231-01} {AI12-0039-1} if the type of the
tested_simple_expression is class-wide, the value has a tag that identifies
a type covered by the tested type;

  Ramification: [AI12-0039-1] Note that the tag is not checked if the tested_simple_expression is of a specific type.

• {AI95-00231-01} {AI05-0149-1} {AI12-0039-1} if the tested type is an access type and the
  named subtype excludes null, the value of the tested_simple_expression is not null;

• {AI05-0149-1} {AI12-0039-1} if the tested type is a general access-to-object type, the type of the
  tested simple_expression is convertible to the tested type and its
  accessibility level is no deeper than that of the tested type; further, if the designated type of the
tested type is tagged and the tested_simple_expression is nonnull, the
tag of the object designated by the value of the tested_simple_expression is covered by the designated type of the tested type.

  To be honest: [AI12-0005-1] In some of these cases, the bulleted checks need to pass before any predicate check is
  executed. Otherwise, a predicate check could be performed on an object of the wrong type. Consider:
type Root is tagged null record;
  type Ext is new Root with record Data : Integer; end record;
function Is_Even (Param : Ext) return Boolean is
  (Param.Data mod 2 = 0);
subtype Even_Ext is Ext
  with Dynamic Predicate => Is_Even (Even_Ext);
function F (X : Root'Class) return Boolean is
  (X in Even_Ext);
Flag : Boolean := F (Root'(null record)));

If the predicate check is performed before the tag check or regardless of the result of that check, Is_Even would be called on an object that does not have a Data component. Similar cases can be constructed for general access types.

{AI05-0264-1} Otherwise, the test yields the result False.

A membership test using not in gives the complementary result to the corresponding membership test using in.

To be honest: {AI05-0158-1} {AI12-0039-1} X not in A | B | C is intended to be exactly equivalent to not (X in A | B | C), including the order of evaluation of the tested simple_expression and membership_choice.

Implementation Requirements

{8652/0016} {AI95-00123-01} For all nonlimited types declared in language-defined packages, the "=" and "/=" operators of the type shall behave as if they were the predefined equality operators for the purposes of the equality of composite types and generic formal types.

Ramification: {AI95-00123-01} {AI05-0123-1} If any language-defined types are implemented with a user-defined "=" operator, then either the full type must be a record type or, or the compiler must use "magic" to implement equality for this type. A normal user-defined "=" operator for a non-record type does not meet this requirement.

This paragraph was deleted

NOTE {AI95-00123-01} If a composite type has components that depend on discriminants, two values of this type have matching components if and only if their discriminants are equal. Two nonnull arrays have matching components if and only if the length of each dimension is the same for both.

Examples

Examples of expressions involving relational operators and membership tests:

X /= Y

{AI12-0178-1} {AI12-0425-1} A String = "A"

"" < A String and A String < "A"

A_String < "B" and A_String < "A"

My_Car = null

My_Car = Your_Car

My_Car.all = Your_Car.all

N not in 1..10

Today in Mon..Fri

Today in Weekday

Card in Clubs | Spades

Archive in Disk_Unit

Tree.all in Addition'Class

Extensions to Ada 83

Membership tests can be used to test the tag of a class-wide value.

Predefined equality for a composite type is defined in terms of the primitive equals operator for tagged components or the parent part.
Wording Changes from Ada 83
The term “membership test” refers to the relation "X in S" rather than simply the reserved words in or not in.

Wording Changes from Ada 83
We use the term “equality operator” to refer to both the = (equals) and /= (not equals) operators. Ada 83 referred to = as the equality operator, and /= as the inequality operator. The new wording is more consistent with the ISO 10646 name for "=" (equals sign) and provides a category similar to “ordering operator” to refer to both = and /=.

Extensions to Ada 95
The universal access equality operators are new. They provide equality operations (most importantly, testing against null) for anonymous access types.

Wording Changes from Ada 95
We have changed the term “catenate” to “concatenate”.

Extensions to Ada 95
The universal access equality operators are new. They provide equality operations (most importantly, testing against null) for anonymous access types.

Wording Changes from Ada 95
We use the term “equality operator” to refer to both the = (equals) and /= (not equals) operators. Ada 83 referred to = as the equality operator, and /= as the inequality operator. The new wording is more consistent with the ISO 10646 name for "=" (equals sign) and provides a category similar to “ordering operator” to refer to both = and /=.

Extensions to Ada 95
The universal access equality operators are new. They provide equality operations (most importantly, testing against null) for anonymous access types.

Inconsistencies With Ada 2005
User-defined untagged record equality is now defined to compose and be used in generics. Any code which assumes that the predefined equality reemerges in generics and in predefined equals for composite types could fail. However, it is much more likely that this change will fix bugs, as the behavior that would be expected (the user-defined "=" is used) will be true in more cases.

Inconsistencies With Ada 2005
If a composite type contains a component of an untagged record type with an abstract equality operation, calling "=" on the composite type will raise Program_Error, while in the past a result will be returned using the predefined equality. This is quite possible in ASIS programs; it will detect a bug in such programs but of course the programs will need to be fixed before they will work.

Incompatibilities With Ada 2005
Late and hidden overriding of equality for untagged record types is now prohibited. This is necessary to make composition of equality predictable. It should always be possible to move the overriding to an earlier spot where it will be legal.

Extensions to Ada 2005
Membership tests for valid accessibility levels and tag coverage by the designated type for general access types are new.

Extensions to Ada 2005
Membership tests now include a predicate check.

Extensions to Ada 2005
Membership tests now allow multiple choices.

Wording Changes from Ada 2005
Correction: Wording was added to clarify that universal access "=" does not apply if an appropriate operator is declared for a partial or incomplete view of the designated type. Otherwise, adding a partial or incomplete view could make some "=" operators ambiguous.

Inconsistencies With Ada 2012
Removed the incompatible rule preventing the declaration of "=" in the private part of a package specification for an untagged record type that completes a private type. Any code that calls the predefined "=" on the private type will now execute the body for the redefined "=" instead of the predefined "=". Eliminating the rule eliminates an unnecessary incompatibility (especially for programs that never call the predefined "="). Moreover, (like the composition of untagged record "=" in Ada 2012) this is more likely to fix bugs than cause them (who defines an "=" with a presumably different result and does not want clients to use it?).

Incompatibilities With Ada 2012
A membership test is now illegal if all of the following are True:
- The membership test has one or more choice_simple_expressions;
4.5.3 Binary Adding Operators

Static Semantics

The binary adding operators + (addition) and – (subtraction) are predefined for every specific numeric type $T$ with their conventional meaning. They have the following specifications:

1

\begin{verbatim}
function "+"(Left, Right : $T$) return $T$
function "-"(Left, Right : $T$) return $T$
\end{verbatim}

The concatenation operators & are predefined for every nonlimited, one-dimensional array type $T$ with component type $C$. They have the following specifications:

2

\begin{verbatim}
function "&"(Left : $T$; Right : $T$) return $T$
function "&"(Left : $T$; Right : $C$) return $T$
function "&"(Left : $C$; Right : $T$) return $T$
function "&"(Left : $C$; Right : $C$) return $T$
\end{verbatim}

Dynamic Semantics

For the evaluation of a concatenation with result type $T$, if both operands are of type $T$, the result of the concatenation is a one-dimensional array whose length is the sum of the lengths of its operands, and whose components comprise the components of the left operand followed by the components of the right operand. If the left operand is a null array, the result of the concatenation is the right operand. Otherwise, the lower bound of the result is determined as follows:

3

- If the ultimate ancestor of the array type was defined by a constrained_array_definition, then the lower bound of the result is that of the index subtype;

4

**Reason:** This rule avoids Constraint_Error when using concatenation on an array type whose first subtype is constrained.

5

- If the ultimate ancestor of the array type was defined by an unconstrained_array_definition, then the lower bound of the result is that of the left operand.

6

[The upper bound is determined by the lower bound and the length.] A check is made that the upper bound of the result of the concatenation belongs to the range of the index subtype, unless the result is a null array. Constraint_Error is raised if this check fails.

7

If either operand is of the component type $C$, the result of the concatenation is given by the above rules, using in place of such an operand an array having this operand as its only component (converted to the component subtype) and having the lower bound of the index subtype of the array type as its lower bound.
Ramification: The conversion might raise Constraint_Error. The conversion provides “sliding” for the component in the case of an array-of-arrays, consistent with the normal Ada 95 rules that allow sliding during parameter passing.

The result of a concatenation is defined in terms of an assignment to an anonymous object, as for any function call (see 6.5).

Ramification: This implies that value adjustment is performed as appropriate — see 7.6. We don't bother saying this for other predefined operators, even though they are all function calls, because this is the only one where it matters. It is the only one that can return a value having controlled parts.

NOTE As for all predefined operators on modular types, the binary adding operators + and – on modular types include a final reduction modulo the modulus if the result is outside the base range of the type.

Implementation Note: A full "modulus" operation need not be performed after addition or subtraction of modular types. For binary moduli, a simple mask is sufficient. For nonbinary moduli, a check after addition to see if the value is greater than the high bound of the base range can be followed by a conditional subtraction of the modulus. Conversely, a check after subtraction to see if a "borrow" was performed can be followed by a conditional addition of the modulus.

Examples of expressions involving binary adding operators:

- \( Z + 0.1 \) -- \( Z \) has to be of a real type
- "A" & "BCD" -- concatenation of two string literals
- 'A' & "BCD" -- concatenation of a character literal and a string literal
- 'A' & 'A' -- concatenation of two character literals

Inconsistencies With Ada 83

The lower bound of the result of concatenation, for a type whose first subtype is constrained, is now that of the index subtype. This is inconsistent with Ada 83, but generally only for Ada 83 programs that raise Constraint_Error. For example, the concatenation operator in

\[
X : \text{array}(1..10) \text{ of Integer};
\begin{align*}
X := X(6..10) & \text{ & } X(1..5); \\
\end{align*}
\]

would raise Constraint_Error in Ada 83 (because the bounds of the result of the concatenation would be 6..15, which is outside of 1..10), but would succeed and swap the halves of X (as expected) in Ada 95.

Extensions to Ada 83

Concatenation is now useful for array types whose first subtype is constrained. When the result type of a concatenation is such an array type, Constraint_Error is avoided by effectively first sliding the left operand (if nonnull) so that its lower bound is that of the index subtype.

### 4.5.4 Unary Adding Operators

Static Semantics

The unary adding operators + (identity) and – (negation) are predefined for every specific numeric type \( T \) with their conventional meaning. They have the following specifications:

- function "+" (Right : \( T \)) return \( T \)
- function "+" (Right : \( T \)) return \( T \)

NOTE For modular integer types, the unary adding operator –, when given a nonzero operand, returns the result of subtracting the value of the operand from the modulus; for a zero operand, the result is zero.

### 4.5.5 Multiplying Operators

Static Semantics

The multiplying operators * (multiplication), / (division), mod (modulus), and rem (remainder) are predefined for every specific integer type \( T \):
function ** (Left, Right : T) return T
function */ (Left, Right : T) return T
function "mod"(Left, Right : T) return T
function "rem"(Left, Right : T) return T

Signed integer multiplication has its conventional meaning.

Signed integer division and remainder are defined by the relation:

\[ A = (A/B) \times B + (A \text{ rem } B) \]

where \((A \text{ rem } B)\) has the sign of \(A\) and an absolute value less than the absolute value of \(B\). Signed integer division satisfies the identity:

\[ (-A)/B = -(A/B) = A/(-B) \]

The multiplying operators on modular types are defined in terms of the corresponding signed integer operators[, followed by a reduction modulo the modulus if the result is outside the base range of the type] [(which is only possible for the "**" operator)].

{AI05-0260-1} The signed integer modulus operator is defined such that the result of \(A \text{ mod } B\) is either zero, or has the sign of \(B\) and an absolute value less than the absolute value of \(B\); in addition, for some signed integer value \(N\), this result satisfies the relation:

\[ A = B \times N + (A \text{ mod } B) \]

The multiplying operators on modular types are defined in terms of the corresponding signed integer operators[, followed by a reduction modulo the modulus if the result is outside the base range of the type] [(which is only possible for the "**" operator)].

\[ (\text{Ramification:}\ \text{The above identity satisfied by signed integer division is not satisfied by modular division because of the difference in effect of negation.}} \]

Multiplication and division operators are predefined for every specific floating point type \(T\):

function ** (Left, Right : T) return T
function */ (Left, Right : T) return T

The following multiplication and division operators, with an operand of the predefined type Integer, are predefined for every specific fixed point type \(T\):

function ** (Left : T; Right : Integer) return T
function ** (Left : Integer; Right : T) return T
function */ (Left : T; Right : Integer) return T

[All of the above multiplying operators are usable with an operand of an appropriate universal numeric type.] The following additional multiplying operators for \(\text{root_real}\) are predefined[, and are usable when both operands are of an appropriate universal or root numeric type, and the result is allowed to be of type \(\text{root_real}\), as in a \text{number_declaration}]:

\[ (\text{Ramification:}\ \text{These operators are analogous to the multiplying operators involving fixed or floating point types where \text{root_real} substitutes for the fixed or floating point type, and \text{root_integer} substitutes for Integer. Only values of the corresponding universal numeric types are implicitly convertible to these root numeric types, so these operators are really restricted to use with operands of a universal type, or the specified root numeric types.}} \]

function ** (Left, Right : root_real) return root_real
function */ (Left, Right : root_real) return root_real
function ** (Left : root_real; Right : root_integer) return root_real
function ** (Left : root_integer; Right : root_real) return root_real
function */ (Left : root_real; Right : root_integer) return root_real

Multiplication and division between any two fixed point types are provided by the following two predefined operators:

\[ (\text{Ramification:}\ {\{AI12-0005-1\}\} \text{Universal_fixed is the universal type for the class of fixed point types, meaning that these operators take operands of any fixed point \text{typenames} (not necessarily the same) and return a result that is implicitly (or explicitly) convertible to any fixed point type.}} \]

function ** (Left, Right : universal_fixed) return universal_fixed
function */ (Left, Right : universal_fixed) return universal_fixed
The above two fixed-fixed multiplying operators shall not be used in a context where the expected type for the result is itself `universal_fixed` — the context has to identify some other numeric type to which the result is to be converted, either explicitly or implicitly. Unless the predefined universal operator is identified using an expanded name with prefix denoting the package Standard, an explicit conversion is required on the result when using the above fixed-fixed multiplication operator if either operand is of a type having a user-defined primitive multiplication operator such that:

- it is declared immediately within the same declaration list as the type or any partial or incomplete view thereof; and
- both of its formal parameters are of a fixed-point type.

A corresponding requirement applies to the universal fixed-fixed division operator.

**Discussion:** The small of `universal_fixed` is infinitesimal; no loss of precision is permitted. However, fixed-fixed division is impractical to implement when an exact result is required, and multiplication will sometimes result in unanticipated overflows in such circumstances, so we require an explicit conversion to be inserted in expressions like `A * B * C` if `A`, `B`, and `C` are each of some fixed point type.

On the other hand, `X := A * B;` is permitted by this rule, even if `X`, `A`, and `B` are all of different fixed point types, since the expected type for the result of the multiplication is the type of `X`, which is necessarily not `universal_fixed`.

We have made these into Name Resolution rules to ensure that user-defined primitive fixed-fixed operators are not made unusable due to the presence of these universal fixed-fixed operators. But we do allow these operators to be used if prefixed by package Standard, so that they can be used in the definitions of user-defined operators.

**Legality Rules**

The above two fixed-fixed multiplying operators shall not be used in a context where the expected type for the result is itself `universal_fixed` — [the context has to identify some other numeric type to which the result is to be converted, either explicitly or implicitly].

**Discussion:** The small of `universal_fixed` is infinitesimal; no loss of precision is permitted. However, fixed fixed division is impractical to implement when an exact result is required, and multiplication will sometimes result in unanticipated overflows in such circumstances, so we require an explicit conversion to be inserted in expressions like `A * B * C` if `A`, `B`, and `C` are each of some fixed point type.

On the other hand, `X := A * B;` is permitted by this rule, even if `X`, `A`, and `B` are all of different fixed point types, since the expected type for the result of the multiplication is the type of `X`, which is necessarily not `universal_fixed`.

Paragraph 20 was deleted.

**Dynamic Semantics**

The multiplication and division operators for real types have their conventional meaning. [For floating point types, the accuracy of the result is determined by the precision of the result type. For decimal fixed point types, the result is truncated toward zero if the mathematical result is between two multiples of the `small` of the specific result type (possibly determined by context); for ordinary fixed point types, if the mathematical result is between two multiples of the `small`, it is unspecified which of the two is the result.]

The exception `Constraint_Error` is raised by integer division, `rem`, and `mod` if the right operand is zero. [Similarly, for a real type `T` with `T'Machine_Overflows True`, division by zero raises `Constraint_Error`.

**NOTE 1** For positive `A` and `B`, `A/B` is the quotient and `A rem B` is the remainder when `A` is divided by `B`. The following relations are satisfied by the `rem` operator:

```
A rem (-B) = A rem B
(-A) rem B = -(A rem B)
```

**NOTE 2** For any signed integer `K`, the following identity holds:

```
A mod B = (A + K*B) mod B
```
The relations between signed integer division, remainder, and modulus are illustrated by the following table:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A/B</th>
<th>A rem B</th>
<th>A mod B</th>
<th>A</th>
<th>B</th>
<th>A/B</th>
<th>A rem B</th>
<th>A mod B</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>-10</td>
<td>5</td>
<td>-2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>-11</td>
<td>5</td>
<td>-2</td>
<td>-1</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>-12</td>
<td>5</td>
<td>-2</td>
<td>-2</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>-13</td>
<td>5</td>
<td>-2</td>
<td>-3</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>5</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>-14</td>
<td>5</td>
<td>-2</td>
<td>-4</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A/B</th>
<th>A rem B</th>
<th>A mod B</th>
<th>A</th>
<th>B</th>
<th>A/B</th>
<th>A rem B</th>
<th>A mod B</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>-5</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>-10</td>
<td>-5</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>-5</td>
<td>-2</td>
<td>1</td>
<td>-4</td>
<td>-11</td>
<td>-5</td>
<td>2</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>12</td>
<td>-5</td>
<td>-2</td>
<td>2</td>
<td>-3</td>
<td>-12</td>
<td>-5</td>
<td>2</td>
<td>-2</td>
<td>-2</td>
</tr>
<tr>
<td>13</td>
<td>-5</td>
<td>-2</td>
<td>3</td>
<td>-2</td>
<td>-13</td>
<td>-5</td>
<td>2</td>
<td>-3</td>
<td>-3</td>
</tr>
<tr>
<td>14</td>
<td>-5</td>
<td>-2</td>
<td>4</td>
<td>-1</td>
<td>-14</td>
<td>-5</td>
<td>2</td>
<td>-4</td>
<td>-4</td>
</tr>
</tbody>
</table>

**Examples**

Examples of expressions involving multiplying operators:

```ada
I : Integer := 1;
J : Integer := 2;
K : Integer := 3;
X : Real := 1.0;                      -- see 3.5.7
Y : Real := 2.0;
F : Fraction := 0.25;                 -- see 3.5.9
G : Fraction := 0.5;
```

<table>
<thead>
<tr>
<th>Expression</th>
<th>Value</th>
<th>Result Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>I*J</td>
<td>2</td>
<td>same as I and J, that is, Integer</td>
</tr>
<tr>
<td>K/J</td>
<td>1</td>
<td>same as K and J, that is, Integer</td>
</tr>
<tr>
<td>K mod J</td>
<td>1</td>
<td>same as K and J, that is, Integer</td>
</tr>
<tr>
<td>X/Y</td>
<td>0.5</td>
<td>same as X and Y, that is, Real</td>
</tr>
<tr>
<td>F/2</td>
<td>0.125</td>
<td>same as F, that is, Fraction</td>
</tr>
<tr>
<td>3*F</td>
<td>0.75</td>
<td>same as F, that is, Fraction</td>
</tr>
<tr>
<td>0.75*G</td>
<td>0.375</td>
<td>universal_fixed, implicitly convertible to any fixed point type</td>
</tr>
<tr>
<td>Fraction(F*G)</td>
<td>0.125</td>
<td>Fraction, as stated by the conversion</td>
</tr>
<tr>
<td>Real(J)*Y</td>
<td>4.0</td>
<td>Real, the type of both operands after conversion of J</td>
</tr>
</tbody>
</table>

**Incompatibilities With Ada 83**

[AI95-00364-01] [AI95-00420-01] The universal fixed-fixed multiplying operators are now directly available (see below). Any attempt to use user-defined fixed-fixed multiplying operators will be ambiguous with the universal ones. The only way to use the user-defined operators is to fully qualify them in a prefix call. This problem was not documented during the design of Ada 95, and has been mitigated by Ada 2005.

**Extensions to Ada 83**

Explicit conversion of the result of multiplying or dividing two fixed point numbers is no longer required, provided the context uniquely determines some specific fixed point result type. This is to improve support for decimal fixed point, where requiring explicit conversion on every fixed-fixed multiply or divide was felt to be inappropriate.

The type `universal_fixed` is covered by `universal_real`, so real literals and fixed point operands may be multiplied or divided directly, without any explicit conversions required.

**Wording Changes from Ada 83**

We have used the normal syntax for function definition rather than a tabular format.

**Incompatibilities With Ada 95**

[AI95-00364-01] We have changed the resolution rules for the universal fixed-fixed multiplying operators to remove the incompatibility with Ada 83 discussed above. The solution is to hide the universal operators in some circumstances. As a result, some legal Ada 95 programs will require the insertion of an explicit conversion around a fixed-fixed
multiply operator. This change is likely to catch as many bugs as it causes, since it is unlikely that the user wanted to use predefined operators when they had defined user-defined versions.

Wording Changes from Ada 2005

{AI05-0020-1} {AI05-0209-1} **Correction:** Wording was added to clarify that universal fixed "*" and "/" does not apply if an appropriate operator is declared for a partial (or incomplete) view of the designated type. Otherwise, adding a partial (or incomplete) view could make some "*" and "/" operators ambiguous.

{AI05-0260-1} **Correction:** The wording for the mod operator was corrected so that a result of 0 does not have to have "the sign of B" (which is impossible if B is negative).

4.5.6 Highest Precedence Operators

Static Semantics

The highest precedence unary operator abs (absolute value) is predefined for every specific numeric type $T$, with the following specification:

\[
\text{function } \text{"abs"(Right : } T) \text{ return } T
\]

The highest precedence unary operator not (logical negation) is predefined for every boolean type $T$, every modular type $T$, and for every one-dimensional array type $T$ whose components are of a boolean type, with the following specification:

\[
\text{function } \text{"not"(Right : } T) \text{ return } T
\]

The result of the operator not for a modular type is defined as the difference between the high bound of the base range of the type and the value of the operand. [For a binary modulus, this corresponds to a bit-wise complement of the binary representation of the value of the operand.]

The operator not that applies to a one-dimensional array of boolean components yields a one-dimensional boolean array with the same bounds; each component of the result is obtained by logical negation of the corresponding component of the operand (that is, the component that has the same index value). A check is made that each component of the result belongs to the component subtype; the exception Constraint_Error is raised if this check fails.

Discussion: The check against the component subtype is per AI83-00535.

The highest precedence exponentiation operator ** is predefined for every specific integer type $T$ with the following specification:

\[
\text{function } \text{"**"(Left : } T; \text{ Right : Natural) return } T
\]

Exponentiation is also predefined for every specific floating point type as well as root_real, with the following specification (where $T$ is root_real or the floating point type):

\[
\text{function } \text{"**"(Left : } T; \text{ Right : Integer'Base) return } T
\]

{AI05-0088-1} The right operand of an exponentiation is the exponent. The value of expression $X^{**N}$ with the value of the exponent $N$ positive is the same as the value of $X*\ldots X$ (with $N$–1 multiplications) except that the multiplications are associated in an arbitrary order. With $N$ equal to zero, the result is one. With the value of $N$ negative [(only defined for a floating point operand)], the result is the reciprocal of the result using the absolute value of $N$ as the exponent.

Ramification: The language does not specify the order of association of the multiplications inherent in an exponentiation. For a floating point type, the accuracy of the result might depend on the particular association order chosen.

Implementation Permissions

The implementation of exponentiation for the case of a negative exponent is allowed to raise Constraint_Error if the intermediate result of the repeated multiplications is outside the safe range of the
type, even though the final result (after taking the reciprocal) would not be. (The best machine approximation to the final result in this case would generally be 0.0.)

NOTE As implied by the specification given above for exponentiation of an integer type, a check is made that the exponent is not negative. Constraint_Error is raised if this check fails.

Inconsistencies With Ada 83

13.a.1/1 {8652/0100} {AI95-00018-01} The definition of "**" allows arbitrary association of the multiplications which make up the result. Ada 83 required left-to-right associations (confirmed by AI83-00137). Thus it is possible that "**" would provide a slightly different (and more potentially accurate) answer in Ada 95 than in the same Ada 83 program.

Wording Changes from Ada 83

We now show the specification for "**" for integer types with a parameter subtype of Natural rather than Integer for the exponent. This reflects the fact that Constraint_Error is raised if a negative value is provided for the exponent.

Wording Changes from Ada 2005

13.b/3 {AI05-0088-1] Correction: The equivalence definition for "**" was corrected so that it does not imply that the operands are evaluated multiple times.

4.5.7 Conditional Expressions

A conditional expression selects for evaluation at most one of the enclosed dependent expressions, depending on a decision among the alternatives. One kind of conditional expression is the if expression, which selects for evaluation a dependent expression depending on the value of one or more corresponding conditions. The other kind of conditional expression is the case expression, which selects for evaluation one of a number of alternative dependent expressions; the chosen alternative is determined by the value of a selecting expression.

Language Design Principles

1.a/3 {AI05-0188-1] As previously noted, there are two kinds of conditional expression, if expressions and case expressions. Whenever possible, we have written the rules in terms of conditional expressions to avoid duplication.

1.b/3 {AI05-0147-1} The rules for conditional expressions have been designed as much as possible to work similarly to a parenthesized expression. The intent is that as much as possible, wherever a parenthesized expression would be allowed, a conditional expression would be allowed, and it should work the same way.

Syntax

2/3 {AI05-0188-1] conditional_expression ::= if_expression | case_expression

3/3 {AI05-0147-1} {AI05-0188-1} if_expression ::= if condition then dependent_expression

{el1f condition then dependent_expression}
[else dependent_expression]

4/3 {AI05-0147-1] condition ::= boolean_expression

5/3 {AI05-0188-1] case_expression ::= case selecting_expression is case_expression_alternative |

case_expression_alternative |

6/3 {AI05-0188-1] case_expression_alternative ::= when discrete_choice_list => dependent_expression
Wherever the Syntax Rules allow an expression, a conditional_expression may be used in place of the expression, so long as it is immediately surrounded by parentheses.

Discussion: {AI05-0147-1} The syntactic category conditional_expression appears only as a primary that is parenthesized. The above rule allows it to additionally be used in other contexts where it would be directly surrounded by parentheses.

The grammar makes the following directly legal:

```plaintext
A := (if X then Y else Z);  -- parentheses required
A := B + (if X then Y else Z);  -- parentheses required
```

The following procedure calls are syntactically legal; the first uses the above rule to eliminate the redundant parentheses found in the second:

```plaintext
P(if X then Y else Z);
P((if X then Y else Z));  -- redundant parentheses
P((if X then Y else Z), Some Other Param);
P(Some Other Param, (if X then Y else Z));
P(Formal => (if X then Y else Z));
```

whereas the following are illegal:

```plaintext
P(if X then Y else Z, Some Other Param);
P(Some Other Param, if X then Y else Z);
P(Formal => if X then Y else Z);
```

because in these latter cases, the conditional_expression is not immediately surrounded by parentheses (which means on both sides!),

The English-language rule applies in all places that could surround an expression with parentheses, including pragma arguments, type conversion and qualified expression operands, and array index expressions.

This English-language rule could have been implemented instead by adding a nonterminal expression_within_parentheses, which would consist of expressions and conditional_expressions. Then, that could be used in all of the syntax which could consist of parens directly around an expression. We did not do that because of the large amount of change required. A complete grammar is given in AI05-0147-1.

Implementation Note: {AI05-0147-1} Implementers are cautioned to consider error detection when implementing the syntax for conditional_expressions. An if_expression and an if_statement are very similar syntactically, (as are a case_expression and a case_statement) and simple mistakes can appear to change one into the other, potentially causing errors to be moved far away from their actual location. The absence of end if to terminate an if_expression (and end case for a case_expression) also may make error handling harder.

Name Resolution Rules

If a conditional_expression is expected to be of a type T, then each dependent_expression of the conditional_expression is expected to be of type T. Similarly, if a conditional_expression is expected to be of some class of types, then each dependent_expression of the conditional_expression is subject to the same expectation. If a conditional_expression shall resolve to be of a type T, then each dependent_expression shall resolve to be of type T.

The possible types of a conditional_expression are further determined as follows:

- If the conditional_expression is the operand of a type conversion, the type of the conditional_expression is the target type of the conversion; otherwise.
  - Reason: This rule distributes an enclosing type conversion to the dependent_expressions. This means that
    ```plaintext
    T(if C then A else B)
    ```
    has the same semantics as
    ```plaintext
    (if C then T(A) else T(B))
    ```

- If all of the dependent_expressions are of the same type, the type of the conditional_expression is that type; otherwise.

- If a dependent_expression is of an elementary type, the type of the conditional_expression shall be covered by that type; otherwise.
  - Reason: This rule supports the use of numeric literals and universal expressions within a conditional_expression.
• If the conditional_expression is expected to be of type T or shall resolve to type T, then the conditional_expression is of type T.

Ramification: If the type of the conditional_expression cannot be determined by one of these rules, then Name Resolution has failed for that expression, even if the dependent expressions would resolve individually.

A condition is expected to be of any boolean type.

The expected type for the selecting_expression and the discrete choices are as for case statements (see 5.4).

Legality Rules

All of the dependent expressions shall be convertible (see 4.6) to the type of the conditional_expression.

If the expected type of a conditional_expression is a specific tagged type, all of the dependent expressions of the conditional_expression shall be dynamically tagged, or none shall be dynamically tagged. In this case, the conditional_expression is dynamically tagged if all of the dependent expressions are dynamically tagged, is tag-indeterminate if all of the dependent expressions are tag-indeterminate, and is statically tagged otherwise.

If there is no else dependent_expression, the if_expression shall be of a boolean type.

All Legality Rules that apply to the discrete choices of a case_statement (see 5.4) also apply to the discrete choices of a case_expression except within an instance of a generic unit.

Reason: The exemption for a case_expression that occurs in an instance allows the following example:

```ada
generic
  with function Int_Func return Integer;
package G is
  X : Float := case Int_Func is
    when Integer'First .. 1 => 1.0,
    when 0 => 0.0,
    when Positive => 1.0;
end G;
package I is new G (Int_Func => Nat_Func); --Legal
```

Note that the Legality Rules still apply in the generic unit itself; they are just not enforced in an instance of the unit.

Dynamic Semantics

For the evaluation of an if_expression, the condition specified after if, and any conditions specified after elsif, are evaluated in succession (treating a final else as elsif True then), until one evaluates to True or all conditions are evaluated and yield False. If a condition evaluates to True, the associated dependent_expression is evaluated, converted to the type of the if_expression, and the resulting value is the value of the if_expression. Otherwise (when there is no else clause), the value of the if_expression is True.

Ramification: Else is required unless the if_expression has a boolean type, so the last sentence can only apply to if_expressions with a boolean type.

For the evaluation of a case_expression, the selecting_expression is first evaluated. If the value of the selecting_expression is covered by the discrete choice list of some case_expression_alternative, then the dependent expression of the case_expression_alternative is evaluated, converted to the type of the case_expression, and the resulting value is the value of the case_expression. Otherwise (the value is not covered by any discrete_choice_list, perhaps due to being outside the base range), Constraint_Error is raised.
Examples

A112-0429-1 Example of use of an if expression:
A112-0312-1 Put_Line ("Casey is 
   (if Casey.Sex = M then "Male" else "Female") ); -- see 3.10.1

A112-0429-1 Example of use of a case expression:
A112-0312-1 function Card_Color (Card : Suit) return Color is -- see 3.5.1
   (case Card is
      when Clubs | Spades => Black,
      when Hearts | Diamonds => Red);

Extensions to Ada 2005
A105-0147-1 If expressions and case expressions are new.

4.5.8 Quantified Expressions

A112-0158-1 Quantified expressions provide a way to write universally and existentially quantified predicates over containers and arrays.

Syntax

A105-0176-1 quantified_expression ::= 
   for quantifier loop_parameter_specification => predicate 
   | for quantifier iterator_specification => predicate
   quantifier ::= all | some
   predicate ::= boolean_expression

A105-0176-1 Wherever the Syntax Rules allow an expression, a quantified_expression may be used in place of the expression, so long as it is immediately surrounded by parentheses.

Discussion: The syntactic category quantified_expression appears only as a primary that is parenthesized. The above rule allows it to additionally be used in other contexts where it would be directly surrounded by parentheses. This is the same rule that is used for conditional_expressions; see 4.5.7 for a detailed discussion of the meaning and effects of this rule.

Name Resolution Rules

A105-0176-1 The expected type of a quantified_expression is any Boolean type. The predicate in a quantified_expression is expected to be of the same type.

Dynamic Semantics

A105-0176-1 A112-0158-1 A112-0327-1 For the evaluation of a quantified_expression, the loop_parameter_specification or iterator_specification is first elaborated. The evaluation of a quantified_expression then performs an iteration, and evaluates the predicate for each value conditionally produced by the iteration. These values are examined in the order specified by the loop_parameter_specification (see 5.5 and) or iterator_specification (see 5.5.2).

Ramification: A112-0327-1 The order of evaluation of the predicates is that in which the values are produced, as specified in 5.5 or 5.5.2.

A105-0176-1 The value of the quantified_expression is determined as follows:

A112-0158-1 If the quantifier is all, the expression is FalseTrue if the evaluation of any predicate yields False; evaluation of the quantified_expression stops at that point. Otherwise (every predicate has been evaluated and yielded True), the expression is TrueTrue for each value of the loop parameter. It is False otherwise. Evaluation of the quantified_expression stops when
all values of the domain have been examined, or when the predicate yields False for a given value. Any exception raised by evaluation of the predicate is propagated.

**Ramification:** The expression is True if the domain contains no values.

- **{AI12-0158-1}** If the quantifier is `some`, the expression is True if the evaluation of any the predicate yields True; evaluation of the quantified expression stops at that point. Otherwise (every predicate has been evaluated and yielded False), the expression is False for some value of the loop parameter. It is False otherwise. Evaluation of the quantified expression stops when all values of the domain have been examined, or when the predicate yields True for a given value. Any exception raised by evaluation of the predicate is propagated.

**Ramification:** The expression is False if the domain contains no values.

**Examples**

- **{AI05-0176-1}** **{AI12-0429-1}** **Example of a quantified expression as a postcondition for a sorting routine on an array A with an index subtype T:** The postcondition for a sorting routine on an array A with an index subtype T can be written:
  
  ```ada
  Post => (A'Length < 2 or else 
    (for all I in A'First .. T'Pred(A'Last) => A (I) <= A (T'Succ (I))))
  ```

- **{AI05-0176-1}** **{AI12-0429-1}** **{AI12-0430-1}** **Example of use of a quantified expression as an assertion that a positive number N is composite (as opposed to prime):** The assertion that a positive number is composite (as opposed to prime) can be written:
  
  ```ada
  {AI12-0312-1} pragma Assert (for some X in 2 .. N when X * X <= N / 2 => N mod X = 0);
  ```

**Extensions to Ada 2005**

**{AI05-0176-1}** Quantified expressions are new.

**Wording Changes from Ada 2012**

**{AI12-0158-1}** **Corrigendum:** Revised the wording to make it clear that the semantics is short-circuited, and what the result is when there are no values for the loop parameter.

### 4.5.9 Declare Expressions

**{AI112-0236-1}** Declare expressions provide a way to declare local constants and object renamings in an expression context.

**Syntax**

- **{AI12-0236-1}**

  ```ada
  declare_expression ::= 
    declare {declare_item}
    begin body expression
  ```

- **{AI12-0236-1}**

  ```ada
  declare_item ::= object_declaration | object_renaming_declaration
  ```

**Reason:** We allow `(declare begin expression)` with no declare_items, for uniformity with block statements, which also allow a pointless declare.

**Discussion:** The syntactic category `declare_expression` appears only as a primary that is parenthesized. The above rule allows it to additionally be used in other contexts where it would be directly surrounded by parentheses. This is the same rule that is used for conditional expressions; see 4.5.7 for a detailed discussion of the meaning and effects of this rule.
Legality Rules

*A declare item that is an object declaration shall declare a constant of a nonlimited type.*

**Reason:** We disallow limited objects to avoid the horror of task waiting in the middle of an expression. The solution used for controlled objects (wait until the entire expression is finished) isn't appropriate for tasks. This restriction also eliminates build-in-place complexities and the need to activate tasks found in a declare item.

*A declare item that is an object renaming declaration (see 8.5.1) shall not rename an object of a limited type if any operative constituent of the object name is part of a value conversion or is part of a newly constructed object (see 4.4).*

**Reason:** We disallow renaming limited temporary objects (like the result of a function call) for the same reasons as for stand-alone objects. We do allow renaming existing limited objects because these don't cause any problems. Note that one cannot directly rename an aggregate, parenthesized expression, conditional expression, or declare expression (these are not names), but any of these can appear inside of a qualified expression or type conversion (which are names and thus can be renamed).

The following are not allowed within a declare expression: a declaration containing the reserved word aliased; the attribute designator Access or Unchecked Access; or an anonymous access type.

**Reason:** We do not want to define accessibility rules for declare items, as nested declare expressions cause complexities or usage warts. We want to keep this feature simple to use, understand, and implement. Thus, we do not allow any of the features that would require accessibility rules.

Name Resolution Rules

*If a declare expression is expected to be of a type T, then the body expression is expected to be of type T. Similarly, if a declare expression is expected to be of some class of types, then the body expression is subject to the same expectation. If a declare expression shall resolve to be of a type T, then the body expression shall resolve to be of type T.*

The type of a declare expression is the type of the body expression.

Dynamic Semantics

*For the evaluation of a declare expression, the declare items are elaborated in order, and then the body expression is evaluated. The value of the declare expression is that of the body expression.*

Examples

*Example of use of a declare expression as a replacement postcondition for Ada Containers.Vectors."&" (see A.18.2):*

```ada
with Post =>
declare
   Result renames Vectors."&" Result;
   Length : constant Count_Type := Left.Length + Right.Length;
begin
   Result.Length = Length and then
   not Tampering With Elements Prohibited (Result) and then
   not Tampering With Cursors Prohibited (Result) and then
   Result.Capacity >= Length)
```

Extensions to Ada 2012

*Declare expressions are new.*

Incompatibilities With Ada 2022

*Corrigendum: Renaming of limited newly constructed objects is not allowed in a declare expression in original Ada 2022; this is now extended to any parts of such objects. Thus, a (nonlimited) component or slice of a
4.5.10 Reduction Expressions

Reduction expressions provide a way to map or transform a collection of values into a new set of values, and then summarize the values produced by applying an operation to reduce the set to a single value result. A reduction expression is represented as an attribute reference of the reduction attributes Reduce or Parallel_Reduce.

Term entry: reduction expression — expression that defines how to map or transform a collection of values into a new set of values, and then summarize the values by applying an operation to reduce the set to a single value.

Syntax

The chunk specification, if any, of a value_sequence shall be an integer simple_expression.

Name Resolution Rules

The expected type for a reduction_attribute_reference shall be a single nonlimited type.

In the remainder of this subclause, we will refer to nonlimited subtypes Value_Type and Accum_Type of a reduction_attribute_reference. These subtypes and interpretations of the names and expressions of a reduction_attribute_reference are determined by the following rules:

Discussion: Accum_Type represents the result of the reduction (the accumulator type), and Value_Type represents the type of the input values to the reduction.

• Accum_Type is a subtype of the expected type of the reduction_attribute_reference.

• A reducer subprogram is subtype conformant with one of the following specifications:

  function Reducer (Accumulator : Accum_Type;
                  Value : Value_Type) return Accum_Type;

  procedure Reducer (Accumulator : in out Accum_Type;
                     Value : in Value_Type);

• The reducer name of a reduction_specification denotes a reducer subprogram.
• \{A112-0262-1\} The expected type of an initial value expression of a reduction specification is that of subtype Accum_Type.

• \{A112-0250-1\} \{A112-0262-1\} The expected type of the expression of the iterated element association of a value sequence is that of subtype Value_Type.

Legality Rules

\{A112-0262-1\} \{A112-0348-1\} If the reduction attribute reference has a value sequence with the reserved word parallel, the subtypes Accum_Type and Value_Type shall statically match.

\{A112-0262-1\} \{A112-0348-1\} If the identifier of a reduction attribute designator is Parallel_Reduce, the subtypes Accum_Type and Value_Type shall statically match.

Reason: For a reduction attribute reference with a value sequence that does not have the reserved word parallel or has a prefix and the identifier of the reduction attribute designator is Reduce, the subtypes Accum_Type and Value_Type can be different because only one logical thread of control is presumed so there is no need to combine multiple results.

Static Semantics

\{A112-0262-1\} A reduction attribute reference denotes a value, with its nominal subtype being the subtype of the first parameter of the subprogram denoted by the reducer_name.

Dynamic Semantics

\{A112-0250-1\} \{A112-0262-1\} \{A112-0327-1\} \{A112-0355-2\} For the evaluation of a value sequence, the iterated element association, the chunk specification, and the aspect specification, if any, are elaborated in an arbitrary order. Next an iteration is performed, and for each value conditionally produced by the iteration (see 5.5 and 5.5.2), the associated expression is evaluated with the loop parameter having this value, which produces a result that is converted to Value_Type and is used to define the next value in the sequence.

\{A112-0262-1\} If the value sequence does not have the reserved word parallel, it is produced as a single sequence of values by a single logical thread of control. If the reserved word parallel is present in the value sequence, the enclosing reduction attribute reference is a parallel construct, and the sequence of values is generated by a parallel iteration (as defined in 5.5, 5.5.1, and 5.5.2), as a set of non-empty, non-overlapping contiguous chunks (subsequences) with one logical thread of control (see Clause 9) associated with each subsequence. If there is a chunk specification, it determines the maximum number of chunks, as defined in 5.5; otherwise the maximum number of chunks is implementation defined.

Implementation defined: The maximum number of chunks for a parallel reduction expression without a chunk specification.

\{A112-0262-1\} For a value_sequence V, the following attribute is defined:

V'Reduce(Reducer, Initial_Value)

\{A112-0262-1\} \{A112-0348-1\} This attribute represents a reduction expression, and is in the form of a reduction attribute reference.

\{A112-0262-1\} \{A112-0348-1\} The evaluation of a use of this attribute begins by evaluating the parts of the reduction attribute designator (the reducer name Reducer and the initial value expression Initial Value), in an arbitrary order. It then initializes the accumulator of the reduction expression to the value of the initial value expression (the initial value). The value_sequence V is then evaluated.

\{A112-0262-1\} \{A112-0348-1\} If the value_sequence does not have the reserved word parallel, each value of the value_sequence is passed, in order, as the second (Value) parameter to a call on Reducer, with the first (Accumulator) parameter being the prior value...
of the accumulator, saving the result as the new value of the accumulator. The reduction expression yields the final value of the accumulator.

\{AI12-0262-1\} If the reserved word \texttt{parallel} is present in a \texttt{value_sequence}, then the (parallel) reduction expression is a parallel construct and the sequence has been partitioned into one or more subsequences (see above) each with its own separate logical thread of control.

\{AI12-0262-1\} \{AI12-0348-1\} Each logical thread of control creates a local accumulator for processing its subsequence. The accumulator for a subsequence is initialized to the first value of the subsequence, and calls on Reducer start with the second value of the subsequence (if any). The result for the subsequence is the final value of its local accumulator.

\{AI12-0262-1\} \{AI12-0348-1\} After all logical threads of control of a parallel reduction expression have completed, Reducer is called for each subsequence, in the original sequence order, passing the local accumulator for that subsequence as the second (Value) parameter, and the overall accumulator ([initialized above to the initial value]) as the first (Accumulator) parameter, with the result saved back in the overall accumulator. The parallel reduction expression yields the final value of the overall accumulator.

\{AI12-0262-1\} If the evaluation of the \texttt{value_sequence} yields an empty sequence of values, the reduction expression yields the initial value.

\{AI12-0262-1\} \{AI12-0348-1\} If an exception is propagated by one of the calls on Reducer, that exception is propagated from the reduction expression. If different exceptions are propagated in different logical threads of control, one is chosen arbitrarily to be propagated from the reduction expression as a whole.

**Implementation Note:** [AI12-0262-1] For a reduction \texttt{attribute_reference} that has a \texttt{value_sequence} without the reserved word \texttt{parallel} or a prefix where the identifier of the \texttt{reduction_attribute_designator} is \texttt{Reduce} (see below), generally the compiler can still choose to execute the reduction in parallel, presuming doing so would not change the results. However sequential execution is necessary if the subtypes of the parameters of Reducer do not statically match, since there is no subprogram identified in the construct that could be used for combining the results in parallel.

**Discussion:** [AI12-0262-1] We say the calls to Reducer that combine the results of parallel execution are sequentially ordered in increasing order because certain reductions, such as vector concatenation, can be non-commutative (but still associative) operations. In order to return a deterministic result for parallel execution that is consistent with sequential execution, we need to specify an order for the iteration, and for the combination of results from the logical threads of control. It is also necessary that combining calls to Reducer are issued sequentially with respect to each other, which may require extra synchronization if the calls to Reducer are being executed by different logical threads of control.

\{AI12-0262-1\} For a prefix \texttt{X} of an array type \[ (after any implicit dereference) \], or that denotes an iterable container object (see 5.5.1), the following attributes are defined:

\begin{verbatim}
X'Reduce(Reducer, Initial_Value)
\end{verbatim}

\{AI12-0262-1\} \{AI12-0348-1\] X'Reduce is a reduction expression that yields a result equivalent to replacing the prefix of the attribute with the value_sequence:

\begin{verbatim}
[for Item of X => Item]
\end{verbatim}

\begin{verbatim}
X'Parallel_Reduce(Reducer, Initial_Value)
\end{verbatim}

\{AI12-0262-1\} \{AI12-0348-1\] X'Parallel_Reduce is a reduction expression that yields a result equivalent to replacing the attribute identifier with Reducer and the prefix of the attribute with the value_sequence:

\begin{verbatim}
[parallel for Item of X => Item]
\end{verbatim}

**Bounded (Run-Time) Errors**

\{AI12-0262-1\} \{AI12-0348-1\] For a parallel reduction expression, it is a bounded error if the reducer subprogram is not associative. That is, for any arbitrary values of subtype \texttt{Value_Type A, B, C} and a reducer function \texttt{R}, the result of \texttt{R (A, R (B, C))} should produce a result equal to \texttt{R (R (A, B), C)}; it is a bounded error if \texttt{R} does not. The possible consequences are \texttt{Program_Error}, or a result that does not
match the equivalent sequential reduction expression due to the order of calls on the reducer subprogram being unspecified in the overall reduction. Analogous rules apply in the case of a reduction procedure.

**Reason:** In a sequential reduction expression, the reducer subprogram is called in a left-to-right order, whereas in a parallel reduction expression, the reducer subprogram is called in an order that depends on the number of logical threads of control that execute the reduction and on the elements/components given to each chunk. If the reducer is associative, this order does not matter, but in other cases, very different results are possible. While one can specify the maximum number of chunks, the actual number of chunks is unspecified. Similarly, the split of elements has only weak requirements. Thus, to get a consistent and portable result, an associative reducer is required for a parallel reduction. We define this as a Bounded (Run-Time) Errors to provide a stern warning about the required nature of the reducer subprogram and to let compilers detect the problem when possible.

**To be honest:** In this rule, “equal” means semantically equal. We don’t care if the bit patterns differ but that the results mean the same thing. In particular, if the primitive equal is user-defined, that equality would be the one used to determine if this rule is violated.

**Examples**

```
function Factorial(N : Natural) return Natural is
  (for J in 1..N => J)'Reduce("*", 1));

function Sine (X : Float; Num_Terms : Positive := 5) return Float is
  (for I in 1..Num_Terms =>
   ((-1.0)**(I-1) * X**(2*I-1)/Float(Factorial(2*I-1)))
    'Reduce("+", 0.0));

Put_Line ("Sum of Squares is" &
  Integer'Image((for I in 1..10 => I**2)'Reduce("+", 0)));

-- See 3.5.7.
function Pi (Number_Of_Steps : Natural := 10_000) return Real is
  (1.0 / Real (Number_Of_Steps) *
   (for I in 1..Number_Of_Steps =>
    (4.0 / (1.0 + ((Real (I) - 0.5) *
    (1.0 / Real (Number_Of_Steps)))**2)))
    'Reduce("+", 0.0));

A'Reduce("+", 0)  -- See 4.3.3.
```

**AI12-0262-1** **AI12-0429-1** Example of an expression function that returns its result as a reduction expression:

```
function Factorial(N : Natural) return Natural is
  (for J in 1..N => J)'Reduce("*", 1));
```

**AI12-0262-1** **AI12-0429-1** Example of a reduction expression that computes the Sine of X using a Taylor expansion:

```
function Sine (X : Float; Num_Terms : Positive := 5) return Float is
  (for I in 1..Num_Terms =>
   ((-1.0)**(I-1) * X**(2*I-1)/Float(Factorial(2*I-1)))
    'Reduce("+", 0.0));
```

**AI12-0262-1** **AI12-0379-1** **AI12-0429-1** Example of a reduction expression that outputs the sum of squares:

```
Put_Line ("Sum of Squares is" &
  Integer'Image((for I in 1..10 => I**2)'Reduce("+", 0)));
```

**AI12-0262-1** **AI12-0379-1** **AI12-0429-1** Example of a reduction expression used to compute the value of Pi:

```
-- See 3.5.7.
function Pi (Number_Of_Steps : Natural := 10_000) return Real is
  (1.0 / Real (Number_Of_Steps) *
   (for I in 1..Number_Of_Steps =>
    (4.0 / (1.0 + ((Real (I) - 0.5) *
    (1.0 / Real (Number_Of_Steps)))**2)))
    'Reduce("+", 0.0));
```

**AI12-0242-1** **AI12-0429-1** Example of a reduction expression used to calculate the sum of elements of an array of integers:

```
A'Reduce("+", 0)  -- See 4.3.3.
```

**AI12-0242-1** **AI12-0429-1** Example of a reduction expression used to determine if all elements in a two-dimensional array of booleans are set to true:

```
Grid'Reduce("and", True)  -- See 3.6.
```

**AI12-0242-1** **AI12-0429-1** Example of a reduction expression used to calculate the minimum value of an array of integers in parallel:

```
A'Parallel_Reduce(Integer'Min, Integer'Last)
```

**AI12-0312-1** **AI12-0429-1** Example of a parallel reduction expression used to calculate the mean of the elements of a two-dimensional array of subtype Matrix (see 3.6) that are greater than 100.0:
type Accumulator is record
  Sum    : Real; -- See 3.5.7.
  Count  : Integer;
end record;

function Accumulate (L, R : Accumulator) return Accumulator is
  (Sum   => L.Sum   + R.Sum,
   Count => L.Count + R.Count);

function Average_of_Values_Greater_Than_100 (M : Matrix) return Real is
  (declare
    Acc : constant Accumulator := [parallel for Val of M when Val > 100.0 => (Val, 1)]
    'Reduce(Accumulate, (Sum => 0, Count => 0));
  begin
    Acc.Sum / Real(Acc.Count));

Extensions to Ada 2012

\{AI12-0005-1\} \{AI12-0242-1\} \{AI12-0262-1\} \{AI12-0348-1\} Reduction expressions and the associated attributes are new.

4.6 Type Conversions

\{AI05-0299-1\} [Explicit type conversions, both value conversions and view conversions, are allowed between closely related types as defined below. This subclause also defines rules for value and view conversions to a particular subtype of a type, both explicit ones and those implicit in other constructs.]

Syntax

\begin{align*}
type_conversion ::= \\
  \text{subtype\_mark(expression)} \\
  | \text{subtype\_mark(name)}
\end{align*}

The target subtype of a type_conversion is the subtype denoted by the subtype_mark. The operand of a type_conversion is the expression or name within the parentheses; its type is the operand type.

\{AI05-0299-1\} One type is convertible to a second type if a type_conversion with the first type as operand type and the second type as target type is legal according to the rules of this subclause. Two types are convertible if each is convertible to the other.

\textbf{Ramification:} Note that “convertible” is defined in terms of legality of the conversion. Whether the conversion would raise an exception at run time is irrelevant to this definition.

\{AI95-00184-01\} \{AI95-00330-01\} \{AI12-0392-1\} A type_conversion whose operand is the name of an object is called a view conversion if both its target type and operand type are tagged, or if it appears in a call as an actual parameter of mode out or in out; other type_conversions are called value conversions.

\textbf{Ramification:} A view conversion to a tagged type can appear in any context that requires an object name, including in an object renaming, the prefix of a selected_component, and if the operand is a variable, on the left side of an assignment_statement. View conversions to other types only occur as actual parameters. Allowing view conversions of untagged types in all contexts seemed to incur an undue implementation burden.

\textbf{Ramification:} A type_conversion appearing as an in out parameter in a generic instantiation is not a view conversion; the second part of the rule only applies to subprogram calls, not instantiations.

\textbf{Name Resolution Rules}

\textbf{Discussion:} This replaces the “must be determinable” wording of Ada 83. This is equivalent to (but hopefully more intuitive than) saying that the operand of a type_conversion is a “complete context”.

4.5.10 Reduction Expressions
The operand of a view conversion is interpreted only as a name; the operand of a value conversion is interpreted as an expression.

**Reason:** {AI12-0005-1} This formally resolves the syntactic ambiguity between the two forms of type_conversion. This matter because an expression that is a name is evaluated and represents a value while a name by itself can be an object, we want a view conversion to be an object, not that it really matters.

**Ramification:** {AI12-0005-1} This wording uses "interpreted as" rather than "shall be" so that this rule is not used to resolve overloading; it is solely about evaluation as described above.

### Legality Rules

**AI95-00251-01** In a view conversion for an untagged type, the target type shall be convertible (back) to the operand type. If the target type is a numeric type, then the operand type shall be a numeric type.

**Reason:** Untagged view conversions appear only as in or out parameters. Hence, the reverse conversion must be legal as well. The forward conversion must be legal even for an out parameter, because (for example) actual parameters of an access type are always copied in anyway.

### Discussion

Paragraphs 9 through 20 were reorganized and moved below.

**Discussion:** {AI95-00251-01} The entire Legality Rules section has been reorganized to eliminate an unintentional incompatibility with Ada 83. In rare cases, a type conversion between two types related by derivation is not allowed by Ada 95, while it is allowed in Ada 83. The reorganization fixes this. Much of the wording of the legality section is unchanged, but it is reordered and reformatted. Because of the limitations of our tools, we had to delete and replace nearly the entire section. The text of Ada 95 paragraphs 8 through 12, 14, 15, 17, 19, 20, and 24 are unchanged (just moved); these are now 24.1 through 24.5, 24.12, 24.13, 24.17, 24.19, 24.20, and 8.

**AI95-00251-01** If the target type is an array type, then the operand type shall be an array type. Further:

- **AI95-00251-01** The types shall have the same dimensionality;
- **8652/0008** {AI95-00168-01} {AI95-00251-01} Corresponding index types shall be convertible; and
- **8652/0008** {AI95-00168-01} {AI95-00251-01} The component subtypes shall statically match; and
- **8652/0008** {AI95-00168-01} {AI95-00251-01} In a view conversion, the target type and the operand type shall both or neither have aliased components.

**Reason:** Without this rule, it is possible to violate the constrained status of aliased array components. Consider:

```ada
package P is
  type T is private;
  A : constant T;
  Type A1 is array (1 .. 10) of aliased T;
  Type A2 is array (1 .. 10) of T;
private
  type T (D : Integer := 0) is null record;
  A : constant T := (D => 1);
end P;
with P;
procedure Exam is
  X : P.A1;
  procedure S (Y : in out P.A2) is
  begin
    Y (1) := P.A;
  end S;
begin
  S (P.A2 (X)); -- This call will change the discriminant of X (1),
  -- so we cannot allow the conversion.
end Exam;
```

**AI95-00251-01** If the target type is a general access type, then the operand type shall be an access to object type. Further:

**Discussion:** The Legality Rules and Dynamic Semantics are worded so that a type_conversion T(X) (where T is an access type) is (almost) equivalent to the attribute_reference X.all'Access, where the result is of type T. The type_conversion accepts a null value, whereas the attribute_reference would raise Constraint_Error.
• `{AI95-00251-01}` If the target type is an access to variable type, then the operand type shall be an access to variable type;

  **Ramification:** If the target type is an access to constant type, then the operand type can be access to constant or access to variable.

• `{AI95-00251-01}` If the target designated type is tagged, then the operand designated type shall be convertible to the target designated type.

• `{AI95-00251-01}` If the target designated type is not tagged, then the designated types shall be the same, and either the designated subtypes shall statically match or the target designated subtype shall be discriminated and unconstrained; and

  **Reason:** These rules are designed to ensure that aliased array objects only need "dope" if their nominal subtype is unconstrained, but they can always have dope if required by the run-time model (since no sliding is permitted as part of access type conversion). By contrast, aliased discriminated objects will always need their discriminants stored with them, even if nominally constrained. (Here, we are assuming an implementation that represents an access value as a single pointer.)

• `{AI95-00251-01}` The accessibility level of the operand type shall not be statically deeper than that of the target type. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

  **Ramification:** The access parameter case is handled by a runtime check. Runtime checks are also done in instance bodies.

• `{AI95-00251-01}` If the target type is an access to subprogram type, then the operand type shall be an access to subprogram type. Further:

  • `{AI95-00251-01}` The designated profiles shall be subtype conformant.

  • `{AI95-00251-01}` The accessibility level of the operand type shall not be statically deeper than that of the target type. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit. If the operand type is declared within a generic body, the target type shall be declared within the generic body.

  **Reason:** The reason it is illegal to convert from an access to subprogram type declared in a generic body to one declared outside that body is that in an implementation that shares generic bodies, procedures declared inside the generic need to have a different calling convention—they need an extra parameter pointing to the data declared in the current instance. For procedures declared in the spec, that's OK, because the compiler can know about them at compile time of the instantiation.

• `{AI95-00251-01}` If there is a type (other than a root numeric type) that is an ancestor of both the target type and the operand type, or both types are class-wide types, then at least one of the following rules shall apply; if the target type is not included in any of the above four cases, there shall be a type that is an ancestor of both the target type and the operand type. Further, if the target type is tagged, then either:

  • `{AI95-00251-01}` The target type shall be untagged; or

  • `{AI95-00251-01}` The operand type shall be a class-wide type that covers the target type; or

  **Ramification:** This is a conversion toward the root, which is always safe.

  • `{AI95-00251-01}` The operand type shall be a class-wide type that covers the target type; or

  **Ramification:** This is a conversion of a class-wide type toward the leaves, which requires a tag check. See Dynamic Semantics.

• `{AI95-00251-01}` These two rules imply that a conversion from an ancestor parent type to a type extension is not permitted, as this would require specifying the values for additional components, in general, and changing the tag. An extension aggregate has to be used instead, constructing a new value, rather than converting an existing value. However, a conversion from the class-wide type rooted at an ancestor parent type is permitted; such a conversion just verifies that the operand's tag is a descendant of the target.

• `{AI95-00251-01}` The operand and target types shall both be class-wide types and the specific type associated with at least one of them shall be an interface type.
Ramification: We allow converting any class-wide type T'Class to or from a class-wide interface type even if the specific type T does not have an appropriate interface ancestor, because some extension of T might have the needed ancestor. This is similar to a conversion of a class-wide type toward the leaves of the tree, and we need to be consistent. Of course, there is a runtime check that the actual object has the needed interface.

\{AI95-00251-01\} \{AI05-0115-1\} If there is no type (other than a root numeric type) that is the ancestor of both the target type and the operand type, and they are not both class-wide types, one of the following rules shall apply: In a view conversion for an untagged type, the target type shall be convertible (back) to the operand type.

Reason: Untagged view conversions appear only as [in] out parameters. Hence, the reverse conversion must be legal as well. The forward conversion must be legal even if an out parameter, because actual parameters of an access type are always copied in anyway.

- \{AI95-00251-01\} If the target type is a numeric type, then the operand type shall be a numeric type.
- \{AI95-00251-01\} If the target type is an array type, then the operand type shall be an array type. Further:
  - \{AI95-00251-01\} The types shall have the same dimensionality;
  - \{AI95-00251-01\} Corresponding index types shall be convertible;
  - \{AI95-00251-01\} The component subtypes shall statically match;
  - \{AI95-00392-01\} If the component types are anonymous access types, then the accessibility level of the operand type shall not be statically deeper than that of the target type;

Reason: For unrelated array types, the component types could have different accessibility, and we had better not allow a conversion of a local type into a global type, in case the local type points at local objects. We don't need a check for other types of components; such components necessarily are for related types, and either have the same accessibility or (for access discriminants) cannot be changed so the discriminant check will prevent problems.

- \{AI95-00246-01\} Neither the target type nor the operand type shall be limited;
  Reason: We cannot allow conversions between unrelated limited types, as they may have different representations, and (since the types are limited), a copy cannot be made to reconcile the representations.

- \{AI95-00251-01\} \{AI95-00363-01\} If the target type of a view conversion has aliased components, then so shall the operand type; and

Reason: \{AI95-00363-01\} We cannot allow a view conversion from an object with unaliased components to an object with aliased components, because that would effectively allow pointers to unaliased components. This rule was missing from Ada 95.

- \{AI95-00246-01\} \{AI95-00251-01\} The operand type of a view conversion shall not have a tagged, private, or volatile subcomponent.

Reason: \{AI95-00246-01\} We cannot allow view conversions between unrelated might-be-by-reference types, as they may have different representations, and a copy cannot be made to reconcile the representations.

Ramification: These rules only apply to unrelated array conversions; different (weaker) rules apply to conversions between related types.

- \{AI95-00230-01\} If the target type is universal access, then the operand type shall be an access type.
  Discussion: Such a conversion cannot be written explicitly, of course, but it can be implicit (see below).

- \{AI95-00230-01\} \{AI95-00251-01\} If the target type is a general access-to-object type, then the operand type shall be universal access or an access-to-object type. Further, if the operand type is not universal access:

  Discussion: The Legality Rules and Dynamic Semantics are worded so that a type conversion T(X) (where T is an access type) is (almost) equivalent to the attribute reference X.all'Access, where the result is of type T. The only difference is that the type conversion accepts a null value, whereas the attribute reference would raise Constraint_Error.
• \{AI95-00251-01\} If the target type is an access-to-variable type, then the operand type shall be an access-to-variable type;

**Ramification:** If the target type is an access-to-constant type, then the operand type can be access-to-constant or access-to-variable.

• \{AI95-00251-01\} If the target designated type is tagged, then the operand designated type shall be convertible to the target designated type;

• \{AI95-00251-01\} \{AI95-00363-01\} If the target designated type is not tagged, then the designated types shall be the same, and either:
  - \{AI95-00363-01\} the designated subtypes shall statically match; or
  - \{AI95-00363-01\} \{AI95-00384-01\} the designated type shall be discriminated in its full view and unconstrained in any partial view, and one of the designated subtypes shall be unconstrained;

**Ramification:** \{AI95-00363-01\} This does not require that types have a partial view in order to allow the conversion, simply that any partial view that does exist is unconstrained.

• \{AI95-00384-01\} This allows conversions both ways (either subtype can be unconstrained); while Ada 95 only allowed the conversion if the target subtype is unconstrained. We generally want type conversions to be symmetric; which type is the target shouldn’t matter for legality.

**Reason:** \{AI95-00363-01\} If the visible partial view is constrained, we do not allow conversion between unconstrained and constrained subtypes. This means that whether the full type had discriminants is not visible to clients of the partial view.

**Discussion:** \{AI12-0005-1\} \{AI12-0005-1\} We assume the worst in a generic body about whether or not a formal subtype has a constrained partial view; specifically, in a generic body a discriminated subtype is considered to have a constrained partial view if it is a descendant of an untagged generic formal private or derived type (see 12.5.1 for the formal definition of this rule).

**Reason:** These rules are designed to ensure that aliased array objects only need "dope" if their nominal subtype is unconstrained, but they can always have dope if required by the run-time model (since no sliding is permitted as part of access type conversion). By contrast, aliased discriminated objects will always need their discriminants stored with them, even if nominally constrained. (Here, we are assuming an implementation that represents an access value as a single pointer.)

• \{AI95-00251-01\} \{AI05-0148-1\} \{AI05-0248-1\} \{AI12-0027-1\} The accessibility level of the operand type shall not be statically deeper than that of the target type, unless the target type is an anonymous access type of a stand-alone object. If the target type is that of such a stand-alone object, the accessibility level of the operand type shall not be statically deeper than that of the declaration of the stand-alone object. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

**Ramification:** \{AI05-0148-1\} The access parameter case is handled by a run-time check. runtime checks are also done in instance bodies, and for stand-alone objects of anonymous access types.

**Reason:** We prohibit storing accesses to objects deeper than a stand-alone object of an anonymous access-to-object (even while we allow storing all other accesses) in order to prevent dangling accesses.

• \{AI95-00230-01\} If the target type is a pool-specific access-to-object type, then the operand type shall be \textit{universal access}.

**Reason:** This allows \textit{null} to be converted to pool-specific types. Without it, \textit{null} could be converted to general access types but not pool-specific ones, which would be too inconsistent. Remember that these rules only apply to unrelated types, so we don't have to talk about conversions to derived or other related types.

• \{AI95-00230-01\} \{AI95-00251-01\} If the target type is an access-to-subprogram type, then the operand type shall be \textit{universal access} or an access-to-subprogram type. Further, if the operand type is not \textit{universal access}:
  - \{AI95-00251-01\} \{AI05-0239-1\} The designated profiles shall be subtype conformantsubtype conformant.
{AI95-00251-01} {AI12-0027-1} The accessibility level of the operand type shall not be 
statically deeper than that of the target type. In addition to the places where Legality Rules 
normally apply (see 12.3), this rule applies also in the private part of an instance of a generic 
unit. If the operand type is declared within a generic body, the target type shall be declared 
within the generic body.

**Reason:** The reason it is illegal to convert from an access-to-subprogram type declared in a generic body to one 
declared outside that body is that in an implementation that shares generic bodies, subprograms declared inside the 
generic need to have a different calling convention — they need an extra parameter pointing to the data declared in the 
current instance. For subprograms declared in the spec, that's OK, because the compiler can know about them at 
compile time of the instantiation.

{AI12-0380-1} If the target type has a Global aspect other than in out all or Unspecified, 
then each mode of the Global aspect of the operand type shall identify a subset of the 
variables identified by the corresponding mode of the target type Global aspect, or by the in out 
mode of the target type Global aspect.

{AI12-0064-2} If the target type is nonblocking, the operand type shall be nonblocking.

{AI11-0027-1} In addition to the places where Legality Rules normally apply (see 12.3), these rules apply 
also in the private part of an instance of a generic unit.

**Discussion:** {AI12-0005-1} This applies to all of the Legality Rules in this section. It won't matter for the majority of 
these rules, but in any case that it does, we want to apply the same rules in the private part. (Ada got the default 
wrong for these, as there is only one known case where we don't want to recheck in the private part, see derivations 
without record extensions in 3.4.)

### Static Semantics

A type_conversion that is a value conversion denotes the value that is the result of converting the value 
of the operand to the target subtype.

{AI05-0264-1} A type_conversion that is a view conversion denotes a view of the object denoted by the 
operand. This view is a variable of the target type if the operand denotes a variable; otherwise, it is a 
constant of the target type.

The nominal subtype of a type_conversion is its target subtype.

### Dynamic Semantics

For the evaluation of a type_conversion that is a value conversion, the operand is evaluated, and then the 
value of the operand is converted to a corresponding value of the target type, if any. If there is no value of 
the target type that corresponds to the operand value, Constraint_Error is raised; this can only happen on 
conversion to a modular type, and only when the operand value is outside the base range of the modular 
type.] Additional rules follow:

- **Numeric Type Conversion**
  - If the target and the operand types are both integer types, then the result is the value of the 
target type that corresponds to the same mathematical integer as the operand.
  - If the target type is a decimal fixed point type, then the result is truncated (toward 0) if the 
value of the operand is not a multiple of the small of the target type.
  - If the target type is some other real type, then the result is within the accuracy of the target 
type (see G.2, “Numeric Performance Requirements”, for implementations that support the 
Numerics Annex).

  **Discussion:** An integer type might have more bits of precision than a real type, so on conversion (of a large integer), 
some precision might be lost.

- If the target type is an integer type and the operand type is real, the result is rounded to the 
nearest integer (away from zero if exactly halfway between two integers).
4.6 Type Conversions

Discussion: \{AI95-00267-01\} This was implementation defined in Ada 83. There seems no reason to preserve the nonportability in Ada 95. Round-away-from-zero is the conventional definition of rounding, and standard Fortran and COBOL both specify rounding away from zero, so for interoperability, it seems important to pick this. This is also the most easily “undone” by hand. Round-to-nearest-even is an alternative, but that is quite complicated if not supported by the hardware. In any case, this operation is not usually expected to be part of an inner loop, so predictability and portability are judged most important. A floating point attribute function Unbiased Rounding will be provided (see A.5.3) for those applications that require round-to-nearest-even, and a floating point attribute function Machine Rounding (also see A.5.3) is provided for those applications that require the highest possible performance. “Deterministic” rounding is required for static conversions to integer as well. See 4.9.

- **Enumeration Type Conversion**
  - The result is the value of the target type with the same position number as that of the operand value.

- **Array Type Conversion**
  - If the target subtype is a constrained array subtype, then a check is made that the length of each dimension of the value of the operand equals the length of the corresponding dimension of the target subtype. The bounds of the result are those of the target subtype.
  - If the target subtype is an unconstrained array subtype, then the bounds of the result are obtained by converting each bound of the value of the operand to the corresponding index type of the target type. For each nonnull index range, a check is made that the bounds of the range belong to the corresponding index subtype.

  Discussion: Only nonnull index ranges are checked, per AI83-00313.

  In either array case, the value of each component of the result is that of the matching component of the operand value (see 4.5.2).

  Ramification: This applies whether or not the component is initialized.

- **Composite (Non-Array) Type Conversion**
  - The value of each nondiscriminant component of the result is that of the matching component of the operand value.

  Ramification: This applies whether or not the component is initialized.

  [The tag of the result is that of the operand.] If the operand type is class-wide, a check is made that the tag of the operand identifies a (specific) type that is covered by or descended from the target type.

  Ramification: This check is certain to succeed if the operand type is itself covered by or descended from the target type.

  Proof: The fact that a type_conversion preserves the tag is stated officially in 3.9, “Tagged Types and Type Extensions”

  For each discriminant of the target type that corresponds to a discriminant of the operand type, its value is that of the corresponding discriminant of the operand value; if it corresponds to more than one discriminant of the operand type, a check is made that all these discriminants are equal in the operand value.

  For each discriminant of the target type that corresponds to a discriminant that is specified by the derived_type_definition for some ancestor of the operand type (or if class-wide, some ancestor of the specific type identified by the tag of the operand), its value in the result is that specified by the derived_type_definition.
Ramification: It is a ramification of the rules for the discriminants of derived types that each discriminant of the result is covered either by this paragraph or the previous one. See 3.7.

- For each discriminant of the operand type that corresponds to a discriminant that is specified by the derived_type_definition for some ancestor of the target type, a check is made that in the operand value it equals the value specified for it.
- For each discriminant of the result, a check is made that its value belongs to its subtype.

Access Type Conversion

- \{AI05-0148-1\} \{AI05-0248-1\} For an access-to-object type, a check is made that the accessibility level of the operand type is not deeper than that of the target type, unless the target type is an anonymous access type of a stand-alone object. If the target type is that of such a stand-alone object, a check is made that the accessibility level of the operand type is not deeper than that of the declaration of the stand-alone object; then if the check succeeds, the accessibility level of the target type becomes that of the operand type.

Ramification: \{AI05-0148-1\} This check is needed for operands that are access parameters, for stand-alone anonymous access objects, and in instance bodies.

Access Type Conversion

Note that this check can never fail for the implicit conversion to the anonymous type of an access parameter that is done when calling a subprogram with an access parameter.

- \{AI95-00230-01\} \{AI95-00231-01\} If the target type is an anonymous access type, a check is made that the value of the operand is not null; if the target is not an anonymous access type, then the result is null if the operand value is null, the result of the conversion is the null value of the target type.

Ramification: A conversion to an anonymous access type happens implicitly as part of initializing or assigning to an anonymous access object, access discriminant, or access parameter.

Reason: \{AI95-00231-01\} As explained in 3.10, "Access Types", it is important that a value of an anonymous access type can never be null.

- If the operand value is not null, then the result designates the same object (or subprogram) as is designated by the operand value, but viewed as being of the target designated subtype (or profile); any checks associated with evaluating a conversion to the target designated subtype are performed.

Ramification: The checks are certain to succeed if the target and operand designated subtypes statically match.

\{AI95-00231-01\} \{AI95-0153-3\} \{AI05-0290-1\} \{AI12-0071-1\} \{AI12-0333-1\} After conversion of the value to the target type, if the target subtype is constrained, a check is performed that the value satisfies this constraint. If the target subtype excludes null, then a check is made that the value is not null. If predicate checks are enabled for the target subtype (see 3.2.4), a check is performed that the value satisfies the predicate predicate of the target subtype is satisfied for the value, unless the conversion is:

- \{AI12-0333-1\} \{AI12-0333-1\} a view conversion that is the target of an assignment statement and is not referenced with a target_name, or an actual parameter of mode out; or
- \{AI12-0333-1\} an implicit subtype conversion of an actual parameter of mode out to the nominal subtype of its formal parameter.

Ramification: \{AI12-0333-1\} The reverse conversion applied to by-copy out parameters is not a view conversion and it is to the nominal subtype of the actual parameter, therefore any enabled predicate checks are performed.

For the evaluation of a view conversion, the operand name is evaluated, and a new view of the object denoted by the operand is created, whose type is the target type; if the target type is composite, checks are performed as above for a value conversion.
The properties of this new view are as follows:

- \(\{8652/0017\} \{AI95-00184-01\}\) If the target type is composite, the bounds or discriminants (if any) of the view are as defined above for a value conversion; each nondiscriminant component of the view denotes the matching component of the operand object; the subtype of the view is constrained if either the target subtype or the operand object is constrained, or if the target subtype is indefinite, or if the operand type is a descendant of the target type, and has discriminants that were not inherited from the target type;

- \(\{AI12-0439-1\}\) If the target type is tagged, then an assignment to the view assigns to the corresponding part of the object denoted by the operand; otherwise, an assignment to the view assigns to the object, after converting the assigned value to the subtype of the object (which can raise Constraint_Error);

- \(\{AI12-0074-1\} \{AI12-0439-1\}\) Reading the value of the view yields the result of converting the value of the operand object to the target subtype (which can raise Constraint_Error), except if the object is of an elementary access type and the view conversion is passed as an out parameter; in this latter case, the value of the operand object may be used to initialize the formal parameter without checking against any constraint of the target subtype (as described more precisely in 6.4.1).

Rea son: \(\{AI12-0074-1\}\) This ensures that even an out parameter of an elementary access type is initialized reasonably.

- \(\{AI105-0290-1\} \{AI12-0096-1\} \{AI12-0449-1\}\) If an Accessibility_Check fails, Program_Error is raised. Any other check associated with a conversion raises Constraint_Error if it fails.

Conversion to a type is the same as conversion to an unconstrained subtype of the type.

Reason: This definition is needed because the semantics of various constructs involves converting to a type, whereas an explicit type_conversion actually converts to a subtype. For example, the evaluation of a range is defined to convert the values of the expressions to the type of the range.

Ramification: A conversion to a scalar type, or, equivalently, to an unconstrained scalar subtype, can raise Constraint_Error if the value is outside the base range of the type.

- \(\{AI12-0027-1\} \{AI12-0226-1\}\) Evaluation of a value conversion of an object of composite type either creates a new anonymous object (similar to the object created by the evaluation of an aggregate or a function call) or yields a new view of the operand object without creating a new object:

  - If the target type is a by-reference type and there is a type that is an ancestor of both the target type and the operand type then no new object is created;
  - If the target type is an array type having aliased components and the operand type is an array type having unaliased components, then a new object is created;
  - \(\{AI12-0226-1\}\) If the target type is an elementary type, then a new object is created;
  - Otherwise, it is unspecified whether a new object is created.

Reason: This makes a difference in the case of converting from an array type with unaliased components to one with aliased components if the element type has a controlled part.

Implementation Note: \(\{AI12-0226-1\}\) The temporary object need not be materialized in most cases; it should be handled like the return object of a predefined operator. Generally, whether the object exists can only be detected if it is renamed (unless a part of the type is controlled).

Discussion: \(\{AI12-0226-1\}\) This set of rules does not apply in those cases where the operand is not an object (such as a value conversion of a named number); in such cases, the result isn't an object, so it isn't necessary to describe what that means. The rules cover all value conversions of composite types (since there aren't any values of composite types separate from objects).
NOTE 1 In addition to explicit type conversions, type conversions are performed implicitly in situations where the expected type and the actual type of a construct differ, as is permitted by the type resolution rules (see 8.6). For example, an integer literal is of the type `universal_integer`, and is implicitly converted when assigned to a target of some specific integer type. Similarly, an actual parameter of a specific tagged type is implicitly converted when the corresponding formal parameter is of a class-wide type.

Even when the expected and actual types are the same, implicit subtype conversions are performed to adjust the array bounds (if any) of an operand to match the desired target subtype, or to raise Constraint_Error if the (possibly adjusted) value does not satisfy the constraints of the target subtype.

NOTE 2 {AI95-00230-01} A ramification of the overload resolution rules is that the operand of an (explicit) type_conversion cannot be the literal `null`, an allocator, an aggregate, a string_literal, a character_literal, or an attribute_reference for an Access or Unchecked_Access attribute. Similarly, such an expression enclosed by parentheses is not allowed. A qualified_expression (see 4.7) can be used instead of such a type_conversion.

NOTE 3 The constraint of the target subtype has no effect for a type_conversion of an elementary type passed as an out parameter. Hence, it is recommended that the first subtype be specified as the target to minimize confusion (a similar recommendation applies to renaming and generic formal in out objects).

Examples

Examples of numeric type conversion:

```
Real(2*J)     -- value is converted to floating point
Integer(1.6)  -- value is 2
Integer(-0.4) -- value is 0
```

Example of conversion between derived types:

```
type A_Form is new B_Form;
X : A_Form;
Y : B_Form;
X := A_Form(Y);  
Y := B_Form(X);  -- the reverse conversion
```

Examples of conversions between array types:

```
type Sequence is array (Integer range <>) of Integer;
subtype Dozen is Sequence(1 .. 12);
Ledger : array(1 .. 100) of Integer;
Sequence(Ledger) -- bounds are those of Ledger
Sequence(Ledger(31 .. 42)) -- bounds are 31 and 42
Dozen(Ledger(31 .. 42))  -- bounds are those of Dozen
```

Incompatibilities With Ada 83

A character_literal is not allowed as the operand of a type_conversion, since there are now two character types in package Standard.

The component subtypes have to statically match in an array conversion, rather than being checked for matching constraints at run time.

Because sliding of array bounds is now provided for operations where it was not in Ada 83, programs that used to raise Constraint_Error might now continue executing and produce a reasonable result. This is likely to fix more bugs than it creates.

Extensions to Ada 83

A type_conversion is considered the name of an object in certain circumstances (such as a type_conversion is called a view conversion). In particular, as in Ada 83, a type_conversion can appear as an in out or out actual parameter. In addition, if the target type is tagged and the operand is the name of an object, then so is the type_conversion, and it can be used as the prefix to a selected_component, in an object_renaming_declaration, etc.

We no longer require type-mark conformance between a parameter of the form of a type conversion, and the corresponding formal parameter. This had caused some problems for inherited subprograms (since there isn't really a type-mark for converted formals), as well as for renamings, formal subprograms, etc. See AI83-00245, AI83-00318, AI83-00547.

We now specify “deterministic” rounding from real to integer types when the value of the operand is exactly between two integers (rounding is away from zero in this case).
“Sliding” of array bounds (which is part of conversion to an array subtype) is performed in more cases in Ada 95 than in Ada 83. Sliding is not performed on the operand of a membership test, nor on the operand of a qualified expression. It wouldn't make sense on a membership test, and we wish to retain a connection between subtype membership and subtype qualification. In general, a subtype membership test returns True if and only if a corresponding subtype qualification succeeds without raising an exception. Other operations that take arrays perform sliding.

**Wording Changes from Ada 83**

We no longer explicitly list the kinds of things that are not allowed as the operand of a type_conversion, except in a NOTE.

\{AI05-0299-1\} The rules in this subclause subsume the rules for "parameters of the form of a type conversion", and have been generalized to cover the use of a type conversion as a name.

**Incompatibilities With Ada 95**

\{AI95-00246-01\} **Amendment Correction:** Conversions between unrelated array types that are limited or (for view conversions) might be by-reference types are now illegal. The representations of two such arrays may differ, making the conversions impossible. We make the check here, because legality should not be based on representation properties. Such conversions are likely to be rare, anyway. There is a potential that this change would make a working program illegal (if the types have the same representation).

\{AI95-00363-01\} If a discriminated full type has a partial view (private type) that is constrained, we do not allow conversion between access-to-unconstrained and access-to-constrained subtypes designating the type. Ada 95 allowed this conversion and the declaration of various access subtypes, requiring that the designated object be constrained and thus making details of the implementation of the private type visible to the client of the private type. See 4.8 for more on this topic.

**Extensions to Ada 95**

\{AI95-00230-01\} Conversion rules for universal access were defined. These allow the use of anonymous access values in equality tests (see 4.5.2), and also allow the use of null in type conversions and other contexts that do not provide a single expected type.

\{AI95-00384-01\} A type conversion from an access-to-discriminated and unconstrained object to an access-to-discriminated and constrained one is allowed. Ada 95 only allowed the reverse conversion, which was weird and asymmetric. Of course, a constraint check will be performed for this conversion.

**Wording Changes from Ada 95**

\{8652/0017\} \{AI95-00184-01\} **Corrigendum:** Wording was added to ensure that view conversions are constrained, and that a tagged view conversion has a tagged object. Both rules are needed to avoid having a way to change the discriminants of a constrained object.

\{8652/0008\} \{AI95-00168-01\} **Corrigendum:** Wording was added to ensure that the aliased status of array components cannot change in a view conversion. This rule was needed to avoid having a way to change the discriminants of an aliased object. This rule was repealed later, as Ada 2005 allows changing the discriminants of an aliased object.

\{AI95-00231-01\} Wording was added to check subtypes that exclude null (see 3.10).

\{AI95-00231-01\} The organization of the legality rules was changed, both to make it clearer, and to eliminate an unintentional incompatibility with Ada 83. The old organization prevented type conversions between some types that were related by derivation (which Ada 83 always allowed).

\{AI95-00330-01\} \{AI05-0005-1\} **Clarified that an untagged type conversion appearing as a generic actual parameter for a generic in out formal parameter is not a view conversion (and thus is illegal). This confirms the ACATS tests, so all implementations already follow this interpretation.**

\{AI95-00363-01\} Rules added by the Corrigendum to eliminate problems with discriminants of aliased components changing were removed, as we now generally allow discriminants of aliased components to be changed.

\{AI95-00392-01\} **Accessibility checks on conversions involving types with anonymous access components were added. These components have the level of the type, and conversions can be between types at different levels, which could cause dangling access values in the absence of such checks.**

**Inconsistencies With Ada 2005**

\{AI05-0148-1\} A stand-alone object of an anonymous access-to-object type now has dynamic accessibility. Normally, this will make programs legal that were illegal in Ada 2005. However, it is possible that a program that previously
raised Program_Error now will not. It is very unlikely that an existing program intentionally depends on the exception being raised; the change is more likely to fix bugs than introduce them.

Wording Changes from Ada 2005

\{AI05-0115-1\} Correction: Clarified that a root numeric type is not considered a common ancestor for a conversion.
\{AI05-0153-3\} \{AI05-0290-1\} Added rules so that predicate aspects (see 3.2.4) are enforced on subtype conversion.

Inconsistencies With Ada 2012

\{AI12-0333-1\} \{AI12-0432-1\} Correction: Predicate checks are no longer made on any out parameters before a call (they're still made when the call returns). This was already true for elementary out parameters. If a program depends on a predicate check failing on an inbound out composite parameter, it will get an incorrect result. Similarly, predicate checks are no longer made on the view conversion of a target of an assignment statement. Both of these cases seem quite unlikely, as programs (outside of ACATS tests) that depend on the failure of checks are very rare, and the predicate might be checking uninitialized components (making check failure unreliable).

Incompatibilities With Ada 2012

\{AI12-0095-1\} \{AI12-0005-1\} Corrigendum: Because of a rule added in 12.5.1, the checks for the legality of an access type conversion in a generic body were strengthened to use an assume-the-worst rule. This case is rather unlikely because a formal private or derived type with discriminants is required along with a conversion between two access types whose designated types don't statically match, and any such programs were at risk having objects disappear while valid access values still pointed at them.

Wording Changes from Ada 2012

\{AI12-0027-1\} Corrigendum: Moved the generic boilerplate so that it covers all Legality Rules in this subclause. This was always intended, but it is not expected to change anything other than conversions between unrelated arrays.
\{AI12-0027-1\} Corrigendum: Added a formal definition of the copy potentially created by a value conversion of a composite type, so properties like finalization and accessibility are properly defined. This model was always intended and expected (else 13.6 would not work), but it was not previously formally defined.
\{AI12-0071-1\} Corrigendum: Updated wording of type conversions to use the new term "satisfies the predicates" (see 3.2.4).
\{AI12-0074-1\} Corrigendum: Clarified the wording describing the effect of view conversions of out parameters such that it is clear that the detailed effect is defined in 6.4.1, not here.
\{AI12-0096-1\} Corrigendum: Updated wording of type conversions so that the exception raise or other effect of a failed predicate check is as defined in 3.2.4; we don't want to repeat those rules here. This doesn't change the behavior for predicate checks possible in original Ada 2012, only ones using the new aspect Predicate Failure.
\{AI12-0064-2\} \{AI12-0380-1\} Required Global (see 6.1.2) and Nonblocking (see 9.5) aspect matching for access-to-subprogram conversions.
\{AI12-0226-1\} Described the objects associated with value conversions of elementary types. This is necessary to support an extension documented in 3.3.
\{AI12-0392-1\} Correction: Eliminated the requirement that the operand of a view conversion be a simple name. The requirement could cause unintended consequences in the case where the operand of a type conversion represents an object but is more complex than a simple name (such as a qualified_expression or conditional_expression).

4.7 Qualified Expressions

[A qualified_expression is used to state explicitly the type, and to verify the subtype, of an operand that is either an expression or an aggregate.]

Syntax

qualified_expression ::= subtype_mark'(expression) | subtype_mark'aggregate
Name Resolution Rules

3/5 {AII2-0325-1} The expected type for the operand (the expression or aggregate) shall resolve to be of the type determined by the subtype_mark, or a universal type that covers it. Furthermore, the operand shall resolve to be either the specified expected type or a universal type that covers it.

Reason: {AII2-0325-1} The first sentence defines the expected type for rules that assume one is defined. The second sentence prevents the use of the various implicit conversions that are usually allowed for expected types (except the one for numeric literals). The intent is that a qualified expression is similar to an assertion about the subtype of the operand, and thus implicit conversions would interfere with that intent.

Static Semantics

3.1/3 {AI05-0003-1} If the operand of a qualified_expression denotes an object, the qualified_expression denotes a constant view of that object. The nominal subtype of a qualified_expression is the subtype denoted by the subtype_mark.

Proof: {AI05-0003-1} This is stated in 3.3.

Dynamic Semantics

4/5 {AII2-0100-1} {AII2-0449-1} The evaluation of a qualified_expression evaluates the operand (and if of a universal type, converts it to the type determined by the subtype_mark) and checks that its value belongs to the subtype denoted by the subtype_mark. The exception Constraint_Error is raised if this check fails. Furthermore, if predicate checks are enabled for the subtype denoted by the subtype_mark, a check is performed as defined in 3.2.4, subclause 3.2.4, “Subtype Predicates,” that the value satisfies the predicates of the subtype.

Ramification: This is one of the few contexts in Ada 95 where implicit subtype conversion is not performed prior to a constraint check, and hence no “sliding” of array bounds is provided.

4.a/4 {AII2-0100-1} The effect of a failed predicate check is as defined in 3.2.4, such a check could raise any exception, not just Constraint_Error or Assertion_Error.

Reason: Implicit subtype conversion is not provided because a qualified_expression with a constrained target subtype is essentially an assertion about the subtype of the operand, rather than a request for conversion. An explicit type_conversion can be used rather than a qualified_expression if subtype conversion is desired.

4.c/4 {AII2-0100-1} We do a predicate check here so that a qualified_expression never allows something that the equivalent type_conversion would not allow.

5/5 NOTE {AII2-0440-1} When a given context does not uniquely identify an expected type, a qualified_expression can be used to disambiguate it. In particular, if an overloaded name or aggregate is passed to an overloaded subprogram, it might be necessary to qualify the operand to resolve its type.

Examples of disambiguating expressions using qualification:

```ada
type Mask is (Fix, Dec, Exp, Signif);
type Code is (Fix, Cla, Dec, Tnz, Sub);
Print (Mask'((Dec))); -- Dec is of type Mask
Print (Code'((Dec))); -- Dec is of type Code
```

9/5 {AI12-0442-1} for J in Code'((Fix)) .. Code'((Dec)) loop ... -- qualification is necessary
for J in Code range Fix .. Dec loop ... -- qualification unnecessary
for J in Code'((Fix)) .. Dec loop ... -- qualification unnecessary for Dec

10 Dozen'1 | 3 | 5 | 7 => 2, others => 0) -- see 4.6

Wording Changes from Ada 2005

10.a/3 {AI05-0003-1} Added a definition of the nominal subtype of a qualified_expression.
Inconsistencies With Ada 2012

Corrigendum: A qualified_expression now performs a predicate check for the named subtype (if it is enabled). Original Ada 2012 did not include that check (an omission). While this is formally inconsistent (an exception could be raised when none would be raised by original Ada 2012), cases where this scenario arises could be the case are likely to be rare (the qualified expression would have to have a stricter subtype than the following usage) and the check is more likely to detect bugs than be unexpected.

Wording Changes from Ada 2012

Reworded the resolution rule so that the operand of a qualified_expression has an expected type. This eliminates an annoying inconsistency in the language definition.

4.8 Allocators

[The evaluation of an allocator creates an object and yields an access value that designates the object. ]

Syntax

new [subpool_specification] subtype_indication
| new [subpool_specification] qualified_expression

subpool_specification ::= (subpool_handle_name)

For an allocator with a subtype_indication, the subtype_indication shall not specify a null_exclusion.

Reason: Such an uninitialized allocator would necessarily raise Constraint_Error, as the default value is null. Also note that the syntax does not allow a null_exclusion in an initialized allocator, so it makes sense to make the uninitialized case illegal as well.

Name Resolution Rules

The expected type for an allocator shall be a single access-to-object type with whose designated type D such that either D covers the type determined by the subtype_mark of the subtype_indication or qualified_expression, or the expected type is anonymous and the determined type is D'Class. A subpool_handle_name is expected to be of any type descended from Subpool_Handle, which is the type used to identify a subpool, declared in package System.Storage_Pools.Subpools (see 13.11.4).

Discussion: See 8.6, “The Context of Overload Resolution” for the meaning of “shall be a single ... type whose ...”.

Ramification: For example, new S'Class ... (with no initialization expression) is illegal, but new S'Class(X) ... is legal, and takes its tag and constraints from the initial value X. (Note that the former case cannot have a constraint.)

Legality Rules

An initialized allocator is an allocator with a qualified_expression. An uninitialized allocator is one with a subtype_indication. In the subtype_indication of an uninitialized allocator, a constraint is permitted only if the subtype_mark denotes an [unconstrained] composite subtype; if there is no constraint, then the subtype_mark shall denote a definite subtype.

Ramification: For example, ... new S'Class ... (with no initialization expression) is illegal, but ... new S'Class(X) ... is legal, and takes its tag and constraints from the initial value X. (Note that the former case cannot have a constraint.)

If the type of the allocator is an access-to-constant type, the allocator shall be an initialized allocator. If the designated type is limited, the allocator shall be an uninitialized allocator.

This paragraph was deleted.

Ramification: For an access to constant type whose designated type is limited, allocators are illegal. The Access attribute is legal for such a type, however.
5.1/3 {AI05-0111-3} If a subpool specification is given, the type of the storage pool of the access type shall be a descendant of Root_Storage_Pool_With_Subpools.

5.2/3 {AI95-00344-01} If the designated type of the type of the allocator is class-wide, the accessibility level of the type determined by the subtype indication or qualified expression shall not be statically deeper than that of the type of the allocator.

Reason: This prevents the allocated object from outliving its type.

5.3/3 {AI95-00416-01} An allocator shall not be of an access type for which the Storage_Size has been specified by a static expression with value zero or is defined by the language to be zero. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit. This rule does not apply in the body of a generic unit or within a body declared within the declarative region of a generic unit, if the type of the allocator is a descendant of a formal access type declared within the formal part of the generic unit.

Reason: This prevents the allocated object from outliving its discriminants.

5.4/3 {AI95-00366-01} An allocator shall not be of an access type from which the Storage_Size has been specified by a static expression with value zero or is defined by the language to be zero. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit. This rule does not apply in the body of a generic unit or within a body declared within the declarative region of a generic unit, if the type of the allocator is a descendant of a formal access type declared within the formal part of the generic unit.

Reason: An allocator for an access type that has Storage_Size specified to be zero is required to raise Storage_Error anyway. It's better to detect the error at compile-time, as the allocator might be executed infrequently. This also simplifies the rules for Pure units, where we do not want to allow any allocators for library-level access types, as they would represent state.

5.5/3 {AI05-0157-1} We don't need a special rule to cover generic forms (unlike many other similar Legality Rules). There are only two cases of interest. For formal access types, the Storage_Size property is not known in the generic, and surely isn't static, so this Legality Rule can never apply. For a formal derived type, this Legality Rule can only be triggered by a parent type having one of the appropriate properties. But Storage_Size can never be specified for a derived access type, so it always has the same value for all child types; additionally, a type derived from a remote access type (which has Storage_Size defined to be zero) is also a remote access type. That means that any actual that would match the formal derived type necessarily has the same Storage_Size properties, so it is harmless (and preferable) to check them in the body - they are always known in that case. For other formal types, allocators are not allowed, so we don't need to consider them. So we don't need an assume-the-best rule here. The last sentence covers the case of children of generics, and formal access types of formal packages of the generic unit.

5.6/3 {AI05-0052-1} If the designated type of the type of the allocator is limited, then the allocator shall not be used to define the value of an access discriminant, unless the discriminated type is immutably limited (see 7.5).

Reason: Because coextensions work very much like parts, we don't want users creating limited coextensions for nonlimited types. This would be similar to extending a nonlimited type with a limited component. We check this on the allocator. Note that there is an asymmetry in what types are considered limited; this is required to preserve privacy. We have to assume that the designated type might be limited as soon as we see a limited partial view, but we want to ensure that the containing object is of a type that is always limited.

5.6/3 In addition to the places where Legality Rules normally apply (see 12.3), these rules apply also in the private part of an instance of a generic unit.

Discussion: This applies to all of the Legality Rules of this subclause.

Static Semantics

6/3 {AI95-00363-01} If the designated type of the type of the allocator is elementary, then the subtype of the created object is the designated subtype. If the designated type is composite, then the subtype of the created object is the designated subtype when the designated subtype is constrained or there is an ancestor of the designated type that has a constrained partial view of the designated type that is constrained; otherwise, the created object is constrained, if the designated subtype is constrained, then it...
provides the constraint of the created object; otherwise, the object is constrained by its initial value [(even if the designated subtype is unconstrained with defaults)].

Discussion: See AI83-00331.

Reason: {AI95-00363-01} All objects created by an allocator are aliased, and most aliased composite objects need to be constrained so that access subtypes work reasonably. Problematic access subtypes are prohibited for types with a constrained partial view.

Discussion: {AI95-00363-01} If there is a constrained partial view of the type, this allows the objects to be unconstrained. This eliminates privacy breaking (we don't want the objects to act differently simply because they're allocated). Such a created object is effectively constrained by its initial value if the access type is an access-to-constant type, or the designated type is limited (in all views), but we don't need to state that here. It is implicit in other rules.

Note, however, that a value of an access-to-constant type can designate a variable object via 'Access or conversion, and the variable object might be assigned by some other access path, and that assignment might alter the discriminants.

Dynamic Semantics

{AI95-00373-01} For the evaluation of an initialized allocator, the elaboration of the subtype indication or the evaluation of the qualified expression is performed first. An object of the designated type is created and the value of the qualified expression is converted to the designated subtype and assigned to the object.

Ramification: The conversion might raise Constraint_Error.

For the evaluation of an uninitialized allocator, the elaboration of the subtype indication is performed first. Then:

• {AI95-00373-01} If the designated type is elementary, an object of the designated subtype is created and any implicit initial value is assigned;

• {8652/0002} {AI95-00171-01} {AI95-00373-01} If the designated type is composite, an object of the designated type is created with tag, if any, determined by the subtype_mark of the subtype indication. This object is then initialized by default (see 3.3.1) using: any per-object constraints on subcomponents are elaborated (see 3.8) and any implicit initial values for the subcomponents of the object are obtained as determined by the subtype indication to determine its nominal subtype and assigned to the corresponding subcomponents. A check is made that the value of the object belongs to the designated subtype. Constraint_Error is raised if this check fails. This check and the initialization of the object are performed in an arbitrary order.

Discussion: AI83-00150.

{AI95-00344-01} {AI95-00416-01} {AI05-0024-1} {AI05-0051-1} {AI05-0234-1} For any allocator, if the designated type of the type of the allocator is class-wide, then a check is made that the masteraccessibility level of the type determined by the subtype indication, or by the tag of the value of the qualified expression, includes the elaboration's not deeper than that of the type of the allocator. If any part of the subtype determined by the subtype indication or qualified expression of the allocator (or by the tag of the value if the type of the qualified expression is class-wide) has one or more unconstrained access discriminants, then a check is made that the accessibility level of the anonymous access type of each access discriminant is not deeper than that of the type of the allocator. Program_Error is raised if either such check fails.

Reason: {AI95-00344-01} {AI05-0024-1} The masteraccessibility check on class-wide types prevents the allocated object from outliving its type. We need the run-time check in instance bodies, or when the type of the qualified expression is class-wide (other cases are statically detected).

{AI05-0024-1} We can’t use the normal accessibility level “deeper than” check here because we may have “incomparable” levels if the appropriate master and the type declaration belong to two different tasks. This can happen when checking the master of the tag for an allocator initialized by a parameter passed in to an accept statement, if the type of the allocator is an access type declared in the enclosing task body. For example:
task body TT is
  type Acc_TC is access T'Class;
  P : Acc_TC;
begin
  accept E(X : T'Class) do
    P := new T'Class'(X);
    -- Master check on tag of X.
    -- Can't use "accessibility levels" since they might be incomparable.
    -- Must revert to checking that the master of the type identified by
    -- X'tag includes the elaboration of Acc_TC, so it is sure to outlive it.
  end E;
{AI95-00416-01} The accessibility check on access discriminants prevents the allocated object from outliving its discriminants.
{AI95-00280-01} If the object to be created by an allocator has a controlled or protected part, and the finalization of the collection of the type of the allocator (see 7.6.1) has started, Program_Error is raised.  

  Reason: If the object has a controlled or protected part, its finalization is likely to be nontrivial. If the allocation was allowed, we could not know whether the finalization would actually be performed. That would be dangerous to otherwise safe abstractions, so we mandate a check here. On the other hand, if the finalization of the object will be trivial, we do not require (but allow) the check, as no real harm could come from late allocation.

  Discussion: This check can only fail if an allocator is evaluated in code reached from a Finalize routine for a type declared in the same master. That's highly unlikely; Finalize routines are much more likely to be deallocating objects than allocating them.

{AI95-00280-01} If the object to be created by an allocator contains any tasks, and the master of the type of the allocator is completed, and all of the dependent tasks of the master are terminated (see 9.3), then Program_Error is raised.

  Reason: A task created after waiting for tasks has finished could depend on freed data structures, and certainly would never be awaited.

{AI05-0111-3} If the allocator includes a subpool handle name, Constraint_Error is raised if the subpool handle is null. Program_Error is raised if the subpool does not belong (see 13.11.4) to the storage pool of the access type of the allocator.

  Implementation Note: This can be implemented by comparing the result of Pool_of_Subpool to a reference to the storage pool object. Pool_of_Subpool's parameter is not null, so the check for null falls out naturally.

  Reason: This detects cases where the subpool belongs to another pool, or to no pool at all. This includes detecting dangling subpool handles so long as the subpool object (the object designated by the handle) still exists. (If the subpool object has been deallocated, execution is erroneous; it is likely that this check will still detect the problem, but there cannot be a guarantee.)

If the created object contains any tasks, they are activated (see 9.2).] Finally, an access value that designates the created object is returned.

Bounded (Run-Time) Errors

{AI95-00280-01} It is a bounded error if the finalization of the collection of the type (see 7.6.1) of the allocator has started. If the error is detected, Program_Error is raised. Otherwise, the allocation proceeds normally.

  Discussion: This check is required in some cases; see above.

NOTE 1 Allocators cannot create objects of an abstract type. See 3.9.3.

NOTE 2 If any part of the created object is controlled, the initialization includes calls on corresponding Initialize or Adjust procedures. See 7.6.

NOTE 3 As explained in 13.11, “Storage Management”, the storage for an object allocated by an allocator comes from a storage pool (possibly user defined). The exception Storage_Error is raised by an allocator if there is not enough storage. Instances of Unchecked_Deallocation cannot be used to explicitly reclaim storage.

NOTE 4 Implementations can, if desired, are permitted, but not required, to provide garbage collection (see 13.11.3).
Ramification: Note that in an allocator, the exception Constraint_Error can be raised by the evaluation of the qualified_expression, by the elaboration of the subtype_indication, or by the initialization.

Discussion: By default, the implementation provides the storage pool. The user may exercise more control over storage management by associating a user-defined pool with an access type.

Examples of allocators:

```
new Cell'(0, null, null)        -- initialized explicitly, see 3.10.1
new Cell'(Value => 0, Succ => null, Pred => null)  -- initialized explicitly
new Cell                       -- not initialized
new Matrix(1 .. 10, 1 .. 20)   -- the bounds only are given
new Matrix'(1 .. 10 => (1 .. 20 => 0.0))   -- initialized explicitly
new Buffer(100)                -- the discriminant only is given
new Buffer'(Size => 80, Pos => 0, Value => (1 .. 80 => 'A'))  -- initialized explicitly
Expr_Ptr'(new Literal)         -- allocator for access-to-class-wide type, see 3.9.1
Expr_Ptr'(new Literal'(Expression with 3.5)) -- initialized explicitly
```

Incompatibilities With Ada 83

The subtype_indication of an uninitialized allocator may not have an explicit constraint if the designated type is an access type. In Ada 83, this was permitted even though the constraint had no effect on the subtype of the created object.

Extensions to Ada 83

Allocators creating objects of type T are now overloaded on access types designating TClass and all class-wide types that cover T.

Implicit array subtype conversion (sliding) is now performed as part of an initialized allocator.

Wording Changes from Ada 83

We have used a new organization, inspired by the ACID document, that makes it clearer what is the subtype of the created object, and what subtype conversions take place.

Discussion of storage management issues, such as garbage collection and the raising of Storage_Error, has been moved to 13.11, “Storage Management”.

Inconsistencies With Ada 95

��1AI95-00363-01ariatype has a constrained partial view, the allocated object can be unconstrained. This might cause the object to take up a different amount of memory, and might cause the operations to work where they previously would have raised Constraint_Error. It's unlikely that the latter would actually matter in a real program (Constraint_Error usually indicates a bug that would be fixed, not left in a program.) The former might cause Storage_Error to be raised at a different time than in an Ada 95 program.

Incompatibilities With Ada 95

 Atatürk An allocator for an access type that has Storage_Size specified to be zero is now illegal. Ada 95 allowed the allocator, but it had to raise Storage_Error if executed. The primary impact of this change should be to detect bugs.

Extensions to Ada 95

Corrigendum: An allocator can be a controlling parameter of a dispatching call. This was an oversight in Ada 95.

Corrigendum: Initialized allocators are allowed when the designated type is limited.

Wording Changes from Ada 95

Corrigendum: Clarified the elaboration of per-object constraints for an uninitialized allocator.
4.9 Static Expressions and Static Subtypes

Certain expressions of a scalar or string type are defined to be static. Similarly, certain discrete ranges are defined to be static, and certain scalar and string subtypes are defined to be static subtypes. \([\text{Static} \text{ means }\text{determinable at compile time, using the declared properties or values of the program entities.}]\)

**Discussion:** As opposed to more elaborate data flow analysis, etc.

**Language Design Principles**

For an expression to be static, it has to be calculable at compile time.

Only scalar and string expressions are static.

To be static, an expression cannot have any nonscalar, nonstring subexpressions (though it can have nonscalar constituent names). A static scalar expression cannot have any nonscalar subexpressions. There is one exception — a membership test for a string subtype can be static, and the result is scalar, even though a subexpression is nonscalar.

The rules for evaluating static expressions are designed to maximize portability of static calculations.

**Reason:** \([\text{AI12-0201-1}]\) We support static string expressions so that, for example, the aspect definition for a Link_Name aspect can contain a concatenation. We don't support static aggregates (even for string types) or non-string static nonscalar types; we're trying to keep it cheap and simple (from the implementer's viewpoint).

**Static Semantics**

A static expression is [a scalar or string expression that is] one of the following:

- \([\text{AI12-0249-1}]\) a numeric_literal of a numeric type;

**Ramification:** \([\text{AI12-0249-1}]\) A numeric_literal of a numeric type is always a static expression, even if its expected type is not that of a static subtype. However, if its value is explicitly converted to, or qualified by, a nonstatic subtype,
the resulting expression is nonstatic. Non-numeric types can have numeric literals if aspect Integer_Literal or Real_Literal is used; these are never static.

- a string_literal of a static string subtype;
  
  **Ramification:** That is, the constrained subtype defined by the index range of the string is static. Note that elementary values don't generally have subtypes, while composite values do (since the bounds or discriminants are inherent in the value).

- `{AI12-0394-1}` a name that denotes the declaration of a named number or a static constant;

- `{AI12-0394-1}` a name that denotes a named number, and that is interpreted as a value of a numeric type;
  
  **To be honest:** `{AI12-0394-1}` This is referring the resolution of the named number and not the Static Semantics (for which all named numbers are values of a universal numeric type). The word “interpreted” is intended to make the distinction.

  **Ramification:** Note that enumeration literals are covered by the function_call case.

- a function_call whose function_name or function_prefix statically denotes a static function, and whose actual parameters, if any (whether given explicitly or by default), are all static expressions;

  **Ramification:** This includes uses of operators that are equivalent to function_calls.

- an attribute_reference that denotes a scalar value, and whose prefix denotes a static scalar subtype;

  **Ramification:** Note that this does not include the case of an attribute that is a function; a reference to such an attribute is not even an expression. See above for function calls.

  An implementation may define the staticness and other properties of implementation-defined attributes.

- `{AI12-0368-1}` an attribute_reference whose prefix statically names a statically constrained array object or array subtype, and whose attribute_designator is First, Last, or Length, with an optional dimension;

- `{AI12-0064-2}` `{AI22-0018-1}` an attribute_reference whose prefix denotes a non-generic entity that is not declared in a generic unit, and whose attribute_designator is Nonblocking;

- `{AI12-0201-1}` a type_conversion whose subtype_mark denotes a static [(scalar or string)] scalar subtype, and whose operand is a static expression;

- a qualified_expression whose subtype_mark denotes a static [(scalar or string)] subtype, and whose operand is a static expression;

  **Ramification:** This rules out the subtype_mark'aggregate case.

  **Reason:** Adding qualification to an expression shouldn't make it nonstatic, even for strings.

- `{AI05-0158-1}` `{AI05-0269-1}` `{AI12-0039-1}` a membership test whose tested simple_expression is a static expression, and whose membership_choice_list contains only of membership choices that are either static choice simple_expression or subtype marks that denote range is a static range or whose subtype_mark denotes a static [(scalar or string)] subtype;

  **Reason:** Clearly, we should allow membership tests in exactly the same cases where we allow qualified_expressions.

- a short-circuit control form both of whose relations are static expressions;

- `{AI05-0147-1}` `{AI05-0188-1}` a conditional_expression all of whose conditions, selecting_expressions, and dependent_expressions are static expressions;

- `{AI12-0368-1}` a declare_expression whose body_expression is static and each of whose declarations, if any, is either the declaration of a static constant or is an object renaming_declaration with an object_name that statically names the renamed object;

- a static expression enclosed in parentheses.

**Discussion:** Informally, we talk about a static value. When we do, we mean a value specified by a static expression.
Ramification: The language requires a static expression in a number_declaration, a numeric type definition, a discrete_choice (sometimes), certain representation items, and a number of other contexts.

A name statically denotes an entity if it denotes the entity and:

- It is a direct_name, expanded name, or character_literal, and it denotes a declaration other than a renaming_declaration; or
- It is an attribute_reference whose prefix statically denotes some entity; or
- \{AI12-0322-1\} It is a target_name (see 5.2.1) in an assignment_statement whose variable_name statically denotes some entity; or
- It denotes a renaming_declaration with a name that statically denotes the renamed entity.

Ramification: Selected components that are not expanded names and indexed_components do not statically denote things.

\[\{AI12-0368-1\} \text{ A name statically names an object if it:} \]

- statically denotes the declaration of an object [(possibly through one or more renames)];

Proof: Follows from the definition of statically denotes.

\[\{AI12-0368-1\} \text{ is a selected component whose prefix statically names an object, there is no implicit dereference of the prefix, and the selector_name does not denote a component_declaration occurring within a variant_part; or} \]

Reason: We disallow components in a variant_part so that no discriminant checks are needed to evaluate the selected_component. Note that other kinds of discriminant-dependent components do not need any checks on access (only when they are changed).

\[\{AI12-0368-1\} \text{ is an indexed_component whose prefix statically names an object, there is no implicit dereference of the prefix, the object is statically constrained, and the index expressions of the object are static and have values that are within the range of the index constraint.} \]

\[\{AI12-0368-1\} \text{ For an entity other than an object, a name statically names an entity if the name statically denotes the entity.} \]

A static function is one of the following:

- a predefined operator whose parameter and result types are all scalar types none of which are descendants of formal scalar types;
- a predefined relational operator whose parameters are of a string type that is not a descendant of a formal array type;
- a predefined concatenation operator whose result type is a string type that is not a descendant of a formal array type;
- a shifting or rotating function associated with a modular type declared in package Interfaces (see B.2);
- an enumeration literal;
- a static expression function (see 6.8);

In any case, a generic formal subprogram is not a static function.
A static constant is a constant view declared by a full constant declaration or an object_renaming_declaration with a static nominal subtype, having a value defined by a static scalar expression or by a static string expression, and which satisfies any constraint or predicate that applies to the nominal subtype—whose value has a length not exceeding the maximum length of a string_literal in the implementation.

Ramification: A deferred constant is not static; the view introduced by the corresponding full constant declaration can be static.

This paragraph was deleted. Reason: The reason for restricting the length of static string constants is so that compilers don't have to store giant strings in their symbol tables. Since most string constants will be initialized from string_literals, the length limit seems pretty natural. The reason for avoiding nonstring types is also to save symbol table space. We're trying to keep it cheap and simple (from the implementer's viewpoint), while still allowing, for example, the aspect_definition for a Link_Name aspect_link name of a pragma_Import to contain a concatenation.

This paragraph was deleted. Reason: The length we're talking about is the maximum number of characters in the value represented by a string_literal, not the number of characters in the source representation; the quotes don't count.

A static range is a range whose bounds are static expressions, [or a range_attribute_reference that is equivalent to such a range.] A static discrete_range is one that is a static range or is a subtype_indication that defines a static scalar subtype. The base range of a scalar type is a static range, unless the type is a descendant of a formal scalar type.

A static subtype is either a static scalar subtype or a static string subtype. A static scalar subtype is an unconstrained scalar subtype whose type is not a descendant of a formal scalar type, or a constrained scalar subtype formed by imposing a compatible static constraint on a static scalar subtype. A static string subtype is an unconstrained string subtype whose index subtype and component subtype are static (and whose type is not a descendant of a formal array type), or a constrained string subtype formed by imposing a compatible static constraint on a static string subtype. In any case, the subtype of a generic formal object of mode in out, and the result subtype of a generic formal function, are not static. Also, a subtype is not static if any Dynamic_Predicate specifications apply to it.

Ramification: String subtypes are the only composite subtypes that can be static.

Reason: The part about generic formal objects of mode in out is necessary because the subtype of the formal is not required to have anything to do with the subtype of the actual. For example:

```
subtype Int10 is Integer range 1..10;
generic
  F: in out Int10;
procedure G;
procedure G is
begin
  case F is
    when 1..10 => null;  -- Illegal!
  end case;
end G;
X: Integer range 1..20;
procedure I is new G(F => X); -- OK.
```

The case_statement is illegal, because the subtype of F is not static, so the choices have to cover all values of Integer, not just those in the range 1..10. A similar issue arises for generic formal functions, now that function calls are object names.

The different kinds of static constraint are defined as follows:

- A null constraint is always static;
- A scalar constraint is static if it has no range_constraint, or one with a static range;
- An index constraint is static if each discrete_range is static, and each index subtype of the corresponding array type is static;
A discriminant constraint is static if each expression of the constraint is static, and the subtype of each discriminant is static.

In any case, the constraint of the first subtype of a scalar formal type is neither static nor null.

A subtype is statically constrained if it is constrained, and its constraint is static. An object is statically constrained if its nominal subtype is statically constrained, or if it is a static string constant.

Legality Rules

An expression is statically unevaluated if it is part of:

- the right operand of a static short-circuit control form whose value is determined by its left operand; or
- a dependent expression of an if expression whose associated condition is static and equals False; or
- a condition or dependent expression of an if expression where the condition corresponding to at least one preceding dependent expression of the if expression is static and equals True; or
- a dependent expression of an if expression whose selecting expression is static and whose value is not covered by the corresponding discrete choice list; or
- a choice simple expression choice expression (or a simple expression of a range that occurs as a membership choice of a membership choice list) of a static membership test that is preceded in the enclosing membership choice list by another item whose individual membership test (see 4.5.2) statically yields True.

A static expression is evaluated at compile time except when it is statically unevaluated part of the right operand of a static short-circuit control form whose value is determined by its left operand. The compile-time evaluation of a static expression is performed exactly, without performing Overflow_Checks. For a static expression that is evaluated:

- The expression is illegal if its evaluation fails a language-defined check other than Overflow_Check. For the purposes of this evaluation, the assertion policy is assumed to be Check.

- If the expression is not part of a larger static expression and the expression is expected to be of a single specific type, then its value shall be within the base range of its expected type. Otherwise, the value may be arbitrarily large or small.

- If the expression is expected to be of a universal type, or of “any integer type”, there are no limits on the value of the expression.

If the expression is of type universal real and its expected type is a decimal fixed point type, then its value shall be a multiple of the small of the decimal type. This
restriction does not apply if the expected type is a descendant of a formal scalar type (or a corresponding actual type in an instance).

Ramification: This means that a numeric literal for a decimal type cannot have “extra” significant digits.

Reason: {AI95-00269-01} The small is not known for a generic formal type, so we have to exclude formal types from this check.

{AI95-00269-01} In addition to the places where Legality Rules normally apply (see 12.3), the above restrictions also apply in the private part of an instance of a generic unit. The last two restrictions above do not apply if the expected type is a descendant of a formal scalar type (or a corresponding actual type in an instance).

Discussion: Values outside the base range are not permitted when crossing from the “static” domain to the “dynamic” domain. This rule is designed to enhance portability of programs containing static expressions. Note that this rule applies to the exact value, not the value after any rounding or truncation. (See below for the rounding and truncation requirements.)

Short-circuit control forms are a special case:

\[
N: \text{constant} := 0.0;
\]

\[
X: \text{constant} \text{ Boolean} := (N = 0.0) \text{ or else } (1.0/N > 0.5); -- \text{ Static.}
\]

The declaration of X is legal, since the divide-by-zero part of the expression is not evaluated. X is a static constant equal to True.

{AI12-0075-1} The preceding “statically unevaluated” rule allows

\[X : \text{constant} := (\text{if True then } 37 \text{ else } (1 \div 0));\]

but does not allow

\[
\text{function If Then Else (Flag: Boolean; X, Y: Integer) return Integer is}
\]

\[
(\text{if Flag then } X \text{ else } Y) \text{ with Static;} -- \text{ see } 6.8
\]

\[X : \text{constant} := \text{If Then Else (True, 37, 1 \div 0)};\]

because evaluation of a function call includes evaluation of all of its actual parameters.

Ramification: {AI95-00269-01} There is no requirement to recheck these rules in an instance; the base range check will generally be performed at run time anyway.

Implementation Requirements

{AI95-00268-01} {AI95-00269-01} For a real static expression that is not part of a larger static expression, and whose expected type is not a descendant of a formal scalar type, the implementation shall round or truncate the value (according to the Machine_Rounds attribute of the expected type) to the nearest machine number of the expected type; if the value is exactly half-way between two machine numbers, the rounding shall be performed is implementation-defined away from zero. If the expected type is a descendant of a formal scalar type, or if the static expression appears in the body of an instance of a generic unit and the corresponding expression is nonstatic in the corresponding generic body, then no special rounding or truncating is required — normal accuracy rules apply (see Annex G).

Implementation defined: Rounding of real static expressions which are exactly half-way between two machine numbers.

Reason: {AI95-00268-01} Discarding extended precision enhances portability by ensuring that the value of a static constant of a real type is always a machine number of the type. Deterministic rounding of exact halves also enhances portability.

When the expected type is a descendant of a formal floating point type, extended precision (beyond that of the machine numbers) can be retained when evaluating a static expression, to ease code sharing for generic instantiations. For similar reasons, normal (nondeterministic) rounding or truncating rules apply for descendants of a formal fixed point type.

{AI95-00269-01} There is no requirement for exact evaluation or special rounding in an instance body (unless the expression is static in the generic body). This eliminates a potential contract issue where the exact value of a static expression depends on the actual parameters (which could then affect the legality of other code).

Implementation Note: Note that the implementation of static expressions has to keep track of plus and minus zero for a type whose Signed_Zeros attribute is True.
Note that the only machine number values of a fixed point type are the multiples of the small, so a static conversion to a fixed-point type, or division by an integer, must do truncation to a multiple of small. It is not correct for the implementation to do all static calculations in infinite precision.

Implementation Advice

For a real static expression that is not part of a larger static expression, and whose expected type is not a descendant of a formal type, the rounding should be the same as the default rounding for the target system.

Implementation Advice: A real static expression with a nonformal type that is not part of a larger static expression should be rounded the same as the target system.

NOTE 1 An expression can be static even if it occurs in a context where staticness is not required.

Ramification: For example:

X : Float := Float'(1.0E+400) + 1.0 - Float'(1.0E+400);

The expression is static, which means that the value of X must be exactly 1.0, independent of the accuracy or range of the run-time floating point implementation.

The following kinds of expressions are never static: explicit_dereference, indexed_component, slice, null, aggregate, allocator.

NOTE 2 A static (or run-time) type_conversion from a real type to an integer type performs rounding. If the operand value is exactly halfway between two integers, the rounding is performed away from zero.

Reason: We specify this for portability. The reason for not choosing round-to-nearest-even, for example, is that this method is easier to undo.

Ramification: The attribute Truncation (see A.5.3) can be used to perform a (static) truncation prior to conversion, to prevent rounding.

Implementation Note: The value of the literal 0E999999999999999999999999999999999999999999999 is zero. The implementation must take care to evaluate such literals properly.

Examples of static expressions:

1 + 1       == 2
abs(-10)*3  == 30
Kilo : constant := 1000;
Mega : constant := Kilo*Kilo;     == 1_000_000
Long : constant := Float'(Digits*2);
Half_Pi    : constant := Pi/2;        == see 3.3.2
Deg_To_Rad : constant := Half_Pi/90;
Rad_To_Deg : constant := 1.0/Deg_To_Rad;
           == equivalent to 1.0/((3.14159_26536/2)/90)

The rules for static expressions and static subtypes are generalized to allow more kinds of compile-time-known expressions to be used where compile-time-known values are required, as follows:

- Membership tests and short-circuit control forms may appear in a static expression.
- The bounds and length of statically constrained array objects or subtypes are static.
- The Range attribute of a statically constrained array subtype or object gives a static range.
- A type_conversion is static if the subtype_mark denotes a static scalar subtype and the operand is a static expression.
- All numeric literals are now static, even if the expected type is a formal scalar type. This is useful in case_statements and variant_parts, which both now allow a value of a formal scalar type to control the selection, to ease conversion of a package into a generic package. Similarly, named array aggregates are also permitted for array types with an index type that is a formal scalar type.

The rules for the evaluation of static expressions are revised to require exact evaluation at compile time, and force a machine number result when crossing from the static realm to the dynamic realm, to enhance portability and predictability. Exact evaluation is not required for descendants of a formal scalar type, to simplify generic code sharing and to avoid generic contract model problems.
Static expressions are legal even if an intermediate in the expression goes outside the base range of the type. Therefore, the following will succeed in Ada 95, whereas it might raise an exception in Ada 83:

```ada
type Short_Int is range -32_768 .. 32_767;
I : Short_Int := -32_768;
```

This might raise an exception in Ada 83 because "32_768" is out of range, even though "-32_768" is not. In Ada 95, this will always succeed.

Certain expressions involving string operations (in particular concatenation and membership tests) are considered static in Ada 95.

The reason for this change is to simplify the rule requiring compile-time-known string expressions as the link name in an interfacing pragma, and to simplify the preelaborability rules.

### Incompatibilities With Ada 83

An Ada 83 program that uses an out-of-range static value is illegal in Ada 95, unless the expression is part of a larger static expression, or the expression is not evaluated due to being on the right-hand side of a short-circuit control form.

### Wording Changes from Ada 83

{AI05-0299-1} This subclause clause (and 4.5.5, “Multiplying Operators”) subsumes the RM83 section on Universal Expressions.

The existence of static string expressions necessitated changing the definition of static subtype to include string subtypes. Most occurrences of "static subtype" have been changed to "static scalar subtype", in order to preserve the effect of the Ada 83 rules. This has the added benefit of clarifying the difference between "static subtype" and "statically constrained subtype", which has been a source of confusion. In cases where we allow static string subtypes, we explicitly use phrases like "static string subtype" or "static (scalar or string) subtype", in order to clarify the meaning for those who have gotten used to the Ada 83 terminology.

In Ada 83, an expression was considered nonstatic if it raised an exception. Thus, for example:

```ada
Bad: constant := 1/0; -- Illegal!
```

was illegal because 1/0 was not static. In Ada 95, the above example is still illegal, but for a different reason: 1/0 is static, but there's a separate rule forbidding the exception raising.

### Inconsistencies With Ada 95

{AI95-00268-01} Amendment Correction: Rounding of static real expressions is implementation-defined in Ada 2005, while it was specified as away from zero in (original) Ada 95. This could make subtle differences in programs. However, the original Ada 95 rule required rounding that (probably) differed from the target processor, thus creating anomalies where the value of a static expression was required to be different than the same expression evaluated at run time.

### Wording Changes from Ada 95

{AI95-00263-01} {AI95-00268-01} The Ada 95 wording that defined static subtypes unintentionally failed to exclude formal derived types that happen to be scalar (these aren't formal scalar types); and had a parenthetical remark excluding formal string types - but that was neither necessary nor parenthetical (it didn't follow from other wording). This issue also applies to the rounding rules for real static expressions.

{AI95-00269-01} Ada 95 didn't clearly define the bounds of a value of a static expression for universal types and for "any integer/float/fixed type". We also make it clear that we do not intend exact evaluation of static expressions in an instance body if the expressions aren't static in the generic body.

{AI95-00311-01} We clarify that the first subtype of a scalar formal type has a nonstatic, nonnull constraint.

### Wording Changes from Ada 2005

{AI05-0147-1} {AI05-0188-1} Added wording to define staticness and the lack of evaluation for if_expression and case_expression. These are new and defined elsewhere.

{AI05-0153-3} Added wording to prevent subtypes that have dynamic predicates (see 3.2.4) from being static.

{AI05-0158-1} Revised wording for membership tests to allow for the new possibilities allowed by the membership_choice_list.
Incompatibilities With Ada 2012

{AI12-0201-1} Added a missing exclusion for concatenations of a string type descended from a formal array type. This could potentially make some expression non-static; but as that could only matter in a context where a static string is required (such as the Link_Name aspect), it is quite unlikely.

{AI12-0385-1} Shifting and rotating functions declared in package Interfaces are now static. This could potentially make some expression illegal that is legal if nonstatic (as in Ada 2012). While this can happen especially in conditional code that is not in use, it is quite unlikely given typical uses of shifting or rotating functions.

Extensions to Ada 2012

{AI12-0201-1} Expressions involving string relational operators or string type conversions now can be static. Additionally, the length limit on static string constants was removed as being a hazard without much help to implementations.

Wording Changes from Ada 2012

This paragraph was deleted. {AI12-0064-2} {AI22-0018-1} Defined the staticness of the Nonblocking attribute (see 9.5).

{AI12-0075-1} Expression functions can be static if declared correctly; this is documented as an extension in 6.8.

{AI12-0249-1} {AI12-0394-1} A numeric literal or named number can be non-static if they interpreted using an Integer_Literal or Real_Literal aspect (see 4.2.1).

{AI12-0322-1} Clarified that a target name symbol can statically denote an entity if the associated variable_name statically denotes an entity. This is necessary so that target names participate in the anti-order-dependence checks of 6.4.1.

{AI12-0368-1} {AI12-0373-1} Added wording to define staticness for declare_expressions. Also moved “statically names” definition here and used it in array attribute prefix wording.

{AI12-0393-1} Correction: Clarified that constants whose values do not belong to their nominal subtype are not static. This change potentially would be incompatible, but this case is considered pathological and will not be checked by the ACATS.

Wording Changes from Ada 2022

{AI22-0018-1} Corrigendum: Removed text about a non-existent attribute.

4.9.1 Statically Matching Constraints and Subtypes

Static Semantics

{AI95-00311-01} A constraint statically matches another constraint if:

- both are null constraints,
- both are nonstatic and have equal corresponding bounds or discriminant values, or
- both are static and have equal corresponding bounds or discriminant values, or
- both are nonstatic and result from the same elaboration of a constraint of a subtype_indication or the same evaluation of a range of a discrete_subtype_definition.

- both are null constraints:

  Discussion: A null constraint has nothing to do with null exclusions! Unconstrained array subtypes, subtypes with unknown discriminants, and subtypes with no explicit constraint have null constraints (see 3.2). This terminology became confusing when null exclusions were introduced in the 2007 Amendment.

- both are static and have equal corresponding bounds or discriminant values:

- both are nonstatic and result from the same elaboration of a constraint of a subtype_indication or the same evaluation of a range of a discrete_subtype_definition; or

- {AI95-00311-01} both are nonstatic and come from the same formal_type_declaration.

- {AI12-0374-2} {AI12-0427-1} The Global or Global'Class aspects (see 6.1.2) of two entities statically match if both consist of a single global_aspect_definition where each is the reserved word null, or each is of the form “global_mode global_designator” with each global_mode being the same sequence of reserved words and each global_designator being the same reserved word, or each being a global_name that statically names the same entity.
A subtype statically matches another subtype of the same type if they have statically matching constraints, all predicate specifications that apply to them come from the same declarations, Nonblocking aspects have the same value, global aspects statically match, Object Size (see 13.3) has been specified to have a nonconforming value for either both or neither, and the nonconforming values, if any, are the same, and, for access subtypes, either both or neither exclude null. Two anonymous access-to-object subtypes statically match if their designated subtypes statically match, and either both or neither exclude null, and either both or neither are access-to-constant. Two anonymous access-to-subprogram subtypes statically match if their designated profiles are subtype conformant, and either both or neither exclude null.

Ramification: Statically matching constraints and subtypes are the basis for subtype conformance of profiles (see 6.3.1).

Reason: Even though anonymous access types always represent different types, they can statically match. That's important so that they can be used widely. For instance, if this wasn't true, access parameters and access discriminants could never conform, so they couldn't be used in separate specifications.

Ramification: [AI12-0059-1] If one of the subtypes is not yet frozen, an implementation may have to repeat the check when the subtypes are both frozen (as it is impossible to check the Object Size part before the subtypes are frozen). This recheck can only make a previously statically matching subtype fail to match; it cannot make a match legal.

Discussion: [AI12-0059-1] We exclude the case where both Object Sizes are confirming so that we don't introduce an incompatibility for existing Ada code. But practically the implementation can simply check that the Object Size values are the same, as we have a rule in 13.1 that the subtype-specific aspects (such as Object Size) are always the same for statically matching subtypes. We wrote the rules this way to avoid having wording that appeared to require predicting the future ("would statically match if ...").

Two ranges of the same type statically match if both result from the same evaluation of a range, or if both are static and have equal corresponding bounds.

Ramification: The notion of static matching of ranges is used in 12.5.3, “Formal Array Types”; the index ranges of formal and actual constrained array subtypes have to statically match.

A constraint is statically compatible with a scalar subtype if it statically matches the constraint of the subtype, or if both are static and the constraint is compatible with the subtype. A constraint is statically compatible with an access or composite subtype if it statically matches the constraint of the subtype, or if the subtype is unconstrained. One subtype is statically compatible with a second subtype if the constraint of the first is statically compatible with the second subtype.

Discussion: Static compatibility is required when constraining a parent subtype with a discriminant from a new discriminant_part. See 3.7. Static compatibility is also used in matching generic derived types.

Note that statically compatible with a subtype does not imply compatible with a type. It is OK since the terms are used in different contexts.

Two statically matching subtypes are statically compatible with each other. In addition, a subtype SI is statically compatible with a subtype S2 if:

- the constraint of SI is statically compatible with S2, and
- [AI05-0086-1] if S2 excludes null, so does SI, and
- either:
  - all predicate specifications that apply to S2 apply also to SI, or
  - [AI05-0290-1] both subtypes are static, every value that satisfies the predicates of SI also satisfies the predicates of S2, and it is not the case that both types each have at least one applicable predicate specification, predicate checks are enabled (see 11.4.2) for S2, and predicate checks are not enabled for SI.

This subclause is new to Ada 95.
4.9.1 Static Matching Constraints and Subtypes

Wording Changes from Ada 95

\{AI95-00231-01\} \{AI95-00254-01\} \textbf{Added static matching rules for null exclusions and anonymous access-to-subprogram types; both of these are new.}

\{AI95-00311-01\} \textbf{We clarify that the constraint of the first subtype of a scalar formal type statically matches itself.}

Incompatibilities With Ada 2005

\{AI05-0086-1\} \textbf{Correction: Updated the statically compatible rules to take null exclusions into account. This is technically incompatible, as it could cause a legal Ada 2005 program to be rejected; however, such a program violates the intent of the rules (for instance, 3.7(15)) and this probably will simply detect bugs.}

Wording Changes from Ada 2005

\{AI05-0153-3\} \{AI05-0290-1\} \textbf{Modified static matching and static compatibility to take predicate aspects (see 3.2.4) into account.}

Wording Changes from Ada 2012

\{AI12-0071-1\} \textbf{Corrigendum: Updated wording of static compatibility to use the new term "satisfies the predicates" (see 3.2.4).}

\{AI12-0059-1\} \textbf{Updated wording to take nonconfirming values of Object_Size into account.}

\{AI12-0374-2\} \textbf{Static matching now includes the effects of Global aspects and the Nonblocking aspect.}

4.10 Image Attributes

\{AI12-0315-1\} \textbf{An image of a value is a string representing the value in display form. The attributes Image, Wide Image, and Wide Wide Image are available to produce the image of a value as a String, Wide String, or Wide Wide String (respectively). User-defined images for a given type can be implemented by overriding the default implementation of the attribute Put Image.}

Static Semantics

\{AI12-0020-1\} \{AI12-0315-1\} \textbf{For every subtype S of a type T other than universal real or universal fixed, the following type-related operational attribute is defined:}

\{AI12-0020-1\} \{AI12-0320-1\} \{AI12-0340-1\} \textbf{S'Put(Image) denotes a procedure with the following specification:}

\textbf{procedure \textit{S'Put(Image)}}
\begin{verbatim}
  (Buffer : in out Ada.Strings.Text_Buffers.Root_Buffer_Type'Class;
   Arg : in T);
\end{verbatim}

\{AI12-0315-1\} \{AI12-0340-1\} \textbf{The default implementation of S'Put(Image) writes (using Wide_Wide_Put) an image of the value of Arg.}

\{AI12-0020-1\} \{AI12-0419-1\} \textbf{The Put Image attribute may be specified for any specific type T either via an attribute definition clause or via an aspect specification specifying the Put Image aspect of the type. [The Put Image aspect is not inherited, but rather is implicitly composed for derived types, as defined below.]}

Aspect Description for Put Image: Procedure to define the image of a given type.

Discussion: In contrast, the Image, Wide Image, and Wide Wide Image attributes and their associated aspects can not be specified. The behavior of any of these attributes is defined in terms of calls to the corresponding Put Image procedure, so changes in their behavior may be accomplished via a Put Image specification.

In earlier versions of Ada, Image and related attributes were defined only for scalar types. The definition of these attributes is now very different, but there should be no change in the behavior of existing programs as a result of these changes.
For an aspect specification or attribute definition clause specifying Put_Image, the subtype of the Arg parameter shall be the first subtype or the base subtype if scalar, and the first subtype if not scalar.

The behavior of the default implementation of S'Put_Image depends on the class of T.

For an untagged derived type, or a null extension, the default implementation of T'Put_Image invokes the Put_Image for its parent type on a conversion of the parameter of type T to the parent type.

For a nonderived elementary type, the implementation is equivalent to:

```ada
procedure Scalar_Type'Put_Image (Buffer : in out Ada.Strings.Text_Buffers.Root_Buffer_Type'Class; Arg : in Scalar_Type) is
begin
  Buffer.Wide_Wide_Put (<described below>);
end Scalar_Type'Put_Image;
```

where the Wide_Wide_String value written out to the text buffer is defined as follows:

- For an integer type, the image written out is the corresponding decimal literal, without underlines, leading zeros, exponent, or trailing spaces, but with a single leading character that is either a minus sign or a space.

  **Implementation Note:** If the machine supports negative zeros for signed integer types, it is not specified whether "0" or "-0" should be returned for negative zero. We don't have enough experience with such machines to know what is appropriate, and what other languages do. In any case, the implementation should be consistent.

  **Discussion:** We allow S'Put_Image when S is universal_integer or root_integer, because the details of the desired string do not depend on properties of an integer type. While S'Put_Image cannot be called directly for these types (as they cannot be named), it can be called as part of evaluating an Image attribute. Note that other rules of the language ensure that an implementation can evaluate any universal_integer attribute using type root_integer; therefore, Constraint_Error could be raised by the evaluation of an Image attribute if the value of the prefix is outside of the range of root_integer.

- For an enumeration type, the image written out is either the corresponding identifier in upper case or the corresponding character literal (including the two apostrophes); neither leading nor trailing spaces are included. For a nongraphic character (a value of a character type that has no enumeration literal associated with it), the value is a corresponding language-defined name in upper case (for example, the image of the nongraphic character identified as nul is "NUL" — the quotes are not part of the image).

  **Implementation Note:** For an enumeration type T that has "holes" (caused by an enumeration_representation_clause), T'Put_Image should raise Program_Error if the value is one of the holes (which is a bounded error anyway, since holes can be generated only via uninitialized variables and similar things).

- For a floating point type, the image written out is a decimal real literal best approximating the value (rounded away from zero if halfway between) with a single leading character that is either a minus sign or a space, a single digit (that is nonzero unless the value is zero), a decimal point, S'Digits-1 (see 3.5.8) digits after the decimal point (but one if S'Digits is one), an upper case E, the sign of the exponent (either + or -), and two or more digits (with leading zeros if necessary) representing the exponent. If S'Signed_Zeros is True, then the leading character is a minus sign for a negatively signed zero.

  **To be honest:** Leading zeros are present in the exponent only if necessary to make the exponent at least two digits.

  **Reason:** This image is intended to conform to that produced by Text_IO.Float_IO.Put in its default format.

  **Implementation Note:** The rounding direction is specified here to ensure portability of output results.

  **Reason:** AI12-0315-1 We do not allow S'Put_Image when S is universal_real, as the details of the desired string depend on the properties of the (specific) type of S. Specifically, universal_real does not have a defined value for S'Digits.
• **AI12-0020-1** For a fixed point type, the image written out is a decimal real literal best approximating the value (rounded away from zero if halfway between) with a single leading character that is either a minus sign or a space, one or more digits before the decimal point (with no redundant leading zeros), a decimal point, and S'Aft (see 3.5.10) digits after the decimal point.

**Reason:** This image is intended to conform to that produced by Text IO.Fixed.IO.Put.

**Implementation Note:** The rounding direction is specified here to ensure portability of output results.

For a machine that supports negative zeros, it is not specified whether " 0.000" or "-0.000" is returned. See corresponding comment above about integer types with signed zeros.

**Reason:** **AI12-0315-1** We do not allow S'Put_Image when S is universal fixed, as the details of the desired string depend on the properties of the (specific) type of S. Specifically, universal fixed does not have a defined value for S'Aft.

• **AI12-0020-1** For an access type (named or anonymous), the image written out depends on whether the value is null. If it is null, then the image is "NULL". Otherwise the image is a left parenthesis followed by "ACCESS", a space, and a sequence of graphic characters, other than space or right parenthesis, representing the location of the designated object, followed by a right parenthesis, as in "(ACCESS_FF0012AC)".

**To be honest:** **AI12-0315-1** S'Put_Image is defined for universal access, but it can never be called (as no legal prefix of Image has that type, and that type cannot be named preventing direct calls).

• **AI12-0020-1** **AI12-0419-1** **AI12-0435-1** For a nonnull type extension, the default implementation of T'Put_Image depends on whether there exists a noninterface ancestor of T (other than T itself) for which the Put_Image aspect has been directly specified. If so, then T'Put_Image will generate an image based on extension aggregate syntax where the ancestor type of the extension aggregate is the nearest ancestor type whose Put_Image aspect has been specified. If no such ancestor exists, then the default implementation of T'Put_Image is the same as described below for a nonderived record type.

**Discussion:** This might generate an image such as "(This Text Was User-Generated with C1 => 123, C2 => 456)" where the "This Text was User-Generated" portion of the text was generated by the call to the user-specified Put_Image routine.

• **AI12-0020-1** **AI12-0419-1** For a specific, nonderived composite type:

• **AI12-0020-1** If the default implementation of Put_Image writes components, the order in which components are written is the same canonical order in which components of a composite type T are written out by the default implementation of T'Write. [This is also the order that is used in determining the meaning of a positional aggregate of type T.]

**Discussion:** **AI12-0020-1** **AI12-0384-2** In general, the default implementation of T'Put_Image for a composite type will involve some sequence of calls to Put and its Wide and Wide_Wide variants and calls to the Put_Image procedures of component types and, in the case of an array type, index types. The Put calls may pass in either literal values (e.g., ",", "", or ",", " => ", or ",") or other things (such as component names for record values, task id images for tasks, or the Wide_Expanded_Name of the tag in the class-wide case).

• **AI12-0020-1** **AI12-0419-1** For an array type T, the default implementation of T'Put_Image generates an image based on named (not positional) array aggregate syntax (with '[' and ']' as the delimiters) using calls to the Put Image procedures of the index type(s) and the element type to generate images for values of those types.

**Discussion:** An array type might generate an image such as:

```
[ 1 => [ 1 => [ 123 => True, 124 => False]
  2 => [ 123 => False, 124 => False]]],
2 => [ 123 => True, 124 => True],
  2 => [ 123 => True, 124 => False]]
```

although perhaps with different white space and/or line breaking.

• **AI12-0020-1** The case of a null array is handled specially, using ranges for index bounds and "<>" as a syntactic component-value placeholder.

**Discussion:** This might generate an image such as "[[ 1 ..  3 => [ 1 ..  0 => [ 1 ..  5 => <>]]]", where the use of "<>" (among other things) indicates that the overall array is a null array and has no actual elements.
For a record type (or, as indicated above, a type extension with no noninterface ancestor specifying Put Image), or a protected type, the default implementation of T'Put_Image generates an image based on named (not positional) record aggregate syntax (except that for a protected type, the initial left parenthesis is followed by "PROTECTED with "). Component names are displayed in upper case, following the rules for the image of an enumeration value. Component values are displayed via calls to the component type's Put Image procedure.

**Discussion:** This might generate an image such as:

```
(FOO => [1 => 'c', 2 => 'a', 3 => 't'], BAR => TRUE)
```

The image written out for a record having no components (including any interface type) is "(NULL RECORD)". The image written out for a componentless protected type is "(PROTECTED NULL RECORD)". In the case of a protected type T, a call to the default implementation of T'Put_Image begins only one protected (read-only) action.

**Implementation Note:** The expected, but not required, implementation model for generating the image of a protected record involves the compiler producing a "helper" protected function which T'Put_Image would call. The result type of this function might be a null record; it is only a function because it does not need a write-lock, not because it returns a meaningful result.

The assertion in the following example should succeed:

```ada
type T1 (D1, D2 : Positive) is record ... end record; -- untagged
type T2 (D : Positive) is new T1 (D1 => D, D2 => D);
X : T2 (D => 123) := ... ;
pragma Assert (X'Image /= T1(X)'Image);
```

For an undiscriminated task type, the default implementation of T'Put_Image generates an image of the form "(TASK <task_id_image>)" where <task_id_image> is the result obtained by calling Task_Identification.Image with the id of the given task and then passing that String to Characters.Conversions.To_Wide_Wide_String.

For a discriminated task type, the default implementation of T'Put_Image also includes discriminant values, as in:

```
(TASK <task_id_image> with D1 => 123, D2 => 456).
```

For a class-wide type, the default implementation of T'Put_Image generates an image based on qualified expression syntax. Wide Wide Put is called with Wide Wide Expanded Name of Arg'Tag. Then S'Put_Image is called, where S is the specific type identified by Arg'Tag.

**Implementation Note:** This will typically require a dispatching call.

**Discussion:** This might generate an image such as:

```
SOME_PACKAGE.SOME_TAGGED_TYPE'
  (COMPONENT_1 => 123, COMPONENT_2 => 456)
```

The parentheses in this case are generated by the call to Some_Tagged_Type'Put_Image.

In the parameter and result profile for the default implementation of Put Image, the subtype of the Arg parameter is the base subtype of T if T is a scalar type, and the first subtype otherwise.

**Proof:** For an aspect specification or attribute definition clause specifying Put Image, the subprogram name shall denote a nonabstract procedure whose second parameter is either of the first subtype of T, or as an option when T is scalar, the base subtype of T.

**Ramification:** Put Image is never an abstract routine, even for an abstract type. Thus, Put Image and Image can be called for any type.
For every subtype \( S \) of a type \( T \), the following attributes are defined:

\[ S'\text{Wide\_Wide\_Image} \]

\[ \text{function} \quad S'\text{Wide\_Wide\_Image}(\text{Arg} : S'\text{Base}) \quad \text{return} \quad \text{Wide\_Wide\_String} \]

\( S'\text{Wide\_Wide\_Image} \) calls \( S'\text{Put\_Image} \) passing \( \text{Arg} \) (which will typically store a sequence of character values in a text buffer) and then returns the result of retrieving the contents of that buffer with function \( \text{Wide\_Wide\_Get} \). The lower bound of the result is one. [Any exception propagated by the call of \( S'\text{Put\_Image} \) is propagated.]

\[ S'\text{Wide\_Image} \]

\[ \text{function} \quad S'\text{Wide\_Image}(\text{Arg} : S'\text{Base}) \quad \text{return} \quad \text{Wide\_String} \]

\( S'\text{Wide\_Image} \) calls \( S'\text{Put\_Image} \) passing \( \text{Arg} \) (which will typically store a sequence of character values in a text buffer) and then returns the result of retrieving the contents of that buffer with function \( \text{Wide\_Get} \). The lower bound of the result is one. [Any exception propagated by the call of \( S'\text{Put\_Image} \) is propagated.]

\[ S'\text{Image} \]

\[ \text{function} \quad S'\text{Image}(\text{Arg} : S'\text{Base}) \quad \text{return} \quad \text{String} \]

\( S'\text{Image} \) calls \( S'\text{Put\_Image} \) passing \( \text{Arg} \) (which will typically store a sequence of character values in a text buffer) and then returns the result of retrieving the contents of that buffer with function \( \text{Get} \). The lower bound of the result is one. [Any exception propagated by the call of \( S'\text{Put\_Image} \) is propagated.]

For a prefix \( X \) of a type \( T \) other than \( \text{universal\_real} \) or \( \text{universal\_fixed} \), the following attributes are defined:

\[ X'\text{Wide\_Wide\_Image} \]

\[ \text{X'Wide\_Wide\_Image} \] denotes the result of calling function \( S'\text{Wide\_Wide\_Image} \) with \( \text{Arg} \) being \( X \), where \( S \) is the nominal subtype of \( X \).

\[ X'\text{Wide\_Image} \]

\[ \text{X'Wide\_Image} \] denotes the result of calling function \( S'\text{Wide\_Image} \) with \( \text{Arg} \) being \( X \), where \( S \) is the nominal subtype of \( X \).

\[ X'\text{Image} \]

\[ \text{X'Image} \] denotes the result of calling function \( S'\text{Image} \) with \( \text{Arg} \) being \( X \), where \( S \) is the nominal subtype of \( X \).

**Implementation Permissions**

An implementation may transform the image generated by the default implementation of \( S'\text{Put\_Image} \) for a composite subtype \( S \) in the following ways:

- If \( S \) is a composite subtype, the leading character of the image \( M \) of a component value or index value is a space, and the immediately preceding character (if any) is an open parenthesis, open bracket, or space, then the leading space of the image \( M \) may be omitted.

**Discussion:** This means that it is permitted to generate "\([1 => 123, 2 => 456]\)" instead of "\([1 => 123, 2 => 456]\)."
• If S is an array subtype, the low bound of the array in each dimension equals the low bound of the corresponding index subtype, and the array value is not a null array value, then positional array aggregate syntax may be used.

Discussion: This means that it is permitted to generate "[TRUE, TRUE, FALSE]" instead of "[ 1 => TRUE, 2 => TRUE, 3 => FALSE]" if the low bound of the index subtype is one.

• If S is an array subtype and the given value can be displayed using named array aggregate syntax where some discrete choice list identifies more than one index value by identifying a sequence of one or more ranges and values separated by vertical bars, then this image may be generated instead; this may involve the reordering of component values.

Discussion: This means that it is permitted to generate "[ 1 .. 2 | 5 => TRUE, 3 .. 4 => FALSE]" instead of "[ 1 => TRUE, 2 => TRUE, 3 => FALSE, 4 => FALSE, 5 => TRUE]".

• Similarly, if S is a record subtype (or a discriminated type) and the given value can be displayed using named component association syntax where the length of some component choice list is greater than one, then this image may be generated instead; this may involve the reordering of component values.

Discussion: This means that it is permitted to generate "(F1 | F2 => TRUE)" instead of "(F1 => TRUE, F2 => TRUE)".

• \{AI12-0020-1\}, \{AI12-0340-1\}, \{AI12-0384-2\} Additional spaces (Wide Wide Characters with position 32), and calls to the New_Line operation of a text buffer, may be inserted to improve readability of the generated image, with the spaces inserted directly or via use of the Increase_Indent and Decrease_Indent procedures.

• \{AI12-0384-2\} For a string type, implementations may produce an image corresponding to a string literal.

• \{AI12-0384-2\} For an unchecked union type, implementations may raise Program_Error or produce some recognizable image (such as "(UNCHECKED UNION)") that does not require reading the discriminants.

\{AI12-0304-1\} For each language-defined nonscalar type T, T’Put_Image may be specified.

Discussion: This permission applies, in particular, to nonscalar types declared in language-defined generic packages, and to any language-defined private type, even if an implementation chooses to complete it as a scalar type.

Ramification: For any language-defined scalar type T, T’Put_Image should not be specified; the Image attribute needs to return the language-defined image for such types. This is important for compatibility: the Image attribute has been available for scalar types for many Ada revisions, and programs can (and do!) depend on its behavior.

Implementation Requirements

\{AI12-0304-1\} For each language-defined container type T (that is, each of the Vector, List, Map, Set, Tree, and Holder types defined in the various children of Ada.Containers), T’Put_Image shall be specified so that T’Image produces a result consistent with array aggregate syntax (using '[' and ']' as delimiters) as follows:

• Vector images shall be consistent with the default image of an array type with the same index and component types.

Discussion: In particular, this means that the format is that of a named array aggregate. We have no recommendation on how to handle empty elements; if the implementation can identify them, it may wish to display them specially, but otherwise, they're just uninitialized elements.

• Map images shall be consistent with named array aggregate syntax, using key value images in place of discrete choice names. For example, [Key1 => Value1, Key2 => Value2].

Discussion: There is no recommendation about the order in which key/element pairs occur within a map image. In the case of multiple key values whose corresponding element values have the same image, there is no recommendation about factoring (that is, generating Key1 | Key2 => Some Value instead of Key1 => Some Value, Key2 => Some Value).
4.10 Image Attributes

- **Set, List, and Holder images** shall be consistent with positional array aggregate syntax. List elements shall occur in order within an image of a list. The image of an empty holder shall be `[]`.

  **Discussion:** There is no recommendation about the order in which set elements occur within the image of a set.

- **Tree images** (and images of subtrees of trees) shall be consistent with positional array aggregate syntax. For example, `[[1, 2], [111, 222, 333]]`.

  `{AI12-0304-1}` For each language-defined non-scalar type T that has a primitive language-defined Image function whose profile is type conformant with that of T'Image (for example, Ada.Numerics.Float_Random.State has such an Image function), T'Put_Image shall be specified so that T'Image yields the same result as that Image function.

  **Implementation Advice:**
  
  For each language-defined private type T, T'Image should generate an image that would be meaningful based only on the relevant public interfaces, as opposed to requiring knowledge of the implementation of the private type.

  `{AI12-0020-1} {AI12-0315-1} {AI12-0340-1} {AI12-0419-1} {AI12-0427-1} {AI12-0435-1} Attribute Put_Image is new. Attributes Image, Wide_Image, and Wide_Wide_Image now can be used with any type, and are defined in terms of Put_Image so that they can be redefined.
5 Statements

[A statement defines an action to be performed upon its execution.]

{AI95-00318-02} {AI05-0299-1} {AI12-0449-1} [This clause section describes the general rules applicable to all statements. Some statements are discussed in later clause sections: Procedure_call_-statements and return_statements. Entry_-call_statements, requeue_statements, delay_statements, accept_statements, select_statements, and abort_statements are described in Clause 9, “Tasks and Synchronization”. Raise_statements are described in Clause 11, “Exceptions”, and code_statements in Clause 13, “Representation Issues”. The remaining forms of statements are presented in this clause section.]

Wording Changes from Ada 83

{AI95-00318-02} The description of return_statements has been moved to 6.5, “Return Statements”, so that it is closer to the description of subprograms.

5.1 Simple and Compound Statements - Sequences of Statements

{AI12-0119-1} [A statement is either simple or compound. A simple_statement encloses no other statement. A compound_statement can enclose simple_statements and other compound_statements.]

A parallel construct is a construct that introduces additional logical threads of control (see Clause 9) without creating a new task. Parallel loops (see 5.5) and parallel_block_statements (see 5.6.1) are parallel constructs.

Term entry: parallel construct — executable construct that defines multiple activities of a single task that can proceed in parallel, via the execution of multiple logical threads of control

Syntax

{AI05-0179-1} sequence_of_statements ::= statement {statement} {label}

statement ::= {label} simple_statement | {label} compound_statement


{AI95-00318-02} {AI12-0119-1} compound_statement ::= if_statement | case_statement | loop_statement | block_statement | extended_return_statement | parallel_block_statement | accept_statement | select_statement

null_statement ::= null;

label ::= <<label_statement_identifier>>

statement_identifier ::= direct_name

The direct_name of a statement_identifier shall be an identifier (not an operator_symbol).
Name Resolution Rules

10 The direct_name of a statement_identifier shall resolve to denote its corresponding implicit declaration (see below).

Legality Rules

11 Distinct identifiers shall be used for all statement_identifiers that appear in the same body, including inner block_statements but excluding inner program units.

Static Semantics

12 For each statement_identifier, there is an implicit declaration (with the specified identifier) at the end of the declarative_part of the innermost block_statement or body that encloses the statement_identifier. The implicit declarations occur in the same order as the statement_identifiers occur in the source text. If a usage name denotes such an implicit declaration, the entity it denotes is the label, loop_statement, or block_statement with the given statement_identifier.

Reason: We talk in terms of individual statement_identifiers here rather than in terms of the corresponding statements, since a given statement may have multiple statement_identifiers.

12.a A block_statement that has no explicit declarative_part has an implicit empty declarative_part, so this rule can safely refer to the declarative_part of a block_statement.

12.c The scope of a declaration starts at the place of the declaration itself (see 8.2). In the case of a label, loop, or block name, it follows from this rule that the scope of the implicit declaration starts before the first explicit occurrence of the corresponding name, since this occurrence is either in a statement label, a loop_statement, a block_statement, or a goto_statement. An implicit declaration in a block_statement may hide a declaration given in an outer program unit or block_statement (according to the usual rules of hiding explained in 8.3).

12.b The syntax rule for label uses statement_identifier which is a direct_name (not a defining_identifier), because labels are implicitly declared. The same applies to loop and block names. In other words, the label itself is not the defining occurrence; the implicit declaration is.

We cannot consider the label to be a defining occurrence. An example that can tell the difference is this:

12[f]

declare
-- Label Foo is implicitly declared here.
begin
  for Foo in ... loop
  ... <<Foo>> -- Illegal.
  ... end loop;
end;

12.g5 {A05-0299-1} {AI12-0449-1} The label in this example is hidden from itself by the loop parameter with the same name; the example is illegal. We considered creating a new syntactic category name, separate from direct_name and selector_name, for use in the case of statement labels. However, that would confuse the rules in 8.3ClauseSection 8, so we didn’t do it.

12.1/3 {A105-0179-1} If one or more labels end a sequence_of_statements, an implicit null_statement follows the labels before any following constructs.

Reason: The semantics of a goto_statement is defined in terms of the statement having (following) that label. Thus we ensure that every label has a following statement, which might be implicit.

Dynamic Semantics

13 The execution of a null_statement has no effect.

14/2 {A95-00318-02} A transfer of control is the run-time action of an exit_statement, return_statement, goto_statement, or requeue_statement, selection of a terminate_alternative, raising of an exception, or an abort, which causes the next action performed to be one other than what would normally be expected from the other rules of the language. [As explained in
7.6.1, a transfer of control can cause the execution of constructs to be completed and then left, which may trigger finalization.]

The execution of a sequence_of_statements consists of the execution of the individual statements in succession until the sequence is completed.

**Ramification:** It could be completed by reaching the end of it, or by a transfer of control.

{AI12-0119-1} Within a parallel construct, if a transfer of control out of the construct is initiated by one of the logical threads of control, an attempt is made to cancel all other logical threads of control initiated by the parallel construct. Once all other logical threads of control of the construct either complete or are canceled, the transfer of control occurs. If two or more logical threads of control of the same construct initiate such a transfer of control concurrently, one of them is chosen arbitrarily and the others are canceled.

{AI12-0119-1} When a logical thread of control is canceled, the cancellation causes it to complete as though it had performed a transfer of control to the point where it would have finished its execution. Such a cancellation is deferred while the logical thread of control is executing within an abort-deferred operation (see 9.8), and may be deferred further, but not past a point where the logical thread initiates a new nested parallel construct or reaches an exception handler that is outside such an abort-deferred operation.

**Bounded (Run-Time) Errors**

{AI12-0119-1} {AI12-0442-1} During the execution of a parallel construct, it is a bounded error to invoke an operation that is potentially blocking (see 9.5). Program_Error is raised if the error is detected by the implementation; otherwise, the execution of the potentially blocking operation can either proceed normally, or it can result in the indefinite blocking of some or all of the logical threads of control making up the current task.

**NOTE** A statement_identifier that appears immediately within the declarative region of a named loop_statement or an accept_statement is nevertheless implicitly declared immediately within the declarative region of the innermost enclosing body or block_statement; in other words, the expanded name for a named statement is not affected by whether the statement occurs inside or outside a named loop or an accept_statement — only nesting within block_statements is relevant to the form of its expanded name.

**Discussion:** Each comment in the following example gives the expanded name associated with an entity declared in the task body:

```ada
task body Compute is
begin
  Outer:
  for I in 1..10 loop -- Compute.Outer.I
    Blk:
    declare
    begin
      accept Ent(I : out Integer; J : in Integer) do
        Inner:                                      -- Compute.Blk.Inner
          for J in 1..10 loop -- Compute.Blk.Inner.J
          end loop Inner;
        end Ent;
      end loop;                                    -- Compute.Blk.Sum
    end Blk;
  end loop Outer;
  Record_Result(Sum);
end Compute;
```
Examples

Examples of labeled statements:

<<Here>> <<Ici>> <<Aqui>> <<Hier>> null;
<<After>> X := 1;

Extensions to Ada 83

22.a The requeue_statement is new.

Wording Changes from Ada 83

22.b We define the syntactic category statement_identifier to simplify the description. It is used for labels, loop names, and block names. We define the entity associated with the implicit declarations of statement names.

22.c Completion includes completion caused by a transfer of control, although RM83-5.1(6) did not take this view.

Extensions to Ada 95

22.d2 \{AI95-00318-02\} The extended_return_statement is new (simple_return_statement is merely renamed).

Extensions to Ada 2005

22.e3 \{AI05-0179-1\} A label can end a sequence_of_statements, eliminating the requirement for having an explicit null; statement after an ending label (a common use).

Extensions to Ada 2012

22.f5 \{AI12-0119-1\} The definition of “parallel constructs” and the parallel_block_statement are new.

5.2 Assignment Statements

[An assignment_statement replaces the current value of a variable with the result of evaluating an expression.]

Syntax

assignment_statement ::= 
variable_name := expression;

The execution of an assignment_statement includes the evaluation of the expression and the assignment of the value of the expression into the target. [An assignment operation (as opposed to an assignment_statement) is performed in other contexts as well, including object initialization and by-copy parameter passing.] The target of an assignment operation is the view of the object to which a value is being assigned; the target of an assignment_statement is the variable denoted by the variable_name.

Discussion: Don't confuse this notion of the “target” of an assignment with the notion of the “target object” of an entry call or requeue.

Don't confuse the term “assignment operation” with the assignment_statement. The assignment operation is just one part of the execution of an assignment_statement. The assignment operation is also a part of the execution of various other constructs; see 7.6.1, “Completion and Finalization” for a complete list. Note that when we say, “such-and-such is assigned to so-and-so”, we mean that the assignment operation is being applied, and that so-and-so is the target of the assignment operation.

Name Resolution Rules

4/2 \{AI95-00287-01\} The variable_name of an assignment_statement is expected to be of any nonlimited type. The expected type for the expression is the type of the target.

Implementation Note: An assignment_statement as a whole is a “complete context”, so if the variable_name of an assignment_statement is overloaded, the expression can be used to help disambiguate it. For example:

\begin{verbatim}
type P1 is access R1;
type P2 is access R2;
\end{verbatim}
function F return P1;
function F return P2;
X : R1;
begin
  F.all := X;  -- Right hand side helps resolve left hand side

Legality Rules

{AI95-00287-01} The target [denoted by the variable_name] shall be a variable of a nonlimited type.
If the target is of a tagged class-wide type T'Class, then the expression shall either be dynamically tagged, or of type T and tag-indeterminate (see 3.9.2).

Reason: This is consistent with the general rule that a single dispatching operation shall not have both dynamically tagged and statically tagged operands. Note that for an object initialization (as opposed to the assignment_statement), a statically tagged initialization expression is permitted, since there is no chance for confusion (or Tag_Check failure). Also, in an object initialization, tag-indeterminate expressions of any type covered by T'Class would be allowed, but with an assignment_statement, that might not work if the tag of the target was for a type that didn't have one of the dispatching operations in the tag-indeterminate expression.

Dynamic Semantics

For the execution of an assignment_statement, the variable_name and the expression are first evaluated in an arbitrary order.

Ramification: Other rules of the language may require that the bounds of the variable be determined prior to evaluating the expression, but that does not necessarily require evaluation of the variable_name, as pointed out by the ACID.

When the type of the target is class-wide:

- If the expression is tag-indeterminate (see 3.9.2), then the controlling tag value for the expression is the tag of the target;

  Ramification: See 3.9.2, “Dispatching Operations of Tagged Types”.

- Otherwise [(the expression is dynamically tagged)], a check is made that the tag of the value of the expression is the same as that of the target; if this check fails, Constraint_Error is raised.

{AI12-0439-1} The value of the expression is converted to the subtype of the target. [The conversion can might raise an exception (see 4.6).]

  Ramification: 4.6, “Type Conversions” defines what actions and checks are associated with subtype conversion. For non-array subtypes, it is just a constraint check presuming the types match. For array subtypes, it checks the lengths and slides if the target is constrained. “Sliding” means the array doesn't have to have the same bounds, so long as it is the same length.

{AI12-0439-1} In cases involving controlled types, the target is finalized, and an anonymous object can might be used as an intermediate in the assignment, as described in 7.6.1, “Completion and Finalization”. In any case, the converted value of the expression is then assigned to the target, which consists of the following two steps:

  To be honest: 7.6.1 actually says that finalization happens always, but unless controlled types are involved, this finalization during an assignment_statement does nothing.

- The value of the target becomes the converted value.

- {AI05-0299-1} {AI12-0449-1} If any part of the target is controlled, its value is adjusted as explained in subclause 7.6.

  Ramification: If any parts of the object are controlled, abort is deferred during the assignment operation itself, but not during the rest of the execution of an assignment_statement.

NOTE The tag of an object never changes; in particular, an assignment_statement does not change the tag of the target.

This paragraph was deleted NOTE —{AI95-00363-01} The values of the discriminants of an object designated by an access value cannot be changed (not even by assigning a complete value to the object itself) since such objects are always constrained, however, subcomponents of such objects may be unconstrained.
Ramification: The implicit subtype conversion described above for assignment statements is performed only for the value of the right-hand side expression as a whole; it is not performed for subcomponents of the value.

The determination of the type of the variable of an assignment statement may require consideration of the expression if the variable name can be interpreted as the name of a variable designated by the access value returned by a function call, and similarly, as a component or slice of such a variable (see 8.6, “The Context of Overload Resolution”).

Examples

Examples of assignment statements:

Value := Max_Value - 1;
Shade := Blue;
Next_Frame(F)(M, N) := 2.5; -- see 4.1.1
U := Dot_Product(V, W); -- see 6.3
{AI12-0056-1} Writer := (Status => Open, Unit => Printer, Line_Count => 60); -- see 3.8.1
Next_Car.all := (72074, null, Head); -- see 3.10.1

Examples involving scalar subtype conversions:

I, J : Integer range 1 .. 10 := 5;
K : Integer range 1 .. 20 := 15;
...
I := J; -- identical ranges
K := J; -- compatible ranges
J := K; -- will raise Constraint_Error if K > 10

Examples involving array subtype conversions:

A : String(1 .. 31);
B : String(3 .. 33);
...
A := B; -- same number of components
A(1 .. 9) := "tar sauce";
A(4 .. 12) := A(1 .. 9); -- A(1 .. 12) = "tartar sauce"

Assignment statements are well-defined even in the case of overlapping slices of the same array, because the variable name and expression are both evaluated before copying the value into the variable. In the above example, an implementation yielding A(1 .. 12) = "tartartartar" would be incorrect.

Extensions to Ada 83

We now allow user-defined finalization and value adjustment actions as part of assignment statements (see 7.6, “Assignment and Finalization”).

Wording Changes from Ada 83

The special case of array assignment is subsumed by the concept of a subtype conversion, which is applied for all kinds of types, not just arrays. For arrays it provides “sliding”. For numeric types it provides conversion of a value of a universal type to the specific type of the target. For other types, it generally has no run-time effect, other than a constraint check.

We now cover in a general way in 3.7.2 the erroneous execution possible due to changing the value of a discriminant when the variable in an assignment statement is a subcomponent that depends on discriminants.

Incompatibilities With Ada 95

The change of the limited check from a resolution rule to a legality rule is not quite upward compatible. For example
where NonLim is a nonlimited type and Lim is a limited type. The assignment is legal in Ada 95 (only the first \texttt{Foo} would be considered), and is ambiguous in Ada 2005. We made the change because we want limited types to be as similar to nonlimited types as possible. Limited expressions are now allowed in all other contexts (with a similar incompatibility), and it would be odd if assignments had different resolution rules (which would eliminate ambiguities in some cases). Moreover, examples like this one are rare, as they depend on assigning into overloaded function calls.

### 5.2.1 Target Name Symbols

{\texttt{AI12-0125-3}} @, known as the target name of an assignment statement, provides an abbreviation to avoid repetition of potentially long names in assignment statements.

#### Syntax

{\texttt{AI12-0125-3}} \texttt{target \_name ::= @}

#### Name Resolution Rules

{\texttt{AI12-0125-3}} \texttt{If a target \_name occurs in an assignment \_statement \texttt{A}, the variable \_name \texttt{V} of \texttt{A} is a complete context. The target name is a constant view of \texttt{V}, having the nominal subtype of \texttt{V}.}

\textbf{Proof:} {\texttt{AI12-0125-3}} {\texttt{AI12-0322-1}} The complete context rule is formally given in 8.6. The constant view rule is formally given in 3.3; the nominal subtype is a property taken from the target object as described below in Dynamic Semantics.

#### Legality Rules

{\texttt{AI12-0125-3}} {\texttt{AI12-0322-1}} \texttt{A target \_name shall appear only in the expression of an assignment \_statement.}

#### Dynamic Semantics

{\texttt{AI12-0125-3}} {\texttt{AI12-0322-1}} {\texttt{AI12-0449-1}} \texttt{For the execution of an assignment \_statement with one or more target \_names appearing in its expression, the variable \_name \texttt{V} of the assignment \_statement is evaluated first to determine the object denoted by \texttt{V}, and then the expression of the assignment \_statement is evaluated with the evaluation of each target \_name yielding a constant view of the target whose properties are otherwise identical to those of the view provided by \texttt{V}. The remainder of the execution of the assignment \_statement is as given in 5.2.}

\textbf{To be honest:} The properties here include static properties like whether the target \_name is aliased and the nominal subtype of the target \_name. It was too weird to give separate rules for static and dynamic properties that said almost the same thing.

\textbf{Ramification:} {\texttt{AI12-0322-1}} Use of a target \_name can be erroneous if the variable \_name \texttt{V} is a discriminant-dependent component, and some other constituent of the expression modifies the discriminant governing the component \texttt{V}. The assignment probably would be erroneous anyway, but the use of a target \_name eliminates the possibility that a later evaluation of \texttt{V} raises an exception before any erroneous execution occurs. See 3.7.2.

#### Examples

{\texttt{AI12-0429-1}} \texttt{Examples of the use of target name symbols:}

{\texttt{AI12-0125-3}} {\texttt{AI12-0379-1}} {\texttt{AI12-0442-1}} \texttt{Board(1, 1) := @ + 1.0;}

\texttt{-- An abbreviation for Board(1, 1) := Board(1, 1) + 1.0;}

\texttt{-- (Board is declared in 3.6.1).}
5.3 If Statements

1 [An if_statement selects for execution at most one of the enclosed sequences_of_statements, depending on the (truth) value of one or more corresponding conditions.]

Syntax

2 if_statement ::=  
   if condition then  
   sequence_of_statements  
   elsif condition then  
   sequence_of_statements  
   [else  
   sequence_of_statements  
   end if;

3/3 {AI05-0147-1} condition ::= boolean_expression

Name Resolution Rules

4/3 {AI05-0147-1} A condition is expected to be of any boolean type.

Paragraphs 3 and 4 were deleted.

Dynamic Semantics

5/3 {AI05-0264-1} For the execution of an if_statement, the condition specified after if, and any conditions specified after elsif, are evaluated in succession (treating a final else as elsif True then), until one evaluates to True or all conditions are evaluated and yield False. If a condition evaluates to True, then the corresponding sequence_of_statements is executed; otherwise, none of them is executed.

5.a Ramification: The part about all evaluating to False can't happen if there is an else, since that is herein considered equivalent to elsif True then.

Examples

6 Examples of if statements:

7 if Month = December and Day = 31 then  
   Month := January;  
   Day := 1;  
   Year := Year + 1;  
   end if;

Extensions to Ada 2012

8/a/5 {AI12-0125-3} {AI12-0322-1} The target name symbol @ is new.
if Line_Too_Short then
  raise Layout_Error;
elsif Line_Full then
  New_Line;
else
  Put(Item);
end if;
if My_Car.Owner.Vehicle /= My_Car then
  -- see 3.10.1
  Report ("Incorrect data");
end if;

Wording Changes from Ada 2005

{AI05-0147-1} Moved definition of condition to 4.5.7 in order to eliminate a forward reference.

5.4 Case Statements

[A case_statement selects for execution one of a number of alternative sequences_of_statements; the chosen alternative is defined by the value of an expression.]

Syntax

{AI05-0188-1} case_statement ::= case selecting_expression is
  case_statement_alternative
  case_statement_alternative
end case;

{AI05-0188-1} case_statement_alternative ::= when discrete_choice_list =>
  sequence_of_statements

Name Resolution Rules

{AI05-0188-1} The selecting_expression is expected to be of any discrete type. The expected type for each discrete_choice is the type of the selecting_expression.

Legality Rules

{AI05-0153-3} The choice_expressions, subtype_indications, expressions, and range_discrete_ranges given as discrete_choices of a case_statement shall be static. [A discrete_choice others, if present, shall appear alone and in the last discrete_choice_list.]

{AI05-0188-1} {AI05-0240-1} The possible values of the selecting_expression shall be covered (see 3.8.1) as follows:

Discussion: {AI05-0240-1} The meaning of "covered" here and in the following rules is that of the term "cover a value" that is defined in 3.8.1.

• {AI05-0003-1} {AI05-0153-3} {AI05-0188-1} {AI05-0262-1} {AI12-0071-1} If the selecting_expression is a name [(including a type_conversion, qualified_expression, or a function_call)] having a static and constrained nominal subtype, or is a qualified_expression whose subtype_mark denotes a static and constrained scalar subtype, then each non-others discrete_choice shall cover only values in that subtype that satisfy its predicates (see 3.2.4), and each value of that subtype that satisfies its predicates shall be covered by some discrete_choice [(either explicitly or by others)].

Ramification: Although not official names of objects, a value conversion still has a defined nominal subtype, namely its target subtype. See 4.6.
• \{AI05-0188-1\} If the type of the selecting expression is root_integer, universal_integer, or a descendant of a formal scalar type, then the case_statement shall have an others discrete_choice.

Reason: This is because the base range is implementation defined for root_integer and universal_integer, and not known statically in the case of a formal scalar type.

• \{AI05-0188-1\} Otherwise, each value of the base range of the type of the selecting_expression shall be covered [(either explicitly or by others)].

Two distinct discrete_choices of a case_statement shall not cover the same value.

Ramification: \{AI05-0188-1\} The goal of these coverage rules is that any possible value of the selecting_expression of a case_statement should be covered by exactly one discrete_choice of the case_statement, and that this should be checked at compile time. The goal is achieved in most cases, but there are two minor loopholes:

• If the expression reads an object with an invalid representation (e.g. an uninitialized object), then the value can be outside the covered range. This can happen for static constrained subtypes, as well as nonstatic or unconstrained subtypes. It cannot, however, happen if the case_statement has the discrete_choice others, because others covers all values, even those outside the subtype.

• \{AI95-00114-01\} \{AI05-0188-1\} If the compiler chooses to represent the value of an expression of an unconstrained subtype in a way that includes values outside the bounds of the subtype, then those values can be outside the covered range. For example, if X: Integer := Integer’Last, and the case selecting_expression is X+1, then the implementation might choose to produce the correct value, which is outside the bounds of Integer. (It might raise Constraint_Error instead.) This case can only happen for nongeneric subtypes that are either unconstrained or non-static (or both). It can only happen if there is no others discrete_choice.

In the uninitialized variable case, the value might be anything; hence, any alternative can be chosen, or Constraint_Error can be raised. (We intend to prevent, however, jumping to random memory locations and the like.) In the out-of-range case, the behavior is more sensible: if there is an others, then the implementation may choose to raise Constraint_Error on the evaluation of the expression (as usual), or it may choose to correctly evaluate the expression and therefore choose the others alternative. Otherwise (no others), Constraint_Error is raised either way — on the expression evaluation, or for the case_statement itself.

For an enumeration type with a discontiguous set of internal codes (see 13.4), the only way to get values in between the proper values is via an object with an invalid representation; there is no “out-of-range” situation that can produce them.

Dynamic Semantics

\{AI05-0188-1\} For the execution of a case_statement, the selecting_expression is first evaluated.

\{AI05-0188-1\} If the value of the selecting_expression is covered by the discrete_choice_list of some case_statement_alternative, then the sequence_of_statements of the _alternative is executed.

Otherwise (the value is not covered by any discrete_choice_list, perhaps due to being outside the base range), Constraint_Error is raised.

Ramification: \{AI12-0005-1\} In this case, the value fails to satisfy its (static) predicate (possible when the predicate is disabled), is outside the base range of its type, or is an invalid representation.

NOTE \{AI12-0440-1\} The execution of a case_statement chooses one and only one alternative. Qualification of the expression of a case_statement by a static subtype can often be used to limit the number of choices that can be given explicitly.

Examples of case statements:

```ada
case Sensor is
  when Elevation => Record_Elevation(Sensor_Value);
  when Azimuth  => Record_Azimuth  (Sensor_Value);
  when Distance => Record_Distance (Sensor_Value);
  when others   => null;
end case;
```

5.4 Case Statements
case Today is
  when Mon => Compute_Initial_Balance;
  when Fri => Compute_Closing_Balance;
  when Tue .. Thu => Generate_Report(Today);
  when Sat .. Sun => null;
end case;

case Bin.Number(Count) is
  when 1 => Update_Bin(1);
  when 2 => Update_Bin(2);
  when 3 | 4 =>
    Empty_Bin(1);
    Empty_Bin(2);
  when others => raise Error;
end case;

Incomaptibilities With Ada 83

In Ada 95, function calls and type conversions are names, whereas in Ada 83, they were expressions. Therefore, if the expression of a case statement is a function call or type conversion, and the result subtype is static, it is illegal to specify a choice outside the bounds of the subtype. For this case in Ada 83 choices only are required to be in the base range of the type.

In addition, the rule about which choices must be covered is unchanged in Ada 95. Therefore, for a case statement whose expression is a function call or type conversion, Ada 83 required covering all choices in the base range, while Ada 95 only requires covering choices in the bounds of the subtype. If the case statement does not include an others discrete choice, then a legal Ada 83 case statement will be illegal in Ada 95 if the bounds of the subtype are different than the bounds of the base type.

Extensions to Ada 83

In Ada 83, the expression in a case statement is not allowed to be of a generic formal type. This restriction is removed in Ada 95; an others discrete choice is required instead.

In Ada 95, a function call is the name of an object; this was not true in Ada 83 (see 4.1, “Names”). This change makes the following case statement legal:

```
subtype S is Integer range 1..2;
function F return S;
end case;
```

Note that the result subtype given in a function renaming declaration is ignored; for a case statement whose expression calls such a function, the full coverage rules are checked using the result subtype of the original function. Note that predefined operators such as “+” have an unconstrained result subtype (see 4.5.1). Note that generic formal functions do not have static result subtypes. Note that the result subtype of an inherited subprogram need not correspond to any namable subtype; there is still a perfectly good result subtype, though.

Wording Changes from Ada 83

Ada 83 forgot to say what happens for “legally” out-of-bounds values.

We take advantage of rules and terms (e.g. cover a value) defined for discrete choices and discrete_choice_lists in 3.8.1, “Variant Parts and Discrete Choices”. In the Name Resolution Rule for the case expression, we no longer need RM83-5.4(3)’s “which must be determinable independently of the context in which the expression occurs, but using the fact that the expression must be of a discrete type”, because the expression is now a complete context. See 8.6, “The Context of Overload Resolution”.

Since type conversions are now defined as names, their coverage rule is now covered under the general rule for names, rather than being separated out along with qualified expressions.

Wording Changes from Ada 2005

{AI05-0003-1} Rewording to reflect that a qualified expression is now a name.

{AI05-0153-3} Revised for changes to discrete choices made to allow static predicates (see 3.2.4) as case choices (see 3.8.1).
5.5 Loop Statements

[AII12-0119-1] A loop_statement includes a sequence_of_statements that is to be executed repeatedly, zero or more times with the iterations running sequentially or concurrently with one another.

Syntax

```
loop_statement ::= [loop_statement_identifier:] [iteration_scheme] loop sequence_of_statements end loop [loop_identifier];
```

[AII12-0119-1] iteration_scheme ::= while condition | [parallel [aspect_specification]] for loop_parameter_specification | [parallel] [chunk_specification] [aspect_specification] for loop_parameter_specification | [parallel] [chunk_specification] [aspect_specification] for iterator_specification

[AII12-0119-1] chunk_specification ::= integer_simple_expression | defining_identifier in discrete_subtype_definition

[AII12-0120-1] loop_parameter_specification ::= defining_identifier in [reverse] discrete_subtype_definition | [iterator_filter]

[AII12-0119-1] iterator_filter ::= when condition

If a loop_statement has a loop_statement_identifier, then the identifier shall be repeated after the end loop; otherwise, there shall not be an identifier after the end loop.

[AII12-0119-1] An iteration_scheme that begins with the reserved word parallel shall not have the reserved word reverse in its loop_parameter_specification.

Name Resolution Rules

[AII12-0120-1] In a chunk specification that is an integer_simple_expression, the integer_simple_expression is expected to be of any integer type.

Static Semantics

[AII12-0120-1] A loop_parameter_specification declares a loop parameter, which is an object whose subtype (and nominal subtype) is that defined by the discrete_subtype_definition.
In a chunk specification that has a discrete subtype definition, the chunk specification declares a chunk parameter object whose subtype (and nominal subtype) is that defined by the discrete subtype definition.

Dynamic Semantics

The filter of an iterator construct (a loop parameter specification, iterator specification, or procedural iterator) is defined to be satisfied when there is no iterator filter for the iterator construct, or when the condition of the iterator filter evaluates to True for a given iteration of the iterator construct.

Term entry: iterator filter — construct that is used to restrict the elements produced by an iteration to those for which a boolean condition evaluates to True.

If a sequence of statements of a loop statement with an iterator construct is said to be conditionally executed, then the statements are executed only when the filter of the iterator construct is satisfied.

The loop iterators loop parameter specification and iterator specification can also be used in contexts other than loop statements (for example, see 4.3.5 and 4.5.8). In such a context, the iterator conditionally produces values in the order specified for the associated construct below or in 5.5.2. The values produced are the values given to the loop parameter when the filter of the iterator construct is satisfied for that value. [No value is produced when the condition of an iterator filter evaluates to False.]

For the execution of a loop statement, the sequence of statements is executed repeatedly, zero or more times, until the loop statement is complete. The loop statement is complete when a transfer of control occurs that transfers control out of the loop, or, in the case of an iteration scheme, as specified below.

For the execution of a loop statement with a while iteration scheme, the condition is evaluated before each execution of the sequence of statements; if the value of the condition is True, the sequence of statements is executed; if False, the execution of the loop statement is complete.

If the reserved word parallel is present in the iteration scheme of a loop statement (a parallel loop), the iterations are partitioned into one or more chunks, each with its own separate logical thread of control (see Clause 9). If a chunk specification is present in a parallel loop, it is elaborated first, and the result of the elaboration determines the maximum number of chunks used for the parallel loop. If the chunk specification is an integer simple expression, the elaboration evaluates the expression, and the value of the expression determines the maximum number of chunks. If a discrete subtype definition is present, the elaboration elaborates the discrete subtype definition, which defines the subtype of the chunk parameter, and the number of values in this subtype determines the maximum number of chunks. After elaborating the chunk specification, a check is made that the determined maximum number of chunks is greater than zero. If this check fails, Program_Error is raised.

For the execution of a loop statement that has an with the for iteration scheme including being for loop parameter specification, after elaborating the chunk specification and aspect specification, if any, the loop parameter specification is first elaborated. This elaboration creates the loop parameter and elaborates the discrete subtype definition, which defines the subtype of the loop parameter. If the discrete subtype definition defines a subtype with a null range, the execution of the loop statement is complete. Otherwise, the sequence of statements is conditionally executed once for each value of the discrete subtype defined by the discrete subtype definition that satisfies the predicate predicate of the subtype (or until the loop is left as a consequence of a transfer of control). Prior to each such iteration, the corresponding value of the
discrete subtype is assigned to the loop parameter associated with the given iteration. If the loop is a parallel loop, each chunk has its own logical thread of control with its own copy of the loop parameter; otherwise (a sequential loop), a single logical thread of control performs the loop, and there is a single copy of the loop parameter. Each logical thread of control handles a distinct subrange of the values of the subtype of the loop parameter such that all values are covered with no overlaps. Within each logical thread of control, these values are assigned to the loop parameter in increasing order unless the reserved word reverse is present, in which case the values are assigned in decreasing order. In the absence of a transfer of control, the associated parallel construct of a loop parameter specification is complete when all of its logical threads of control are complete.

To be honest: This wording does not describe when the loop parameter object(s) are created. That creation has no side-effects (other than possibly raising Storage Error, but anything can do that), so we simplified the wording by leaving it out. Each object has to be created before any iteration that depends on it starts, but we do not (for instance) require that the objects are all created at once at the start of the loop, nor that the objects are created after the elaboration of the discrete_subtype_definition.

This paragraph was deleted. Ramification: The order of creating the loop parameter and evaluating the discrete_subtype_definition doesn’t matter, since the creation of the loop parameter has no side effects (other than possibly raising Storage_Error, but anything can do that).

Reason: If there is a predicate, the loop still visits the values in the order of the underlying base type; the order of the values in the predicate is irrelevant. This is the case so that the following loops have the same sequence of calls and parameters on procedure Call for any subtype S:

```ada
for I in S loop
  Call (I);
end loop;
```

```ada
for I in S'Base loop
  if I in S then
    Call (I);
  end if;
end loop;
```

Discussion: The rules for completing a parallel construct when there is a transfer of control are given in 5.1.

If a chunk_specification with a discrete_subtype_definition is present, then the logical thread of control associated with a given chunk has its own copy of the chunk parameter initialized with a distinct value from the discrete subtype defined by the discrete_subtype_definition. The values of the chunk parameters are assigned such that they increase with increasing values of the ranges covered by the corresponding loop parameters.

Whether or not a chunk_specification is present in a parallel loop, the total number of iterations of the loop represents an upper bound on the number of logical threads of control devoted to the loop.

NOTE 1 A loop parameter declared by a loop_parameter_specification is a constant; it cannot be updated within the sequence_of_statements of the loop (see 3.3).

NOTE 2 No separate object_declaration is expected for a loop parameter, since the loop parameter is automatically declared by the loop_parameter_specification. The scope of a loop parameter extends from the loop_parameter_specification to the end of the loop_statement, and the visibility rules are such that a loop parameter is only visible within the sequence_of_statements of the loop.

Implementation Note: An implementation could give a warning if a variable is hidden by a loop_parameter_specification.

NOTE 3 The discrete_subtype_definition of a for loop is elaborated just once. Use of the reserved word reverse does not alter the discrete subtype defined, so that the following iteration_schemes are not equivalent; the first has a null range.
for J in reverse 1 .. 0
for J in 0 .. 1

Rambification: If a loop_parameter_specification has a static discrete range, the subtype of the loop parameter is static.

Examples

Example of a loop statement without an iteration scheme:

loop
  Get(Current_Character);
  exit when Current_Character = '"';
end loop;

Example of a loop statement with a while iteration scheme:

while Bid(N).Price < Cut_Off.Price loop
  Record_Bid(Bid(N).Price);
  N := N + 1;
end loop;

Example of a loop statement with a for iteration scheme:

for J in Buffer'Range loop
  -- works even with a null range
  if Buffer(J) /= Space then
    Put(Buffer(J));
  end if;
end loop;

Example of a loop statement with a name:

Summation:
  while Next /= Head loop
    Sum := Sum + Next.Value;
    Next := Next.Succ;
  end loop Summation;

Example of a simple parallel loop:

-- see 3.6
parallel
  for I in Grid'Range(1) loop
    Grid(I, 1) := (for all J in Grid'Range(2) => Grid(I,J) = True);
  end loop;

Example of a parallel loop with a chunk specification:

declare
  subtype Chunk_Number is Natural range 1 .. 8;
  Partial Sum,
  Partial Max : array (Chunk_Number) of Natural := (others => 0);
  Partial Min : array (Chunk_Number) of Natural :=
    (others => Natural'Last);
begin
  parallel (Chunk in Chunk_Number)
    for I in Grid'Range(1) loop
      declare
        True_Count : constant Natural :=
          (for J in Grid'Range(2) =>
            (if Grid (I, J) then 1 else 0))'Reduce("++", 0);
      begin
        Partial Sum (Chunk) := @ + True_Count;
        Partial Min (Chunk) := Natural'Min(@, True_Count);
        Partial Max (Chunk) := Natural'Max(@, True_Count);
      end;
    end loop,

The constant-ness of loop parameters is specified in 3.3, “Objects and Named Numbers”.

Wording Changes from Ada 2005

Generalized iterator specifications are allowed in for loops; these are documented as an extension in the appropriate subclause.

Extensions to Ada 2012

Parallel loops are new.

An iterator filter is now allowed on loop parameter specifications. This is mainly for consistency with aggregate and reduction iterators, where it eliminates the need for temporary objects.

Wording Changes from Ada 2012

Corrigendum: Updated wording of loop execution to use the new term “satisfies the predicates” (see 3.2.4).

Added text so that the nominal subtype of a loop parameter is clearly defined.

5.5.1 User-Defined Iterator Types

Static Semantics

The following language-defined generic library package exists:

```ada
generic
  type Cursor is limited interface;
package Ada.Iterator_Interfaces is
  with Pure, Nonblocking => False
  pragma Pure (Iterator_Interfaces);
  type Forward_Iterator is limited interface;
  function First (Object : Forward_Iterator) return Cursor is abstract;
  function Next (Object : Forward_Iterator; Position : Cursor) return Cursor is abstract;
  type Reversible_Iterator is limited interface and Forward_Iterator;
  function Last (Object : Reversible_Iterator) return Cursor is abstract;
  function Previous (Object : Reversible_Iterator; Position : Cursor) return Cursor is abstract;
  type Parallel_Iterator is limited interface and Forward_Iterator;
  function Is_Split (Object : Parallel_Iterator) return Boolean is abstract;
  procedure Split_Into_Chunks (Object : in out Parallel_Iterator; Max_Chunks : in Chunk_Index) is abstract;
  function Chunk_Count (Object : Parallel_Iterator) return Chunk_Index is abstract;
```

Instead of the `Put_Line` function, you can use the `Partial_Sum` function to calculate sums, along with `Partial_Min` and `Partial_Max` to find minimum and maximum values.

```ada
{AI12-0386-1}
Put_Line
("Total=" & Partial_Sum'Reduce("+", 0)'Image
"; Min=" & Partial_Min'Reduce(Natural'Min, Natural'Last)'Image
"; Max=" & Partial_Max'Reduce(Natural'Max, 0)'Image);
end;
```

For an example of an iterator filter, see 4.5.8.
333      16 October 2023  User-Defined Iterator Types  5.5.1

{AI12-0266-1}  function First (Object : Parallel_Iterator;  
                  Chunk : Chunk_Index) return Cursor is abstract  
    with Pre'Class => (Object.Is_Split and then 
                   Chunk <= Object.Chunk_Count)  
        or else raise Program_Error;  

{AI12-0266-1}  function Next (Object   : Parallel_Iterator;  
                   Position : Cursor; 
                   Chunk    : Chunk_Index) return Cursor is abstract  
    with Pre'Class => (Object.Is_Split and then 
                   Chunk <= Object.Chunk_Count)  
        or else raise Program_Error;  

{AI12-0266-1}  type Parallel_Reversible_Iterator  
  is limited interface and Parallel_Iterator and Reversible_Iterator;  
end Ada.Iterator_Interfaces;  

Reason: {AI12-0241-1}  This package must allow blocking (Nonblocking => False) for compatibility. The purpose of 
                     this package is to provide a template for overriding user-defined routines; and such routines can only allow blocking if 
                     the root type does so. Users can still declare their overriding routines nonblocking if they wish.  

{AI05-0139-2}  An iterator type is a type descended from the Forward_Iterator interface 
                     from some instance of Ada.Iterator_Interfaces. A reversible iterator type is a type descended from the 
                     Reversible_Iterator interface from some instance of Ada.Iterator_Interfaces. A parallel iterator type is a 
                     type descended from the Parallel_Iterator interface from some instance of Ada.Iterator_Interfaces. A type 
                     descended from the Parallel_Reversible_Iterator interface from some instance of Ada.Iterator_Interfaces 
                     is both a parallel iterator type and a reversible iterator type. An iterator object is an object of an iterator 
                     type. A reversible iterator object is an object of a reversible iterator type. A parallel iterator object is an 
                     object of a parallel iterator type. The formal subtype Cursor from the associated instance of 
                     Ada.Iterator_Interfaces is the iteration cursor subtype for the iterator type.  

{AI05-0139-2}  The following type-related operational aspects may be specified for an 
                     indexable container type T (see 4.1.6):  

{AI12-0111-1}  Default_Iterator  
  This aspect is specified by a name that denotes exactly one function declared immediately 
  within the same declaration list in which T, or the declaration completed by T, is declared, 
  whose first parameter is of type T or T'Class or an access parameter whose designated type is 
  type T or T'Class, whose other parameters, if any, have default expressions, and whose result 
  type is an iterator type. This function is the default iterator function for T. Its result subtype is 
  the default iterator subtype for T. The iteration cursor subtype for the default iterator subtype 
  is the default cursor subtype for T. This aspect is inherited by descendants of type T 
  (including T'Class).  

Aspect Description for Default_Iterator: Default iterator to be used in for loops.  
Reason: {AI22-0002-1}  {AI22-0005-1}  For a function that has a parameter of T or access T, a blanket rule in 13.1.1 
                     requires the function to be a primitive operation of T, the wording about the same declaration list is redundant in that 
                     case. That 13.1.1 rule does not apply to functions that have parameters of T'Class or access T'Class (which is good, as 
                     those can never be primitive); the wording about the declaration list is necessary in that case.  

{AI12-0111-1}  Iterator_Element  
  This aspect is specified by a name that denotes a subtype. This is the default element subtype 
  for T. This aspect is inherited by descendants of type T (including T'Class).  

Aspect Description for Iterator_Element: Element type to be used for user-defined iterators.  

{AI12-0111-1}  Iterator_View  
  This aspect is specified by a name that denotes a type T2 with the following properties: 
  • T2 is declared in the same compilation unit as T; 
  • T2 is an iterable container type; 
  • T2 has a single discriminant which is an access discriminant designating T; and 

333      16 October 2023  User-Defined Iterator Types  5.5.1
The default iterator subtypes for \( T \) and \( T_2 \) statically match.

This aspect is never inherited, even by \( T\text{Class} \).

**Reason:** Iterator View allows specifying an alternative type to be automatically used by container element iterators; see 5.5.2. This allows setting state for an iteration only once rather than for each individual reference.

**Ramification:** Since Iterator View is not inherited, it does not apply to \( T\text{Class} \). Otherwise, the type of the iterator object would not be known at compile-time (since it necessarily has to be different for each descendant).

**Aspect Description for Iterator View:** An alternative type to used for container element iterators.

This paragraph was deleted.\[AI12-0111-1\] These aspects are inherited by descendants of type \( T \) (including \( T\text{Class} \)).

\{AI05-0139-2\} \{AI05-0292-1\} \{AI12-0266-1\} An iterable container type is an indexable container type with specified Default_Iterator and Iterator_Element aspects. A reversible iterable container type is an iterable container type with the default iterator type being a reversible iterator type. A parallel iterable container type is an iterable container type with the default iterator type being a parallel iterator type. An iterable container object is an object of an iterable container type. A reversible iterable container object is an object of a reversible iterable container type. A parallel iterable container object is an object of a parallel iterable container type.

**Term entry:** iterable container type — type that has user-defined behavior for iteration, via the Default_Iterator and Iterator_Element aspects

\{AI12-0138-1\} The Default_Iterator and Iterator_Element aspects are nonoverridable (see 13.1.1).

**Reason:** This ensures that all descendants of an iterable container type have aspects with the same properties. This prevents generic contract problems with formal derived types.

**Legality Rules**

\{AI05-0139-2\} \{AI05-0292-1\} The Constant_Indexing aspect (if any) of an iterable container type \( T \) shall denote exactly one function with the following properties:

- the result type of the function is covered by the default element type of \( T \) or is a reference type (see 4.1.5) with an access discriminant designating a type covered by the default element type of \( T \);
- the type of the second parameter of the function covers the default cursor type for \( T \);
- if there are more than two parameters, the additional parameters all have default expressions.

This function (if any) is the default constant indexing function for \( T \).

**Ramification:** This does not mean that Constant_Indexing has to designate only one subprogram, only that there is only one routine that meets all of these properties. There can be other routines designated by Constant_Indexing, but they cannot have the profile described above. For instance, map containers have a version of Constant_Indexing that takes a key instead of a cursor; this is allowed.

\{AI05-0139-2\} \{AI05-0292-1\} The Variable_Indexing aspect (if any) of an iterable container type \( T \) shall denote exactly one function with the following properties:

- the result type of the function is a reference type (see 4.1.5) with an access discriminant designating a type covered by the default element type of \( T \);
- the type of the second parameter of the function covers the default cursor type for \( T \);
- if there are more than two parameters, the additional parameters all have default expressions.

This function (if any) is the default variable indexing function for \( T \).
Erroneous Execution

{AI12-0354-1} A call on the First or Next operation on a given Parallel Iterator object with a given Chunk value, which does not propagate an exception, should return a Cursor value that either yields False when passed to Has Element, or that identifies an element distinct from any Cursor value returned by a call on a First or Next operation on the same Parallel Iterator object with a different Chunk value. If the First or Next operations with a Chunk parameter behave in any other manner, execution is erroneous.

Reason: This describes the expectations from a user-written parallel iterator. If the expectations are not met, execution is erroneous so that implementations do not need to go to heroic efforts to avoid problems caused by bad iterators. This is similar to the handling of storage pools, see 13.11.

Extensions to Ada 2005

{AI05-0139-2} User-defined iterator types are new in Ada 2012.

Incompatibilities With Ada 2012

{AI12-0138-1} Corrigendum: Defined Default Iterator and Iterator Element to be nonoverridable, which makes redefinitions and hiding of these aspects illegal. It's possible that some program could violate one of these new restrictions, but in most cases this can easily be worked around by using overriding rather than redefinition.

{AI12-0266-1} Various new types and subprograms are newly added to Ada.Iterator_Interfaces. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

Extensions to Ada 2012

{AI12-0111-1} Aspect Iterator_View is new; it allows container element iterators to set the tampering state once rather than for each use of the element.

{AI12-0266-1} {AI12-0354-1} Parallel iterator interfaces are new; they allow user-defined parallel loops to be defined.

5.5.2 Generalized Loop Iteration

{AI05-0139-2} Generalized forms of loop iteration are provided by an iterator_specification.

Syntax

{AI05-0139-2} {AI05-0292-1} {AI12-0156-1} {AI12-0250-1} iterator_specification ::= _defining_identifier [: loop_parameter_subtype_indication] in [reverse] iterator_name _[iterator_filter] _| defining_identifier [: loop_parameter_subtype_indications subtype_indication] of [reverse] iterable_name _[iterator_filter] _

{AI12-0156-1} loop_parameter_subtype_indication ::= subtype_indication [ access_definition

{AI12-0266-1} If an iterator_specification is for a parallel construct, the reserved word reverse shall not appear in the iterator_specification.

Name Resolution Rules

{AI05-0139-2} {AI05-0292-1} For the first form of iterator_specification, called a generalized iterator, the expected type for the iterator_name is any iterator type. For the second form of iterator_specification, the expected type for the iterable_name is any array or iterable container type. If the iterable_name denotes an array object, the iterator_specification is called an array_component iterator; otherwise it is called a container_element iterator.

Term entry: iterator — construct that is used to loop over the elements of an array or container

Note: Iterators can be user defined, and can perform arbitrary computations to access elements from a container.
Legality Rules

If the reserved word `reverse` appears, the iterator specification is a reverse iterator. If the iterator specification is for a parallel construct, the iterator specification is a parallel iterator. Otherwise, it is a forward iterator. Forward and reverse iterators are collectively called sequential iterators. In a reverse generalized iterator, the iterator name shall be of a reversible iterator type. In a parallel generalized iterator, the iterator name shall be of a parallel iterator type. In a reverse container element iterator, the default iterator type for the type of the `iterable_name` shall be a reversible iterator type. In a parallel container element iterator, the default iterator type for the type of the `iterable_name` shall be of a parallel iterator type.

The subtype defined by the loop parameter subtype indication, if any, of a generalized iterator shall statically match the iteration cursor subtype. The subtype defined by the loop parameter subtype indication, if any, of an array component iterator shall statically match the component subtype of the type of the `iterable_name`. The subtype defined by the loop parameter subtype indication, if any, of a container element iterator shall statically match the default element subtype for the type of the `iterable_name`.

In a container element iterator whose `iterable_name` has type `T`, if the `iterable_name` denotes a constant or the Variable Indexing aspect is not specified for `T`, then the Constant Indexing aspect shall be specified for `T`.

The iterator name or `iterable_name` of an iterator specification shall not denote an object for which renaming is allowed (see 8.5.1) a subcomponent that depends on discriminants of an object whose nominal subtype is unconstrained, unless the object is known to be constrained.

Reason: This prevents the same rule that applies to renames; it serves the same purpose of preventing the object from disappearing while the iterator is still using it.

A container element iterator is illegal if the call of the default iterator function that creates the loop iterator (see below) is illegal.

Ramification: This can happen if the parameter to the default iterator function is in out and the `iterable_name` is a constant. The wording applies to any reason that the call would be illegal, as it's possible that one of the default parameters would be illegal, or that some accessibility check would fail.

A generalized iterator is illegal if the iteration cursor subtype of the `iterator_name` is a limited type at the point of the generalized iterator. A container element iterator is illegal if the default cursor subtype of the type of the `iterable_name` is a limited type at the point of the container element iterator.

Reason: If the cursor type is limited, the assignment to the loop parameter for a generalized iterator would be illegal. The same is true for a container element iterator. We have to say "at the point of the iterator" as the limitedness of a type can change due to visibility.

Static Semantics

An iterator specification declares a loop parameter. In a generalized iterator, the nominal subtype of the loop parameter is the iteration cursor subtype. In an array component iterator, or a container element iterator, if a loop parameter subtype indication is present, it determines the nominal subtype of the loop parameter. In a generalized iterator, if a loop parameter subtype indication is not present, the nominal subtype of the loop parameter is the iteration cursor subtype. In an array component iterator, if a loop parameter subtype indication is not present, the nominal subtype of the loop parameter is the component subtype of the type of the `iterable_name`. In a container element iterator, if a
loop parameter subtype indications subtype indication is not present, the nominal subtype of the loop parameter is the default element subtype for the type of the iterable_name.

\texttt{10.5-0139-2} \texttt{10.5-0292-1} In a generalized iterator, the loop parameter is a constant. In an array component iterator, the loop parameter is a constant if the iterable_name denotes a constant; otherwise it denotes a variable. In a container element iterator, the loop parameter is a constant if the iterable_name denotes a constant, or if the Variable_ Indexing aspect is not specified for the type of the iterable_name; otherwise it is a variable.

\textbf{Ramification:} \texttt{10.12-0093-1} \texttt{10.12-0156-1} The loop parameter of a generalized iterator has the same accessibility as the loop statement. This means that the loop parameter object is finalized when the loop statement is left. (It also may be finalized as part of assigning a new value to the loop parameter.) For array component iterators and container element iterators, the loop parameter directly denotes an element of the array or container and has the accessibility of the associated array or container. For container element iterators, the loop parameter denotes the result of the indexing function call (in the case of a constant indexing) or a generalized reference thereof (in the case of a variable indexing). Roughly speaking, the function result (or the generalized reference thereof) is considered to be renamed in the declarative part of a notional block statement which immediately encloses the loop's sequence of statements; the accessibility of the loop parameter is that of the block statement.

\textbf{Dynamic Semantics}

\texttt{10.5-0139-2} For the execution of a loop statement with an iterator specification, the iterator specification is first elaborated. This elaboration elaborates the subtype indication, if any.

\texttt{10.5-0139-2} \texttt{10.11-0250-1} \texttt{10.11-0266-1} For a sequential generalized iterator, the loop parameter is created, the iterator name is evaluated, and the denoted iterator object becomes the loop iterator. In a forward generalized iterator, the operation First of the iterator type is called on the loop iterator, to produce the initial value for the loop parameter. If the result of calling Has_Element on the initial value is False, then the execution of the loop statement is complete. Otherwise, the sequence of statements is conditionally executed and then the Next operation of the iterator type is called with the loop iterator and the current value of the loop parameter to produce the next value to be assigned to the loop parameter. This repeats until the result of calling Has_Element on the loop parameter is False, or the loop is left as a consequence of a transfer of control. For a reverse generalized iterator, the operations Last and Previous are called rather than First and Next.

\textbf{Ramification:} \texttt{10.12-0093-1} The loop parameter of a generalized iterator is a variable of which the user only has a constant view. It follows the normal rules for a variable of its nominal subtype. In particular, if the nominal subtype is indefinite, the variable is constrained by its initial value. Similarly, if the nominal subtype is class-wide, the variable (like all variables) has the tag of the initial value. Constraint Error may be raised by a subsequent iteration if Next or Previous return an object with a different tag or constraint.

\texttt{10.11-0266-1} For a parallel generalized iterator, the chunk specification, if any, of the associated parallel construct, is first elaborated, to determine the maximum number of chunks (see 5.5), and then the operation Split Into Chunks of the iterator type is called, with the determined maximum passed as the Max_Chunks parameter, specifying the upper bound for the number of loop parameter objects (and the number of logical threads of control) to be associated with the iterator. In the absence of a chunk specification, the maximum number of chunks is determined in an implementation-defined manner.

\textbf{Implementation defined:} The maximum number of chunks for a parallel generalized iterator without a chunk specification.

\textbf{Discussion:} The Max_Chunks parameter of the Split Into Chunks procedure is an upper bound for the number of chunks to be associated with a loop. A container implementation may opt for a lower value for the number of chunks if a more optimal split can be determined. For instance, a tree-based container might create the split based on the number of branches at the top levels of the tree.

\texttt{10.11-0250-1} \texttt{10.11-0266-1} \texttt{10.11-0418-1} Upon return from Split Into Chunks, the actual number of chunks for the loop is determined by calling the Chunk_Count operation of the iterator, at which point
one logical thread of control is initiated for each chunk, with an associated chunk index in the range from one to the actual number of chunks.

Within each logical thread of control, a loop parameter is created. If a chunk specification with a discrete subtype definition is present in the associated parallel construct, then a chunk parameter is created and initialized with a value from the discrete subtype defined by the discrete subtype definition, so that the order of the chosen chunk parameter values correspond to the order of the chunk indices associated with the logical threads of control. The operation First of the iterator type that has a Chunk parameter is called on the loop iterator, with Chunk initialized from the corresponding chunk index, to produce the initial value for the loop parameter. If the result of calling Has Element on this initial value is False, then the execution of the logical thread of control is complete. Otherwise, the sequence of statements is conditionally executed, and then the Next operation of the iterator type that has a Chunk parameter is called with the loop iterator, the current value of the loop parameter, and the corresponding chunk index, to produce the next value to be assigned to the loop parameter. This repeats until the result of calling Has Element on the loop parameter is False, or the associated parallel construct is left as a consequence of a transfer of control.

In the absence of a transfer of control, the associated parallel construct of a parallel generalized iterator is complete when all of its logical threads of control are complete.

For an array component iterator, the chunk specification of the associated parallel construct, if any, is first elaborated to determine the maximum number of chunks (see 5.5), and then the iterable name is evaluated and the denoted array object becomes the array for the loop. If the array for the loop is a null array, then the execution of the loop statement is complete. Otherwise, the sequence of statements is conditionally executed with the loop parameter denoting each component of the array for the loop, using a canonical order of components, which is last dimension varying fastest (unless the array has convention Fortran, in which case it is first dimension varying fastest). For a forward array component iterator, the iteration starts with the component whose index values are each the first in their index range, and continues in the canonical order. For a reverse array component iterator, the iteration starts with the component whose index values are each the last in their index range, and continues in the reverse of the canonical order. For a parallel array component iterator, the iteration is broken up into contiguous chunks of the canonical order, such that all components are covered with no overlaps; each chunk has its own logical thread of control with its own loop parameter and iteration within each chunk is in the canonical order. The number of chunks is implementation defined, but is limited in the presence of a chunk specification to the determined maximum. The loop iteration proceeds until the sequence of statements has been conditionally executed for each component of the array for the loop, or until the loop is left as a consequence of a transfer of control.

Implementation defined: The number of chunks for an array component iterator.

If a chunk specification with a discrete subtype definition is present in the associated parallel construct, then the logical thread of control associated with a given chunk has a chunk parameter initialized with a distinct value from the discrete subtype defined by the discrete subtype definition. The values of the chunk parameters are assigned such that they increase in the canonical order of the starting array components for the chunks.

For a container element iterator, the chunk specification of the associated parallel construct, if any, is first elaborated to determine the maximum number of chunks (see 5.5), and then the iterable name is evaluated. If the container type has Iterator View specified, an object of the Iterator View type is created with the discriminant referencing the iterable container object denoted by the iterable name. This is the iterable container object for the
loop. Otherwise, and the iterable container object denoted by the iterable name becomes the iterable container object for the loop. The default iterator function for the type of the iterable container object for the loop is called on the iterable container object and the result is the loop iterator. For a sequential container element iterator, an object of the default cursor subtype is created (the loop cursor). For a parallel container element iterator, each chunk of iterations will have its own loop cursor, again of the default cursor subtype.

Reason: [AI12-0111-1] If Iterator View is specified, we add an extra object and use that object for this iteration. This allows these iterators to automatically use the stable view (defined in each of the language-defined containers) to do the iteration. That eliminates the need to set and clear the tampering with elements indication each time Reference is called; that eliminates substantial overhead as finalization is typically used to implement the tampering reset.

{AI05-0139-2} {AI05-0292-1} {AI12-0266-1} A container element iterator then proceeds as described above for a generalized iterator, except that each reference to a loop parameter is replaced by a reference to the corresponding loop cursor. For a container element iterator, the loop parameter for each iteration instead denotes the operation First of the iterator type is called on the loop iterator, to produce the initial value for the loop cursor. If the result of calling Has Element on the initial value is False, then the execution of the loop statement is complete. Otherwise, the sequence of statements is executed with the loop parameter denoting an indexing (see 4.1.6) into the iterable container object for the loop, with the only parameter to the indexing being the current value of the loop cursor for the given iteration; then the Next operation of the iterator type is called with the loop iterator and the loop cursor to produce the next value to be assigned to the loop cursor. This repeats until the result of calling Has Element on the loop cursor is False, or until the loop is left as a consequence of a transfer of control. For a reverse container element iterator, the operations Last and Previous are called rather than First and Next. If the loop parameter is a constant (see above), then the indexing uses the default constant indexing function for the type of the iterable container object for the loop; otherwise it uses the default variable indexing function.

Reason: [AI12-0111-1] If Iterator View is specified, we add an extra object and use that object for this iteration. This allows these iterators to automatically use the stable view (defined in each of the language-defined containers) to do the iteration. That eliminates the need to set and clear the tampering with elements indication each time Reference is called; that eliminates substantial overhead as finalization is typically used to implement the tampering reset.

{AI12-0120-1} Any exception propagated by the execution of a generalized iterator or container element iterator is propagated by the immediately enclosing loop statement.

Reason: This text covers exceptions raised by called functions that make up the execution of the iterator as well as exceptions raised by the assignment to the loop parameter or cursor.

Examples

{AI12-0429-1} Example of a parallel generalized loop over an array:

{AI05-0269-1} {AI12-0266-1} {AI12-0429-1} parallel -- Array component iterator example:

for Element of Board loop -- See 3.6.1.
   Element := Element * 2.0; -- Double each element of Board, a two-dimensional array.
end loop;

{AI05-0268-1} {AI12-0429-1} For examples of use of generalized iterators, see A.18.33 and the corresponding container packages in A.18.2 and A.18.3.

Extensions to Ada 2005

{AI05-0139-2} Generalized forms of loop iteration are new.

Incompatibilities With Ada 2012

{AI12-0047-1} Corrigendum: Added a rule to ensure that the object being iterated cannot be a component that could disappear before the loop completes. This could be incompatible by making a loop that was legal (and worked correctly, so long as the enclosing object is not modified during the loop) from the original Ada 2012 illegal in corrected Ada 2012. Such loops should be pretty rare, especially as these iterator forms are new to Ada 2012.

{AI12-0120-1} Corrigendum: Added rules to reject loops if the call to the default iterator function for a container element iterator is illegal, or if the cursor type of an iterator is limited. These are formally incompatible with original Ada 2012, but as it's unlikely that any Ada 2012 compiler ever allowed the illegal usages in an expansion of a loop (it's
much more likely that they would have just caused an internal error in the compiler), this should have no effect in practice.

\{AI12-0151-1\} Corrigendum: Added a requirement that the given subtype statically match the subtype of the element or component for a component element iterator or array component iterator. Original Ada 2012 text allowed any type that covered the subtype of the element or component, but that led to questions of what the meaning was if they are different. In this case, the element is essentially a renaming of the container element, and it doesn’t make sense for the constraints to be different. Ignoring explicitly defined constraints in renames is a mistake that we don’t want to continue, thus we require static matching. This means that some programs might be illegal, but those programs were misleading at best, and potentially would raise unexpected exceptions because the element values might have been invalid or abnormal with respect to the declared constraint.

Extensions to Ada 2012

\{AI12-0156-1\} For consistency, we now allow a subtype indication on a generalized iterator, and anonymous access types on all forms of iterator. We introduced a new syntax non-terminal, loop_parameter_subtype_indication to simplify the wording.

\{AI12-0250-1\} An iterator filter is now allowed on iterator specifications. This is mainly for consistency with aggregate and reduction iterators, where it eliminates the need for temporary objects.

Wording Changes from Ada 2012

\{AI12-0120-1\} Corrigendum: Added wording to specify that a loop propagates any exceptions propagated by the execution of an iterator. Since that’s what naturally would happen from a macro-style expansion of the parts of an iterator, and no other interpretation makes sense given the way the rest of Ada works, we consider it so unlikely that any Ada 2012 implementation ever did anything else that we don’t document this as a possible inconsistency.

\{AI12-0111-1\} Added wording to include the use of the iterator view in a container element iterator.

\{AI12-0266-1\} Added wording to describe the execution of parallel iterators.

Incompatibilities With Ada 2022

\{AI22-0030-1\} Corrigendum: Made the requirement that the iterator object has be able able to be renamed, in order to ensure that all renaming rules are imported. We use this formulation elsewhere in the RM, so it is appropriate here, too. The effect of this rule change is that a program that does an array iteration over a slice of an object that is not allowed to be renamed is legal in original Ada 2022 (but dubious in execution), but illegal in Ada 202y.

5.5.3 Procedural Iterators

\{AI12-0189-1\} A procedural iterator invokes a user-defined procedure, passing in the body of the enclosing loop statement as a parameter of an anonymous access-to-procedure type, to allow the loop body to be executed repeatedly as part of the invocation of the user-defined procedure.

Syntax

\{AI12-0189-1\} \{AI12-0250-1\} procedural_iterator ::= 
    iterator_parameter_specification of iterator_procedure_call
    [iterator_filter]

\{AI12-0189-1\} \{AI12-0308-1\} iterator_parameter_specification ::= 
    formal_part
    | (defining_identifier\, defining_identifier)

\{AI12-0189-1\} iterator_procedure_call ::= 
    procedure_name
    | procedure_prefix iterator_actual_parameter_part

\{AI12-0189-1\} iterator_actual_parameter_part ::= 
    (iterator_parameter_association \, iterator_parameter_association)

\{AI12-0189-1\} iterator_parameter_association ::= 
    parameter_association
parameter_association_with_box

\{AI12-0189-1\} \textbf{parameter association with box} ::=  
\left[ \text{formal parameter selector name} \Rightarrow \text{box} \right] \textless \textgreater 

\{AI12-0189-1\} \textbf{At most one iterator parameter association within an iterator actual parameter part shall be a parameter association with box.}

\textbf{Name Resolution Rules}

\{AI12-0189-1\} \{AI12-0292-1\} \{AI12-0326-2\} The name or prefix given in an iterator procedure call shall resolve to denote a callable entity \(C\) (the iterating procedure) that is a procedure, or an entry renamed as (viewed as) a procedure. [When there is an iterator actual parameter part, the prefix can be an implicit dereference of an access-to-subprogram value.]

\{AI12-0189-1\} An iterator procedure call without a parameter association with box is equivalent to one with an iterator actual parameter part with an additional parameter association with box at the end, with the formal parameter selector name identifying the last formal parameter of the callable entity denoted by the name or prefix.

\{AI12-0189-1\} \{AI12-0320-1\} An iterator procedure call shall contain at most one iterator parameter association for each formal parameter of the callable entity \(C\). Each formal parameter without an iterator parameter association shall have a default expression (in the profile of the view of \(C\) denoted by the name or prefix).

\{AI12-0189-1\} The formal parameter of the callable entity \(C\) associated with the parameter association with box shall be of an anonymous access-to-procedure type \(A\).

\textbf{Legality Rules}

\{AI12-0189-1\} \{AI12-0308-1\} The anonymous access-to-procedure type \(A\) shall have at least one formal parameter in its parameter profile. If the iterator parameter specification is a formal part, then this formal part shall be mode conformant with that of \(A\). If the iterator parameter specification is a list of defining identifiers, the number of formal parameters of \(A\) shall be the same as the length of this list.

\{AI12-0189-1\} \{AI12-0292-1\} [If the name or prefix given in an iterator procedure call denotes an abstract subprogram, the subprogram shall be a dispatching subprogram.]

\textbf{Proof:} \{AI12-0320-1\} This is stated normatively in 3.9.3.

\textbf{Static Semantics}

\{AI12-0189-1\} \{AI12-0250-1\} \{AI12-0308-1\} \{AI12-0326-2\} A loop statement with an iteration scheme that has a procedural iterator is equivalent to a local declaration of a procedure \(P\) followed by a procedure call statement that is formed from the iterator procedure call by replacing the \textless \textgreater of the parameter association with box with \(P'\text{Access}\). The formal part of the locally declared procedure \(P\) is formed from the formal part of the anonymous access-to-procedure type \(A\), by replacing the identifier of each formal parameter of this formal part with the identifier of the corresponding formal parameter or element of the list of defining identifiers given in the iterator parameter specification. The body of \(P\) consists of the conditionally executed sequence of statements. The procedure \(P\) is called the loop body procedure.

\textbf{Implementation Note:} \{AI12-0250-1\} For a procedural iterator with an iterator filter, the body of the routine would be something like:
procedure P ... is
begin
  if iterator_filter then
    sequence_of_statements
  end if;
end P;

{AI12-0344-1} In a procedural iterator, the Parallel_Calls aspect (see 9.10.1) of the loop body procedure is True if the reserved word parallel occurs in the corresponding loop statement, and False otherwise.

{AI12-0189-1} {AI12-0326-2} {AI12-0344-1} The following aspects may be specified for a callable entity \( S \) that has exactly one formal parameter of an anonymous access-to-subprogram type:

**Allows Exit**

The Allows Exit aspect is of type Boolean. The specified value shall be static. The Allows Exit aspect of an inherited primitive subprogram is True if Allows Exit is True either for the corresponding subprogram of the progenitor type or for any other inherited subprogram that it overrides. If not specified or inherited as True, the Allows Exit aspect of a callable entity is False. For an entry, only a confirming specification of False is permitted for the Allows Exit aspect.

**Reason:** An entry does not allow exit, because implementing a transfer of control out of a task or protected entry creates unnecessarily complex dynamic semantics.

**Aspect Description for Allows Exit:** An indication of whether a subprogram will operate correctly for arbitrary transfers of control.

**Ramification:** A subprogram that does not need cleanup satisfies the requirements, and thus can specify Allows Exit as True. If a subprogram \( S \) allows exit, it cannot expect to get control other than via finalization if the loop body procedure initiates a transfer of control as part of a procedural iterator. In particular, exception handlers in \( S \), even when others handlers, will not be executed when a transfer of control occurs. The mechanism that the implementation uses to implement such transfers of control needs to avoid triggering exception handlers.

**Parallel Iterator**

The Parallel Iterator aspect is of type Boolean. The specified value shall be static. The Parallel Iterator aspect of an inherited primitive subprogram is True if Parallel Iterator is True either for the corresponding subprogram of the progenitor type or for any other inherited subprogram that it overrides. If not specified or inherited as True, the Parallel Iterator aspect of a callable entity is False.

{AI12-0189-1} {AI12-0442-1} Specifying the Parallel Iterator aspect to be True for a callable entity indicates that the entity is allowed to invoke the loop body procedure from multiple distinct logical threads of control. The Parallel Iterator aspect for a subprogram shall be statically False if the subprogram allows exit.

**Aspect Description for Parallel Iterator:** An indication of whether a subprogram may use multiple threads of control to invoke a loop body procedure.

**Reason:** Permitting exit from a parallel procedural iterator introduces additional semantic and implementation complexity.

**Legality Rules**

{AI12-0189-1} {AI12-0326-2} If a callable entity overrides an inherited dispatching subprogram that allows exit, the overriding callable entity also shall allow exit. If a callable entity overrides an inherited dispatching subprogram that has a True Parallel Iterator aspect, the overriding callable entity also shall have a True Parallel Iterator aspect.
Ramification: Since an entry never allows exit, attempting to implement an allows exit subprogram with a task or protected entry is always illegal. However, the Parallel Iterator aspect can be applied to an entry, so a subprogram with the Parallel Iterator aspect True can be implemented by an entry.

\{AI12-0326-2\} A loop statement with a procedural iterator as its iteration scheme shall begin with the reserved word parallel if and only if the callable entity identified in the iterator procedure call has a Parallel_iterator aspect of True.

\{AI12-0326-2\} If the actual parameter of an anonymous access-to-subprogram type, passed in an explicit call of a subprogram for which the Parallel Iterator aspect is True, is of the form P\texttt{Access}, the designated subprogram P shall have a Parallel_Calls aspect True (see 9.10.1).

\{AI12-0189-1\} \{AI12-0326-2\} The sequence of statements of a loop statement with a procedural iterator as its iteration scheme shall contain an exit statement, return statement, goto_statement, or requeue_statement that leaves the loop only if the callable entity associated with the procedural iterator allows exit.

\{AI12-0294-1\} The sequence of statements of a loop statement with a procedural iterator as its iteration scheme shall not contain an accept statement whose entry declaration occurs outside the loop_statement.

Reason: An accept_statement is not allowed in a procedure (see 9.5.2), it has to be directly in a task_body. Since the loop body here is implemented as a procedure, we can't allow accept statements there, either, even if the loop itself is directly in a task_body.

Ramification: This includes cases where the accept_statement is part of another construct, for instance, a select_statement.

Dynamic Semantics

\{AI12-0326-2\} \{AI12-0355-2\} \{AI12-0445-1\} [For the execution of a loop statement with an iteration scheme that has a procedural iterator, the procedure denoted by the name or prefix of the iterator procedure call (the iterating procedure) is invoked, passing an access value designating the loop body procedure as a parameter. The iterating procedure then calls the loop body procedure zero or more times and returns, whereupon the loop_statement is complete. If the parallel reserved word is present, the iterating procedure is allowed to invoke the loop body procedure from multiple distinct logical threads of control.] The aspect_specification, if any, is elaborated prior to the invocation of the iterating procedure.

Proof: The stated dynamic semantics are implied by the static semantics given above and the bounded errors given below.

Bounded (Run-Time) Errors

\{AI12-0326-2\} \{AI12-0445-1\} If the callable entity identified in the iterator procedure call allows exit, then it is a bounded error for a call of the loop body procedure to be performed from within an abort-deferred operation (see 9.8), unless the entire loop_statement was within the same abort-deferred operation. If detected, Program_Error is raised at the point of the call; otherwise, a transfer of control from the sequence of statements of the loop_statement will not necessarily terminate the loop_statement, and the loop body procedure can be called again.

\{AI12-0326-2\} \{AI12-0445-1\} If a loop_statement with the procedural iterator as its iteration scheme (see 5.5) does not begin with the reserved word parallel, it is a bounded error if the loop body procedure is invoked from a different logical thread of control than the one that initiates the loop_statement. If detected, Program_Error is raised; otherwise, conflicts associated with concurrent executions of the loop body procedure can occur without being detected by the applicable conflict check policy (see 9.10.1). Furthermore, propagating an exception or making an attempt to exit in the presence of multiple threads of
control will not necessarily terminate the loop statement, deadlock can occur, or the loop body procedure can be called again.

Discussion: [AI12-0326-2] Other Ada rules are still in effect for the allows exit subprogram A, of course. For instance, if a transfer of control causes finalization which raises an exception, Program_Error will be propagated by A (rather than the transfer of control). In such a case, the bounded error above would still apply. Another example is the case where an unrelated task is waiting on the normal completion of the loop body procedure call in A. Such a task might end up waiting forever if a transfer of control happens (this is a deadlock situation). This case does not require additional wording, as the same thing would happen if an exception is propagated from the loop body procedure or if A executed a transfer of control (such as a return statement).

Examples

{AI12-0189-1} {AI12-0379-1} {AI12-0429-1} Example of iterating over a map from My_Key_Type to My_Element_Type (see A.18.4):

\begin{verbatim}
for C : Cursor of My_Map.Iterate loop
    Put_Line (My_Key_Type'Image (Key (C)) & " => " &
              My_Element_Type'Image (Element (C)));
end loop;
-- The above is equivalent to:
declare
    procedure P (C : Cursor) is
    begin
        Put_Line (My_Key_Type'Image (Key (C)) & " => " &
                   My_Element_Type'Image (Element (C)));
    end P;
begin
    My_Map.Iterate (P'Access);
end;
\end{verbatim}

{AI12-0189-1} {AI12-0429-1} Example of iterating over the environment variables (see A.17):

\begin{verbatim}
for Name, Val of Ada.Environment_Variables.Iterate<> loop
    Put_Line (Name & " => " & Val);
end loop;
-- The above is equivalent to:
declare
    procedure P (Name : String; Val : String) is
    begin
        Put_Line (Name & " => " & Val);
    end P;
begin
    Ada.Environment_Variables.Iterate (P'Access);
end;
\end{verbatim}

Extensions to Ada 2012

{AI12-0189-1} {AI12-0292-1} {AI12-0294-1} {AI12-0326-2} {AI12-0344-1} Procedural iterators, and the Allows_Exit and Parallel_Iterator aspects are new in Ada 2022.

5.6 Block Statements

[A block_statement encloses a handled_sequence_of_statements optionally preceded by a declarative_part.]

\[\text{Syntax}\]

\begin{verbatim}
block_statement ::= [block_statement_identifier:] [declare declarative_part]
\end{verbatim}
begin
  handled_sequence_of_statements
end [block_identifier];

If a block_statement has a block_statement_identifier, then the identifier shall be repeated after the end; otherwise, there shall not be an identifier after the end.

Static Semantics

A block_statement that has no explicit declarative_part has an implicit empty declarative_part.

Ramification: Thus, other rules can always refer to the declarative_part of a block_statement.

Dynamic Semantics

The execution of a block_statement consists of the elaboration of its declarative_part followed by the execution of its handled_sequence_of_statements.

Examples

Example of a block statement with a local variable:

Swap:

```
declare
  Temp : Integer;
begin
  Temp := V; V := U; U := Temp;
end Swap;
```

Ramification: If task objects are declared within a block_statement whose execution is completed, the block_statement is not left until all its dependent tasks are terminated (see 7.6). This rule applies to completion caused by a transfer of control.

Within a block_statement, the block name can be used in expanded names denoting local entities such as Swap.Temp in the above example (see 4.1.3).

Wording Changes from Ada 83

The syntax rule for block_statement now uses the syntactic category handled_sequence_of_statements.

5.6.1 Parallel Block Statements

A parallel block_statement comprises two or more sequence_of_statements separated by and where each represents an independent activity that is intended to proceed concurrently with the others.

Syntax

```
{AI12-0119-1} {AI12-0436-1} parallel_block_statement ::= parallel [[chunk_specification]] [aspect_specification] do
  _sequence_of_statements
  and
  _sequence_of_statements
  {and
    _sequence_of_statements};
end do;
```

The chunk_specification, if any, of a parallel block_statement shall be an integer simple expression.
Dynamic Semantics

For the execution of a parallel block statement, the chunk specification and the aspect specification, if any, are elaborated in an arbitrary order. After elaborating the chunk specification, if any, a check is made that the determined maximum number of chunks is greater than zero. If this check fails, Program_Error is raised.

Then, the various sequence of statements are grouped into one or more chunks, each with its own logical thread of control (see Clause 9), up to the maximum number of chunks specified by the chunk specification, if any. Within each chunk every sequence of statements of the chunk is executed in turn, in an arbitrary order. The parallel block statement is complete once every one of the sequence of statements has completed, either by reaching the end of its execution, or due to a transfer of control out of the construct by one of the sequence of statements (see 5.1).

Implementation Note: Although each sequence of statements of a parallel block represents a separate logical thread of control, the implementation may choose to combine two or more such logical threads of control into a single physical thread of control to reduce the cost of creating numerous physical threads of control.

Examples

Example of a parallel block used to walk a binary tree in parallel:

BEGIN
  IF T /= null AND
     T.all IN Binary_Operation'Class -- see 3.9.1
  THEN -- recurse down the binary tree
    PARALLEL DO
      TRAVERSE (T.Left);
      AND
      TRAVERSE (T.Right);
      AND
      Ada.Text_IO.Put_Line ("Processing " & Ada.Tags.Expanded_Name (T'Tag));
    END DO;
  END IF;
END Traverse;
Example of a parallel block used to search two halves of a string in parallel:

function Search (S : String; Char : Character) return Boolean is
begin
  if S'Length <= 1000 then
    -- Sequential scan
    return (for some C of S => C = Char);
  else
    -- Parallel divide and conquer
    declare
      Mid : constant Positive := S'First + S'Length/2 - 1;
    begin
      parallel do
        for C of S(S'First .. Mid) loop
          if C = Char then
            return True; -- Terminates enclosing do
        end if;
        end loop;
        and
        for C of S(Mid + 1 .. S'Last) loop
          if C = Char then
            return True; -- Terminates enclosing do
        end if;
        end loop;
      end do;
      -- Not found
      return False;
    end if;
  end if;
end Search;

Extensions to Ada 2012

The parallel_block_statement is new.

5.7 Exit Statements

[An exit_statement is used to complete the execution of an enclosing loop_statement; the completion is conditional if the exit_statement includes a condition.]

Syntax

exit_statement ::= exit [loop_name] [when condition];

Name Resolution Rules

The loop_name, if any, in an exit_statement shall resolve to denote a loop_statement.

Legality Rules

Each exit_statement applies to a loop_statement; this is the loop_statement being exited. An exit_statement with a name is only allowed within the loop_statement denoted by the name, and applies to that loop_statement. An exit_statement without a name is only allowed within a loop_statement, and applies to the innermost enclosing one. An exit_statement that applies to a given loop_statement shall not appear within a body or accept_statement, if this construct is itself enclosed by the given loop_statement.
5.7 Exit Statements

For the execution of an **exit_statement**, the **condition**, if present, is first evaluated. If the value of the condition is True, or if there is no condition, a transfer of control is done to complete the **loop_statement**. If the value of the condition is False, no transfer of control takes place.

NOTE Several nested loops can be exited by an **exit_statement** that names the outer loop.

**Examples**

Examples of loops with exit statements:

```ada
for N in 1 .. Max_Num_Items loop
  Get_New_Item(New_Item);
  Merge_Item(New_Item, Storage_File);
  exit when New_Item = Terminal_Item;
end loop;
```

```
Main_Cycle:
loop
  -- initial statements
  exit Main_Cycle when Found;
  -- final statements
end loop Main_Cycle;
```

5.8 Goto Statements

[A **goto_statement** specifies an explicit transfer of control from this **statement** to a target statement with a given **label**.]

**Syntax**

```
goto_statement ::= goto label_name;
```

**Name Resolution Rules**

The **label_name** shall resolve to denote a **label**; the **statement** with that **label** is the **target_statement**.

**Legality Rules**

The innermost **sequence_of_statements** that encloses the target statement shall also enclose the **goto_statement**. Furthermore, if a **goto_statement** is enclosed by an **accept_statement** or a body, then the target statement shall not be outside this enclosing construct.

**Ramification:** The **goto_statement** can be a **statement** of an inner **sequence**.

It follows from the second rule that if the target **statement** is enclosed by such a construct, then the **goto_statement** cannot be outside.

**Dynamic Semantics**

The execution of a **goto_statement** transfers control to the target **statement**, completing the execution of any **compound_statement** that encloses the **goto_statement** but does not enclose the target.

NOTE The above rules allow transfer of control to a **statement** of an enclosing **sequence_of_statements** but not the reverse. Similarly, they prohibit transfers of control such as between alternatives of a **case_statement**, **if_statement**, or **select_statement**, between **exception_handler**s; or from an **exception_handler** of a **handled_sequence_of_statements** back to its **sequence_of_statements**.
Examples

Example of a loop containing a goto statement:

```
<<Sort>>
for I in 1 .. N-1 loop
  if A(I) > A(I+1) then
    Exchange(A(I), A(I+1));
    goto Sort;
  end if;
end loop;
```
6 Subprograms

A subprogram is a program unit or intrinsic operation whose execution is invoked by a subprogram call. There are two forms of subprogram: procedures and functions. A procedure call is a statement; a function call is an expression and returns a value. The definition of a subprogram can be given in two parts: a subprogram declaration defining its interface, and a subprogram_body defining its execution. [Operators and enumeration literals are functions.]

To be honest: A function call is an expression, but more specifically it is a name.

Term entry: subprogram — unit of a program that can be brought into execution in various contexts, with the invocation being a subprogram call that can parameterize the effect of the subprogram through the passing of operands. Note: There are two forms of subprograms: functions, which return values, and procedures, which do not.

Term entry: function — form of subprogram that returns a result and can be called as part of an expression

Term entry: procedure — form of subprogram that does not return a result and can only be invoked by a statement

{AI05-0299-1} A callable entity is a subprogram or entry (see Section 9.5.2). A callable entity is invoked by a call; that is, a subprogram call or entry call. A callable construct is a construct that defines the action of a call upon a callable entity: a subprogram_body, entry_body, or accept_statement.

Ramification: Note that “callable entity” includes predefined operators, enumeration literals, and abstract subprograms. “Call” includes calls of these things. They do not have callable constructs, since they don’t have completions.

6.1 Subprogram Declarations

[A subprogram_declaration declares a procedure or function.]

Syntax

{AI95-00218-03} {AI05-0183-1} subprogram_declaration ::=  
| [overriding_indicator]  
| subprogram_specification  
| [aspect_specification];

This paragraph was deleted.{AI95-00348-01} abstract_subprogram_declaration ::=  
subprogram_specification is abstract;

{AI95-00348-01} subprogram_specification ::=  
| procedure_specification  
| function_specification  
| [overriding_indicator]  
| procedure defining_program_unit_name parameter_profile  
| function defining_designator parameter_and_result_profile

{AI95-00348-01} procedure_specification ::=  
| procedure defining_program_unit_name parameter_profile

{AI95-00348-01} function_specification ::=  
| function defining_designator parameter_and_result_profile

designator ::= [parent_unit_name . ]identifier | operator_symbol

defining_designator ::=  
| defining_program_unit_name | defining_operator_symbol

defining_program_unit_name ::= [parent_unit_name . ]defining_identifier

[The optional parent_unit_name is only allowed for library units (see 10.1.1).]
operator_symbol ::= string_literal

\{AI95-00395-01\} \{AI05-0299-1\} \{AI12-0449-1\} The sequence of characters in an operator_symbol shall form a reserved word, a delimiter, or compound delimiter that corresponds to an operator belonging to one of the six categories of operators defined in subclause 4.5 (spaces are not allowed and the case of letters is not significant).

Reason: \{AI95-00395-01\} \{AI05-0090-1\} The “sequence of characters” of the string literal of the operator is a technical term (see 2.6), and does not include the surrounding quote characters. As defined in 2.2, lexical elements are “formed” from a sequence of characters. Spaces are not allowed, and upper and lower case is not significant. See 2.2 and 2.9 for rules related to the use of other format characters in delimiters and reserved words.

defining_operator_symbol ::= operator_symbol

parameter_profile ::= [formal_part]

\{AI95-00231-01\} \{AI95-00318-02\} parameter_and_result_profile ::= __[formal_part] \textit{return} [null_exclusion] subtype_mark | [formal_part] \textit{return} access_definition

formal_part ::= (parameter_specification {; parameter_specification})


Discussion: \{AI12-0395-1\} Only implementation-defined aspects are allowed on formal parameters in Ada 2022. Implementers are cautioned that any aspect allowed on a formal parameter will need conformance rules. If, for instance, an aspect changed the representation of a parameter, rules would be needed to ensure that the representation is the same for the specification and body.

mode ::= [in] | in out | out

Name Resolution Rules

A formal parameter is an object [directly visible within a subprogram_body] that represents the actual parameter passed to the subprogram in a call; it is declared by a parameter_specification. For a formal parameter, the expected type for its default_expression, if any, is that of the formal parameter.

Legality Rules

\{AI05-0143-1\} The parameter mode of a formal parameter conveys the direction of information transfer with the actual parameter: in, in out, or out. Mode in is the default, and is the mode of a parameter defined by an access_definition. The formal parameters of a function, if any, shall have the mode in.

This paragraph was deleted. Ramification: \{AI05-0143-1\} Access parameters are permitted. This restriction to in parameters is primarily a methodological restriction, though it also simplifies implementation for some compiler technologies.

A default_expression is only allowed in a parameter_specification for a formal parameter of mode in.

\{AI95-00348-01\} \{AI05-0177-1\} \{AI05-0229-1\} A subprogram_declaration or a generic_subprogram_declaration requires a completion: unless the Import aspect (see B.1) is True for the declaration; the completion shall be a body or, a renaming_declaration (see 8.5), or a pragma Import (see B.1). [A completion is not allowed for an abstract_subprogram_declaration (see 3.9.3), or a null procedure_declaration (see 6.7), or an expression_function_declaration (see 6.8).]
Ramification: {AI95-00348-01} {AI05-0177-1} Abstract subprograms and null procedures, and expression functions are not declared by subprogram declarations, and so do not require completion (although the latter two can be completions). Protected subprograms are declared by subprogram declarations, and so require completion. Note that an abstract subprogram is a subprogram, a null procedure is a subprogram, an expression function is a subprogram, and a protected subprogram is a subprogram, but a generic subprogram is not a subprogram.

Proof: {AI05-0229-1} When the Import aspect is True for any entity, no completion is allowed (see B.1).

A name that denotes a formal parameter is not allowed within the formal_part in which it is declared, nor within the formal_part of a corresponding body or accept_statement.

Ramification: By contrast, generic_formal_parameter_declarations are visible to subsequent declarations in the same generic_formal_part.

Static Semantics

The profile of (a view of) a callable entity is either a parameter_profile or parameter_and_result_profile; it embodies information about the interface to that entity — for example, the profile includes information about parameters passed to the callable entity. All callable entities have a profile — enumeration literals, other subprograms, and entries. An access-to-subprogram type has a designated profile.] Associated with a profile is a calling convention. A subprogram_declaration declares a procedure or a function, as indicated by the initial reserved word, with name and profile as given by its specification.

{AI95-00231-01} {AI95-00318-02} The nominal subtype of a formal parameter is the subtype determined denoted by the optional null exclusion and the subtype_mark, or defined by the access_definition, in the parameter_specification. The nominal subtype of a function result is the subtype determined by the optional null exclusion and the subtype_mark, or defined by the access_definition, in the parameter_and_result_profile.

{AI05-0142-4} An explicitly aliased parameter is a formal parameter whose parameter_specification includes the reserved word aliased.

{AI95-00231-01} {AI95-00254-01} {AI95-00318-02} An access parameter is a formal in parameter specified by an access_definition. An access parameter or result_type is of an anonymous access general access-to-variable type (see 3.10). [Access parameters of an access-to-object type allow dispatching calls to be controlled by access values. Access parameters of an access-to-subprogram type permit calls to subprograms passed as parameters irrespective of their accessibility level.]

Discussion: {AI95-00318-02} Access result types have normal accessibility and thus don't have any special properties worth noting here.

The subtypes of a profile are:

- For any non-access parameters, the nominal subtype of the parameter.
- {AI95-00254-01} For any access parameters of an access-to-object type, the designated subtype of the parameter type.
- {AI95-00254-01} {AI05-0164-1} For any access parameters of an access-to-subprogram type, the subtypes of the designated profile of the parameter type.
- {AI95-00231-01} {AI95-00318-02} For any non-access result, the nominal subtype of the function result for any result, the result subtype.
- {AI95-00318-02} For any access result type of an access-to-object type, the designated subtype of the result type.
- {AI95-00318-02} {AI05-0164-1} For any access result type of an access-to-subprogram type, the subtypes of the designated profile of the result type.
The types of a profile are the types of those subtypes.

[AI95-00348-01] {AI05-0177-1} [A subprogram declared by an abstract_subprogram_declaration is abstract; a subprogram declared by a subprogram_declaration is not. See 3.9.3, “Abstract Types and Subprograms”. Similarly, a procedure declared by a null_procedure_declaration is a null procedure; a procedure declared by a subprogram_declaration is not. See 6.7, “Null Procedures”. Finally, a function declared by an expression_function_declaration is an expression function; a function declared by a subprogram_declaration is not. See 6.8, “Expression Functions”.

An overriding_indicator is used to indicate whether overriding is intended. See 8.3.1, “Overriding Indicators”.

The elaboration of a subprogram_declaration or an abstract_subprogram_declaration has no effect.

NOTE 1 A parameter_specification with several identifiers is equivalent to a sequence of single parameter_specifications, as explained in 3.3.

NOTE 2 Abstract subprograms do not have bodies, and cannot be used in a nondispatching call (see 3.9.3, “Abstract Types and Subprograms”).

NOTE 3 The evaluation of default_expressions is caused by certain calls, as described in 6.4.1. They are not evaluated during the elaboration of the subprogram declaration.

NOTE 4 Subprograms can be called recursively and can be called concurrently from multiple tasks.

Examples of subprogram declarations:

procedure Traverse_Tree;
procedure Increment(X : in out Integer);
procedure Right_Indent(Margin : out Line_Size); -- see 3.5.4
procedure Switch(From, To : in out Link); -- see 3.10.1
function Random return Probability; -- see 3.5.7
function Min_Cell(X : Link) return Cell; -- see 3.10.1
function Next_Frame(K : Positive) return Frame; -- see 3.10
function Dot_Product(Left, Right : Vector) return Real; -- see 3.6
function Find(B : aliased in out Barrel; Key : String) return Real; -- see 4.1.5
function "*"(Left, Right : Matrix) return Matrix; -- see 3.6

Examples of in parameters with default expressions:

procedure Print_Header(Pages : in Natural;
Header : in Line := (1 .. Line'Last => ' '); -- see 3.6
Center : in Boolean := True);

Extensions to Ada 83

The syntax for abstract_subprogram_declaration is added. The syntax for parameter_specification is revised to allow for access parameters (see 3.10)

Program units that are library units may have a parent_unit_name to indicate the parent of a child (see 10.1.1 Section 10).

Wording Changes from Ada 83

We have incorporated the rules from RM83-6.5, “Function Subprograms” here and in 6.3, “Subprogram Bodies”

We have incorporated the definitions of RM83-6.6, “Parameter and Result Type Profile - Overloading of Subprograms” here.
The syntax rule for defining_operator_symbol is new. It is used for the defining occurrence of an operator_symbol, analogously to defining_identifier. Usage occurrences use the direct_name or selector_name syntactic categories. The syntax rules for defining_designator and defining_program_unit_name are new.

**Extensions to Ada 95**

- `{AI95-00218-03}` Subprograms now allow overriding_indicators for better error checking of overriding.
- `{AI95-00231-01}` An optional null_exclusion can be used in a formal parameter declaration. Similarly, an optional null_exclusion can be used in a function result.
- `{AI95-00318-02}` The return type of a function can be an anonymous access type.

**Wording Changes from Ada 95**

- `{AI95-00254-01}` A description of the purpose of anonymous access-to-subprogram parameters and the definition of the profile of subprograms containing them was added.
- `{AI95-00348-01}` Split the production for subprogram_specification in order to make the declaration of null procedures (see 6.7) easier.
- `{AI95-00348-01}` Moved the Syntax and Dynamic Semantics for abstract_subprogram_declaration to 3.9.3, so that the syntax and semantics are together. This also keeps abstract and null subprograms similar.
- `{AI95-00395-01}` Revised to allow other_format characters in operator_symbols in the same way as the underlying constructs.

**Extensions to Ada 2005**

- `{AI05-0142-4}` Parameters can now be explicitly aliased, allowing parts of function results to designate parameters and forcing by-reference parameter passing.
- `{AI05-0143-1}` The parameters of a function can now have any mode.
- `{AI05-0183-1}` An optional aspect_specification can be used in a subprogram_declaration. This is described in 13.1.1.

**Wording Changes from Ada 2005**

- `{AI05-0177-1}` Added expression functions (see 6.8) to the wording.

**Extensions to Ada 2012**

- `{AI12-0395-1}` Parameters now can have an aspect_specification, allowing the specification of (implementation-defined) aspects for individual parameters.

### 6.1.1 Preconditions and Postconditions

For a noninstance subprogram [including a generic formal subprogram], a generic subprogram, or an entry, or an access-to-subprogram type, the following language-defined assertion aspects may be specified with an aspect_specification (see 13.1.1):

**Ramification:** `{AI12-0045-1}` “Noninstance subprogram” excludes a subprogram that is an instance of a generic subprogram. In that case, the aspects should be specified on the generic subprogram. If preconditions or postconditions need to be added to an instance of a generic subprogram, it can be accomplished by creating a separate subprogram specification and then completing that specification with a renames-as-body of the instance.

**Proof:** `{AI12-0272-1}` A generic formal subprogram is a subprogram, and there are no rules to prevent using these attributes on it.

- `{AI12-0220-1}` **Pre**
  
  This aspect specifies a specific precondition for a callable entity or an access-to-subprogram type; it shall be specified by an expression, called a specific precondition expression. If not specified for an entity, the specific precondition expression for the entity is the enumeration literal True.
To be honest: In this and the following rules, we are talking about the enumeration literal True declared in package Standard (see A.1), and not some other value or identifier True. That matters as some rules depend on full conformance of these expressions, which depends on the specific declarations involved.

Aspect Description for Pre: Precondition; a condition that is expected to hold true before a call.

This aspect specifies a class-wide precondition for a dispatching operation of a tagged type and its descendants; it shall be specified by an expression, called a class-wide precondition expression. If not specified for an entity, then if no other class-wide precondition applies to the entity, the class-wide precondition expression for the entity is the enumeration literal True.

Ramification: If other class-wide preconditions apply to the entity and no class-wide precondition is specified, no class-wide precondition is defined for the entity; of course, the class-wide preconditions (of ancestors) that apply are still going to be checked. We need subprograms that don't have ancestors and don't specify a class-wide precondition to have a class-wide precondition of True, so that adding such a precondition to a descendant has no effect (necessary as a dispatching call through the root routine would not check any precondition).

Aspect Description for Pre'Class: Precondition that applies to corresponding subprograms of descendant types inherited on type derivation.

This aspect specifies a specific postcondition for a callable entity or an access-to-subprogram type; it shall be specified by an expression, called a specific postcondition expression. If not specified for an entity, the specific postcondition expression for the entity is the enumeration literal True.

Aspect Description for Post: Postcondition; a condition that will hold true after a call.

This aspect specifies a class-wide postcondition for a dispatching operation of a tagged type and its descendants; it shall be specified by an expression, called a class-wide postcondition expression. If not specified for an entity, the class-wide postcondition expression for the entity is the enumeration literal True.

Aspect Description for Post'Class: Postcondition that applies to corresponding subprograms of descendant types inherited on type derivation.

Discussion: In the AARM notes below, we use the terms “inherited” and “inheritance” informally with respect to class-wide pre/post-conditions, to mean that the aspect applies to corresponding subprograms in descendant types.

Term entry: precondition — assertion that is expected to be True when a given subprogram is called

Term entry: postcondition — assertion that is expected to be True when a given subprogram returns normally

Name Resolution Rules

The expected type for a precondition or postcondition expression is any boolean type.

Within the expression for a Pre'Class or Post'Class aspect for a primitive subprogram S of a tagged type T, a name that denotes a formal parameter (or S'Result) of type T is interpreted as though it had a (notional) nonabstract type NT that is a formal derived type whose ancestor type is T, with directly visible primitive operations having type T'Class. Similarly, a name that denotes a formal access parameter (or S'Result for an access result) of type access-to-T is interpreted as having type access-to-NT'Class. [The result of this interpretation is that the only operations that can be applied to such names are those defined for such a formal derived type. This ensures that the expression is well-defined for a primitive subprogram of a type descended from T.]
Preconditions and Postconditions

Reason: {AI12-0159-1} This ensures that the expression is well-defined for any primitive subprogram of a type descended from T.

Ramification: {AI12-0170-1} The operations of NT are also nonabstract, so the rule against a call of an abstract subprogram does not trigger for a class-wide precondition or postcondition.

{AI05-0145-2} {AI05-0264-1} {AI12-0418-1} For an attribute_reference attribute_reference with attribute_designator attribute_designator Old, if the attribute reference has an expected type (or class of types) or shall resolve to a given type, the same applies to the prefix; otherwise, the prefix shall be resolved independently of context.

Legality Rules

{AI05-0145-2} {AI05-0230-1} The Pre or Post aspect shall not be specified for an abstract subprogram or a null procedure. [Only the Pre'Class and Post'Class aspects may be specified for such a subprogram.]

Discussion: {AI05-0183-1} Pre'Class and Post'Class can only be specified on primitive routines of tagged types, by a blanket rule found in 13.1.1.

{AI05-0247-1} {AI05-0254-1} If a type T has an implicitly declared subprogram P inherited from a parent type T1 and a homograph (see 8.3) of P from a progenitor type T2, and

- the corresponding primitive subprogram P1 of type T1 is neither null nor abstract; and
- the class-wide precondition expression True does not apply to P1 (implicitly or explicitly); and
- there is a class-wide precondition expression that applies to the corresponding primitive subprogram P2 of T2 that does not fully conform to any class-wide precondition expression that applies to P1,

{AI05-0247-1} {AI05-0254-1} then:

- If the type T is abstract, the implicitly declared subprogram P is abstract.
- Otherwise, the subprogram P requires overriding and shall be overridden with a nonabstract subprogram.

Discussion: We use the term "requires overriding" here so that this rule is taken into account when calculating visibility in 8.3; otherwise we would have a mess when this routine is overridden.

Reason: Such an inherited subprogram would necessarily violate the Liskov Substitutability Principle (LSP) if called via a dispatching call from an ancestor other than the one that provides the called body. In such a case, the class-wide precondition of the actual body is stronger than the class-wide precondition of the ancestor. If we did not enforce that precondition for the body, the body could be called when the precondition it knows about is False — such "counterfeiting" of preconditions has to be avoided. But enforcing the precondition violates LSP. We do not want the language to be implicitly creating bodies that violate LSP; the programmer can still write an explicit body that calls the appropriate parent subprogram. In that case, the violation of LSP is explicit in the code and obvious to code reviewers (both human and automated).

We have to say that the subprogram is abstract for an abstract type in this case, so that the next concrete type has to override it for the reasons above. Otherwise, inserting an extra level of abstract types would eliminate the requirement to override (as there is only one declared operation for the concrete type), and that would be bad for the reasons given above.

Ramification: This requires the set of class-wide preconditions that apply to the interface routine to be strictly stronger than those that apply to the concrete routine. Since full conformance requires each name to denote the same declaration, it is unlikely that independently declared preconditions would conform. This rule does allow "diamond inheritance" of preconditions, and of course no preconditions at all match.

We considered adopting a rule that would allow examples where the expressions would conform after all inheritance has been applied, but this is complex and is not likely to be common in practice. Since the penalty here is just that an explicit overriding is required, the complexity is too much.

{AI05-0247-1} If a renaming of a subprogram or entry S1 overrides an inherited subprogram S2, then the overriding is illegal unless each class-wide precondition expression that applies to S1 fully conforms to some class-wide precondition expression that applies to S2 and each class-wide precondition expression that applies to S2 fully conforms to some class-wide precondition expression that applies to S1.
Reason: Such an overriding subprogram would violate LSP, as the precondition of \( S' \) would usually be different (and thus stronger) than the one known to a dispatching call through an ancestor routine of \( S' \). This is always OK if the preconditions match, so we always allow that.

Ramification: This only applies to primitives of tagged types; other routines cannot have class-wide preconditions.

\{AI12-0131-1\} Pre'Class shall not be specified for an overriding primitive subprogram of a tagged type \( T \) unless the Pre'Class aspect is specified for the corresponding primitive subprogram of some ancestor of \( T \).

Reason: Any such Pre'Class will have no effect, as it will be ordered with True. As such, it is highly misleading for readers, especially for those who are determining the assumptions that can be made in the body of the primitive subprogram. Note that in this case there is nothing explicit that might indicate that the class-wide precondition is ineffective. This rule does not prevent explicitly writing an ineffective class-wide precondition (for instance, if the parent subprogram has explicitly specified a precondition of True).

\{AI12-0131-1\} In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

Static Semantics

\{AI05-0145-2\} \{AI12-0113-1\} \{AI12-0131-1\} \{AI12-0170-1\} If a Pre'Class or Post'Class aspect is specified for a primitive subprogram \( S \) of a tagged type \( T \), or such an aspect defaults to True, then a corresponding expression also applies to the corresponding primitive subprogram \( S \) of each descendant of \( T \) ([including \( T \) itself]). The corresponding expression is constructed from the associated expression as follows:

\begin{itemize}
  \item \{AI12-0113-1\} References to formal parameters of \( S \) (or to \( S \) itself) are replaced with references to the corresponding formal parameters of the corresponding inherited or overriding subprogram \( S \) (or to the corresponding subprogram \( S \) itself).
  \item \{AI12-0113-1\} If the primitive subprogram \( S \) is not abstract, but the given descendant of \( T \) is abstract, then a nondispatching call on \( S \) is illegal if any Pre'Class or Post'Class aspect that applies to \( S \) is other than a static boolean expression. Similarly, a primitive subprogram of an abstract type \( T \), to which a non-static Pre'Class or Post'Class aspect applies, shall neither be the prefix of an Access attribute reference, nor shall it be a generic actual subprogram for a formal subprogram declared by a formal concrete subprogram declaration; illegal if it is not abstract and the corresponding expression for a Pre'Class or Post'Class aspect would be illegal.
\end{itemize}

This paragraph was deleted. Ramification: This can happen, for instance, if one of the subprograms called in the corresponding expression is abstract. We made the rule general so that we don't have to worry about exactly which cases can cause this to happen, both now and in the future.

Reason: \{AI12-0412-1\} The above rules mean that a concrete primitive of an abstract type is effectively treated as abstract, if any nontrivial Pre'Class or Post'Class aspects apply to it. This makes sense because we are using a notional formal derived type model for such aspects, and an abstract type is not permitted as an actual type for such a formal type. If we didn't do this, the evaluation of the precondition or postcondition of a concrete subprogram of an abstract type could possibly call abstract functions. We allow illegal corresponding expressions on abstract subprograms as they could never be evaluated, and we need to allow such expressions to contain calls to abstract subprograms.

Discussion: \{AI12-0412-1\} As this Reference Manual was frozen, a significant incompatibility has come to light with the above rule. The wording makes some calls to non-abstract primitives of a tagged abstract type illegal even if no abstract routines are involved in the Pre'Class or Post'Class. It is likely that the above rule will be adjusted; check with ARG work at www.ada-auth.org/arg.html to find the adjusted rules.
If performing checks is required by the Pre, Pre'Class, Post, or Post'Class assertion policies (see 11.4.2) in effect at the point of a corresponding aspect specification applicable to a given subprogram, or entry, or access-to-subprogram type, then the respective precondition or postcondition expressions are considered enabled.

**Ramification:** If a class-wide precondition or postcondition expression is enabled, it remains enabled when inherited by an overriding subprogram, even if the policy in effect is Ignore for the inheriting subprogram.

A subexpression of a postcondition expression is known on entry if it is any of:

- a static subexpression (see 4.9) any part of an if_expression other than the first condition;
- a literal whose type does not have any Integer Literal, Real Literal, or String Literal aspect specified, or the function specified by such an attribute has aspect Global specified to be null dependent_expression of a case_expression;
  - **Reason:** We mention literals explicitly in case they are not static (as when their subtype is not static, they are the literal null, and so on). We exclude literals of types with the aspects that are not Global => null as those cause a user-written subprogram with possible side effects to be called.
- a name statically denoting a full constant declaration which is known to have no variable views (see 3.3) a predicate of a quantified_expression;
  - **Ramification:** Constants of types with immutably limited or controlled parts are not allowed by this rule. Generic formal in objects are allowed by this rule (as they are defined to be full constant declarations).
  - **Reason:** We only want things that cannot be changed. We can't just say “constant” since that includes views of variables in some cases (for instance, a dereference of an access to constant object can be a view of a variable). There are other things we could have allowed (like a loop parameter), but having a subprogram declaration where those could be used (like inside of a loop) seems unusual enough to not be worth defining.
- a name statically denoting a nonaliased in parameter of an elementary type;
  - **Ramification:** All such parameters are by-copy, so the value won't change during the execution of the subprogram.
- an Old attribute_reference;
- an invocation of a predefined operator where all of the operands are known on entry;
- a function call where the function has aspect Global => null where all of the actual parameters are known on entry;
  - **Reason:** Such a function can only depend on the values of its parameters.
- a selected_component of a known-on-entry prefix;
- an indexed_component of a known-on-entry prefix where all index expressions are known on entry;
- a parenthesized known-on-entry expression;
- a qualified_expression or type_conversion whose operand is a known-on-entry expression;
- a conditional_expression where all of the conditions, selecting_expressions, and dependent_expressions are known on entry.
  - **Discussion:** It's OK if such an expression raises an exception, so long as every evaluation of the expression raises the same exception.
- A subexpression of a postcondition expression is unconditionally evaluated, conditionally evaluated, or repeatedly evaluated. A subexpression is considered unconditionally evaluated unless it is conditionally evaluated or repeatedly evaluated.
The following subexpressions are repeatedly evaluated:

- A subexpression of a predicate of a quantified_expression;
- A subexpression of the expression of an array_component_association;
- A subexpression of the expression of a container_element_association.

For a subexpression that is conditionally evaluated, there is a set of determining expressions that determine whether the subexpression is actually evaluated at run time. Subexpressions that are conditionally evaluated and their determining expressions are as follows:

- For an if_expression that is not repeatedly evaluated, a subexpression of any part other than the first condition is conditionally evaluated, and its determining expressions include all conditions of the if_expression that precede the subexpression textually.
- For a case_expression that is not repeatedly evaluated, a subexpression of any dependent_expression is conditionally evaluated, and its determining expressions include the selecting_expression of the case_expression;
- For the right operand of a short-circuit control form that is not repeatedly evaluated, a subexpression of the right-hand operand is conditionally evaluated, and its determining expressions include the left-hand operand of the short-circuit control form;
- For a membership test that is not repeatedly evaluated, a subexpression of a membership_choice other than the first is conditionally evaluated, and its determining expressions include the tested_simple_expression and the preceding membership_choices of the membership test of a membership operation.

A conditionally evaluated subexpression is determined to be unevaluated at run time if its set of determining expressions are all known on entry, and when evaluated on entry their values are such that the given subexpression is not evaluated.

Ramification: To be precise, a conditionally evaluated expression is determined to be unevaluated (including all of its subexpressions) under the following circumstances:

- Within an if_expression, a dependent_expression with an associated condition that evaluates to False, or a condition or dependent_expression where a condition of a preceding part of the if_expression evaluates to True;
- Within a case_expression, a dependent_expression with a discrete_choice_list that is not covered by the value of the selecting_expression;
- The right-hand operand of a short-circuit control form where the left-hand operand evaluates to False for and True for or else;
- A membership_choice of a membership test where the individual membership test defined by any prior membership_choice evaluates to True.

For a prefix X that denotes an object of a nonlimited type, the following attribute is defined:

X'Old

Ramification: If X'Old occurs in a subexpression that is determined to be unevaluated, then there is no associated constant, and no evaluation of the prefix takes place. In general, this will require evaluating one or more known-on-entry subexpressions before creating and initializing any X'Old constants. Note that any 'Old in a known-on-entry subexpression evaluated this way represents the current value of the prefix (the 'Old itself can be ignored).
In the case of an accept statement, the constant is declared inside of the rendezvous. It is considered part of the initialization of the postcondition check, which is part of the rendezvous by definition (see 9.5.2).

**AI12-0032-1** {AI12-0159-1} The implicitly declared entity denoted by each occurrence of X'Old is declared as follows:

- If X is of an anonymous access type defined by an access definition A then
  
  \[
  X'\text{Old} : \text{constant } A := X;
  \]

- If X is of a specific tagged type T then
  
  \[
  X'\text{Old} : \text{ constant } T'\text{Class} := T'\text{Class}(X);
  \]

where the name X'Old denotes the object renaming.

**Ramification:** This means that the underlying tag associated with X'Old is that of X and not that of the nominal type of X.

- Otherwise
  
  \[
  X'\text{Old} : \text{constant } S := X;
  \]

  where S is the nominal subtype of X. This includes the case where the type of S is an anonymous array type or a universal type.

**AI12-0032-1** {AI12-0185-1} {AI12-0388-1} The type and nominal subtype of X'Old are as implied by the above definitions. The expected type of the prefix of an Old attribute is that of the attribute. Similarly, if an Old attribute shall resolve to be of some type, then the prefix of the attribute shall resolve to be of that type.

**AI05-0145-2** {AI05-0262-1} {AI05-0273-1} {AI12-0217-1} {AI12-0280-2} Reference to this attribute is only allowed within a postcondition expression. The prefix of an Old attribute reference shall not contain a Result attribute reference, nor an Old attribute reference, nor a use of an entity declared within the postcondition expression but not within prefix itself (for example, the loop parameter of an enclosing quantified expression). The prefix of an Old attribute reference that is potentially unevaluated shall statically name an entity, unless the attribute reference is unconditionally evaluated, or is conditionally evaluated where all of the determining expressions are known on entry.

**Discussion:** The prefix X can be any nonlimited object that obeys the syntax for prefix other than the few exceptions given above (discussed below). Useful cases are: the name of a formal parameter of mode in or out, the name of a global variable updated by the subprogram, a function call passing those as parameters, a subcomponent of those things, etc.

A qualified expression can be used to make an arbitrary expression into a valid prefix, so T'(X + Y)'Old is legal, even though (X + Y)'Old is not. The value being saved here is the sum of X and Y (a function result is an object). Of course, in this case "+"(X, Y)'Old is also legal, but the qualified expression is arguably more readable.

Note that F(X)'Old and F(X'Old) are not necessarily equal. The former calls F(X) and saves that value for later use during the postcondition. The latter saves the value of X, and during the postcondition, passes that saved value to F. In most cases, the former is what one wants (but it is not always legal, see below).

**AI12-0032-1** If X has controlled parts, adjustment and finalization are implied by the implicit constant declaration. Similarly, the implicit constant declaration defines the accessibility level of X'Old.

If postconditions are disabled, we want the compiler to avoid any overhead associated with saving 'Old values.

'Old makes no sense for limited types, because its implementation involves copying. It might make semantic sense to allow build-in-place, but it's not worth the trouble.

**Reason:** {AI05-0273-1} {AI12-0280-2} {AI12-0005-1} Since the prefix of an Old attribute reference is evaluated unconditionally when the subprogram is called (if it is evaluated at all), we cannot allow it to include values that do not exist at that time (like Result and loop parameters of quantified expressions). We also do not allow the prefix itself to include 'Old references, as those would be redundant (because the evaluation of the entire prefix, if it occurs, already happens on entry to a subprogram being called), and allowing them would require some sort of order to the implicit constant declarations (because in A('TOld)'Old, we surely would want the value of T'Old evaluated before the A('TOld) is evaluated).
An additional rule applies when it cannot be determined on entry to the subprogram whether the Old attribute reference will or will not be evaluated when the overall postcondition expression is evaluated. In such cases, we require that only allow simple names as the prefix of the Old attribute reference to statically name some object attribute if the attribute reference might not be evaluated when the postcondition expression is evaluated. This is necessary because the Old prefixes have to be unconditionally evaluated when the subprogram is called if there is any possibility that they might be needed; the compiler cannot in general know whether they will be needed in the postcondition expression. To see the problem, consider:

Table: array (1..10) of Integer := ...
procedure Bar (I : in out Natural)
with Post => I > 0 and then Table(I)'Old = 1; -- Illegal

In this example, the compiler cannot know on entry what will be the value of I when the subprogram returns (since the subprogram execution can change it), and thus it does not know whether Table(I)'Old will be needed then. Thus it has to always create an implicit constant and evaluate Table(I) when Bar is called (because not having the value when it is needed is not acceptable). But if I = 0 when the subprogram is called, that evaluation will raise Constraint_Error, and that will happen even if I is unchanged by the subprogram and the value of Table(I)'Old is not ultimately needed. It's easy to see how a similar problem could occur for a dereference of an access type. This would be mystifying (since the point of the short circuit is to eliminate this possibility, but it cannot do so). Therefore, we require the prefix of any Old attribute reference in such a context to statically name some object, which eliminates anything that could change at runtime.

It is easy to work around most errors that occur because of this rule. Just move the 'Old to the outer object, before any indexing, dereferences, or components. (That does not work for function calls, however, nor does it work for array indexing if the index can change during the execution of the subprogram.)

Ramification: An accept statement for a task entry with enabled postconditions such as

accept E do
  statements
except
    handlers
end;

behaves (at runtime) as follows:

accept E do
  declare
  begin
    begin
      statements
    exception
      handlers
    end;
  postcondition checks
end;

Preconditions are checked by the caller before the rendezvous begins. Postcondition expressions might, of course, reference 'Old constants.

In the case of a protected operation with enabled postconditions, 'Old constant declarations (if any) are elaborated after the start of the protected action. Postcondition checks (which might reference these constants) are performed before the end of the protected action as described below.

The prefix of an Old attribute reference has to statically name an entity if it appears within a repeatedly evaluated expression.

For a prefix F that denotes a function declaration or an access-to-function type, the following attribute is defined:

F'Result

Within a postcondition expression for function F, denotes the return result object of the function call for which the postcondition expression is evaluated. The type of this attribute is that of the result subtype of the function or access-to-function type result except within a Post'Class postcondition expression for a function with a controlling result or with a controlling access result; in those cases the type of the attribute is described above as part of the Name Resolution Rules for Post'Class. For a controlling result, the type of the attribute is 7'Class, where 7 is the function result type.
an anonymous access type whose designated type is \( T'\text{Class} \), where \( T \) is the designated type of the function result type.

\{AI05-0262-1\} Use of this attribute is allowed only within a postcondition expression for \( F \).

\{AI05-0220-1\} An “access-to-function type” is an access-to-subprogram type whose designated profile is a function profile.

\{AI12-0143-1\} For a prefix \( E \) that denotes an entry declaration of an entry family (see 9.5.2), the following attribute is defined:

\[ E'\text{Index} \]

\{AI12-0143-1\} Within a precondition or postcondition expression for entry family \( E \), denotes the value of the entry index for the call of \( E \). The nominal subtype of this attribute is the entry index subtype.

\{AI12-0143-1\} Use of this attribute is allowed only within a precondition or postcondition expression for \( E \).

\section*{Dynamic Semantics}

\{AI05-0145-2\} \{AI05-0247-1\} \{AI05-0290-1\} Upon a call of the subprogram or entry, after evaluating any actual parameters, precondition checks are performed as follows:

- The specific precondition check begins with the evaluation of the specific precondition expression that applies to the subprogram or entry, if it is enabled; if the expression evaluates to False, Assertions.Assertion_Error is raised; if the expression is not enabled, the check succeeds.

- The class-wide precondition check begins with the evaluation of any enabled class-wide precondition expressions that apply to the subprogram or entry. If and only if all the class-wide precondition expressions evaluate to False, Assertions.Assertion_Error is raised.

\paragraph{Ramification:} The class-wide precondition expressions of the entity itself as well as those of any parent or progenitor operations are evaluated, as these expressions apply to the corresponding operations of all descendants. Class-wide precondition checks are performed for all appropriate calls, but only enabled precondition expressions are evaluated. Thus, the check would be trivial if no precondition expressions are enabled.

\{AI05-0145-2\} \{AI05-0247-1\} \{AI05-0254-1\} \{AI05-0269-1\} \{AI12-0166-1\} The precondition checks are performed in an arbitrary order, and if any of the class-wide precondition expressions evaluate to True, it is not specified whether the other class-wide precondition expressions are evaluated. The precondition checks and any check for elaboration of the subprogram body are performed in an arbitrary order. \textit{Init} is not specified whether in a call on a protected operation, the checks are performed before or after starting the protected action. For an entry call, the checks are performed prior to checking whether the entry is open.

\paragraph{Reason:} We need to explicitly allow short-circuiting of the evaluation of the class-wide precondition check if any expression fails, as it consists of multiple expressions; we don't need a similar permission for the specific precondition check as it consists only of a single expression. Nothing is evaluated for the call after a check fails, as the failed check propagates an exception.

\{AI05-0145-2\} \{AI05-0247-1\} \{AI05-0254-1\} \{AI05-0262-1\} \{AI05-0290-1\} Upon successful return from a call of the subprogram or entry, prior to copying back any by-copy \texttt{in out} or \texttt{out} parameters, the postcondition check is performed. This consists of the evaluation of any enabled specific and class-wide postcondition expressions that apply to the subprogram or entry. If any of the postcondition expressions evaluate to False, then Assertions.Assertion_Error is raised. The postcondition expressions are evaluated in an arbitrary order, and if any postcondition expression evaluates to False, it is not specified whether any other postcondition expressions are evaluated. The postcondition check, and any constraint or predicate checks associated with \texttt{in out} or \texttt{out} parameters are performed in an arbitrary order.
Ramification: The class-wide postcondition expressions of the entity itself as well as those of any parent or progenitor operations are evaluated, as these apply to all descendants; in contrast, only the specific postcondition of the entity applies. Postconditions can always be evaluated inside the invoked body.

Reason: If a postcondition references the implicitly-declared constant associated with an Old attribute, the postcondition must be evaluated before the constant is finalized. One way to think of this is to imagine declaring a controlled object between any implicit "Old" constant declarations and any explicit declarations, then performing postcondition checks during the finalization of this object.

AI05-0145-2} AI05-0262-1} If a precondition or postcondition check fails, the exception is raised at the point of the call; the exception cannot be handled inside the called subprogram or entry. Similarly, any exception raised by the evaluation of a precondition or postcondition expression is raised at the point of call.

For any call to a subprogram or entry Seal (including dispatching calls), the checks that are performed to verify specific precondition expressions and specific and class-wide postcondition expressions are determined by those for the subprogram or entry actually invoked. Note that the class-wide postcondition expressions verified by the postcondition check that is part of a call on a primitive subprogram of type T includes all class-wide postcondition expressions originating in any progenitor of T, even if the primitive subprogram called is inherited from a type T1 and some of the postcondition expressions do not apply to the corresponding primitive subprogram of T1. Any operations within a class-wide postcondition expression that were resolved as primitive operations of the (notional) formal derived type NT, are in the evaluation of the postcondition bound to the corresponding operations of the type identified by the controlling tag of the call on S. This applies to both dispatching and non-dispatching calls on S.

Ramification: This applies to access-to-subprogram calls, dispatching calls, and to statically bound calls. We need this rule to cover statically bound calls as well, as specific pre- and postconditions are not inherited, but the subprogram might be.

For concrete subprograms, we require the original specific postcondition to be evaluated as well as the inherited class-wide postcondition in order that the semantics of an explicitly defined wrapper that does nothing but call the original subprogram is the same as that of an inherited subprogram.

Note that this rule does not apply to class-wide preconditions; they have their own rules mentioned below.

The class-wide precondition check for a call to a subprogram or entry S consists solely of checking the class-wide precondition expressions that apply to the denoted callable entity (not necessarily to the one that is invoked). Any operations within such an expression that were resolved as primitive operations of the (notional) formal derived type NT are in the evaluation of the precondition bound to the corresponding operations of the type identified by the controlling tag of the call on S. This applies to both dispatching and non-dispatching calls on S.

Ramification: For a dispatching call, we are talking about the PreClass(es) that apply to the subprogram that the dispatching call is resolving to, not the PreClass(es) for the subprogram that is ultimately dispatched to. The class-wide precondition of the resolved call is necessarily the same or stronger than that of the invoked call. For a statically bound call, these are the same; for an access-to-subprogram, (which has no class-wide preconditions of its own), we check the class-wide preconditions of the invoked routine.

Since this check is based on the "callable entity", it does not depend on the view of the entity. This matters any time the ancestor type (if any) of the partial view differs from the parent type of the full view. In such a case, the view of the callable entity associated with the full view might inherit a PreClass while the view of the same callable entity associated with the partial view does not.
Preconditions and Postconditions

Implementation Note: These rules imply that logically, class-wide preconditions of routines must be checked at the point of call (other than for access-to-subprogram calls, which must be checked in the body, probably using a wrapper). Specific preconditions that might be called with a dispatching call or via an access-to-subprogram value must be checked inside of the subprogram body. In contrast, the postcondition checks always need to be checked inside the body of the routine. Of course, an implementation can evaluate all of these at the point of call for statically bound calls if the implementation uses wrappers for dispatching bodies and for 'Access values.

There is no requirement for an implementation to generate special code for routines that are imported from outside of the Ada program. That's because there is a requirement on the programmer that the use of interfacing aspects do not violate Ada semantics (see B.1). That includes making pre- and postcondition checks. For instance, if the implementation expects routines to make their own postcondition checks in the body before returning, C code can be assumed to do this (even though that is highly unlikely). That's even though the formal definition of those checks is that they are evaluated at the call site. Note that pre- and postconditions can be very useful for verification tools (even if they aren't checked), because they tell the tool about the expectations on the foreign code that it most likely cannot analyze.

\{AI12-0195-1\} For the purposes of the above rules, a call on an inherited subprogram is considered to involve a call on a subprogram \(S'\) whose body consists only of a call (with appropriate conversions) on the non-inherited subprogram \(S\) from which the inherited subprogram was derived. It is not specified whether class-wide precondition or postcondition expressions that are equivalent (with respect to which non-inherited function bodies are executed) for \(S\) and \(S'\) are evaluated once or twice. If evaluated only once, the value returned is used for both associated checks.

Implementation Note: If the class-wide pre- and postcondition expressions are equivalent for \(S\) and \(S'\) because none of the primitive subprograms called in those expressions were overridden, no wrapper is needed. Otherwise, a wrapper is presumably needed to provide the correct logic.

\{AI05-0145-2\} \{AI05-0247-1\} \{AI12-0220-1\} For a call via an access-to-subprogram value, all-precondition and postcondition checks performed are as determined by the subprogram or entry denoted by the prefix of the Access attribute reference that produced the value. In addition, a precondition check of any postcondition expression associated with the access-to-subprogram type is performed. Similarly, a postcondition check of any postcondition expression associated with the access-to-subprogram type is performed.

Implementation Note: \{AI12-0220-1\} A call via an access-to-subprogram value can be considered equivalent (with respect to dynamic semantics) to a call to a notional "wrapper" subprogram which has the Pre and Post aspects and the profile of the access-to-subprogram type and whose body contains (and returns, in the case of a function) only a call to the designated subprogram. However, other evaluation orders for the checks are allowed beyond those allowed by strictly following this model. This equivalence can be used to determine the appropriate point at which the constant associated with an Old attribute reference in the Post aspect for an access-to-subprogram type is elaborated and finalized.

Ramiﬁcation: \{AI12-0220-1\} In the case of type conversion between two access-to-subprogram types, the Pre and Post aspects of the source type of the conversion play no role in any subsequent call via the conversion result; only the Pre and Post aspects of the target type of the conversion are relevant in that case. The same applies in the case of a "conversion" (using the term loosely) which is accomplished by combining a dereference and an Access attribute reference, as in Some_Pointer.all'Access.

\{AI12-0272-1\} [For a call on a generic formal subprogram, precondition and postcondition checks performed are as determined by the subprogram or entry denoted by the actual subprogram, along with any specific precondition and specific postcondition of the formal subprogram itself.]

Proof: \{AI12-0272-1\} This follows from the general Dynamic Semantics rules given above, but we mention it explicitly so that there can be no doubt that it is intended.

To be honest: \{AI12-0371-1\} The specific precondition and postcondition that apply to a generic formal subprogram also apply to any renaming of that subprogram, even if that renaming is visible in the instance and called from outside of the generic instance.

Implementation Permissions

\{AI12-0280-2\} \{AI12-0373-1\} An implementation may evaluate a known-on-entry subexpression of a postcondition expression of an entity at the place where X'Old constants are created for the entity, with the normal evaluation of the postcondition expression, or both.
42.a/5  
**Reason:** `{AI12-0280-2}` We allow the evaluation of known-on-entry subexpressions when they might be needed to determine whether to create a particular `Old` constant. We allow them to be evaluated later as well, or for the results to be saved somehow. This permission shouldn't matter, as the results ought to be same wherever they are evaluated and there should not be any side effects. The main effect of the permission is to determine when any exceptions caused by such subexpressions may be raised. We never require waiting to determine the value of such subexpressions, even if they aren't used to determine the creation of a constant for `Old`.

43/5  
**NOTE 1** `{AI05-0145-2} {AI05-0262-1} {AI12-0442-1}` A precondition is checked just before the call. If another task can change any value that the precondition expression depends on, the precondition can evaluate to False and need not hold within the subprogram or entity body.

44/5  
**NOTE 2** `{AI12-0312-1}` For an example of the use of these aspects and attributes, see the Streams Subsystem definitions in 13.13.1.

**Extensions to Ada 2005**

44.a/3  
{AI05-0145-2} {AI05-0230-1} {AI05-0247-1} {AI05-0254-1} {AI05-0262-1} {AI05-0273-1} {AI05-0274-1} Pre and Post aspects are new.

**Inconsistencies With Ada 2012**

44.b/4  
{AI12-0032-1}  
**Corrigendum:** The Old attribute is defined more carefully. This changes the nominal subtype and place of declaration of the attribute compared to the published Ada 2012 Reference Manual. In extreme cases, this could change the runtime behavior of the attribute (for instance, the tag might be different). The changes are most likely going to prevent bugs by being more intuitive, but it is possible that a program that previously worked might fail.

44.c/4  
{AI12-0113-1} {AI12-0159-1}  
**Corrigendum:** Eliminated unintentional redispaching from class-wide preconditions and postconditions. This means that a different body might be evaluated for a statically bound call to a routine that has a class-wide precondition or postcondition. The change means that the behavior of Pre and Pre'Class will be the same for a particular subprogram, and that the known behavior of the operations can be assumed within the body of that subprogram for Pre'Class. We expect that this change will primarily fix bugs, as it will make Pre'Class and Post'Class work more like expected. In the case where redispatching is desired, an explicit conversion to a class-wide type can be used.

44.d/5  
{AI12-0166-1}  
**Correction:** Specified that precondition checks always take place before starting a protected action. Original Ada 2012 left this unspecified, so if an implementation made the checks after starting the protected action, and a program depended upon that, the program might fail in a different compiler. But such a program was depending on unspecified behavior anyway, and thus was never portable; as such, such programs should be rare.

44.d.1/5  
{AI12-0195-1}  
**Correction:** Specified that an inherited subprogram check both the original and new versions of a class-wide precondition. If a call on an inherited subprogram fails the original class-wide precondition when it passes the new class-wide precondition, then the call will fail the precondition check whereas it would have passed in original Ada 2012. (A similar possibility exists for class-wide postconditions.) This can only happen if the overriding subprograms somehow fail to follow the guidelines of LSP, so this should be rare (the entire point of class-wide preconditions and postconditions is to use them in cases where LSP is followed).

**Incompatibilities With Ada 2012**

44.e/5  
{AI12-0045-1} {AI12-0005-1}  
**Corrigendum:** Precondition and postcondition aspects cannot be specified on instances of generic subprograms (they should be specified on the generic subprogram instead). This was (unintentionally) allowed by the Ada 2012 standard. These are not be allowed on instances as there is no corresponding way to add preconditions and postconditions to subprograms declared within the instance of a generic package. Therefore, allowing specification on a subprogram instance could present a maintenance problem in the future if the entity needs to be converted to a generic package (a common conversion).

44.f/4  
{AI12-0131-1}  
**Corrigendum:** PreClass is no longer allowed to be specified for an overriding primitive subprogram unless there are also inherited class-wide preconditions. This incompatibility prevents cases where the explicit PreClass is counterfeited by an implicit class-wide precondition of True. This rule should catch more bugs than it creates; the programmer should have written Pre rather than Pre'Class in this case (or written Pre'Class on the original subprogram, not an overriding). Note that this incompatibility eliminates what otherwise would be an inconsistency with original Ada 2012, where precondition checks that would have previously been made for a statically bound call would no longer be made. That dynamic change was necessary to eliminate cases where the evaluated class-wide precondition on a dispatching call would have been weaker than the class-wide precondition of a statically bound call. (The original Ada 2012 violated the LSP semantics that class-wide preconditions were intended to model.)

44.g/5  
{AI12-0198-1}  
**Correction:** A component expression in an array aggregate can now be potentially unevaluated, requiring the prefix to be statically determined. Existing code that uses the `Old` attribute with a dynamic prefix in such contexts will now be illegal. However, in many cases, the existing code will not do what the programmer is expecting.
(as Old is evaluated textually, once per occurrence, while array aggregate components are evaluated once per component). In addition, Old is a new Ada 2012 feature, so most Ada legacy code will not contain it. The problem is usually easily fixed by moving Old to an outer object (such as the entire aggregate).

Extensions to Ada 2012

{AI12-0143-1} The Index attribute is new.

{AI12-0217-1} Correction: The prefix of a statically unevaluated Old attribute_reference can be a selected_component or indexed_component. This is considered a correction as the old rule is unintentionally too fierce, rejecting safe cases.

{AI12-0280-2} We make no restriction on the prefix of an Old attribute_reference if we can determine when the subprogram is entered (which is the point when Old prefixes are evaluated) whether it will be needed in the evaluation of the postcondition.

{AI12-0220-1} {AI12-0272-1} Pre and Post can be given on an access-to-subprogram type and on a generic formal subprogram.

{AI12-0412-1} Correction: We now allow the definition of a concrete subprogram S that has applicable Pre'Class or Post'Class expressions that is primitive for an abstract type T even when a Pre'Class or Post'Class may call an abstract subprogram. Rather, S is treated as if it is abstract (meaning that uses that might require evaluating a statically bound Pre'Class or Post'Class expression are not allowed).

Wording Changes from Ada 2012

{AI05-0170-1} Correction: Clarified the wording about the meaning of the notional type NT and the corresponding expression. Both changes follow from other rules but are nonobvious.

{AI05-0185-1} Correction: Removed redundant (and sometimes incorrect) wording about the resolution of the Old and Result attributes.

6.1.2 The Global and Global'Class Aspects

{AI12-0425-1} {AI12-0439-1} The Global and Global'Class aspects of a program unit are used to identify the objects global to the unit that can be read or written during its execution.

Syntax

{AI12-0079-3} {AI12-0380-1} {AI12-0425-1} global_aspect_definition ::= null
   | Unspecified
   | global_mode global_designator
   | (global_aspect_element; global_aspect_element)

{AI12-0079-3} {AI12-0380-1} global_aspect_element ::= global_mode global_set
   | global_mode all
   | global_mode synchronized

global_mode ::= basic_global_mode
   | extended_global_mode

basic_global_mode ::= in | in out | out

global_set ::= global_name {, global_name}

global_designator ::= all | synchronized | global_name

{AI12-0079-1} {AI12-0310-1} global_name ::= object_name | package_name
Name Resolution Rules

\[ \{AI12-0079-3\} \{AI12-0425-1\} \{AI12-0427-1\} \] A global name shall resolve to statically name an object or a package (including a limited view of a package).

Static Semantics

\[ \{AI12-0079-3\} \] For a subprogram, an entry, an access-to-subprogram type, a task unit, a protected unit, or a library package or generic library package, the following language-defined aspect may be specified with an aspect specification (see 13.1.1):

\[ \{AI12-0079-3\} \{AI12-0425-1\} \] Global

The Global aspect shall be specified with a global_aspect_definition.

Aspect Description for Global: Global object usage contract.

\[ \{AI12-0079-3\} \{AI12-0422-1\} \] The Global aspect identifies the set of variables (which, for the purposes of this clause, includes all constants except those which are known to have no variable views (see 3.3)) that are global to a callable entity or task body, and that are read or updated as part of the execution of the callable entity or task body. If specified for a protected unit, it refers to all of the protected operations of the protected unit. Constants of any type may also be mentioned in a Global aspect.

\[ \{AI12-0079-3\} \] If not specified or otherwise defined below, the aspect defaults to the Global aspect for the enclosing library unit if the entity is declared at library level, and to Unspecified otherwise. If not specified for a library unit, the aspect defaults to Global => null for a library unit that is declared Pure, and to Global => Unspecified otherwise.

\[ \{AI12-0079-3\} \] For a dispatching subprogram, the following language-defined aspect may be specified with an aspect specification (see 13.1.1):

\[ \{AI12-0079-3\} \{AI12-0425-1\} \] Global'Class

The Global'Class aspect shall be specified with a global_aspect_definition. This aspect identifies an upper bound on the set of variables global to a dispatching operation that can be read or updated as a result of a dispatching call on the operation. If not specified, the aspect defaults to the Global aspect for the dispatching subprogram.

Aspect Description for Global'Class: Global object usage contract inherited on derivation.

\[ \{AI12-0380-1\} \] Together, we refer to the Global and Global'Class aspects as global aspects.

\[ \{AI12-0079-3\} \] A global_aspect_definition defines the Global or Global'Class aspect of some entity. The Global aspect identifies the sets of global variables that can be read, written, or modified as a side effect of executing the operation(s) associated with the entity. The Global'Class aspect associated with a dispatching operation of type \( T \) represents a restriction on the Global aspect on a corresponding operation of any descendant of type \( T \).

\[ \{AI12-0079-3\} \{AI12-0416-1\} \{AI12-0442-1\} \] The Global aspect for a callable entity defines the global variables that can be referenced as part of a call on the entity, including any assertion expressions that apply to the call (even if not enabled), such as preconditions, postconditions, predicates, and type invariants.

\[ \{AI12-0079-3\} \{AI12-0439-1\} \] The Global aspect for an access-to-subprogram object (or subtype) identifies the global variables that can be referenced when calling via the object (or any object of that subtype) including assertion expressions that apply.

\[ \{AI12-0079-3\} \{AI12-0405-1\} \] For a predefined operator of an elementary type, the function representing an enumeration literal, or any other static function (see 4.9), the Global aspect is null. For a predefined
operator of a composite type, the Global aspect of the operator defaults to that of the enclosing library unit (unless a Global aspect is specified for the type — see H.7).

\{AI12-0079-3\} \{AI12-0380-1\} The following is defined in terms of operations that are performed by or on behalf of an entity. The rules on operations apply to the entity(s) associated with those operations.

Discussion: \{AI12-0380-1\} The operations performed by a callable entity are those associated with the body of the entity. For other kinds of entities (such as subtypes, see H.7), we explicitly list the associated operations.

\{AI12-0079-3\} The global variables associated with any global mode can be read as a side effect of an operation. The in out and out global modes together identify the set of global variables that can be updated as a side effect of an operation. Creating an access-to-variable value that designates an object is considered an update of the designated object, and creating an access-to-constant value that designates an object is considered a read of the designated object.

\{AI12-0079-3\} The overall set of objects associated with each global mode includes all objects identified for the mode in the global aspect definition.

\{AI12-0079-3\} A global set identifies a global variable set as follows:

- all identifies the set of all global variables;
- synchronized identifies the set of all synchronized variables (see 9.10), as well as variables of a composite type all of whose non-discriminant subcomponents are synchronized;
- global name\{, global name\} identifies the union of the sets of variables identified by the global names in the list, for the following forms of global name:
  - object name identifies the specified global variable (or constant);
  - package name identifies the set of all variables declared in the private part or body of the package, or anywhere within a private descendant of the package.

Legality Rules

\{AI12-0079-1\} Within a global aspect definition, a given global mode shall be specified at most once. Similarly, within a global aspect definition, a given entity shall be named at most once by a global name.

\{AI12-0079-3\} If an entity (other than a library package or generic library package) has a Global aspect other than Unspecified or in out all, then the associated operation(s) shall read only those variables global to the entity that are within the global variable set associated with the in, in out, or out global modes, and the operation(s) shall update only those variables global to the entity that are within the global variable set associated with either the in out or out global modes. In the absence of the No Hidden Indirect Globals restriction (see H.4), this ignores objects reached via a dereference of an access value. The above rule includes any possible Global effects of calls occurring during the execution of the operation, except for the following excluded calls:

- calls to formal subprograms;
- calls associated with operations on formal subtypes;
- calls through formal objects of an access-to-subprogram type;
- calls through access-to-subprogram parameters;
- calls on operations with Global aspect Unspecified.

\{AI12-0079-3\} The possible Global effects of these excluded calls (other than those that are Unspecified) are taken into account by the caller of the original operation, by presuming they occur at least once during its execution. For calls that are not excluded, the possible Global effects of the call are those permitted by the Global aspect of the associated entity, or by its Global'Class aspect if a dispatching call.
Ramification: For a predefined equality operator of a composite type, the possible Global effects includes those of the equality operations invoked as part of the evaluation of the operator (which might not be predefined and thus might have a different Global specification than the component types).

\{AI12-0079-3\} If a Global aspect other than Unspecified or in out all applies to an access-to-subprogram type, then the prefix of an Access attribute reference producing a value of such a type shall denote a subprogram whose Global aspect is not Unspecified and is covered by that of the result type, where a global aspect \(G_1\) is covered by a global aspect \(G_2\) if the set of variables that \(G_1\) identifies as readable or updatable is a subset of the corresponding set for \(G_2\). Similarly on a conversion to such a type, the operand shall be of a named access-to-subprogram type whose Global aspect is covered by that of the target type.

\{AI12-0079-3\} If an implementation-defined global mode applies to a given set of variables, an implementation-defined rule determines what sort of references to them are permitted.

\{AI12-0079-1\} For a subprogram that is a dispatching operation of a tagged type \(T\), each mode of its Global aspect shall identify a subset of the variables identified by the corresponding mode, or by the in out mode, of the Global'Class aspect of a corresponding dispatching subprogram of any ancestor of \(T\), unless the aspect of that ancestor is Unspecified.

Implementation Permissions

\{AI12-0079-3\} \{AI12-0444-1\} An implementation can allow some references to a constant object which are not accounted for by the Global or Global'Class aspect when it is considered a variable in the above rules, if the implementation can determine that the object is in fact immutable.

Ramification: In particular, this allows the implementation to violate privacy in order to determine whether a constant needs to be covered by a Global aspect.

\{AI12-0079-3\} Implementations may perform additional checks on calls to operations with an Unspecified Global aspect to ensure that they do not violate any limitations associated with the point of call.

Discussion: In this sense, Global => Unspecified is not permission to violate the caller's Global restrictions. It is rather that the implementor of the subprogram is presuming other means are being used to ensure safety. Note the No Unspecified Globals Restriction (H.4), which prevents the use of Unspecified with the Global aspect in a given partition.

\{AI12-0079-3\} Implementations may extend the syntax or semantics of the Global aspect in an implementation-defined manner[; for example, supporting additional global modes].

Implementation defined: Any extensions of the Global aspect.

Reason: This is intended to allow preexisting usages from SPARK 2014 to remain acceptable in conforming implementations, as well as to provide flexibility for future enhancements. Note the word “extend” in this permission: we expect that any aspect usage that conforms with the (other) rules of this subclause will be accepted by any Ada implementation, regardless of any implementation-defined extensions.

NOTE \{AI12-0312-1\} For an example of the use of these aspects, see the Vector container definition in A.18.2.

Extensions to Ada 2012

\{AI12-0079-1\} \{AI12-0240-6\} \{AI12-0310-1\} The Global and Global'Class aspects are new.

6.2 Formal Parameter Modes

[A parameter_specification declares a formal parameter of mode in, in out, or out.]

Static Semantics

A parameter is passed either by copy or by reference. [When a parameter is passed by copy, the formal parameter denotes a separate object from the actual parameter, and any information transfer between the
two occurs only before and after executing the subprogram. When a parameter is passed by reference, the formal parameter denotes (a view of) the object denoted by the actual parameter; reads and updates of the formal parameter directly reference the actual parameter object.

A type is a by-copy type if it is an elementary type, or if it is a descendant of a private type whose full type is a by-copy type. A parameter of a by-copy type is passed by copy,

unless the formal parameter is explicitly aliased.

A type is a by-reference type if it is a descendant of one of the following:

- a tagged type;
- a task or protected type;
- an explicitly limited record type a nonprivate type with the reserved word limited in its declaration;
- a composite type with a subcomponent of a by-reference type;
- a private type whose full type is a by-reference type.

A parameter of a by-reference type is passed by reference, as is an explicitly aliased parameter of any type. Each value of a by-reference type has an associated object. For a parenthesized expression, qualified_expression, or view conversion type_conversion, this object is the one associated with the operand. For a value conversion, the associated object is the anonymous result object if such an object is created (see 4.6); otherwise it is the associated object of the operand. In other cases, the object associated with the evaluated operative constituent of the name or expression (see 4.4) determines its associated object. For a conditional_expression, this object is the one associated with the evaluated dependent_expression.

Ramification: By-reference parameter passing makes sense only if there is an object to reference; hence, we define such an object for each case.

Since tagged types are by-reference types, this implies that every value of a tagged type has an associated object. This simplifies things, because we can define the tag to be a property of the object, and not of the value of the object, which makes it clearer that object tags never change.

A construct like parenthesized expression or qualified_expression is ignored for the purposes of determining the associated object; for a conditional_expression, it is relevant only in that it determines which dependent_expression defines the associated object.

We considered simplifying things even more by making every value (and therefore every expression) have an associated object. After all, there is little semantic difference between a constant object and a value. However, this would cause problems for untagged types. In particular, we would have to do a constraint check on every read of a type conversion (or a renaming thereof) in certain cases.

We do not want this definition to depend on the view of the type; privativeness is essentially ignored for this definition. Otherwise, things would be confusing (does the rule apply at the call site, at the site of the declaration of the subprogram, at the site of the return_statement?'), and requiring different calls to use different mechanisms would be an implementation burden.

C.6, “Shared Variable Control” says that a composite type with an atomic or volatile subcomponent is a by-reference type, among other things.

Every value of a limited by-reference type is the value of one and only one limited object. The associated object of a value of a limited by-reference type is the object whose value it represents. Two values of a limited by-reference type are the same if and only if they represent the value of the same object.

We say “by-reference” above because these statements are not always true for limited private types whose underlying type is nonlimited (unfortunately).

For other parameters of other types, it is unspecified whether the parameter is passed by copy or by reference.
Discussion: {AI05-0005-1} There is no need to incorporate the discussion of AI83-00178, which requires pass-by-copy for certain kinds of actual parameters, while allowing pass-by-reference for others. This is because we explicitly indicate that a function creates an anonymous constant object for its result unless the type is a return by-reference type (see 6.5). We also provide a special dispensation for instances of Unchecked_Conversion to return by-reference, even if the result type is not a return by-reference type (see 13.9).

Bounded (Run-Time) Errors

11.a/3

Discussion: \{AI05-0240-1\} If one name denotes a part of a formal parameter, and a second name denotes a part of a distinct formal parameter or an object that is not part of a formal parameter, then the two names are considered distinct access paths. If an object is of a type for which the parameter passing mechanism is not specified and is not an explicitly aliased parameter, then it is a bounded error to assign to the object via one access path, and then read the value of the object via a distinct access path, unless the first access path denotes a part of a formal parameter that no longer exists at the point of the second access [(due to leaving the corresponding callable construct).] The possible consequences are that Program_Error is raised, or the newly assigned value is read, or some old value of the object is read.

12.a

Discussion: For example, if we call “P(X => Global_Variable, Y => Global_Variable)”, then within P, the names “X”, “Y”, and “Global_Variable” are all distinct access paths. If Global_Variable's type is neither pass-by-copy nor pass-by-reference, then it is a bounded error to assign to Global_Variable and then read X or Y, since the language does not specify whether the old or the new value would be read. On the other hand, if Global_Variable's type is pass-by-copy, then the old value would always be read, and there is no error. Similarly, if Global_Variable's type is defined by the language to be pass-by-reference, then the new value would always be read, and again there is no error.

12.b

Reason: We are saying assign here, not update, because updating any subcomponent is considered to update the enclosing object.

12.c

The “still exists” part is so that a read after the subprogram returns is OK.

12.d

If the parameter is of a by-copy type, then there is no issue here — the formal is not a view of the actual. If the parameter is of a by-reference type, then the programmer may depend on updates through one access path being visible through some other access path, just as if the parameter were of an access type.

12.e

Implementation Note: The implementation can keep a copy in a register of a parameter whose parameter-passing mechanism is not specified. If a different access path is used to update the object (creating a bounded error situation), then the implementation can still use the value of the register, even though the in-memory version of the object has been changed. However, to keep the error properly bounded, if the implementation chooses to read the in-memory version, it has to be consistent — it cannot then assume that something it has proven about the register is true of the memory location. For example, suppose the formal parameter is L, the value of L(6) is now in a register, and L(6) is used in an indexed_component as in “A(L(6)) := 99;”, where A has bounds 1..3. If the implementation can prove that the value for L(6) in the register is in the range 1..3, then it need not perform the constraint check if it uses the register value. However, if the memory value of L(6) has been changed to 4, and the implementation uses that memory value, then it had better not alter memory outside of A.

12.f

Note that the rule allows the implementation to pass a parameter by reference and then keep just part of it in a register, or, equivalently, to pass part of the parameter by reference and another part by copy.

12.g

Reason: We do not want to go so far as to say that the mere presence of aliasing is wrong. We wish to be able to write the following sorts of things in standard Ada:

12.h

procedure Move ( Source : in String; Target : out String; Drop : in Truncation := Error; Justify : in Alignment := Left; Pad : in Character := Space);  
--- Copies elements from Source to Target (safely if they overlap)

12.i

This is from the standard string handling package. It would be embarrassing if this couldn't be written in Ada!

12.j

The “then” before “read” in the rule implies that the implementation can move a read to an earlier place in the code, but not to a later place after a potentially aliased assignment. Thus, if the subprogram reads one of its parameters into a local variable, and then updates another potentially aliased one, the local copy is safe — it is known to have the old value. For example, the above-mentioned Move subprogram can be implemented by copying Source into a local variable before assigning into Target.

12.k

For an assignment_statement assigning one array parameter to another, the implementation has to check which direction to copy at run time, in general, in case the actual parameters are overlapping slices. For example:
procedure Copy(X : in out String; Y: String) is
begin
X := Y;
end Copy;

It would be wrong for the compiler to assume that X and Y do not overlap (unless, of course, it can prove otherwise).

NOTE 1 {AI12-0056-1} The mode of a formal parameter describes the direction of information transfer to or from the subprogram_body (see 6.1).

NOTE 2 A formal parameter of mode in is a constant view (see 3.3); it cannot be updated within the subprogram_body.

NOTE 3 {AI12-0056-1} {AI12-0440-1} A formal parameter of mode out can might be uninitialized at the start of the subprogram_body (see 6.4.1).

Extensions to Ada 83

The value of an out parameter may be read. An out parameter is treated like a declared variable without an explicit initial expression.

Wording Changes from Ada 83

Discussion of copy-in for parts of out parameters is now covered in 6.4.1, “Parameter Associations”.

The concept of a by-reference type is new to Ada 95.

We now cover in a general way in 3.7.2 the rule regarding erroneous execution when a discriminant is changed and one of the parameters depends on the discriminant.

Wording Changes from Ada 2005

{AI05-0096-1} Correction: Corrected so that limited derived types are by-reference only if their parent is.

{AI05-0142-4} Defined that explicitly aliased parameters (see 6.1) are always passed by reference.

Wording Changes from Ada 2012

{AI05-0027-1} Corrigendum: Corrected so that value conversions that are copies are the “associated object” for parameter passing of by-reference types. This can only happen if the conversion is between unrelated non-limited types, and it is necessary just so the correct object is defined.

6.3 Subprogram Bodies

[A subprogram_body specifies the execution of a subprogram.]

Syntax

{AI95-00218-03} {AI05-0183-1} subprogram_body ::= [overriding_indicator]

  subprogram_specification [aspect_specification] is declarative_part
  begin handled_sequence_of_statements end [designator];

If a designator appears at the end of a subprogram_body, it shall repeat the defining_designator of the subprogram_specification.

Legality Rules

{AI12-0444-1} In contrast to other bodies, a subprogram_body is allowed to be defined without it being need not be the completion of a previous declaration[. in which case the body declares the subprogram]. If the body is a completion, it shall be the completion of a subprogram_declaration or generic_subprogram_declaration. The profile of a subprogram_body that completes a declaration shall conform fully to that of the declaration.
Static Semantics

A subprogram_body is considered a declaration. It can either complete a previous declaration, or itself be the initial declaration of the subprogram.

Dynamic Semantics

The elaboration of a nongeneric subprogram_body has no other effect than to establish that the subprogram can from then on be called without failing the Elaboration_Check.

Ramification: See 12.2 for elaboration of a generic body. Note that protected subprogram_bodies never get elaborated; the elaboration of the containing protected_body allows them to be called without failing the Elaboration_Check.

The execution of a subprogram_body is invoked by a subprogram call. For this execution the declarative_part is elaborated, and the handled_sequence_of_statements is then executed.

Examples

Example of procedure body:

```ada
procedure Push(E : in Element_Type; S : in out Stack) is
begin
  if S.Index = S.Size then
    raise Stack_Overflow;
  else
    S.Index := S.Index + 1;
    S.Space(S.Index) := E;
  end if;
end Push;
```

Example of a function body:

```ada
function Dot_Product(Left, Right : Vector) return Real is
  Sum : Real := 0.0;
begin
  Check(Left'First = Right'First and Left'Last = Right'Last);
  for J in Left'Range loop
    Sum := Sum + Left(J)*Right(J);
  end loop;
  return Sum;
end Dot_Product;
```

Extensions to Ada 83

A renaming_declaration may be used instead of a subprogram_body.

Wording Changes from Ada 83

The syntax rule for subprogram_body now uses the syntactic category handled_sequence_of_statements.

The declarative_part of a subprogram_body is now required; that doesn't make any real difference, because a declarative_part can be empty.

We have incorporated some rules from RM83-6.5 here.

RM83 forgot to restrict the definition of elaboration of a subprogram_body to nongenerics.

Wording Changes from Ada 95

| {AI95-00218-03} Overriding_indicator is added to subprogram_body |

Extensions to Ada 2005

| {AI05-0183-1} An optional aspect_specification can be used in a subprogram_body. This is described in 13.1.1. |
6.3.1 Conformance Rules

[When subprogram profiles are given in more than one place, they are required to conform in one of four ways: type conformance, mode conformance, subtype conformance, or full conformance.]

Static Semantics

\{8652/0011\} \{AI95-00117-01\} [As explained in B.1, “Interfacing Aspects”, a \textit{convention} can be specified for an entity.] Unless this document states otherwise, the default convention of an entity is \textit{Ada}. [For a callable entity or access-to-subprogram type, the convention is called the \textit{calling convention}.) The following conventions are defined by the language:

- \{AI05-0229-1\} The default calling convention for any subprogram not listed below is \textit{Ada}. [The \texttt{Pragm} \texttt{Convention} aspect, \texttt{Import}, or \texttt{Export} may be specified used to override the default calling convention (see B.1)].

  Ramification: See also the rule about renamings-as-body in 8.5.4.

- The \textit{Intrinsic} calling convention represents subprograms that are “built in” to the compiler. The default calling convention is Intrinsic for the following:
  - an enumeration literal;
  - a "/=" operator declared implicitly due to the declaration of "/=" (see 6.6);
  - any other implicitly declared subprogram unless it is a dispatching operation of a tagged type;
  - an inherited subprogram of a generic formal tagged type with unknown discriminants;

Reason: Consider:

\begin{verbatim}
package P is
  type Root is tagged null record;
  procedure Proc(X: Root);
end P;

generic
  type Formal<> is new Root with private;
package G is
  ...;
end G;

package body G is
  ...;
  X: Formal := ...;
  ...;
  Proc(X); -- This is a dispatching call in Instance, because
  -- the actual type for Formal is class-wide.
  ...;
  -- Proc'Access would be illegal here, because it is of
  -- convention Intrinsic, by the above rule.
end G;

package body G is
  ...;
  Proc(X); -- This is a dispatching call in Instance, because
  -- the actual type for Formal is class-wide.
  ...;
  -- Proc'Access would be illegal here, because it is of
  -- convention Intrinsic, by the above rule.
end G;

package body G is
  ...;
  Proc(X); -- This is a dispatching call in Instance, because
  -- the actual type for Formal is class-wide.
  ...;
  -- Proc'Access would be illegal here, because it is of
  -- convention Intrinsic, by the above rule.
end G;

Within Instance, all calls to Proc will be dispatching calls, so Proc doesn't really exist in machine code, so we wish to avoid taking 'Access of it. This rule applies to those cases where the actual type might be class-wide, and makes these Intrinsic, thus forbidding 'Access.

- an attribute that is a subprogram;
- \{AI95-00252-01\} a subprogram declared immediately within a \texttt{protected_body}.
- \{AI95-00252-01\} \{AI95-00407-01\} \{AI12-0107-1\} any prefixed view of a subprogram (see 4.1.3) without synchronization kind (see 9.5) By \texttt{Entry} or \texttt{By Protected Procedure}.
10.a/5 **Reason:** [{AI12-0005-1}] The profile of a prefixed view is different from the “real” profile of the subprogram (it doesn’t have the first parameter), so we don’t want to be able to take ‘Access of it, as that would require generating a wrapper of some sort.

10.b/4 **Reason:** [{AI12-0107-1}] We except prefixed views that have synchronization kind By.Protected.Procedure so that they can be used with an access-to-protected-procedure type. These don’t require special wrappers (this is the normal form for a protected subprogram call). The By_Entry part is just for consistency (there is no access-to-entry type in Ada).

[The Access attribute is not allowed for Intrinsic subprograms.]

11.a **Ramification:** The Intrinsic calling convention really represents any number of calling conventions at the machine code level; the compiler might have a different instruction sequence for each intrinsic. That’s why the Access attribute is disallowed. We do not wish to require the implementation to generate an out of line body for an intrinsic.

11.b/3 **Reason:** [{AI05-0229-1}] Whenever we wish to disallow the Access attribute in order to ease implementation, we make the subprogram Intrinsic. Several language-defined subprograms have “pragma Convention => Intrinsic;”. An implementation might actually implement this as “pragma Import => True, Convention => (Intrinsic,);”, if there is really no body, and the implementation of the subprogram is built into the code generator.

11.c Subprograms declared in **protected bodies** will generally have a special calling convention so as to pass along the identification of the current instance of the protected type. The convention is not protected since such local subprograms need not contain any “locking” logic since they are not callable via “external” calls; this rule prevents an access value designating such a subprogram from being passed outside the protected unit.

11.d The “implicitly declared subprogram” above refers to predefined operators (other than the “=” of a tagged type) and the inherited subprograms of untagged types.

12/4 • [{AI12-0107-1}] {AI12-0159-1} The default calling convention is protected for a prefixed view of a subprogram with a synchronization kind of By.Protected.Procedure, and for an access-to-subprogram type with the reserved word protected in its definition.

13/4 • [{AI12-0107-1}] {AI12-0159-1} The default calling convention is entry for an entry and for a prefixed view of a subprogram with a synchronization kind of By.Entry.

13.1/5 • [{AI95-00254-01}] {AI95-00409-01} {AI05-0264-1} {AI12-0207-1} The calling convention for an anonymous access-to-subprogram parameter or anonymous access-to-subprogram result is protected if the reserved word protected appears in its definition; and otherwise it is the convention of the entity subprogram that has the parameter or result, unless that entity has convention protected, entry, or Intrinsic, in which case the convention is Ada.

13.a/2 **Ramification:** The calling convention for other anonymous access-to-subprogram types is Ada.

13.2/1 • [{8652/0011}] {AI95-00117-01} If not specified above as Intrinsic, the calling convention for any inherited or overriding dispatching operation of a tagged type is that of the corresponding subprogram of the parent type. The default calling convention for a new dispatching operation of a tagged type is the convention of the type.

13.a/1/1 **Reason:** The first rule is officially stated in 3.9.2. The second is intended to make interfacing to foreign OOP languages easier, by making the default be that the type and operations all have the same convention.

14/3 **Reason:** [{AI05-0229-1}] Of these four conventions, only Ada and Intrinsic are allowed as a convention_identifier in the specification of a pragma Convention aspect, Import, or Export.

14.a/3 **Discussion:** [{AI05-0229-1}] The names of the protected and entry calling conventions cannot be used in the specification of Convention interfacing pragmas. Note that protected and entry are reserved words.

15/2 **Reason:** [{AI95-00409-01}] Two profiles are type conformant if they have the same number of parameters, and both have a result if either does, and corresponding parameter and result types are the same, or for access parameters or access results, corresponding designated types are the same, or corresponding designated profiles are type conformant.

15.a/2 **Discussion:** [{AI95-00409-01}] For anonymous access-to-object(parameters, the designated types have to be the same for type conformance, not the access types, since in general each access parameter has its own anonymous access type, created when the subprogram is called. Of course, corresponding parameters have to be either both access parameters or both not access parameters.
Similarly, for anonymous access-to-subprogram parameters, the designated profiles of the types, not the types themselves, have to be conformant.

Two profiles are mode conformant if they are type conformant, and corresponding parameters have identical modes, and, for access parameters or access result types, the designated subtypes statically match, or the designated profiles are subtype conformant.

- they are type conformant; and
- corresponding parameters have identical modes and both or neither are explicitly aliased parameters; and
- for corresponding access parameters and any access result type, the designated subtypes statically match and either both or neither are access-to-constant, or the designated profiles are subtype conformant.

Two profiles are subtype conformant if they are mode conformant, corresponding subtypes of the profile statically match, and the associated calling conventions are the same. The profile of a generic formal subprogram is not subtype conformant with any other profile.

Ramication:

Two profiles are fully conformant if they are subtype conformant, if they have access-to-subprogram results whose designated profiles are fully conformant, and for corresponding parameters, have the same names and have default expressions that are fully conformant with one another.

- they have the same names; and
- both or neither have null_exclusions; and
- neither have default expressions, or they both have default expressions that are fully conformant with one another; and
- for access-to-subprogram parameters, the designated profiles are fully conformant.

Ramication: Full conformance requires subtype conformance, which requires the same calling conventions. However, the calling convention of the declaration and body of a subprogram or entry are always the same by definition.

Reason: The part about null_exclusions is necessary to prevent controlling parameters from having different exclusions, as such a parameter is defined to exclude null whether or not an exclusion is given.

The parts about access-to-subprogram parameters and results is necessary to prevent such types from having different default expressions in the specification and body of a subprogram. If that was allowed, it would be undefined which default_expression was used in a call of an access-to-subprogram parameter.

Two expressions are fully conformant if, [after replacing each use of an operator with the equivalent function_call:]

- each constituent construct of one corresponds to an instance of the same syntactic category in the other, except that an expanded name may correspond to a direct_name (or character_literal) or to a different expanded name in the other; and

- corresponding defining identifiers occurring within the two expressions are the same; and

- each direct_name, character_literal, and selector_name that is not part of the prefix of an expanded name in one denotes the same declaration as the corresponding direct_name, character_literal, or selector_name in the other, or they denote corresponding declarations occurring within the two expressions; and

Ramication: Note that it doesn't say “respectively” because a direct_name can correspond to a selector_name, and vice-versa, by the previous bullet. This rule allows the prefix of an expanded name to be
removed, or replaced with a different prefix that denotes a renaming of the same entity. However, it does not allow a direct_name or selector_name to be replaced with one denoting a distinct renaming (except for direct_names and selector_names in prefixes of expanded names). Note that calls using operator notation are equivalent to calls using prefix notation.

21.b

Given the following declarations:

21.c

package A is
  function F(X : Integer := 1) return Boolean;
end A;

{AI05-0005-1} with A;

package B is
  package A_View renames A;
  function F_View(X : Integer := 9999) return Boolean renames A.F;
end B;

with A, B;

procedure Main is
...

Within Main, the expressions “F”, “A.F”, “B.A_View.F”, and “A_View.F” are all fully conformant with one another. However, “F” and “F_View” are not fully conformant. If they were, it would be bad news, since the two denoted views have different default_expressions.

Discussion: {AI12-0050-1} We talk about defining_identifier and "corresponding declarations" because of the possibility of iterator specifications occurring within the expressions; each iterator_specification is a separate declaration, which we need to allow, but we do want to require that the defining_identifier are the same.

21.e

• {8652/0018} {AI95-00175-01} {AI05-0092-1} each attribute_designator in one is the same as the corresponding attribute_designator in the other; and

21.f/4

• {AI12-0342-1} each primary that is a literal in one is a user-defined literal if and only if the corresponding literal in the other is also a user-defined literal. Furthermore, if neither are user-defined literals then they shall have the same values, but they may have differing textual representations; if both are user-defined literals then they shall have the same textual representation has the same value as the corresponding literal in the other.

Ramification: {AI12-0342-1} This rule applies to character litersals, so even though other rules would allow a rename of a character literal to conform to the literal, this rule prevents that: The literals may be written differently.

22.a/5

Ramification: Note that the above definition makes full conformance a transitive relation.

23

Two known_discriminant_parts are fully conformant if they have the same number of discriminants, and discriminants in the same positions have the same names, statically matching subtypes, and default_expressions that are fully conformant with one another.

24

Two discrete_subtype_definitions are fully conformant if they are both subtype_indications or are both ranges, the subtype_marks (if any) denote the same subtype, and the corresponding simple_expressions of the ranges (if any) fully conform.

Ramification: In the subtype_indication case, any ranges have to be corresponding; that is, two subtype_indications cannot conform unless both or neither has a range.

Discussion: This definition is used in 9.5.2, “Entries and Accept Statements” for the conformance required between the discrete_subtype_definitions of an entry_declaration for a family of entries and the corresponding entry_index_specification of the entry_body.

The prefixed view profile of a subprogram is the profile obtained by omitting the first parameter of that subprogram. There is no prefixed view profile for a parameterless subprogram. For the purposes of defining subtype and mode conformance, the convention of a prefixed view profile is considered to match that of either an entry or a protected operation.

Discussion: This definition is used to define how primitive subprograms of interfaces match operations in task and protected type definitions (see 9.1 and 9.4).

Reason: The weird rule about conventions is pretty much required for synchronized interfaces to make any sense. There will be wrappers all over the place for interfaces anyway. Of course, this doesn't imply that entries have the same convention as protected operations.
An implementation may declare an operator declared in a language-defined library unit to be intrinsic.

NOTE {AI12-0398-1} Any conformance requirements between aspect specifications that are part of a profile or known discriminant part are defined by the semantics of each particular aspect. In particular, there is no general requirement for aspect specifications to match in conforming profiles or discriminant parts.

Extensions to Ada 83

The rules for full conformance are relaxed — they are now based on the structure of constructs, rather than the sequence of lexical elements. This implies, for example, that "(X, Y: T)" conforms fully with "(X: T; Y: T)", and "(X: T)" conforms fully with "(X: in T)".

Wording Changes from Ada 95

{8652/0011} {AI95-00117-01} **Corrigendum:** Clarified that the default convention is Ada. Also clarified that the convention of a primitive operation of a tagged type is the same as that of the type.

{8652/0018} {AI95-00175-01} **Corrigendum:** Added wording to ensure that two attributes conform only if they have the same attribute_designator.

{AI95-00252-01} {AI95-00254-01} {AI95-00407-01} Defined the calling convention for anonymous access-to-subprogram types and for prefixed views of subprograms (see 4.1.3).

{AI95-00318-02} Defined the conformance of access result types (see 6.1).

{AI95-00345-01} {AI95-00397-01} Defined the prefixed view profile of subprograms for later use.

{AI95-00409-01} Defined the conformance of anonymous access-to-subprogram parameters.

Incompatibilities With Ada 2005

{AI05-0046-1} **Correction:** Now require null_exclusions to match for full conformance. While this is technically incompatible with Ada 2005 as defined by Amendment 1, it is a new Ada 2005 feature and it is unlikely that users have been intentionally taking advantage of the ability to write mismatching exclusions. In any case, it is easy to fix: add a null_exclusion where needed for conformance.

{AI05-0134-1} **Correction:** Now require full conformance of anonymous access-to-subprogram parameters and results for full conformance. This is necessary so that there is no confusion about the default expression that is used for a call. While this is technically incompatible with Ada 2005 as defined by Amendment 1, it is a new Ada 2005 feature and it is unlikely that users have been intentionally taking advantage and writing different default expressions. In any case, it is easy to fix: change any default expressions that don't conform so that they do conform.

{AI05-0207-1} **Correction:** Now include the presence or absence of constant in access parameters to be considered when checking mode conformance. This is necessary to prevent modification of constants. While this is technically incompatible with Ada 2005 as defined by Amendment 1, it is a new Ada 2005 feature and it is unlikely that users have been intentionally taking advantage and writing mismatching access types.

Wording Changes from Ada 2005

{AI05-0142-4} Explicitly aliased parameters are included as part of mode conformance (since it affects the parameter passing mechanism).

Incompatibilities With Ada 2012

{AI12-0207-1} **Correction:** The convention of an anonymous access-to-subprogram parameter of a protected entry or subprogram is Ada; if one wants it to be protected it can be declared with the keyword protected. This is incompatible, but only in a very rare case; usually the intent is to pass a normal subprogram to a protected subprogram (and this was impossible in Ada 2012).

Extensions to Ada 2012

{AI12-0107-1} {AI12-0159-1} **Corrigendum:** We now define that a prefixed view of a subprogram with synchronization kind By_Protected_Procedure can be used as the prefix of 'Access for an access-to-protected type. We consider this a correction as it certainly appears that it ought to work, but in original Ada 2012 it would have had a convention mismatch.
6.3.1 Conformance Rules

Wording Changes from Ada 2012

{AI12-0050-1} Corrigendum: We now define how two expressions containing quantified expressions can fully conform. This wasn't incompatible, as the original Ada 2012 never allowed such expressions to conform (the declarations in each formally being different). Neither is it an extension as one would expect these to conform.

{AI12-0342-1} The conformance of literals is tightened up to not assume anything about the value of a user-defined literal.

6.3.2 Inline Expansion of Subprograms

[Subprograms may be expanded in line at the call site.]

{AI05-0229-1} The form of a pragma Inline, which is a program unit pragma (see 10.1.5), is as follows:

```
pragma Inline(name {, name});
```

Legality Rules

{AI05-0229-1} The pragma shall apply to one or more callable entities or generic subprograms.

Static Semantics

{AI05-0229-1} For if a pragma Inline applies to a callable entity or a generic subprogram, the following language-defined representation aspect may be specified: this indicates that inline expansion is desired for all calls to all instances of that generic subprogram.

5.1/3 Inline

The type of aspect Inline is Boolean. When aspect Inline is True for a callable entity, inline expansion is desired for all calls to that entity. When aspect Inline is True for a generic subprogram, inline expansion is desired for all calls to all instances of that generic subprogram.

5.2/3 If directly specified, the aspect definition shall be a static expression. [This aspect is never inherited;] if not directly specified, the aspect is False.

5.a/3 Aspect Description for Inline: For efficiency, Inline calls are requested for a subprogram.

5.b/3 This paragraph was deleted. Ramification: {AI05-0229-1} Note that inline expansion is desired no matter what name is used in the call. This allows one to request inlining for only one of several overloaded subprograms as follows:

5.c/3 This paragraph was deleted. package IO is

```
procedure Put(X : in Integer);
procedure Put(X : in String);
procedure Put(X : in Character);
private
  procedure Character_Put(X : in Character) renames Put;
pragma Inline(Character_Put);
end IO;
```

5.d/3 This paragraph was deleted. with IO, use IO.

procedure Main is

```
I : Integer;
C : Character;
begin
  Put(I); -- Inline expansion is desired
  Put(C); -- Inline expansion is NOT desired
end Main;
```

5.e/3 Ramification: {AI05-0229-1} The meaning of a subprogram can be changed by inline expansion as requested by aspect pragma Inline only in the presence of failing checks (see 11.6).
Implementation Permissions

For each call, an implementation is free to follow or to ignore the recommendation determined expressed by the Inline aspect pragma.

Ramification: Note, in particular, that the recommendation cannot always be followed for a recursive call, and is often infeasible for entries. Note also that the implementation can inline calls even when no such desire was expressed via the Inline aspect by a pragma, so long as the semantics of the program remains unchanged.

An implementation may allow a pragma Inline that has an argument which is a direct name denoting a subprogram_body of the same declarative_part.

Reason: This is allowed for Ada 83 compatibility. This is only a permission as this usage is considered obsolescent.

Discussion: We only need to allow this in declarative_parts, because a body is only allowed in another body, and these all have declarative_parts.

NOTE The name in a pragma Inline can denote more than one entity in the case of overloading. Such a pragma applies to all of the denoted entities.

Incompatibilities With Ada 83

This paragraph was deleted.

A pragma Inline cannot refer to a subprogram_body outside of that body. The pragma can be given inside of the subprogram_body. Ada 2005 adds an Implementation Permission to allow this usage for compatibility (and Ada 95 implementations also can use this permission), but implementations do not have to allow such pragmas.

Extensions to Ada 83

This paragraph was deleted.

A pragma Inline is allowed inside a subprogram_body if there is no corresponding subprogram_declaration. This is for uniformity with other program unit pragmas.

Extensions to Ada 95

This paragraph was deleted.

Amendment Correction: Implementations are allowed to letPragma Inline apply to a subprogram_body.

Extensions to Ada 2005

Aspect Inline is new; pragma Inline is now obsolescent.

6.4 Subprogram Calls

A subprogram call is either a procedure_call_statement or a function_call; it invokes the execution of the subprogram_body. The call specifies the association of the actual parameters, if any, with formal parameters of the subprogram.

Syntax

procedure_call_statement ::= procedure_name;
| procedure_prefix actual_parameter_part;

function_call ::= function_name
| function_prefix actual_parameter_part

To be honest: For the purpose of non-syntactic rules, infix operator calls are considered function_calls.

actual_parameter_part ::= (parameter_association {, parameter_association})

parameter_association ::= [formal_parameter_selector_name =>] explicit_actual_parameter
6.4 Subprogram Calls

explicit_actual_parameter ::= expression | variable_name

{AI12-0416-1} A parameter_association is named or positional according to whether or not the formal_parameter_selector_name is specified. For the parameter_associations of a single actual_parameter_part or iterator_actual_parameter_part, any positional associations shall precede any named associations. Named associations are not allowed if the prefix in a subprogram call is an attribute_reference.

Ramification: This means that the formal parameter names used in describing predefined attributes are to aid presentation of their semantics, but are not intended for use in actual calls.

Name Resolution Rules

{AI95-00310-01} The name or prefix given in a procedure_call_statement shall resolve to denote a callable entity that is a procedure, or an entry renamed as (viewed as) a procedure. The name or prefix given in a function_call shall resolve to denote a callable entity that is a function. The name or prefix shall not resolve to denote an abstract subprogram unless it is also a dispatching subprogram. [When there is an actual_parameter_part, the prefix can be an implicit_dereference of an access-to-subprogram value.]

Discussion: {AI95-00310-01} This rule is talking about dispatching operations (which is a static concept) and not about dispatching calls (which is a dynamic concept).

Ramification: The function can be an operator, enumeration literal, attribute that is a function, etc.

A subprogram call shall contain at most one association for each formal parameter. Each formal parameter without an association shall have a default_expression (in the profile of the view denoted by the name or prefix). [This rule is an overloading rule (see 8.6).]

Proof: {AI05-0240-1} All Name Resolution Rules are overloading rules, see 8.6.

Static Semantics

{AI95-00407-01} {AI12-0416-1} If the name or prefix of a subprogram call denotes a prefixed view (see 4.1.3), the subprogram call is equivalent to a call on the underlying subprogram, with the first actual parameter being provided by the prefix of the prefixed view (or the Access attribute of this prefix if the first formal parameter is an access parameter), and the remaining actual parameters given by the actual_parameter_part, if any.

Dynamic Semantics

{AI95-00345-01} For the execution of a subprogram call, the name or prefix of the call is evaluated, and each parameter_association is evaluated (see 6.4.1). If a default_expression is used, an implicit parameter_association is assumed for this rule. These evaluations are done in an arbitrary order. The subprogram_body is then executed, or a call on an entry or protected subprogram is performed (see 3.9.2). Finally, if the subprogram completes normally, then after it is left, any necessary assigning back of formal to actual parameters occurs (see 6.4.1).

Discussion: The implicit association for a default is only for this run-time rule. At compile time, the visibility rules are applied to the default at the place where it occurs, not at the place of a call.

To be honest: If the subprogram is inherited, see 3.4, “Derived Types and Classes”.

If the subprogram is protected, see 9.5.1, “Protected Subprograms and Protected Actions”.

If the subprogram is really a renaming of an entry, see 9.5.3, “Entry Calls”.

{AI95-00345-01} If the subprogram is implemented by an entry or protected subprogram, it will be treated as a dispatching call to the corresponding entry (see 9.5.3, “Entry Calls”) or protected subprogram (see 9.5.1, “Protected Subprograms and Protected Actions”).

{AI95-00348-01} Normally, the subprogram_body that is executed by the above rule is the one for the subprogram being called. For an enumeration literal, implicitly declared (but noninherited) subprogram, null procedure, or an
attribute that is a subprogram, an implicit body is assumed. For a dispatching call, 3.9.2, “Dispatching Operations of Tagged Types” defines which subprogram_body is executed.

\{AI95-00407-01\} \{AI12-0416-1\} If the name or prefix of a subprogram call denotes a prefixed view (see 4.1.3), the subprogram call is equivalent to a call on the underlying subprogram, with the first actual parameter being provided by the prefix of the prefixed view (or the Access attribute of this prefix if the first_formal_parameter is an access parameter), and the remaining actual parameters given by the actual_parameter_part, if any.

\{AI95-00318-02\} The exception Program_Error is raised at the point of a function_call if the function completes normally without executing a return_statement.

Discussion: We are committing to raising the exception at the point of call, for uniformity — see AI83-00152. This happens after the function is left, of course.

Note that there is no name for suppressing this check, since the check imposes no time overhead and minimal space overhead (since it can usually be statically eliminated as dead code).

\{AI95-00231-01\} A function_call denotes a constant, as defined in 6.5; the nominal subtype of the constant is given by the nominal_result subtype of the function result.

Examples

Examples of procedure calls:

Traverse_Tree; -- see 6.1
Print_Header(128, Title, True); -- see 6.1
Switch(From => X, To => Next); -- see 6.1
Print_Header(128, Header => Title, Center => True); -- see 6.1
Print_Header(Header => Title, Center => True, Pages => 128); -- see 6.1

Examples of function calls:

Dot_Product(U, V) -- see 6.1 and 6.3
Clock -- see 9.6
F.all -- presuming F is of an access-to-subprogram type — see 3.10

Examples of procedures with default expressions:

procedure Activate(Process : in Process_Name;
   After   : in Process_Name := No_Process;
   Wait    : in Duration := 0.0;
   Prior   : in Boolean := False);

\{AI05-0299-1\} procedure Pair(Left, Right : in Person_Name := new Person(M)); -- see 3.10

Examples of their calls:

Activate(X);
Activate(X, After => Y);
Activate(X, Wait => 60.0, Prior => True);
Activate(X, Y, 10.0, False);

\{AI05-0299-1\} Pair;
Pair(Left => new Person(F), Right => new Person(M));

NOTE If a default_expression is used for two or more parameters in a multiple parameter_specification, the default_expression is evaluated once for each omitted parameter. Hence in the above examples, the two calls of Pair are equivalent.

Examples

Examples of overloaded subprograms:

procedure Put(X : in Integer);
procedure Put(X : in String);
procedure Set(Tint   : in Color);
procedure Set(Signal : in Light);
Examples of their calls:

```ada
Put(28);
Put("no possible ambiguity here");
Set(Tint => Red);
Set(Signal => Red);
Set(Color'(Red));
```

```
{AI12-0440-1} -- Set(Red) would be ambiguous since Red cannot denote a value either of type Color or of type Light
```

Wording Changes from Ada 83

31.a We have gotten rid of parameters “of the form of a type conversion” (see RM83-6.4.1(3)). The new view semantics of type conversions allows us to use normal type conversions instead.

31.b We have moved wording about run-time semantics of parameter associations to 6.4.1.

31.c We have moved wording about raising Program_Error for a function that falls off the end to here from RM83-6.5.

Extensions to Ada 95

31.d/2 {AI95-00310-01} Nondispatching abstract operations are no longer considered when resolving a subprogram call. That makes it possible to use abstract to “undefine” a predefined operation for an untagged type. That's especially helpful when defining custom arithmetic packages.

Wording Changes from Ada 95

31.e/2 {AI95-00231-01} Changed the definition of the nominal subtype of a function_call to use the nominal subtype wording of 6.1, to take into account null_exclusions and access result types.

31.f/2 {AI95-00345-01} Added wording to clarify that the meaning of a call on a subprogram “implemented by” an entry or protected operation is defined by 3.9.2.

31.g/2 {AI95-00407-01} Defined the meaning of a call on a prefixed view of a subprogram (see 4.1.3).

Wording Changes from Ada 2012

31.h/5 {AI12-0416-1} Moved the equivalence definition for a prefixed view to Static Semantics, in order that it is clear Legality Rules that apply to calls and the parameters of calls apply to prefixed views (including the prefix).

6.4.1 Parameter Associations

[A parameter association defines the association between an actual parameter and a formal parameter.]

Language Design Principles

1.a The parameter passing rules for out parameters are designed to ensure that the parts of a type that have implicit initial values (see 3.3.1) don't become “de-initialized” by being passed as an out parameter.

1.b/3 {AI05-0142-4} For explicitly aliased parameters of functions, we will ensure at the call site that a part of the parameter can be returned as part of the function result without creating a dangling pointer. We do this with accessibility checks at the call site that all actual objects of explicitly aliased parameters live at least as long as the function result; then we can allow them to be returned as access discriminants or anonymous access results, as those have the master of the function result.

Name Resolution Rules

2/3 {AI05-0118-1} The formal_parameter_selector_name of a named parameter_association shall resolve to denote a parameter_specification of the view being called; this is the formal parameter of the association. The formal parameter for a positional parameter_association is the parameter with the corresponding position in the formal part of the view being called.

To be honest: {AI05-0118-1} For positional parameters, the “corresponding position” is calculated after any transformation of prefixed views.

2.a/3 The actual parameter is either the explicit_actual_parameter given in a parameter_association for a given formal parameter, or the corresponding default_expression if no parameter_association is given.
for the formal parameter. The expected type for an actual parameter is the type of the corresponding formal parameter.

To be honest: The corresponding default_expression is the one of the corresponding formal parameter in the profile of the view denoted by the name or prefix of the call.

If the mode is in, the actual is interpreted as an expression; otherwise, the actual is interpreted only as a name, if possible.

Ramification: {AI12-0005-1} This formally resolves the ambiguity present in the syntax rule for explicit_actual_parameter. This matters as an expression that is a name is evaluated and represents a value while a name by itself can be an object; if the mode is not in, we want the parameter to interpreted as an object. Note that we don't actually require that the actual be a name if the mode is not in; we do that below.

{AI12-0005-1} This wording uses "interpreted as" rather than "shall be" so that this rule is not used to resolve overloading; it is solely about evaluation as described above. We definitely do not want to allow oddities like the presence of parentheses requiring the selection of an in formal parameter as opposed to an otherwise matching in out parameter.

Legality Rules

If the mode is in out or out, the actual shall be a name that denotes a variable.

Discussion: {AI12-0005-1} We no longer need “or a type_conversion whose argument is the name of a variable”, because a type_conversion is now a name, and a view_conversion type_conversion of a variable is a variable while any other conversion (which should not be legal here) is a constant.

Reason: The requirement that the actual be a (variable) name is not an overload resolution rule, since we don't want the difference between expression and name to be used to resolve overloading. For example:

```ada
procedure Print(X : in Integer; Y : in Boolean := True);
procedure Print(Z : in out Integer);

Print(3); -- Ambiguous!
```

The above call to Print is ambiguous even though the call is not compatible with the second Print which requires an actual that is a (variable) name ("3" is an expression, not a name). This requirement is a legality rule, so overload resolution fails before it is considered, meaning that the call is ambiguous.

{AI12-0074-1} {AI12-0159-1} {AI12-0377-1} If the mode is out, the actual parameter is a view conversion, and the type of the formal parameter is an access type or a scalar type that has the Default_Value aspect specified, then

- neither there shall exist a type (other than a root numeric type) that is an ancestor of both the target type nor and the operand type has the Default_Value aspect specified; or
- both the target type and in the case of a scalar type, the type of the operand type of the conversion shall have the Default_Value aspect specified, and there shall exist a type (other than a root numeric type) that is an ancestor of both the target type and the operand type.

{AI12-0074-1} {AI12-0159-1} In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

Reason: These rules are needed in order to ensure that a well-defined parameter value is passed.

{AI05-0102-1} {AI05-0142-4} If the formal parameter is an explicitly aliased parameter, the type of the actual parameter shall be tagged or the actual parameter shall be an aliased view of an object. Further, if the formal parameter subtype F is untagged. The type of the actual parameter associated with an access parameter shall be convertible (see 4.6) to its anonymous access type.

- the subtype F shall statically match the nominal subtype of the actual object; or
- the subtype F shall be unconstrained, discriminated in its full view, and unconstrained in any partial view.
Ramification: Tagged objects (and tagged aggregates for in parameters) do not need to be aliased. This matches the behavior of unaliased formal parameters of tagged types, which allow 'Access to be taken of the formal parameter regardless of the form of the actual parameter.

Reason: We need the subtype check on untagged actual parameters so that the requirements of 'Access are not lost. 'Access makes its checks against the nominal subtype of its prefix, and parameter passing can change that subtype. But we don't want this parameter passing to change the objects that would be allowed as the prefix of 'Access. This is particularly important for arrays, where we don't want to require any additional implementation burden.

Discussion: \{AI12-0095-1\} We assume the worst in a generic body regarding whether or not a formal subtype has a constrained partial view; specifically, in a generic body a discriminated subtype is considered to have a constrained partial view if it is a descendant of an untagged generic formal private or derived type (see 12.5.1 for the formal definition of this rule).

{AI12-0095-1} In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

{AI05-0142-4} {AI05-0234-1} In a function call, the accessibility level of the actual object for each explicitly aliased parameter shall not be statically deeper than the accessibility level of the master of the call (see 3.10.2).

Discussion: Since explicitly aliased parameters are either tagged or required to be objects, there is always an object (possibly anonymous) to talk about. This is discussing the static accessibility level of the actual object; it does not depend on any runtime information (for instance when the actual object is a formal parameter of another subprogram, it does not depend on the actual parameter of that other subprogram).

Ramification: \{AI12-0095-1\} This accessibility check (and its dynamic cousin as well) can only fail if the master of the function call (which is defined in the Heart of Darkness, or 3.10.2 if you prefer) is different than the master directly enclosing the call (function call is used to directly initialize a built-in-place object with a master different than that enclosing the call. The most likely case where this will occur all of those conditions exist is in the initializer of an allocator; in almost all other cases this check will always pass.

{AI05-0144-2} Two names are known to denote the same object if:

- both names statically denote the same stand-alone object or parameter; or
- both names are selected components, their prefixes are known to denote the same object, and their selector names denote the same component; or
- both names are dereferences (implicit or explicit) and the dereferenced names are known to denote the same object; or
- both names are indexed components, their prefixes are known to denote the same object, and each of the pairs of corresponding index values are either both static expressions with the same static value or both names that are known to denote the same object; or
- both names are slices, their prefixes are known to denote the same object, and the two slices have statically matching index constraints; or
- one of the two names statically denotes a renaming declaration whose renamed object name is known to denote the same object as the other, the prefix of any dereference within the renamed object name is not a variable, and any expression within the renamed object name contains no references to variables or calls on nonstatic functions.

Reason: This exposes known renamings of slices, indexing, and so on to this definition. In particular, if we have

```ada
C : Character renames S(1);  
then C and S(1) are known to denote the same object.
```

We need the requirement that no variables occur in the prefixes of dereferences and in (index) expressions of the renamed object in order to avoid problems from later changes to those parts of renamed names. Consider:

```ada
type Ref is access Some_Type;  
__Ptr : Ref := new Some_Type'(...);  
X : Some_Type renames __Ptr.all;  
begin  
  __Ptr := new Some_Type'(...);  
  P (Func With Out_Params (Ptr.all), X);
```

6.4.1 Parameter Associations
X and \texttt{Ptr.all} should not be known to denote the same object, since they denote different allocated objects (and this is not an unreasonable thing to do).

\textbf{To be honest:} The exclusion of variables from renamed object \texttt{names} is not enough to prevent altering the value of the name or expression by another access path. For instance, both \texttt{in} parameters passed by reference and access-to-constant values can designate variables. For the intended use of "known to be the same object", this is OK; the modification via another access path is very tricky and it is OK to reject code that would be buggy except for the tricky code. Assuming \texttt{Element} is an elementary type, consider the following example:

\begin{verbatim}
Global : Tagged_Type;
procedure Foo (Param : in Tagged_Type := Global) is
   X : Element renames Some_Global_Array (Param.C);
begin
   Global.C := Global.C + 1;
   Swap (X, Some_Global_Array (Param.C));
\end{verbatim}

The rules will flag the call of procedure \texttt{Swap} as illegal, since \texttt{X} and \texttt{Some_Global_Array (Param.C)} are known to denote the same object (even though they will actually represent different objects if \texttt{Param = Global}). But this is only incorrect if the parameter actually is \texttt{Global} and not some other value; the error could exist for some calls. So this flagging seems harmless.

Similar examples can be constructed using stand-alone composite constants with controlled or immutably limited components, and (as previously noted) with dereferences of access-to-constant values. Even when these examples flag a call incorrectly, that call depends on very tricky code (modifying the value of a constant); the code is likely to confuse future maintainers as well and thus we do not mind rejecting it.

\textbf{Discussion:} Whether or not names or prefixes are known to denote the same object is determined statically. If the name contains some dynamic portion other than a dereference, \texttt{indexed \texttt{component}}, or \texttt{slice}, it is not "known to denote the same object".

These rules make no attempt to handle slices of objects that are known to be the same when the slices have dynamic bounds (other than the trivial case of bounds being defined by the same subtype), even when the bounds could be proven to be the same, as it is just too complex to get right and these rules are intended to be conservative.

\textbf{Ramification:} "Known to denote the same object" is intended to be an equivalence relationship, that is, it is reflexive, symmetric, and transitive. We believe this follows from the rules. For instance, given the following declarations:

\begin{verbatim}
S : String(1..10);
ONE : constant Natural := 1;
R : Character renames S(1);
\end{verbatim}

the names \texttt{R} and \texttt{S(1)} are known to denote the same object by the sixth bullet, and \texttt{S(1)} and \texttt{S(ONE)} are known to denote the same object by the fourth bullet, so using the sixth bullet on \texttt{R} and \texttt{S(ONE)}, we simply have to test \texttt{S(1)} vs. \texttt{S(ONE)}, which we already know denote the same object.

\begin{itemize}
\item \texttt{Two names are known to refer to the same object if}
\begin{itemize}
\item The two names are known to denote the same object; or
\item One of the names is a \texttt{selected \texttt{component}}, \texttt{indexed \texttt{component}}, or \texttt{slice} and its prefix is known to refer to the same object as the other name; or
\item One of the two names statically denotes a renaming declaration whose renamed \texttt{object \texttt{name}} is known to refer to the same object as the other name.
\end{itemize}
\end{itemize}

\textbf{Reason:} This ensures that names Prefix Comp and Prefix are known to refer to the same object for the purposes of the rules below. This intentionally does not include dereferences; we only want to worry about accesses to the same object, and a dereference changes the object in question. (There is nothing shared between an access value and the object it designates.)

\begin{itemize}
\item \texttt{If a call \texttt{C} has two or more parameters of mode \texttt{in out or out} that are of an elementary type, then the call is legal only if:}
\begin{itemize}
\item \texttt{For each name \texttt{N} denoting an object of an elementary type that is passed as a parameter of mode \texttt{in out or out} to the call \texttt{C}, there is no other name among the other parameters of mode \texttt{in out or out} to \texttt{C} that is known to denote the same object.}
\end{itemize}
\end{itemize}

\textbf{To be honest:} This means \textit{visibly} an elementary type; it does not include partial views of elementary types (partial views are always composite). That's necessary to avoid having Legality Rules depend on the contents of the private part.
If a construct C has two or more direct constituents that are names or expressions whose evaluation may occur in an arbitrary order, at least one of which contains a function call with an in out or out parameter, then the construct is legal only if:

**Ramification:** All of the places where the language allows an arbitrary order can be found by looking in the index under “arbitrary order, allowed”. Note that this listing includes places that don’t involve names or expressions (such as checks or finalization).

- For each name N that is passed as a parameter of mode in out or out to some inner function call C2 (not including the construct C itself), there is no other name anywhere within a direct constituent of the construct C other than the one containing C2, that is known to refer to the same object.

**Ramification:** This requirement cannot fail for a procedure or entry call alone; there must be at least one function with an in out or out parameter called as part of a parameter expression of the call in order for it to fail.

**Reason:** These rules prevent obvious cases of dependence on the order of evaluation of names or expressions. Such dependence is usually a bug, and in any case, is not portable to another implementation (or even another optimization setting).

In the case that the top-level construct C is a call, these rules do not require checks for most in out parameters, as the rules about evaluation of calls prevent problems. Similarly, we do not need checks for short circuit operations or other operations with a defined order of evaluation. The rules about arbitrary order (see 1.1.4) allow evaluating parameters and writing parameters back in an arbitrary order, but not interleaving of evaluating parameters of one call with writing parameters back from another — that would not correspond to any allowed sequential order.

For the purposes of checking this rule:

- For an array aggregate, an expression associated with a discrete_choice_list that has two or more discrete choices, or that has a nonstatic range, is considered as two or more separate occurrences of the expression;

- For a record aggregate:
  - The expression of a record_component_association is considered to occur once for each associated component; and
  - The default_expression for each record_component_association with <> for which the associated component has a default_expression is considered part of the aggregate;

- For a call, any default_expression evaluated as part of the call is considered part of the call.

**Ramification:** We do not check expressions that are evaluated only because of a component initialized by default in an aggregate (via <>).

### Dynamic Semantics

For the evaluation of a parameter_association:

- The actual parameter is first evaluated.
- For an access parameter, the access_definition is elaborated, which creates the anonymous access type.
- For a parameter [(of any mode)] that is passed by reference (see 6.2), a view conversion of the actual parameter to the nominal subtype of the formal parameter is evaluated, and the formal parameter denotes that conversion.

**Discussion:** We are always allowing sliding, even for [in] out by-reference parameters.

- For an in or in out parameter that is passed by copy (see 6.2), the formal parameter object is created, and the value of the actual parameter is converted to the nominal subtype of the formal parameter and assigned to the formal.

**Ramification:** The conversion mentioned here is a value conversion.
For an `out` parameter that is passed by copy, the formal parameter object is created, and:

- `{AI05-0153-3} {AI05-0196-1} {AI12-0378-1}` For an access type, the formal parameter is initialized from the value of the actual, without checking whether the value satisfies any constraints, predicates, or null exclusions, but including any dynamic accessibility checks associated with a conversion to the type of the formal parameter constraint, any predicate, or any exclusion of the null value a constraint check.

**Reason:** This preserves the Language Design Principle that an object of an access type is always initialized with a “reasonable” value.

**Ramification:** `{AI12-0378-1}` The permission to pass `null` (see below) can be used in any case where an accessibility check could fail, rather than making a check.

- `{AI05-0153-3} {AI05-0228-1} {AI12-0074-1} {AI12-0159-1} {AI12-0377-1}` For a scalar type that has the `Default_Value` aspect specified, the formal parameter is initialized from the value of the actual, without checking that the value satisfies any constraint or any predicate. Furthermore, if the actual parameter is a view conversion and either:
  - `{AI12-0074-1} {AI12-0377-1}` there exists no type (other than a root numeric type) that is an ancestor of both the target type and the type of the operand of the conversion; or
  - `{AI12-0074-1} {AI12-0377-1}` the `Default_Value` aspect is unspecified for the type of the operand of the conversion

*{AI12-0074-1} {AI12-0377-1}* then `Program_Error` is raised.

**Reason:** This preserves the Language Design Principle that all objects of a type with an implicit initial value are initialized. This is important so that a programmer can guarantee that all objects of a scalar type have a valid value with a carefully chosen `Default_Value`.

**Implementation Note:** This rule means that `out` parameters of a subtype `T` with a specified `Default_Value` need to be large enough to support any possible value of the base type of `T`. In contrast, a type that does not have a `Default_Value` only need support the size of the subtype (since no values are passed in).

**Discussion:** The `Program_Error` case can only occur in the body of an instance of a generic unit. Legality Rules will catch all other cases. Implementations that macro-expand generics can always detect this case when the enclosing instance body is expanded.

- `{AI12-0333-1}` For a composite type with discriminants or that has implicit initial values for any subcomponents (see 3.3.1), the behavior is as for an `in out` parameter passed by copy[, except that no predicate check is performed].

**Reason:** This ensures that no part of an object of such a type can become “de-initialized” by being part of an `out` parameter.

**Ramification:** This includes an array type whose component type is an access type, and a record type with a component that has a `default_expression`, among other things.

**Proof:** `{AI12-0333-1}` No predicate check follows from the definition of subtype conversion in 4.6.

- `{AI12-0439-1}` For any other type, the formal parameter is uninitialized. If composite, a view conversion of the actual parameter to the nominal subtype of the formal is evaluated [(which can might raise `Constraint_Error`)], and the actual subtype of the formal is that of the view conversion. If elementary, the actual subtype of the formal is given by its nominal subtype.

**Ramification:** `{AI05-0228-1}` This case covers scalar types that do not have `Default_Value` specified, and composite types whose subcomponent's subtypes do not have any implicit initial values. The view conversion for composite types ensures that if the lengths don't match between an actual and a formal array parameter, the `Constraint_Error` is raised before the call, rather than after.

- `{AI12-0377-1}` Furthermore, if the type is a scalar type, and the actual parameter is a view conversion, then `Program_Error` is raised if either the target or the operand type has the `Default_Value` aspect specified, unless they both have the `Default_Value` aspect specified, and there is a type (other than a root numeric type) that is an ancestor of both the target type and the operand type.
Discussion: This can only occur in the body of an instance of a generic unit. Legality Rules will catch all other cases. Implementations that macro-expand generics can always detect this case when the enclosing instance body is expanded.

\{AI05-0142-4\} \{AI05-0234-1\} In a function call, for each explicitly aliased parameter, a check is made that the accessibility level of the master of the actual object is not deeper than that of the master of the call (see 3.10.2).

Ramification: If the actual object to a call \( C \) is a formal parameter of some function call \( F \), no dynamic check against the master of the actual parameter of \( F \) is necessary. Any case which could fail the dynamic check is already statically illegal (either at the call site of \( F \), or at the call site \( C \)). This is important, as it would require nasty distributed overhead to accurately know the dynamic accessibility of a formal parameter (all tagged and explicitly aliased parameters would have to carry accessibility levels).

A formal parameter of mode **in out** or **out** with discriminants is constrained if either its nominal subtype or the actual parameter is constrained.

After normal completion and leaving of a subprogram, for each **in out** or **out** parameter that is passed by copy, the value of the formal parameter is converted to the subtype of the variable given as the actual parameter and assigned to it. These conversions and assignments occur in an arbitrary order.

\{AI05-0008-1\} If the nominal subtype of a formal parameter with discriminants is constrained or indefinite, and the parameter is passed by reference, then the execution of the call is erroneous if the value of any discriminant of the actual is changed while the formal parameter exists (that is, before leaving the corresponding callable construct).

**Erroneous Execution**

\{AI12-0378-1\} **If the actual parameter in a parameter association with mode out is a view conversion between two access types that do not share a common ancestor type, the implementation may pass in the null value of the type of the formal parameter instead of the value of the actual parameter. It is implementation-defined under what circumstances the implementation passes in the null value.**

**Implementation defined:** The circumstances in which the implementation passes in the null value for a view conversion of an access type used as an **out** parameter.

Extensions to Ada 83

In Ada 95, a program can rely on the fact that passing an object as an **out** parameter does not “de-initialize” any parts of the object whose subtypes have implicit initial values. (This generalizes the RM83 rule that required copy-in for parts that were discriminants or of an access type.)

Wording Changes from Ada 83

\{AI05-0299-1\} We have eliminated the subclause on Default Parameters, as it is subsumed by earlier clauses and subclauses.

Inconsistencies With Ada 2005

\{AI05-0196-1\} **Correction:** Clarified that **out** parameters of an access type are not checked for null exclusions when they are passed in (which is similar to the behavior for constraints). This was unspecified in Ada 2005, so a program
which depends on the behavior of an implementation which does check the exclusion may malfunction. But a program depending on an exception being raised is unlikely.

Incompatibilities With Ada 2005

\{AI05-0144-2\} Additional rules have been added to make illegal passing the same elementary object to more than one \texttt{in} or \texttt{out} parameters of the same call. In this case, the result in the object could depend on the compiler version, optimization settings, and potentially the phase of the moon, so this check will mostly reject programs that are nonportable and could fail with any change. Even when the result is expected to be the same in both parameters, the code is unnecessarily tricky. Programs which fail this new check should be rare and are easily fixed by adding a temporary object.

Wording Changes from Ada 2005

\{AI05-0008-1\} \textbf{Correction:} A missing rule was added to cover cases that were missed in Ada 95 and Ada 2005, specifically, that an \texttt{in} parameter passed by reference might have its discriminants changed via another path. Such cases are erroneous as requiring compilers to detect such errors would be expensive, and requiring such cases to work would be a major change of the user model (\texttt{in} parameters with discriminants could no longer be assumed constant). This is not an inconsistency, as compilers are not required to change any current behavior.

\{AI05-0102-1\} \textbf{Correction:} Moved implicit conversion Legality Rule to 8.6.

\{AI05-0118-1\} \textbf{Correction:} Added a definition for positional parameters, as this is missing from Ada 95 and later.

\{AI05-0142-4\} Rules have been added defining the legality and dynamic checks needed for explicitly aliased parameters (see 6.1).

\{AI05-0144-2\} Additional rules have been added such that passing an object to an \texttt{in} or \texttt{out} parameter of a function is illegal if it is used elsewhere in a construct which allows evaluation in an arbitrary order. Such calls are not portable (since the results may depend on the evaluation order), and the results could even vary because of optimization settings, and the like. Thus they've been banned.

Inconsistencies With Ada 2012

\{AI12-0378-1\} \textbf{Correction:} Added a permission to pass \texttt{null} so that value passed into an \texttt{out} parameter for access types is well-defined in the case of a view conversion. \texttt{Null} may be passed for any view conversion between unrelated access types; this is important for conversions that may have problematic accessibility or tags. If the permission is used and the \texttt{out} parameter is read before it is written (perhaps to read a bound or discriminant), \texttt{Constraint_Error} may be raised by Ada 2022 when it would not have been in Ada 2012. Additionally, if the called subprogram does not write the \texttt{out} parameter at all, the actual object will be overwritten with \texttt{null} (and possibly raise \texttt{Constraint_Error} if the object is \texttt{null} excluding), while the object would be unchanged in Ada 2012. Such cases are thought to be rare, as most \texttt{out} parameters of access types are overwritten before being read. In addition, at least one widely-used Ada compiler already passes \texttt{null} in these cases.

Incompatibilities With Ada 2012

\{AI12-0074-1\} \{AI12-0159-1\} \{AI12-0377-1\} \{AI12-0378-1\} \textbf{Corrigendum:} Added rules to ensure that the value passed into an \texttt{out} parameter for scalar elementary types is well-defined in the case of a view conversion. The new rules can be incompatible. View conversions from a view conversion to an unrelated type with the Default Value aspect specified are unlikely to occur in existing code, as the aspect is new in Ada 2012 so it should be unlikely to occur in existing code. Declaring a view conversion to an unrelated access type, the incompatibility is possible as this could be written in Ada 95, but such a view conversion is thought to be rare. In both cases, declaring and passing a temporary rather than a view conversion will eliminate the problem.

\{AI12-0095-1\} \textbf{Corrigendum:} Because of a rule added in 12.5.1, the checks for the passing of an object to an explicitly aliased parameter in a generic body were strengthened to use an assume the worst rule. This case is rather unlikely as a formal private or derived type with discriminants is required along with an explicitly aliased parameter whose type doesn't statically match the formal type. Such a program is very unlikely, especially as explicitly aliased parameters are a new Ada 2012 feature.

Wording Changes from Ada 2012

\{AI12-0216-1\} \textbf{Correction:} The \texttt{in out} parameter rule only applies to actual parameters of elementary types. While this allows additional programs (and thus could be considered an extension), it is unlikely to change anything in a real program (it could only matter in a call with 4 or more parameters, and then only if two composite parameters have matching actuals). Thus we document it as a wording change.

\{AI12-0333-1\} \textbf{Correction:} Predicate checks are not made for inbound \texttt{out} parameters. The actual rule change that has this effect is found in 4.6 and is documented there.
6.5 Return Statements

A simple return statement or extended return statement (collectively called a return statement) is used to complete the execution of the innermost enclosing subprogram_body, entry_body, or accept_statement.

Syntax

```ada
simple_return_statement ::= return [expression];
extended_return_object_declaration ::= defining_identifier : [aliased] [constant] return_subtype_indication [:= expression] [aspect_specification];
extended_return_statement ::= return extended_return_object_declaration defining_identifier : [constant aliased] return_subtype_indication [:= expression] [do
  handled_sequence_of_statements
  end return];
return_subtype_indication ::= subtype_indication | access_definition
```

Name Resolution Rules

The result subtype of a function is the subtype denoted by the subtype_mark, or defined by the access_definition, after the reserved word return in the profile of the function. The expression, if any, of a return_statement is called the return_expression. The result subtype of a function is the subtype denoted by the subtype_mark after the reserved word return in the profile of the function. The expected type for the expression, if any, of a simple_return_statement return_expression is the result type of the corresponding function. The expected type for the expression of an extended_return_object_declaration extended_return_statement is that of the return_subtype_indication.

To be honest: The same applies to generic functions.

Legality Rules

A return_statement shall be within a callable construct, and it applies to the innermost callable_construct or extended return_statement that contains it. A return_statement shall not be within a body that is within the construct to which the return_statement applies.

To be honest: The above also applies to generic subprograms, even though they are not callable constructs. (An instance of a generic subprogram is a callable construct, but not a generic subprogram itself.)

A function body shall contain at least one return_statement that applies to the function body, unless the function contains code_statements. A simple_return_statement return_statement shall include an expression return_expression if and only if it applies to a function body. An extended_return_statement shall apply to a function body. An extended_return_object_declaration extended_return_statement with the reserved word constant shall include an expression.

Reason: The requirement that a function body has to have at least one return_statement is a “helpful” restriction. There has been some interest in lifting this restriction, or allowing a raise statement to substitute for the return_statement. However, there was enough interest in leaving it as is that we decided not to change it. Note that for Ada 2012, Corrigendum 1, a return_statement whose...
expression is a raise_expression can be given in any function body (the raise_expression will match any type), so there is much less need to eliminate this rule.

**Ramification: [AI95-00318-02]** A return statement can apply to an extended return statement, so a simple-return statement without an expression can be given in one. However, neither simple return statement with an expression nor an extended return statement can be given inside an extended return statement, as they must apply (directly) to a function body.

{AI12-0089-1} Since a "function body" includes a generic function body, this rule and all of the following Legality Rules apply to generic function bodies as well as non-generic function bodies. This is true even though a generic function is not a function.

{AI12-0173-1} {AI12-0418-1} The expression of an extended return statement is the expression (if any) of the extended return object declaration of the extended return statement.

**Ramification: [AI12-0173-1] [AI12-0418-1]** The expression of a return statement is either the expression of a simple return statement or the expression of an extended return statement as defined above.

{AI95-00318-02} For an extended return statement that applies to a function body:

- {AI95-00318-02} {AI05-0032-1} {AI05-0103-1} If the result subtype of the function is defined by a subtype_mark, the return subtype indication shall be a subtype indication. The type of the subtype indication shall be covered by the result type of the function. The result subtype of the function is constrained, then the subtype defined by the subtype indication shall be statically compatible with the result subtype of the function; if the result type of the function is elementary, the two subtypes also be constrained and shall statically match this result subtype. If the result subtype of the function is indefinite or constrained, then the subtype defined by the subtype indication shall be a definite subtype, or there shall be an expression.

- {AI95-00318-02} If the result subtype of the function is defined by an access_definition, the return subtype indication shall be an access definition. The subtype defined by the access_definition shall statically match the result subtype of the function. [The accessibility level of this anonymous access subtype is that of the result subtype.]

**Proof: [AI12-0070-1]** The accessibility of such anonymous access types is defined in the Heart of Darkness (aka 5.10.2).

- {AI05-0032-1} If the result subtype of the function is class-wide, the accessibility level of the type of the subtype defined by the return subtype indication shall not be statically deeper than that of the master that elaborated the function body.

**Reason:** In this case, the return subtype indication could be a specific type initialized by default; in that case there is no expression to check.

{AI95-00318-02} {AI05-0032-1} For any return statement that applies to a function body:

- {AI95-00318-02} {AI05-0188-1} [If the result subtype of the function is limited, then the expression of the return statement (if any) shall meet the restrictions described in 7.5 concerning aggregate, a function call (or equivalent use of an operator), or a qualified expression or parenthesized expression whose operand is one of these.]

This paragraph was deleted. **Discussion: [AI05-0188-1]** In other words, if limited, the expression must produce a "new" object, rather than being the name of a preexisting object (which would imply copying).

- {AI95-00416-01} {AI05-0032-1} {AI05-0051-1} If the result subtype of the function is class-wide, the accessibility level of the type of the expression (if any) of the return statement shall not be statically deeper than that of the master that elaborated the function body. If the result subtype has one or more unconstrained access discriminants, the accessibility level of the anonymous access type of each access discriminant, as determined by the expression of the simple_return_statement or the return subtype indication, shall not be statically deeper than that of the master that elaborated the function body.

**Discussion: [AI05-0032-1] [AI05-0051-1] [AI12-0005-1]** If we know that if the result type is class-wide, then there must be an expression of the return statement unless this is an extended return statement whose return subtype indication is a specific type. We have a separate rule to cover that case. Note that if an extended_return_statement has an expression, then both this rule and the next one must be satisfied. Similarly, if the...
result subtype is unconstrained, then either the return_subtype_indication (if any) is constrained, or there must be an expression.

5.9/5

- {AI05-0051-1} If the subtype determined by the expression of the simple_return_statement or by the return_subtype_indication has one or more access discriminants, the accessibility level of the anonymous access type of each access discriminant shall not be statically deeper than that of the master that elaborated the function body.

Discussion: We use the type used by the return statement rather than from the function return type since we want to check whenever the return object has access discriminants, even if the function return type doesn't have any (mostly for a class-wide type).

5.10/5

{AI05-0277-1} {AI12-0426-1} If the reserved word keyword aliased is present in an extended_return_object_declaration, the type of the extended return object shall be immutably limited.

Static Semantics

5.11/5

{AI95-00318-02} {AI05-0015-1} {AI05-0144-2} Within an extended_return_statement, the return object is declared with the given defining_identifier, with the nominal subtype defined by the return_subtype_indication. An extended_return_statement with the reserved word constant is a full constant declaration that declares the return object to be a constant object.

Dynamic Semantics

5.12/5

{AI95-00318-02} {AI95-00416-01} {AI05-0032-1} {AI12-0439-1} For the execution of an extended_return_statement, the subtype_indication or access_definition is elaborated. This creates the nominal subtype of the return object. If there is an expression, it is evaluated and converted to the nominal subtype (which cannot raise Constraint_Error — see 4.6); the return object is created and the converted value is assigned to the return object. Otherwise, the return object is created and initialized by default as for a stand-alone object of its nominal subtype (see 3.3.1). If the nominal subtype is indefinite, the return object is constrained by its initial value. A check is made that the value of the return object belongs to the function result subtype. Constraint_Error is raised if this check fails.

Ramification: If the result type is controlled or has a controlled part, appropriate calls on Initialize or Adjust are performed prior to executing the handled_sequence_of_statements, except when the initial expression is an aggregate (which requires build-in-place with no call on Adjust).

5.6/2

{AI05-0005-1} If the return statement is left without resulting in a return (for example, due to an exception propagated from the expression or the handled_sequence_of_statements, or a goto out of the handled_sequence_of_statements), if the return object has been created, it is finalized prior to leaving the return statement. If it has not been created, the return statement is left, it is not created or finalized.

5.6/3

{AI05-0032-1} Other rules ensure that the check required by this rule cannot fail unless the function has a class-wide result subtype where the associated specific subtype is constrained. In other cases, either the subtypes have to match or the function's subtype is unconstrained and needs no checking.

6/2

{AI95-00318-02} For the execution of a simple_return_statement, the expression (if any) is first evaluated, and converted to the result subtype, and then is assigned to the anonymous return object.

Ramification: The conversion might raise Constraint_Error — (see 4.6).

6.2

7/2

{AI95-00318-02} {AI95-00416-01} If the return object has any parts that are tasks, the activation of those tasks does not occur until after the function returns (see 9.2). If the result type is class-wide, then the tag of the result is the tag of the value of the expression.

Proof: This is specified by the rules in 9.2.

Reason: Only the caller can know when task activations should take place, as it depends on the context of the call. If the function is being used to initialize the component of some larger object, then that entire object must be initialized before any task activations. Even after the outer object is fully initialized, task activations are still postponed until the begin at the end of the declarative part if the function is being used to initialize part of a declared object.
If the result type of a function is a specific tagged type, the tag of the return object is that of the result type. If the result type is class-wide, the tag of the return object is that of the value of the expression of the return statement, unless the return object is defined by an extended return object declaration with a subtype indication that is specific, in which case it is that of the type of the subtype indication, if it is specific, or otherwise that of the value of the expression. A check is made that the master accessibility level of the type identified by the tag of the result includes the elaboration not deeper than that of the master that elaborated the function body. If this check fails, Program_Error is raised.

**Ramification:**
8.a/2

The first sentence is true even if the tag of the expression is different, which could happen if the expression were a view conversion or a dereference of an access value. Note that for a limited type, because of the restriction to aggregates and function calls (and no conversions), the tag will already match.

**Reason:**
8.b/2

The first rule ensures that a function whose result type is a specific tagged type always returns an object whose tag is that of the result type. This is important for dispatching on controlling result, and allows the caller to allocate the appropriate amount of space to hold the value being returned (assuming there are no discriminants).

The master check prevents the returned object from outliving its type. Note that this check cannot fail for a specific tagged type, as the tag represents the function's type, which necessarily must be declared outside of the function.

We can't use the normal accessibility level "deeper than" check here because we may have "incomparable" levels if the masters belong to two different tasks. This can happen when an accept statement calls a function declared in the enclosing task body, and the function returns an object passed to it from the accept statement, and this object was itself a parameter to the accept statement.

**To be honest:**
8.d/3

If it is limited, then a check is made that the tag of the value of the return expression identifies the result type. Constraint_Error is raised if this check fails.

**Reason:**
8.g/3

This check is needed so that dispatching on controlling access results works for tag-indeterminate functions.

If it was not made, it would be possible for such functions to return an access to a descendant type, meaning the function could return an object with a tag different than the one assumed by the dispatching rules.

For the execution of an extended return statement, the handled sequence of statements is executed. Within this handled sequence of statements, the execution of a simple return statement that applies to the extended return statement causes a transfer of control that completes the extended return statement. Upon completion of a return statement that applies to a callable construct by the normal completion of a simple return statement or by reaching the end return of an extended return statement, a transfer of control is performed which completes the execution of the callable construct, and returns to the caller.

**Ramification:**
8.e/5

A transfer of control that completes an extended return statement (such as an exit or goto) does not cause a return to the caller unless it is caused by simple_return_statement (that is, triggers the second sentence of this paragraph). The return to the caller occurs for the simple return statement that applies to an extended return statement because the last sentence says "the normal completion of a simple return statement", which includes the one nested in the extended return statement.

**AI12-0343-1**
8.f/5

The check on the tag of the object occurs when the object is created (before any sequence of statements); the checks which follow occur after the execution of any sequence of statements. This is implicit in the order of definition of these Dynamic Semantics.

If the result subtype of the function is defined by an access_definition designating a specific tagged type T, a check is made that the result value is null or the tag of the object designated by the result value identifies T. Constraint_Error is raised if this check fails.

**Reason:**
8.g/3

This check is needed so that dispatching on controlling access results works for tag-indeterminate functions.

If it was not made, it would be possible for such functions to return an access to a descendant type, meaning the function could return an object with a tag different than the one assumed by the dispatching rules.

**Paragraphs 9 through 20 were deleted.**

- **AI95-00318-02**
  If it is limited, then a check is made that the tag of the value of the return expression identifies the result type. Constraint_Error is raised if this check fails.

- **AI95-00318-02**
  If it is nonlimited, then the tag of the result is that of the result type.
A type is a return-by-reference type if it is a descendant of one of the following:

- A tagged limited type;
- A task or protected type;
- A nonprivate type with the reserved word limited in its declaration;
- A composite type with a subcomponent of a return-by-reference type;
- A private type whose full type is a return-by-reference type.

Reason: These rules ensure that a function whose result type is a specific tagged type always returns an object whose tag is that of the result type. This is important for dispatching on controlling result, and, if nonlimited, allows the caller to allocate the appropriate amount of space to hold the value being returned (assuming there are no discriminants).

Discussion: This rule was unnecessarily confusing, and the parenthetical remark "(or a value with an associated object, see 6.2)" was added—and then the entire concept was deleted.

Implementation Note: The reason for saying "any part of the specific type" is to simplify implementation. In the case of class-wide result objects, this allows the testing of a simple flag in the tagged type descriptor that indicates whether the specific type has any parts with access discriminants. By basing the test on the accessibility level of the master of the call (see 3.10.2), that of the master that elaborated the function body; or

This is true even if the tag of the return expression is different.

Discussion: Compare the definition of return-by-reference with that of by-reference.

Reason: The return-by-reference types are all limited types except those that are limited only because of a limited private type with a nonlimited untagged full type.

Reason: This check can often be performed at compile time. It is defined to be a runtime check to avoid generic contract model problems. In a future version of the standard, we anticipate that function return of a local variable will be illegal for all limited types, eliminating the need for the runtime check except for dereferences of an access parameter.

Discussion: This rule was unnecessarily confusing, and the parenthetical remark "(or a value with an associated object, see 6.2)" was added—and then the entire concept was deleted.

If any part of the specific type of the return object the result subtype of a function (or coextension thereof) has one or more unconstrained access discriminants whose value is not constrained by the result subtype of the function, a check is made that the accessibility level of the anonymous access type of each access discriminant, as determined by the expression or the return_subtype_indication of the return_statement/function, is not deeper than the level of the master of the call (see 3.10.2) that of the master that elaborated the function body. If this check fails, Program_Error is raised. For a function with a return-by-reference result type the result is returned by reference; that is, the function call denotes a constant view of the object associated with the value of the return expression. For any other function, the result is returned by copy; that is, the converted value is assigned into an anonymous constant created at the point of the return_statement, and the function call denotes that object.

This paragraph was deleted. Ramification: The assignment operation does the necessary value adjustment, as described in 7.6, "Assignment and Finalization". 7.6.1 describes when the anonymous constant is finalized.

Reason: The check prevents the returned object (for a nonlimited type) from outliving the object designated by one of its discriminants. The check is made on the values of the discriminants, which may come from the return_subtype_indication (if constrained), or the expression, but it is never necessary to check both.

Implementation Note: The reason for saying "any part of the specific type" is to simplify implementation. In the case of class-wide result objects, this allows the testing of a simple flag in the tagged type descriptor that indicates whether the specific type has any parts with access discriminants. By basing the test on the
type of the object rather than the object itself, we avoid concerns about whether subcomponents in variant parts and of arrays (which might be empty) are present.

**Discussion:** {AI05-0234-1} For a function with a class-wide result type, the access values that need to be checked are determined by the tag of the return object. In order to implement this accessibility check in the case where the tag of the result is not known statically at the point of the return statement, an implementation may need to somehow associate with the tag of a specific tagged type an indication of whether the type has unconstrained access discriminants (explicit or inherited) or has any subcomponents with such discriminants. If an implementation is already maintaining a statically initialized descriptor of some kind for each specific tagged type, then an additional Boolean could be added to this descriptor.

{AI05-0005-1} {AI05-0234-1} Note that the flag should only be queried in the case where the result object might have access discriminants that might have subtypes with "bad" accessibility levels (as determined by the rules of 3.10.2 for determining the accessibility level of the type of an access discriminant in the expression or return_subtype_indication of a return statement).

Thus, in a case like

```ada
type Global is access T'Class;
function F (Ptr : Global) return T'Class is
begin
  return Ptr.all;
end F;
```

there is no need for a run-time accessibility check. While an object of T'Class "might have" access discriminants, the accessibility of those potential discriminants cannot be bad. The setting of the bit doesn't matter and there is no need to query it.

On the other hand, given

```ada
function F return T'Class is
  Local : T'Class := ... ;
begin
  return Local;
end F;
```

In this case, a check would typically be required.

The need for including subcomponents in this check is illustrated by the following example:

```ada
X : aliased Integer;

type Component_Type (Discrim : access Integer := X'Access) is
  limited null record;

type Undiscriminated is record
  Fld : Component_Type;
end record;

function F return Undiscriminated is
  Local : aliased Integer;
begin
  return X : Undiscriminated := (Fld => (Discrim => Local'Access)) do
    Foo;
  end return;
  -- raises Program_Error after calling Foo.
end F;
```

**Ramification:** {AI05-0234-1} In the case where the tag of the result is not known statically at the point of the return statement and the run-time accessibility check is needed, discriminant values and array bounds play no role in performing this check. That is, array components are assumed to have nonzero length and components declared within variant parts are assumed to be present. Thus, the check may be implemented simply by testing the aforementioned descriptor bit and conditionally raising Program_Error.

{AI95-00318-02} {AI05-0058-1} {AI12-0343-1} {AI12-0449-1} A check is performed that the return value satisfies the predicates of the return subtype. If this check fails, the effect is as defined in 3.2.4. For the execution of an extended_return_statement, the handled_sequence_of_statements is executed. Within this handled_sequence_of_statements, the execution of a simple_return_statement that applies to the extended_return_statement causes a transfer of control that completes the extended_return_statement. Upon completion of a return statement that applies to a callable construct by the normal completion of a simple_return_statement or by reaching the end_return of an extended_return_statement, a transfer of control is performed which completes the execution of the callable construct to which the return_statement applies, and returns to the caller.
This paragraph was deleted

Ramification: {AI05-0058-1} {AI12-0343-1} A transfer of control that completes an extended return statement (such as an exit or goto) does not cause a return to the caller unless it is caused by simple return statement (that is, triggers the second sentence of this paragraph). The return to the caller occurs for the simple return statement that applies to an extended return statement because the last sentence says “the normal completion of a simple return statement”, which includes the one nested in the extended return statement.

Implementation Note: {AI12-0005-1} {AI12-0343-1} The subtype conversion of the return expression for a simple return statement performs this same check. The permissions of 11.4.2 ensure that duplicate evaluation of a predicate at a single point is not required (other than pathological, not portable cases), so a single evaluation of the predicate is enough in this case.

22.a/5

22.b/5

AI95-00318-02 In the case of a function, the function call denotes a constant view of the return object.

Implementation Permissions

24/3

AI95-00416-01 AI05-0050-1 For a function call used to initialize a composite: If the result subtype of a function is unconstrained, and a call on the function is used to provide the initial value of an object with a constrained nominal subtype or used to initialize a return object that is built in place into such an object, Constraint_Error may be raised at the point of the call (after abandoning the execution of the function body) if, while elaborating the return subtype indication or evaluating the expression of a return statement that applies to the function body, it is determined that the value of the result will violate the constraint of the subtype of this object:

- {AI05-0050-1} If the result subtype of the function is constrained, and conversion of an object of this subtype to the subtype of the object being initialized would raise Constraint_Error, then Constraint_Error may be raised before calling the function.
- {AI05-0050-1} If the result subtype of the function is unconstrained, and a return statement is executed such that the return object is known to be constrained, and conversion of the return object to the subtype of the object being initialized would raise Constraint_Error, then Constraint_Error may be raised at the point of the call (after abandoning the execution of the function body).

Reason: AI95-00416-01 AI05-0050-1 Without such a permission, it would be very difficult to implement “built-in-place build-in-place” semantics. The intention is that the exception is raised at the same point that it would have been raised without the permission; it should not change handlers if the implementation switches between return-by-copy and built-in-place. This means that the such exception is not handleable within the function, because in the return-by-copy case, the constraint check to verify that the result satisfies the constraints of the object being initialized happens after the function returns and we want the semantics to change as little as possible when switching between return-by-copy and build-in-place. This implies further that upon detecting such a situation, the implementation may need to simulate a goto to a point outside any local exception handlers prior to raising the exception.

Ramification: AI95-00416-01 AI05-0050-1 These permissions do not apply in the case of an extended return object with mutable discriminants. That's necessary because in that case a return object can be created with the “wrong” discriminants and then changed to the “right” discriminants later (but before returning). We don't want this case raising an exception when the canonical semantics will not do so. This permission is allowed during the evaluation of the expression of an extended return statement because the return_subtype_indication may be unconstrained and the expression then would provide the constraints.

AI05-0050-1 It's still possible to write a program that will raise an exception using this permission that would not in the canonical semantics. That could happen if a return statement with the “wrong” discriminants or bounds is abandoned (via an exception, or for an extended return statement, via an exit or goto statement), and then a return statement with the “right” discriminants or bounds is executed. The only solution for this problem is to not have the permission at all, but this is too unusual of a case to worry about the effects of the permission, especially given the implementation difficulties for built-in-place objects that this permission is intended to ease.

AI05-0050-1 Note that the mutable-discriminant case only happens when built-in-place initialization is optional. This means that any difficulties associated with implementing built-in-place initialization without these permissions can be sidestepped by not building in place.
Examples

Examples of return statements:

```ada
{AI95-00318-02} return; -- in a procedure body, entry_body
accept_statement
return Key_Value(Last_Index); -- in a function body
{AI95-00318-02} return Node : Cell do
  Node.Value := Result;
  Node.Succ := Next_Node;
end return;
```

Incompatibilities With Ada 83

{AI95-00318-02} In Ada 95, if the result type of a function has a part that is a task, then an attempt to return a local variable will raise Program_Error. This is illegal in Ada 2005, see below. In Ada 83, if a function returns a local variable containing a task, execution is erroneous according to AI83-00867. However, there are other situations where functions that return tasks (or that return a variant record only one of whose variants includes a task) are correct in Ada 83 but will raise Program_Error according to the new rules.

The rule change was made because there will be more types (protected types, limited controlled types) in Ada 95 for which it will be meaningless to return a local variable, and making all of these erroneous is unacceptable. The current rule was felt to be the simplest that kept upward incompatibilities to situations involving returning tasks, which are quite rare.

Wording Changes from Ada 83

{AI05-0299-1} This subclause has been moved here from chapter 5, since it has mainly to do with subprograms.

A function now creates an anonymous object. This is necessary so that controlled types will work.

{AI95-00318-02} We have clarified that a return statement applies to a callable construct, not to a callable entity.

{AI95-00318-02} There is no need to mention generics in the rules about where a return statement can appear and what it applies to; the phrase “body of a subprogram or generic subprogram” is syntactic, and refers exactly to “subprogram_body”.

Inconsistencies With Ada 95

{AI95-0416-1} {AI05-0005-1} {AI05-0050-1} Added an Implementation Permission allowing early raising of Constraint_Error if the result cannot fit in the ultimate object. This gives implementations more flexibility to do built-in-place returns, and is essential for limited types (which cannot be built in a temporary). However, it allows raising an Constraint_Error in some cases where it would not be raised if the permission was not used. See Inconsistencies With Ada 2005 for additional changes. This case is potentially inconsistent with Ada 95, but a compiler does not have to take advantage of these permissions for any Ada 95 code, so there should be little practical impact.

Incompatibilities With Ada 95

{AI95-00318-02} The entire business about return-by-reference types has been dropped. Instead, the expression of a return statement of a limited type can only be an aggregate or function call (see 7.5). This means that returning a global object or type_conversion, legal in Ada 95, is now illegal. Such functions can be converted to use anonymous access return types by adding access in the function definition and return statement, adding aliased in the object declarations. This has the advantage of making the reference return semantics much clearer to the casual reader.

We changed these rules so that functions, combined with the new rules for limited types (7.5), can be used as build-in-place constructors for limited types. This reduces the differences between limited and nonlimited types, which will make limited types useful in more circumstances.

Extensions to Ada 95

{AI95-00318-02} The extended return_statement is new. This provides a name for the object being returned, which reduces the copying needed to return complex objects (including no copying at all for limited objects). It also allows component-by-component construction of the return object.

Wording Changes from Ada 95

{AI95-00318-02} The wording was updated to support anonymous access return subtypes.
Inconsistencies With Ada 2005

{AI05-0050-1} **Correction:** The Implementation Permission allowing early raising of Constraint_Error was modified to remove the most common of these cases from the permission (returning an object with mutable discriminants, where the return object is created with one set of discriminants and then changed to another). (The permission was also widened to allow the early check for constrained functions when that constraint is wrong.) However, there still is an unlikely case where the permission would allow an exception to be raised when none would be raised by the canonical semantics (when a return statement is abandoned). These changes can only remove the raising of an exception (or change the place where it is raised) compared to Ada 2005, so programs that depend on the previous behavior should be very rare.

{AI05-0051-1} **Correction:** Accessibility checks for access discriminants now depend on the master of the call rather than the point of declaration of the function. This will result in cases that used to raise Program_Error now running without raising any exception. This is technically inconsistent with Ada 2005 (as defined by Amendment 1), but it is unlikely that any real code depends on the raising of this exception.

{AI05-0072-1} **Correction:** Added a tag check for functions returning anonymous access-to-tagged types, so that dispatching of tag-indeterminate function works as expected. This is technically inconsistent with Ada 2005 (as defined by Amendment 1), but as the feature in question was newly added to Ada 2005, there should be little code that depends on the behavior that now raises an exception.

Incompatibilities With Ada 2005

{AI05-0053-1} **Correction:** The aliased keyword can now only appear on extended return objects with an immutably limited type. Other types would provide a way to get an aliased view of an object that is not necessarily aliased, which would be very bad. This is incompatible, but since the feature was added in Ada 2005, the keyword had no defined meaning in Ada 2005 (a significant oversight), and most sensible uses involve immutably limited types, it is unlikely that it appears meaningfully in existing programs.

{AI05-0103-1} **Correction:** Added wording to require static matching for unconstrained access types in extended return statements. This disallows adding or omitting null exclusions, and adding access constraints, in the declaration of the return object. While this is incompatible, the incompatible cases in question are either useless (access constraints – the constraint can be given on an allocator if necessary, and still must be given there even if given on the return object) or wrong (null exclusions – null could be returned from a function declared to be null excluding), so we expect them to be extremely rare in practice.

Extensions to Ada 2005

{AI05-0015-1} **Correction:** The return object of an extended_return_statement can be declared constant; this works similarly to a constant object declaration.

Wording Changes from Ada 2005

{AI05-0024-1} **Correction:** Corrected the master check for tags since the masters may be for different tasks and thus incomparable.

{AI05-0058-1} **Correction:** Corrected the wording defining returns for extended_return_statements, since leaving by an exit or goto is considered “normal” completion of the statement.

{AI05-0205-1} **Correction:** Added the extended_return_object_declaration to make other rules easier to write and eliminate the problem described in AI05-0205-1.

Inconsistencies With Ada 2012

{AI12-0343-1} **Correction:** Reordered the checks associated with return statements to clarify when they happen relative to the sequence_of_statements of an extended_return_statement, and to add an additional predicate check.

6.5 Return Statements
on the returned value. This latter check can fail if the value to be returned is changed in the statements of an extended return. Thus, the following function now raises Assertion_Error, while no exception would be raised in Ada 2012:

```ada
type Rec is record
  Count, Max : Natural;
end record with Dynamic_Predicate => Rec.Count <= Rec.Max;

function Foo return Rec is
begin
  Result : Rec := (Count => 5, Max => 10)
  do
    Result.Max := 0;
  end return;
end Foo;
```

This will detect a program bug (returning a value that does not meet the predicate of the return subtype) rather than leaving it hidden, so the inconsistency is tolerable.

**Extensions to Ada 2012**

{AI12-0398-1} Extended return objects now can have an **aspect specification**, allowing the specification of (implementation-defined) aspects for return objects.

**Wording Changes from Ada 2012**

{AI05-0097-1} **Corrigendum:** Clarified the wording so that it is clear where the tag of the return object comes from. While a literal reading of the original Ada 2012 rule could have caused some weird results (by using some nearby subtype indication to provide the tag in the case of a simple return statement), such a reading would be so unlike the rest of the language that we do not believe anyone would ever have thought it was intended. As such, we do not believe any implementation ever did this wrong (at least because of the old wording), and thus do not document this as a possible inconsistency.

{AI12-0173-1} **Correction:** Added a definition of the term **expression** of an extended return statement. That wording was commonly used before the extended return object declaration was split into a separate syntax production, leaving the extended return statement without any expression of its own. Moreover, the wording often just uses “expression of a return statement” to cover both kinds of return statement. Changing the wording in more than a dozen places was unappealing, and some of the changes would be awkward to read, so we defined the term and left the majority of the wording unchanged.

### 6.5.1 Nonreturning Subprograms

**Pragma No_Return**

{AI95-00329-01} {AI95-00414-01} {AI05-0229-1} {AI12-0269-1} {AI12-0418-1} Specifying **aspect** **Pragma No_Return** to have the value True indicates that a subprogramprocedure cannot return normally; it may, for example, propagate an exception or loop forever.

**Discussion:** AspectPragma No_Deposit will have to wait for Ada 2017.

Paragraphs 2 and 3 were moved to Annex J, "Obsolescent Features".

**Syntax**

{AI95-00329-01} {AI95-00414-01} {AI05-0229-1} The form of a **pragma No_Return**, which is a representation **pragma** (see 13.1), is as follows:

```
pragma No_Return(procedure_local_name, procedure_local_name);
```

**Static Semantics**

{AI05-0229-1} {AI12-0269-1} For a subprogramprocedure or generic subprogramprocedure, the following language-defined representation aspect may be specified:

**No_Return**

The type of aspect No_Return is Boolean. When aspect No_Return is True for an entity, the entity is said to be nonreturning.

{AI12-0423-1} If directly specified, the aspect definition shall be a static expression. When not directly specified, if the subprogram is a primitive subprogram inherited by a derived type, then the aspect is True if any corresponding subprogram of the parent or progenitor
types is nonreturning. Otherwise [This aspect is never inherited;] if not directly specified, the aspect is False.

Aspect Description for No_Return: A subprogramprocedure will not return normally.

{AI05-0229-1} {AI12-0269-1} If a generic subprogramprocedure is nonreturning, then so are its instances. If a subprogramprocedure declared within a generic unit is nonreturning, then so are the corresponding copies of that subprogramprocedure in instances.

Legality Rules

{AI95-00329-01} {AI95-00414-01} {AI05-0229-1} Aspect No_Return Each procedure local name shall denote one or more procedures or generic procedures; the denoted entities are nonreturning. The procedure local name shall not be specified for denote a null procedure nor an instance of a generic unit.

Reason: A null procedure cannot have the appropriate nonreturning semantics, as it does not raise an exception or loop forever.

Ramification: {AI05-0229-1} {AI12-0269-1} The procedure can be abstract. The denoted declaration can be a renaming declaration if it obeys the usual rules for representation pragmas; the renaming has to occur immediately within the same declarative region as the renamed subprogram. If a nonreturning subprogramprocedure is renamed (anywhere) calls through the new name still have the nonreturning semantics.

{AI95-00329-01} {AI95-00414-01} A return statement shall not apply to a nonreturning procedure or generic procedure.

{AI12-0269-1} Any return statement that applies to a nonreturning function or generic function shall be a simple return statement with an expression that is a raise expression, a call on a nonreturning function, or a parenthesized expression of one of these.

Reason: We still require at least one return statement in a function; we just require that all such return statements don't actually return a value.

Ramification: We still require at least one return statement in a function; we just require that all such return statements don't actually return a value.

{AI95-00414-01} {AI12-0269-1} A subprogramprocedure shall be nonreturning if it overrides a dispatching nonreturning subprogramprocedure. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

Reason: This ensures that dispatching calls to nonreturning subprogramprocedures will, in fact, not return.

{AI95-00414-01} {AI12-0269-1} If a renaming-as-body completes a nonreturning subprogramprocedure declaration, then the renamed subprogramprocedure shall be nonreturning.

Reason: This ensures that no extra code is needed to implement the renames (that is, no wrapper is needed) as the body has the same property.

Paragraph 8 was deleted.

Static Semantics

{AI95-00329-01} {AI95-00414-01} {AI05-0229-1} If a generic procedure is nonreturning, then so are its instances. If a procedure declared within a generic unit is nonreturning, then so are the corresponding copies of that procedure in instances.

Dynamic Semantics

{AI95-00329-01} {AI95-00414-01} If the body of a nonreturning procedure completes normally, Program_Error is raised at the point of the call.

Discussion: {AI12-0269-1} Note that there is no name for suppressing this check, since the check represents a bug, imposes no time overhead, and minimal space overhead (since it can usually be statically eliminated as dead code). We don't need a similar rule for nonreturning functions as this is standard semantics for all functions that normally complete without a transfer of control (such as a return statement).

Implementation Note: If a nonreturning procedure tries to return, we raise Program_Error. This is stated as happening at the call site, because we do not wish to allow the procedure to handle the exception (and then, perhaps, try to return.
again!). However, the expected run-time model is that the compiler will generate `raise Program_Error` at the end of the procedure body (but not handleable by the procedure itself), as opposed to doing it at the call site. (This is just like the typical run-time model for functions that fall off the end without returning a value). The reason is indirect calls: in `P.all(...);`, the compiler cannot know whether `P` designates a nonreturning procedure or a normal one. Putting the `raise Program_Error` in the procedure's generated code solves this problem neatly.

Similarly, if one passes a nonreturning procedure to a generic formal parameter, the compiler cannot know this at call sites (in shared code implementations); the `raise-in-body` solution deals with this neatly.

**Examples**

```ada
{AI12-0429-1} Example of a specification of a No_Return aspect:

```{AI95-00433-01} {AI05-0229-1} procedure Fail(Msg : String); -- raises Fatal_Error exception
 withpragma No_Return(Fail); -- inform compiler and reader that procedure never returns normally

```{AI95-00414-01} {AI05-0229-1} Pragma No_Return is new.

```{AI95-00329-01} {AI95-00433-01} Pragma No_Return is now obsolescent.

```

**Incompatibilities With Ada 2012**

```{AI12-0423-1} Correction: Clarified that the nonreturning property is inherited by derivation. A literal implementation of the Ada 2012 would mean that no overriding would ever be rejected, as the inherited routine would never be nonreturning. Ada 2022 requires overridings of dispatching nonreturning subprograms to be rejected. This is formally incompatible, but practically such overridings have been rejected in practice.

```

**Extensions to Ada 2012**

```{AI12-0269-1} Aspect No_Return can now be applied to functions as well as procedures.

```

6.6 Overloading of Operators

An operator is a function whose designator is an operator_symbol. [Operators, like other functions, may be overloaded.]

**Name Resolution Rules**

Each use of a unary or binary operator is equivalent to a function_call with function_prefix being the corresponding operator_symbol, and with (respectively) one or two positional actual parameters being the operand(s) of the operator (in order).

**To be honest:**

```{AI05-0005-1} {AI05-0005-1} We also use the term operator (in Clause 4ClauseSection 4 and in 6.1) to refer to one of the syntactic categories defined in 4.5, “Operators and Expression Evaluation” whose names end with “_operator:” logical_operator, relational_operator, binary_adding_operator, unary_adding_operator, multiplying_operator, and highest_precedence_operator.

**Discussion:**

```{AI05-0005-1} This equivalence extends to uses of function_call in most other language rules. However, as often happens, the equivalence is not perfect, as operator calls are not a name, while a function call is a name. Thus, operator calls cannot be used in contexts that require a name (such as a rename of an object). A direct fix for this problem would be very disruptive, and thus we have not done that. However, qualifying an operator call can be used as a workaround in contexts that require a name.

**Legality Rules**

```{AI05-0143-1} The subprogram_specification of a unary or binary operator shall have one or two parameters, respectively. The parameters shall be of mode in. A generic function instantiation whose designator is an operator_symbol is only allowed if the specification of the generic function has the corresponding number of parameters, and they are all of mode in.
Default expressions are not allowed for the parameters of an operator (whether the operator is declared with an explicit subprogram specification or by a generic instantiation).

An explicit declaration of "/=" shall not have a result type of the predefined type Boolean.

Static Semantics

\[{A105-0128-1}\] An explicit declaration of "=" whose result type is Boolean implicitly declares an operator declaration of "/=" that gives the complementary result.

Discussion: \[{A105-0128-1}\] A "/=" defined by this rule is considered user-defined, which means that it will be inherited by a derived type. "User-defined" means "not language-defined" for the purposes of inheritance, that is anything other than predefined operators.

NOTE \[{A112-0440-1}\] The operators "+" and "-" are both unary and binary operators, and hence \textit{cannot} be overloaded with both one- and two-parameter functions.

Examples of user-defined operators:

function "+" (Left, Right : Matrix) return Matrix;
function "+" (Left, Right : Vector) return Vector;

assuming that A, B, and C are of the type Vector
the following two statements are equivalent:

\begin{align*}
A & := B + C; \\
A & := "+"(B, C);
\end{align*}

Extensions to Ada 83

Explicit declarations of "=" are now permitted for any combination of parameter and result types.

Explicit declarations of "/=" are now permitted, so long as the result type is not Boolean.

Wording Changes from Ada 2005

Correction: Corrected the wording so that only explicit declarations of "=" cause an implicit declaration of "/="; otherwise, we could get multiple implicit definitions of "/=" without an obvious way to chose between them.

Added wording so that operators only allow parameters of mode \texttt{in}. This was made necessary by the elimination elsewhere of the restriction that function parameters be only of mode \texttt{in}.

6.7 Null Procedures

A null procedure declaration provides a shorthand to declare a procedure with an empty body.

Syntax

\[{A195-00348-01}\] null procedure declaration ::= 

\[{A195-00348-01}\] \[{A105-0183-1}\] procedure specification is null

\[{A195-00348-01}\] \[{A105-0177-1}\] If a null procedure declaration is a completion, it shall be the completion of a subprogram declaration or generic subprogram declaration. The profile of a null procedure declaration that completes a declaration shall conform fully to that of the declaration.
Null Procedures

Static Semantics

A null procedure declaration that is not a completion declares a null procedure. A completion is not allowed for a null procedure declaration; however, a null procedure declaration can complete a previous declaration.

Reason: There are no null functions because the return value has to be constructed somehow; a function that always raises Program_Error doesn’t seem very useful or worth the complication.

Dynamic Semantics

The execution of a null procedure is invoked by a subprogram call. For the execution of a subprogram call on a null procedure, or on a procedure completed with a null procedure declaration, the execution of the subprogram body has no effect.

Ramification: Thus, a null procedure is equivalent to the body

```
begin
  null;
end;
```

with the exception that a null procedure can be used in place of a procedure specification.

The elaboration of a null procedure declaration has no other effect than to establish that the null procedure can be called without failing the Elaboration_Check.

Examples

Example of the declaration of a null procedure:

```
procedure Simplify(Expr : in out Expression) is null;
-- see 3.9
-- By default, Simplify does nothing, but it cannot be overridden in extensions of Expression
```

Extensions to Ada 95

Null procedures are new.

Extensions to Ada 2005

A null procedure declaration can now be a completion.

An optional aspect specification can be used in a null procedure declaration. This is described in 13.1.1.

Wording Changes from Ada 2012

Clarified the term “null procedure” so it matches the meaning expected in 6.1.

6.8 Expression Functions

An expression function declaration provides a shorthand to declare a function whose body consists of a single return statement.

Syntax

```
expression_function_declaration ::= 
  [overriding_indicator]
  function_specification is 
  (expression)
  [aspect_specification];
| [overriding_indicator]
  function_specification is
```

7.a/2

7.b/3

7.c/3

7.d/5

7/5

3/5

3.a/2

4/5

4.a/2

4.b/2

4.c/2

5/3

6/5

7/5

4/5
aggregate
   [aspect_specification];

Name Resolution Rules

3/4  {AI05-0177-1}  {AI12-0157-1} The expected type for the expression or aggregate of an expression function declaration is the result type (see 6.5) of the function.

Static Semantics

3.1/5  {AI05-0177-1}  {AI05-0264-1}  {AI12-0075-1}  {AI12-0157-1}  {AI12-0408-1} An expression function declaration that is not a completion declares an expression function. The return expression of an expression function is the expression or aggregate of the expression function declaration. A completion is not allowed for an expression function declaration; however, an expression function declaration can complete a previous declaration.

3.2/5  {AI12-0075-1} A potentially static expression is defined in the same way as a static expression except that

3.3/5  • a name denoting a formal parameter of an expression function is a potentially static expression; and

3.4/5  • each use of “static expression” in the definition of “static expression” is replaced with a corresponding use of “potentially static expression” in the definition of “potentially static expression”.

Discussion: These uses occur in the definition of “static expression” in the cases of function calls, type conversions, qualified expressions, membership tests, short circuit control forms, conditional expressions, and parenthesized expressions.

3.5/5  {AI12-0075-1} The following language-defined representation aspect may be specified for an expression function:

3.6/5  Static

The type of aspect Static is Boolean. When aspect Static is True for an expression function, the function is a static expression function. If directly specified, the aspect definition shall be a static expression.

3.b/5  Aspect Description for Static: Specifies that an associated expression function can be used in static expressions.

3.7/5  The Static value for an inherited function is True if some corresponding primitive function of the parent or progenitor type is a static expression function; otherwise, if not directly specified, the aspect is False.

3.8/5  {AI12-0075-1} [A static expression function is a static function; see 4.9.]

Legality Rules

4/3  {AI05-0177-1} If an expression function declaration is a completion, it shall be the completion of a subprogram declaration or generic subprogram declaration. The profile of an expression function declaration that completes a declaration shall conform fully to that of the declaration.

5/4  {AI05-0177-1}  {AI12-0157-1} If the result subtype has one or more unconstrained access discriminants, the accessibility level of the anonymous access type of each access discriminant, as determined by the expression or aggregate of the expression function declaration, shall not be statically deeper than that of the master that elaborated the expression function declaration.

5.a/3  Ramification: This can only fail if the discriminant is an access to a part of a nonaliased parameter, as there can be no local declarations here.
Discussion: \{AI12-0005-1\} We don't need to repeat any of the other Legality Rules for return statements since none of them can fail here: the implicit return statement has to apply to this function (and isn't nested in something), there clearly is a return statement in this function, and the static class-wide accessibility check cannot fail as a tagged type cannot be declared locally in an expression function.

\{AI12-0075-1\} Aspect Static shall be specified to have the value True only if the associated expression-function_declaration:
- is not a completion;
- has an expression that is a potentially static expression;
- contains no calls to itself;
- each parameter (if any) is of mode in and is of a static subtype;
- has a result subtype that is a static subtype;
- has no applicable precondition or postcondition expression; and
- \{AI12-0075-1\} \{AI12-0191-1\} for result type \(R\), if the function is a boundary entity for type \(R\) (see 7.3.2), no type invariant applies to type \(R\); if \(R\) has a component type \(C\), a similar rule applies to \(C\).

Ramification: Since a string subtype can be static, this allows an expression function of a string type to be static.

Paragraph 6 was deleted.

Static Semantics

\{AI05-0177-1\} \{AI05-0264-1\} \{AI12-0157-1\} \{AI12-0075-1\} An expression-function_declaration declares an expression function. The return expression of an expression function is the expression or aggregate of the expression-function_declaration. A completion is not allowed for an expression-function_declaration; however, an expression-function_declaration can complete a previous declaration.

Dynamic Semantics

\{AI05-0177-1\} \{AI05-0262-1\} \{AI12-0157-1\} \{AI12-0408-1\} The execution of an expression function is invoked by a subprogram call. For the execution of a subprogram call on an expression function, or on a function completed with a expression-function_declaration, the execution of the subprogram_body executes an implicit function body containing only a simple return_statement whose expression is the return expression that of the expression function.

Discussion: The last sentence effectively means that all of the dynamic wording in 6.5 applies as needed, and we don't have to repeat it here.

\{AI05-0177-1\} The elaboration of an expression-function_declaration has no other effect than to establish that the expression function can be called without failing the Elaboration_Check.

Examples

\{AI12-0429-1\} Example of an expression function:

\{AI05-0177-1\} function Is-Origin (P : in Point) return Boolean is -- see 3.9
\(\text{(P.X = 0.0 and P.Y = 0.0)}\);

Extensions to Ada 2005

\{AI05-0177-1\} Expression functions are new in Ada 2012.

Extensions to Ada 2012

\{AI12-0157-1\} Corrigendum: A aggregate can directly be the return expression of an expression function. This eliminates the double parentheses that otherwise would be necessary.
Aspect Static is new; it allows using suitable expression functions in static expressions.

Wording Changes from Ada 2012

Clarified the term “expression function” so it matches the meaning expected in 6.1.
7 Packages

[Packages are program units that allow the specification of groups of logically related entities. Typically, a package contains the declaration of a type (often a private type or private extension) along with the declarations of primitive subprograms of the type, which can be called from outside the package, while their inner workings remain hidden from outside users.]

**Term entry: package** — program unit that defines the interface to a group of logically related entities, along with their implementation

Note: Typically, a package contains the declaration of a type (often a private type or private extension) along with the declarations of primitive subprograms of the type, which can be called from outside the package, while their inner workings remain hidden from outside users.

7.1 Package Specifications and Declarations

[A package is generally provided in two parts: a package_specification and a package_body. Every package has a package_specification, but not all packages have a package_body.]

Syntax

```
package_declaration ::= package_specification

{AI05-0183-1} package_specification ::= 
    package defining_program_unit_name
        [aspect_specification] is
        {basic_declarative_item}
        [private
        {basic_declarative_item}]
    end ([parent_unit_name.]identifier)
```

If an identifier or parent_unit_name.identifier appears at the end of a package_specification, then this sequence of lexical elements shall repeat the defining_program_unit_name.

Legality Rules

```
{AI95-00434-01} A package_declaration or generic_package_declaration requires a completion [(a body)] if it contains any basic_declarative_item that requires a completion, but whose completion is not in its package_specification.

**To be honest:** {AI05-0229-1} If an implementation supports it, a pragma_Import may substitute for the body of a package or generic package, may be imported (using aspect Import, see B.1), in which case no explicit body is allowed.
```

Static Semantics

```
{AI95-00434-01} {AI95-00434-01} The first list of basic_declarative_item of a package_specification of a package other than a generic formal package is called the visible part of the package. [ The optional list of basic_declarative_item after the reserved word private (of any package_specification) is called the private part of the package. If the reserved word private does not appear, the package has an implicit empty private part.] Each list of basic_declarative_item of a package_specification forms a declaration list of the package.

**Ramification:** This definition of visible part does not apply to generic formal packages — 12.7 defines the visible part of a generic formal package.

The implicit empty private part is important because certain implicit declarations occur there if the package is a child package, and it defines types in its visible part that are derived from, or contain as components, private types declared within the parent package. These implicit declarations are visible in children of the child package. See 10.1.1.
[An entity declared in the private part of a package is visible only within the declarative region of the package itself (including any child units — see 10.1.1). In contrast, expanded names denoting entities declared in the visible part can be used even outside the package; furthermore, direct visibility of such entities can be achieved by means of use clauses (see 4.1.3 and 8.4).]

Dynamic Semantics

The elaboration of a package_declaration consists of the elaboration of its basic_declarative_items in the given order.

NOTE 1 The visible part of a package contains all the information that another program unit is able to know about the package.

NOTE 2 If a declaration occurs immediately within the specification of a package, and the declaration has a corresponding completion that is a body, then that body has to occur immediately within the body of the package.

Proof: This follows from the fact that the declaration and completion are required to occur immediately within the same declarative region, and the fact that bodies are disallowed (by the Syntax Rules) in package Specifications. This does not apply to instances of generic units, whose bodies can occur in package Specifications.

Examples

Example of a package declaration:

```
package Rational_Numbers is
  type Rational is record
    Numerator   : Integer;
    Denominator : Positive;
  end record;

  function "="(X,Y : Rational) return Boolean;
  function "/" (X,Y : Integer) return Rational;  -- to construct a rational number
  function "+" (X,Y : Rational) return Rational;
  function "-" (X,Y : Rational) return Rational;
  function "+" (X,Y : Rational) return Rational;
  function "/" (X,Y : Rational) return Rational;
end Rational_Numbers;
```

There are also many examples of package declarations in the predefined language environment (see Annex A).

Incompatibilities With Ada 83

{AI12-0417-1} In Ada 83, a library package is allowed to have a body even if it doesn't need one. In Ada 95, a library package body is either required or forbidden — never optional. The workaround is to add aspect pragma Elaborate_Body, or something else requiring a body, to each library package that has a body that isn't otherwise required.

Wording Changes from Ada 83

{AI05-0299-1} We have moved the syntax into this subclause and the next subclause from RM83-7.1, “Package Structure”, which we have removed.

RM83 was unclear on the rules about when a package requires a body. For example, RM83-7.1(4) and RM83-7.1(8) clearly forgot about the case of an incomplete type declared in a package_declaration but completed in the body. In addition, RM83 forgot to make this rule apply to a generic package. We have corrected these rules. Finally, since we now allow a pragma Import for any explicit declaration, the completion rules need to take this into account as well.

Wording Changes from Ada 95

{AI95-00420-01} Defined “declaration list” to avoid ambiguity in other rules as to whether packages are included.

Extensions to Ada 2005

{AI05-0183-1} An optional aspect_specification can be used in a package_specification. This is described in 13.1.1.
7.2 Package Bodies

[In contrast to the entities declared in the visible part of a package, the entities declared in the package_body are visible only within the package_body itself. As a consequence, a package with a package_body can be used for the construction of a group of related subprograms in which the logical operations available to clients are clearly isolated from the internal entities.]

### Syntax

```
{AI05-0267-1} package_body ::=  
  package_body defining_program_unit_name
  [aspect_specification] is
  declarative_part
  [begin
    handled_sequence_of_statements
  end [parent_unit_name.]identifier];
```

If an identifier or parent_unit_name.identifier appears at the end of a package_body, then this sequence of lexical elements shall repeat the defining_program_unit_name.

### Legality Rules

```
{AI12-0417-1} A package_body shall be the completion of a previous package_declaration or generic_package_declaration. A library package_declaration or library generic_package_declaration shall not have a body unless it requires a body if the pragma Elaborate_Body aspect can be used to require a library_unit_declaration to have a body (see 10.2.1) if it would not otherwise require one].
```

**Ramification:** The first part of the rule forbids a package_body from standing alone — it has to belong to some previous package_declaration or generic_package_declaration.

A nonlibrary package_declaration or nonlibrary generic_package_declaration that does not require a completion may have a corresponding body anyway.

### Static Semantics

In any package_body without statements there is an implicit null_statement. For any package_declaration without an explicit completion, there is an implicit package_body containing a single null_statement. For a noninstance, nonlibrary package, this body occurs at the end of the declarative_part of the innermost enclosing program unit or block_statement; if there are several such packages, the order of the implicit package_bodies is unspecified. [(For an instance, the implicit package_body occurs at the place of the instantiation (see 12.3). For a library package, the place is partially determined by the elaboration dependences (see Clause 10).)]

**Discussion:** Thus, for example, we can refer to something happening just after the begin of a package_body, and we can refer to the handled_sequence_of_statements of a package_body, without worrying about all the optional pieces. The place of the implicit body makes a difference for tasks activated by the package. See also RM83-9.3(5).

The implicit body would be illegal if explicit in the case of a library package that does not require (and therefore does not allow) a body. This is a bit strange, but not harmful.

### Dynamic Semantics

For the elaboration of a nongeneric package_body, its declarative_part is first elaborated, and its handled_sequence_of_statements is then executed.

**NOTE** A variable declared in the body of a package is only visible within this body and, consequently, its value can only be changed within the package_body. In the absence of local tasks, the value of such a variable remains unchanged between calls issued from outside the package to subprograms declared in the visible part. The properties of such a variable are similar to those of a “static” variable of C.
NOTE 2   The elaboration of the body of a subprogram explicitly declared in the visible part of a package is caused by the elaboration of the body of the package. Hence a call of such a subprogram by an outside program unit raises the exception Program_Error if the call takes place before the elaboration of the package_body (see 3.11).

Examples

Example of a package body (see 7.1):

```ada
package body Rational_Numbers is
    procedure Same_Denominator (X,Y : in out Rational) is begin
        -- reduces X and Y to the same denominator:
        ...
    end Same_Denominator;

    function "="(X,Y : Rational) return Boolean is
        U : Rational := X;
        V : Rational := Y;
    begin
        Same_Denominator (U,V);
        return U.Numerator = V.Numerator;
    end "=";

    function "/" (X,Y : Integer) return Rational is
    begin
        if Y > 0
            return (Numerator => X, Denominator => Y);
        else
            return (Numerator => -X, Denominator => -Y);
        end if;
    end "/";

    function "+" (X,Y : Rational) return Rational is ... end "+";
    function "-" (X,Y : Rational) return Rational is ... end "-";
    function "*" (X,Y : Rational) return Rational is ... end "*";
    function "/" (X,Y : Rational) return Rational is ... end "/";
end Rational_Numbers;
```

Wording Changes from Ada 83

The syntax rule for package_body now uses the syntactic category handled_sequence_of_statements.

The declarative_part of a package_body is now required; that doesn't make any real difference, since a declarative_part can be empty.

RM83 seems to have forgotten to say that a package_body can't stand alone, without a previous declaration. We state that rule here.

RM83 forgot to restrict the definition of elaboration of package_bodies to nongeneric ones. We have corrected that omission.

The rule about implicit bodies (from RM83-9.3(5)) is moved here, since it is more generally applicable.

Extensions to Ada 2005

{AI05-0267-1} An optional aspect_specification can be used in a package_body. This is described in 13.1.1.

7.3 Private Types and Private Extensions

[The declaration (in the visible part of a package) of a type as a private type or private extension serves to separate the characteristics that can be used directly by outside program units (that is, the logical properties) from other characteristics whose direct use is confined to the package (the details of the definition of the type itself). See 3.9.1 for an overview of type extensions. ]

Language Design Principles

A private (untagged) type can be thought of as a record type with the type of its single (hidden) component being the full view.
A private tagged type can be thought of as a private extension of an anonymous parent with no components. The only dispatching operation of the parent is equality (although the Size attribute, and, if nonlimited, assignment are allowed, and those will presumably be implemented in terms of dispatching).

**Syntax**

\{AI05-0183-1\} private_type_declaration ::=  
  type defining_identifier [discriminant_part] is [[abstract] tagged] [limited] private  
    [aspect_specification];

\{AI95-00251-01\} \{AI95-00419-01\} \{AI95-00443-01\} \{AI05-0183-1\} private_extension_declaration ::=  
  type defining_identifier [discriminant_part] is  
    [abstract] [limited | synchronized] new ancestor_subtype_indication  
    [and interface_list] with private  
    [aspect_specification];

**Legality Rules**

A private_type_declaration or private_extension_declaration declares a partial view of the type; such a declaration is allowed only as a declarative_item of the visible part of a package, and it requires a completion, which shall be a full_type_declaration that occurs as a declarative_item of the private part of the package. [The view of the type declared by the full_type_declaration is called the full view.] A generic formal private type or a generic formal private extension is also a partial view.

To be honest: A private type can also be imported (using aspect Import, see B.1), in which case no completion is allowed completed by a pragma import, if supported by an implementation.

Reason: We originally used the term “private view”, but this was easily confused with the view provided from the private part, namely the full view.

Proof: \{AI95-00326-01\} Full view is now defined in 3.2.1, “Type Declarations”, as all types now have them.

[A type shall be completely defined before it is frozen (see 3.11.1 and 13.14). Thus, neither the declaration of a variable of a partial view of a type, nor the creation by an allocator of an object of the partial view are allowed before the full declaration of the type. Similarly, before the full declaration, the name of the partial view cannot be used in a generic_instantiation or in a representation item.]

Proof: This rule is stated officially in 3.11.1, “Completions of Declarations”.

\{AI95-00419-01\} \{AI95-00443-01\} [A private type is limited if its declaration includes the reserved word limited; a private extension is limited if its ancestor type is a limited type that is not an interface type, or if the reserved word limited or synchronized appears in its definition limited.] If the partial view is nonlimited, then the full view shall be nonlimited. If a tagged partial view is limited, then the full view shall be limited. [On the other hand, if an untagged partial view is limited, the full view may be limited or nonlimited.]

If the partial view is tagged, then the full view shall be tagged. [On the other hand, if the partial view is untagged, then the full view may be tagged or untagged.] In the case where the partial view is untagged and the full view is tagged, no derivatives of the partial view are allowed within the immediate scope of the partial view; [derivatives of the full view are allowed.]

Ramification: Note that deriving from a partial view within its immediate scope can only occur in a package that is a child of the one where the partial view is declared. The rule implies that in the visible part of a public child package, it is impossible to derive from an untagged private type declared in the visible part of the parent package in the case where the full view of the parent type turns out to be tagged. We considered a model in which the derived type was implicitly redeclared at the earliest place within its immediate scope where characteristics needed to be added. However, we rejected that model, because (1) it would imply that (for an untagged type) subprograms explicitly declared after the derived type could be inherited, and (2) to make this model work for composite types as well, several implicit redeclarations would be needed, since new characteristics can become visible one by one; that seemed like too much mechanism.
**Discussion:** The rule for tagged partial views is redundant for partial views that are private extensions, since all extensions of a given ancestor tagged type are tagged, and limited if the ancestor is limited. We phrase this rule partially redundantly to keep its structure parallel with the other rules.

**To be honest:** This rule is checked in a generic unit, rather than using the “assume the best” or “assume the worst” method.

**Reason:** \{AI95-00230-01\} Tagged limited private types have certain capabilities that are incompatible with having assignment for the full view of the type. In particular, tagged limited private types can be extended with access discriminants and components of a limited type, which works only because assignment is not allowed. Consider the following example:

```ada
package P1 is
  type T1 is tagged limited private;
  procedure Foo(X : in T1'decls);
private
  type T1 is tagged null record; -- Illegal!
  -- This should say “tagged limited null record”.
end P1;

package body P1 is
  type A is access T1'decls;
  Global : A;
  procedure Foo(X : in T1'decls) is begin
    Global := new T1'decls'(X);
    -- This would be illegal if the full view of T1 were limited, like it's supposed to be.
  end Foo;
end P1;

package P2 is
  type T2(D : access Integer) -- Trouble!
    is new P1.T1 with
  record
    My_Task : Some_Task_Type; -- Trouble! More trouble!
  end record;
end P2;

with P1;
with P2;

procedure Main is
begin
  Local : aliased Integer;
  Y : P2.T2(D => Local'Access);
  P1.Foo(Y);
end Main;

{AI95-00230-01} If the above example were legal, we would have succeeded in making an access value that points to Main.Local after Main has been left, and we would also have succeeded in doing an assignment of a task object, both of which are supposed to be a no-no if T1 were tagged.

This rule is not needed for private extensions, because they inherit their limitedness from their ancestor, and there is a separate rule forbidding limited components of the corresponding record extension if the parent is nonlimited.

**Ramification:** A type derived from an untagged private type is untagged, even if the full view of the parent is tagged, and even at places that can see the parent:

```ada
package P is
  type Parent is private;
private
  type Parent is tagged
    record
      X : Integer;
    end record;
end P;

with P;
package Q is
  type T is new P.Parent;
end Q;
```
The declaration of T declares an untagged view. This view is always untagged, so T'Class is illegal, it would be illegal to extend T, and so forth. The component name X is never visible for this view, although the component is still there — one can get one's hands on it via a type_conversion.

{AI95-00396-01} If a full type has a partial view that is tagged, then:

- the partial view shall be a synchronized tagged type (see 3.9.4) if and only if the full type is a synchronized tagged type;

  Reason: Since we do not allow record extensions of synchronized tagged types, this property has to be visible in the partial view to avoid privacy breaking. Generic formals do not need a similar rule as any extensions are rechecked for legality in the specification, and extensions of tagged formals are always illegal in a generic body.

- the partial view shall be a descendant of an interface type (see 3.9.4) if and only if the full type is a descendant of the interface type.

  Reason: Consider the following example:

```ada
package P is
  package Pkg is
    type Ifc is interface;
    procedure Foo (X : Ifc) is abstract;
  end Pkg;

  type Parent_1 is tagged null record;
  type Parent_2 is new Parent_1 with private;
  private
    type Parent_3 is new Parent_1 and Pkg.Ifc with null record;
    procedure Foo (X : Parent_3); -- Foo #1
  end Parent_2;

  type T1 is new Parent_2 with null record; -- Illegal.
end P;

with P;
package PClient is
  type T2 is new P.T1 and P.Pkg.Ifc with null record;
  procedure Foo (X : T2); -- Foo #2
  X : T2;
end PClient;

package body P is
  ... {AI12-0005-1} procedure Bar (X : T1'Class) is
    begin
      Pkg.Foo (Pkg.Ifc'Class (X)); -- should call Foo #1 or an override thereof
    end;

    begin
      Pkg.Foo (Pkg.Ifc'Class (PClient.X)); -- should call Foo #2
      Bar (T1'Class (PClient.X));
    end P;

begin
  with Q; use Q;
  package body P is
    ... T'Class ... -- Illegal!
    Object: T;
    ... Object.X ... -- Illegal!
    ... Parent(Object).X ... -- OK.
  end P;

This example is illegal because the completion of T1 is descended from an interface that the partial view is not descended from. If it were legal, T2 would implement Ifc twice, once in the visible part of P, and once in the visible part of P Client. We would need to decide how Foo #1 and Foo #2 relate to each other. There are two options: either Foo #2 overrides Foo #1, or it doesn't.

If Foo #2 overrides Foo #1, we have a problem because the client redefines a behavior that it doesn't know about, and we try to avoid this at all costs, as it would lead to a breakdown of whatever abstraction was implemented. If the abstraction didn't expose that it implements Ifc, there must be a reason, and it should be able to depend on the fact that no overriding takes place in clients. Also, during maintenance, things may change and the full view might implement a different set of interfaces. Furthermore, the situation is even worse if the full type implements another interface Ifc2 that happens to have a conforming Foo (otherwise unrelated, except for its name and profile).

If Foo #2 doesn't override Foo #1, there is some similarity with the case of normal tagged private types, where a client can declare an operation that happens to conform to some private operation, and that's OK, it gets a different slot in the type descriptor. The problem here is that T2 would implement Ifc in two different ways, and through conversions to...
Ifc'Class we could end up with visibility on both of these two different implementations. This is the “diamond inheritance” problem of C++ all over again, and we would need some kind of a preference rule to pick one implementation. We don't want to go there (if we did, we might as well provide full-fledged multiple inheritance).

Note that there wouldn't be any difficulty to implement the first option, so the restriction is essentially methodological. The second option might be harder to implement, depending on the language rules that we would choose.

**Ramification:**[AI05-0005-1] This rule also prevents completing a private type with an interface. An interface, like all types, is a descendant of itself, and thus this rule is triggered. One reason this is necessary is that a client of a private extension should be able to inherit limitedness without having to look in the private part to see if the type is an interface (remember that limitedness of interfaces is never inherited, while it is inherited from other types).

The ancestor subtype of a private_extension_declaration is the subtype defined by the ancestor_subtype indication; the ancestor type shall be a specific tagged type. The full view of a private extension shall be derived (directly or indirectly) from the ancestor type. In addition to the places where Legality Rules normally apply (see 12.3), the requirement that the ancestor be specific applies also in the private part of an instance of a generic unit.

**Reason:** This rule allows the full view to be defined through several intermediate derivations, possibly from a series of types produced by generic instantiations.

**Ramification:**[AI95-00419-01] [AI95-00443-01] If the reserved word `limited` appears in a private_extension_declaration, the ancestor type shall be a limited type. If the reserved word `synchronized` appears in a private_extension_declaration, the ancestor type shall be a limited interface.

**Reason:**[AI12-0449-1] If the declaration of a partial view includes a known_discriminant_part, then the full_type_declaration shall have a fully conforming [(explicit)] known_discriminant_part [(see [6.3.16.3.1,”Conformance Rules”])]. [The ancestor subtype may be unconstrained; the parent subtype of the full view is required to be constrained (see 3.7).]

**Discussion:** If the ancestor subtype has discriminants, then it is usually best to make it unconstrained.

**Ramification:** If the partial view has a known_discriminant_part, then the full view has to be a composite, non-array type, since only such types may have known discriminants. Also, the full view cannot inherit the discriminants in this case; the known_discriminant_part has to be explicit.

That is, the following is illegal:

```
package P is
  type T(D : Integer) is private;
  private
    type T is new Some_Other_Type; -- Illegal!
  end P;
```

even if Some_Other_Type has an integer discriminant called D.

It is a ramification of this and other rules that in order for a tagged type to privately inherit unconstrained discriminants, the private type declaration has to have an unknown_discriminant_part.

If a private extension inherits known discriminants from the ancestor subtype, then the full view shall also inherit its discriminants from the ancestor subtype, and the parent subtype of the full view shall be constrained if and only if the ancestor subtype is constrained.

**Reason:** The first part ensures that the full view has the same discriminants as the partial view. The second part ensures that if the partial view is unconstrained, then the full view is also unconstrained; otherwise, a client might constrain the partial view in a way that conflicts with the constraint on the full view.

**Ramification:**[AI95-00419-01] [AI05-0004-1] If the full_type_declaration for a private_extension_includes a derived_type_definition, then the reserved word `limited` shall appear in the full_type_declaration if and only if it also appears in the private_extension_declaration.

**Reason:**[AI05-0004-1] The word `limited` is optional (unless the ancestor is an interface), but it should be used consistently. Otherwise things would be too confusing for the reader. Of course, we only require that if the full type includes is defined by a derived_type_definition, as we want to allow task and protected types to complete extensions of synchronized interfaces.
If a partial view has unknown discriminants, then the full_type_declaration may define a definite or an indefinite subtype, with or without discriminants.

If a partial view has neither known nor unknown discriminants, then the full_type_declaration shall define a definite subtype.

If the ancestor subtype of a private extension has constrained discriminants, then the parent subtype of the full view shall impose a statically matching constraint on those discriminants.

Ramification: If the parent type of the full view is not the ancestor type, but is rather some descendant thereof, the constraint on the discriminants of the parent type might come from the declaration of some intermediate type in the derivation chain between the ancestor type and the parent type.

Reason: This prevents the following:

```ada
package P is
  type T2 is new T1(Discrim => 3) with private;
  private
  type T2 is new T1(Discrim => 999) -- Illegal!
    with record ...;
  end P;
end P;
```

The constraints in this example do not statically match.

If the constraint on the parent subtype of the full view depends on discriminants of the full view, then the ancestor subtype has to be unconstrained:

```ada
type One_Discrim(A: Integer) is tagged ...;
...
package P is
  type Two_Discrims(B: Boolean; C: Integer) is new One_Discrim with private;
  private
  type Two_Discrims(B: Boolean; C: Integer) is new One_Discrim(A => C) with record
    ...;
  end record;
  end P;
```

The above example would be illegal if the private extension said “is new One_Discrim(A => C);”, because then the constraints would not statically match. (Constraints that depend on discriminants are not static.)

**Static Semantics**

A private_type_declaration declares a private type and its first subtype. Similarly, a private_extension_declaration declares a private extension and its first subtype.

Discussion: A package-private type is one declared by a private_type_declaration; that is, a private type other than a generic formal private type. Similarly, a package-private extension is one declared by a private_extension_declaration. These terms are not used in the RM95 version of this document.

{AI05-0269-1} A declaration of a partial view and the corresponding full_type_declaration define two views of a single type. The declaration of a partial view together with the visible part define the operations that are available to outside program units; the declaration of the full view together with the private part define other operations whose direct use is possible only within the declarative region of the package itself. Moreover, within the scope of the declaration of the full view, the characteristics (see 3.4) of the type are determined by the full view; in particular, within its scope, the full view determines the classes that include the type, which components, entries, and protected subprograms are visible, what attributes and other predefined operations are allowed, and whether the first subtype is static. See 7.3.1.

{AI95-00401-01} {AI05-0110-1} For a private extension, the characteristics of the type are determined by those of the components and user-defined primitive subprograms from its parent type and its progenitor types (if any), in the same way that those of a record extension are determined by those of its components and user-defined primitive subprograms from its parent type and its progenitor types (see 3.4 and 7.3.1).
To be honest: \{AI05-0010-1\} If an operation of the ancestor or parent type is abstract, then the abstractness of the inherited operation is different for nonabstract record extensions than for nonabstract private extensions (see 3.9.3).

**Dynamic Semantics**

The elaboration of a private_type_declaration creates a partial view of a type. The elaboration of a private_extension_declaration elaborates the ancestor_subtype_indication, and creates a partial view of a type.

NOTE 1 \{AI12-0442-1\} The partial view of a type as declared by a private_type_declaration is defined to be a composite view (in 3.2). The full view of the type can or might not be elementary or composite. A private extension is also composite, as is its full view.

NOTE 2 \{AI95-00318-02\} Declaring a private type with an unknown_discriminant_part is a way of preventing clients from creating uninitialized objects of the type; they are then forced to initialize each object by calling some operation declared in the visible part of the package. If such a type is also limited, then no objects of the type can be declared outside the scope of the full_type_declaration, restricting all object creation to the package defining the type. This allows complete control over all storage allocation for the type. Objects of such a type can still be passed as parameters, however.

**Discussion:** Packages with private types are analogous to generic packages with formal private types, as follows: The declaration of a package-private type is like the declaration of a formal private type. The visible part of the package is like the generic formal part; these both specify a contract (that is, a set of operations and other things available for the private type). The private part of the package is like an instantiation of the generic; they both give a full_type_declaration that specifies implementation details of the private type. The clients of the package are like the body of the generic; usage of the private type in these places is restricted to the operations defined by the contract.

In other words, being inside the package is like being outside the generic, and being outside the package is like being inside the generic; a generic is like an “inside-out” package.

This analogy also works for private extensions in the same inside-out way.

Many of the legality rules are defined with this analogy in mind. See, for example, the rules relating to operations of [formal] derived types.

The completion rules for a private type are intentionally quite similar to the matching rules for a generic formal private type.

This analogy breaks down in one respect: a generic actual subtype is a subtype, whereas the full view for a private type is always a new type. (We considered allowing the completion of a private_type_declaration to be a subtype_declaration, but the semantics just won’t work.) This difference is behind the fact that a generic actual type can be class-wide, whereas the completion of a private type always declares a specific type.

NOTE 3 \{AI95-00401\} \{AI12-0442-1\} The ancestor type specified in a private_extension_declaration and the parent type specified in the corresponding declaration of a record extension given in the private part can be different. If the ancestor type is not an interface type— the parent type of the full view can be any descendant of the ancestor type. In this case, for a primitive subprogram that is inherited from the ancestor type and not overridden, the formal parameter names and default expressions (if any) come from the corresponding primitive subprogram of the specified ancestor type, while the body comes from the corresponding primitive subprogram of the parent type of the full view. See 3.9.2.

NOTE 4 \{AI95-00401\} \{AI12-0442-1\} If the ancestor type specified in a private_extension_declaration is an interface type, the parent type can be any type so long as the full view is a descendant of the ancestor type. The progenitor types specified in a private_extension_declaration and the progenitor types specified in the corresponding declaration of a record extension given in the private part are not necessarily the same — it is only necessary that the private extension and the record extension be descended from the same set of interfaces.

**Examples**

**Examples of private type declarations:**

```ada
type Key is private;
type File_Name is limited private;
```

**Example of a private extension declaration:**

```ada
type List is new Ada.Finalization.Controlled with private;
```

**Extensions to Ada 83**

The syntax for a private_type_declaration is augmented to allow the reserved word tagged.
In Ada 83, a private type without discriminants cannot be completed with a type with discriminants. Ada 95 allows the full view to have discriminants, so long as they have defaults (that is, so long as the first subtype is definite). This change is made for uniformity with generics, and because the rule as stated is simpler and easier to remember than the Ada 83 rule. In the original version of Ada 83, the same restriction applied to generic formal private types. However, the restriction was removed by the ARG for generics. In order to maintain the “generic contract/private type contract analogy” discussed above, we have to apply the same rule to package-private types. Note that a private untagged type without discriminants can be completed with a tagged type with discriminants only if the full view is constrained, because discriminants of tagged types cannot have defaults.

Wording Changes from Ada 83

RM83-7.4.1(4), “Within the specification of the package that declares a private type and before the end of the corresponding full type declaration, a restriction applies...”, is subsumed (and corrected) by the rule that a type shall be completely defined before it is frozen, and the rule that the parent type of a derived type declaration shall be completely defined, unless the derived type is a private extension.

Extensions to Ada 95

{AI95-00251-01} {AI95-00396-01} {AI95-00401-01} Added interface list to private extensions to support interfaces and multiple inheritance (see 3.9.4).

{AI95-00419-01} A private extension may specify that it is a limited type. This is required for interface ancestors (from which limitedness is not inherited), but it is generally useful as documentation of limitedness.

{AI95-00443-01} A private extension may specify that it is a synchronized type. This is required in order so that a regular limited interface can be used as the ancestor of a synchronized type (we do not allow hiding of synchronization).

Extensions to Ada 2005

{AI05-0183-1} An optional aspect specification can be used in a private type declaration and a private extension declaration. This is described in 13.1.1.

Wording Changes from Ada 2005

{AI05-0110-1} Correction: The description of how a private extension inherits characteristics was made consistent with the way formal derived types inherit characteristics (see 12.5.1).

7.3.1 Private Operations

[For a type declared in the visible part of a package or generic package, certain operations on the type do not become visible until later in the package — either in the private part or the body. Such private operations are available only inside the declarative region of the package or generic package.]

Static Semantics

The predefined operators that exist for a given type are determined by the classes to which the type belongs. For example, an integer type has a predefined "+" operator. In most cases, the predefined operators of a type are declared immediately after the definition of the type; the exceptions are explained below. Inherited subprograms are also implicitly declared immediately after the definition of the type, except as stated below.

{8652/0019} {AI95-00033-01} {AI05-0029-1} For a composite type, the characteristics (see 7.3) of the type are determined in part by the characteristics of its component types. At the place where the composite type is declared, the only characteristics of component types used are those characteristics visible at that place. If later immediately within the declarative region in which the composite type is declared within the immediate scope of the composite type additional characteristics become visible for a component type, then any corresponding characteristics become visible for the composite type. Any additional predefined operators are implicitly declared at that place. If there is no such place, then additional predefined operators are not declared at all, but they still exist.

Reason: {AI05-0029-1} We say that the predefined operators exist because they can emerge in some unusual generic instantiations. See 12.5.
Discussion: {AI05-0029-1} The predefined operators for the underlying class of a type always exist, even if there is no visibility on that underlying class. This rule is simply about where (if ever) those operators are declared (and thus become usable). The “additional predefined operators” defined by this rule are any that are not declared at the point of the original type declaration. For instance, a type derived from a private type whose full type is type String always will have a “>” operator, but where that operator is declared (and thus whether it is visible) will depend on the visibility of the full type of the parent type.

{AI95-00033-01} The predefined operators for the underlying class of a type always exist, even if there is no visibility on that underlying class. This rule is simply about where (if ever) those operators are declared (and thus become usable). The “additional predefined operators” defined by this rule are any that are not declared at the point of the original type declaration. For instance, a type derived from a private type whose full type is type String always will have a “>” operator, but where that operator is declared (and thus whether it is visible) will depend on the visibility of the full type of the parent type.

{AI95-00033-01} The correspondence rule applies to a type defined by a derived_type_definition, if there is a place immediately within the declarative region in which the type is declared, where additional characteristics of its parent type become visible. For example, an array type whose component type is limited private becomes nonlimited if the full view of the component type is nonlimited and visible at some later place immediately within the declarative region in which the array type is declared, where additional characteristics of its parent type become visible. In such a case, the predefined "=" operator is implicitly declared at that place, and assignment is allowed after that place.

Discussion: Here is an example of this situation:

```ada
package P is
  type T is private;
  C : constant T;
private
  type T is new Integer;
  C : constant T := 42;
end P;
{AI12-0065-1} with P;
package Q is
  type T2 is new P.T;  -- T2 is not a descendant of Integer
end Q;
```

{AI12-0140-1} The characteristics and constraints of the designated subtype of an access type follow a somewhat different rule. The view of the designated subtype of a view of an access type at a given place is determined by the view of the designated subtype that is visible at that place, rather than the view at the place where the access type is declared.

Discussion: Here is an example of this situation:

```ada
package P is
  type T is private;
  C : constant T;
private
  type T is new Integer;
  C : constant T := 42;
end P;
{AI12-0065-1} with P;
package Q is
  type T2 is new P.T;  -- T2 is not a descendant of Integer
end Q;
```
with Q;
package P.Child is
  type T3 is new Q.T2;
private
  -- Here T3 is known to be indirectly derived from Integer, but inherits
  -- no characteristics from Integer, since T2 inherits no characteristics
  -- from Integer.
  -- However, we allow an explicit conversion of T3 to/from Integer.
  -- Hence, T3 is effectively a descendant of an "incomplete" view of Integer.
  Int : Integer := 52;
  V : T3 := T3(P.C);  -- Legal: conversion allowed
  W : T3 := T3(Int);  -- Legal: conversion allowed
  X : T3 := T3(42);   -- Error: T3 is not a numeric type
  Y : T3 := X + 1;    -- Error: no visible "+" operator
  Z : T3 := T3(Integer(W) + 1);   -- Legal: convert to Integer first
end P.Child;

Inherited primitive subprograms follow a different rule. For a derived_type_definition, each inherited primitive subprogram is implicitly declared at the earliest place, if any, immediately within the declarative region in which the corresponding declaration from the parent is visible. If there is no such place, then the inherited subprogram is not declared at all, but it still exists. [For a tagged type, it is possible to dispatch to an inherited subprogram that is not declared at all, but it cannot be named in a call and cannot be overridden, but for a tagged type, it is possible to dispatch to it.]

For a private_extension_declaration, each inherited subprogram is declared immediately after the private_extension_declaration if the corresponding declaration from the ancestor is visible at that place. Otherwise, the inherited subprogram is not declared for the private extension, [though it can be for the full type].

Reason: There is no need for the “earliest place immediately within the declarative region within the immediate scope” business here, because a private_extension_declaration will be completed with a full_type_declaration, so we can hang the necessary private implicit declarations on the full_type_declaration.

Discussion: The above rules matter only when the component type (or parent type) is declared in the visible part of a package, and the composite type (or derived type) is declared within the declarative region of that package (possibly in a nested package or a child package).

Consider:

package Parent is
  type Root is tagged null record;
  procedure Op1(X : Root);
  type My_Int is range 1..10;
private
  procedure Op2(X : Root);
  type Another_Int is new My_Int;
  procedure Int_Op(X : My_Int);
end Parent;

with Parent, use Parent;
package Unrelated is
  type T2 is new Root with null record;
  procedure Op2(X : T2);
end Unrelated;

package Parent.Child is
  type T3 is new Root with null record;
  -- Op1(T3) implicitly declared here.
  type T4 is new Root with null record;
private
end Parent.Child;
with Unrelated; use Unrelated;
package body Parent.Child is
  package body Nested is
    -- Op2(T4) implicitly declared here.
  end Nested;

  type T5 is new T2 with null record;
end Parent.Child;

Another_Int does not inherit Int_Op, because Int_Op does not “exist” at the place where Another_Int is declared.

Type T2 inherits Op1 and Op2 from Root. However, the inherited Op2 is never declared, because Parent.Op2 is never visible immediately within the declarative region within the immediate scope of T2. T2 explicitly declares its own Op2, but this is unrelated to the inherited one — it does not override the inherited one, and occupies a different slot in the type descriptor.

T3 inherits both Op1 and Op2. Op1 is implicitly declared immediately after the type declaration, whereas Op2 is declared at the beginning of the private part. Note that if Child were a private child of Parent, then Op1 and Op2 would both be implicitly declared immediately after the type declaration.

T4 is similar to T3, except that the earliest place immediately within the declarative region containing T4 within T4’s immediate scope where Root’s Op2 is visible is in the body of Nested.

If T3 or T4 were to declare a type-conformant Op2, this would override the one inherited from Root. This is different from the situation with T2.

T5 inherits Op1 and two Op2’s from T2. Op1 is implicitly declared immediately after the declaration of T5, as is the Op2 that came from Unrelated.Op2. However, the Op2 that originally came from Parent.Op2 is never implicitly declared for T5, since T2’s version of that Op2 is never visible (anywhere — it never got declared either).

For all of these rules, implicit private parts and bodies are assumed as needed.

It is possible for characteristics of a type to be revealed in more than one place:

package P is
  type Comp1 is private;
  private
    type Comp1 is new Boolean;
  end P;

package P.Q is
  package R is
    type Comp2 is limited private;
    type A is array (Integer range <>) of Comp2;
    private
      type Comp2 is new Comp1;
      -- A becomes nonlimited here.
      -- "=(A,A) return Boolean is implicitly declared here.
      ...
    end R;
  end P.Q;

package body P.Q is
  package body R is
    -- Things like "xor"(A,A) return A are implicitly declared here.
  end R;
end P.Q;

We say immediately within the declarative region in order that types do not gain operations within a nested scope. Consider:

package Outer is
  package Inner is
    type Inner_Type is private;
    private
      type Inner_Type is new Boolean;
    end Inner;
  end Inner;
  type Outer_Type is array (Natural range <>) of Inner.Inner_Type;
end Outer;
package body Outer is
  package body Inner is
    -- At this point, we can see that Inner_Type is a Boolean type.
    -- But we don't want Outer_Type to gain an "and" operator here.
  end Inner;
end Outer;

[The Class attribute is defined for tagged subtypes in 3.9. In addition,] for every subtype S of an untagged private type whose full view is tagged, the following attribute is defined:

S'Class  Denotes the class-wide subtype corresponding to the full view of S. This attribute is allowed only from the beginning of the private part in which the full view is declared, until the declaration of the full view. [After the full view, the Class attribute of the full view can be used.]

NOTE 1  Because a partial view and a full view are two different views of one and the same type, outside of the defining package the characteristics of the type are those defined by the visible part. Within these outside program units the type is just a private type or private extension, and any language rule that applies only to another class of types does not apply. The fact that the full declaration comment implement a private type with a type of a particular class (for example, as an array type) is relevant only within the declarative region of the package itself including any child units.

The consequences of this actual implementation are, however, valid everywhere. For example: any default initialization of components takes place; the attribute Size provides the size of the full view; finalization is still done for controlled components of the full view; task dependence rules still apply to components that are task objects.

NOTE 2  {AI95-00287-01} Partial views provide initialization assignment (unless the view is limited), membership tests, selected components for the selection of discriminants and inherited components, qualification, and explicit conversion. Nonlimited partial views also allow use of assignment statements.

NOTE 3  For a subtype S of a partial view, S'Size is defined (see 13.3). For an object A of a partial view, the attributes A'Size and A'Address are defined (see 13.3). The Position, First_Bit, and Last_Bit attributes are also defined for discriminants and inherited components.

Examples

Example of a type with private operations:

    package Key_Manager
      is
        type Key is private;
        Null_Key : constant Key; -- a deferred constant declaration (see 7.4)
        procedure Get_Key(K : out Key);
        function "<" (X, Y : Key) return Boolean;
    private
      type Key is new Natural;
      Null_Key : constant Key := Key'First;
    end Key_Manager;
    package body Key_Manager
      is
        Last_Key : Key := Null_Key;
        procedure Get_Key(K : out Key) is
          begin
            Last_Key := Last_Key + 1;
            K := Last_Key;
          end Get_Key;
        function "<" (X, Y : Key) return Boolean is
          begin
            return Natural(X) < Natural(Y);
          end "<";
    end Key_Manager;

{AI12-0452-1} Outside of the package Key_Manager, the operations available for objects of type Key include assignment, the comparison for equality or inequality, the procedure Get_Key and the operator "<"; they do not include other relational operators such as ">=", or arithmetic operators.

{AI12-0440-1} {AI12-0452-1} The explicitly declared operator "<" hides the predefined operator "<" implicitly declared by the full type declaration. Within the body of the function, an explicit conversion of X and Y to the subtype Natural is necessary to invoke the "<" operator of the parent type.
Alternatively, the result of the function can be written as not (X >= Y), since the operator ">=" is not redefined.

{AI12-0452-1} The value of the variable Last_Key, declared in the package body, remains unchanged between calls of the procedure Get_Key. (See also the NOTES of 7.2.)

NOTE 4 {AI12-0452-1} Notes on the example: Outside of the package Key_Manager, the operations available for objects of type Key include assignment, the comparison for equality or inequality, the procedure Get_Key and the operator "<"; they do not include other relational operators such as "=", or arithmetic operators.

{AI12-0452-1} The explicitly declared operator "<" hides the predefined operator "<" implicitly declared by the full_type_declaration. Within the body of the function, an explicit conversion of X and Y to the subtype Natural is necessary to invoke the "<" operator of the parent type. Alternatively, the result of the function could be written as not (X >= Y), since the operator ">=" is not redefined.

{AI12-0452-1} The value of the variable Last_Key, declared in the package body, remains unchanged between calls of the procedure Get_Key. (See also the NOTES of 7.2.)

Wording Changes from Ada 83

The phrase in RM83-7.4.2(7), “...after the full type declaration”, doesn't work in the presence of child units, so we define that rule in terms of visibility.

The definition of the Constrained attribute for private types has been moved to “Obsolescent Features”. (The Constrained attribute of an object has not been moved there.)

Wording Changes from Ada 95

{8652/0018} {AI05-00033-01} Corrigendum: Clarified when additional operations are declared.

{AI95-00287-01} Revised the note on operations of partial views to reflect that limited types do have an assignment operation, but not assignment_statements.

Wording Changes from Ada 2005

{AI05-0029-1} Correction: Revised the wording to say that predefined operations still exist even if they are never declared, because it is possible to reference them in a generic unit.

{AI05-0115-1} Correction: Clarified that the characteristics of a descendant of a private type depend on the visibility of the full view of the direct ancestor. This has to be the case (so that privacy is not violated), but it wasn't spelled out in earlier versions of Ada.

Wording Changes from Ada 2012

{AI12-0065-1} Corrigendum: Clarified the clarification added by AI05-0115-1, as it turned out to not be that clear. Hopefully this version is better.

{AI12-0140-1} Correction: Clarified the constraints and properties that apply to a designated subtype. This additional wording does not mean to change existing practice.

7.3.2 Type Invariants

For a private type or private extension, or interface, the following language-defined assertion aspects may be specified with an aspect_specification (see 13.1.1):

Type Invariant

This aspect shall be specified by an expression, called an invariant expression. Type Invariant may be specified on a private_type_declaration, on a private_extension_declaration, or on a full_type_declaration that declares the completion of a private type or private extension.

Aspect Description for Type_Invariant: A condition that will hold true for all objects of a type.

Type Invariant'Class

This aspect shall be specified by an expression, called an invariant expression. Type_Invariant'Class may be specified on a private_type_declaration, or a private_extension_declaration, or a full_type_declaration for an interface type.
Type_Invariant'Class determines a class-wide type invariant for a tagged type. [The Type_Invariant'Class aspect is not inherited, but its effects are additive, as defined below.]

Reason: {AI05-0254-1} A class-wide type invariant cannot be hidden in the private part, as the creator of an extension needs to know about it in order to conform to it in any new or overriding operations. On the other hand, a specific type invariant is not inherited, so that no operation outside of the original package needs to conform to it; thus there is no need for it to be visible.

Aspect Description for Type_Invariant'Class: A condition that will hold true for all objects in a class of types.

Term entry: invariant — assertion that is expected to be True for all objects of a given private type when viewed from outside the defining package

Name Resolution Rules

{AI05-0146-1} The expected type for an invariant expression is any boolean type.

{AI05-0146-1} {AI12-0150-1} {AI12-0159-1} {AI12-0199-1} [Within an invariant expression, the identifier of the first subtype of the associated type denotes the current instance of the type.] Within an invariant expression for the Type_Invariant aspect of a type T, the type of this current instance is T. Within an invariant expression for the Type_Invariant aspect and T'Class for the Type_Invariant'Class aspect of a type T, the type of this current instance is interpreted as though it had a (notional) nonabstract type NT that is a visible formal derived type whose ancestor type is T. [The effect of this interpretation is that the only operations that can be applied to this current instance are those defined for such a formal derived type.]

Proof: The first sentence is given formally in 13.1.1.

Reason: {AI12-0159-1} The rules for Type_Invariant'Class ensure that the invariant expression is well-defined for any type descended from T.

Legality Rules

{AI05-0146-1} [The Type_Invariant'Class aspect shall not be specified for an untagged type.] The Type_Invariant aspect shall not be specified for an abstract type.

Proof: The first sentence is given formally in 13.1.1.

{AI12-0042-1} {AI12-0382-1} If a type extension occurs immediately within the visible part of a package specification, at a point where a private operation of some ancestor is visible and inherited, and a Type_Invariant'Class expression applies to that ancestor, then the inherited operation shall be abstract or shall be overridden.

Static Semantics

{AI05-0250-1} [If the Type_Invariant aspect is specified for a type T, then the invariant expression applies to T.]

{AI05-0146-1} {AI12-0199-1} If the Type_Invariant'Class aspect is specified for a tagged type T, then a corresponding expression also applies to each nonabstract descendant TI of T [(including T itself if it is nonabstract)]. The corresponding expression is constructed from the associated expression as follows: the invariant expression applies to all descendants of T:

- {AI12-0199-1} References to nondiscriminant components of T (or to T itself) are replaced with references to the corresponding components of TI (or to TI as a whole).

  Ramification: {AI12-0199-1} The only nondiscriminant components visible at the point of such an aspect specification are necessarily inherited from some nonprivate ancestor.

- {AI12-0199-1} References to discriminants of T are replaced with references to the corresponding discriminant of TI, or to the specified value for the discriminant, if the discriminant is specified by the derived_type_definition for some type that is an ancestor of TI and a descendant of T (see 3.7).
This paragraph was deleted

**Proof:** "Applies" is formally defined in 13.1.1.

**Discussion:** The associated expression from which the corresponding expression is constructed is the one that applies to the descendant type; "applies" is formally defined in 13.1.1.

8.3/5

\{AI12-0075-1\} \{AI12-0191-1\} For a nonabstract type \( T \), a callable entity is said to be a **boundary entity** for \( T \) if it is declared within the immediate scope of \( T \) (or by an instance of a generic unit, and the generic is declared within the immediate scope of type \( T \)), or is the Read or Input stream-oriented attribute of type \( T \), and either:

- \( T \) is a private type or a private extension and the callable entity is visible outside the immediate scope of type \( T \) or overrides an inherited operation that is visible outside the immediate scope of \( T \); or
- \( T \) is a record extension, and the callable entity is a primitive operation visible outside the immediate scope of type \( T \) or overrides an inherited operation that is visible outside the immediate scope of \( T \).

**Reason:** \{AI12-0191-1\} A **boundary entity** for type \( T \) is one that might require an invariant check for \( T \). It includes subprograms that don't (visibly) involve \( T \); since we don't want to break privacy, we can't statically know if some private type has some part of \( T \). We'll reduce the set when we describe the actual checks.

**Dynamic Semantics**

8.4/5

- \( T \) is a private type or a private extension and the callable entity is visible outside the immediate scope of type \( T \) or overrides an inherited operation that is visible outside the immediate scope of \( T \); or
- \( T \) is a record extension, and the callable entity is a primitive operation visible outside the immediate scope of type \( T \) or overrides an inherited operation that is visible outside the immediate scope of \( T \).

**Reason:** \{AI12-0191-1\} A **boundary entity** for type \( T \) is one that might require an invariant check for \( T \). It includes subprograms that don't (visibly) involve \( T \); since we don't want to break privacy, we can't statically know if some private type has some part of \( T \). We'll reduce the set when we describe the actual checks.

9/4

\{AI05-0146-1\} \{AI05-0247-1\} \{AI05-0290-1\} \{AI12-0150-1\} If one or more invariant expressions apply to a nonabstract type \( T \), then an invariant check is performed at the following places, on the specified object(s):

- \{AI12-0133-1\} After successful default initialization of an object of type \( T \) by default (see 3.3.1), the check is performed on the new object unless the partial view of \( T \) has unknown discriminants;

**Reason:** \{AI12-0133-1\} The check applies everywhere, even in the package body, because default initialization has to work the same for clients as it does within the package. As such, checks within the package are either harmless or will uncover a bug that could also happen to a client. However, if the partial view of the type has unknown discriminants, no client of the package can declare a default-initialized object. Therefore, no invariant check is needed, as all default initialized objects are necessarily inside the package.

10/4

- \{AI12-0133-1\} After successful explicit initialization of the completion of a deferred constant whose nominal type has with a part of type \( T \), if the completion is inside the immediate scope of the full view of \( T \), and the deferred constant is visible outside the immediate scope of \( T \), the check is performed on the part(s) of type \( T \);

10.1/5

- \{AI12-0049-1\} \{AI12-0191-1\} After successful explicit initialization of the completion of a deferred constant whose nominal type has with a part of type \( T \), if the completion is inside the immediate scope of the full view of \( T \), and the deferred constant is visible outside the immediate scope of \( T \), the check is performed on the part(s) of type \( T \);

11/3

- After successful conversion to type \( T \), the check is performed on the result of the conversion;

12/3

- \{AI05-0146-1\} \{AI05-0269-1\} For a view conversion, outside the immediate scope of \( T \) that converts from a descendant of \( T \) (including \( T \) itself) to an ancestor of type \( T \) (other than \( T \) itself), a check is performed on the part of the object that is of type \( T \):

  - after assigning to the view conversion; and
  - after successful return from a call that passes the view conversion as an **in out** or **out** parameter.

13/3

**Ramification:** For a single view conversion that converts between distantly related types, this rule could be triggered for multiple types and thus multiple invariant checks may be needed.

14/3

**Implementation Note:** \{AI05-0299-1\} For calls to inherited subprograms (including dispatching calls), the implied view conversions mean that a wrapper is probably needed. (See the Note at the bottom of this subclause for more on the model of checks for inherited subprograms.)

For view conversions involving class-wide types, the exact checks needed may not be known at compile-time. One way to deal with this is to have an implicit dispatching operation that is given the object to check and the tag of the target of the conversion, and which first checks if the passed tag is not for itself, and if not, checks the its invariant on the object and then calls the operation of its parent type. If the tag is for itself, the operation is complete.
Upon a successful return from a call on any callable entity which is a boundary entity for \( T \), an invariant is checked for each object which is subject to an invariant check for \( T \). In the case of a call to a protected operation, the check is performed before the end of the protected action. In the case of a call to a task entry, the check is performed before the end of the rendezvous. The object initialized by the stream attribute is subject to an invariant check for \( T \).

An invariant is checked upon successful return from a call on any subprogram or entry that:

1. A result with a nominal type that has a part declared within the immediate scope of type \( T \), or by an instance of a generic unit, and the generic is declared within the immediate scope of type \( T \), and
2. An out or in out parameter whose nominal type has a part of type \( T \), is visible outside the immediate scope of type \( T \) or overrides an operation that is visible outside the immediate scope of type \( T \), and
3. An access-to-object parameter or result whose designated nominal type has a part of type \( T \), or
4. A procedure or entry parameter whose nominal type has a part of type \( T \), and either has a result with a part of type \( T \), or one or more parameters with a part of type \( T \), or an access to a variable parameter whose designated type has a part of type \( T \).

This is a Dynamic Semantics rule, so we ignore privacy when determining if a check is needed. We do, however, use the nominal type of objects to determine if a part of type \( T \) is present; therefore, parts that aren’t known at compile-time (after ignoring privacy) are never subject to an invariant check. This is preferable, as we don’t want overhead associated with the possibility that there might exist an extension of a tagged type that has a part of type \( T \). (See the “leaks” note below for avoidance advice.)

1. Has a result with a part of type \( T \), or
2. Has one or more out or in out parameters with a part of type \( T \), or
3. Has an access-to-object parameter or result whose designated type has a part of type \( T \), or
4. Is a procedure or entry that has an in parameter with a part of type \( T \).

Discussion: We don’t check in parameters for functions to avoid infinite recursion for calls to public functions appearing in invariant expressions. Such function calls are unavoidable for class-wide invariants and likely for other invariants. This is the simplest rule that avoids trouble, and functions are much more likely to be queries that don’t modify their parameters than other callable entities.

If the nominal type of a formal parameter (or the designated nominal type of an access-to-object parameter or result) is
incomplete at the point of the declaration of the callable entity, and if the completion of that incomplete type does not occur in the same declaration list as the incomplete declaration, then for purposes of the preceding rules the nominal type is considered to have no parts. The check is performed on each such part of type \( T \).

- \{AI12-0042-1\} For a view conversion to a class-wide type occurring within the immediate scope of \( T \), from a specific type that is a descendant of \( T \) (including \( T \) itself), a check is performed on the part of the object that is of type \( T \).

**Reason:** Class-wide objects are treated as though they exist outside the scope of every type, and may be passed across package "boundaries" freely without further invariant checks.

- \{AI12-0167-1\} Despite this model, if an object of type \( T \) that is a component of a class-wide object is modified within the scope of the full view of type \( T \), then there is no invariant check for \( T \) at that point.

- \{AI05-0290-1\} \{AI12-0080-1\} \{AI12-0159-1\} If performing checks is required by the Type_Invariant or Type_Invariant'Class invariant assertion policies (see 11.4.2) in effect at the point of the corresponding aspect specification applicable to a given type, then the respective invariant expression is considered enabled.

**Ramification:** If a class-wide invariant expression is enabled for a type, it remains enabled when inherited by descendants of that type, even if the policy in effect is Ignore for the inheriting type.

- \{AI05-0146-1\} \{AI05-0250-1\} \{AI05-0289-1\} \{AI05-0290-1\} The invariant check consists of the evaluation of each enabled invariant expression that applies to \( T \), on each of the objects specified above. If any of these evaluate to False, Assertions.Assertion Error is raised at the point of the object initialization, conversion, or call. If a given call requires more than one evaluation of an invariant expression, either for multiple objects of a single type or for multiple types with invariants, the evaluations are performed in an arbitrary order, and if one of them evaluates to False, it is not specified whether the others are evaluated. Any invariant check is performed prior to copying back any by-copy in out or out parameters. Invariant checks, any postcondition check, and any constraint or predicate checks associated with in out or out parameters are performed in an arbitrary order.

- \{AI12-0150-1\} \{AI12-0159-1\} For an invariant check on a value of type \( T1 \) based on a class-wide invariant expression inherited from an ancestor type \( T \), any operations within the invariant expression that were resolved as primitive operations of the (notional) formal derived type \( NT \) are bound to the corresponding operations of type \( T1 \) in the evaluation of the invariant expression for the check on \( T1 \).

- \{AI05-0146-1\} \{AI05-0247-1\} \{AI05-0250-1\} The invariant checks performed on a call are determined by the subprogram or entry actually invoked, whether directly, as part of a dispatching call, or as part of a call through an access-to-subprogram value.

**Ramification:** \{AI12-0149-1\} \{AI12-0167-1\} \{AI12-0210-1\} Type invariant checks are intended to prevent invariant-violating values from inadvertently "leaking out"; that is, code which cannot see the completion of the private type should not be able to reference invariant-violating values of the type (assuming the type invariant condition itself is well behaved - for example, no uses of global variables during evaluation of the invariant expression). This goal is not completely achieved; such leaking is possible but, importantly, it requires assistance (deliberate or not) of some form from the package that declares the invariant-bearing private type (or a child unit thereof); a client of a well-crafted package cannot use these holes to obtain an invariant-violating value without help. Invariant checks on subprogram return are not performed on objects that are accessible only through access values that are subcomponents of some other object. It is also possible to call through an access-to-subprogram value and reach a subprogram body that has visibility on the full declaration of a type, from outside the immediate scope of the type. No invariant checks will be performed if the designated subprogram is not itself externally visible. These cases represent "holes" in the protection provided by invariant checks, but note that these holes cannot be caused by clients of the type \( T \) with the invariant. The designer of the package has to declare a visible type with an access-to-\( T \) subcomponent and use it as a parameter or result to subprograms in the package, or pass the client an access-to-subprogram value representing a private operation of the package. In the absence of such things, all values that the client can see will be checked for a private type or extension without help for the designer of the package containing \( T \).

- \{AI12-0210-1\} The list of known techniques whereby this kind of leak can occur (ignoring things like erroneous execution and the various forms of unchecked type conversion) consists of:
• A boundary entity might assign an invariant-violating value to a global variable that is visible to client code.

• \{AI12-0149-1\} Invariant checks on subprogram return are not performed on objects that are accessible only through access-valued components of other objects. This can only cause a leak if there is a type with access-valued components that is used as a parameter or result type of a boundary entity. For a type \( T \) that has a type invariant, avoiding the declaration of types with access-valued components designating objects with parts of \( T \) in the package that contains \( T \) is sufficient to prevent this leak.

• A client could call through an access-to-subprogram value and reach a subprogram body that has visibility on the full declaration of a type; no invariant checks will be performed if the designated subprogram is not itself a boundary subprogram. This leak can only happen if an access-to-subprogram value of a subprogram that is not visible to clients is passed out to clients.

• \{AI12-0167-1\} \{AI12-0191-1\} Invariant checks are only performed for parts of the nominal type for tagged parameters and function results. This means that components of extensions are not checked (these would be very expensive to check as any tagged type might have such an extension in the future, even though that would be very unlikely). For this leak to occur for a type \( T \) that has a type invariant, the body of a boundary entity of \( T \) needs to have visibility on a type extension that has components of \( T \) or access-to-\( T \) and also has an ancestor type (or class) as a parameter or result of the subprogram.

• \{AI12-0383-1\} Invariant checks are not performed for parts of incomplete types when the completion is not available. For this leak to occur for a type \( T \) that has a type invariant and is declared in a package \( P \), one has to use a \texttt{limited with} on a package that has \( P \) in its semantic closure, and then use a type from that package as a parameter or result of a boundary subprogram for \( T \) (or as the designated type of a parameter or result of such a subprogram).

• \{AI12-0210-1\} Consider a package \( P \) which declares an invariant-bearing private type \( T \) and a generic package \( P.G1 \), which in turn declares another generic package \( P.G1.G2 \). Outside of package \( P \), there are declarations of an instantiation \( I1 \) of \( P.G1 \) and an instantiation \( I2 \) of \( I1.G2 \). \( I2 \) can declare visible subprograms whose bodies see the full view of \( T \) and yet these subprograms are not boundary subprograms (because the generic \( I1.G2 \) is not declared within the immediate scope of \( T.G1.G2 \) is, but that's irrelevant). So a call to one of these subprograms from outside of \( P \) could yield an invariant-violating value. So long as a nested generic of a nested generic unit of \( P \) is not declared, no such leaks are possible.

\{AI12-0210-1\} All of these leaks require cooperation of some form (as detailed above) from within the immediate scope of the invariant-bearing type.

\textbf{Implementation Note:} The implementation might want to produce a warning if a private extension has an ancestor type that is a visible extension, and an invariant expression depends on the value of one of the components from a visible extension part.

\textbf{NOTE} \{AI05-0250-1\} \{AI05-0269-1\} For a call of a primitive subprogram of type \( NT \) that is inherited from type \( T \), the specified checks of the specific invariants of both the types \( NT \) and \( T \) are performed. For a call of a primitive subprogram of type \( NT \) that is overridden for type \( T \), the specified checks of the specific invariants of only type \( NT \) are performed.

\textbf{Proof:} This follows from the definition of a call on an inherited subprogram as view conversions of the parameters of the type and a call to the original subprogram (see 3.4), along with the normal invariant checking rules. In particular, the call to the original subprogram takes care of any checks needed on type \( T \), and the checks required on view conversions take care of any checks needed on type \( NT \), specifically on \texttt{in} \, \texttt{out} \, and \texttt{out} parameters. We require this in order that the semantics of an explicitly defined wrapper that does nothing but call the original subprogram is the same as that of an inherited subprogram.

\textbf{Examples}

\{AI12-0312-1\} \{AI12-0429-1\} \textbf{Example of a work scheduler where only urgent work can be scheduled for weekends:}

\begin{verbatim}
package Work_Orders is
   -- See 3.5.1 for type declarations of Level, Day, and Weekday
   type Work_Order is private with
     Type_Invariant => Day_Scheduled (Work_Order) in Weekday
     or else Priority (Work_Order) = Urgent;
   function Schedule Work (Urgency : in Level;
     To Occur : in Day) return Work_Order
     with Pre => Urgency = Urgent or else To Occur in Weekday;
   function Day_Scheduled (Order : in Work_Order) return Day;
   function Priority (Order : in Work_Order) return Level;
end Work_Orders;
\end{verbatim}
procedure Change_Priority (Order        : in out Work_Order;
                            New Priority : in   Level;
                            Changed      : out   Boolean)
with Post => Changed = (Day_Scheduled(Order) in Weekday
                           or else Priority(Order) = Urgent);

private

  type Work_Order is record
    Scheduled : Day;
    Urgency   : Level;
  end record;
end Work_Orders;

package body Work_Orders is

  function Schedule_Work (Urgency  : in   Level;
                           To_Occur   : in   Day) return Work_Order is
    (Scheduled => To_Occur, Urgency => Urgency);
  function Day_Scheduled (Order    : in   Work_Order) return Day is
    (Order.Scheduled);
  function Priority (Order        : in   Work_Order) return Level is
    (Order.Urgency);

  procedure Change_Priority (Order        : in out Work_Order;
                              New Priority : in   Level;
                              Changed      : out   Boolean) is
    begin
      -- Ensure type invariant is not violated
      if Order.Urgency = Urgent or else (Order.Scheduled in Weekday) then
        Changed := True;
        Order.Urgency := New Priority;
      else
        Changed := False;
      end if;
    end Change_Priority;
end Work_Orders;

Extensions to Ada 2005

{AI05-0146-1} {AI05-0247-1} {AI05-0250-1} {AI05-0289-1} Type Invariant aspects are new.

Inconsistencies With Ada 2012

{AI12-0042-1} Corrigendum: Clarified the definition of when invariant checks occur for inherited subprograms. This might cause checks to be added or removed in some cases. These are all rare cases involving class-wide type invariants and either record extensions or multiple levels of derivation. Additionally, implementations probably make the checks as the intent seems clear, even though the formal language did not include them. So we do not expect this to be a problem in practice.

{AI12-0042-1} Corrigendum: Added invariant checks for conversions to class-wide types. This might cause an invariant check to fail in some cases where they would not be made in the original definition of Ada 2012. Such cases represent a hole where a value that fails an invariant could "leak out" of a package, and as such will detect far more bugs than it causes.

{AI12-0044-1} Corrigendum: Removed the invariant check for in parameters of functions, so that typical invariants don't cause infinite recursion. This is strictly inconsistent, as the Ada 2012 definition has this check; therefore, programs could depend on Assertion_Error being raised upon the return from some call on a public function. However, as the intent of assertion checking is to uncover bugs, a program that depends on a bug occurring seems very unlikely.

{AI12-0049-1} {AI12-0149-1} Corrigendum: Added an invariant check for deferred constants and for access values returned from functions, so they cannot be used to "leak" values that violate the invariant from a package. This is strictly inconsistent, as the Ada 2012 definition is missing these checks; therefore, programs could depend on using values that violate an invariant outside of the package of definition. These will not raise Assertion_Error in Ada 2012 as defined in the Ada 2012 Reference Manual, but ought to do so (as noted by this change). As these are a violation of the intent of invariants, we think that this change will mainly reveal bugs rather than cause them.

{AI12-0150-1} {AI12-0159-1} Corrigendum: Eliminated unintentional redispacthing from class-wide type invariants. This means that a different body might be evaluated for a type invariant check where the value has a different tag than
that of the type. The change means that the behavior of Type_Invariant and Type_Invariant'Class will be the same for a particular subprogram, and that the known behavior of the operations can be assumed. We expect that this change will primarily fix bugs, as it will make class-wide type invariants work more like expected. In the case where redispating is desired, an explicit conversion to a class-wide type can be used.

**Correction:** Class-wide type invariants are no longer checked for abstract types. Thus, a program that previously raised Assertion_Error because of a call to a concrete subprogram of an abstract type will no longer do so. However, programs that depend on assertion failure are likely to be very rare, some explicit conversion to the abstract type is needed to get static binding, and additionally many such checks would call abstract functions (likely causing some compiler failure). As such, this incompatibility most likely will never be seen in practice.

**Incompatibilities With Ada 2012**

**Correction:** A private operation that is inherited in the visible part of a package to which a class-wide invariant applies now requires overriding. This is a very unlikely situation, and will prevent problems with invariant checks being added to routines that assume that they don't have them. Note: The original wording was missing the restriction to the visible part of the package, this was added later for Ada 2022.

**Extensions to Ada 2012**

**Correction:** Class-wide type invariants can now be specified on interfaces as well as private types.

**Wording Changes from Ada 2012**

**Correction:** Clarified when type invariant checks happen for protected actions and entry calls.

**Correction:** Clarified that type invariant checks do not occur for parts of incomplete types unless the completion is available.

### 7.3.3 Default Initial Conditions

**For a private type or private extension (including a generic formal type), the following language-defined assertion aspect may be specified with an aspect_specification (see 13.1.1):**

**Default_Initial_Condition**

This aspect shall be specified by an expression, called a *default initial condition expression*. Default_Initial_Condition may be specified on a private_type_declaration, a private_extension_declaration, a formal_private_type_definition, or a formal_derived_type_definition. [The Default_Initial_Condition aspect is not inherited, but its effects are additive, as defined below.]

**Aspect Description for Default_Initial_Condition:** A condition that will hold true after the default initialization of an object.

**Term entry:** default initial condition — property that holds for every default-initialized object of a given type

**Name Resolution Rules**

**The expected type for a default initial condition expression is any boolean type.**

**Within a default initial condition expression associated with a declaration for a type T, a name that denotes the declaration is interpreted as a current instance of a notional (nonabstract) formal derived type NT with ancestor T, that has directly visible primitive operations.**
Reason: This is analogous to the rule for Post'Class (see 6.1.1) and ensures that the expression is well-defined for any descendant of type T.

Ramification: The operations of NT are also nonabstract, so the rule against a call of an abstract subprogram does not trigger for a default initial condition for an abstract type. Note that, presuming T is tagged, it is possible to call class-wide operations of the type T given an object of type NT. Similarly it is possible to explicitly convert an object of type NT to a subtype of T, and pass it to a nonprimitive operation expecting a parameter of type T. [Note that one cannot directly convert to (the first subtype of) T since it represents the current instance of the type within the aspect expression, but one can convert to a subtype of T (including a subtype that matches the first subtype).]

Legality Rules

| 5/5 | \{AI12-0265-1\} The Default Initial Condition aspect shall not be specified for a type whose partial view has unknown discriminants, whether explicitly declared or inherited. |

Static Semantics

| 6/5 | \{AI12-0265-1\} If the Default Initial Condition aspect is specified for a type T, then the default initial condition expression applies to T and to all descendants of T. |

Dynamic Semantics

| 7/5 | \{AI12-0265-1\} \{AI12-0397-1\} If one or more default initial condition expressions apply to a [nonabstract] type T, then a default initial condition check is performed after successful initialization of an object of type T by default (see 3.3.1). In the case of a controlled type, the check is performed after the call to the type's Initialize procedure (see 7.6). |
| 7.a/5 | **Proof:** \{AI12-0397-1\} If T is an abstract type, then there will never be an initialization of an object of the type. |

| 8/5 | \{AI12-0265-1\} If performing checks is required by the Default Initial Condition assertion policy (see 11.4.2) in effect at the point of the corresponding aspect specification applicable to a given type, then the respective default initial condition expression is considered enabled. |

| 9/5 | \{AI12-0265-1\} \{AI12-0397-1\} The default initial condition check consists of the evaluation of each enabled default initial condition expression that applies to T. Any operations within such an expression that were resolved as primitive operations of the (notional) formal derived type NT, are in the evaluation of the expression resolved as for a formal derived type in an instance with T as the actual type for NT (see 12.5.1). These evaluations, if there are more than one, are performed in an arbitrary order. If any of these evaluate to False, Assertions.Assertion_Error is raised at the point of the object initialization. |
| 9.a/5 | **Ramification:** \{AI12-0397-1\} Just as is true for a formal derived type (see 12.5.1), for a tagged type T, the controlling tag of a call on a primitive of NT will cause the body of the corresponding primitive of T to be executed. For an untagged type T, invoking a primitive of NT will cause the body of the operation of the type where the aspect originated to be executed, with conversions performed as for an inherited subprogram. |

| 10/5 | \{AI12-0272-1\} [For a generic formal type T, default initial condition checks performed are as determined by the actual type, along with any default initial condition of the formal type itself.] |
| 10.a/5 | **Proof:** This follows from the general dynamic semantics rules given above, but we mention it explicitly so that there can be no doubt that it is intended. |

Implementation Permissions

| 11/5 | \{AI12-0332-1\} Implementations may extend the syntax or semantics of the Default Initial Condition aspect in an implementation-defined manner. |
| 11.a/5 | **Implementation defined:** Any extensions of the Default Initial Condition aspect. |
| 11.b/5 | **Reason:** This is intended to allow preexisting usages from SPARK 2014 to remain acceptable in conforming implementations, as well as to provide future flexibility. Note the word “extend” in this permission; we expect that any aspect usage that conforms with the (other) rules of this subclause will be accepted by any Ada implementation, regardless of any implementation-defined extensions. |
| 12/5 | **NOTE:** \{AI12-0312-1\} For an example of the use of this aspect, see the Vector container definition in A.18.2. |
### 7.3.4 Stable Properties of a Type

**{AI12-0187-1} {AI12-0324-1}** Certain characteristics of an object of a given type are unchanged by most of the primitive operations of the type. Such characteristics are called stable properties of the type.

**Term entry: stable property** — characteristic associated with objects of a given type that is preserved by many of the primitive operations of the type.

**Static Semantics**

**{AI12-0187-1}** A property function of type \( T \) is a function with a single parameter of type \( T \) or of a class-wide type that covers \( T \).

**Reason:** This provides restrictions on name resolution so overloaded functions can be used as a stable property function.

**{AI12-0285-1} {AI12-0324-1} {AI12-0388-1}** A type property aspect definition is a list of names written in the syntax of a positional array aggregate. A subprogram property aspect definition is a list of names, each optionally preceded by reserved word not, also written in the syntax of a positional array aggregate.

**To be honest:** A single name would technically be a parenthesized expression rather than an aggregate; we mean to include that here. We say "syntax of a positional array aggregate" to hopefully clarify that the specification is in no other way an actual aggregate.

**{AI12-0187-1} {AI12-0272-1}** For a nonformal private type, nonformal private extension, or full type that does not have a partial view, the following language-defined aspects may be specified with an aspect specification (see 13.1.1):

**{AI12-0187-1} {AI12-0285-1}** Stable_Properties

This aspect shall be specified by a type property aspect definition; each name shall statically denote a single property function of the type. This aspect defines the specific stable property functions of the associated type.

**Discussion:** We do not allow this aspect on generic formal types, as it is only meaningful for primitive subprograms and generic formal types have no such subprograms.

**Ramification:** Class-wide aspects are only allowed on tagged types (see 13.1.1), so we don't say that here.

**Aspect Description for Stable_Properties:** A list of functions describing characteristics that usually are unchanged by primitive operations of the type or an individual primitive subprogram.

**{AI12-0187-1} {AI12-0285-1} Stable_Properties'Class**

This aspect shall be specified by a type property aspect definition; each name shall statically denote a single property function of the type. This aspect defines the class-wide stable property functions of the associated type. [Unlike most class-wide aspects, Stable_Properties'Class is not inherited by descendant types and subprograms, but the enhanced class-wide postconditions are inherited in the normal manner.]

**Proof:** Class-wide inheritance has to be explicitly defined. Here we are not making such a definition, so there is no inheritance. 6.1.1 defines the inheritance of class-wide postconditions.

**Discussion:** Since class-wide postconditions are inherited by descendants, we don't need the stable property functions to be inherited; if they were inherited, we'd be duplicating the checks, which we don't want.

**Ramification:** Class-wide aspects are only allowed on primitive subprograms of tagged types (see 13.1.1), so we don't say that here.

**Aspect Description for Stable_Properties'Class:** A list of functions describing characteristics that usually are unchanged by primitive operations of a class of types or a primitive subprogram for such a class.
The specific and class-wide stable properties of a type together comprise the stable properties of the type.

For a primitive subprogram, the following language-defined aspects may be specified with an aspect specification (see 13.1.1):

**Stable_Properties**

This aspect shall be specified by a subprogram property aspect definition; each name shall statically denote a single property function of a type for which the associated subprogram is primitive.

**Stable_Properties'Class**

This aspect shall be specified by a subprogram property aspect definition; each name shall statically denote a single property function of a tagged type for which the associated subprogram is primitive. [Unlike most class-wide aspects, Stable_Properties'Class is not inherited by descendant subprograms, but the enhanced class-wide postconditions are inherited in the normal manner.]

**Reason:** The subprogram versions of Stable_Properties are provided to allow overriding the stable properties of a type for an individual primitive subprogram. While they can be used even if the type has no stable properties, that is not an intended use (as simply modifying the postcondition directly makes more sense for something that only happens in one place).

**Legality Rules**

A stable property function of a type \( T \) shall have a nonlimited return type and shall be:

- a primitive function with a single parameter of mode \( \text{in} \) of type \( T \); or
- a function that is declared immediately within the declarative region in which an ancestor type of \( T \) is declared and has a single parameter of mode \( \text{in} \) of a class-wide type that covers \( T \).

In a subprogram property aspect definition for a subprogram \( S \):

- all or none of the items shall be preceded by \( \text{not} \);  
  **Ramification:** Mixing \( \text{not} \) functions with regular functions is not allowed.
- any property functions mentioned after \( \text{not} \) shall be a stable property function of a type for which \( S \) is primitive.

If a subprogram renaming declaration declares a primitive subprogram of a type \( T \), then the renamed callable entity shall also be a primitive subprogram of type \( T \) and the two primitive subprograms shall have the same specific stable property functions and the same class-wide stable property functions (see below).

**Static Semantics**

For a primitive subprogram \( S \) of a type \( T \), the specific stable property functions of \( S \) for type \( T \) are:

- if \( S \) has an aspect Stable_Properties specified that does not include \( \text{not} \), those functions denoted in the aspect Stable_Properties for \( S \) that have a parameter of \( T \) or \( T'\text{Class} \);
- if \( S \) has an aspect Stable_Properties specified that includes \( \text{not} \), those functions denoted in the aspect Stable_Properties for \( T \), excluding those denoted in the aspect Stable_Properties for \( S \);
- if \( S \) does not have an aspect Stable_Properties, those functions denoted in the aspect Stable_Properties for \( T \), if any.

**Discussion:** A primitive subprogram can be primitive for more than one type, and thus there can be more than one such set of specific stable properties for a subprogram. Thus we say "specific stable property functions for subprogram \( S \) for type \( T \)".
A similar definition applies for class-wide stable property functions by replacing aspect Stable_Properties with aspect Stable_Properties'Class in the above definition.

The explicit specific postcondition expression for a subprogram $S$ is the expression directly specified for $S$ with the Post aspect. Similarly, the explicit class-wide postcondition expression for a subprogram $S$ is the expression directly specified for $S$ with the Post'Class aspect.

For a primitive subprogram $S$ of a type $T$ that has a parameter $P$ of type $T$, the parameter is excluded from stable property checks if:

- $S$ is a stable property function of $T$;
  
  **Reason:** This prevents possible infinite recursion, where the postcondition calls the function itself (directly or indirectly).

- $P$ has mode `out`;
  
  **Reason:** A parameter of mode `out` doesn't necessarily have a defined input value, so there is no old value to compare with. Ideally, the postcondition will include expressions defining the values of the stable properties after the call, but we do not try to ensure this.

- the Global aspect of $S$ is `null`, and $P$ has mode `in` and the mode is not overridden by a global aspect.
  
  **Reason:** An in parameter of a Global `=> null` subprogram cannot be modified, even if it has indirect parts, without violating the Global aspect. Thus, there is no need to assert that the properties don't change.

For every primitive subprogram $S$ of a type $T$ that is not an abstract subprogram or null procedure, the specific postcondition expression of $S$ is modified to include expressions of the form $F(P) = F(P)'Old$, all anded with each other and any explicit specific postcondition expression, with one such equality included for each specific stable property function $F$ of $S$ for type $T$ that does not occur in the explicit specific postcondition expression of $S$, and $P$ is each parameter of $S$ that has type $T$ and is not excluded from stable property checks. The resulting specific postcondition expression of $S$ is used in place of the explicit specific postcondition expression of $S$ [when interpreting the meaning of the postcondition as defined in 6.1.1].

**Ramification:** There is one $F(P) = F(P)'Old$ subexpression for every combination of a specific stable property function of type $T$ and a parameter of type $T$. For instance, if there are three specific stable property functions for type $T$ and two parameters of type $T$, then there are six such subexpressions appended to the postcondition. The resulting specific postcondition is evaluated as described in 6.1.1. One hopes that compilers can be smart enough to prove that many of these added postcondition subexpressions cannot fail, but that is not required here.

**Reason:** Null procedures and abstract subprograms are excluded as they do not allow specific postconditions. Moreover, for null procedures, static analysis tools can be certain that their parameters aren't modified so there is no need to assert that the properties don't change. Abstract subprograms cannot be called directly.

For every primitive subprogram $S$ of a type $T$, the class-wide postcondition expression of $S$ is modified to include expressions of the form $F(P) = F(P)'Old$, all anded with each other and any explicit class-wide postcondition expression, with one such equality included for each class-wide stable property function $F$ of $S$ for type $T$ that does not occur in any class-wide postcondition expression that applies to $S$, and $P$ is each parameter of $S$ that has type $T$ and is not excluded from stable property checks. The resulting class-wide postcondition expression of $S$ is used in place of the explicit class-wide postcondition expression of $S$ [when interpreting the meaning of the postcondition as defined in 6.1.1].

**Reason:** We suppress stable property expressions if the property function appears in the explicit class-wide postcondition, or in any inherited class-wide postconditions. If we didn't do that, we could have conflicting requirements in an inherited postcondition and the current one. We also avoid redundant property checks.

**Ramification:** The resulting class-wide postcondition is evaluated as described in 6.1.1. In particular, the enhanced class-wide postcondition is the class-wide postcondition for $S$, and therefore inherited postconditions include any stable property expressions for $S$. 

---

435  16 October 2023  Stable Properties of a Type 7.3.4
In the case of a derived type \( T \), when the preceding rules refer to “every primitive subprogram \( S \) of a type \( T \),” the referenced set of subprograms includes any inherited subprograms.

The equality operation that is used in the aforementioned equality expressions is as described in the case of an individual membership test whose membership choice is a choice simple expression (see 4.5.2).

The Post expression additions described above are enabled or disabled depending on the Post assertion policy that is in effect at the point of declaration of the subprogram \( S \). A similar rule applies to the Post'Class expression additions.

NOTE For an example of the use of these aspects, see the Vector container definition in A.18.2.

These aspects are new.

### 7.4 Deferred Constants

Deferred constant declarations may be used to declare constants in the visible part of a package, but with the value of the constant given in the private part. They may also be used to declare constants imported from other languages (see Annex B).

**Legality Rules**

A deferred constant declaration is an object declaration with the reserved word constant but no initialization expression.] The constant declared by a deferred constant declaration is called a deferred constant. [Unless the Import aspect (see B.1) is True for a deferred constant declaration, the deferred constant declaration requires a completion, which shall be a full constant declaration (called the full declaration of the deferred constant), or a pragma Import (see Annex B).

Proof: The first sentence is redundant, as it is stated officially in 3.3.1.

A deferred constant declaration that is completed by a full constant declaration shall occur immediately within the visible part of a package specification. For this case, the following additional rules apply to the corresponding full declaration:

- The full declaration shall occur immediately within the private part of the same package;
- The deferred and full constants shall have the same type, or shall have statically matching anonymous access subtypes;
- If the deferred constant declaration includes a subtype defined by the subtype indication that defines an un constrained subtype, then the constraint defined by the subtype indication in the full declaration shall match the constraint defined by \( S \) statically.[ On the other hand, if the subtype of the deferred constant is unconstrained, then the full declaration is still allowed to impose a constraint. The constant itself will be constrained, like all constants;]
- If the deferred constant declaration includes the reserved word aliased, then the full declaration shall also.

Ramification: This implies that both the deferred declaration and the full declaration have to have a subtype indication or access definition rather than an array type definition, because each array type definition would define a new type.

If the deferred constant declaration includes a subtype defined by the subtype indication that defines an constrained subtype, then the constraint defined by the subtype indication in the full declaration shall match the constraint defined by \( S \) statically.[ On the other hand, if the subtype of the deferred constant is unconstrained, then the full declaration is still allowed to impose a constraint. The constant itself will be constrained, like all constants;]
If the subtype of the deferred constant declaration excludes null, the subtype of the full declaration shall also exclude null.

Ramification: On the other hand, the full constant can exclude null even if the deferred constant does not. But that can only happen for a subtype_indication, as anonymous access types are required to statically match (which includes any null_exclusion).

A deferred constant declaration for which the completion is completed by a pragma Import aspect is True cannot appear anywhere that an object_declaration is allowed in the visible part of a package_specification, and has no full constant declaration.

The completion of a deferred constant declaration shall occur before the constant is frozen (see 13.147.4).

Dynamic Semantics

The elaboration of a deferred constant declaration elaborates the subtype_indication, access_definition, or (only allowed in the case of an imported constant) the array_type_definition.

Ramification: For nonimported constants, these elaborations cannot require any code or checks for a legal program, because the given subtype_indication has to be indefinite or statically match that of the full constant, meaning that either it is a subtype_mark or it has static constraints. If the deferred constant instead has an access_definition, the designated subtype must be a subtype_mark. We still say that these are elaborated, however, because part of elaboration is creating the type, which is clearly needed for access_definitions. (A deferred constant and its full constant have different types when they are specified by an access_definition, although there is no visible effect of these types being different as neither can be named.)

NOTE The full constant declaration for a deferred constant that is of a given private type or private extension is not allowed before the corresponding full_type_declaration. This is a consequence of the freezing rules for types (see 13.14).

Examples of deferred constant declarations:

Null_Key : constant Key; -- see 7.3.1

CPU_Identifier : constant String(1..8);
with pragma Import => True, Convention => (Assembler, CPU_Identifier => "CPU_ID"); -- see B.1

Extensions to Ada 83

In Ada 83, a deferred constant is required to be of a private type declared in the same visible part. This restriction is removed for Ada 95; deferred constants can be of any type.

In Ada 83, a deferred constant declaration was not permitted to include a constraint, nor the reserved word aliased.

In Ada 83, the rules required conformance of type marks; here we require static matching of subtypes if the deferred constant is constrained.

A deferred constant declaration can be completed with a pragma Import. Such a deferred constant declaration need not be within a package_specification.

The rules for too-early uses of deferred constants are modified in Ada 95 to allow more cases, and catch all errors at compile time. This change is necessary in order to allow deferred constants of a tagged type without violating the principle that for a dispatching call, there is always an implementation to dispatch to. It has the beneficial side effect of catching some Ada-83-erroneous programs at compile time. The new rule fits in well with the new freezing-point rules. Furthermore, we are trying to convert undefined-value problems into bounded errors, and we were having trouble for the case of deferred constants. Furthermore, uninitialized deferred constants cause trouble for the shared variable / tasking rules, since they are really variable, even though they purport to be constant. In Ada 95, they cannot be touched until they become constant.
Note that we do not consider this change to be an upward incompatibility, because it merely changes an erroneous execution in Ada 83 into a compile-time error.

The Ada 83 semantics are unclear in the case where the full view turns out to be an access type. It is a goal of the language design to prevent uninitialized access objects. One wonders if the implementation is required to initialize the deferred constant to null, and then initialize it (again!) to its real value. In Ada 95, the problem goes away.

Wording Changes from Ada 83

Since deferred constants can now be of a nonprivate type, we have made this a stand-alone subclause, rather than a subclause of 7.3, “Private Types and Private Extensions”.

Deferred constant declarations used to have their own syntax, but now they are simply a special case of object_declarations.

Extensions to Ada 95

Deferred constants were enhanced to allow the use of anonymous access types in them.

Wording Changes from Ada 95

Added matching rules for subtypes that exclude null.

Wording Changes from Ada 2005

Correction: Corrected rules so that the intent that a full constant may have a null exclusion even if the deferred constant does not is actually met.

7.5 Limited Types

[A limited type is (a view of) a type for which copying (such as for an assignment_statement) the assignment operation is not allowed. A nonlimited type is a (view of a) type for which copying the assignment operation is allowed.]

Discussion: The concept of the value of a limited type is difficult to define, since the abstract value of a limited type often extends beyond its physical representation. In some sense, values of a limited type cannot be divorced from their object. The value is the object.

In Ada 83, in the two places where limited types were defined by the language, namely tasks and files, an implicit level of indirection was implied by the semantics to avoid the separation of the value from an associated object. In Ada 95, most limited types are passed by reference, and even return-ed by reference. In Ada 2005, most limited types are built-in-place upon return, rather than returned by reference. Thus the object “identity” is part of the logical value of most limited types.

To be honest: For a limited partial view whose full view is nonlimited, copying is possible on parameter passing and function return. To prevent any copying whatsoever, one should make both the partial and full views limited.

Term entry: limited type — type for which copying (such as in an assignment_statement) is not allowed
Note: All types are either limited types or nonlimited types.

Term entry: nonlimited type — type for which copying is allowed

Legality Rules

If a tagged record type has any limited components, then the reserved word limited shall appear in its record_type_definition. [If the reserved word limited appears in the definition of a derived_type_definition, its parent type and any progenitor interfaces shall be limited.]

Proof: The rule about the parent type being required to be limited can be found in 3.4. Rules about progenitor interfaces can be found in 3.9.4. Specifically, a nonlimited interface can appear only on a nonlimited type. We repeat these rules here to gather these scattered rules in one obvious place.

Reason: This prevents tagged limited types from becoming nonlimited. Otherwise, the following could happen:
package P is
  type T is limited private;
  type R is tagged record -- Illegal!
    X : T;
  end record;
private
  type T is new Integer; -- R becomes nonlimited here.
end P;
package Q is
  type R2(Access_Discrim : access ...) is new R with
  record
    Y : Some_Task_Type;
  end record;
end Q;

{AI95-00230-01} If the above were legal, then assignment would be defined
for R'Class in the body of P, which is bad news, given the access
discriminant and the task.

{AI95-00287-01} {AI95-00318-02} {AI05-0147-1} {AI12-0236-1} {AI12-0317-1} In the
following contexts, an expression of a limited type is not permitted only if
each of its operative constituents is newly constructed (see 4.4) unless it is an
aggregate, a function_call, or a parenthesized_expression or qualified_expression
whose operand is permitted by this rule, or a conditional_expression all of whose
dependent_expressions are permitted by this rule:

- the initialization expression of an object_declaration (see 3.3.1)
- the default_expression of a component_declaration (see 3.8)
- the expression of a record_component_association (see 4.3.1)
- the expression for an ancestor_part of an extension_aggregate (see 4.3.2)
- an expression of a positional_array_aggregate or the expression of an
  array_component_association (see 4.3.3)
- the base_expression of a record_delta_aggregate (see 4.3.4)

{AI12-0127-1} The base_expression of a record_delta_aggregate (see 4.3.4)

Ramification: {AI12-0127-1} We don't need to mention the base_expression of
an array_delta_aggregate here, as its type cannot be limited (see 4.3.4), and thus
neither can its base_expression. Similarly, we do not need any rules for
components of a delta_aggregate nor the elements of a container_aggregate, as
neither are allowed to be limited (see 4.3.4 and 4.3.5)

- the qualified_expression of an initialized allocator (see 4.8)
- the expression of a return_statement (see 6.5)
- the return_expression of an expression function_declaration (see 6.8)
- the default_expression or actual parameter for a formal object of mode in
  (see 12.4)

Discussion: All of these contexts normally require copying; by restricting the uses as above,
we can require the new object to be built-in-place.

Static Semantics

{AI95-00419-01} {AI05-0178-1} A view of a type is limited if it is a descendant of one of the
following:

- a type with the reserved word limited, synchronized, task, or protected
  in its definition;

Ramification: Note that there is always a “definition”, conceptually, even if there is no
syntactic category called “...definition”.

{AI95-00419-01} This includes interfaces of the above kinds, derived types with the reserved word limited, as well as
task and protected types.

- a class-wide type whose specific type is limited;

This paragraph was deleted: a task or protected type;
• \{AI95-00419-01\} a composite type with a limited component.
• \{AI05-0178-1\} an incomplete view;
• \{AI95-00419-01\} a derived type whose parent is limited and is not an interface.

**Ramification:** \{AI95-00419-01\} Limitedness is not inherited from interfaces; it must be explicitly specified when the parent is an interface.

**To be honest:** \{AI95-00419-01\} A derived type can become nonlimited if **limited** does not appear and the derivation takes place in the visible part of a child package, and the parent type is nonlimited as viewed from the private part or body of the child package.

**Reason:** \{AI95-00419-01\} We considered a rule where limitedness was always inherited from the parent for derived types, but in the case of a type whose parent is an interface, this meant that the first interface is treated differently than other interfaces. It also would have forced users to declare dummy nonlimited interfaces just to get the limitedness right. We also considered a syntax like **not limited** to specify nonlimitedness when the parent was limited, but that was unsavory. The rule given is more uniform and simpler to understand.

\{AI95-00419-01\} The rules for interfaces are asymmetrical, but the language is not: if the parent interface is limited, the presence of the word **limited** determines the limitedness, and nonlimited progenitors are illegal by the rules in 3.9.4 if **limited** is present. If the parent interface is nonlimited, the word **limited** is illegal by the rules in 3.4. The net effect is that the order of the interfaces doesn't matter.

Otherwise, the type is nonlimited.

\[There are no predefined equality operators for a limited type.\]

\{AI05-0052-1\} A type is **immutably limited** if it is one of the following:

• An explicitly limited record type;
• \{AI05-0217-1\} A record extension with the reserved word **limited**;
• A nonformal limited private type that is tagged or has at least one access discriminant with a **default expression**;
• A task type, a protected type, or a synchronized interface;
• A type derived from an immutably limited type.

**Discussion:** An immutably limited type is a type that cannot become nonlimited subsequently in a private part or in a child unit. If a view of the type makes it immutably limited, then no copying (assignment) operations are ever available for objects of the type. This allows other properties; for instance, it is safe for such objects to have access discriminants that have defaults or designate other limited objects.

**Ramification:** A nonsynchronized limited interface type is not immutably limited; a type derived from it can be nonlimited.

\{AI05-0052-1\} A descendant of a generic formal limited private type is presumed to be immutably limited except within the body of a generic unit or a body declared within the declarative region of a generic unit, if the formal type is declared within the formal part of the generic unit.

**Ramification:** In an instance, a type is descended from the actual type corresponding to the formal, and all rules are rechecked in the specification. Bodies are excepted so that we assume the worst there; the complex wording is required to handle children of generics and unrelated bodies properly.

**Implementation Requirements**

\{AI95-00287-01\} \{AI95-00318-02\} \{AI05-0067-1\} For an aggregate of a limited type used to initialize an object as allowed above, the implementation shall not create a separate anonymous object for the aggregate. For a function call of a type with a part that is of a task, protected, or explicitly limited record type that is used to initialize an object as allowed above, the implementation shall not create a separate return object (see 6.5) for the function call. The aggregate or function call shall be constructed directly in the new object.
Discussion: {AI95-00318-02} {AI05-0067-1} For a function_call, we only require build-in-place for a limited type that would have been a return-by-reference type in Ada 95. We do this because we want to minimize disruption to Ada 95 implementations and users.

NOTE 1 {AI95-00287-01} {AI95-00318-02} {AI05-0067-1} While it is allowed to write initializations of limited objects, such initializations never copy a limited object. The source of such an assignment operation will be an aggregate or function call, and such aggregates and function calls will be built directly in the target object (see 7.6). The following are consequences of the rules for limited types:

To be honest: This isn't quite true if the type can become nonlimited (see below); function calls only are required to be build-in-place for “really” limited types.

Paragraphs 10 through 15 were deleted.

• {AI95-00287-01} An initialization expression is not allowed in an object_declaration if the type of the object is limited.
• {AI95-00287-01} A default expression is not allowed in a component_declaration if the type of the record component is limited.
• {AI95-00287-01} An initialized allocator is not allowed if the designated type is limited.
• {AI95-00287-01} A generic formal parameter of mode in must not be of a limited type.

NOTE 2 {AI95-00287-01} Aggregates are not available for a limited composite type. Concatenation is not available for a limited array type.

NOTE 3 {AI95-00287-01} The rules do not exclude a default_expression for a formal parameter of a limited type; they do not exclude a deferred constant of a limited type if the full declaration of the constant is of a nonlimited type.

NOTE 4 As illustrated in 7.3.1, an untagged limited type can become nonlimited under certain circumstances.

Ramification: Limited private types do not become nonlimited; instead, their full view can be nonlimited, which has a similar effect.

It is important to remember that a single nonprivate type can be both limited and nonlimited in different parts of its scope. In other words, “limited” is a property that depends on where you are in the scope of the type. We don't call this a “view property” because there is no particular declaration to declare the nonlimited view.

Tagged types never become nonlimited.

Examples

Example of a package with a limited type:

```ada
package IO_Package is
type File_Name is limited private;
procedure Open (F : in out File_Name);
procedure Close(F : in out File_Name);
procedure Read (F : in File_Name; Item : out Integer);
procedure Write(F : in File_Name; Item : in Integer);
private
  type File_Name is
    limited record
      Internal_Name : Integer := 0;
    end record;
end IO_Package;

package body IO_Package is
  Limit : constant := 200;
  type File_Descriptor is record ... end record;
  Directory : array (1 .. Limit) of File_Descriptor;
  ...procedure Open (F : in out File_Name) is ... end;
  procedure Close(F : in out File_Name) is ... end;
  procedure Read (F : in File_Name; Item : out Integer) is ... end;
  procedure Write(F : in File_Name; Item : in Integer) is ... end;
begin
  ...
end IO_Package;
```

{AI12-0440-1} {AI12-0452-1} In the example, an outside subprogram making use of IO Package cannot obtain a file name by calling Open and later use it in calls to Read and Write. Thus, outside the
package, a file name obtained from Open acts as a kind of password; its internal properties (such as containing a numeric value) are not known and no other operations (such as addition or comparison of internal names) can be performed on a file name. Most importantly, clients of the package cannot make copies of objects of type File_Name.

This example is characteristic of any case where complete control over the operations of a type is desired. Such packages serve a dual purpose. They prevent a user from making use of the internal structure of the type. They also implement the notion of an encapsulated data type where the only operations on the type are those given in the package specification.

The fact that the full view of File_Name is explicitly declared limited means that parameter passing will always be by reference and function results will always be built directly in the result object (see 6.2 and 6.5).

NOTE 5 Notes on the example: In the example above, an outside subprogram making use of IO_Package may obtain a file name by calling Open and later use it in calls to Read and Write. Thus, outside the package, a file name obtained from Open acts as a kind of password; its internal properties (such as containing a numeric value) are not known and no other operations (such as addition or comparison of internal names) can be performed on a file name. Most importantly, clients of the package cannot make copies of objects of type File_Name.

This example is characteristic of any case where complete control over the operations of a type is desired. Such packages serve a dual purpose. They prevent a user from making use of the internal structure of the type. They also implement the notion of an encapsulated data type where the only operations on the type are those given in the package specification.

The fact that the full view of File_Name is explicitly declared limited means that parameter passing and function return will always be by reference and function results will always be built directly in the result object (see 6.2 and 6.5).

Extensions to Ada 83
The restrictions in RM83-7.4.4(4), which disallowed out parameters of limited types in certain cases, are removed.

Wording Changes from Ada 83
Since limitedness and privativeness are orthogonal in Ada 95 (and to some extent in Ada 83), this is now its own subclause rather than being a subclause of 7.3, “Private Types and Private Extensions”.

Extensions to Ada 95
Limited types now have an assignment operation, but its use is restricted such that all uses are build-in-place. This is accomplished by restricting uses to aggregates and function calls. Aggregates were not allowed to have a limited type in Ada 95, which causes a compatibility issue discussed in 4.3, “Aggregates”. Compatibility issues with return statements for limited function calls are discussed in 6.5, “Return Statements”.

Wording Changes from Ada 95
Rewrote the definition of limited to ensure that interfaces are covered, but that limitedness is not inherited from interfaces. Derived types that explicitly include limited are now also covered.

Wording Changes from Ada 2005
Correction: Added a definition for immutably limited types, so that the fairly complex definition does not need to be repeated in rules elsewhere in the Reference Manual.
Correction: The built-in-place rules are consolidated in 7.6, and thus they are removed from this subclause.
Correction: Fixed an oversight: class-wide types were never defined to be limited, even if their associated specific type is. It is thought that this oversight was never implemented incorrectly by any compiler, thus we have not classified it as an incompatibility.
Allowed conditional expressions in limited constructor contexts — we want to treat these as closely to parentheses as possible.
Added wording so that expression functions can return limited entities.
7.6 Assignment and Finalization

User-Defined Assignment and Finalization

Three kinds of actions are fundamental to the manipulation of objects: initialization, finalization, and assignment. Every object is initialized, either explicitly or by default, after being created (for example, by an object_declaration or allocator). Every object is finalized before being destroyed (for example, by leaving a subprogram_body containing an object_declaration, or by a call to an instance of Unchecked_Deallocation). An assignment operation is used as part of assignment_statements, explicit initialization, parameter passing, and other operations.

Default definitions for these three fundamental operations are provided by the language, but a controlled type gives the user additional control over parts of these operations. In particular, the user can define, for a controlled type, an Initialize procedure which is invoked immediately after the normal default initialization of a controlled object, a Finalize procedure which is invoked immediately before finalization of any of the components of a controlled object, and an Adjust procedure which is invoked as the last step of an assignment to a (nonlimited) controlled object.

Term entry: controlled type — type that supports user-defined assignment and finalization

Note: Objects are always finalized before being destroyed.

Ramification: {AI95-00114-01} {AI95-00287-01} Here's the basic idea of initialization, value adjustment, and finalization, whether or not user defined: When an object is created, if it is explicitly assigned an initial value, the object is either built-in-place from an aggregate or function call (in which case neither Adjust nor Initialize is applied), or the assignment copies and adjusts the initial value. Otherwise, Initialize is applied to it (except in the case of an aggregate as a whole). An assignment_statement finalizes the target before copying in and adjusting the new value. Whenever an object goes away, it is finalized. Calls on Initialize and Adjust happen bottom-up; that is, components first, followed by the containing object. Calls on Finalize happen top-down; that is, first the containing object, and then its components. These ordering rules ensure that any components will be in a well-defined state when Initialize, Adjust, or Finalize is applied to the containing object.

Static Semantics

The following language-defined library package exists:

```ada
package Ada.Finalization is
  with Pure, Nonblocking => False
  pragma Pure, Preelaborate(Finalization);
  pragma Remote_Types(Finalization);
  type Controlled is abstract tagged private
    withpragma Preelaborable_Initialization(Controlled);
  type Limited_Controlled is abstract tagged limited private
    withpragma Preelaborable_Initialization(Limited_Controlled);

  procedure Initialize (Object : in out Controlled) is null;
  procedure Adjust     (Object : in out Controlled) is null;
  procedure Finalize   (Object : in out Controlled) is null;
end Ada.Finalization;
```

Correction: Added incomplete views to the list of reasons for a view of a type to be limited. This is not a change as the definition already was in 3.10.1. But it is much better to have all of the reasons for limitedness together.

Correction: A raise_expression can be used in an expression used in a limited context. This is harmless (no object will be created if an exception is raised instead), useful, and thus appears to have been an omission when raise_expressions were added to the language.

Correction: Added the base_expression of a delta_aggregate as a limited context.
procedure Initialize (Object : in out Limited_Controlled) is
  null;
procedure Finalize   (Object : in out Limited_Controlled) is null;
private
  ... -- not specified by the language
end Ada.Finalization;

Reason: [AI12-0241-1] This package must allow blocking (Nonblocking => False) for compatibility. The purpose of this package is to provide a template for overriding user-defined routines; and such routines can only allow blocking if the root type does so. Users can still declare their overriding routines nonblocking if they wish.

A controlled type is a descendant of Controlled or Limited_Controlled. The (default) implementations of Initialize, Adjust, and Finalize have no effect. The predefined "=" operator of type Controlled always returns True, [since this operator is incorporated into the implementation of the predefined equality operator of types derived from Controlled, as explained in 4.5.2.] The type Limited_Controlled is like Controlled, except that it is limited and it lacks the primitive subprogram Adjust.

Discussion: We say “nonlimited controlled type” (rather than just “controlled type”;) when we want to talk about descendents of Controlled only.

Reason: We considered making Adjust and Finalize abstract. However, a reasonable coding convention is e.g. for Finalize to always call the parent's Finalize after doing whatever work is needed for the extension part. (Unlike CLOS, we have no way to do that automatically in Ada 95.) For this to work, Finalize cannot be abstract. In a generic unit, for a generic formal abstract derived type whose ancestor is Controlled or Limited_Controlled, calling the ancestor's Finalize would be illegal if it were abstract, even though the actual type might have a concrete version.

Types Controlled and Limited_Controlled are abstract, even though they have no abstract primitive subprograms. It is not clear that they need to be abstract, but there seems to be no harm in it, and it might make an implementation's life easier to know that there are no objects of these types — in case the implementation wishes to make them “magic” in some way.

For Ada 2005, we considered making these types interfaces. That would have the advantage of allowing them to be added to existing trees. But that was rejected both because it would cause massive disruptions to existing implementations, and because it would be very incompatible due to the "no hidden interfaces" rule. The latter rule would prevent a tagged private type from being completed with a derivation from Controlled or Limited_Controlled — a very common idiom.

A type is said to need finalization if:

• it is a controlled type, a task type or a protected type; or
• it has a component whose type that needs finalization; or
• it is a class-wide type; or it is a limited type that has an access discriminant whose designated type needs finalization; or
• it is a partial view whose full view needs finalization; or
• it is one of a number of language-defined types that are explicitly defined to need finalization.

Ramification: The fact that a type needs finalization does not require it to be implemented with a controlled type. It just has to be recognized by the No_Nested_Finalization restriction.

This property is defined for the type, not for a particular view. That's necessary as restrictions look in private parts to enforce their restrictions; the point is to eliminate all controlled parts, not just ones that are visible.

Dynamic Semantics

During the elaboration or evaluation of a construct that causes an object to be initialized by default of an object declaration, for every controlled subcomponent of the object that is not assigned an initial value (as defined in 3.3.1), Initialize is called on that subcomponent. Similarly, if the object that is initialized by default as a whole is controlled and is not assigned an initial value, Initialize is called on the object. The same applies to the evaluation of an allocator, as explained in 4.8.
called, or its initial value is assigned, as appropriate. Initialize is called on all controlled subcomponents of the ancestor part; if the type of the ancestor part is itself controlled subtype, the Initialize procedure of the ancestor type is called, unless that Initialize procedure is abstract.

Discussion: Example:

```ada
type T1 is new Controlled with record
    ... -- some components might have defaults
end record;

type T2 is new Controlled with record
    X : T1; -- no default
    Y : T1 := ...; -- default
end record;

A : T2;
B : T2 := ...
```

As part of the elaboration of A's declaration, A.Y is assigned a value; therefore Initialize is not applied to A.Y. Instead, Adjust is applied to A.Y as part of the assignment operation. Initialize is applied to A.X and to A, since those objects are not assigned an initial value. The assignment to A.Y is not considered an assignment to A.

For the elaboration of B's declaration, Initialize is not called at all. Instead the assignment adjusts B's value; that is, it applies Adjust to B.X, B.Y, and B.

{8652/0021} {AI95-00182-01} {AI95-00373-01} The ancestor part of an extension aggregate, <> in aggregates, and the return object of an extended_return_statement are handled similarly.

Initialize and other initialization operations are done in an arbitrary order, except as follows. Initialize is applied to an object after initialization of its subcomponents, if any [(including both implicit initialization and Initialize calls)]. If an object has a component with an access discriminant constrained by a per-object expression, Initialize is applied to this component after any components that do not have such discriminants. For an object with several components with such a discriminant, Initialize is applied to them in order of their component declarations. For an allocator, any task activations follow all calls on Initialize.

Reason: The fact that Initialize is done for subcomponents first allows Initialize for a composite object to refer to its subcomponents knowing they have been properly initialized.

The fact that Initialize is done for components with access discriminants after other components allows the Initialize operation for a component with a self-referential access discriminant to assume that other components of the enclosing object have already been properly initialized. For multiple such components, it allows some predictability.

When a target object with any controlled parts is assigned a value, [either when created or in a subsequent assignment_statement,] the assignment operation proceeds as follows:

- The value of the target becomes the assigned value.
- The value of the target is adjusted.

Ramification: If any parts of the object are controlled, abort is deferred during the assignment operation.

{AI05-0067-1} To adjust the value of a [(nonlimited)] composite object, the values of the components of the object are first adjusted in an arbitrary order, and then, if the object is nonlimited controlled, Adjust is called. Adjusting the value of an elementary object has no effect[, nor does adjusting the value of a composite object with no controlled parts.]

Ramification: {AI05-0067-1} Adjustment is never actually performed for values of an immutably_a_by-reference limited type, since all assignment operations for such types are required to be built-in-place. Even so, we still define adjustment for all types in order that the canonical semantics is well-defined; these types do not support copying.

Reason: {AI05-0005-1} The verbiage in the Initialize rule about access discriminants constrained by per-object expressions is not necessary here, since such types are either limited or do not have defaults, so the discriminant can only be changed by an assignment to an outer object. Such an assignment could happen only before any adjustments or (if part of an outer Adjust) only after any inner (component) adjustments have completed, and therefore are never adjusted.
For an assignment statement, after the name and expression have been evaluated, and any conversion (including constraint checking) has been done, an anonymous object is created, and the value is assigned into it; that is, the assignment operation is applied. The target of the assignment statement is then finalized. The value of the anonymous object is then assigned into the target of the assignment statement. Finally, the anonymous object is finalized. [As explained below, the implementation may eliminate the intermediate anonymous object, so this description subsumes the one given in 5.2, “Assignment Statements.”]

Reason: An alternative design for user-defined assignment might involve an Assign operation instead of Adjust:

```ada
procedure Assign(Target : in out Controlled; Source : in out Controlled);
```

Or perhaps even a syntax like this:

```ada
procedure "="(Target : in out Controlled; Source : in out Controlled);
```

Assign (or "=") would have the responsibility of doing the copy, as well as whatever else is necessary. This would have the advantage that the Assign operation knows about both the target and the source at the same time — it would be possible to do things like reuse storage belonging to the target, for example, which Adjust cannot do. However, this sort of design would not work in the case of unconstrained discriminated variables, because there is no way to change the discriminants individually. For example:

```ada
type Mutable(D : Integer := 0) is
  record
    X : Array_Of_Controlled_Things(1..D);
    case D is
    when 17 => Y : Controlled_Thing;
    when others => null;
    end D;
  end record;
end record;
```

An assignment to an unconstrained variable of type Mutable can cause some of the components of X, and the component Y, to appear and/or disappear. There is no way to write the Assign operation to handle this sort of case.

Forbidding such cases is not an option — it would cause generic contract model violations.

Discussion: We say assignment to built-in-place objects does not involve copying, which matches the intended implementation (see below). Of course, the implementation can do any copying it likes, if it can make such copying semantically invisible (by patching up access values to point to the copy, and so forth).

- If the full type of any part of the object is immutably limited, the anonymous object is built in place.

Reason: We talk about the full types being immutably limited, as this is independent of the view of a type (in the same way that it is for determining the technique of parameter passing). That is, privacy is ignored for this purpose.

- In the case of an aggregate, if the full type of any part of the newly-created object is controlled, the anonymous object is built in place.

Reason: This is necessary to prevent elaboration problems with deferred constants of controlled types.
package P is
  type Dyn_String is private;
  Null_String : constant Dyn_String;
...
private
  type Dyn_String is new Ada.Finalization.Controlled with...
  procedure Finalize(X : in out Dyn_String);
  procedure Adjust(X : in out Dyn_String);
  Null_String : constant Dyn_String :=
...(Ada.Finalization.Controlled with ...);
end P;

When Null_String is elaborated, the bodies of Finalize and Adjust clearly have not been elaborated. Without this rule, this declaration would necessarily raise Program_Error (unless the permissions given below are used by the implementation).

Ramification: An aggregate with a controlled part used in the return expression of a simple_return_statement has to be built in place in the anonymous return object, as this is similar to an object declaration. (This is a change from Ada 95, but it is not an inconsistency as it only serves to restrict implementation choices.) But this only covers the aggregate; a separate anonymous return object can still be used unless it too is required to be built in place.

Similarly, an aggregate that has a controlled part but is not itself controlled and that is used to initialize an object also has to be built in place. This is also a change from Ada 95, but it is not an inconsistency as it only serves to restrict implementation choices. This avoids problems if a type like Dyn_String (in the example above) is used as a component in a type used as a deferred constant in package P.

• In other cases, it is unspecified whether the anonymous object is built in place.

Reason: This is left unspecified so the implementation can use any appropriate criteria for determining when to build in place. That includes making the decision on a call-by-call basis. Reasonable programs will not care what decision is made here anyway.

\{AI05-0067-1\} Notwithstanding what this document says elsewhere, if an object is built in place:

• Upon successful completion of the return_statement or aggregate, the anonymous object mutates into the newly-created object; that is, the anonymous object ceases to exist, and the newly-created object appears in its place.

• Finalization is not performed on the anonymous object.

• Adjustment is not performed on the newly-created object.

• All access values that designate parts of the anonymous object now designate the corresponding parts of the newly-created object.

• All renamings of parts of the anonymous object now denote views of the corresponding parts of the newly-created object.

• Coextensions of the anonymous object become coextensions of the newly-created object.

To be honest: \{AI12-0005-1\} This “mutating” does not necessarily happen atomically with respect to abort and other tasks. For example, if a function call is used as the ancestorparent part of an extension_aggregate, then the tag of the anonymous object (the function result) will be different from the tag of the newly-created object (the ancestorparent part of the extension_aggregate). In implementation terms, this involves modifying the tag field. If the current task is aborted during this modification, the object might become abnormal. Likewise, if some other task accesses the tag field during this modification, it constitutes improper use of shared variables, and is erroneous.

Implementation Note: The intended implementation is that the anonymous object is allocated at the same address as the newly-created object. Thus, no run-time action is required to cause all the access values and renamings to point to the right place. They just point to the newly-created object, which is what the return object has magically “mutated into”.

There is no requirement that ′Address of the return object is equal to ′Address of the newly-created object, but that will be true in the intended implementation.

For a function call, if the size of the newly-created object is known at the call site, the object is allocated there, and the address is implicitly passed to the function; the return object is created at that address. Otherwise, a storage pool is implicitly passed to the function; the size is determined at the point of the return statement, and passed to the Allocate procedure. The address returned by the storage pool is returned from the function, and the newly-created object uses
that same address. If the return statement is left without returning (via an exception or a goto, for example), then
Deallocate is called. The storage pool might be a dummy pool that represents “allocate on the stack”.

The Tag of the newly-created object may be different from that of the result object. Likewise, the master and
accessibility level may be different.

An alternative implementation model might allow objects to move around to different addresses. In this case, access
values and renamings would need to be modified at run time. It seems that this model requires the full power of tracing
garbage collection.

Implementation Requirements

{8652/0022} {AI95-00083-01} {AI95-00318-02} {AI05-0067-1} For an aggregate of a controlled type
whose value is assigned, other than by an assignment_statement or a return_statement, the
implementation shall not create a separate anonymous object for the aggregate. The aggregate value
shall be constructed directly in the target of the assignment operation and Adjust is not called on the
target object.

Reason: {AI95-00318-02} {AI05-0067-1} This build-in-place requirement is necessary to prevent elaboration
problems with deferred constants of controlled types. Consider:

package P is
  type Dyn_String is private;
  Null_String : constant Dyn_String;
  private
  type Dyn_String is new Ada.Finalization.Controlled with...
  procedure Finalize(X : in out Dyn_String);
  procedure Adjust(X : in out Dyn_String);
  Null_String : constant Dyn_String :=
      (Ada.Finalization.Controlled with ...);
  and P;
end P;

When Null_String is elaborated, the bodies of Finalize and Adjust clearly have not been elaborated. Without this rule,
this declaration would necessarily raise Program_Error (unless the permissions given below are used by the
implementation).

Ramification: An aggregate of a controlled type used in the return expression of a simple_return_statement has to
be built in place in the anonymous return object, as this is similar to an object declaration. (This is a change from Ada 95,
but it is not an inconsistency as it only serves to restrict implementation choices.) But this only covers the
aggregate; a separate anonymous return object can still be used unless it too is required to be built in place (see 7.5).

Implementation Permissions

{AI05-0067-1} An implementation is allowed to relax the above rules for assignment_statements[[for nonlimited controlled types]] in the following ways:

This paragraph was deleted.

Proof: {AI05-0067-1} The phrase “for nonlimited controlled types” follows from the fact that
all of the following permissions apply to cases involving assignment. It is important because the programmer can count
on a stricter semantics for limited controlled types.

Ramification: {AI05-0067-1} {AI12-0005-1} The relaxations apply only to nonlimited types, as
assignment_statements are not allowed for limited types. This is important so that the programmer can count on a
stricter semantics for limited controlled types.

• {AI05-0067-1} {AI12-0044-1} If for an assignment_statement that assigns to an object is
assigned the value of that same object, the implementation may omit the entire assignment
need not do anything.

Ramification: In other words, even if an object is controlled and a combination of Finalize and Adjust on the object
might have a net side effect, they need not be performed.

• {AI05-0067-1} For assignment of an assignment_statement for a noncontrolled type, the
implementation may finalize and assign each component of the variable separately (rather than
finalizing the entire variable and assigning the entire new value) unless a discriminant of the
variable is changed by the assignment.
Reason: For example, in a slice assignment, an anonymous object is not necessary if the slice is copied component-by-component in the right direction, since array types are not controlled (although their components may be). Note that the direction, and even the fact that it's a slice assignment, can in general be determined only at run time.

Ramification: This potentially breaks a single assignment operation into many, and thus abort deferral (see 9.8) needs to last only across an individual component assignment when the component has a controlled part. It is only important that the copy step is not separated (by an abort) from the adjust step, so aborts between component assignments is not harmful.

- \{AI95-00147-01\} \{AI05-0067-1\} \{AI12-0444-1\} The for an aggregate or function call whose value is assigned into a target object, the implementation need not create a separate anonymous object if it can safely create the value of the aggregate or function call directly in the target object. Similarly, for an assignment statement, the implementation may avoid creating a new anonymous object if the value being assigned is the result of evaluating a name denoting an object (the source object) whose storage cannot overlap with the target. If the source object can overlap with the target object, then the implementation can avoid the need for an intermediary anonymous object by exercising one of the above permissions and perform the assignment one component at a time (for an overlapping array assignment), or not at all (for an assignment where the target and the source of the assignment are the same object).

Even if an anonymous object is created, the implementation may move its value to the target object as part of the assignment without re-adjusting so long as the anonymous object has no aliased subcomponents.

Ramification: If the anonymous object is eliminated by this permission, in the aggregate case, only one value adjustment is necessary, and there is no anonymous object to be finalized and thus the Finalize call on it is eliminated.

Note that if the anonymous object is eliminated but the new value is not built in place in the target object in the function call case, the anonymous object can be eliminated. Note, however, that Adjust must be called in the assignment statement case as well, no finalization of the anonymous object is needed. On the other hand, if the target has aliased subcomponents, then an adjustment takes place directly on the target object as the last step of the assignment, since some of the subcomponents may be self-referential or otherwise position-dependent. This Adjust can be eliminated only by using one of the following permissions.

Furthermore, an implementation is permitted to omit implicit Initialize, Adjust, and Finalize calls and associated assignment operations on an object of a nonlimited controlled type provided that:

- any omitted Initialize call is not a call on a user-defined Initialize procedure, and

  To be honest: This does not apply to any calls to a user-defined Initialize routine that happen to occur in an Adjust or Finalize routine. It is intended that it is never necessary to look inside of an Adjust or Finalize routine to determine if the call can be omitted.

  Reason: We don't want to eliminate objects for which the Initialize might have side effects (such as locking a resource).

- any usage of the value of the object after the implicit Initialize or Adjust call and before any subsequent Finalize call on the object does not change the external effect of the program, and

- after the omission of such calls and operations, any execution of the program that executes an Initialize or Adjust call on an object or initializes an object by an aggregate will also later execute a Finalize call on the object and will always do so prior to assigning a new value to the object, and

- the assignment operations associated with omitted Adjust calls are also omitted.

This permission applies to Adjust and Finalize calls even if the implicit calls have additional external effects.

Reason: The goal of the above permissions is to allow typical dead assignment and dead variable removal algorithms to work for nonlimited controlled types. We require that "pairs" of Initialize/Adjust/Finalize operations are removed. (These aren't always pairs, which is why we talk about "any execution of the program".)
Extensions to Ada 83

Controlled types and user-defined finalization are new to Ada 95. (Ada 83 had finalization semantics only for masters of tasks.)

Extensions to Ada 95

27.a2
\{AI95-00161-01\} \textbf{Amendment Correction:} Types \texttt{Controlled} and \texttt{Limited Controlled} now have Preelaborable Initialization, so that objects of types derived from these types can be used in preelaborated packages.

Wording Changes from Ada 95

27.d/2 \{8652/0020\} \{AI95-00126-01\} \textbf{Corrigendum:} Clarified that Ada.Finalization is a remote types package.

27.e/2 \{8652/0021\} \{AI95-00182-01\} \textbf{Corrigendum:} Added wording to clarify that the default initialization (whatever it is) of an ancestor part is used.

27.f/2 \{8652/0022\} \{AI95-00083-01\} \textbf{Corrigendum:} Clarified that Adjust is never called on an aggregate used for the initialization of an object or subaggregate, or passed as a parameter.

27.g/2 \{AI95-00147-01\} Additional optimizations are allowed for nonlimited controlled types. These allow traditional dead variable elimination to be applied to such types.

27.h/2 \{AI95-00318-02\} Corrected the build-in-place requirement for controlled aggregates to be consistent with the requirements for limited types.

27.i/2 \{AI95-00348-01\} The operations of types \texttt{Controlled} and \texttt{Limited Controlled} are now declared as null procedures (see 6.7) to make the semantics clear (and to provide a good example of what null procedures can be used for).

27.j/2 \{AI95-00360-01\} Types that need finalization are defined; this is used by the No Nested Finalization restriction (see D.7, “Tasking Restrictions”).

27.k/2 \{AI95-00373-01\} Generalized the description of objects that have \texttt{Initialize} called for them to say that it is done for all objects that are initialized by default. This is needed so that all of the new cases are covered.

Extensions to Ada 2005

27.l/3 \{AI05-0212-1\} Package Ada.Finalization now has Pure categorization, so it can be mentioned for any package. Note that this does not change the preelaborability of objects descended from \texttt{Controlled} and \texttt{Limited Controlled}.

Wording Changes from Ada 2005

27.m/3 \{AI05-0013-1\} \textbf{Correction:} Eliminated coextensions from the “needs finalization” rules, as this cannot be determined in general in the compilation unit that declares the type. (The designated type of the coextension may have been imported as a limited view.) Uses of “needs finalization” need to ensure that coextensions are handled by other means (such as in No Nested Finalization – see D.7) or that coextensions cannot happen.

27.n/3 \{AI05-0013-1\} \textbf{Correction:} Corrected the “needs finalization” rules to include class-wide types, as a future extension can include a part that needs finalization.

27.o/3 \{AI05-0026-1\} \textbf{Correction:} Corrected the “needs finalization” rules to clearly say that they ignore privacy.

27.p/3 \{AI05-0067-1\} \textbf{Correction:} Changed “built in place” to Dynamic Semantics and centralized the rules here. This eliminates the fiction that built in place is just a combination of a permission and a requirement; it clearly has noticeable semantic effects. This wording change is not intended to change the semantics of any correct Ada program.

7.6.1 Completion and Finalization

This subclause defines completion and leaving of the execution of constructs and entities. A master is the execution of a construct that includes finalization of local objects after it is complete (and after waiting for any local tasks — see 9.3), but before leaving. Other constructs and entities are left immediately upon completion.

Dynamic Semantics

2/2 \{AI95-00318-02\} The execution of a construct or entity is \textit{complete} when the end of that execution has been reached, or when a transfer of control (see 5.1) causes it to be abandoned. Completion due to reaching the end of execution, or due to the transfer of control of an \texttt{exit statement}, \texttt{return statement}, \texttt{goto statement} \texttt{exit, return, goto}, or \texttt{requeue statement} or of the selection of a
terminate_alternative is normal completion. Completion is abnormal otherwise [— when control is transferred out of a construct due to abort or the raising of an exception].

Discussion: Don't confuse the run-time concept of completion with the compile-time concept of completion defined in 3.11.1.

{AI95-00162-01} {AI95-00416-01} {AI12-0406-1} After execution of a construct or entity is complete, it is left, meaning that execution continues with the next action, as defined for the execution that is taking place. Leaving an execution happens immediately after its completion, except in the case of the execution of a master construct. A master is finalized after it is complete, and before it is left.

Reason: {AI95-00162-01} {AI95-00416-01} Expressions and statements are masters so that objects created by subprogram calls (in aggregates, allocators for anonymous access-to-object types, and so on) are finalized and have their tasks awaited before the expressions or statements are left. Note that expressions like the condition of an if statement are masters, because they are not enclosed by a simple statement. Similarly, a function call which is renamed is a master, as it is not in a simple statement. Note that although an accept_statement has no declarative_part, it can call functions and evaluate aggregates, possibly causing anonymous controlled objects to be created, and we don't want those objects to escape outside the rendezvous.

{AI95-00416-01} We have to include function calls in the contexts that do not cause masters to occur so that expressions contained in a function_call (that is not part of an expression or simple_statement) do not individually become masters. We certainly do not want the parameter expressions of a function_call to be separate masters, as they would then be finalized before the function is called.

Ramification: {AI95-00416-01} The fact that a function_call is a master does not change the accessibility of the return object denoted by the function_call, that depends on the use of the function_call. The function_call is the master of any short-lived entities (such as aggregates used as parameters of types with task or controlled parts).

Term entry: master — execution of a master construct

Note: Each object and task is associated with a master. When a master is left, associated tasks are awaited and associated objects are finalized.

Term entry: master construct — one of certain executable constructs for which there can be objects or tasks whose lifetime ends when the construct completes.

Note: Execution of a master construct is a master, with which objects and tasks are associated for the purposes of waiting and finalization.

For the finalization of a master, dependent tasks are first awaited, as explained in 9.3. Then each object whose accessibility level is the same as that of the master is finalized if the object was successfully initialized and still exists. [These actions are performed whether the master is left by reaching the last statement or via a transfer of control.] When a transfer of control causes completion of an execution, each included master is finalized in order, from innermost outward.

Ramification: As explained in 3.10.2, the set of objects with the same accessibility level as that of the master includes objects declared immediately within the master, objects declared in nested packages, objects created by allocators (if the ultimate ancestor access type is declared in one of those places) and subcomponents of all of these things. If an object was already finalized by Unchecked_Deallocation, then it is not finalized again when the master is left.

Note that any object whose accessibility level is deeper than that of the master would no longer exist; those objects would have been finalized by some inner master. Thus, after leaving a master, the only objects yet to be finalized are those whose accessibility level is less deep than that of the master.

To be honest: Subcomponents of objects due to be finalized are not finalized by the finalization of the master; they are finalized by the finalization of the containing object.

Reason: We need to finalize subcomponents of objects even if the containing object is not going to get finalized because it was not fully initialized. But if the containing object is finalized, we don't want to require repeated finalization of the subcomponents, as might normally be implied by the recursion in finalization of a master and the recursion in finalization of an object.
To be honest: Formally, completion and leaving refer to executions of constructs or entities. However, the standard sometimes (informally) refers to the constructs or entities whose executions are being completed. Thus, for example, “the subprogram call or task is complete” really means “the execution of the subprogram call or task is complete”.

For the finalization of an object:

- **{AI05-0099-1}** If the full type of the object is an elementary type, finalization has no effect;  
  **Reason:** {AI05-0099-1} We say “full type” in this and the following bullets as privacy is ignored for the purpose of determining the finalization actions of an object; that is as expected for Dynamic Semantics rules.

- **{AI05-0099-1}** If the full type of the object is a tagged type, and the tag of the object identifies a controlled type, the Finalize procedure of that controlled type is called;  

- **{AI05-0099-1}** If the full type of the object is a protected type, or if the full type of the object is a tagged type and the tag of the object identifies a protected type, the actions defined in 9.4 are performed;  

- **{AI95-00416-01}** {AI05-0099-1} If the full type of the object is a composite type, then after performing the above actions, if any, every component of the object is finalized in an arbitrary order, except as follows: if the object has a component with an access discriminant constrained by a per-object expression, this component is finalized before any components that do not have such discriminants; for an object with several components with such a discriminant, they are finalized in the reverse of the order of their component declarations.

**Reason:** This allows the finalization of a component with an access discriminant to refer to other components of the enclosing object prior to their being finalized.

**To be honest:** {AI05-0099-1} {AI12-0005-1} The components discussed here are all of the components that the object actually has, not just those components that are statically identified by the type of the object. These can be different if the object has a class-wide class-wide type.

- **{AI95-00416-01}** If the object has coextensions (see 3.10.2), each coextension is finalized after the object whose access discriminant designates it.
  
  **Ramification:** {AI05-0066-1} In the case of an aggregate or function call that is used (in its entirety) to directly initialize a part of an object, the coextensions of the result of evaluating the aggregate or function call are transferred to become coextensions of the object being initialized and are not finalized until the object being initialized is ultimately finalized, even if an anonymous object is created as part of the operation.

Immediately before an instance of Unchecked_Deallocation reclaims the storage of an object, the object is finalized. [If an instance of Unchecked_Deallocation is never applied to an object created by an allocator, the object will still exist when the corresponding master completes, and it will be finalized then.]

**{AI95-00280-01}** {AI05-0051-1} {AI05-0190-1} The order in which the finalization of a master performs finalization of objects is as follows: Objects created by declarations in the master are finalized in the reverse order of their creation. For objects that were created by allocators for an access type whose ultimate ancestor is declared in the master, this rule is applied as though each such object that still exists had been created in an arbitrary order at the first freezing point (see 13.14) of the ultimate ancestor type; the finalization of these objects is called the finalization of the collection. Objects created by allocators for an anonymous access type that are not coextensions of some other object, are finalized in an arbitrary order during the finalization of their associated master. After the finalization of a master is complete, the objects finalized as part of its finalization cease to exist, as do any types and subtypes defined and created within the master.

This paragraph was deleted. **Reason:** {AI05-0190-1} Note that we talk about the type of the allocator here. There may be access values of a (general) access type pointing at objects created by allocators for some other type; these are not finalized at this point.

This paragraph was deleted. **Reason:** {AI05-0190-1} The freezing point of the ultimate ancestor access type is chosen because before that point, pool elements cannot be created, and after that point, access values designating (parts of) the pool elements can be created. This is also the point after which the pool object cannot have been declared. We don’t want to finalize the pool elements until after anything finalizing objects that contain access values designating them. Nor do we want to finalize pool elements after finalizing the pool object itself.
This paragraph was deleted. Ramification: [AI05-0190-1] Finalization of allocated objects is done according to the (ultimate ancestor) allocator type, not according to the storage pool in which they are allocated. Pool finalization might reclaim storage (see 13.11, “Storage Management”), but has nothing (directly) to do with finalization of the pool elements.

This paragraph was deleted. [AI05-0190-1] Note that finalization is done only for objects that still exist; if an instance of Unchecked_Deallocation has already gotten rid of a given pool element, that pool element will not be finalized when the master is left.

Note that a deferred constant declaration does not create the constant; the full constant declaration creates it. Therefore, the order of finalization depends on where the full constant declaration occurs, not the deferred constant declaration.

An imported object is not created by its declaration. It is neither initialized nor finalized.

Implementation Note: An implementation has to ensure that the storage for an object is not reclaimed when references to the object are still possible (unless, of course, the user explicitly requests reclamation via an instance of Unchecked_Deallocation). This implies, in general, that objects cannot be deallocated one by one as they are finalized; a subsequent finalization might reference an object that has been finalized, and that object had better be in its (well-defined) finalized state.

{AI05-0190-1} Each nonderived access type T has an associated collection, which is the set of objects created by allocators of T, or of types derived from T. Unchecked_Deallocation removes an object from its collection. Finalization of a collection consists of finalization of each object in the collection, in an arbitrary order. The collection of an access type is an object implicitly declared at the following place:

Ramification: [AI05-0190-1] The place of the implicit declaration determines when allocated objects are finalized. For multiple collections declared at the same place, we do not define the order of their implicit declarations.

{AI05-0190-1} Finalization of allocated objects is done according to the (ultimate ancestor) allocator type, not according to the storage pool in which they are allocated. Pool finalization might reclaim storage (see 13.11, “Storage Management”), but has nothing (directly) to do with finalization of the pool elements.

{AI05-0190-1} Note that finalization is done only for objects that still exist; if an instance of Unchecked_Deallocation has already gotten rid of a given pool element, that pool element will not be finalized when the master is left.

Reason: [AI05-0190-1] Note that we talk about the type of the allocator here. There may be access values of a (general) access type pointing at objects created by allocators for some other type; these are not (necessarily) finalized at this point.

- For a named access type, the first freezing point (see 13.14) of the type.
  
  Reason: [AI05-0190-1] The freezing point of the ultimate ancestor access type is chosen because before that point, pool elements cannot be created, and after that point, access values designating (parts off) the pool elements can be created. This is also the point after which the pool object cannot have been declared. We don’t want to finalize the pool elements until after anything finalizing objects that contain access values designating them. Nor do we want to finalize pool elements after finalizing the pool object itself.

- For the type of an access parameter, the call that contains the allocator.

- For the type of an access result, within the master of the call (see 3.10.2).

  To be honest: [AI05-0005-1] [AI05-0190-1] We mean at a place within the master consistent with the execution of the call within the master. We don’t say that normatively, as it is difficult to explain that when the master of the call need not be the master that immediately includes the call (such as when an anonymous result is converted to a named access type).

- For any other anonymous access type, the first freezing point of the innermost enclosing declaration.

{AI05-0005-1} The target of an assignment_statement is finalized before copying in the new value, as explained in 7.6.

{AI05-0142-4} {AI05-0066-1} {AI05-0269-1} The master of an object is the master enclosing its creation whose accessibility level (see 3.10.2) is equal to that of the object, except in the case of an anonymous object representing the result of an aggregate or function call. If such an anonymous object is part of the result of evaluating the actual parameter expression for an explicitly aliased parameter of a function call, the master of the object is the innermost master enclosing the evaluation of the aggregate or function call, excluding the aggregate or function
call itself. Otherwise, the master of such an anonymous object is the innermost master enclosing the evaluation of the aggregate or function call, which may be the aggregate or function call itself. If the object name in an object renaming declaration, or the actual parameter for a generic formal in out parameter in a generic instantiation, denotes any part of an anonymous object created by a function call, the anonymous object is not finalized until after it is no longer accessible via any name. Otherwise, anonymous objects created by a function call or calls and by an aggregate are finalized no later than the end of the innermost enclosing declarative item or statement, if that is a compound_statement, the object is finalized before starting the execution of any statement within the compound_statement.

This paragraph was deleted. To be honest: [AI95-00162-01] This is not to be construed as permission to call Finalize asynchronously with respect to normal user code. For example,

```
This paragraph was deleted. declare
   X : Some_Controlled_Type := F(G(....));
   The anonymous objects created for F and G are finalized
   no later than this point.
begin
   ...
end;
```

The anonymous object for G should not be finalized at some random point in the middle of the body of F, because F might manipulate the same data structures as the Finalize operation, resulting in erroneous access to shared variables.

Reason: [AI95-00162-01] This effectively imports all of the special rules for the accessibility level of renames, allocators, and so on, and applies them to determine where objects created in them are finalized. For instance, the master of a rename of a subprogram is that of the renamed subprogram. It might be quite inconvenient for the implementation to defer finalization of the anonymous object for G until after copying the value of F into X, especially if the size of the result is not known at the call site.

In 3.10.2 we assign an accessibility level to the result of an aggregate or function call that is used to directly initialize a part of an object based on the object being initialized. This is important to ensure that any access discriminants denote objects that live at least as long as the object being initialized. However, if the result of the aggregate or function call is not built directly in the target object, but instead is built in an anonymous object that is then assigned to the target, the anonymous object needs to be finalized after the assignment rather than persisting until the target object is finalized (but not its coextensions). (Note than an implementation is never required to create such an anonymous object, and in some cases is required to not have such a separate object, but rather to build the result directly in the target.)

The special case for explicitly aliased parameters of functions is needed for the same reason, as access discriminants of the returned object may designate one of these parameters. In that case, we want to lengthen the lifetime of the anonymous objects as long as the possible lifetime of the result.

We don't do a similar change for other kinds of calls, because the extended lifetime of the parameters adds no value, but could constitute a storage leak. For instance, such an anonymous object created by a procedure call in the elaboration part of a package body would have to live until the end of the program, even though it could not be used after the procedure returns (other than via Unchecked_Access).

Note that the lifetime of the master given to anonymous objects in explicitly aliased parameters of functions is not necessarily as long as the lifetime of the master of the object being initialized (if the function call is used to initialize an allocator, for instance). In that case, the accessibility check on explicitly aliased parameters will necessarily fail if any such anonymous objects exist. This is necessary to avoid requiring the objects to live as long as the access type or having the implementation complexity of an implicit coextension.

In the case of an expression that is a master, finalization of any (anonymous) objects occurs after completing as the final part of evaluation of the expression and all use of the objects, prior to starting the execution of any subsequent construct. If a transfer of control or raising of an exception occurs prior to performing a finalization of an anonymous object, the anonymous object is finalized as part of the finalizations due to be performed for the object's innermost enclosing master.
Bounded (Run-Time) Errors

{8652/0023} \{AI95-00169-01\} It is a bounded error for a call on Finalize or Adjust \textit{that occurs as part of object finalization or assignment} to propagate an exception. The possible consequences depend on what action invoked the Finalize or Adjust operation:

\textbf{Ramification:} It is not a bounded error for Initialize to propagate an exception. If Initialize propagates an exception, then no further calls on Initialize are performed, and those components that have already been initialized (either explicitly or by default) are finalized in the usual way.

{8652/0023} \{AI95-00169-01\} \textbf{It also is not a bounded error for an explicit call to Finalize or Adjust to propagate an exception. We do not want implementations to have to treat explicit calls to these routines specially.}

\begin{itemize}
  \item For a Finalize invoked as part of an assignment\_statement, Program\_Error is raised at that point.
  \item {8652/0024} \{AI95-00193-01\} \{AI95-00256-01\} \{AI12-0445-1\} \textbf{For an Adjust invoked as part of assignment\_operations other than those invoked as part of an assignment\_statement the initialization of a controlled object, some of the other adjustments due to be performed might or might not be performed, and then Program Error is raised. During its propagation, finalization might or might not be applied to objects whose Adjust failed. For an Adjust invoked as part of an assignment\_statement assignment\_statement operation, any other adjustments due to be performed are performed, and then Program\_Error is raised.}
  \begin{itemize}
    \item \textbf{Reason:} {8652/0024} \{AI95-00193-01\} \{AI95-00256-01\} In the case of assignments that are part of initialization, there is no need to complete all adjustments if one propagates an exception, as the object will immediately be finalized. So long as a subcomponent is not going to be finalized, it need not be adjusted, even if it is initialized as part of an enclosing composite assignment operation for which some adjustments are performed. However, there is no harm in an implementation making additional Adjust calls (as long as any additional components that are adjusted are also finalized), so we allow the implementation flexibility here. On the other hand, for an assignment\_statement assignment\_statement operation, it is important that all adjustments be performed, even if one fails, because all controlled subcomponents are going to be finalized. Other kinds of assignment are more like initialization than assignment\_statements, so we include them as well in the permission.
    \item \textbf{Ramification:} {8652/0024} \{AI95-00193-01\} Even if an Adjust invoked as part of the initialization of a controlled object propagates an exception, objects whose initialization (including any Adjust or Initialize calls) successfully completed will be finalized. The permission above only applies to objects whose Adjust failed. Objects for which Adjust was never even invoked must not be finalized.
  \end{itemize}
\end{itemize}

\begin{itemize}
  \item For a Finalize invoked as part of a call on an instance of Unchecked\_Deallocation, any other finalizations due to be performed are performed, and then Program\_Error is raised.
  \begin{itemize}
    \item \textbf{Discussion:} {8652/0104} \{AI95-00179-01\} The standard does not specify if storage is recovered in this case. If storage is not recovered (and the object continues to exist), Finalize may be called on the object again (when the allocator's master is finalized).
    \item \textbf{This paragraph was deleted.}{8652/0023} \{AI95-00169-01\} \{AI05-0064-1\} \textbf{For a Finalize invoked as part of the finalization of the anonymous object created by a function call or aggregate, any other finalizations due to be performed are performed, and then Program Error is raised immediately after leaving the master.}
    \begin{itemize}
      \item \textbf{Discussion:} \{AI05-0064-1\} This rule covers both ordinary objects created by a declaration, and anonymous objects created as part of evaluating an expression. All contexts that create objects that need finalization are defined to be masters.
    \end{itemize}
    \item {8652/0023} \{AI95-00169-01\} \textbf{For a Finalize invoked due to reaching the end of the execution of a master, any other finalizations associated with the master are performed, and Program Error is raised immediately after leaving the master.}
      \begin{itemize}
        \item \textbf{Discussion:} \{AI05-0064-1\} This rule covers both ordinary objects created by a declaration, and anonymous objects created as part of evaluating an expression. All contexts that create objects that need finalization are defined to be masters.
      \end{itemize}
    \item \{AI95-00318-02\} \textbf{For a Finalize invoked by the transfer of control of an exit\_statement, return statement, goto statement, exit\_return, return\_goto, or requeue statement, Program Error is raised no earlier than after the finalization of the master being finalized when the exception occurred, and no later than the point where normal execution would have continued. Any other finalizations due to be performed up to that point are performed before raising Program\_Error.}
  \end{itemize}
\end{itemize}
Ramification: For example, upon leaving a block_statement due to a goto_statement, the Program_Error would be raised at the point of the target statement denoted by the label, or else in some more dynamically nested place, but not so nested as to allow an exception_handler that has visibility upon the finalized object to handle it. For example,

```
procedure Main is
begin
  <<The_Label>>
  Outer_Block_Statement : declare
    X : Some_Controlled_Type;
  begin
    Inner_Block_Statement : declare
      Y : Some_Controlled_Type;
      Z : Some_Controlled_Type;
    begin
      goto The_Label;
      exception
        when Program_Error => ... -- Handler number 1.
      end;
      exception
        when Program_Error => ... -- Handler number 2.
      end;
      exception
        when Program_Error => ... -- Handler number 3.
    end
  end
end Main;
```

\{AI12-0005-1\} The goto_statement will first cause Finalize(Z,Y) to be called. Suppose that Finalize(Z,Y) propagates an exception. Program_Error will be raised after leaving Inner_Block_Statement, but before leaving Main. Thus, handler number 1 cannot handle this Program_Error; it will be handled either by handler number 2 or handler number 3. If it is handled by handler number 2, then Finalize(Y,Z) will be done before executing the handler. If it is handled by handler number 3, then Finalize(Y,Z) and Finalize(X) will both be done before executing the handler.

- For a Finalize invoked by a transfer of control that is due to raising an exception, any other finalizations due to be performed for the same master are performed; Program_Error is raised immediately after leaving the master.

Ramification: {AI12-0005-1} If, in the above example, the goto_statement were replaced by a raise_statement, then the Program_Error would be handled by handler number 2, and Finalize(Y,Z) would be done before executing the handler.

Reason: We considered treating this case in the same way as the others, but that would render certain exception_handlers useless. For example, suppose the only exception_handler is one for others in the main subprogram. If some deeply nested call raises an exception, causing some Finalize operation to be called, which then raises an exception, then normal execution “would have continued” at the beginning of the exception_handler. Raising Program_Error at that point would cause that handler's code to be skipped. One would need two nested exception_handlers to be sure of catching such cases!

On the other hand, the exception_handler for a given master should not be allowed to handle exceptions raised during finalization of that master.

- For a Finalize invoked by a transfer of control due to an abort or selection of a terminate alternative, the exception is ignored; any other finalizations due to be performed are performed.

Ramification: This case includes an asynchronous transfer of control.

To be honest: This violates the general principle that it is always possible for a bounded error to raise Program_Error (see 1.1.5, “Classification of Errors”).

Implementation Permissions

\{AI05-0107-1\} If the execution of an allocator propagates an exception, any parts of the allocated object that were successfully initialized may be finalized as part of the finalization of the innermost master enclosing the allocator.

Reason: This allows deallocating the memory for the allocated object at the innermost master, preventing a storage leak. Otherwise, the object would have to stay around until the finalization of the collection that it belongs to, which could be the entire life of the program if the associated access type is library level.

\{AI05-0111-3\} {AI05-0262-1\} The implementation may finalize objects created by allocators for an access type whose storage pool supports subpools (see 13.11.4) as if the objects were created (in an
arbitrary order) at the point where the storage pool was elaborated instead of at the first freezing point of the access type.

**Ramiﬁcation:** This allows the ﬁnalization of such objects to occur later than they otherwise would, but still as part of the ﬁnalization of the same master. Accessibility rules in 13.11.4 ensure that it is the same master (usually that of the environment task).

**Implementation Note:** {AI12-0005-1} This permission is intended to allow the allocated objects to "belong" to the subpool objects and to allow those objects to be ﬁnalized at the time that the storage pool is ﬁnalized (if they are not ﬁnalized earlier). This is expected to ease implementation, as the remaining yet-to-be-deallocated objects will only need to be accessible at run time from the subpool header and not also from the overall access type collection header. That is, they only need to belong to a single list, rather than to belong to the subpool and not also to the collection.

**NOTE 1** {AI05-0299-1} {AI12-0049-1} The rules of Clause 10 Clause 10 Section 10 imply that immediately prior to partition termination, Finalize operations are applied to library-level controlled objects (including those created by allocators of library-level access types, except those already ﬁnalized). This occurs after waiting for library-level tasks to terminate.

**Discussion:** We considered deﬁning a pragma that would apply to a controlled type that would suppress Finalize operations for library-level objects of the type upon partition termination. This would be useful for types whose ﬁnalization actions consist of simply reclaiming global heap storage, when this is already provided automatically by the environment upon program termination.

**NOTE 2** A constant is only constant between its initialization and ﬁnalization. Both initialization and ﬁnalization are allowed to change the value of a constant.

**NOTE 3** Abort is deferred during certain operations related to controlled types, as explained in 9.8. Those rules prevent an abort from causing a controlled object to be left in an ill-deﬁned state.

**NOTE 4** The Finalize procedure is called upon ﬁnalization of a controlled object, even if Finalize was called earlier, either explicitly or as part of an assignment; hence, if a controlled type is visibly controlled (implying that its Finalize primitive is directly callable), or is nonlimited (implying that assignment is allowed), its Finalize procedure is **ideally should be designed** to have no ill effect if it is applied a second time to the same object.

**Discussion:** Or equivalently, a Finalize procedure should be ‘idempotent’; applying it twice to the same object should be equivalent to applying it once.

**Reason:** A user-written Finalize procedure should be idempotent since it can be called explicitly by a client (at least if the type is "visibly" controlled). Also, Finalize is used implicitly as part of the assignment statement if the type is nonlimited, and an abort is permitted to disrupt an assignment statement between ﬁnalizing the left-hand side and assigning the new value to it (an abort is not permitted to disrupt an assignment operation between copying in the new value and adjusting it).

**Discussion:** {AI95-00287-01} Either Initialize or Adjust, but not both, is applied to (almost) every controlled object when it is created: Initialize is done when no initial value is assigned to the object, whereas Adjust is done as part of assigning the initial value. The one exception is the anonymous object initialized created by an aggregate (both the anonymous object created for an aggregate, or an object initialized by an aggregate that is built-in-place). Initialize is not applied to the aggregate as a whole, nor is the value of the aggregate or object adjusted.

All of the following use the assignment operation, and thus perform value adjustment:

- the assignment_statement (see 5.2);
- explicit initialization of a stand-alone object (see 3.3.1) or of a pool element (see 4.8);
- default initialization of a component of a stand-alone object or pool element (in this case, the value of each component is assigned, and therefore adjusted, but the value of the object as a whole is not adjusted);
- {AI95-00318-02} function return, when the result is not built-in-place type is not a return-by-reference type (see 6.5); (adjustment of the result happens before ﬁnalization of the function; values of return-by-reference types are not adjusted);
- predefined operators (although the only one that matters is concatenation; see 4.5.3);
- generic formal objects of mode in (see 12.4); these are deﬁned in terms of constant declarations; and
- {AI95-00287-01} {AI12-0005-1} aggregates (see 4.3), when the result is not built-in-place (in this case, the value of each component, and the ancestor parent part, for an extension aggregate, is assigned, and therefore adjusted, but the value of the aggregate as a whole is not adjusted; neither is Initialize called);

The following also use the assignment operation, but adjustment never does anything interesting in these cases:

- By-copy parameter passing uses the assignment operation (see 6.4.1), but controlled objects are always passed by reference, so the assignment operation never does anything interesting in this case. If we were to allow by-copy parameter passing for controlled objects, we would need to make sure that the actual is ﬁnalized before doing the copy back for [in] out parameters. The initialization of the parameter itself needs to

<table>
<thead>
<tr>
<th>Page</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.d/3</td>
<td>Ramification: This allows the finalization of such objects to occur later than they otherwise would, but still as part of the finalization of the same master. Accessibility rules in 13.11.4 ensure that it is the same master (usually that of the environment task).</td>
</tr>
<tr>
<td>20.e/5</td>
<td>Implementation Note: {AI12-0005-1} This permission is intended to allow the allocated objects to &quot;belong&quot; to the subpool objects and to allow those objects to be finalized at the time that the storage pool is finalized (if they are not finalized earlier). This is expected to ease implementation, as the remaining yet-to-be-deallocated objects will only need to be accessible at run time from the subpool header and not also from the overall access type collection header. That is, they only need to belong to a single list, rather than to belong to the subpool and not also to the collection.</td>
</tr>
<tr>
<td>21/5</td>
<td>NOTE 1 {AI05-0299-1} {AI12-0049-1} The rules of Clause 10 Clause 10 Section 10 imply that immediately prior to partition termination, Finalize operations are applied to library-level controlled objects (including those created by allocators of library-level access types, except those already finalized). This occurs after waiting for library-level tasks to terminate.</td>
</tr>
<tr>
<td>21.a</td>
<td>Discussion: We considered defining a pragma that would apply to a controlled type that would suppress Finalize operations for library-level objects of the type upon partition termination. This would be useful for types whose finalization actions consist of simply reclaiming global heap storage, when this is already provided automatically by the environment upon program termination.</td>
</tr>
<tr>
<td>22</td>
<td>NOTE 2 A constant is only constant between its initialization and finalization. Both initialization and finalization are allowed to change the value of a constant.</td>
</tr>
<tr>
<td>23</td>
<td>NOTE 3 Abort is deferred during certain operations related to controlled types, as explained in 9.8. Those rules prevent an abort from causing a controlled object to be left in an ill-defined state.</td>
</tr>
<tr>
<td>24</td>
<td>NOTE 4 The Finalize procedure is called upon finalization of a controlled object, even if Finalize was called earlier, either explicitly or as part of an assignment; hence, if a controlled type is visibly controlled (implying that its Finalize primitive is directly callable), or is nonlimited (implying that assignment is allowed), its Finalize procedure is ideally should be designed to have no ill effect if it is applied a second time to the same object.</td>
</tr>
<tr>
<td>24.a</td>
<td>Discussion: Or equivalently, a Finalize procedure should be “idempotent”; applying it twice to the same object should be equivalent to applying it once.</td>
</tr>
<tr>
<td>24.b</td>
<td>Reason: A user-written Finalize procedure should be idempotent since it can be called explicitly by a client (at least if the type is &quot;visibly&quot; controlled). Also, Finalize is used implicitly as part of the assignment statement if the type is nonlimited, and an abort is permitted to disrupt an assignment statement between finalizing the left-hand side and assigning the new value to it (an abort is not permitted to disrupt an assignment operation between copying in the new value and adjusting it).</td>
</tr>
<tr>
<td>24.c/2</td>
<td>Discussion: {AI95-00287-01} Either Initialize or Adjust, but not both, is applied to (almost) every controlled object when it is created: Initialize is done when no initial value is assigned to the object, whereas Adjust is done as part of assigning the initial value. The one exception is the anonymous object initialized created by an aggregate (both the anonymous object created for an aggregate, or an object initialized by an aggregate that is built-in-place). Initialize is not applied to the aggregate as a whole, nor is the value of the aggregate or object adjusted.</td>
</tr>
<tr>
<td>24.d</td>
<td>All of the following use the assignment operation, and thus perform value adjustment:</td>
</tr>
<tr>
<td>24.e</td>
<td>- the assignment_statement (see 5.2);</td>
</tr>
<tr>
<td>24.f</td>
<td>- explicit initialization of a stand-alone object (see 3.3.1) or of a pool element (see 4.8);</td>
</tr>
<tr>
<td>24.g</td>
<td>- default initialization of a component of a stand-alone object or pool element (in this case, the value of each component is assigned, and therefore adjusted, but the value of the object as a whole is not adjusted);</td>
</tr>
<tr>
<td>24.h/2</td>
<td>- {AI95-00318-02} function return, when the result is not built-in-place type is not a return-by-reference type (see 6.5); (adjustment of the result happens before finalization of the function; values of return-by-reference types are not adjusted);</td>
</tr>
<tr>
<td>24.i</td>
<td>- predefined operators (although the only one that matters is concatenation; see 4.5.3);</td>
</tr>
<tr>
<td>24.j</td>
<td>- generic formal objects of mode in (see 12.4); these are defined in terms of constant declarations; and</td>
</tr>
<tr>
<td>24.k/5</td>
<td>- {AI95-00287-01} {AI12-0005-1} aggregates (see 4.3), when the result is not built-in-place (in this case, the value of each component, and the ancestor parent part, for an extension aggregate, is assigned, and therefore adjusted, but the value of the aggregate as a whole is not adjusted; neither is Initialize called);</td>
</tr>
<tr>
<td>24.l</td>
<td>The following also use the assignment operation, but adjustment never does anything interesting in these cases:</td>
</tr>
<tr>
<td>24.m</td>
<td>- By-copy parameter passing uses the assignment operation (see 6.4.1), but controlled objects are always passed by reference, so the assignment operation never does anything interesting in this case. If we were to allow by-copy parameter passing for controlled objects, we would need to make sure that the actual is finalized before doing the copy back for [in] out parameters. The initialization of the parameter itself needs to</td>
</tr>
</tbody>
</table>
happen after the copy back (if any), similar to the finalization of an anonymous function return object or aggregate object.

- **For** loops use the assignment operation (see 5.5), but since the type of the loop parameter is never controlled, nothing interesting happens there, either.

- **AI95-00318-02** Objects initialized by function results and aggregates that are built-in-place. In this case, the assignment operation is never executed, and no adjustment takes place. While built-in-place is always allowed, it is required for some types — see 7.5 and 7.6 — and that's important since limited types have no Adjust to call.

This paragraph was deleted. *AI95-00287-01* Because Controlled and Limited_Controlled are library-level tagged types, all controlled types will be library-level types, because of the accessibility rules (see 3.10.2 and 3.9.1). This ensures that the Finalize operations may be applied without providing any "display" or "static-link". This simplifies finalization as a result of garbage collection, abort, and asynchronous transfer of control.

Finalization of the parts of a protected object are not done as protected actions. It is possible (in pathological cases) to create tasks during finalization that access these parts in parallel with the finalization itself. This is an erroneous use of shared variables.

**Implementation Note:** One implementation technique for finalization is to chain the controlled objects together on a per-task list. When leaving a master, the list can be walked up to a marked place. The links needed to implement the list can be declared (privately) in types Controlled and Limited_Controlled, so they will be inherited by all controlled types.

Another implementation technique, which we refer to as the "PC-map" approach essentially implies inserting exception handlers at various places, and finalizing objects based on where the exception was raised.

The PC-map approach is for the compiler/linker to create a map of code addresses; when an exception is raised, or abort occurs, the map can be consulted to see where the task was executing, and what finalization needs to be performed. This approach was given in the Ada 83 Rationale as a possible implementation strategy for exception handling — the map is consulted to determine which exception handler applies.

If the PC-map approach is used, the implementation must take care in the case of arrays. The generated code will generally contain a loop to initialize an array. If an exception is raised part way through the array, the components that have been initialized must be finalized, and the others must not be finalized.

It is our intention that both of these implementation methods should be possible.

**Wording Changes from Ada 83**

Finalization depends on the concepts of completion and leaving, and on the concept of a master. Therefore, we have moved the definitions of these concepts here, from where they used to be in Clause 9. These concepts also needed to be generalized somewhat. Task waiting is closely related to user-defined finalization; the rules here refer to the task-waiting rules of Clause 9.

**Inconsistencies With Ada 95**

*AI95-0066-1* **Ada 2012 Correction:** Changed the definition of the master of an anonymous object used to directly initialize an object, so it can be finalized immediately rather than having to hang around as long as the object. In this case, the Ada 2005 definition was inconsistent with Ada 95, and Ada 2012 changes it back. It is unlikely that many compilers implemented the rule as written in Amendment 1, so an inconsistency is unlikely to arise in practice.

**Wording Changes from Ada 95**

*AI95-00182-01* **Corrigendum:** Fixed the wording to say that anonymous objects aren't finalized until the object can't be used anymore.

*AI95-00169-01* **Corrigendum:** Added wording to clarify what happens when Adjust or Finalize raises an exception; some cases had been omitted.

*AI95-00193-01* Stated that if Adjust raises an exception during initialization, nothing further is required. This is corrected in Ada 2005 to include all kinds of assignment other than assignment_statements.

*AI95-00193-01* **Corrigendum:** Stated that if Adjust raises an exception during initialization, nothing further is required. This is corrected in Ada 2005 to include all kinds of assignment other than assignment_statements.

*AI95-00162-01* Revised the definition of master to include expressions and statements, in order to cleanly define what happens for tasks and controlled objects created as part of a subprogram call. Having done that, all of the special wording to cover those cases is eliminated (at least until the Ada comments start rolling in).

*AI95-00280-01* We define finalization of the collection here, so as to be able to conveniently refer to it in other rules (especially in 4.8, “Allocators”).

*AI95-00416-01* Clarified that a coextension is finalized at the same time as the outer object. (This was intended for Ada 95, but since the concept did not have a name, it was overlooked.)
Inconsistencies With Ada 2005

{AI05-0051-1} {AI05-0190-1} Correction: Better defined when objects allocated from anonymous access types are finalized. This could be inconsistent if objects are finalized in a different order than in an Ada 2005 implementation and that order caused different program behavior; however programs that depend on the order of finalization within a single master are already fragile and hopefully are rare.

Wording Changes from Ada 2005

{AI05-0064-1} Correction: Removed a redundant rule, which is now covered by the additional places where masters are defined.

{AI05-0099-1} {AI12-0005-1} Correction: Clarified the finalization rules so that there is no doubt that privacy is ignored, and to ensure that objects of class-wide interface types are finalized based on their specific concrete type.

{AI05-0107-1} Correction: Allowed premature finalization of parts of failed allocator. This could be an inconsistency, but the previous behavior is still allowed and there is no requirement that implementations take advantage of the permission.

{AI05-0111-3} Added a permission to finalize an object allocated from a subpool later than usual.

{AI05-0142-4} Added text to specially define the master of anonymous objects which are passed as explicitly aliased parameters (see 6.1) of functions. The model for these parameters is explained in detail in 6.4.1.

Wording Changes from Ada 2012

{AI12-0406-1} Correction: Defined the term “master construct”, so as to put static accessibility rules on a firmer basis, including ensuring that those rules apply inside of generic bodies.
8 Visibility Rules

{AI05-0299-1} [The rules defining the scope of declarations and the rules defining which identifiers, character literals, and operator symbols are visible at (or from) various places in the text of the program are described in this clause section. The formulation of these rules uses the notion of a declarative region.

{AI12-0439-1} As explained in Clause 3, a declaration declares a view of an entity and associates a defining name with that view. The view comprises an identification of the viewed entity, and possibly additional properties. A usage name denotes a declaration. It also denotes the view declared by that declaration, and denotes the entity of that view. Thus, two different usage names cannot denote two different views of the same entity; in this case they denote the same entity.]

To be honest: In some cases, a usage name that denotes a declaration does not denote the view declared by that declaration, nor the entity of that view; but instead denotes a view of the current instance of the entity, and denotes the current instance of the entity. This sometimes happens when the usage name occurs inside the declarative region of the declaration.

Wording Changes from Ada 83

We no longer define the term “basic operation;” thus we no longer have to worry about the visibility of them. Since they were essentially always visible in Ada 83, this change has no effect. The reason for this change is that the definition in Ada 83 was confusing, and not quite correct, and we found it difficult to fix. For example, one wonders why an if_statement was not a basic operation of type Boolean. For another example, one wonders what it meant for a basic operation to be “inherent in” something. Finally, this fixes the problem addressed by A183-00027/07.

8.1 Declarative Region

Static Semantics

For each of the following constructs, there is a portion of the program text called its declarative region, [within which nested declarations can occur]:

- any declaration, other than that of an enumeration type, that is not a completion [of a previous declaration];
- {AI12-0094-1} an access_definition;
- {AI12-0061-1} an iterated_component_association;
- {AI12-0308-1} an iterated_element_association;
- {AI05-0255-1} {AI12-0308-1} a quantified_expression;
- {AI12-0236-1} a declare_expression;
- a block_statement;
- a loop_statement;
- {This paragraph was deleted.} {AI05-0255-1} {AI12-0308-1} a quantified_expression;
- {AI95-00318-02} an extended_return_statement;
- an accept_statement;
- an exception_handler.

The declarative region includes the text of the construct together with additional text determined [(recursively)], as follows:

- If a declaration is included, so is its completion, if any.
• If the declaration of a library unit [(including Standard — see 10.1.1)] is included, so are the declarations of any child units [(and their completions, by the previous rule)]. The child declarations occur after the declaration.

• If a body_stub is included, so is the corresponding subunit.

• If a type_declaration is included, then so is a corresponding record_representation_clause, if any.

  **Reason:** This is so that the component_declarations can be directly visible in the record_representation_clause.

The declarative region of a declaration is also called the declarative region of any view or entity declared by the declaration.

  **Reason:** The constructs that have declarative regions are the constructs that can have declarations nested inside them. Nested declarations are declared in that declarative region. The one exception is for enumeration literals; although they are nested inside an enumeration type declaration, they behave as if they were declared at the same level as the type.

  **To be honest:** A declarative region does not include parent_unit_names.

  **Ramification:** A declarative region does not include context_clauses.

A declaration occurs immediately within a declarative region if this region is the innermost declarative region that encloses the declaration (the immediately enclosing declarative region), not counting the declarative region (if any) associated with the declaration itself.

  **Discussion:** Don't confuse the declarative region of a declaration with the declarative region in which it immediately occurs.

A declaration is local to a declarative region if the declaration occurs immediately within the declarative region.] [An entity is local to a declarative region if the entity is declared by a declaration that is local to the declarative region.]

  **Ramification:** "Occurs immediately within" and "local to" are synonyms (when referring to declarations).

Thus, “local to” applies to both declarations and entities, whereas “occurs immediately within” only applies to declarations. We use this term only informally, for cases where precision is required, we use the term "occurs immediately within", since it is less likely to cause confusion.

A declaration is global to a declarative region if the declaration occurs immediately within another declarative region that encloses the declarative region. An entity is global to a declarative region if the entity is declared by a declaration that is global to the declarative region.

---

**NOTE 1** The children of a parent library unit are inside the parent's declarative region, even though they do not occur inside the parent's declaration or body. This implies that one can use (for example) "P.Q" to refer to a child of P whose defining name is Q, and that after "use P;" Q can refer (directly) to that child.

**NOTE 2** As explained above and in 10.1.1, “Compilation Units - Library Units”, all library units are descendants of Standard, and so are contained in the declarative region of Standard. They are not inside the declaration or body of Standard, but they are inside its declarative region.

**NOTE 3** {AI12-0442-1} For a declarative region that comes in multiple parts, the text of the declarative region does not include any of the text that appears between the parts. Thus, when a portion of a declarative region is said to extend from one place to another in the declarative region, the portion does not contain any of the text that appears between the parts of the declarative region.

**Discussion:** It is necessary for the things that have a declarative region to include anything that contains declarations (except for enumeration type declarations). This includes any declaration that has a profile (that is, subprogram_declaration, subprogram_body, entry_declaration, subprogram_renaming_declaration, formal_subprogram_declaration, access-to-subprogram_type_declaration), anything that has a discriminant_part (that is, various kinds of type_declaration), anything that has a component_list (that is, record type_declaration and record extension type_declaration), and finally the declarations of task and protected units and packages.

**Wording Changes from Ada 83**

---

8.1 Declarative Region
• Derived types/type extensions — we need a declarative region for inherited components and also for new components.
• All the kinds of types that allow discriminants.
• Protected units.
• Entries that have bodies instead of accept statements.
• The choice parameter specification of an exception_handler.
• The formal parameters of access-to-subprogram types.
• Renamings-as-body.

Discriminated and access-to-subprogram type declarations need a declarative region. Enumeration type declarations cannot have one, because you don't have to say "Color.Red" to refer to the literal Red of Color. For other type declarations, it doesn't really matter whether or not there is an associated declarative region, so for simplicity, we give one to all types except enumeration types.

We now say that an accept_statement has its own declarative region, rather than being part of the declarative region of the entry_declaration, so that declarative regions are properly nested regions of text, so that it makes sense to talk about "inner declarative regions", and "...extends to the end of a declarative region". Inside an accept_statement, the name of one of the parameters denotes the parameter specification of the accept_statement, not that of the entry_declaration. If the accept_statement is nested within a block_statement, these parameterSpecifications can hide declarations of the block_statement. The semantics of such cases was unclear in RM83.

To be honest: Unfortunately, we have the same problem for the entry name itself — it should denote the accept_statement, but accept_statements are not declarations. They should be, and they should hide the entry from all visibility within themselves.

Note that we can't generalize this to entry_bodies, or other bodies, because the declarative_part of a body is not supposed to contain (explicit) homographs of things in the declaration. It works for accept_statements only because an accept_statement does not have a declarative_part.

To avoid confusion, we use the term “local to” only informally in Ada 95. Even RM83 used the term incorrectly (see, for example, RM83-12.3(13)).

In Ada 83, (root) library units were inside Standard; it was not clear whether the declaration or body of Standard was meant. In Ada 95, they are children of Standard, and so occur immediately within Standard’s declarative region, but not within either the declaration or the body. (See RM83-8.6(2) and RM83-10.1.1(5).)

Wording Changes from Ada 95

{AI95-00318-02} Extended return statement (see 6.5) is added to the list of constructs that have a declarative region.

Extensions to Ada 2012

{AI12-0094-1} Corrigendum: access definition is added to the list of constructs that have a declarative region. This allows parameter names declared in anonymous access type subprogram types to be the same as other names declared outside. For instance:

```ada
type Foo is record
  A : Natural;
  B : access procedure (A : Boolean);
end record;
```

{AI12-0005-1} This is now legal, as one would expect; it was illegal in previous versions of Ada as the parameter A and the component A were homographs in the same declarative region (see 8.3). Note that some implementations already allow this common sense interpretation, so this extension might in fact already be used in existing code.

Wording Changes from Ada 2012

{AI12-0061-1} {AI12-0236-1} {AI12-0308-1} Added iterated_component_association, iterated_element_association, and declare_expression to the rapidly expanding list of constructs that have a declarative region.

8.2 Scope of Declarations

[For each declaration, the language rules define a certain portion of the program text called the scope of the declaration. The scope of a declaration is also called the scope of any view or entity declared by the
declaration. Within the scope of an entity, and only there, there are places where it is legal to refer to the declared entity. These places are defined by the rules of visibility and overloading.]

Static Semantics

2  The immediate scope of a declaration is a portion of the declarative region immediately enclosing the declaration. The immediate scope starts at the beginning of the declaration, except in the case of an overloadable declaration, in which case the immediate scope starts just after the place where the profile of the callable entity is determined (which is at the end of the _specification for the callable entity, or at the end of the generic_instantiation if an instance). The immediate scope extends to the end of the declarative region, with the following exceptions:

2.a  Reason: The reason for making overloadable declarations with profiles special is to simplify compilation: until the compiler has determined the profile, it doesn't know which other declarations are homographs of this one, so it doesn't know which ones this one should hide. Without this rule, two passes over the _specification or generic_instantiation would be required to resolve names that denote things with the same name as this one.

3  • The immediate scope of a library_item includes only its semantic dependents.

3.a/3  Reason: Clause 10 defines only a partial ordering of library_items. Therefore, it is a good idea to restrict the immediate scope (and the scope, defined below) to semantic dependents.

3.b  Consider also examples like this:

3.c  package P is end P;
3.d  package P.Q is  
      I : Integer := 0;
    end P.Q;
3.e/1  with P;
5    package R is
      package X renames P;
      J : Integer := X.Q.I := 17; -- Illegal
    end R;
3.f  The scope of P.Q does not contain R. Hence, neither P.Q nor X.Q are visible within R. However, the name R.X.Q would be visible in some other library unit where both R and P.Q are visible (assuming R were made legal by removing the offending declaration).

3.g/2  Ramification: This rule applies to limited views as well as “normal” library items. In that case, the semantic dependents are the units that have a limited_with_clause for the limited view.

4  • The immediate scope of a declaration in the private part of a library unit does not include the visible part of any public descendant of that library unit.

4.a  Ramification: In other words, a declaration in the private part can be visible within the visible part, private part and body of a private child unit. On the other hand, such a declaration can be visible within only the private part and body of a public child unit.

4.b  Reason: The purpose of this rule is to prevent children from giving private information to clients.

4.c/2  Ramification: For a public child subprogram, this means that the parent's private part is not visible in the profile formal_parts of the declaration and of the body. This is true even for subprogram_bodies that are not completions. For a public child generic unit, it means that the parent's private part is not visible in the generic formal_part, as well as in the first list of basic declarative_items (for a generic package), or the syntactic profile formal_part(s) (for a generic subprogram).

5  [The visible part of (a view of) an entity is a portion of the text of its declaration containing declarations that are visible from outside.] The private part of (a view of) an entity that has a visible part contains all declarations within the declaration of (the view of) the entity, except those in the visible part; [these are not visible from outside. Visible and private parts are defined only for these kinds of entities: callable entities, other program units, and composite types.]

6  • The visible part of a view of a callable entity is its profile.

7  • The visible part of a composite type other than a task or protected type consists of the declarations of all components declared [(explicitly or implicitly)] within the type declaration.
The visible part of a generic unit includes the \texttt{generic\_formal\_part}. For a generic package, it also includes the first list of \texttt{basic\_declarative\_items} of the \texttt{package\_specification}. For a generic subprogram, it also includes the profile.

\textbf{Reason:} Although there is no way to reference anything but the formals from outside a generic unit, they are still in the visible part in the sense that the corresponding declarations in an instance can be referenced (at least in some cases). In other words, these declarations have an effect on the outside world. The visible part of a generic unit needs to be defined this way in order to properly support the rule that makes a parent's private part invisible within a public child's visible part.

\textbf{Ramification:} The visible part of an instance of a generic unit is as defined for packages and subprograms; it is not defined in terms of the visible part of a generic unit.

\item The visible part of a package, task unit, or protected unit consists of declarations in the program unit's declaration other than those following the reserved word \texttt{private}, if any; see 7.1 and 12.7 for packages, 9.1 for task units, and 9.4 for protected units.

The scope of a declaration always contains the immediate scope of the declaration. In addition, for a given declaration that occurs immediately within the visible part of an outer declaration, or is a public child of an outer declaration, the scope of the given declaration extends to the end of the scope of the outer declaration, except that the scope of a \texttt{library\_item} includes only its semantic dependents.

\textbf{Ramification:} Note the recursion. If a declaration appears in the visible part of a library unit, its scope extends to the end of the scope of the library unit, but since that only includes dependents of the declaration of the library unit, the scope of the inner declaration also only includes those dependents. If X renames library package P, which has a child Q, a \texttt{with\_clause} mentioning P.Q is necessary to be able to refer to X.Q, even if P.Q is visible at the place where X is declared.

\textbf{AI95-00408-01} \textbf{AI05-0183-1} The scope of an \texttt{attribute\_definition\_clause} is identical to the scope of a declaration that would occur at the point of the \texttt{attribute\_definition\_clause}. The scope of an \texttt{aspect\_specification} is identical to the scope of the associated declaration.

The immediate scope of a declaration is also the immediate scope of the entity or view declared by the declaration. Similarly, the scope of a declaration is also the scope of the entity or view declared by the declaration.

\textbf{Ramification:} The rule for immediate scope implies the following:

\item If the declaration is that of a library unit, then the immediate scope includes the declarative region of the declaration itself, but not other places, unless they are within the scope of a \texttt{with\_clause} that mentions the library unit.

It is necessary to attach the semantics of \texttt{with\_clauses} to [immediate] scopes (as opposed to visibility), in order for various rules to work properly. A library unit should hide a homographic implicit declaration that appears in its parent, but only within the scope of a \texttt{with\_clause} that mentions the library unit. Otherwise, we would violate the "legality determinable via semantic dependences" rule of 10, "Program Structure and Compilation Issues". The declaration of a library unit should be allowed to be a homograph of an explicit declaration in its parent's body, so long as that body does not mention the library unit in a \texttt{with\_clause}.

This means that one cannot declare the declaration of the library unit, but one might still be able to denote the library unit via another view.

A \texttt{with\_clause} does not make the declaration of a library unit visible; the lack of a \texttt{with\_clause} prevents it from being visible. Even if a library unit is mentioned in a \texttt{with\_clause}, its declaration can still be hidden.

\item The completion of the declaration of a library unit (assuming that's also a declaration) is not visible, neither directly nor by selection, outside that completion.

\item The immediate scope of a declaration immediately within the body of a library unit does not include any child of that library unit.

This is needed to prevent children from looking inside their parent's body. The children are in the declarative region of the parent, and they might be after the parent's body. Therefore, the scope of a declaration that occurs immediately within the body might include some children.

\textbf{AI12-0003-1} The immediate scope of a pragma that is not used as a configuration pragma is defined to be the region extending from immediately after the pragma to the end of the declarative region immediately enclosing the pragma.
NOTE \{AI05-0299-1\} There are notations for denoting visible declarations that are not directly visible. For example, parameter specifications are in the visible part of a subprogram declaration so that they can be used in named-notation calls appearing outside the called subprogram. For another example, declarations of the visible part of a package can be denoted by expanded names appearing outside the package, and can be made directly visible by a use_clause.

Ramification: \{AI95-00114-01\} There are some obscure cases involving generics in which there is no such notation. See Clause 12.

Extensions to Ada 83

The fact that the immediate scope of an overloadable declaration does not include its profile is new to Ada 95. It replaces RM83-8.3(16), which said that within a subprogram specification and within the formal part of an entry declaration or accept statement, all declarations with the same designator as the subprogram or entry were hidden from all visibility. The RM83-8.3(16) rule seemed to be overkill, and created both implementation difficulties and unnecessary semantic complexity.

Wording Changes from Ada 83

We no longer need to talk about the scope of notations, identifiers, character_literals, and operator_symbols.

\{AI05-0299-1\} The notion of "visible part" has been extended in Ada 95. The syntax of task and protected units now allows private parts, thus requiring us to be able to talk about the visible part as well. It was necessary to extend the concept to subprograms and to generic units, in order for the visibility rules related to child library units to work properly. It was necessary to define the concept separately for generic formal packages, since their visible part is slightly different from that of a normal package. Extending the concept to composite types made the definition of scope slightly simpler. We define visible part for some things elsewhere, since it makes a big difference to the user for those things. For composite types and subprograms, however, the concept is used only in arcane visibility rules, so we localize it to this subclause.

In Ada 83, the semantics of with_clauses was described in terms of visibility. It is now described in terms of [immediate] scope.

We have clarified that the following is illegal (where Q and R are library units):

```ada
package Q is
    I : Integer := 0;
end Q;

package R is
    package X renames Standard;
    X.Q.I := 17; -- Illegal!
end R;
```

even though Q is declared in the declarative region of Standard, because R does not mention Q in a with_clause.

Wording Changes from Ada 95

\{AI95-00408-01\} The scope of an attribute_definition_clause is defined so that it can be used to define the visibility of such a clause, so that can be used by the stream attribute availability rules (see 13.13.2).

Wording Changes from Ada 2005

\{AI05-0183-1\} The scope of an aspect_specification is defined for similar reasons that it was defined for attribute_definition_clauses.

Wording Changes from Ada 2012

\{AI12-0003-1\} The immediate scope of a pragma is defined as it is used in other rules in the Reference Manual.

8.3 Visibility

1 [The visibility rules, given below, determine which declarations are visible and directly visible at each place within a program. The visibility rules apply to both explicit and implicit declarations.]

Static Semantics

2 A declaration is defined to be directly visible at places where a name consisting of only an identifier or operator_symbol is sufficient to denote the declaration; that is, no selected_component notation or special context (such as preceding => in a named association) is necessary to denote the declaration. A
declaration is defined to be visible wherever it is directly visible, as well as at other places where some name (such as a selected_component) can denote the declaration.

The syntactic category direct_name is used to indicate contexts where direct visibility is required. The syntactic category selector_name is used to indicate contexts where visibility, but not direct visibility, is required.

There are two kinds of direct visibility: immediate visibility and use-visibility. A declaration is immediately visible at a place if it is directly visible because the place is within its immediate scope. A declaration is use-visible if it is directly visible because of a use_clause (see 8.4). Both conditions can apply.

A declaration can be hidden, either from direct visibility, or from all visibility, within certain parts of its scope. Where hidden from all visibility, it is not visible at all (neither using a direct_name nor a selector_name). Where hidden from direct visibility, only direct visibility is lost; visibility using a selector_name is still possible.

Two or more declarations are overloaded if they all have the same defining name and there is a place where they are all directly visible.

Ramification: Note that a name can have more than one possible interpretation even if it denotes a nonoverloadable entity. For example, if there are two functions F that return records, both containing a component called C, then the name F.C has two possible interpretations, even though component declarations are not overloadable.

The declarations of callable entities [(including enumeration literals)] are overloadable, meaning that overloading is allowed for them.

Ramification: A generic_declaration is not overloadable within its own generic_formal_part. This follows from the rules about when a name denotes a current instance. See A183-00286. This implies that within a generic_formal_part, outer declarations with the same defining name are hidden from direct visibility. It also implies that if a generic formal parameter has the same defining name as the generic itself, the formal parameter hides the generic from direct visibility.

Two declarations are homographs if they have the same defining name, and, if both are overloadable, their profiles are type conformant. [An inner declaration hides any outer homograph from direct visibility.]

Term entry: overriding operation — operation that replaces an inherited primitive operation

Note: Operations can be marked explicitly as overriding or not overriding.

{8652/0025} {A195-00044-01} [Two homographs are not generally allowed immediately within the same declarative region unless one overrides the other (see Legality Rules below).] The only declarations that are overloadable are the implicit declarations for predefined operators and inherited primitive subprograms.

A declaration overrides another homograph that occurs immediately within the same declarative region in the following cases:

• {8652/0025} {A195-00044-01} A declaration that is not overloadable overrides one that is overloadable. An explicit declaration overrides an implicit declaration of a primitive subprogram, [regardless of which declaration occurs first];

Ramification: {8652/0025} {A195-00044-01} And regardless of whether the nonoverridable explicit declaration is overloadable or not, For example, statement_identifiers are covered by this rule.

The “regardless of which declaration occurs first” is there because the explicit declaration could be a primitive subprogram of a partial view, and then the full view might inherit a homograph. We are saying that the explicit one wins (within its scope), even though the implicit one comes later.

If the overriding declaration is also a subprogram, then it is a primitive subprogram.

As explained in 7.3.1, “Private Operations”, some inherited primitive subprograms are never declared. Such subprograms cannot be overridden, although they can be reached by dispatching calls in the case of a tagged type.

• The implicit declaration of an inherited operator overrides that of a predefined operator;
Ramification: In a previous version of Ada 9X, we tried to avoid the notion of predefined operators, and say that they were inherited from some magical root type. However, this seemed like too much mechanism. Therefore, a type can have a predefined "+" as well as an inherited "+". The above rule says the inherited one wins.

The "regardless of which declaration occurs first" applies here as well, in the case where a derived type definition in the visible part of a public library unit derives from a private type declared in the parent unit, and the full view of the parent type has additional predefined operators, as explained in 7.3.1, "Private Operations". Those predefined operators can be overridden by inherited subprograms implicitly declared earlier.

• An implicit declaration of an inherited subprogram overrides a previous implicit declaration of an inherited subprogram.

• {AI95-00251-01} If two or more homographs are implicitly declared at the same place:

  • {AI95-00251-01} If at least one is a subprogram that is neither a null procedure nor an abstract subprogram, and does not require overriding (see 3.9.3), then they override those that are null procedures, abstract subprograms, or require overriding. If more than one such homograph remains that is not thus overridden, then they are all hidden from all visibility.

  • {AI95-00251-01} {AI12-0183-1} Otherwise (all are null procedures, abstract subprograms, or require overriding), then any null procedure overrides all abstract subprograms and all subprograms that require overriding; if more than one such homograph remains that is not thus overridden, then if the profiles of the remaining homographs are all fully conformant with one another, one is chosen arbitrarily; if not, they are all hidden from all visibility.

Discussion: In the case where the implementation arbitrarily chooses one override from among a group of inherited subprograms, users should not be able to determine which member was chosen, as the set of inherited subprograms which are chosen from must be fully conformant. This rule is needed in order to allow

```
package Outer is
package P1 is
    type Ifc1 is interface;
    procedure Null_Procedure (X : Ifc1) is null;
    procedure Abstract_Subp (X : Ifc1) is abstract;
end P1;
package P2 is
    type Ifc2 is interface;
    procedure Null_Procedure (X : Ifc2) is null;
    procedure Abstract_Subp (X : Ifc2) is abstract;
end P2;
type T is abstract new P1.Ifc1 and P2.Ifc2 with null record;
end Outer;
```

without requiring that T explicitly override any of its inherited operations.

Full conformance is required here, as we cannot allow the parameter names to differ. If they did differ, the routine which was selected for overriding could be determined by using named parameter notation in a call.

{AI12-0005-1} When the subprograms do not conform, we chose not to adopt the “use clause” rule which would make them all visible resulting in likely ambiguity. If we had used such a rule, any successful calls would be confusing; and the fact that there are no Beaujolais-like effects to worry about means we can consider other rules. The hidden-from-all-visibility homographs are still inherited by further derivations, which avoids order-of-declaration dependencies and other anomalies.

We have to be careful to not include arbitrary selection if the routines have real bodies. (This can happen in generics, see the example in the incompatibilities section below.) We don't want the ability to successfully call routines where the body executed depends on the compiler or a phase of the moon.

Note that if the type is concrete, abstract subprograms are inherited as subprograms that require overriding. We include functions that require overriding as well; these don't have real bodies, so they can use the more liberal rules.

• [For an implicit declaration of a primitive subprogram in a generic unit, there is a copy of this declaration in an instance.] However, a whole new set of primitive subprograms is implicitly declared for each type declared within the visible part of the instance. These new declarations occur immediately after the type declaration, and override the copied ones. [The copied ones can be called only from within the instance; the new ones can be called only from outside the instance, although for tagged types, the body of a new one can be executed by a call to an old one.]
A declaration is visible within its scope, except where hidden from all visibility, as follows:

- An overridden declaration is hidden from all visibility within the scope of the overriding declaration.

**Discussion:** In addition, this is also stated redundantly (again), and is repeated, in 12.3, “Generic Instantiation”. The rationale for the rule is explained there.

**To be honest:** {AI05-0042-01} The implicit subprograms declared when an operation of a progenitor is implemented by an entry or subprogram also override the appropriate implicitly declared inherited operations of the progenitor.

- A declaration is hidden from all visibility until the end of the declaration, except:
  - For a record type or record extension, the declaration is hidden from all visibility only until the reserved word `record`.
  - {AI95-00345-01} For a `package_declaration`, `task_declaration`, `protected declaration`, `generic_package_declaration`, `subprogram_body`, or `expression_function_declaration`, the declaration is hidden from all visibility only until the reserved word `is` of the declaration.
    
    **Ramification:** We're talking about the `is` of the construct itself, here, not some random `is` that might appear in a `generic_formal_part`.

  - {AI95-00345-01} For a `task_declaration` or `protected declaration`, the declaration is hidden from all visibility only until the reserved word `with` of the declaration if there is one, or the reserved word `is` of the declaration if there is no `with`.
    
    **To be honest:** If there is neither a `with` nor an `is`, then the exception does not apply and the name is hidden from all visibility until the end of the declaration. This oddity was inherited from Ada 95.

    **Reason:** We need the “`with` or `is`” rule so that the visibility within an `interface` list does not vary by construct. That would make it harder to complete private extensions and would complicate implementations.

  - If the completion of a declaration is a declaration, then within the scope of the completion, the first declaration is hidden from all visibility. Similarly, a `discriminant_specification` or `parameter_specification` is hidden within the scope of a corresponding `discriminant`-`specification` or `parameter_specification` of a corresponding completion, or of a corresponding `accept_statement`.

    **Ramification:** This rule means, for example, that within the scope of a `full_type_declaration` that completes a `private_type_declaration`, the name of the type will denote the `full_type_declaration`, and therefore the full view of the type. On the other hand, if the completion is not a declaration, then it doesn't hide anything, and you can't denote it.

  - {AI95-00217-06} The declaration of a library unit (including a `library_unit_renaming_declaration`) is hidden from all visibility except at places `outside` that are not within its declarative region that are not within the scope of a `nonlimited_with_clause` that mentions it. The limited view of a library package is hidden from all visibility at places that are not within the scope of a limited `with_clause` that mentions it; in addition, the limited view is hidden from all visibility within the declarative region of the package, as well as within the scope of any `nonlimited_with_clause` that mentions the package. Where the declaration of the limited view of a package is visible, any name that denotes the package denotes the limited view, including those provided by a `package_renaming` (For each declaration or renaming of a generic unit as a child of some parent generic package, there is a corresponding declaration nested immediately within each instance of the parent.) Such a nested declaration is hidden from all visibility except at places that are within the scope of a `with_clause` that mentions the child.

    **Discussion:** {AI95-00217-06} This is the rule that prevents `with_clauses` from being transitive; the [immediate] scope includes indirect semantic dependents. This rule also prevents the limited view of a package from being visible in the same place as the full view of the package, which prevents various ripple effects.
8.3 Visibility

Visibility

For each declaration or renaming of a generic unit as a child of some parent generic package, there is a corresponding declaration nested immediately within each instance of the parent. Such a nested declaration is hidden from all visibility except at places that are within the scope of a with clause that mentions the child.

A declaration with a defining_identifier or defining_operator_symbol is immediately visible [(and hence directly visible)] within its immediate scope except where hidden from direct visibility, as follows:

- A declaration is hidden from direct visibility within the immediate scope of a homograph of the declaration, if the homograph occurs within an inner declarative region;
- A declaration is also hidden from direct visibility where hidden from all visibility.

An attribute_definition_clause or an aspect_specification is visible everywhere within its scope.

Name Resolution Rules

A direct_name shall resolve to denote a directly visible declaration whose defining name is the same as the direct_name. A selector_name shall resolve to denote a visible declaration whose defining name is the same as the selector_name.

Discussion: "The same as" has the obvious meaning here, so for +, the possible interpretations are declarations whose defining name is "+" (an operator_symbol).

These rules on visibility and direct visibility do not apply in a context_clause, a parent_unit_name, or a pragma that appears at the place of a compilation_unit. For those contexts, see the rules in 10.1.6, "Environment-Level Visibility Rules".

Ramification: Direct visibility is irrelevant for character_literals. In terms of overload resolution character_literals are similar to other literals, like null — see 4.2. For character_literals, there is no need to worry about hiding, since there is no way to declare homographs.

Legality Rules

A nonoverridable explicit declaration is illegal if there is a homograph occurring immediately within the same declarative region that is visible at the place of the declaration, and is not hidden from all visibility by the nonoverridable explicit declaration. In addition, a type extension is illegal if somewhere within its immediate scope it has two visible components with the same name. Similarly, the context_clause for a compilation_unit is illegal if it mentions (in a with_clause) some library unit, and there is a homograph of the library unit that is visible at the place of the compilation_unit corresponding stub, and the homograph and the mentioned library unit are both declared immediately within the same declarative region. These rules also apply to dispatching operations declared in the visible part of an instance of a generic unit. However, they do not apply to other overloading declarations in an instance[; such declarations may have type conformant profiles in the instance, so long as the corresponding declarations in the generic were not type conformant].

Discussion: Normally, these rules just mean you can't explicitly declare two homographs immediately within the same declarative region. The wording is designed to handle the following special cases:

- If the second declaration completes the first one, the second declaration is legal.
- If the body of a library unit contains an explicit homograph of a child of that same library unit, this is illegal only if the body mentions the child in its context_clause, or if some subunit mentions the child. Here's an example:
  ```ada
  package P is
  end P;
  package P.Q is
  end P.Q;
  ```
package body P is
  Q : Integer;  -- OK; we cannot see package P.Q here.
procedure Sub is separate;
end P;

with P.Q; separate (P) procedure Sub is -- Illegal.
begin
  null;
end Sub;

If package body P said "with P.Q", then it would be illegal to declare the homograph Q: Integer. But it does not, so the body of P is OK. However, the subunit would be able to see both P.Q's, and is therefore illegal.

A previous version of Ada 9X allowed the subunit, and said that references to P.Q would tend to be ambiguous. However, that was a bad idea, because it requires overload resolution to resolve references to directly visible nonoverloadable homographs, which is something compilers have never before been required to do.

• \{8652/0026\} \{8652/0102\} \{AI95-00150-01\} \{AI95-00157-01\} If a type extension contains a component with the same name as a component in an ancestor type, there must be no place where both components are visible. For instance:

```ada
package A is
  type T is tagged private;
  package B is
    type NT is new T with record
      I : Integer;  -- Illegal because T.I is visible in the body.
    end record;
  end B;
  private
    type T is tagged record
      I : Integer;  -- Illegal because T.I is visible in the body.
    end record;
  end A;
{AI95-00114-01} package A is
  package body A is
    -- T.I becomes visible here.
  end B;
  end A;
{AI95-00114-01} package A.C is
  type NT2 is new A.T with record
    I : Integer;  -- Illegal because T.I is visible in the private part.
  end record;
  private
    -- T.I is visible here.
  end A.C;
with A;
package D is
  type NT3 is new A.T with record
    I : Integer;  -- Legal because T.I is never visible in this package.
  end record;
  end D;
with D;
package A.E is
  type NT4 is new D.NT3 with null record;
  X : NT4;
  I1 : Integer := X.I;  -- D.NT3/I
  I3 : Integer := A.T(X).I;  -- A.T/I
end A.E;
{8652/0102} \{AI95-00157-01\} D.NT3 can have a component I because the component I of the parent type is never visible. The parent component exists, of course, but is never declared for the type D.NT3. In the child package A.E, the component I of A.T is visible, but that does not change the fact that the A.T.I component was never declared for type D.NT3. Thus, A.E.NT4 does not (visibly) inherit the component I from A.T, while it does inherit the component I from D.NT3. Of course, both components exist, and can be accessed by a type conversion as shown above. This behavior stems from the fact that every characteristic of a type (including components) must be declared somewhere in the innermost declarative region containing the type — if the characteristic is never visible in that declarative region, it is never declared. Therefore, such characteristics do not suddenly become available even if they are in fact visible in some other scope. See 7.3.1 for more on the rules.
• \{AI95-00377-01\} It is illegal to mention both an explicit child of an instance, and a child of the generic from which the instance was instantiated. This is easier to understand with an example:

```ada
generic
package G1 is
end G1;

generic
package G1.G2 is
end G1.G2;

with G1;
package I1 is new G1;

package I1.G2 renames ...
with I1.G2;             -- Illegal
package Bad is ...
```

\{AI12-0300-1\} The context clause for Bad is illegal as I1 has an implicit declaration of I1.G2 based on the generic child G1.G2, as well as the mention of the explicit child I1.G2. As in the previous cases, this is illegal only if the context clause makes both children visible; the explicit child can be mentioned as long as the generic child is not (and vice versa).

Note that we need to be careful which things we make "hidden from all visibility" versus which things we make simply illegal for names to denote. The distinction is subtle. The rules that disallow names denoting components within a type declaration (see 3.7) do not make the components invisible at those places, so that the above rule makes components with the same name illegal. The same is true for the rule that disallows names denoting formal parameters within a formal_part (see 6.1).

**Discussion:** The part about instances is from A83-00012. The reason it says “overloadable declarations” is because we don’t want it to apply to type extensions that appear in an instance; components are not overloadable.

NOTE 1 Visibility for compilation units follows from the definition of the environment in 10.1.4, except that it is necessary to apply a with_clause to obtain visibility to a library_unit_declaration or library_unit_renaming_declaration.

NOTE 2 In addition to the visibility rules given above, the meaning of the occurrence of a direct_name or selector_name at a given place in the text can depend on the overloading rules (see 8.6).

NOTE 3 Not all contexts where an identifier, character_literal, or operator_symbol are allowed require visibility of a corresponding declaration. Contexts where visibility is not required are identified by using one of these three syntactic categories directly in a syntax rule, rather than using direct_name or selector_name.

**Ramification:** An identifier, character_literal or operator_symbol that occurs in one of the following contexts is not required to denote a visible or directly visible declaration:

1. A defining name.
2. The identifiers or operator_symbol that appear after the reserved word end in a proper_body. Similarly for "end loop", etc.
3. An attribute_designator.
4. A pragma identifier.
5. A pragma_argument_identifier.
6. An identifier specific to a pragma used in a pragma argument.

7. \{AI05-0183-1\} An aspect_mark;
8. \{AI05-0183-1\} An identifier specific to an aspect used in an aspect_definition.

The visibility rules have nothing to do with the above cases; the meanings of such things are defined elsewhere. Reserved words are not identifiers; the visibility rules don't apply to them either.

Because of the way we have defined "declaration", it is possible for a usage name to denote a subprogram_body, either within that body, or (for a nonlibrary unit) after it (since the body hides the corresponding declaration, if any). Other bodies do not work that way. Completions of type_declarations and deferred constant declarations do work that way. Accept_statements are never denoted, although the parameter Specifications in their profiles can be.

The scope of a subprogram does not start until after its profile. Thus, the following is legal:

```ada
X : constant Integer := 17;
...
package P is
procedure X(Y : in Integer := X);
end P;
```

The body of the subprogram will probably be illegal, however, since the constant X will be hidden by then.
The rule is different for generic subprograms, since they are not overloadable; the following is illegal:

```ada
X : constant Integer := 17;
package P is
  generic
  Z : Integer := X; -- Illegal!
  procedure X(Y : in Integer := X); -- Illegal!
end P;
```

The constant X is hidden from direct visibility by the generic declaration.

Extensions to Ada 83

Declarations with the same defining name as that of a subprogram or entry being defined are nevertheless visible within the subprogram specification or entry declaration.

Wording Changes from Ada 83

The term “visible by selection” is no longer defined. We use the terms “directly visible” and “visible” (among other things). There are only two regions of text that are of interest, here: the region in which a declaration is visible, and the region in which it is directly visible.

Visibility is defined only for declarations.

Incompatibilities With Ada 95

{AI95-00251-01} Added rules to handle the inheritance and overriding of multiple homographs for a single type declaration, in order to support multiple inheritance from interfaces. The new rules are intended to be compatible with the existing rules so that programs that do not use interfaces do not change their legality. However, there is a very rare case where this is not true:

```ada
generic
  type T1 is private;
  type T2 is private;
package G is
  type T is null record;
  procedure P (X : T; Y : T1);
  procedure P (X : T; Z : T2);
end G;
package I is new G (Integer, Integer); -- Exports homographs of P.
end I;
```

```ada
procedure P (X : T; Y : T1);
procedure P (X : T; Z : T2);
end I;
```

The call to P would resolve in Ada 95 by using the parameter name, while the procedures P would be hidden from all visibility in Ada 2005 and thus would not resolve. This case doesn't seem worth making the rules any more complex than they already are.

{AI95-00377-01} Amendment Correction: A with_clause is illegal if it would create a homograph of an implicitly declared generic child (see 10.1.1). An Ada 95 compiler could have allowed this, but which unit of the two units involved would be denoted wasn't specified, so any successful use isn't portable. Removing one of the two with clauses involved will fix the problem.

Wording Changes from Ada 95

{8652/0025} {AI95-00044-01} Corrigendum: Clarified the overriding rules so that "/=" and statement_identifiers are covered.

{8652/0026} {AI95-00150-01} Corrigendum: Clarified that it never possible for two components with the same name to be visible; any such program is illegal.

{AI95-000195-01} {AI95-000408-01} The visibility of an attribute_definition_clause is defined so that it can be used by the stream attribute availability rules (see 13.13.2).

{AI95-00217-06} The visibility of a limited view of a library package is defined (see 10.1.1).

Wording Changes from Ada 2005

{AI05-0177-1} {AI12-0157-1} Added wording so that the parameters of an expression_function_declaration are visible in the return_expression of the function. (It would be pretty useless without such a rule.)
8.3.1 Overriding Indicators

An overriding indicator is used to declare that an operation is intended to override (or not override) an inherited operation.

Syntax

overriding_indicator ::= [not] overriding

Legality Rules

If an abstract subprogram declaration, null procedure declaration, expression function declaration, subprogram body, subprogram body stub, subprogram renaming declaration, generic instantiation of a subprogram, or subprogram declaration other than a protected subprogram has an overriding indicator, then:

• the operation shall be a primitive operation for some type;

• if the overriding indicator is overriding, then the operation shall override a homograph at the place of the declaration or body;

  To be honest: This doesn't require that the overriding happen at precisely the place of the declaration or body; it only requires that the region in which the overriding is known to have happened includes this place. That is, the overriding can happen at or before the place of the declaration or body.

• if the overriding indicator is not overriding, then the operation shall not override any homograph (at any place).

In addition to the places where Legality Rules normally apply, these rules also apply in the private part of an instance of a generic unit.

Discussion: The overriding and not overriding rules differ slightly. For overriding, we want the indicator to reflect the overriding state at the place of the declaration; otherwise the indicator would be “lying”. Whether a homograph is implicitly declared after the declaration (see 7.3.1 to see how this can happen) has no impact on this check. However, not overriding is different; “lying” would happen if a homograph declared later actually is overriding. So, we require this check to take into account later overridings. That can be implemented either by looking ahead, or by rechecking when additional operations are declared.

The “no lying” rules are needed to prevent a subprogram declaration and subprogram body from having contradictory overriding indicators.

NOTE Rules for overriding indicators of task and protected entries and of protected subprograms are found in 9.5.2 and 9.4, respectively.

Examples

Example of use of an overriding indicator when declaring a security queue derived from the Queue interface of 3.9.4:

The use of overriding indicators allows the detection of errors at compile-time that otherwise might not be detected at all. For instance, we might declare a security queue derived from the Queue interface of 3.9.4 as:

```ada
type Security_Queue is new Queue with record ...

overriding procedure Append (Q : in out Security_Queue; Person : in Person_Name);

overriding procedure Remove_First (Q : in out Security_Queue; Person : out in Person_Name);

overriding function Cur_Count (Q : in Security_Queue) return Natural;

overriding function Max_Count (Q : in Security_Queue) return Natural;

not overriding procedure Arrest (Q : in out Security_Queue; Person : in Person_Name);
```
The first four subprogram declarations guarantee that these subprograms will override the four subprograms inherited from the Queue interface. A misspelling in one of these subprograms will be detected at compile time by the implementation. Conversely, the declaration of Arrest guarantees that this is a new operation.

Discussion: In this case, the subprograms are abstract, so misspellings will get detected anyway. But for other subprograms (especially when deriving from concrete types), the error might never be detected, and a body other than the one the programmer intended might be executed without warning. Thus our new motto: “Overriding indicators — don’t derive a type without them!”

Extensions to Ada 95

Overriding indicators are new. These let the programmer state her overriding intentions to the compiler; if the compiler disagrees, an error will be produced rather than a hard to find bug.

Wording Changes from Ada 2005

Expression functions can have overriding indicators.

8.4 Use Clauses

A use_package_clause achieves direct visibility of declarations that appear in the visible part of a package; a use_type_clause achieves direct visibility of the primitive operators of a type.

Language Design Principles

If and only if the visibility rules allow P.A, "use P;" should make A directly visible (barring name conflicts). This means, for example, that child library units, and generic formals of a formal package whose formal_package_actual_part is (<>), should be made visible by a use_clause for the appropriate package.

The rules for use_clauses were carefully constructed to avoid so-called Beaujolais effects, where the addition or removal of a single use_clause, or a single declaration in a "use"d package, would change the meaning of a program from one legal interpretation to another.

Syntax

use_clause ::= use_package_clause | use_type_clause

use_package_clause ::= use package_name {, package_name};

use_type_clause ::= use [all] type subtype_mark {, subtype_mark};

Legality Rules

A package_name of a use_package_clause shall denote a nonlimited view of a package.

Ramification: This includes formal packages.

Static Semantics

For each use_clause, there is a certain region of text called the scope of the use_clause. For a use_clause within a context_clause of a library_unit_declaration or library_unit_renaming_declaration, the scope is the entire declarative region of the declaration. For a use_clause within a context_clause of a body, the scope is the entire body [and any subunits (including multiply nested subunits). The scope does not include context_clauses themselves.]

For a use_clause immediately within a declarative region, the scope is the portion of the declarative region starting just after the use_clause and extending to the end of the declarative region. However, the
scope of a use_clause in the private part of a library unit does not include the visible part of any public descendant of that library unit.

Reason: The exception echoes the similar exception for "immediate scope (of a declaration)" (see 8.2). It makes use_clauses work like this:

```
package P is
  type T is range 1..10;
end P;
with P;
package Parent is
  private
    use P;
    X : T;
  end Parent;
package Parent.Child is
  Y : T; -- Illegal!
  Z : P.T;
  private
    W : T;
  end Parent.Child;
```

The declaration of Y is illegal because the scope of the "use P" does not include that place, so T is not directly visible there. The declarations of X, Z, and W are legal.

{AI95-00217-06} A package is named in a use_package_clause if it is denoted by a package_name of that clause. A type is named in a use_type_clause if it is determined by a subtype_mark of that clause.

{AI95-00217-06} {AI05-0150-1} For each package named in denoted by a package_name of a use_package_clause whose scope encloses a place, each declaration that occurs immediately within the declarative region of the package is potentially use-visible at this place if the declaration is visible at this place. For each type T or T'Class named in determined by a subtype_mark of a use_type_clause whose scope encloses a place, the declaration of each primitive operator of type T is potentially use-visible at this place if its declaration is visible at this place. If a use_type_clause whose scope encloses a place includes the reserved word all, then the following entities are also potentially use-visible at this place if the declaration of the entity is visible at this place:

- Each primitive subprogram of T including each enumeration literal (if any);
- Each subprogram that is declared immediately within the declarative region in which an ancestor type of T is declared and that operates on a class-wide type that covers T.

Ramification: {AI05-0150-1} Primitive subprograms whose defining name is an identifier are not made potentially visible by a use_type_clause unless reserved word all is included. A use_type_clause without all is only for operators.

The semantics described here should be similar to the semantics for expanded names given in 4.1.3, “Selected Components” so as to achieve the effect requested by the “principle of equivalence of use_clauses and selected_components”. Thus, child library units and generic formal parameters of a formal package are potentially use-visible when their enclosing package is use'd.

The "visible at that place" part implies that applying a use_clause to a parent unit does not make all of its children use-visible — only those that have been made visible by a with_clause. It also implies that we don't have to worry about hiding in the definition of "directly visible" — a declaration cannot be use-visible unless it is visible.

Note that "use type T'Class;" is equivalent to "use type T;", which helps avoid breaking the generic contract model.

Certain implicit declarations may become potentially use-visible in certain contexts as described in 12.6.

A declaration is use-visible if it is potentially use-visible, except in these naming-conflict cases:

- A potentially use-visible declaration is not use-visible if the place considered is within the immediate scope of a homograph of the declaration.
- Potentially use-visible declarations that have the same identifier are not use-visible unless each of them is an overloadable declaration.
**Ramification:** Overloadable declarations don’t cancel each other out, even if they are homographs, though if they are not distinguishable by formal parameter names or the presence or absence of default expressions, any use will be ambiguous. We only mention identifiers here, because declarations named by operator symbols are always overloadable, and hence never cancel each other. Direct visibility is irrelevant for character literals.

**Dynamic Semantics**

The elaboration of a `use_clause` has no effect.

**Examples**

*Example of a use clause in a context clause:*

```plaintext
with Ada.Calendar; use Ada;
```

*Example of a use type clause:*

```plaintext
use type Rational_Numbers.Rational; -- see 7.1
Two_Thirds: Rational_Numbers.Rational := 2/3;
```

**Ramification:** In “use X, Y;”, Y cannot refer to something made visible by the “use” of X. Thus, it’s not (quite) equivalent to “use X; use Y;”.

If a given declaration is already immediately visible, then a use_clause that makes it potentially use-visible has no effect. Therefore, a use_type_clause for a type whose declaration appears in a place other than the visible part of a package has no effect; it cannot make a declaration use-visible unless that declaration is already immediately visible.

"use type S1;" and "use type S2;" are equivalent if S1 and S2 are both subtypes of the same type. In particular, "use type S;" and "use type S'Base;" are equivalent.

**Reason:** We considered adding a rule that prevented several declarations of views of the same entity that all have the same semantics from cancelling each other out. For example, if a (possibly implicit) subprogram_declaration for “+” is potentially use-visible, and a fully conformant renaming of it is also potentially use-visible, then they (annoyingly) cancel each other out; neither one is use-visible. The considered rule would have made just one of them use-visible. We gave up on this idea due to the complexity of the rule. It would have had to account for both overloadable and nonoverloadable renaming_declarations, the case where the rule should apply only to some subset of the declarations with the same defining name, and the case of subtype_declarations (since they are claimed to be sufficient for renaming of subtypes).

**Extensions to Ada 83**

The use_type_clause is new to Ada 95.

**Wording Changes from Ada 83**

The phrase “omitting from this set any packages that enclose this place” is no longer necessary to avoid making something visible outside its scope, because we explicitly state that the declaration has to be visible in order to be potentially use-visible.

**Wording Changes from Ada 95**

{AI95-00217-06} Limited views of packages are not allowed in use clauses. Defined named in a use clause for use in other limited view rules (see 10.1.2).

**Extensions to Ada 2005**

{AI05-0150-1} The use all_type version of the use_type_clause is new to Ada 2012. It works similarly to prefixed views.

**Wording Changes from Ada 2005**

{AI05-0131-1} Correction: Added wording to allow other declarations to be potentially use-visible, to support corrections to formal subprograms.
8.5 Renaming Declarations

A renaming_declaration declares another name for an entity, such as an object, exception, package, subprogram, entry, or generic unit. Alternatively, a subprogram_renaming_declaration can be the completion of a previous subprogram_declaration.

**Term entry: renaming** — declaration that does not define a new entity, but instead defines a new view of an existing entity

**Syntax**

renaming_declaration ::= object_renaming_declaration | exception_renaming_declaration | package_renaming_declaration | subprogram_renaming_declaration | generic_renaming_declaration

**Dynamic Semantics**

The elaboration of a renaming_declaration evaluates the name that follows the reserved word renames and thereby determines the view and entity denoted by this name (the renamed view and renamed entity). [A name that denotes the renaming_declaration denotes (a new view of) the renamed entity.]

NOTE 1  
Renaming can be used to resolve name conflicts and to act as a shorthand. Renaming with a different identifier or operator_symbol does not hide the old name; the new name and the old name can need not be visible at different places.

NOTE 2  
A task or protected object that is declared by an explicit object_declaration can be renamed as an object. However, a single task or protected object cannot be renamed since the corresponding type is anonymous (meaning it has no nameable subtypes). For similar reasons, an object of an anonymous array or access type cannot be renamed.

NOTE 3  
A subtype defined without any additional constraint can be used to achieve the effect of renaming another subtype (including a task or protected subtype) as in

```ada
subtype Mode is Ada.Text_IO.File_Mode;
```

Wording Changes from Ada 83

The second sentence of RM83-8.5.3, “At any point where a renaming declaration is visible, the identifier, or operator symbol of this declaration denotes the renamed entity.” is incorrect. It doesn't say directly visible. Also, such an identifier might resolve to something else.

The verbiage about renamings being legal “only if exactly one...”, which appears in RM83-8.5.4 (for objects) and RM83-8.5.7 (for subprograms) is removed, because it follows from the normal rules about overload resolution. For language lawyers, these facts are obvious; for programmers, they are irrelevant, since failing these tests is highly unlikely.

8.5.1 Object Renaming Declarations

[An object_renaming_declaration is used to rename an object or value.]

**Syntax**

object_renaming_declaration ::= 
  defining_identifier [: [null_exclusion] subtype_mark] renames object_name 
  [aspect_specification];

{AI95-00230-01} {AI95-00423-01} {AI05-0183-1} {AI12-0275-1} object_renaming_declaration ::= 
  defining_identifier : access_definition renames object_name 
  [aspect_specification];
Name Resolution Rules

{AI95-00230-01} {AI95-00254-01} {AI95-00409-01} {AI12-0275-1} The type of the object name shall resolve to the type determined by the subtype_mark. If no subtype mark or access_definition is present, the expected type of the object name is any type, or in the case where the type is defined by an access_definition, to an anonymous access type. If the anonymous access type is an access-to-object type, the type of the object name shall have the same designated type as that of the access_definition. If the anonymous access type is an access-to-subprogram type, the type of the object name shall have a designated profile that is type conformant with that of the access_definition.

{AI12-0275-1} In the case where the type is defined by an access_definition, the type of the object name shall resolve to an anonymous access type. If the anonymous access type is an access-to-object type, the type of the object name shall have the same designated type as that of the access_definition. If the anonymous access type is an access-to-subprogram type, the type of the object name shall have a designated profile that is type conformant with that of the access_definition.

Reason: A previous version of Ada 9X used the usual “expected type” wording: “The expected type for the object_name is that determined by the subtype_mark.”

We changed it so that this would be illegal:

X: T;
Y: T'Class renames X; -- Illegal!

When the above was legal, it was unclear whether Y was of type T or T'Class. Note that we still allow this:

Z: T'Class := ...;
W: T renames F(Z);

where F is a function with a controlling parameter and result. This is admittedly a bit odd.

Note that the matching rule for generic formal parameters of mode in out was changed to keep it consistent with the rule for renaming. That makes the rule different for in vs. in out.

Legality Rules

{AI12-0383-1} The renamed entity shall be an object or value.

{AI95-00231-01} {AI95-00409-01} {AI12-0383-1} In the case where the type is defined by an access_definition, the type of the renamed entity/object and the type defined by the access_definition shall both be access-to-object types with statically matching designated subtypes and with both or neither being access-to-constant types; or

• {AI95-00231-01} {AI95-00409-01} shall both be access-to-object types with statically matching designated subtypes and with both or neither being access-to-constant types; or

• {AI95-00409-01} shall both be access-to-subprogram types with subtype conformant designated profiles.

{AI95-00423-01} {AI12-0287-1} For an object renaming declaration with a null exclusion or an access_definition that has a null exclusion, the subtype of the object name shall exclude null. In addition, if the object renaming declaration occurs within the body of a generic unit G or within the body of a generic unit declared within the declarative region of generic unit G, then:

• {AI12-0287-1} if the object_name statically denotes a generic formal object of mode in out of a generic unit G, and the object renaming declaration occurs within the body of G or within the body of a generic unit declared within the declarative region of G, then the declaration of that the formal object of G shall have a null exclusion;

• {AI12-0287-1} if otherwise, the subtype of the object name statically denotes a call of a generic formal function of G, then the declaration of the result of that function shall have a null exclusion shall exclude null. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

Reason: {AI12-0287-1} {AI12-0005-1} These rules prevent “lying”. Null must never be the value of an object with an explicit null exclusion. The bullets are first bullet is an assume-the-worst rule which prevents trouble in twoone obscure cases.
type Acc_I is access Integer;
subtype Acc_NN_I is not null Acc_I;
Obj : Acc_I := null;
generic
  B : in out Acc_NN_I;
package Gen is

end Gen;
package body Gen is
  D : not null Acc_I renames B;
end Gen;
package Inst is new Gen (B => Obj);

{AI12-0287-1} Without the first bullet rule, D would be legal, and contain the value null, because the rule about lying is satisfied for generic matching (Obj matches B; B does not explicitly state not null). Legality Rules are not rechecked in the body of any instance, and the template passes the lying rule as well. The second bullet handles a similar case involving formal functions. The rules are so complex because they have to apply to formal values used in bodies of child generics as well as in the bodies of generics.

{AI12-0401-1} In the case where the object name is a qualified expression with a nominal subtype S and whose expression is a name that denotes an object Q:

- if S is an elementary subtype, then:
  - Q shall be a constant other than a dereference of an access type; or
  - the nominal subtype of Q shall be statically compatible with S; or
  - S shall statically match the base subtype of its type if scalar, or the first subtype of its type if an access type.

- if S is a composite subtype, then Q shall be known to be constrained or S shall statically match the first subtype of its type.

Ramification: There's no restriction if the expression is a value.

Reason: This check prevents the renamed object from violating its nominal subtype. As the subtype is only checked when the object is renamed, we make it illegal if the actual object is a variable whose value could be changed afterwards to violate the subtype. This is messy as “known to be constrained” is only defined for composite objects, so we have to handle elementary objects and all values separately.

{AI95-00184-01} {AI95-00363-01} {AI05-0008-1} {AI12-0401-1} The renamed entity shall not be a subcomponent that depends on discriminants of an object whose nominal subtype is unconstrained, unless the object is known to be constrained this subtype is indefinite, or the variable is constrained by its initial value aliased. A slice of an array shall not be renamed if this restriction disallows renaming of the array. In addition to the places where Legality Rules normally apply, these rules apply also in the private part of an instance of a generic unit. These rules also apply for a renaming that appears in the body of a generic unit, with the additional requirement that even if the nominal subtype of the variable is indefinite, its type shall not be a descendant of an untagged generic formal derived type.

{AI12-0401-1} In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

Discussion: This applies to all of the Legality Rules in this subclause. Rechecks are needed for most of the rules (but not the first two).

Reason: This prevents renaming of subcomponents that might disappear, which might leave dangling references. Similar restrictions exist for the Access attribute.
type T1 (D1 : Boolean) is
  record
    case D1 is
    when False =>
      C1 : Integer;
    when True =>
      null;
    end case;
  end record;
generic
  type F is new T1;
  X : in out F;
package G is
  C1_Ren : Integer renames X.C1;
end G;
type T2 (D2 : Boolean := False) is new T1 (D1 => D2);
Y : T2;
package I is new G (T2, Y);
Y := (D1 => True); -- Oops! What happened to I.C1_Ren?

{AI05-0008-1} In addition, the “known to be constrained” rules include assume-the-worst rules for generic bodies partially to prevent such problems.

Implementation Note: Note that if an implementation chooses to deallocate-then-reallocate on assignment-statement assigning to unconstrained definite objects, then it cannot represent renamings and access values as simple addresses, because the above rule does not apply to all components of such an object.

Ramification: If it is a generic formal object, then the assume-the-best or assume-the-worst rules are applied as appropriate.

Static Semantics

{AI95-00230-01} {AI95-00409-01} {AI12-0383-1} An object_renaming_declaration declares a new view [of the renamed entity object] whose properties are identical to those of the renamed view. [Thus, the properties of the renamed entity object are not affected by the renaming_declaration. In particular, its nominal subtype, whether it is a value or an object, its value if it is an object, and whether or not it is a constant, are unaffected; similarly, the null exclusion or constraints and other properties of its nominal subtype that apply to an object are not affected by renaming (any constraint implied by the subtype_mark or access_definition of the object_renaming_declaration is ignored).]

Discussion: Because the constraints are ignored, it is a good idea to use the nominal subtype of the renamed object when writing an object_renaming_declaration.

{AI95-00409-01} If no null_exclusion is given in the renaming, the object may or may not exclude null. This is similar to the way that constraints need not match, and constant is not specified. The renaming defines a view of the renamed entity, inheriting the original properties.

Examples

Example of renaming an object:

declare
  L : Person renames Leftmost_Person; -- see 3.10.1
begin
  L.Age := L.Age + 1;
end;

{AI12-0383-1} Example of renaming a value:

{AI12-0383-1} Uno renames One; -- see 3.3.2

Wording Changes from Ada 83

The phrase “subtype...as defined in a corresponding object declaration, component declaration, or component subtype indication”, from RM83-8.5(5), is incorrect in Ada 95; therefore we removed it. It is incorrect in the case of an object with an indefinite unconstrained nominal subtype:
Incompatibilities With Ada 95

{AI95-00363-01} Aliased variables are not necessarily constrained in Ada 2005 (see 3.6). Therefore, a subcomponent of an aliased variable may disappear or change shape, and renaming such a subcomponent thus is illegal, while the same operation would have been legal in Ada 95. Note that most allocated objects are still constrained by their initial value (see 4.8), and thus have no change in the legality of renaming for them. For example, using the type T2 of the previous example:

```ada
AT2 : aliased T2;
C1 Ren : Integer renames AT2.C1; -- Illegal in Ada 2005, legal in Ada 95
AT2 := (D1 => True);             -- Raised Constraint_Error in Ada 95,
-- but does not in Ada 2005; so C1 Ren becomes
-- invalid when this is assigned.
```

Extensions to Ada 95

{AI95-00230-01} {AI95-00231-01} A renaming can have an anonymous access type. In that case, the accessibility of the renaming is that of the original object (accessibility is not lost as it is for assignment to a component or stand-alone object).

{AI95-00231-01} A renaming can have a null_exclusion; if so, the renamed object must also exclude null, so that the null_exclusion does not lie. On the other hand, if the renaming does not have a null_exclusion, it excludes null if the renamed object does.

Wording Changes from Ada 95

{8652/0017} {AI95-00184-01} Corrigendum: Fixed to forbid renamings of depends-on-discriminant components if the type might be definite.

Incompatibilities With Ada 2005

{AI05-0008-1} Correction: Simplified the description of when a discriminant-dependent component is allowed to be renamed — it’s now simply when the object is known to be constrained. This fixes a confusion as to whether a subcomponent of an object that is not certain to be constrained can be renamed. The fix introduces an incompatibility, as the rule did not apply in Ada 95 if the prefix was a constant; but it now applies no matter what kind of object is involved. The incompatibility is not too bad, since most kinds of constants are known to be constrained.

Extensions to Ada 2005

{AI05-0183-1} An optional aspect_specification can be used in an object_renaming_declaration. This is described in 13.1.1.

Incompatibilities With Ada 2012

{AI12-0287-1} Correction: The Legality Rules for renames with null exclusions no longer applies to generic formal objects of mode in, but does apply to renames of generic formal functions. This means a few unlikely programs are now illegal that were previously allowed by original Ada 2012, while more programs that were previously illegal will be allowed.

{AI12-0401-1} Correction: Added a rule to ensure that a renaming of a qualified_expression of a variable is allowed only if the variable will always remain within the nominal subtype of the qualified_expression. This was not required in Ada 2012. Renamings that are now illegal are at risk of causing erroneous execution if the variable value is changed to a bad value; this is consistent with other rules preventing renamings from changing to violate their known properties.

Extensions to Ada 2012

{AI12-0275-1} The subtype_mark in an object renaming is now optional, as the subtype information it provides is not trustworthy anyway (that comes from the renamed object and there is no requirement that it is the same as that of the object).

{AI12-0383-1} An object renaming can now rename values, such as named numbers. The renamed entity still has to be a name, but an arbitrary expression can be renamed by qualifying it.

8.5.2 Exception Renaming Declarations

[An exception_renaming_declaration is used to rename an exception.]
8.5.2 Exception Renaming Declarations

Syntax

\{AI05-0183-1\} \texttt{exception\_renaming\_declaration ::=}
\texttt{defining\_identifier : exception renames exception\_name}
\texttt{[aspect\_specification];}

Legality Rules

The renamed entity shall be an exception.

Static Semantics

An \texttt{exception\_renaming\_declaration} declares a new view [of the renamed exception].

Examples

Example of renaming an exception:

\texttt{EOF : exception renames Ada.IO_Exceptions.End_Error; -- see A.13}

Extensions to Ada 2005

\{AI05-0183-1\} An optional \texttt{aspect\_specification} can be used in an \texttt{exception\_renaming\_declaration}. This is described in 13.1.1.

8.5.3 Package Renaming Declarations

[A \texttt{package\_renaming\_declaration} is used to rename a package.]

Syntax

\{AI05-0183-1\} \texttt{package\_renaming\_declaration ::=}
\texttt{package defining\_program\_unit\_name renames package\_name}
\texttt{[aspect\_specification];}

Legality Rules

The renamed entity shall be a package.

\{AI95-00217-06\} \{AI95-00412-01\} If the \texttt{package\_name} of a \texttt{package\_renaming\_declaration} denotes a limited view of a package \texttt{P}, then a name that denotes the \texttt{package\_renaming\_declaration} shall occur only within the immediate scope of the renaming or the scope of a \texttt{with\_clause} that mentions the package \texttt{P} or, if \texttt{P} is a nested package, the innermost library package enclosing \texttt{P}.

Discussion: The use of a renaming that designates a limited view is restricted to locations where we know whether the view is limited or nonlimited (based on a \texttt{with\_clause}). We don't want to make an implicit limited view, as those are not transitive like a regular view. Implementations should be able to see all limited views needed based on the \texttt{context\_clause}.

Static Semantics

A \texttt{package\_renaming\_declaration} declares a new view [of the renamed package].

\{AI95-00412-01\} [At places where the declaration of the limited view of the renamed package is visible, a name that denotes the \texttt{package\_renaming\_declaration} denotes a limited view of the package (see 10.1.1).]

\textbf{Proof:} This rule is found in 8.3, “Visibility”. 

\textit{Proof:} This rule is found in 8.3, “Visibility”.
Examples

Example of renaming a package:

```ada
package TM renames Table_Manager;
```

Wording Changes from Ada 95

6.a/2

{AI95-00217-06} {AI95-00412-01} Uses of renamed limited views of packages can only be used within the scope of a with_clause for the renamed package.

Extensions to Ada 2005

6.b/3

{AI05-0183-1} An optional aspect_specification can be used in a package_renaming_declaration. This is described in 13.1.1.

8.5.4 Subprogram Renaming Declarations

1/3

{AI05-0299-1} A subprogram_renaming_declaration can serve as the completion of a subprogram_declaration; such a renaming_declaration is called a renaming-as-body. A subprogram_renaming_declaration that is not a completion is called a renaming-as-declaration[, and is used to rename a subprogram (possibly an enumeration literal) or an entry].

1.a

Ramification: A renaming-as-body is a declaration, as defined in Clause 3.

Syntax

2/3

{AI95-00218-03} {AI05-0183-1} subprogram_renaming_declaration ::= 
  [overriding_indicator] 
  subprogram_specification renames callable_entity_name 
  [aspect_specification];

Name Resolution Rules

3

The expected profile for the callable_entity_name is the profile given in the subprogram_specification.

Legality Rules

4/5

{AI05-0239-1} {AI12-0373-1} The profile of a renaming-as-declaration shall be mode_conformant with that of the renamed callable entity.

4.1/2

{AI95-00423-01} For a parameter or result subtype of the subprogram_specification that has an explicit null_exclusion;

4.2/5

• {AI12-0287-1} if the callable_entity_name statically denotes a generic formal subprogram of a generic unit G, and the subprogram_renaming_declaration occurs within the body of a generic unit G or within the body of a generic unit declared within the declarative region of the generic unit G, then the corresponding parameter or result subtype of the formal subprogram of G shall have a null_exclusion;

4.3/2

• otherwise, the subtype of the corresponding parameter or result type of the renamed callable entity shall exclude null. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

4.a/2

Reason: This rule prevents ‘lying’. Null must never be the value of a parameter or result with an explicit null_exclusion. The first bullet is an assume-the-worst rule which prevents trouble in generic bodies (including bodies of child units) when the formal subtype excludes null implicitly.

5/3

{8652/0027} {8652/0028} {AI95-00135-01} {AI95-00145-01} {AI05-0239-1} The profile of a renaming-as-body shall be subtype_conformant with that of the renamed callable entity, and shall conform fully to that of the declaration it completes. If the renaming-as-body completes that declaration before the subprogram it declares is frozen, the profile shall be mode_conformant with that of the
renamed_callable_entity and the subprogram it declares takes its convention from the renamed subprogram; otherwise, the profile shall be subtype conformant subtype-conformant with that of the renamed callable entity and the convention of the renamed subprogram shall not be Intrinsic. A renaming-as-body is illegal if the declaration occurs before the subprogram whose declaration it completes is frozen, and the renaming renames the subprogram itself, through one or more subprogram renaming declarations, none of whose subprograms has been frozen.

Reason: The otherwise part of the second sentence first part of the first sentence is to allow an implementation of a renaming-as-body as a single jump instruction to the target subprogram. Among other things, this prevents a subprogram from being completed with a renaming of an entry. (In most cases, the target of the jump can be filled in at link time. In some cases, such as a renaming of a name like "A(I).all", an indirect jump is needed. Note that the name is evaluated at renaming time, not at call time.)

8652/0028 {AI95-00145-01} The first part of the second sentence is intended to allow renaming-as-body of predefined operators before the subprogram declaration is frozen. For some types (such as integer types), the parameter type for operators is the base type, and it would be very strange for

\[
\begin{align*}
\text{function Equal (A, B : in T) return Boolean;}
\end{align*}
\]

to be illegal. (Note that predefined operators cannot be renamed this way after the subprogram_declaration is frozen, as they have convention Intrinsic.)

The second part of the first sentence is the normal rule for completions of subprogram_declarations.

Ramification: An entry_declaration, unlike a subprogram_declaration, cannot be completed with a renaming_-declaration. Nor can a generic_subprogram_declaration.

The syntax rules prevent a protected subprogram declaration from being completed by a renaming. This is fortunate, because it allows us to avoid worrying about whether the implicit protected object parameter of a protected operation is involved in the conformance rules.

Reason: 8652/0027 {AI95-00135-01} Circular renames before freezing is illegal, as the compiler would not be able to determine the convention of the subprogram. Other circular renames are handled below; see Bounded (Run-Time) Errors.

\{AI95-00228-01\} The callable_entity_name of a renaming shall not denote a subprogram that requires overriding (see 3.9.3).

Reason: {AI95-00228-01} Such a rename cannot be of the inherited subprogram (which requires overriding because it cannot be called), and thus cannot squirrel away a subprogram (see below). That would be confusing, so we make it illegal. The renaming is allowed after the overriding, as then the name will denote the overriding subprogram, not the inherited one.

\{AI95-00228-01\} The callable_entity_name of a renaming-as-body shall not denote an abstract subprogram.

Reason: {AI95-00228-01} Such a subprogram has no body, so it hardly can replace one in the program.

\{AI12-0204-1\} If the callable_entity_name of a renaming is a prefixed view, the prefix of that view shall denote an object for which renaming is allowed.

Reason: {AI12-0204-1} The prefix in such a case is essentially renamed and passed to any calls of the renamed subprogram. If the prefix isn't legal to rename, that doesn't make sense (and allowing it might end up passing a nonexistent object to some calls).

A name that denotes a formal parameter of the subprogram_specification is not allowed within the callable_entity_name.

Reason: This is to prevent things like this:

\[
\begin{align*}
\text{function F(X : Integer) return Integer renames Table(X).all;}
\end{align*}
\]

A similar rule in 6.1 forbids things like this:

\[
\begin{align*}
\text{function F(X : Integer; Y : Integer := X) return Integer;}
\end{align*}
\]

Static Semantics

A renaming-as-declaration declares a new view of the renamed entity. The profile of this new view takes its subtypes, parameter modes, and calling convention from the original profile of the callable entity,
while taking the formal parameter names and default expressions from the profile given in the subprogram_renaming_declaration. The new view is a function or procedure, never an entry.

To be honest: When renaming an entry as a procedure, the compile-time rules apply as if the new view is a procedure, but the run-time semantics of a call are that of an entry call.

Ramification: For example, it is illegal for the entry_call_statement of a timed_entry_call to call the new view. But what looks like a procedure call will do things like barrier waiting.

All properties of the renamed entity are inherited by the new view unless otherwise stated by this document. In particular, if the renamed entity is abstract or requires overriding (see 3.9.3), the new view also is abstract or requires overriding. (The renaming will often be illegal in these cases, as a renaming cannot be overridden.) Similarly, if the renamed entity is not a program unit, then neither is the renaming. (Implicitly declared subprograms are not program units, see 10.1).

Dynamic Semantics

For a call to a subprogram whose body is given as a renaming-as-body, the execution of the renaming-as-body is equivalent to the execution of a subprogram_body that simply calls the renamed subprogram with its formal parameters as the actual parameters and, if it is a function, returns the value of the call.

Ramification: This implies that the subprogram completed by the renaming-as-body has its own elaboration check.

For a call on a renaming of a dispatching subprogram that is overridden, if the overriding occurred before the renaming, then the body executed is that of the overriding declaration, even if the overriding declaration is not visible at the place of the renaming; otherwise, the inherited or predefined subprogram is called. A corresponding rule applies to a call on a renaming of a predefined equality operator for an untagged record type.

Discussion: Note that whether or not the renaming is itself primitive has nothing to do with the renamed subprogram.

Note that the above rule is only for tagged types and equality of untagged record types.

Consider the following example:

package P is
  type T is tagged null record;
  function Predefined_Equal(X, Y : T) return Boolean renames "=";
  private
    function "="(X, Y : T) return Boolean; -- Override predefined ".=".
end P;

with P; use P;
package Q is
  function User_Defined_Equal(X, Y : T) return Boolean renames P."=";
end Q;
A call on Predefined_Equal will execute the predefined equality operator of T, whereas a call on User_Defined_Equal will execute the body of the overriding declaration in the private part of P.

Thus a renaming allows one to squirrel away a copy of an inherited or predefined subprogram before later overriding it.

Bounded (Run-Time) Errors

If a subprogram directly or indirectly renames itself, then it is a bounded error to call that subprogram. Possible consequences are that Program_Error or Storage_Error is raised, or that the call results in infinite recursion.

Reason: This has to be a bounded error, as it is possible for a renaming-as-body appearing in a package body to cause this problem. Thus it is not possible in general to detect this problem at compile time.

NOTE 1 A procedure can only be renamed as a procedure. A function whose defining_designator is either an identifier or an operator_symbol can be renamed with either an identifier or an operator_symbol; for renaming as an operator, the subprogram specification given in the renaming_declaration is subject to the rules given in 6.6 for operator declarations. Enumeration literals can be renamed as functions; similarly, attribute_references that denote functions (such as references to Succ and Pred) can be renamed as functions. An entry can only be renamed as a procedure; the new name is only

8.5.4 Subprogram Renaming Declarations 16 October 2023 486
allowed to appear in contexts that allow a procedure name. An entry of a family can be renamed, but an entry family cannot be renamed as a whole.

NOTE 2 The operators of the root numeric types cannot be renamed because the types in the profile are anonymous, so the corresponding specifications cannot be written; the same holds for certain attributes, such as Pos.

This paragraph was deleted.

NOTE 3 Calls with the new name of a renamed entry are procedure_call_statements and are not allowed at places where the syntax requires an entry_call_statement in conditional_ and timed_entry_calls, nor in an asynchronous_select; similarly, the Count attribute is not available for the new name.

NOTE 4 The primitiveness of a renaming-as-declaration is determined by its profile, and by where it occurs, as for any declaration of (a view of) a subprogram; primitiveness is not determined by the renamed view. In order to perform a dispatching call, the subprogram name has to denote a primitive subprogram, not a nonprimitive renaming of a primitive subprogram.

Reason: A subprogram_renaming_declaration could more properly be called renaming_as_subprogram_declaration, since you're renaming something as a subprogram, but you're not necessarily renaming a subprogram. But that's too much of a mouthful. Or, alternatively, we could call it a callable_entity_renaming_declaration, but that's even worse. Not only is it a mouthful, it emphasizes the entity being renamed, rather than the new view, which we think is a bad idea. We'll live with the oddity.

Examples

Examples of subprogram renaming declarations:

procedure My_Write(C : in Character) renames Pool(K).Write; -- see 4.1.3
function Real_Plus(Left, Right : Real) return Real renames "+";
function Int_Plus(Left, Right : Integer) return Integer renames "+";
function Rouge return Color renames Red; -- see 3.5.1
function Rot return Color renames Red;
function Rosso return Color renames Rouge;
function Next(X : Color) return Color renames Color'Succ; -- see 3.5.1

Example of a subprogram renaming declaration with new parameter names:

function "*" (X,Y : Vector) return Real renames Dot_Product; -- see 6.1

Example of a subprogram renaming declaration with a new default expression:

function Minimum(L : Link := Head) return Cell renames Min_Cell; -- see 6.1

Extensions to Ada 95

{8652/0028} {AI95-00145-01} Corrigendum: Allowed a renaming-as-body to be just mode conformant with the specification if the subprogram is not yet frozen.

{AI95-00218-03} Overriding_indicator (see 8.3.1) is optionally added to subprogram renamings.

Wording Changes from Ada 95

{8652/0014} {AI95-00064-01} Corrigendum: Described the semantics of renaming-as-body, so that the location of elaboration checks is clear.

{8652/0027} {AI95-00135-01} Corrigendum: Clarified that circular renaming-as-body is illegal (if it can be detected in time) or a bounded error.

{AI95-00228-01} Amendment Correction: Clarified that renaming a shall-be-overridden subprogram is illegal, as well as renaming-as-body an abstract subprogram.

{AI95-00423-01} Added matching rules for null_exclusions.

Inconsistencies With Ada 2005

{AI05-0123-1} Renaming of user-defined untagged record equality is now defined to call the overridden body so long as the overriding occurred before the renames. This could change the body called in unusual cases; the change is necessary to preserve the principle that the body called for an explicit call to “=” (via a renames in this case) is the same as the one inherited for a derived type and used in generics. Note that any renamings before the overriding will be unchanged. Any differences caused by the change will be rare and most likely will fix a bug.
Extensions to Ada 2005

21.g/3 {AI05-0183-1} An optional aspect_specification can be used in a subprogram_renaming_declaration. This is described in 13.1.1.

Incompatibilities With Ada 2012

21.h/5 {AI12-0204-1} Correction: Added a rule to ensure that the prefix of a renaming of a prefixed view continues to exist during the life of a renames. If the prefix is a subcomponent that depends on discriminants, Ada 2005 and 2012 would have allowed the prefix while Ada 2022 would not. Without this change, explicit forms (renaming the object and then using that in calls) would be safer than the renaming; that's inconsistent with other kinds of renaming.

Wording Changes from Ada 2012

21.i/5 {AI12-0287-1} Correction: Added wording to ensure that the object subject to a Legality Rule can be determined at compile-time. The alternative being nonsense, we treat this as a wording change.

8.5.5 Generic Renaming Declarations

1 [A generic_renaming_declaration is used to rename a generic unit.]

Syntax

2/3 {AI05-0183-1} generic_renaming_declaration ::= generic package defining_program_unit_name renames generic_package_name -- [aspect_specification];
| generic procedure defining_program_unit_name renames generic_procedure_name -- [aspect_specification];
| generic function defining_program_unit_name renames generic_function_name -- [aspect_specification];

Legality Rules

3 The renamed entity shall be a generic unit of the corresponding kind.

Static Semantics

4 A generic_renaming_declaration declares a new view [of the renamed generic unit].

5/5 NOTE {AI12-0440-1} Although the properties of the new view are the same as those of the renamed view, the place where the generic_renaming_declaration occurs can affect the legality of subsequent renamings and instantiations that denote the generic_renaming_declaration, in particular if the renamed generic unit is a library unit (see 10.1.1).

Examples

6 Example of renaming a generic unit:

7 generic package Enum_IO renames Ada.Text_IO Enumeration_IO; -- see A.10.10

Extensions to Ada 83

7.a Renaming of generic units is new to Ada 95. It is particularly important for renaming child library units that are generic units. For example, it might be used to rename Numerics.Generic_Elementary_Functions as simply Generic_Elementary_Functions, to match the name for the corresponding Ada-83-based package.

Wording Changes from Ada 83

7.b The information in RM83-8.6, “The Package Standard”, has been updated for the child unit feature, and moved to Annex A, except for the definition of “predefined type”, which has been moved to 3.2.1.

Extensions to Ada 2005

7.c/3 {AI05-0183-1} An optional aspect_specification can be used in a generic_renaming_declaration. This is described in 13.1.1.
8.6 The Context of Overload Resolution

{AI05-0299-1} [Because declarations can be overloaded, it is possible for an occurrence of a usage name to have more than one possible interpretation; in most cases, ambiguity is disallowed. This subclause describes how the possible interpretations resolve to the actual interpretation.]

Certain rules of the language (the Name Resolution Rules) are considered “overloading rules”. If a possible interpretation violates an overloading rule, it is assumed not to be the intended interpretation; some other possible interpretation is assumed to be the actual interpretation. On the other hand, violations of nonoverloading rules do not affect which interpretation is chosen; instead, they cause the construct to be illegal. To be legal, there usually has to be exactly one acceptable interpretation of a construct that is a “complete context”, not counting any nested complete contexts.

The syntax rules of the language and the visibility rules given in 8.3 determine the possible interpretations. Most type checking rules (rules that require a particular type, or a particular class of types, for example) are overloading rules. Various rules for the matching of formal and actual parameters are overloading rules.]


Language Design Principles

The type resolution rules are intended to minimize the need for implicit declarations and preference rules associated with implicit conversion and dispatching operations.

Name Resolution Rules

[Overload resolution is applied separately to each complete context, not counting inner complete contexts.] Each of the following constructs is a complete context:

- A context_item.

- A declarative_item or declaration.

  Ramification: A loop_parameter_specification is a declaration, and hence a complete context.

- A statement.

- A pragma_argument_association.

  Reason: We would make it the whole pragma, except that certain pragma arguments are allowed to be ambiguous, and ambiguity applies to a complete context.

- {AI12-0040-1} The selecting_expression of a case_statement or case_expression.

  Ramification: This means that the expression is resolved without looking at the choices.

- {AI12-0125-3} The variable_name of an assignment_statement A, if the expression of A contains one or more target_names.

An (overall) interpretation of a complete context embodies its meaning, and includes the following information about the constituents of the complete context, not including constituents of inner complete contexts:

- for each constituent of the complete context, to which syntactic categories it belongs, and by which syntax rules; and

  Ramification: Syntactic categories is plural here, because there are lots of trivial productions — an expression might also be all of the following, in this order: identifier, name, primary, factor, term, simple_expression, and relation. Basically, we're trying to capture all the information in the parse tree here, without using compiler-writer's jargon like “parse tree”.

- for each usage name, which declaration it denotes (and, therefore, which view and which entity it denotes); and
12.a/2 Ramification: {AI95-00382-01} In most cases, a usage name denotes the view declared by the denoted declaration. However, in certain cases, a usage name that denotes a declaration and appears inside the declarative region of that same declaration, denotes the current instance of the declaration. For example, within a task_body other than in an access_definition, a usage name that denotes the task_type_declaration denotes the object containing the currently executing task, and not the task type declared by the declaration.

13. for a complete context that is a declarative_item, whether or not it is a completion of a declaration, and (if so) which declaration it completes.

13.a Ramification: Unfortunately, we are not confident that the above list is complete. We'll have to live with that.

13.b To be honest: For “possible” interpretations, the above information is tentative.

13.c Discussion: A possible interpretation (an input to overload resolution) contains information about what a usage name might denote, but what it actually does denote requires overload resolution to determine. Hence the term “tentative” is needed for possible interpretations; otherwise, the definition would be circular.

14 A possible interpretation is one that obeys the syntax rules and the visibility rules. An acceptable interpretation is a possible interpretation that obeys the overloading rules[, that is, those rules that specify an expected type or expected profile, or specify how a construct shall resolve or be interpreted.]

14.a To be honest: One rule that falls into this category, but does not use the above-mentioned magic words, is the rule about numbers of parameter associations in a call (see 6.4).

14.b Ramification: The Name Resolution Rules are the ones that appear under the Name Resolution Rules heading. Some Syntax Rules are written in English, instead of BNF. No rule is a Syntax Rule or Name Resolution Rule unless it appears under the appropriate heading.

15 The interpretation of a constituent of a complete context is determined from the overall interpretation of the complete context as a whole. [Thus, for example, “interpreted as a function_call”, means that the construct’s interpretation says that it belongs to the syntactic category function_call.]

16 [Each occurrence of] a usage name denotes the declaration determined by its interpretation. It also denotes the view declared by its denoted declaration, except in the following cases:

16.a Ramification: As explained below, a pragma argument is allowed to be ambiguous, so it can denote several declarations, and all of the views declared by those declarations.

17.3 • {AI95-00382-01} {AI05-0287-1} If a usage name appears within the declarative region of a type_declaration and denotes that same type_declaration, then it denotes the current instance of the type (rather than the type itself). The current instance of a type is the object or value of the type that is associated with the execution that evaluates the usage name. Similarly, if a usage name appears within the declarative region of a subtype_declaration and denotes that same subtype_declaration, then it denotes the current instance of the subtype. These rules do not apply if the usage name appears within the subtype_mark of an access_definition for an access-to-object type, or within the subtype of a parameter or result of an access-to-subprogram type.

17.a/2 Reason: {AI95-00382-01} This is needed, for example, for references to the Access attribute from within the type_declaration. Also, within a task_body or protected_body, we need to be able to denote the current task or protected object. (For a single_task_declaration or single_protected_declaration, the rule about current instances is not needed.) We exclude anonymous access types so that they can be used to create self-referencing types in the natural manner (otherwise such types would be illegal).

17.b/2 Discussion: {AI95-00382-01} The phrase “within the subtype_mark” in the “this rule does not apply” part is intended to cover a case like access T'Class appearing within the declarative region of T: here T denotes the type, not the current instance.

17.1/5 {AI12-0068-1} {AI12-0324-1} {AI12-0427-1} Within an aspect specification for a type or subtype, the current instance represents a value of the type; it is not an object. Unless otherwise specified, the nominal subtype of this value is given by the subtype itself (the first subtype in the case of a type_declaration), prior to applying any predicate specified directly on the type or subtype. If the type or subtype is by-reference, the associated object of the value is the object associated (see 6.2) with the evaluation of the usage name.
Ramification: For the purposes of Legality Rules, the current instance acts as a value within an aspect_specification.

It might really be an object (and has to be for a by-reference type), but that isn’t discoverable by direct use of the name of the current instance.

- If a usage name appears within the declarative region of a generic_declaration (but not within its generic_formal_part) and it denotes that same generic_declaration, then it denotes the current_instance of the generic unit (rather than the generic unit itself). See also 12.3.

  To be honest: The current instance of a generic unit is the instance created by whichever generic_instantiation is of interest at any given time.

  Ramification: Within a generic_formal_part, a name that denotes the generic_declaration denotes the generic unit, which implies that it is not overloadable.

A usage name that denotes a view also denotes the entity of that view.

Ramification: Usually, a usage name denotes only one declaration, and therefore one view and one entity.

\{AI95-00231-01\} The expected type for a given expression, name, or other construct determines, according to the type_resolution_rules given below, the types considered for the construct during overload resolution. [The type resolution rules provide support for class-wide programming, universal numeric literals, dispatching operations, and anonymous access types:]

  Ramification: Expected types are defined throughout the RM95. The most important definition is that, for a subprogram, the expected type for the actual parameter is the type of the formal parameter.

  The type resolution rules are trivial unless either the actual or expected type is universal, class-wide, or of an anonymous access type.

- If a construct is expected to be of any type in a class of types, or of the universal or class-wide type for a class, then the type of the construct shall resolve to a type in that class or to a universal type that covers the class.

  Ramification: This matching rule handles (among other things) cases like the Val attribute, which denotes a function that takes a parameter of type universal_integer.

  The last part of the rule, “or to a universal type that covers the class” implies that if the expected type for an expression is universal_fixed, then an expression whose type is universal_real (such as a real literal) is OK.

- If the expected type for a construct is a specific type \( T \), then the type of the construct shall resolve either to \( T \), or:

  Ramification: This rule is not intended to create a preference for the specific type — such a preference would cause Beaujolais effects.

  - to \( T\)Class; or

  Ramification: This will only be legal as part of a call on a dispatching operation; see 3.9.2, “Dispatching Operations of Tagged Types”. Note that that rule is not a Name Resolution Rule.

  - to a universal type that covers \( T \); or

  \{AI95-00230-01\} \{AI95-00231-01\} \{AI95-00254-01\} \{AI95-00409-01\} when \( T \) is a specific anonymous access-to-object type (see 3.10) with designated type \( D \), to an access-to-object_variable type whose designated type is \( D\)Class or is covered by \( D\) or.

This paragraph was deleted Ramification: \{AI95-00409-01\} Because it says “access to variable” instead of “access to object”, two subprograms that differ only in that one has a parameter of an access to constant type, and the other has an access parameter, are distinguishable during overload resolution.

The case where the actual is access-to-\( D\)Class will only be legal as part of a call on a dispatching operation; see 3.9.2, “Dispatching Operations of Tagged Types”. Note that that rule is not a Name Resolution Rule.

- \{AI05-0149-1\} when \( T \) is a named general access-to-object type (see 3.10) with designated type \( D \), to an anonymous access-to-object type whose designated type covers or is covered by \( D \); or

- \{AI95-00254-01\} \{AI95-00409-01\} \{AI05-0239-1\} when \( T \) is an anonymous access-to-subprogram type (see 3.10), to an access-to-subprogram type whose designated profile is type conformanttype-conformant with that of \( T \).
In certain contexts, [such as in a subprogram_renaming_declaration,] the Name Resolution Rules define an expected profile for a given name; in such cases, the name shall resolve to the name of a callable entity whose profile is type conformant with the expected profile.

### Ramification: \{AI05-0239-1\}

The parameter and result subtypes are not used in overload resolution. Only type conformance of profiles is considered during overload resolution. Legality rules generally require at least mode conformance in addition, but those rules are not used in overload resolution.

### Legality Rules

#### \{AI95-00332-01\}

When the expected type for a construct is one that requires that its expected type to be a single type in a given class, the type of the construct shall be determinable solely from the context in which the construct appears, excluding the construct itself, but using the requirement that it be in the given class; the type of the construct is then this single expected type. Furthermore, the context shall not be one that expects any type in some class that contains types of the class of the construct; in particular, the context shall not be the operand of a type_conversion.

### Ramification: \{AI95-00230-01, AI12-0005-1\}

For example, the expected type for a characterstring literal is required to be a single characterstring type. But the expected type for the operand of a type_conversion is any type. Therefore, a characterstring literal is not allowed as the operand of a type_conversion. This is true even if there is only one characterstring type in scope (which is never the case). The reason for these rules is so that the compiler will not have to search “everywhere” to see if there is exactly one type in a class in scope.

#### Discussion: \{AI95-00332-01\}

The first sentence is carefully worded so that it only mentions “expected type” as part of identifying the interesting case, but doesn’t require that the context actually provide such an expected type. This allows such constructs to be used inside of constructs that don’t provide an expected type (like qualified expressions and renames). Otherwise, such constructs wouldn’t allow aggregates, ‘Access, and so on.

#### \{AI05-0102-1, AI05-0149-1, AI05-0299-1, AI12-0039-1\}

Other than for the tested simple_expression of a membership test, if the expected type for a name or expression is not the same as the actual type of the name or expression, the actual type shall be convertible to the expected type (see 4.6); further, if the expected type is a named access-to-object type with designated type \(D1\) and the actual type is an anonymous access-to-object type with designated type \(D2\), then \(D1\) shall cover \(D2\), and the name or expression shall denote a view with an accessibility level for which the statically deeper relationship applies; in particular it shall not denote an access parameter nor a stand-alone access object.

#### Reason:

This rule prevents an implicit conversion that would be illegal if it was an explicit conversion. For instance, this prevents assigning an access-to-constant value into a stand-alone anonymous access-to-variable object. It also covers convertibility of the designated type and accessibility checks.

#### Ramification:

This rule does not apply to expressions that don’t have expected types (such as the operand of a qualified expression or the expression of a renames). We don’t need a rule like this in those cases, as the type needs to be the same; there is no implicit conversion.

### A complete context shall have at least one acceptable interpretation; if there is exactly one, then that one is chosen.

#### Ramification:

This, and the rule below about ambiguity, are the ones that suck in all the Syntax Rules and Name Resolution Rules as compile-time rules. Note that this and the ambiguity rule have to be Legality Rules.

### There is a preference for the primitive operators (and ranges) of the root numeric types root_integer and root_real. In particular, if two acceptable interpretations of a constituent of a complete context differ only in that one is for a primitive operator (or range) of the type root_integer or root_real, and the other is not, the interpretation using the primitive operator (or range) of the root numeric type is preferred.

#### Reason:

The reason for this preference is so that expressions involving literals and named numbers can be unambiguous. For example, without the preference rule, the following would be ambiguous:
N : constant := 123;
if N > 100 then -- Preference for root_integer "<=" operator.
...
end if;

{AI05-0149-1} Similarly, there is a preference for the equality operators of the universal access type (see 4.5.2). If two acceptable interpretations of a constituent of a complete context differ only in that one is for an equality operator of the universal access type, and the other is not, the interpretation using the equality operator of the universal access type is preferred.

Reason: This preference is necessary because of implicit conversion from an anonymous access type to a named access type, which would allow the equality operator of any named access type to be used to compare anonymous access values (and that way lies madness).

For a complete context, if there is exactly one overall acceptable interpretation where each constituent's interpretation is the same as or preferred (in the above sense) over those in all other overall acceptable interpretations, then that one overall acceptable interpretation is chosen. Otherwise, the complete context is ambiguous.

A complete context other than a pragma_argument_association shall not be ambiguous.

A complete context that is a pragma_argument_association is allowed to be ambiguous (unless otherwise specified for the particular pragma), but only if every acceptable interpretation of the pragma argument is as a name that statically denotes a callable entity. Such a name denotes all of the declarations determined by its interpretations, and all of the views declared by these declarations.

Ramification: {AI95-00224-01} {AI05-0229-1} This applies to Inline, Suppress, Import, Export, and Convention pragmas. For example, it is OK to say "pragma Export(C, Entity_Name Suppress(Elaboration_Check, On => P.Q));", even if there are two directly visible P's, and there are two Q's declared in the visible part of each P. In this case, P.Q denotes four different declarations. This rule also applies to certain pragmas defined in the Specialized Needs Annexes. It almost applies to Pure, Elaborate_Body, and Elaborate_All pragmas, but those can't have overloading for other reasons. Note that almost all of these pragmas are obsolescent (see J.10 and J.15), and a major reason is that this rule has proven to be too broad in practice (it is common to want to specify something on a single subprogram of an overloaded set, that can't be done easily with this rule). Aspect_specifications, which are given on individual declarations, are preferred in Ada 2012.

Note that if a pragma argument denotes a call to a callable entity, rather than the entity itself, this exception does not apply, and ambiguity is disallowed.

Note that we need to carefully define which pragma-related rules are Name Resolution Rules, so that, for example, a pragma Inline does not pick up subprograms declared in enclosing declarative regions, and therefore make itself illegal.

We say "statically denotes" in the above rule in order to avoid having to worry about how many times the name is evaluated, in case it denotes more than one callable entity.

NOTE If a usage name has only one acceptable interpretation, then it denotes the corresponding entity. However, this does not mean that the usage name is necessarily legal since other requirements exist which are not considered for overload resolution; for example, the fact that an expression is static, whether an object is constant, mode and subtype conformance rules, freezing rules, order of elaboration, and so on.

Similarly, subtypes are not considered for overload resolution (the violation of a constraint does not make a program illegal but raises an exception during program execution).

Incompatibilities With Ada 83

The new preference rule for operators of root numeric types is upward incompatible, but only in cases that involved Beaujolais effects in Ada 83. Such cases are ambiguous in Ada 95.

Extensions to Ada 83

The rule that allows an expected type to match an actual expression of a universal type, in combination with the new preference rule for operators of root numeric types, subsumes the Ada 83 "implicit conversion" rules for universal types.
In Ada 83, it is not clear what the “syntax rules” are. AI83-00157 states that a certain textual rule is a syntax rule, but it's still not clear how one tells in general which textual rules are syntax rules. We have solved the problem by stating exactly which rules are syntax rules — the ones that appear under the “Syntax” heading.

RM83 has a long list of the “forms” of rules that are to be used in overload resolution (in addition to the syntax rules). It is not clear exactly which rules fall under each form. We have solved the problem by explicitly marking all rules that are used in overload resolution. Thus, the list of kinds of rules is unnecessary. It is replaced with some introductory (intentionally vague) text explaining the basic idea of what sorts of rules are overload rules.

[AI03-0299-1] It is not clear from RM83 what information is embodied in a “meaning” or an “interpretation”. “Meaning” and “interpretation” were intended to be synonymous; we now use the latter only in defining the rules about overload resolution. “Meaning” is used only informally. This subclause attempts to clarify what is meant by “interpretation”.

For example, RM83 does not make it clear that overload resolution is required in order to match subprogram_bodies with their corresponding declarations (and even to tell whether a given subprogram_body is the completion of a previous declaration). Clearly, the information needed to do this is part of the “interpretation” of a subprogram_body. The resolution of such things is defined in terms of the “expected profile” concept. Ada 95 has some new cases where expected profiles are needed — the resolution of P'Access, where P might denote a subprogram, is an example.

Ada 95 allowed name resolution to distinguish between anonymous access-to-variable and access-to-constant types. This is similar to distinguishing between subprograms with in and out parameters, which is known to be bad. Thus, that part of the rule was dropped as we now have anonymous access-to-constant types, making this much more likely.

In Ada 95, ambiguous in Ada 2005.

If there is any code like this (such code should be rare), it will be ambiguous in Ada 2005.
Generalized the anonymous access resolution rules to support the new capabilities of anonymous access types (that is, access-to-subprogram and access-to-constant).

We now allow the creation of self-referencing types via anonymous access types. This is an extension in unusual cases involving task and protected types. For example:

```ada
task type T;
task body T is
  procedure P (X : access T) is -- Illegal in Ada 95, legal in Ada 2005
... end P;
begin ...
... end T;
```

Corrected the “single expected type” so that it works in contexts that don’t have expected types (like object renames and qualified expressions). This fixes a hole in Ada 95 that appears to prohibit using aggregates, ‘Access, character literals, string literals, and allocators in qualified expressions.

Implicit conversion is now allowed from anonymous access-to-object types to general access-to-object types. Such conversions can make calls ambiguous. That can only happen when there are two visible subprograms with the same name and have profiles that differ only by a parameter that is of a named or anonymous access type, and the actual argument is of an anonymous access type. This should be rare, as many possible calls would be ambiguous even in Ada 2005 (including allocators and any actual of a named access type if the designated types are the same).

Implicit conversion is allowed from anonymous access-to-object types to general access-to-object types if the designated type is convertible and runtime checks are minimized. See also the incompatibilities section.

Added a requirement here that implicit conversions are convertible to the appropriate type. This rule was scattered about the Reference Manual, we moved a single generalized version here.

Corrigendum: Added a rule to specify that the current instance of a type or subtype is a value within an aspect specification. This could be inconsistent if a predicate or invariant uses the Constrained attribute on the current instance (it will always be False now, while it might have returned True in original Ada 2012). More likely, a usage of a current instance as a prefix of an attribute will become illegal (such as Size or Alignment). Any such code is very tricky. Moreover, as this is a new feature of Ada 2012, there are not that many predicates and invariants, and the ones that exist are very unlikely to be this tricky. Thus we do not believe that there will be any practical effect to this change, other than to explicitly allow common implementation strategies.

Corrigendum: Added wording to clarify that the selecting expression of a case expression is a complete context, just like that of a case statement. Clearly, everyone expects these to work the same way. Moreover, since it would be a lot of extra work to treat case expressions differently, it is quite unlikely that any compiler would implement the much more complicated resolution necessary (and we are not aware of any that did). Therefore, we didn’t document this as a potential incompatibility.

Added a resolution rule for target_name (see 5.2.1).
9 Tasks and Synchronization

{AI05-0299-1} {AI12-0119-1} {AI12-0330-1} The execution of an Ada program consists of the execution of one or more tasks. Each task represents a separable activity, separate thread of control that proceeds independently and concurrently between the points where it interacts with other tasks. A single task, when within the context of a parallel construct, can represent multiple logical threads of control which can proceed in parallel; in other contexts, each task represents one logical thread of control. The various forms of task interaction are described in this clause section, and include:

To be honest: The execution of an Ada program consists of the execution of one or more partitions (see 10.2), each of which in turn consists of the execution of an environment task and zero or more subtasks.

Term entry: logical thread of control — activity within the execution of a program that can proceed in parallel with other activities of the same task, or of separate tasks

{AI12-0119-1} The various forms of task interaction are described in this clause, and include:

• the activation and termination of a task;
• a call on a protected subprogram of a protected object, providing exclusive read-write access, or concurrent read-only access to shared data;
• a call on an entry, either of another task, allowing for synchronous communication with that task, or of a protected object, allowing for asynchronous communication with one or more other tasks using that same protected object;
• a timed operation, including a simple delay statement, a timed entry call or accept, or a timed asynchronous select statement (see next item);
• an asynchronous transfer of control as part of an asynchronous select statement, where a task stops what it is doing and begins execution at a different point in response to the completion of an entry call or the expiration of a delay;
• an abort statement, allowing one task to cause the termination of another task.

In addition, tasks can communicate indirectly by reading and updating (unprotected) shared variables, presuming the access is properly synchronized through some other kind of task interaction.

Static Semantics

The properties of a task are defined by a corresponding task declaration and task_body, which together define a program unit called a task unit.

Dynamic Semantics

{AI12-0119-1} Over time, tasks proceed through various states. A task is initially inactive; upon activation, and prior to its termination it is either blocked (as part of some task interaction) or ready to run. While ready, a task competes for the available execution resources that it requires to run. In the context of a parallel construct, a single task can utilize multiple processing resources simultaneously.

Discussion: {AI05-0229-1} The means for selecting which of the ready tasks to run, given the currently available execution resources, is determined by the task dispatching policy in effect, which is generally implementation defined, but may be controlled by aspects, pragmas, and operations defined in the Real-Time Annex (see D.2 and D.5).

NOTE {AI12-0119-1} {AI12-0440-1} Concurrent task execution can be implemented on multicomputers, multiprocessors, or with interleaved execution on a single physical processor. On the other hand, whenever an implementation can determine that the required semantic effects can be achieved when parts of the execution of a single logical thread of control of a given task are performed by different physical processors acting in parallel, it can choose to perform them in this way.

Wording Changes from Ada 83

The introduction has been rewritten.
We use the term "concurrent" rather than "parallel" when talking about logically independent execution of threads of control. The term "parallel" is reserved for referring to the situation where multiple physical processors run simultaneously.

Wording Changes from Ada 2012

(AI12-0119-1) Rewrote the introduction to emphasize that threads of control can be generated by parallel constructs as well as tasks.

9.1 Task Units and Task Objects

A task unit is declared by a task declaration, which has a corresponding task_body. A task declaration may be a task_type_declaration, in which case it declares a named task type; alternatively, it may be a single_task_declaration, in which case it defines an anonymous task type, as well as declaring a named task object of that type.

Syntax

(task_type_declaration ::= (AI95-00345-01) (AI105-0183-1) task_type_defining_identifier [known_discriminant_part]
   [aspect_specification] [is]
   [new interface_list with]
   _task_definition);

(single_task_declaration ::= (AI95-00399-01) (AI105-0183-1) (AI112-0446-1) task_defining_identifier
   [aspect_specification] [is]
   [new interface_list with]
   _task_definition);

task_definition ::= (AI95-00345-01)
   {task_item}
   [private
    {task_item}]
   end {task_identifier]

(task_item ::= (AI112-0446-1)
   entry_declaration | aspect_clause representation_clause

(task_body ::= (AI105-0267-1) task_defining_identifier
   [aspect_specification] is
   declarative_part
   begin
   handled_sequence_of_statements
   end [task_identifier];

If a task_identifier appears at the end of a task_definition or task_body, it shall repeat the defining_identifier.

Legality Rules

(AI95-00345-01) A task declaration requires a completion[, which shall be a task_body,] and every task_body shall be the completion of some task declaration.

This paragraph was deleted. To be honest: The completion can be a pragma Import, if the implementation supports it.
Paragraph 8 was deleted.

Static Semantics

A task_definition defines a task type and its first subtype. The first list of task_items of a task_definition, together with the known_discriminant_part, if any, is called the visible part of the task unit. [The optional list of task_items after the reserved word private is called the private part of the task unit.]

Proof: Private part is defined in Clause 8.

\{8652/0029\} \{AI95-00116-01\} For a task declaration without a task_definition, a task_definition without task_items is assumed.

\{AI95-00345-01\} \{AI95-00397-01\} \{AI95-00399-01\} \{AI95-00419-01\} \{AI05-0042-1\} For a task declaration with an interface_list, the task type inherits user-defined primitive subprograms from each progenitor_type (see 3.9.4), in the same way that a derived_type inherits user-defined primitive subprograms from its progenitor_types (see 3.4). If the first parameter of a primitive inherited subprogram is of the task type or an access parameter designating the task type, and there is an entry declaration for a single entry with the same identifier within the task declaration, whose profile is type conformant with the prefixed view profile of the inherited subprogram, the inherited subprogram is said to be implemented by the conforming task entry using an implicitly declared nonabstract subprogram which has the same profile as the inherited subprogram and which overrides it.

Ramification: The inherited subprograms can only come from an interface given as part of the task declaration.

Reason: The part about the implicitly declared subprogram is needed so that a subprogram implemented by an entry is considered to be overridden for the purpose of the other rules of the language. Without it, it would, for instance be illegal for an abstract subprogram to be implemented by an entry, because the abstract subprogram would not be overridden. The Legality Rules below ensure that there is no conflict between the implicit overriding subprogram and a user-defined overriding subprogram.

Legality Rules

\{AI95-00345-01\} A task declaration requires a completion[, which shall be a task_body,] and every task_body shall be the completion of some task declaration.

To be honest: \{AI05-0229-1\} [The completion can be a pragma Import, if the implementation supports it, the task_body can be imported (using aspect Import, see B.1), in which case no explicit task_body is allowed.]

\{AI95-00345-01\} \{AI95-00399-01\} [Each interface_subtype_mark of an interface_list appearing within a task declaration shall denote a limited interface type that is not a protected interface.]

Proof: 3.9.4 requires that an interface_list only name interface types, and limits the descendants of the various kinds of interface types. Only a limited, task, or synchronized interface can have a task type descendant. Nonlimited or protected interfaces are not allowed, as they offer operations that a task does not have.

\{AI95-00397-01\} \{AI05-0090-1\} The prefixed view profile of an explicitly declared primitive subprogram of a tagged task type shall not be type conformant with any entry of the task type, if the subprogram has the same defining name as the entry and the first parameter of the subprogram is of the task type or is an access parameter designating the task type.

Reason: This prevents the existence of two operations with the same name and profile which could be called with a prefixed view. If the operation was inherited, this would be illegal by the following rules; this rule puts inherited and noninherited routines on the same footing. Note that this only applies to tagged task types (that is, those with an interface in their declaration); we do that as there is no problem with prefixed view calls of primitive operations for “normal” task types, and having this rule apply to all tasks would be incompatible with Ada 95.

\{AI95-00345-01\} \{AI95-00399-01\} For each primitive subprogram inherited by the type declared by a task declaration, at most one of the following shall apply:

- \{AI95-00345-01\} the inherited subprogram is overridden with a primitive subprogram of the task type, in which case the overriding subprogram shall be subtype conformant with the inherited subprogram and not abstract; or
• \{AI95-00345-01\} \{AI95-00397-01\} the inherited subprogram is implemented by a single entry of the task type; in which case its prefixed view profile shall be subtype conformant with that of the task entry.

Ramification: An entry may implement two subprograms from the ancestors, one whose first parameter is of type \(T\) and one whose first parameter is of type \(\text{access} \ T\). That doesn't cause implementation problems because "implemented by" (unlike "overridden") probably entails the creation of wrappers.

9.9/2 If neither applies, the inherited subprogram shall be a null procedure. In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

Reason: Each inherited subprogram can only have a single implementation (either from overriding a subprogram or implementing an entry), and must have an implementation unless the subprogram is a null procedure.

Dynamic Semantics

[ The elaboration of a task declaration elaborates the task_definition. The elaboration of a single_task_-declaration also creates an object of an (anonymous) task type.]

Proof: This is redundant with the general rules for the elaboration of a full_type_declaration and an object_declaration.

[The elaboration of a task_definition creates the task type and its first subtype; it also includes the elaboration of the entry_declarations in the given order.]

{8652/0009} \{AI95-00137-01\} As part of the initialization of a task object, any aspect_clause, representation_clauses, and any per-object constraints associated with entry_-declarations of the corresponding task_definition are elaborated in the given order.

Reason: The only aspect_clause, representation_clauses defined for task entries are ones that specify the Address of an entry, as part of defining an interrupt entry. These clearly need to be elaborated per-object, not per-type. Normally the address will be a function of a discriminant, if such an Address clause is in a task type rather than a single task declaration, though it could rely on a parameterless function that allocates sequential interrupt vectors.

We do not mention representation pragmas, since each pragma may have its own elaboration rules.

The elaboration of a task_body has no effect other than to establish that tasks of the type can from then on be activated without failing the Elaboration_Check.

[The execution of a task_body is invoked by the activation of a task of the corresponding type (see 9.2.).]

The content of a task object of a given task type includes:

• The values of the discriminants of the task object, if any;

• An entry queue for each entry of the task object;

Ramification: "For each entry" implies one queue for each single entry, plus one for each entry of each entry family.

• A representation of the state of the associated task.

Note 1. \{AI95-00382-01\} Other than in an access_definition, the name of a task unit within the declaration or body of the task unit, the name of the task unit denotes the current instance of the unit (see 8.6), rather than the first subtype of the corresponding task type (and thus the name cannot be used as a subtype_mark).

Discussion: \{AI95-00382-01\} It can be used as a subtype_mark in an anonymous access type. In addition, however, it is possible to refer to some other subtype of the task type within its body, presuming such a subtype has been declared between the task_type_declaration and the task_body.

Note 2. The notation of a selected_component can be used to denote a discriminant of a task (see 4.1.3). Within a task unit, the name of a discriminant of the task type denotes the corresponding discriminant of the current instance of the unit.

Note 3. \{AI95-00242-01\} A task type is a limited type (see 7.5), and hence precludes use of assignment_statements and has neither an assignment operation nor predefined equality operators. If a programmer wants to write an application that stores and exchanges task identities, they can do so by defining an access type designating the corresponding task objects and by using access values for identification purposes. Assignment is
available for such an access type as for any access type. Alternatively, if the implementation supports the Systems Programming Annex, the Identity attribute can be used for task identification (see C.7).  

Examples

task type Server is
  entry Next_Work_Item(WI : in Work_Item);
  entry Shut_Down;
end Server;

{AI95-00433-01} task type Keyboard_Driver(ID : Keyboard_ID := New_ID) is
  new Serial_Device with -- see 3.9.4
  entry Read(C : out Character);
  entry Write(C : in  Character);
end Keyboard_Driver;

Examples of declarations of single tasks:

task Controller is
  entry Request(Level)(D : Item);  -- a family of entries
end Controller;
task Parser is
  entry Next_Lexeme(L : in  Lexical_Element);
  entry Next_Action(A : out Parser_Action);
end;
task User;  -- has no entries

Examples of task objects:

Agent    : Server;
Teletype : Keyboard_Driver(TTY_ID);
Pool     : array(1 .. 10) of Keyboard_Driver;

Example of access type designating task objects:

type Keyboard is access Keyboard_Driver;
Terminal : Keyboard := new Keyboard_Driver(Term_ID);

Extensions to Ada 83

The syntax rules for task declarations are modified to allow a known_discriminant_part, and to allow a private part. They are also modified to allow entry_declarations and aspect_clause, representation_clauses to be mixed.

Wording Changes from Ada 83

The syntax rules for tasks have been split up according to task types and single tasks. In particular: The syntax rules for task_declaration and task_specification are removed. The syntax rules for task_type_declaration, single_task_declaration, task_definition and task_item are new.

The syntax rule for task_body now uses the nonterminal handled_sequence_of_statements.

The declarative_part of a task_body is now required; that doesn't make any real difference, because a declarative_part can be empty.

Extensions to Ada 95

{AI95-00345-01} {AI95-00397-01} {AI95-00399-01} {AI95-00419-01} Task types and single tasks can be derived from one or more interfaces. Entries of the task type can implement the primitive operations of an interface. Overriding indicators can be used to specify whether or not an entry implements a primitive operation.

Wording Changes from Ada 95

Corrigendum: Clarified that a task type has an implicit empty task_definition if none is given.

Corrigendum: Changed representation clauses to aspect clauses to reflect that they are used for more than just representation.
9.2 Task Execution - Task Activation

Dynamic Semantics

The execution of a task of a given task type consists of the execution of the corresponding task_body. The initial part of this execution is called the activation of the task; it consists of the elaboration of the declarative_part of the task_body. Should an exception be propagated by the elaboration of its declarative_part, the activation of the task is defined to have failed, and it becomes a completed task.

A task object (which represents one task) can be a part of a stand-alone object, of an object created by a coextension of one of these. All tasks that are part of the evaluation of an allocator, or of an anonymous object of a limited type, or of an coextension of one of these, are activated together. All tasks that are part or coextensions of a single object that is not a stand-alone object are activated together. Similarly, all tasks created by the evaluation of a single allocator are activated together. The activation of a task is associated with the innermost allocator or object_declaration that is responsible for its creation.

Discussion: The initialization of an object_declaration or allocator can indirectly include the creation of other objects that contain tasks. For example, the default expression for a subcomponent of an object created by an allocator might call a function that evaluates a completely different allocator. Tasks created by the two allocators are not activated together.

For the tasks created by the elaboration of object Declarations of a given declarative region, the activations are initiated within the context of the handled_sequence_of_statements (and its associated exception_handlers if any — see 11.2), just prior to executing the statements of the handled_sequence_of_statements. [For a package without an explicit body or an implicit null_statement is assumed, as defined in 7.2.]

Ramification: If Tasking_Error is raised, it can be handled by handlers of the handled_sequence_of_statements.

For tasks that are part or coextensions of a single object that is not a stand-alone object, activations are initiated after completing any initialization of the outermost object enclosing these tasks, prior to performing any other operation on the outermost object. In particular, for tasks that are part or coextensions of the object created by the evaluation of an allocator, the activations are initiated as the last step of evaluating the allocator, after completing any initialization for the object created by the allocator, and prior to returning the new access value. For tasks that are part or coextensions of an object that is the result of a function call, the activations are not initiated until after the function returns.
Discussion: \{AI95-00416-01\} The intent is that “temporary” objects with task parts (or coextensions) are treated similarly to an object created by an allocator. The “whole” object is initialized, and then all of the task parts (including the coextensions) are activated together. Each such “whole” object has its own task activation sequence, involving the activating task being suspended until all the new tasks complete their activation.

The task that created the new tasks and initiated their activations (the activator) is blocked until all of these activations complete (successfully or not). Once all of these activations are complete, if the activation of any of the tasks has failed [(due to the propagation of an exception)], Tasking_Error is raised in the activator, at the place at which it initiated the activations. Otherwise, the activator proceeds with its execution normally. Any tasks that are aborted prior to completing their activation are ignored when determining whether to raise Tasking_Error.

Ramification: Note that a task created by an allocator does not necessarily depend on its activator; in such a case the activator’s termination can precede the termination of the newly created task.

Discussion: Tasking_Error is raised only once, even if two or more of the tasks being activated fail their activation.

To be honest: \{AI95-00265-01\} The pragma Partition Elaboration Policy (see H.6) can be used to defer task activation to a later point, thus changing many of these rules.

\{AI05-0045-1\} If the master that directly encloses the point where the activation of a task \(T\) would be initiated, completes before the activation of \(T\) is initiated, \(T\) becomes terminated and is never activated. Furthermore, if a return statement is left such that the return object is not returned to the caller, any task that was created as a part of the return object or one of its coextensions immediately becomes Should the task that created the new tasks never reach the point where it would initiate the activations (due to an abort or the raising of an exception), the newly created tasks become terminated and are never activated.

Ramification: \{AI05-0045-1\} The first case can only happen if the activation point of \(T\) is not reached due to an exception being raised or a task or statement being aborted. Note that this is exclusive; if the master completes normally and starts finalization, we’re already past the activation point.

\{AI05-0045-1\} The second case can happen with an exception being raised in a return statement, by an exit or goto from an extended return statement, or by a return statement being aborted. Any tasks created for the return object of such a return statement are never activated.

NOTE 1 An entry of a task can be called before the task has been activated.

NOTE 2 \{AI12-0442-1\} If several tasks are activated together, the execution of any of these tasks can proceed without waiting until need not wait the end of the activation of the other tasks.

NOTE 3 A task can become completed during its activation either because of an exception or because it is aborted (see 9.8).

Examples

Example of task activation:

```
procedure P is
  A, B : Server;  -- elaborate the task objects A, B
  C    : Server;  -- elaborate the task object C
begin
  -- the tasks A, B, C are activated together before the first statement
  ...
end;
```

Wording Changes from Ada 83

We have replaced the term suspended with blocked, since we didn't want to consider a task blocked when it was simply competing for execution resources. “Suspended” is sometimes used more generally to refer to tasks that are not actually running on some processor, due to the lack of resources.

\{AI05-0299-1\} This subclause has been rewritten in an attempt to improve presentation.

Wording Changes from Ada 95

\{AI95-00416-01\} Adjusted the wording for activating tasks to handle the case of anonymous function return objects. This is critical; we don't want to be waiting for the tasks in a return object when we exit the function normally.
9.2 Task Execution - Task Activation

9.3 Task Dependence - Termination of Tasks

Dynamic Semantics

Each task (other than an environment task — see 10.2) depends on one or more masters (see 7.6.1), as follows:

- If the task is created by the evaluation of an allocator for a given named access type, it depends on each master that includes the elaboration of the declaration of the ultimate ancestor of the given access type.

- If the task is created by the elaboration of an object_declaration, it depends on each master that includes this elaboration.

- Otherwise, the task depends on the master of the outermost object of which it is a part (as determined by the accessibility level of that object — see 3.10.2 and 7.6.1), as well as on any master whose execution includes that of the master of the outermost object.

Furthermore, if a task depends on a given master, it is defined to depend on the task that executes the master, and (recursively) on any master of that task.

Discussion: Don't confuse these kinds of dependences with the dependences among compilation units defined in 10.1.1, “Compilation Units - Library Units”.

A task is said to be completed when the execution of its corresponding task_body is completed. A task is said to be terminated when any finalization of the task_body has been performed (see 7.6.1). [The first step of finalizing a master (including a task_body) is to wait for the termination of any tasks dependent on the master.] The task executing the master is blocked until all the dependents have terminated. [Any remaining finalization is then performed and the master is left.]

Completion of a task (and the corresponding task_body) can occur when the task is blocked at a select_statement with an open terminate_alternative (see 9.7.1); the open terminate_alternative is selected if and only if the following conditions are satisfied:

- The task depends on some completed master; and

- Each task that depends on the master considered is either already terminated or similarly blocked at a select_statement with an open terminate_alternative.

When both conditions are satisfied, the task considered becomes completed, together with all tasks that depend on the master considered that are not yet completed.

Ramification: Any required finalization is performed after the selection of terminate_alternatives. The tasks are not calllable during the finalization. In some ways it is as though they were aborted.

NOTE 1 The full view of a limited private type can be a task type, or can have subcomponents of a task type. Creation of an object of such a type creates dependences according to the full type.

NOTE 2 An object_renaming_declaration defines a new view of an existing entity and hence creates no further dependence.

NOTE 3 The rules given for the collective completion of a group of tasks all blocked on select_statements with open terminate_alternatives ensure that the collective completion can occur only when there are no remaining active tasks that can call one of the tasks being collectively completed.
NOTE 4 If two or more tasks are blocked on select_statements with open terminate_alternatives, and become completed collectively, their finalization actions proceed concurrently.

NOTE 5 The completion of a task can occur due to any of the following:

- the raising of an exception during the elaboration of the declarative_part of the corresponding task_body;
- the completion of the handled_sequence_of_statements of the corresponding task_body;
- the selection of an open terminate_alternative of a select_statement in the corresponding task_body;
- the abort of the task.

Example of task dependence:

```ada
declare
    type Global is access Server; -- see 9.1
    A, B : Server;
    G    : Global;
begin
    -- activation of A and B
    declare
        type Local is access Server;
        X : Global := new Server; -- activation of X.all
        L : Local := new Server; -- activation of L.all
        C : Server;
    begin
        -- activation of C
        G := X; -- both G and X designate the same task object
        ...  
    end;  -- await termination of C and L.all (but not X.all)
    ...  
end;  -- await termination of A, B, and G.all
```

Wording Changes from Ada 83

We have revised the wording to be consistent with the definition of master now given in 7.6.1, “Completion and Finalization”.

Tasks that used to depend on library packages in Ada 83, now depend on the (implicit) task_body of the environment task (see 10.2). Therefore, the environment task has to wait for them before performing library level finalization and terminating the partition. In Ada 83 the requirement to wait for tasks that depended on library packages was not as clear.

What was "collective termination" is now "collective completion" resulting from selecting terminate_alternatives. This is because finalization still occurs for such tasks, and this happens after selecting the terminate_alternative, but before termination.

Wording Changes from Ada 95

{AI95-00416-01} Added missing wording that explained the master of tasks that are neither object_declarations nor allocators, such as function returns.

Wording Changes from Ada 2012

{AI12-0070-1} Corrigendum: Ensured that the master of tasks that are not allocators of named access types is correctly determined. (Ignoring the accessibility rules of 3.10.2 could not be intended.)

9.4 Protected Units and Protected Objects

A protected object provides coordinated access to shared data, through calls on its visible protected operations, which can be protected subprograms or protected entries. A protected unit is declared by a protected_declaration, which has a corresponding protected_body. A protected declaration may be a protected_type_declaration, in which case it declares a named protected type; alternatively, it may be a single_protected_declaration, in which case it defines an anonymous protected type, as well as declaring a named protected object of that type.
Syntax

protected_type_declaration ::= protected type defining_identifier [known_discriminant_part]
  | [aspect_specification] is
  | [new interface_list with]
  | protected_definition;

single_protected_declaration ::= protected defining_identifier
  | [aspect_specification] is
  | [new interface_list with]
  | protected_definition;

protected_definition ::= {protected_operation_declaration}
  | [private]
  | {protected_element_declaration; }
end [protected_identifier]

protected_operation_declaration ::= subprogram_declaration
  | entry_declaration
  | aspect_clause representation_clause

protected_element_declaration ::= protected_operation_declaration
  | component_declaration

Reason: We allow the operations and components to be mixed because that’s how other things work (for example, package declarations). We have relaxed the ordering rules for the items inside declarative_parts and task_definitions as well.

protected_body ::= protected body defining_identifier
  | [aspect_specification] is
  | {protected_operation_item; }
end [protected_identifier];

protected_operation_item ::= subprogram_declaration
  | subprogram_body
  | null_procedure_declaration
  | expression_function_declaration
  | entry_body
  | aspect_clause representation_clause

If a protected_identifier appears at the end of a protected_definition or protected_body, it shall repeat the defining_identifier.

Legality Rules

A protected declaration requires a completion[, which shall be a protected_body] and every protected_body shall be the completion of some protected declaration.

This paragraph was deleted. To be honest: The completion can be a pragma Import, if the implementation supports it.

Paragraph 10 was deleted.
A protected definition defines a protected type and its first subtype. The list of protected operation declarations of a protected definition, together with the known-discriminant part, if any, is called the visible part of the protected unit. [The optional list of protected element declarations after the reserved word private is called the private part of the protected unit.]

Proof: Private part is defined in Clause 8.

For a protected declaration with an interface list, the protected type inherits user-defined primitive subprograms from each progenitor type (see 3.9.4), in the same way that a derived type inherits user-defined primitive subprograms from its progenitor types (see 3.4). If the first parameter of a primitive inherited subprogram is of the protected type or an access parameter designating the protected type, and there is a protected operation declaration for a protected subprogram or single entry with the same identifier within the protected declaration, whose profile is type conformant with the prefixed view profile of the inherited subprogram, the inherited subprogram is said to be implemented by the conforming protected subprogram or entry using an implicitly declared nonabstract subprogram which has the same profile as the inherited subprogram and which overrides it.

Ramification: The inherited subprograms can only come from an interface given as part of the protected declaration.

Reason: For a protected declaration with an interface list, the protected type inherits user-defined primitive subprograms from each progenitor type (see 3.9.4), in the same way that a derived type inherits user-defined primitive subprograms from its progenitor types (see 3.4). If the first parameter of a primitive inherited subprogram is of the protected type or an access parameter designating the protected type, and there is a protected operation declaration for a protected subprogram or single entry with the same identifier within the protected declaration, whose profile is type conformant with the prefixed view profile of the inherited subprogram, the inherited subprogram is said to be implemented by the conforming protected subprogram or entry using an implicitly declared nonabstract subprogram which has the same profile as the inherited subprogram and which overrides it.

Legality Rules

A protected declaration requires a completion, which shall be a protected body, and every protected body shall be the completion of some protected declaration.

To be honest: If the completion can be a pragma Import, if the implementation supports it, the protected body can be imported (using aspect Import, see B.1), in which case no explicit protected body is allowed.

[Each interface subtype mark of an interface list appearing within a protected declaration shall denote a limited interface type that is not a task interface.]

Proof: 3.9.4 requires that an interface list only name interface types, and limits the descendants of the various kinds of interface types. Only a limited, protected, or synchronized interface can have a protected type descendant. Nonlimited or task interfaces are not allowed, as they offer operations that a protected type does not have.

The prefixed view profile of an explicitly declared primitive subprogram of a tagged protected type shall not be type conformant with any protected operation of the protected type, if the subprogram has the same defining name as the protected operation and the first parameter of the subprogram is of the protected type or is an access parameter designating the protected type.

Reason: This prevents the existence of two operations with the same name and profile which could be called with a prefixed view. If the operation was inherited, this would be illegal by the following rules; this rule puts inherited and noninherited routines on the same footing. Note that this only applies to tagged protected types (that is, those with an interface in their declaration); we do that as there is no problem with prefixed view calls of primitive operations for “normal” protected types, and having this rule apply to all protected types would be incompatible with Ada 95.

For each primitive subprogram inherited by the type declared by a protected declaration, at most one of the following shall apply:

- the inherited subprogram is overridden with a primitive subprogram of the protected type, in which case the overriding subprogram shall be subtype conformant with the inherited subprogram and not abstract; or
9.4 Protected Units and Protected Objects

11.7/2 • \{AI95-00345-01\} \{AI95-00397-01\} the inherited subprogram is implemented by a protected
subprogram or single entry of the protected type, in which case its prefixed view profile shall be
subtype conformant with that of the protected subprogram or entry.

11.8/2 If neither applies, the inherited subprogram shall be a null procedure. In addition to the places where
Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a
generic unit.

11.f/2  **Reason:** Each inherited subprogram can only have a single implementation (either from overriding a subprogram,
implementing a subprogram, or implementing an entry), and must have an implementation unless the subprogram is a
null procedure.

11.9/3 \{AI95-00345-01\} \{AI05-0291-1\} If an inherited subprogram is implemented by a protected procedure or
an entry, then the first parameter of the inherited subprogram shall be of mode **out** or **in out**, or an access-
to-variable parameter. If an inherited subprogram is implemented by a protected function, then the first
parameter of the inherited subprogram shall be of mode **in**, but not an access-to-variable parameter.

11.g/3  **Reason:** For a protected procedure or entry, the protected object can be read or written (see 9.5.1). A subprogram that
is implemented by a protected procedure or entry must have a profile which reflects that in order to avoid confusion.
Similarly, a protected function has a parameter that is a constant, and the inherited routine should reflect that.

11.10/2 \{AI95-00397-01\} If a protected subprogram declaration has an **overriding_indicator**, then at the point of
the declaration:

11.11/2 • if the **overriding_indicator** is **overriding**, then the subprogram shall implement an inherited
subprogram;

11.12/2 • if the **overriding_indicator** is **not overriding**, then the subprogram shall not implement any
inherited subprogram.

11.13/2 In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the
private part of an instance of a generic unit.

11.h/2  **Discussion:** These rules are subtly different than those for subprograms (see 8.3.1) because there cannot be “late”
inheritance of primitives from interfaces. Hidden (that is, private) interfaces are prohibited explicitly (see 7.3), as are
hidden primitive operations (as private operations of public abstract types are prohibited — see 3.9.3).

12  Dynamic Semantics

12.a [The elaboration of a protected declaration elaborates the **protected_definition**. The elaboration of a
**single_protected_declaration** also creates an object of an (anonymous) protected type.]

12.a  **Proof:** This is redundant with the general rules for the elaboration of a **full_type_declaration** and an
**object_declaration**.

13  [The elaboration of a **protected_definition** creates the protected type and its first subtype; it also includes
the elaboration of the **component Declarations** and **protected Operation Declarations** in the given order.

14  [As part of the initialization of a protected object, any per-object constraints (see 3.8) are elaborated.]

14.a  **Discussion:** We do not mention pragmas since each pragma has its own elaboration rules.

15  The elaboration of a **protected_body** has no other effect than to establish that protected operations of the
type can from then on be called without failing the **Elaboration_Check**.

16  The content of an object of a given protected type includes:

17  • The values of the components of the protected object, including (implicitly) an entry queue for
each entry declared for the protected object;

17.a  **Ramification:** "For each entry" implies one queue for each single entry, plus one for each entry of each entry family.

18  • A representation of the state of the execution resource **associated** with the protected object (one
such resource is associated with each protected object).
[The execution resource associated with a protected object has to be acquired to read or update any components of the protected object; it can be acquired (as part of a protected action — see 9.5.1) either for concurrent read-only access, or for exclusive read-write access.]

As the first step of the finalization of a protected object, each call remaining on any entry queue of the object is removed from its queue and Program_Error is raised at the place of the corresponding entry_call_statement.

Reason: This is analogous to the raising of Tasking_Error in callers of a task that completes before accepting the calls. This situation can only occur due to a requeue (ignoring premature unchecked_deallocation), since any task that has accessibility to a protected object is awaited before finalizing the protected object. For example:

```ada
procedure Main is
  task T is
    entry E;
  end T;
  task body T is
    protected PO is
      entry Ee;
    end PO;
    protected body PO is
      entry Ee when False is
        begin
          null;
        end PO;
      begin
        accept E do
          requeue PO.Ee;
        end E;
    end T;
  begin
    T.E;
  end Main;
```

{AI05-0005-1} The environment task is queued on PO.Ee when PO is finalized.

In a real example, a server task might park callers on a local protected object for some useful purpose, so we didn't want to disallow this case.

Bounded (Run-Time) Errors

{AI95-00280-01} It is a bounded error to call an entry or subprogram of a protected object after that object is finalized. If the error is detected, Program_Error is raised. Otherwise, the call proceeds normally, which may leave a task queued forever.

Reason: This is very similar to the finalization rule. It is a bounded error so that an implementation can avoid the overhead of the check if it can ensure that the call still will operate properly. Such an implementation cannot need to return resources (such as locks) to an executive that it needs to execute calls.

This case can happen (and has happened in production code) when a protected object is accessed from the Finalize routine of a type. For example:

```ada
with Ada.Finalization.Controlled;
package Window_Manager is
  type Root_Window is new Ada.Finalization.Controlled with private;
  type Any_Window is access all Root_Window;
  type Lock is
    entry Get_Lock;
    procedure Free_Lock;
  protected type Lock is
    entry Get_Lock;
    procedure Free_Lock;
  private
    procedure Finalize (Object : in out Root_Window);
  end Window_Manager;
package body Window_Manager is
  protected body Lock is
    entry Get_Lock;
    procedure Free_Lock;
  end Lock;
```
Window_Lock : Lock;

procedure Finalize (Object : in out Root_Window) is
begin
Window_Lock.Get_Lock;
...
Window_Lock.Free_Lock;
end Finalize;
...
A_Window : Any_Window := new Root_Window;
end Window_Manager;

The environment task will call Window_Lock for the object allocated for A_Window when the collection for Any Window is finalized, which will happen after the finalization of Window_Lock (because finalization of the package body will occur before that of the package specification).

NOTE 1 |AI95-00382-01| Within the declaration or body of a protected unit other than in an access_definition, the name of the protected unit denotes the current instance of the unit (see 8.6), rather than the first subtype of the corresponding protected type (and thus the name cannot be used as a subtype_mark).

Discussion: |AI95-00382-01| It can be used as a subtype_mark in an anonymous access type. In addition, it is possible to refer to some other subtype of the protected type within its body, presuming such a subtype has been declared between the protected_type_declaration and the protected_body.

NOTE 2 A selected_component can be used to denote a discriminant of a protected object (see 4.1.3). Within a protected unit, the name of a discriminant of the protected type denotes the corresponding discriminant of the current instance of the unit.

NOTE 3 |AI95-00287-01| A protected type is a limited type (see 7.5), and hence precludes use of assignment_statements and has neither an assignment operation nor predefined equality operators.

NOTE 4 The bodies of the protected operations given in the protected_body define the actions that take place upon calls to the protected operations.

NOTE 5 The declarations in the private part are only visible within the private part and the body of the protected unit.

Reason: Component_declarations are disallowed in a protected_body because, for efficiency, we wish to allow the compiler to determine the size of protected objects (when not dynamic); the compiler cannot necessarily see the body. Furthermore, the semantics of initialization of such objects would be problematic — we do not wish to give protected objects complex initialization semantics similar to task activation.

The same applies to entry_declarations, since an entry involves an implicit component — the entry queue.

Example of declaration of protected type and corresponding body:

protected type Resource is
entry Seize;
procedure Release;
private
Busy : Boolean := False;
end Resource;

protected body Resource is
entry Seize when not Busy is
begin
Busy := True;
end Seize;
procedure Release is
begin
Busy := False;
end Release;
end Resource;

Example of a single protected declaration and corresponding body:

{AI12-0430-1} protected Shared_Array is
-- Index, Item, and Item_Array are global types
function Component (N : in Index) return Item;
procedure Set_Component(N : in Index; E : in Item);
private
Table : Item_Array(Index) := (others => Null_Item);
end Shared_Array;
protected body Shared_Array is
  function Component(N : in Index) return Item is
  begin
    return Table(N);
  end Component;

  procedure Set_Component(N : in Index; E : in Item) is
  begin
    Table(N) := E;
  end Set_Component;
end Shared_Array;

Examples of protected objects:
Control : Resource;
Flags : array(1 .. 100) of Resource;

Extensions to Ada 83
{AI05-0299-1} This entire subclause is new; protected units do not exist in Ada 83.

Extensions to Ada 95
{AI95-00345-01} {AI95-00397-01} {AI95-00399-01} {AI95-00401-01} {AI95-00419-01} Protected types and single protected objects can be derived from one or more interfaces. Operations declared in the protected type can implement the primitive operations of an interface. Overriding indicators can be used to specify whether or not a protected operation implements a primitive operation.

Wording Changes from Ada 95
{8652/0009} {AI95-00137-01} Corrigendum: Changed representation clauses to aspect clauses to reflect that they are used for more than just representation.

{AI95-00280-01} Described what happens when an operation of a finalized protected object is called.

{AI95-00287-01} Revised the note on operations of protected types to reflect that limited types do have an assignment operation, but not copying (assignment statements).

{AI95-00382-01} Revised the note on use of the name of a protected type within itself to reflect the exception for anonymous access types.

Incompatibilities With Ada 2005
{AI05-0291-1} Correction: When an inherited subprogram is implemented by a protected function, the first parameter has to be an in parameter, but not an access-to-variable type. Original Ada 2005 allowed access-to-variable parameters in this case; the parameter will need to be changed to access-to-constant with the addition of the constant keyword.

Extensions to Ada 2005
{AI05-0183-1} {AI05-0267-1} An optional aspect specification can be used in a protected type declaration, a single_protected_declaration, and a protected body. This is described in 13.1.1.

Wording Changes from Ada 2005
{AI05-0042-1} Correction: Clarified that an inherited subprogram of a progenitor is overridden when it is implemented by an entry or subprogram.

{AI05-0090-1} Correction: Added the missing defining name in the no conflicting primitive operation rule.

Extensions to Ada 2012
{AI12-0147-1} {AI12-0005-1} Corrigendum: Null procedures and expression functions are allowed in protected bodies. We consider this an omission, as there is no reason why the convenient shorthand notations should not be allowed in this context.

9.5 Intertask Communication
The primary means for intertask communication is provided by calls on entries and protected subprograms. Calls on protected subprograms allow coordinated access to shared data objects. Entry calls
allow for blocking the caller until a given condition is satisfied (namely, that the corresponding entry is open — see 9.5.3), and then communicating data or control information directly with another task or indirectly via a shared protected object.

**Static Semantics**

{AI05-0225-1} {AI05-0291-1} When a name or prefix denotes any call on an entry, or on a protected subprogram, or a prefixed view of a primitive subprogram of a limited interface whose first parameter is a controlling parameter, the name or prefix determines a target object for the operation, which is either a task (for an entry call) or a protected object (for an entry call or a protected subprogram call). The target object is considered an implicit parameter to the operation, and is determined by the operation name (or prefix) used in the call on the operation, as follows:

To be honest: {AI05-0291-1} This wording uses "denotes" to mean "denotes a view of an entity" (when the term is used in Legality Rules), and "denotes an entity" (when the term is used in Dynamic Semantics rules). It does not mean "view of a declaration", as that would not include renames (a renames is not an entry or protected subprogram).

• {AI05-0291-1} If it is a direct_name or expanded name that denotes the declaration (or body) of the operation, then the target object is implicitly specified to be the current instance of the task or protected unit immediately enclosing the operation; such a call using such a name is defined to be an internal call;

• {AI05-0291-1} If it is a selected_component that is not an expanded name, then the target object is explicitly specified to be the task or protected object denoted by the prefix of the name; such a call using such a name is defined to be an external call;

Discussion: For example:

```ada
protected type Pt is
  procedure Op1;
  procedure Op2;
end Pt;
end Pt;
```

other_object : some_other_protected_type;

```ada
protected body Pt is
  procedure Op1 is begin ... end Op1;
end Op2 is
begin
  Op1; -- An internal call.
  Pt.Op1; -- Another internal call.
  PO.Op1; -- An external call. If the current instance is PO, then
  this is a bounded error (see 9.5.1).
  other_object.some_op; -- An external call.
end Op2;
```

• {AI05-0291-1} If the name or prefix is a dereference (implicit or explicit) of an access-to-protected-subprogram value, then the target object is determined by the prefix of the Access attribute_reference that produced the access value originally; a-and the call using such a name is defined to be an external call;

• If the name or prefix denotes a subprogram_renaming_declaration, then the target object is as determined by the name of the renamed entity.

A corresponding definition of target object applies to a requeue_statement (see 9.5.4), with a corresponding distinction between an internal requeue and an external requeue.
Legality Rules

\{AI95-00345-01\} \{AI05-0225-1\} \{AI05-0291-1\}  If a name or prefix determines a target object, and the name denotes the view of the target protected object associated with a call of a protected entry procedure or procedure, then the target object entry shall be a variable, unless the prefix is for an attribute reference to the Count attribute (see 9.9).

**Reason:** \{AI05-0225-1\} The point is to prevent any calls to such a name whose target object is a constant view of a protected object, directly, or via an access value, renames, or generic formal subprogram. It is, however, legal to say P'Count in a protected function body, even though the protected object is a constant view there.

**Ramification:** \{AI05-0291-1\} This rule does not apply to calls that are not to a prefixed view. Specifically a "normal" call to a primitive operation of a limited interface is not covered by this rule. In that case, the normal parameter passing mode checks will prevent passing a constant protected object to an operation implemented by a protected entry or procedure as the mode is required to be in `out` or `out`.

\{AI12-0166-1\} An internal call on a protected function shall not occur within a precondition expression (see 6.1.1) of a protected operation nor within a default expression of a parameter specification of a protected operation.

**Reason:** \{AI125-0166-1\} These calls will be made before the start of the protected action, and thus would not be subject to the expected mutual exclusion. As such, they would be an automatic race condition (the state of the called object could change before the start of the protected action for the call on the protected entry or subprogram).

**To be honest:** \{AI125-0166-1\} 6.1.1 actually defines "specific precondition expression" and "class-wide precondition expression". This rule is intended to apply to both.

Dynamic Semantics

Within the body of a protected operation, the current instance (see 8.6) of the immediately enclosing protected unit is determined by the target object specified (implicitly or explicitly) in the call (or requeue) on the protected operation.

**To be honest:** The current instance is defined in the same way within the body of a subprogram declared immediately within a protected body.

Any call on a protected procedure or entry of a target protected object is defined to be an update to the object, as is a requeue on such an entry.

**Reason:** Read/write access to the components of a protected object is granted while inside the body of a protected procedure or entry. Also, any protected entry call can change the value of the Count attribute, which represents an update. Any protected procedure call can result in servicing the entries, which again might change the value of a Count attribute.

Syntax

\{AI05-0030-2\} \{AI05-0215-1\}  \begin{verbatim}
synchronization_kind ::= By_Entry | By_Protected_Procedure | Optional
\end{verbatim}

\{AI05-0215-1\} For the declaration of a primitive procedure of a synchronized tagged type the following language-defined representation aspect may be specified with an aspect specification (see 13.1.1):

**Synchronization**

If specified, the aspect definition shall be a `synchronization_kind`.

**Aspect Description for Synchronization:** Defines whether a given primitive operation of a synchronized interface will must be implemented by an entry or protected procedure.

\{AI05-0030-2\} \{AI05-0215-1\} Inherited subprograms inherit the Synchronization aspect, if any, from the corresponding subprogram of the parent or progenitor type. If an overriding operation does not have a directly specified Synchronization aspect then the Synchronization aspect of the inherited operation is inherited by the overriding operation.
### Legality Rules

14/3 \{AI05-0030-2\} \{AI05-0215-1\} The synchronization kind By Protected Procedure shall not be applied to a primitive procedure of a task interface.

15/3 \{AI05-0030-2\} \{AI05-0215-1\} A procedure for which the specified synchronization kind is By Entry shall be implemented by an entry. A procedure for which the specified synchronization kind is By Protected Procedure shall be implemented by a protected procedure. A procedure for which the specified synchronization kind is Optional may be implemented by an entry or by a procedure (including a protected procedure).

16/3 \{AI05-0030-2\} \{AI05-0215-1\} If a primitive procedure overrides an inherited operation for which the Synchronization aspect has been specified to be By Entry or By Protected Procedure, then any specification of the aspect Synchronization applied to the overriding operation shall have the same synchronization kind.

17/3 \{AI05-0030-2\} In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

### Static Semantics

18/5 \{AI12-0064-2\} \{AI12-0374-2\} For a program unit, task entry, formal package, formal subprogram, formal object of an anonymous access-to-subprogram type, enumeration literal, and for a subtype (including a formal subtype), the following language-defined operational aspect is defined:

19/5 Nonblocking

This aspect specifies the blocking restriction for the entity; it shall be specified by a static Boolean expression. [The aspect definition can be omitted from the specification of this aspect; in that case, the aspect for the entity is True.]

Aspect Description for Nonblocking: Specifies that an associated subprogram does not block.

Proof: 13.1.1 allows omitting the aspect expression for any aspect with type Boolean; we take advantage of that here.

\{AI12-0064-2\} The Nonblocking aspect may be specified for all entities for which it is defined, except for protected operations and task entries. In particular, Nonblocking may be specified for generic formal parameters.

20/5 Ramification: The Nonblocking aspect cannot be specified for predefined operators or enumeration literals but we don't need to mention that above. One would have to declare a subprogram in order to specify the aspect in those cases, but that defines a user-defined subprogram which is itself not a predefined operator or an enumeration literal.

\{AI12-0064-2\} \{AI12-0374-2\} \{AI12-0439-1\} When aspect Nonblocking is False for an entity, the entity can contain a potentially blocking operation; such an entity allows blocking.

If the aspect is True for an entity, the entity is said to be nonblocking.

Ramification: Specifying Nonblocking as False imposes no restrictions. Specifying Nonblocking as True imposes additional compile-time checks to prevent blocking, but does not prevent deadlock. A pragma Detect Blocking can be used to ensure that Program Error is raised in a deadlock situation.

\{AI12-0064-2\} \{AI12-0374-2\} For a generic instantiation and entities declared within such an instance, the aspect is determined by the Nonblocking aspect for the corresponding entity of the generic unit, anded with the Nonblocking aspects of the actual generic parameters used by the entity. If the aspect is directly specified for an instance, the specified expression shall have the same value as the Nonblocking aspect of the instance (after anding with the aspects of the used actual parameters). In the absence of a Use Formal aspect, all actual generic parameters are presumed to be used by an entity (see H.7.1).

Reason: We want to allow confirming aspects for instances, but nothing else. The Legality Rules of the generic body were checked assuming the Nonblocking aspect of the generic unit combined with the Nonblocking aspects of the formals where they are used, and if that is overridden on the instance, the instance body might make calls that allow blocking in subprograms that are declared nonblocking.
For a (protected or task) entry, the Nonblocking aspect is False.

Reason: An entry can be renamed as a procedure, so the value of the aspect has to be well-defined (as the attribute can be applied to a procedure). We do not want a nonblocking subprogram to be able to call an entry, no matter how it occurs, so the value ought to be False. Moreover, we do not want a subprogram that renames an entry to be able to override a nonblocking subprogram. We could have used individual rules for these cases, but there were already many of them, and this solution avoids the need for extra rules for entries.

For an enumeration literal, the Nonblocking aspect is True.

Reason: Enumeration literals can be renamed as functions, and passed to generic formal functions, so we need to define the value of the aspect to ensure the other rules are meaningful.

For a predefined operator of an elementary type, the Nonblocking aspect is True. For a predefined operator of a composite type, the Nonblocking aspect of the operator is the same as the Nonblocking aspect for the type.

Reason: Predefined operators of elementary types can never include any potentially blocking operations, so we want them to declare that. Record equality can be composed of operations including user-defined "=" operators, which might allow blocking. Array equality might use some record equality. So we have to have the possibility of allowing blocking for them. We don't just copy the Nonblocking aspect of the type in every case, as someone could declare an elementary type to allow blocking.

Ramification: It's not possible to specify the nonblocking expression of a predefined operator; if an operator is declared in order to do that, it is no longer predefined.

For a dereference of an access-to-subprogram type, the Nonblocking aspect of the designated subprogram is that of the access-to-subprogram type.

For the base subtype of a scalar (sub)type, the Nonblocking aspect is True.

Reason: The first subtype of a scalar type can allow blocking (which can be useful so a predicate can allow blocking), but the base subtype is always Nonblocking. We need this so the Nonblocking value is well-defined for any subtype that is built from the base subtype (T'Base). T'Base of any scalar type, including a generic formal type, is always nonblocking.

For an inherited primitive dispatching subprogram that is null or abstract, the subprogram is nonblocking if and only if a corresponding subprogram of at least one ancestor is nonblocking. For any other inherited subprogram, it is nonblocking if and only if the corresponding subprogram of the parent is nonblocking.

Unless directly specified, overridings of dispatching operations inherit this aspect.

Unless directly specified, for a formal subtype, formal package, or formal subprogram, the Nonblocking aspect is that of the actual subtype, package, or subprogram.

Reason: This means that Nonblocking legality checking for the actual parameters of the instance is only necessary when the aspect is explicitly specified for the formal type.

Unless directly specified, for a non-first subtype $S$, the Nonblocking aspect is that of the subtype identified in the subtype indication defining $S$; unless directly specified for the first subtype of a derived type, the Nonblocking aspect is that of the ancestor subtype.

Discussion: The expressions that can be specified for such a subtype are limited by a Legality Rule, see below.

Unless directly specified, for any other program unit, first subtype, or formal object, the Nonblocking aspect of the entity is determined by the Nonblocking aspect for the innermost program unit enclosing the entity.

If not specified for a library unit, the Nonblocking aspect is True if the library unit is declared pure, or False otherwise.

The following are defined to be potentially blocking operations:
Reason: The primary purpose of these rules is to define what operations are not allowed in a protected operation (blocking is not allowed). Some of these operations are not directly blocking. However, they are still treated as potentially blocking, because allowing them in a protected action might impose an undesirable implementation burden.

- a select_statement;
- an accept_statement;
- an entry_call_statement, or a call on a procedure that renames or is implemented by an entry;
- a delay_statement;
- an abort_statement;
- task creation or activation;
- during a protected action, an external call on a protected subprogram (or an external requeue) with the same target object as that of the protected action.

Reason: This is really a deadlocking call, rather than a blocking call, but we include it in this list for simplicity.

{AI12-0064-2} If a language-defined subprogram allows blocking, then a call on the subprogram is a potentially blocking operation.

Ramification: Calls on other subprograms that allow blocking are not themselves potentially blocking; the execution of the body could execute a potentially blocking operation.

A user-defined instance of a language-defined generic creates user-defined subprograms for the purpose of this rule. A dispatching call to a language-defined abstract subprogram always calls a user-defined concrete subprogram, so that too is not potentially blocking for the purposes of this rule.

Legality Rules

{AI12-0064-2} {AI12-0267-1} {AI12-0374-2} A portion of program text is called a nonblocking region if it is anywhere within a parallel construct, or if the innermost enclosing program unit is nonblocking. A nonblocking region shall not contain any of the following:

- a select_statement;
- an accept_statement;
- a delay_statement;
- an abort_statement;
- task creation or activation.

{AI12-0374-2} Furthermore, a parallel construct shall neither contain a call on a callable entity for which the Nonblocking aspect is False, nor shall it contain a call on a call to a declarer declared within a generic unit that uses a generic formal parameter with Nonblocking aspect False (see Use Formal aspect in H.7.1).

{AI12-0374-2} Finally, a nonblocking region that is outside of a parallel construct shall not contain a call on a callable entity for which the Nonblocking aspect is False, unless the region is within a generic unit and the callable entity is associated with a generic formal parameter of the generic unit, or the call is within the aspect_definition of an assertion aspect for an entity that allows blocking.

Reason: A generic unit or entity declared within one is presumed to use its "used" generic formal parameters at least once each time it is invoked, and this passes through to the parallel construct check.

Ramification: Implicit calls for finalization, storage pools, and the like are covered by the above prohibition. The rules above say "a call", not "an explicit call". Such calls are considered statically bound when that is possible, that is, when the controlling object has a known specific type (even if the actual implementation uses dispatching).

Discussion: We don't need to worry specially about entry calls (even if the entry has been renamed as a procedure), as they will be detected by the prohibition against calls to entities with the Nonblocking aspect False.
Similarly, we don't need to specially worry about subprograms of limited interfaces that are implemented by entries, as any such subprogram necessarily has the value statically False for the Nonblocking aspect, and thus is already covered by the prohibition against calling such subprograms.

\{AI12-0064-2\}  \{AI12-0374-2\}  For the purposes of the above rules, an entry body is considered nonblocking if the immediately enclosing protected unit is nonblocking.

**Reason:** An entry declaration always allows blocking (by rule); but we want to be able to compile-time check for most violations of the prohibition against potentially blocking operations in a protected action (see 9.5.1). We do that by using the nonblocking status of the protected unit as the controlling factor, and enforce that by not allowing the specification of the Nonblocking aspect for any protected operation. We can't do this checking unconditionally, as that would be incompatible: existing Ada protected units might call subprograms that allow blocking. Thus a protected unit that allows blocking (which is the default) must allow calling any subprogram from an entry body.

\{AI12-0374-2\}  For a subtype for which aspect Nonblocking is True, any predicate expression that applies to the subtype shall only contain constructs that are allowed immediately within a nonblocking program unit.

\{AI12-0064-2\}  An entry shall not implement a nonblocking procedure. If an inherited dispatching subprogram allows blocking, then the corresponding subprogram of each ancestor shall allow blocking.

**Discussion:** Rules elsewhere in the standard (4.6 and 3.10.2) ensure that access-to-subprogram conversion and the Access attribute enforce nonblocking.

**Ramification:** A nonblocking dispatching subprogram can override one that allows blocking, but the reverse is illegal. Thus one can declare a Finalize subprogram to be nonblocking, even though it overrides a routine that allows blocking (This works because a nonblocking dispatching subprogram allows a strict subset of the operations allowed in allowing blocking subprograms, so calling such a subprogram as if it allows blocking — as is necessary in a dispatching call — is harmless.)

\{AI12-0064-2\}  \{AI12-0374-2\}  \{AI12-0396-1\}  \{AI12-0399-1\}  It is illegal to directly specify aspect Nonblocking for the first subtype of the full view of a type that has a partial view. If the Nonblocking aspect of the full view is inherited, it shall have the same value as that of the partial view, or have the value True.

**Reason:** We need completions to agree on nonblocking with the original view. One reason this is necessary to prevent the predefined equality operator from being nonblocking in the partial view and allowing blocking.

\{AI12-0064-2\}  \{AI12-0374-2\}  Aspect Nonblocking shall be directly specified for the first subtype of a derived type only if it has the same value as the Nonblocking aspect of the ancestor subtype or if it is specified True. Aspect Nonblocking shall be directly specified for a nonfirst subtype S only if it has the same value as the Nonblocking aspect of the subtype identified in the subtype indication defining S or if it is specified True.

**Reason:** Boolean-valued aspects have a similar rule to the first rule here (see 13.1.1), we want this one to work similarly. We need non-first subtypes to allow blocking only if the original first subtype allows blocking, as that allows the programmer to know that any operation on any subtype of a type are nonblocking if the first subtype is nonblocking.

\{AI12-0319-1\}  For an access-to-object type that is nonblocking, the Allocate, Deallocate, and Storage_Size operations on its storage pool shall be nonblocking.

**Ramification:** Standard storage pools always have nonblocking operations by definition (see 13.11), so this rule only can fail for user-defined storage pools.

\{AI12-0319-1\}  For a composite type that is nonblocking:

- All component subtypes shall be nonblocking;
- For a record type or extension, every call in the default_expression of a component (including discriminants) shall call an operation that is nonblocking;
- For a controlled type, the Initialize, Finalize, and Adjust (if any) subprograms shall be nonblocking.
Reason: These rules ensure that if a type is nonblocking, the default initialization, finalization, and assignment of the type are also nonblocking. This ensures that if a generic formal type is nonblocking, all of the basic operations of the actual type are nonblocking.

Default initialization, finalization, and assignment of elementary types are always nonblocking, so we don't need any rules for those.

\{AI12-0064-2\} \{AI12-0374-2\} The predefined equality operator for a composite type, unless it is for a record type or record extension and the operator is overridden by a primitive equality operator, is illegal if it is nonblocking and:

- for a record type or record extension, the parent primitive "=" allows blocking; or
- some component is of a type \(T\), and:
  - \(T\) is a record type or record extension that has a primitive "=" that allows blocking; or
  - \(T\) is neither a record type nor a record extension, and \(T\) has a predefined "=" that allows blocking.

Ramification: This applies to both record and array "=".

This check occurs when the equality operator is declared, so this rule effectively makes the type illegal if the rule is violated.

Reason: We don't need to check this when the operator is overridden for a record type, as the body of the new definition of equality will enforce the rules, and there is no case where the predefined operator will re-emerge. We do have to check this for array types even if the operator is overridden, as the predefined operator will re-emerge in generics and record equality.

\{AI12-0064-2\} \{AI12-0374-2\} In a generic instantiation:

- the actual subprogram corresponding to a nonblocking formal subprogram shall be nonblocking [(an actual that is an entry is not permitted in this case)];
- the actual subtype corresponding to a nonblocking formal subtype shall be nonblocking;

Ramification: We require matching for formal scalar or access-to-object types, even though their predefined operators are always nonblocking (and they re-emerge in the generic unit) - because a "blocking" predicate might apply to the actual subtype, which will also be enforced on operations of the formal type.

- the actual object corresponding to a formal object of a nonblocking access-to-subprogram type shall be of a nonblocking access-to-subprogram type;
- the actual instance corresponding to a nonblocking formal package shall be nonblocking.

\{AI12-0064-2\} In addition to the places where Legality Rules normally apply (see 12.3), the above rules also apply in the private part of an instance of a generic unit.

Ramification: For a generic formal parameter to be nonblocking (thus, for these rules to apply), it has to explicitly specify aspect Nonblocking to be True. However, if not specified True, these rules do apply in the instance of the specification of the generic unit (the normal re-checking is needed). For instance, the body of an expression function might make a prohibited call.

NOTE \{AI05-0030-2\} \{AI05-0215-1\} The synchronization kind By Protected Procedure implies that the operation will not block.

\{AI95-00345-01\} Added a Legality Rule to make it crystal-clear that the protected object of an entry or procedure call must be a variable. This rule was implied by the Dynamic Semantics here, along with the Static Semantics of 3.3, but it is much better to explicitly say it. While many implementations have gotten this wrong, this is not an incompatibility — allowing updates of protected constants has always been wrong.

Extensions to Ada 2005

\{AI05-0030-2\} \{AI05-0215-1\} Added the Synchronization aspect to allow specifying that an interface procedure is really an entry or a protected procedure.
Wording Changes from Ada 2005

Correction: Clarified that the target object of any name denoted a protected procedure or entry can never be a constant (other than for the 'Count attribute). This closes holes involving calls to access-to-protected, renaming as a procedure, and generic formal subprograms.

Inconsistencies With Ada 2012

Calls on procedures that rename an entry or are implemented by an entry are now defined to be potentially blocking. This means that such a call now might raise Program_Error. However, it never made sense for some entry calls to be excluded from being potentially blocking, and we expect that most implementations already treated all entry calls the same way. Thus do not expect this wording change to actually change the behavior of any implementation, and thus no program will change.

Incompatibilities With Ada 2012

Correction: Internal protected calls are now prohibited in preconditions and default expressions of protected operations. These were allowed in Ada 2012, but as they cause race conditions and as most existing Ada 95 compilers crash when given such a default parameter, we expect such code to be extremely rare.

Extensions to Ada 2012

Aspect Nonblocking is new; it allows compile-time checks to prevent using potentially blocking operations in contexts where that is not allowed.

9.5.1 Protected Subprograms and Protected Actions

A protected subprogram is a subprogram declared immediately within a protected_definition. Protected procedures provide exclusive read-write access to the data of a protected object; protected functions provide concurrent read-only access to the data.

Ramification: A subprogram declared immediately within a protected_body is not a protected subprogram; it is an intrinsic subprogram. See 6.3.1, “Conformance Rules”.

Static Semantics

[Within the body of a protected function (or a function declared immediately within a protected_body), the current instance of the enclosing protected unit is defined to be a constant (that is, its subcomponents may be read but not updated). Within the body of a protected procedure (or a procedure declared immediately within a protected_body), and within an entry_body, the current instance is defined to be a variable (updating is permitted).]

Proof: All constant views are defined in 3.3, “Objects and Named Numbers”, anything not named there is a variable view.

Ramification: The current instance is like an implicit parameter, of mode in for a protected function, and of mode in out for a protected procedure (or protected entry).

For a type declared by a protected_type_declaration or for the anonymous type of an object declared by a single_protected_declaration, the following language-defined type-related representation aspect may be specified:

Exclusive Functions

The type of aspect Exclusive Functions is Boolean. If not specified (including by inheritance), the aspect is False.

A value of True for this aspect indicates that protected functions behave in the same way as protected procedures with respect to mutual exclusion and queue servicing (see below).

Aspect Description for Exclusive Functions: Specifies mutual exclusion behavior of protected functions in a protected type.

A protected procedure or entry is an exclusive protected operation. A protected function of a protected type P is an exclusive protected operation if the Exclusive Functions aspect of P is True.
Dynamic Semantics

For the execution of a call on a protected subprogram, the evaluation of the name or prefix and of the parameter associations, and any assigning back of in out or out parameters, proceeds as for a normal subprogram call (see 6.4). If the call is an internal call (see 9.5), the body of the subprogram is executed as for a normal subprogram call. If the call is an external call, then the body of the subprogram is executed as part of a new protected action on the target protected object; the protected action completes after the body of the subprogram is executed. [A protected action can also be started by an entry call (see 9.5.3).]

\{AI12-0129-1\} A new protected action is not started on a protected object while another protected action on the same protected object is underway, unless both actions are the result of a call on a nonexclusive protected function. This rule is expressible in terms of the execution resource associated with the protected object:

- \{AI12-0129-1\} Starting a protected action on a protected object corresponds to acquiring the execution resource associated with the protected object, either for exclusive read-write concurrent read-only access if the protected action is for a call on an exclusive protected operation, a protected function, or for concurrent read-only exclusive read-write access otherwise;

- Completing the protected action corresponds to releasing the associated execution resource.

\{AI12-0129-1\} [After performing an exclusive protected operation on a protected object other than a call on a protected function, but prior to completing the associated protected action, the entry queues (if any) of the protected object are serviced (see 9.5.3).]

\{AI12-0119-1\} If a parallel construct occurs within a protected action, no new logical threads of control are created. Instead, each element of the parallel construct that would have become a separate logical thread of control executes on the logical thread of control that is performing the protected action. If there are multiple such elements initiated at the same point, they execute in an arbitrary order.

Reason: It would be feasible to allow multiple logical threads of control within a protected action, but it would significantly complicate the definition of "sequential" and "concurrent" actions, since we generally presume that everything occurring within protected actions of a given protected object is sequential. We could simply disallow any use of parallel constructs, but that seems unnecessary, particularly as a parallel construct might be buried within a subprogram that is declared Nonblocking.

Bounded (Run-Time) Errors

\{AI12-0064-2\} During a protected action, it is a bounded error to invoke an operation that is potentially blocking (see 9.5). The following are defined to be potentially blocking operations:

Paragraphs 9 through 16 were moved to 9.5.

Reason: \{AI12-0064-2\} Some of these operations are not directly blocking. However, they are still treated as bounded errors during a protected action, because allowing them might impose an undesirable implementation burden.

- a select_statement;
- an accept_statement;
- an entry_call_statement;
- a delay_statement;
- an abort_statement;
- task creation or activation;
- an external call on a protected subprogram (or an external requeue) with the same target object as that of the protected action;

Reason: This is really a deadlocking call, rather than a blocking call, but we include it in this list for simplicity.
• a call on a subprogram whose body contains a potentially blocking operation.

  **Reason:** This allows an implementation to check and raise Program_Error as soon as a subprogram is called, rather than waiting to find out whether it actually reaches the potentially blocking operation. This in turn allows the potentially blocking operation check to be performed prior to run time in some environments.

  **Discussion:** [AI95-00305-01] By “nested protected action”, we mean that an additional protected action can be started by another task on the same protected object. This means that mutual exclusion may be broken in this bounded error case. A way to ensure that this does not happen is to use pragma Detect_Blocking (see H.5).

  **AI12-0064-2** During a protected action, a call on a subprogram whose body contains a potentially blocking operation is a bounded error. If the bounded error is detected, Program_Error is raised. If not detected, the bounded error can result in deadlock or a (nested) protected action on the same target object.

  **Discussion:** [AI95-00178-01] Any subprogram in a language-defined input-output package that has a file parameter or result or operates on a default file is considered to manipulate a file. An instance of a language defined input-output generic package provides subprograms that are covered by this rule. The only subprograms in language-defined input-output packages not covered by this rule (and thus not potentially blocking) are the Get and Put routines that take string parameters defined in the packages nested in Text.IO.

  **Reason:** [AI95-00247-1] This allows an implementation to check and raise Program_Error as soon as a subprogram is called, rather than waiting to find out whether it actually reaches the potentially blocking operation. This in turn allows the intended implementation on a multi-processor to be considered part of the normal competition for processing resources while it awaits its turn. Unless there is an admission policy (see D.4.1) in effect, there is no language-defined ordering or queuing presumed for tasks competing to start a protected action — on a multiprocessor such tasks can use busy-waiting; for further monoprocessor and multiprocessor considerations, see D.3, “Priority Ceiling Locking”.

**Example**

**Examples of protected subprogram calls (see 9.4):**
Shared_Array.Set_Component(N, E);
E := Shared_Array.Component(M);
Control.Release;

Wording Changes from Ada 95

{AI95-00305-01} Added a note pointing out the existence of pragma Detect_Blocking. This pragma can be used to ensure portable (somewhat pessimistic) behavior of protected actions by converting the Bounded Error into a required check.

Extensions to Ada 2012

{AI12-0129-1} Corrigendum: Aspect Exclusive_Functions is new. The term “exclusive protected operations” is new.

Wording Changes from Ada 2012

{AI12-0064-2} Moved the definition of potentially blocking operations to 9.5, so it could be integrated into the definition of the Nonblocking aspect.

{AI12-0247-1} Correction: Added a separate bounded error for a subprogram containing a blocking operation, to keep compatibility with Ada 95 rules without requiring a correct implementation of pragma Detect_Blocking to do full program analysis.

9.5.2 Entries and Accept Statements

Entry declarations, with the corresponding entry bodies or accept statements, are used to define potentially queued operations on tasks and protected objects.

Syntax

\{AI95-00397-01\} \{AI05-0183-1\} entry_declaration ::= 
[overriding_indicator] 
entry defining_identifier [(discrete_subtype_definition)] parameter_profile 
[aspect_specification];

accept_statement ::= 
accept entry_direct_name [(entry_index)] parameter_profile [do 
handled_sequence_of_statements 
end [entry_identifier]]; 

Reason: We cannot use defining_identifier for accept statements. Although an accept_statement is sort of like a body, it can appear nested within a block_statement, and therefore be hidden from its own entry by an outer homograph.

entry_index ::= expression 

\{AI12-0169-1\} entry_body ::= 
entry defining_identifier entry_body_formal_part 
[aspect_specification]
__entry_barrier is 
declarative_part 
begin 
handled_sequence_of_statements 
end [entry_identifier];

Discussion: \{AI95-00397-01\} We don't allow an overriding_indicator on an entry_body because entries always implement procedures at the point of the type declaration; there is no late implementation. And we don't want to have to think about overriding indicators on accept_statements.

entry_body_formal_part ::= [(entry_index_specification)] parameter_profile

entry_barrier ::= when condition
**Name Resolution Rules**

In an `accept_statement`, the expected profile for the `entry_direct_name` is that of the `entry_declaration`; the expected type for an `entry_index` is that of the subtype defined by the `discrete_subtype_definition` of the corresponding `entry_declaration`.

Within the `handled_sequence_of_statements` of an `accept_statement`, if a `selected_component` has a prefix that denotes the corresponding `entry_declaration`, then the entity denoted by the prefix is the `accept_statement`, and the `selected_component` is interpreted as an expanded name (see 4.1.3); the `selector_name` of the `selected_component` has to be the identifier for some formal parameter of the `accept_statement`.

**Proof:** The only declarations that occur immediately within the declarative region of an `accept_statement` are those for its formal parameters.

**Legality Rules**

An `entry_declaration` in a task declaration shall not contain a specification for an access parameter (see 3.10).

**Reason:** Access parameters for task entries would require a complex implementation. For example:

```ada

8/5

\{AI12-0398-1\} entry_index_specification ::= _
  for defining_identifier in discrete_subtype_definition [aspect_specification]

If an *entry_identifier* appears at the end of an *accept_statement*, it shall repeat the *entry_direct_name*. If an *entry_identifier* appears at the end of an *entry_body*, it shall repeat the *defining_identifier*.

[An *entry_declaration* is allowed only in a protected or task declaration.]

**Proof:** This follows from the BNF.

\{AI95-00397-01\} An *overriding_indicator* is not allowed in an *entry_declaration* that includes a `discrete_subtype_definition`.

**Reason:** An entry family can never implement something, so allowing an indicator is felt by the majority of the ARG to be redundant.

Implementing the Accessibility_Check inside the `accept_statement` for E is difficult, since one does not know whether the entry caller is calling from inside the immediately enclosing declare block or from outside it. This means that the lexical nesting level associated with the designated object is not sufficient to determine whether the Accessibility_Check should pass or fail.
Note that such problems do not arise with protected entries, because entry_bodies are always nested immediately within the protected_body; they cannot be further nested as can accept_statements, nor can they be called from within the protected_body (since no entry calls are permitted inside a protected_body).

13.1.2/1 If an entry_declaration has an overriding_indicator, then at the point of the declaration:

• if the overriding_indicator is overriding, then the entry shall implement an inherited subprogram;
• if the overriding_indicator is not overriding, then the entry shall not implement any inherited subprogram.

In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

Discussion: These rules are subtly different than those for subprograms (see 8.3.1) because there cannot be “late” inheritance of primitives from interfaces. Hidden (that is, private) interfaces are prohibited explicitly (see 7.3), as are hidden primitive operations (as private operations of public abstract types are prohibited — see 3.9.3).

For an accept_statement, the innermost enclosing body shall be a task_body, and the entry_direct_name shall denote an entry_declaration in the corresponding task declaration; the profile of the accept_statement shall conform fully to that of the corresponding entry_declaration. An accept_statement shall have a parenthesized entry_index if and only if the corresponding entry_declaration has a discrete_subtype_definition.

An accept_statement shall not be within another accept_statement that corresponds to the same entry_declaration, nor within an asynchronous_select inner to the enclosing task_body.

Reason: Accept_statements are required to be immediately within the enclosing task_body (as opposed to being in a nested subprogram) to ensure that a nested task does not attempt to accept the entry of its enclosing task. We considered relaxing this restriction, either by making the check a run-time check, or by allowing a nested task to accept an entry of its enclosing task. However, neither change seemed to provide sufficient benefit to justify the additional implementation burden.

Nested accept_statements for the same entry (or entry family) are prohibited to ensure that there is no ambiguity in the resolution of an expanded name for a formal parameter of the entry. This could be relaxed by allowing the inner one to hide the outer one from all visibility, but again the small added benefit didn't seem to justify making the change for Ada 95.

Accept_statements are not permitted within asynchronous_select statements to simplify the semantics and implementation: an accept_statement in an abortable_part could result in Tasking_Error being propagated from an entry call even though the target task was still callable; implementations that use multiple tasks implicitly to implement an asynchronous_select might have trouble supporting "up-level" accepts. Furthermore, if accept_statements were permitted in the abortable_part, a task could call its own entry and then accept it in the abortable_part, leading to rather unusual and possibly difficult-to-specify semantics.

An entry_declaration of a protected unit requires a completion[, which shall be an entry_body,] and every entry_body shall be the completion of an entry_declaration of a protected unit. The profile of the entry_body shall conform fully to that of the corresponding declaration.

Ramification: An entry_declaration, unlike a subprogram_declaration, cannot be completed with a renaming_ declaration.

To be honest: {AI05-0229-1} If the completion can be a pragma if the implementation supports it, the entry body can be imported (using aspect Import, see B.1), in which case no explicit entry_body is allowed.

Discussion: The above applies only to protected entries, which are the only ones completed with entry_bodies. Task entries Need not have corresponding accept_statements instead of having entry_bodies, and we do not consider an accept_statement to be a “completion,” because a task entry_declaration is allowed to have zero, one, or more than one corresponding accept_statements.

An entry_body_formal_part shall have an entry_index_specification if and only if the corresponding entry_declaration has a discrete_subtype_definition. In this case, the discrete_subtype_definitions of the entry_declaration and the entry_index_specification shall fully conform to one another (see 6.3.1).
A name that denotes a formal parameter of an entry_body is not allowed within the entry_barrier of the entry_body.

**Static Semantics**

The parameter modes defined for parameters in the parameter_profile of an entry_declaration are the same as for a subprogram_declaration and have the same meaning (see 6.2).

**Discussion:** Note that access parameters are not allowed for task entries (see above).

An entry_declaration with a discrete_subtype_definition (see 3.6) declares a family of distinct entries having the same profile, with one such entry for each value of the entry index subtype defined by the discrete_subtype_definition. [A name for an entry of a family takes the form of an indexed_component, where the prefix denotes the entry_declaration for the family, and the index value identifies the entry within the family.] The term single entry is used to refer to any entry other than an entry of an entry family.

In the entry_body for an entry family, the entry_index_specification declares a named constant whose subtype is the entry index subtype defined by the corresponding entry_declaration; the value of the named entry index identifies which entry of the family was called.

**Ramification:** The discrete_subtype_definition of the entry_index_specification is not elaborated; the subtype of the named constant declared is defined by the discrete_subtype_definition of the corresponding entry_declaration, which is elaborated, either when the type is declared, or when the object is created, if its constraint is per-object.

**Dynamic Semantics**

{8652/0002} {AI95-00171-01} The elaboration of an entry_declaration for an entry family consists of the elaboration of the discrete_subtype_definition, as described in 3.8. For the elaboration of an entry_declaration for an entry family, if the discrete_subtype_definition contains no per-object expressions (see 3.8), then the discrete_subtype_definition is elaborated. Otherwise, the elaboration of the entry_declaration consists of the evaluation of any expression of the discrete_subtype_definition that is not a per-object expression (or part of one). The elaboration of an entry_declaration for a single entry has no effect.

**Discussion:** {AI05-0299-1} {AI12-0449-1} The elaboration of the declaration of a protected subprogram has no effect, as specified in subclause 6.1. The default initialization of an object of a task or protected type is covered in 3.3.1. [The actions to be performed when an entry is called are specified by the corresponding accept_statements (if any) for an entry of a task unit, and by the corresponding entry_body for an entry of a protected unit.]

{AI12-0193-1} The interaction between a task that calls an entry and an accepting task is called a rendezvous.

{AI12-0193-1} For the execution of an accept_statement, the entry_index, if any, is first evaluated and converted to the entry index subtype; this index value identifies which entry of the family is to be accepted. Further execution of the accept_statement is then blocked until a caller of the corresponding entry is selected (see 9.5.3), whereupon the handled_sequence_of_statements, if any, of the accept_statement is executed, with the formal parameters associated with the corresponding actual parameters of the selected entry call. Execution of the rendezvous consists of the execution of the handled_sequence_of_statements, performance of any postcondition or type invariant checks associated with the entry, and any initialization or finalization associated with these checks, as described in 6.1.1 and 7.3.2. After execution of the rendezvous, the accept_statement completes and is left. [The two tasks then proceed independently.] When an exception is propagated from the handled_sequence_of_statements of an accept_statement, the same exception is also raised by the execution of the corresponding entry_call_statement.
Ramification: This is in addition to propagating it to the construct containing the accept_statement. In other words, for a rendezvous, the raising splits in two, and continues concurrently in both tasks.

The caller gets a new occurrence; this isn't considered propagation.

Note that we say “propagated from the handled_sequence_of_statements of an accept_statement”, not “propagated from an accept_statement”. The latter would be wrong — we don't want exceptions propagated by the entry_index to be sent to the caller (there is none yet!).

Execution of the rendezvous does not include any checks associated with parameter copy back or any post-call subtype predicate check for a parameter which is passed by reference. These checks are performed by the caller after the execution of the rendezvous.

This paragraph was deleted.

The above interaction between a calling task and an accepting task is called a rendezvous. [After a rendezvous, the two tasks continue their execution independently.]

An entry_body is executed when the condition of the entry_barrier evaluates to True and a caller of the corresponding single entry, or entry of the corresponding entry family, has been selected (see 9.5.3). For the execution of the entry_body, the declarative_part of the entry_body is elaborated, and the handled_sequence_of_statements of the body is executed, as for the execution of a subprogram_body. The value of the named entry index, if any, is determined by the value of the entry index specified in the entry_name of the selected entry call (or intermediate requeue_statement — see 9.5.4).

To be honest: If the entry had been renamed as a subprogram, and the call was a procedure_call_statement using the name declared by the renaming, the entry index (if any) comes from the entry name specified in the subprogram_renaming_declaration.

NOTE 1 A task entry has corresponding accept_statements (zero or more), whereas a protected entry has a corresponding entry_body (exactly one).

NOTE 2 A consequence of the rule regarding the allowed placements of accept_statements is that a task can execute accept_statements only for its own entries.

NOTE 3 A return_statement (see 6.5) or a requeue_statement (see 9.5.4) cannot be used to complete the execution of an accept_statement or an entry_body.

Ramification: An accept_statement need not have a handled_sequence_of_statements even if the corresponding entry has parameters. Equally, it can have a handled_sequence_of_statements even if the corresponding entry has no parameters.

Ramification: A single entry overloads a subprogram, an enumeration literal, or another single entry if they have the same defining_identifier. Overloading is not allowed for entry family names. A single entry or an entry of an entry family can be renamed as a procedure as explained in 8.5.4.

NOTE 4 The condition in the entry_barrier cannot refer to anything visible except the formal parameters of the entry. This includes the entry index (if any), the components (including discriminants) of the protected object, the Count attribute of an entry of that protected object, and data global to the protected unit.

The restriction against referencing the formal parameters within an entry_barrier ensures that all calls of the same entry see the same barrier value. If it is necessary to look at the parameters of an entry call before deciding whether to handle it, the entry_barrier can be “when True” and the caller can be requeued (on some private entry) when its parameters indicate that it cannot be handled immediately.

Examples

Examples of entry declarations:
```ada
entry Read(V : out Item);
entry Seize;
entry Request(Level)(D : Item);  -- a family of entries
```

Examples of accept statements:
```ada
accept Shut_Down;
accept Read(V : out Item) do
  V := Local_Item;
end Read;
```
```ada
accept Request(Low)(D : Item) do
  ...
end Request;
```

Extensions to Ada 83

The syntax rule for `entry_body` is new.

Accept statements can now have exception handlers.

Wording Changes from Ada 95

{8652/0002} [AI95-00171-01] Corrigendum: Clarified the elaboration of per-object constraints.

{AI95-00397-01} Overriding indicators can be used on entries; this is only useful when a task or protected type inherits from an interface.

Extensions to Ada 2005

{AI05-0183-1} An optional `aspect_specification` can be used in an `entry_declaration`. This is described in 13.1.1.

Extensions to Ada 2012

{AI12-0169-1} Correction: An optional `aspect_specification` can be used in an `entry_body`. All other kinds of bodies allow (only) implementation-defined aspects, we need to be consistent.

{AI12-0398-1} Named entry indexes now can have an `aspect_specification`, allowing the specification of (implementation-defined) aspects for a named entry index.

Wording Changes from Ada 2012

{AI12-0193-1} Correction: Clarified that postcondition and invariant checks are clearly part of the rendezvous for an entry call. 6.1.1 already said this, so the intent was clear and this is not an inconsistency.

### 9.5.3 Entry Calls

[An `entry_call_statement` (an `entry call`) can appear in various contexts.] A simple entry call is a standalone statement that represents an unconditional call on an entry of a target task or a protected object. [Entry calls can also appear as part of `select_statement`s (see 9.7).]

**Syntax**

```
entry_call_statement ::= entry_name [actual_parameter_part];
```

**Name Resolution Rules**

The `entry_name` given in an `entry_call_statement` shall resolve to denote an entry. The rules for parameter associations are the same as for subprogram calls (see 6.4 and 6.4.1).

**Static Semantics**

[The `entry_name` of an `entry_call_statement` specifies (explicitly or implicitly) the target object of the call, the entry or entry family, and the entry index, if any (see 9.5).]

**Dynamic Semantics**

Under certain circumstances (detailed below), an entry of a task or protected object is checked to see whether it is `open` or `closed`:

- `{AI05-0264-1}` An entry of a task is open if the task is blocked on an `accept_statement` that corresponds to the entry (see 9.5.2), or on a `selective_accept` (see 9.7.1) with an open `accept_alternative` that corresponds to the entry; otherwise, it is closed.

- `{AI05-0264-1}` An entry of a protected object is open if the condition of the `entry_barrier` of the corresponding `entry_body` evaluates to True; otherwise, it is closed. If the evaluation of the
condition propagates an exception, the exception Program_Error is propagated to all current callers of all entries of the protected object.

**Reason:** An exception during barrier evaluation is considered essentially a fatal error. All current entry callers are notified with a Program_Error. In a fault-tolerant system, a protected object might provide a Reset protected procedure, or equivalent, to support attempts to restore such a "broken" protected object to a reasonable state.

**Discussion:** Note that the definition of when a task entry is open is based on the state of the (accepting) task, whereas the "openness" of a protected entry is defined only when it is explicitly checked, since the barrier expression needs to be evaluated. Implementation permissions are given (below) to allow implementations to evaluate the barrier expression more or less often than it is checked, but the basic semantic model presumes it is evaluated at the times when it is checked.

For the execution of an **entry_call_statement**, evaluation of the **name** and of the parameter associations is as for a subprogram call (see 6.4). The entry call is then **issued**: For a call on an entry of a protected object, a new protected action is started on the object (see 9.5.1). The named entry is checked to see if it is open; if open, the entry call is said to be **selected immediately**, and the execution of the call proceeds as follows:

- For a call on an open entry of a task, the accepting task becomes ready and continues the execution of the corresponding **accept_statement** (see 9.5.2).
- For a call on an open entry of a protected object, the corresponding **entry_body** is executed (see 9.5.2) as part of the protected action.

If the **accept_statement** or **entry_body** completes other than by a requeue (see 9.5.4), return is made to the caller (after servicing the entry queues — see below); any necessary assigning back of formal to actual parameters occurs, as for a subprogram call (see 6.4.1); such assignments take place outside of any protected action.

**Ramification:** The return to the caller will generally not occur until the protected action completes, unless some other thread of control is given the job of completing the protected action and releasing the associated execution resource.

If the named entry is closed, the entry call is added to an **entry_queue** (as part of the protected action, for a call on a protected entry), and the call remains queued until it is selected or cancelled; there is a separate (logical) entry queue for each entry of a given task or protected object [(including each entry of an entry family)].

When a queued call is **selected**, it is removed from its entry queue. Selecting a queued call from a particular entry queue is called **servicing** the entry queue. An entry with queued calls can be serviced under the following circumstances:

- When the associated task reaches a corresponding **accept_statement**, or a **selective_accept** with a corresponding open **accept_alternative**;
- {**AI12-0129-1**} If after performing, as part of a protected action on the associated protected object, an **exclusive protected** operation on the object other than a call on a protected function, the entry is checked and found to be open.

If there is at least one call on a queue corresponding to an open entry, then one such call is selected according to the **entry queuing policy** in effect (see below), and the corresponding **accept_statement** or **entry_body** is executed as above for an entry call that is selected immediately.

The entry queuing policy controls selection among queued calls both for task and protected entry queues. The default entry queuing policy is to select calls on a given entry queue in order of arrival. If calls from two or more queues are simultaneously eligible for selection, the default entry queuing policy does not specify which queue is serviced first. Other entry queuing policies can be specified by **pragmas** (see D.4).

For a protected object, the above servicing of entry queues continues until there are no open entries with queued calls, at which point the protected action completes.
**Discussion:** While servicing the entry queues of a protected object, no new calls can be added to any entry queue of the object, except due to an internal requeue (see 9.5.4). This is because the first step of a call on a protected entry is to start a new protected action, which implies acquiring (for exclusive read-write access) the execution resource associated with the protected object, which cannot be done while another protected action is already in progress.

For an entry call that is added to a queue, and that is not the triggering_statement of an asynchronous_select (see 9.7.4), the calling task is blocked until the call is cancelled, or the call is selected and a corresponding accept_statement or entry_body completes without requeuing. In addition, the calling task is blocked during a rendezvous.

**Ramification:** For a call on a protected entry, the caller is not blocked if the call is selected immediately, unless a requeue causes the call to be queued.

An attempt can be made to cancel an entry call upon an abort (see 9.8) and as part of certain forms of select_statement (see 9.7.2, 9.7.3, and 9.7.4). The cancellation does not take place until a point (if any) when the call is on some entry queue, and not protected from cancellation as part of a requeue (see 9.5.4); at such a point, the call is removed from the entry queue and the call completes due to the cancellation. The cancellation of a call on an entry of a protected object is a protected action[1] and as such cannot take place while any other protected action is occurring on the protected object. Like any protected action, it includes servicing of the entry queues (in case some entry barrier depends on a Count attribute).

**Implementation Note:** \{AI95-00114-01\} In the case of an attempted cancellation due to abort, this removal might have to be performed by the calling task itself if the ceiling priority of the protected object is lower than the priority of the task initiating the abort.

A call on an entry of a task that has already completed its execution raises the exception Tasking_Error at the point of the call; similarly, this exception is raised at the point of the call if the called task completes its execution or becomes abnormal before accepting the call or completing the rendezvous (see 9.8). This applies equally to a simple entry call and to an entry call as part of a select_statement.

**Implementation Permissions**

\{AI12-0444-1\} An implementation may perform the sequence of steps of a protected action using any thread of control; it can be a thread other than need not be that of the task that started the protected action. If an entry_body completes without requeuing, then the corresponding calling task may be made ready without waiting for the entire protected action to complete.

**Reason:** These permissions are intended to allow flexibility for implementations on multiprocessors. On a monoprocessor, which thread of control executes the protected action is essentially invisible, since the thread is not abortable in any case, and the "current_task" function is not guaranteed to work during a protected action (see C.7.1).\[2\]

\{AI12-0129-1\} \{AI12-0444-1\} When the entry of a protected object is checked to see whether it is open, the implementation can bypass reevaluating the condition of the corresponding entry_barrier if no variable or attribute referenced by the condition (directly or indirectly) has been altered by the execution (or cancellation) of a protected procedure or entry_call to an exclusive protected operation of the object since the condition was last evaluated.

**Ramification:** Changes to variables referenced by an entry barrier that result from actions outside of a protected procedure or entry_call to an exclusive protected operation of the protected object need not be "noticed". For example, if a global variable is referenced by an entry barrier, it should not be altered (except as part of a protected action on the object) any time after the barrier is first evaluated. In other words, globals can be used to "parameterize" a protected object, but they cannot reliably be used to control it after the first use of the protected object.

**Implementation Note:** Note that even if a global variable is volatile, the implementation need only reevaluate a barrier if the global is updated during a protected action on the protected object. This ensures that an entry-open bit-vector implementation approach is possible, where the bit-vector is computed at the end of a protected action, rather than upon each entry call.

An implementation may evaluate the conditions of all entry_barriers of a given protected object any time any entry of the object is checked to see if it is open.
9.5.3 Entry Calls

Examples of entry calls:

Agent.Shut_Down;          -- see 9.1
Parser.Next_Lexeme(E);    -- see 9.1
Pool(5).Read(Next_Char);  -- see 9.1
Controller.Request(Low)(Some_Item); -- see 9.1
Flags(3).Seize;           -- see 9.4

Examples

AI12-0442-1} The condition of an entry_barrier is allowed to be evaluated by an implementation more often than strictly necessary, even if the evaluation can avoid reevaluating. If the condition references some global variable that is not updated by an action performed from outside of a protected action, even if the condition references some global variable that is valid at run time.

AI12-0444-1} When an attempt is made to cancel an entry call, the implementation can use the thread of control other than that of the task (or interrupt) that initiated the cancellation; in particular, it may use the thread of control of the caller itself to attempt the cancellation, even if this can make the attempt using the thread of control other than that of the task (or interrupt) that initiated the cancellation.

NOTE 1 If an exception is raised during the execution of an entry_body, it is propagated to the corresponding caller (see 11.4).

NOTE 2 For a call on a protected entry, the entry is checked to see if it is open prior to queuing the call, and again thereafter if its Count attribute (see 9.9) is referenced in some entry barrier.

NOTE 3 In addition to simple entry calls, the language permits timed, conditional, and asynchronous entry calls (see 9.7.2, 9.7.3, and see 9.7.4).

NOTE 4 The condition of an entry_barrier is allowed to be evaluated by an implementation more often than strictly necessary, even if the evaluation can avoid reevaluating. If the condition references some global variable that is not updated by an action performed from outside of a protected action.
9.5.4 Requeue Statements

[A requeue_statement can be used to complete an accept_statement or entry_body, while redirecting the corresponding entry call to a new (or the same) entry queue. Such a requeue can be performed with or without allowing an intermediate cancellation of the call, due to an abort or the expiration of a delay.]

Syntax

requeue_statement ::= requeue procedure_or_entry_entry_name [with abort];

Name Resolution Rules

The procedure_or_entry_entry_name of a requeue_statement shall resolve to denote a procedure or an entry (the requeue_target_entry). The profile of the entry, or the profile or prefixed profile of the procedure, shall either have no parameters, or have a profile that is type conformant (see 6.3.1) with the profile of the innermost enclosing entry_body or accept_statement.

Legality Rules

A requeue_statement shall be within a callable construct that is either an entry_body or an accept_statement, and this construct shall be the innermost enclosing body or callable construct.

If the requeue_target_entry has parameters, then its (prefixed) profile shall be subtype conformant with the profile of the innermost enclosing callable construct.

Given a requeue statement where the innermost enclosing callable construct is for an entry E1, for every [specific or class-wide] postcondition expression P1 that applies to E1, there shall exist a postcondition expression P2 that applies to the requeue target E2 such that

- P1 is fully conformant with the expression produced by replacing each reference in P2 to a formal parameter of E2 with a reference to the corresponding formal parameter of E1; and
- if P1 is enabled, then P2 is also enabled.

Discussion: Roughly speaking, the postcondition of the requeue target is required to imply that of the enclosing callable construct.

The requeue_target_entry shall not have an applicable specific or class-wide postcondition that includes an Old or Index attribute reference.

If the requeue_target_entry is declared immediately within the task_definition of a named task type or the protected_definition of a named protected type, and if the requeue statement occurs within the body of that type, and if the requeue is an external requeue, then the requeue target shall not have a specific or class-wide postcondition which includes a name denoting either the current instance of that type or any entity declared within the declaration of that type.

Discussion: The above pair of rules always apply; they don't depend on whether or not any of the postconditions are enabled.

If the target is a procedure, the name shall denote a renaming of an entry, or shall denote a view or a prefixed view of a primitive subprogram of a synchronized interface, where the first parameter of the unprefixed view of the primitive subprogram shall be a controlling parameter, and the Synchronization aspect shall be specified with synchronization_kind By_Entry for the primitive subprogram.
In a requeue_statement of an accept_statement of some task unit, either the target object shall be a part of a formal parameter of the accept_statement, or the accessibility level of the target object shall not be equal to or statically deeper than any enclosing accept_statement of the task unit. In a requeue_statement of an entry_body of some protected unit, either the target object shall be a part of a formal parameter of the entry_body, or the accessibility level of the target object shall not be statically deeper than that of the entry_declaration for the entry_body.

Ramification: In the entry_body case, the intent is that the target object can be global, or can be a component of the protected unit, but cannot be a local variable of the entry_body.

Reason: These restrictions ensure that the target object of the requeue outlives the completion and finalization of the enclosing callable construct. They also prevent requeuing from a nested accept_statement on a parameter of an outer accept_statement, which could create some strange "long-distance" connections between an entry caller and its server.

Note that in the strange case where a task_body is nested inside an accept_statement, it is permissible to requeue from an accept_statement of the inner task_body on parameters of the outer accept_statement. This is not a problem because all calls on the inner task have to complete before returning from the outer accept_statement, meaning no "dangling calls" will be created.

Implementation Note: By disallowing certain requeues, we ensure that the normal terminate_alternative rules remain sensible, and that explicit clearing of the entry queues of a protected object during finalization is rarely necessary. In particular, such clearing of the entry queues is necessary only (ignoring premature Unchecked_Deallocation) for protected objects declared in a task_body (or created by an allocator for an access type declared in such a body) containing one or more requeue_statements. Protected objects declared in subprograms, or at the library level, will never need to have their entry queues explicitly cleared during finalization.

Dynamic Semantics

The execution of a requeue_statement begins with the following sequence of steps: proceeds by first evaluating the procedure_or_entry_name[, including the prefix identifying the target task or protected object and the expression identifying the entry within an entry family, if any]. Precondition checks are then performed as for a call to the requeue target entry or subprogram. The entry_body or accept_statement enclosing the requeue_statement is then completed[, finalized, and left (see 7.6.1)].

1. The procedure_or_entry_name is evaluated. This includes evaluation of the prefix (if any) identifying the target task or protected object and of the expression (if any) identifying the entry within an entry family.

2. If the target object is not a part of a formal parameter of the innermost enclosing callable construct, a check is made that the accessibility level of the target object is not equal to or deeper than the level of the innermost enclosing callable construct. If this check fails, Program_Error is raised.

3. Precondition checks are performed as for a call to the requeue target.

4. The entry_body or accept_statement enclosing the requeue_statement is then completed[, finalized, and left (see 7.6.1)].

For the execution of a requeue on an entry of a target task, after leaving the enclosing callable construct, the named entry is checked to see if it is open and the requeued call is either selected immediately or queued, as for a normal entry call (see 9.5.3).

For the execution of a requeue on an entry of a target protected object, after leaving the enclosing callable construct:

- if the requeue is an internal requeue (that is, the requeue is back on an entry of the same protected object — see 9.5), the call is added to the queue of the named entry and the ongoing protected action continues (see 9.5.1);
Ramification: Note that for an internal requeue, the call is queued without checking whether the target entry is open. This is because the entry queues will be serviced before the current protected action completes anyway, and considering the requeued call immediately might allow it to "jump" ahead of existing callers on the same queue.

- if the requeue is an external requeue (that is, the target protected object is not implicitly the same as the current object — see 9.5), a protected action is started on the target object and proceeds as for a normal entry call (see 9.5.3).

\{AI05-0030-2\} \{AI05-0090-1\} If the requeue_target new_entry named in the requeue_statement has formal parameters, then during the execution of the accept_statement or entry_body corresponding to the new entry and during the checking of any preconditions of the new entry, the formal parameters denote the same objects as did the corresponding formal parameters of the callable construct completed by the requeue. [In any case, no parameters are specified in a requeue_statement; any parameter passing is implicit.]

If the requeue_statement includes the reserved words with abort (it is a requeue-with-abort), then:

- if the original entry call has been aborted (see 9.8), then the requeue acts as an abort completion point for the call, and the call is cancelled and no requeue is performed;

- if the original entry call was timed (or conditional), then the original expiration time is the expiration time for the requeued call.

If the reserved words with abort do not appear, then the call remains protected against cancellation while queued as the result of the requeue_statement.

Ramification: This protection against cancellation lasts only until the call completes or a subsequent requeue-with-abort is performed on the call.

Reason: We chose to protect a requeue, by default, against abort or cancellation. This seemed safer, since it is likely that extra steps need to be taken to allow for possible cancellation once the servicing of an entry call has begun. This also means that in the absence of with abort the usual Ada 83 behavior is preserved, namely that once an entry call is accepted, it cannot be cancelled until it completes.

NOTE \{AI12-0300-1\} A requeue is permitted from a single entry to an entry of an entry family, or vice-versa. The entry index, if any, plays no part in the subtype conformance check between the profiles of the two entries; an entry index is part of the entry_name for an entry of a family.

Examples of requeue statements:

requeue Request (Medium) with abort;
   --requeue on a member of an entry family of the current task, see 9.1

requeue Flags (I).Seize;
   --requeue on an entry of an array component, see 9.4

The requeue_statement is new.

Extensions to Ada 83

Extensions to Ada 2005

\{AI05-0030-2\} \{AI05-0215-1\} Added the ability to requeue on operations of synchronized interfaces that are declared to be an entry.

Inconsistencies With Ada 2012

\{AI12-0090-1\} Corrigendum: We now define that any preconditions of the requeue target are evaluated as part of a requeue_statement. Original Ada 2012 did not specify this, so a program that requeues when the preconditions fail will raise an exception when none would happen in original Ada 2012. We don't expect this to be a problem, as in that case, the entry body would be called with some of its preconditions evaluating as False; the body is likely to assume that they are true and probably will have failed in some other way anyway.

\{AI12-0335-1\} Correction: We now include an accessibility check on requeues. This means Program_Error could be raised for a requeue that worked in Ada 2012; This can only fail for an object for which the statically deeper relationship does not apply, for instance a stand-alone object of an anonymous access type. Most programs that are
affected are erroneous anyway (as they will eventually use a nonexistent object), so we do not believe this will matter in practice.

Incompatibilities With Ada 2012

20.a/4 {AI12-0090-1} Corrigendum: If a requeue target has a different postcondition than the original entry, the requeue is now illegal. In such a case, the original postcondition would never have been evaluated, and assumptions that the caller relied upon might not be true. A requeue should be invisible to the caller with respect to any postconditions, thus we only allow it when the original entry has no postconditions or the requeue target has (at least) the same postconditions.

Wording Changes from Ada 2012

20.b/5 {AI12-0143-1} Added a Legality Rule for the new Index attribute (see 6.1.1).

9.6 Delay Statements, Duration, and Time

[ A delay_statement is used to block further execution until a specified expiration time is reached. The expiration time can be specified either as a particular point in time (in a delay_until_statement), or in seconds from the current time (in a delay_relative_statement). The language-defined package Calendar provides definitions for a type Time and associated operations, including a function Clock that returns the current time. ]

Syntax

2 delay_statement ::= delay_until_statement | delay_relative_statement
3 delay_until_statement ::= delay until delay_expression;
4 delay_relative_statement ::= delay delay_expression;

Name Resolution Rules

5 The expected type for the delay_expression in a delay_relative_statement is the predefined type Duration. The delay_expression in a delay_until_statement is expected to be of any nonlimited type.

Legality Rules

6/3 {AI05-0092-1} There can be multiple time bases, each with a corresponding clock, and a corresponding time type. The type of the delay_expression in a delay_until_statement shall be a time type — either the type Time defined in the language-defined package Calendar (see below), the type Time in the package Real_Time (see D.8), or some other implementation-defined time type (see D.8).

Implementation defined: Any implementation-defined time types.

Static Semantics

7 [There is a predefined fixed point type named Duration, declared in the visible part of package Standard;} a value of type Duration is used to represent the length of an interval of time, expressed in seconds. [The type Duration is not specific to a particular time base, but can be used with any time base.]

8/3 {AI05-0092-1} A value of the type Time in package Calendar, or of some other implementation-defined time type, represents a time as reported by a corresponding clock.

The following language-defined library package exists:

9/10/5 {AI12-0241-1} {AI12-0302-1}
package Ada.Calendar
with Nonblocking, Global => in out synchronized is
  type Time is private;
{AI95-00351-01} subtype Year_Number is Integer range 1901 .. 2399;
subtype Month_Number is Integer range 1 .. 12;
subtype Day_Number is Integer range 1 .. 31;
subtype Day_Duration is Duration range 0.0 .. 86_400.0;

Reason: {AI95-00351-01} A range of 500 years was chosen, as that only requires one extra bit for the year as compared to Ada 95. This was done to minimize disruptions with existing implementations. (One implementor reports that their time values represent nanoseconds, and this year range requires 63.77 bits to represent.)

function Clock return Time;
function Year (Date : Time) return Year_Number;
function Month (Date : Time) return Month_Number;
function Day (Date : Time) return Day_Number;
function Seconds(Date : Time) return Day_Duration;
procedure Split (Date  : in Time;
    Year    : out Year_Number;
    Month   : out Month_Number;
    Day     : out Day_Number;
    Seconds : out Day_Duration);
function Time_Of(Year  : Year_Number;
    Month   : Month_Number;
    Day     : Day_Number;
    Seconds : Day_Duration := 0.0) return Time;
function "+" (Left : Time;   Right : Duration) return Time;
function "+" (Left : Duration; Right : Time) return Time;
function "-" (Left : Time;   Right : Duration) return Time;
function "-" (Left : Time;   Right : Time) return Duration;
function "<" (Left, Right : Time) return Boolean;
function "<="(Left, Right : Time) return Boolean;
function ">" (Left, Right : Time) return Boolean;
function ">="(Left, Right : Time) return Boolean;

Time_Error : exception;

private
... -- not specified by the language
end Ada.Calendar;

Dynamic Semantics

For the execution of a delay_statement, the delay_expression is first evaluated. For a delay_until_statement, the expiration time for the delay is the value of the delay_expression, in the time base associated with the type of the expression. For a delay_relative_statement, the expiration time is defined as the current time, in the time base associated with relative delays, plus the value of the delay_expression converted to the type Duration, and then rounded up to the next clock tick. The time base associated with relative delays is as defined in D.9, “Delay Accuracy” or is implementation defined.

Implementation defined: The time base associated with relative delays.

Ramification: Rounding up to the next clock tick means that the reading of the delay-relative clock when the delay expires should be no less than the current reading of the delay-relative clock plus the specified duration.

The task executing a delay_statement is blocked until the expiration time is reached, at which point it becomes ready again. If the expiration time has already passed, the task is not blocked.

Discussion: For a delay_relative_statement, this case corresponds to when the value of the delay_expression is zero or negative.

Even though the task is not blocked, it might be put back on the end of its ready queue. See D.2, “Priority Scheduling”.

{AI05-0092-1} If an attempt is made to cancel the delay_statement [(as part of an asynchronous_select or abort — see 9.7.4 and 9.8)], the statement_statement is cancelled if the expiration time has not yet passed, thereby completing the delay_statement.
Reason: This is worded this way so that in an asynchronous_select where the triggering_statement is a delay_statement, an attempt to cancel the delay when the abortable_part completes is ignored if the expiration time has already passed, in which case the optional statements of the triggering_alternative are executed.

The time base associated with the type Time of package Calendar is implementation defined. The function Clock of package Calendar returns a value representing the current time for this time base. [The implementation-defined value of the named number System.Tick (see 13.7) is an approximation of the length of the real-time interval during which the value of Calendar.Clock remains constant.]

Implementation defined: The time base of the type Calendar.Time.

Implementation defined: The time zone used for package Calendar operations.

Ramification: The behavior of these values and subprograms if the time zone changes is also implementation-defined. In particular, the changes associated with summer time adjustments (like Daylight Savings Time in the United States) should be treated as a change in the implementation-defined time zone. The language does not specify whether the time zone information is stored in values of type Time; therefore the results of binary operators are unspecified when the operands are the two values with different effective time zones. In particular, the results of "-" may differ from the "real" result by the difference in the time zone adjustment. Similarly, the result of UTC_Time_Offset (see 9.6.1) may or may not reflect a time zone adjustment.

If Time_Of is called with a seconds value of 86400.0, the value returned is equal to the value of Time_Of for the next day with a seconds value of 0.0. The value returned by the function Seconds or through the Seconds parameter of the procedure Split is always less than 86400.0.

The exception Time_Error is raised by the function Time_Of if the actual parameters do not form a proper date. This exception is also raised by the operators "+" and "-" if the result is not representable in the type Time or Duration, as appropriate. This exception is also raised by the functions Year, Month, Day, and Seconds and or the procedure Split if the year number of the given date is outside of the range of the subtype Year_Number.

To be honest: By "proper date" above we mean that the given year has a month with the given day. For example, February 29th is a proper date only for a leap year. We do not mean to include the Seconds in this notion; in particular, we do not mean to require implementations to check for the "missing hour" that occurs when Daylight Savings Time starts in the spring.

Reason: We allow Year and Split to raise Time_Error because the arithmetic operators are allowed (but not required) to produce times that are outside the range of years from 1901 to 2399. This is similar to the way integer operators may return values outside the base range of their type so long as the value is mathematically correct. We allow the functions Month, Day and Seconds to raise Time_Error so that they can be implemented in terms of Split.

Implementation Requirements

The implementation of the type Duration shall allow representation of time intervals (both positive and negative) up to at least 86400 seconds (one day); Duration'Small shall not be greater than twenty milliseconds. The implementation of the type Time shall allow representation of all dates with year numbers in the range of Year_Number; it may allow representation of other dates as well (both earlier and later).]

Implementation Permissions

An implementation may define additional time types (see D.8).
An implementation may raise Time_Error if the value of a delay_expression in a delay_until_statement of a select_statement represents a time more than 90 days past the current time. The actual limit, if any, is implementation-defined.

**Implementation defined:** Any limit on delay_until_statements of select_statements.

**Implementation Note:** This allows an implementation to implement select_statement timeouts using a representation that does not support the full range of a time type. In particular 90 days of seconds can be represented in 23 bits, allowing a signed 24-bit representation for the seconds part of a timeout. There is no similar restriction allowed for stand-alone delay_until_statements, as these can be implemented internally using a loop if necessary to accommodate a long delay.

**Implementation Advice**

Whenever possible in an implementation, the value of Duration'Small should be no greater than 100 microseconds.

**Implementation Note:** This can be satisfied using a 32-bit 2's complement representation with a small of 2.0**(-14) — that is, 61 microseconds — and a range of ± 2.0**17 — that is, 131_072.0.

**Implementation Advice:** The value of Duration'Small should be no greater than 100 microseconds.

{AI12-0444-1} The time base for delay_relative_statements should be monotonic; it can be different than the need not be the same time base as used for Calendar.Clock.

**Implementation Advice:** The time base for delay_relative_statements should be monotonic.

**NOTE 1** A delay_relative_statement with a negative value of the delay_expression is equivalent to one with a zero value.

**NOTE 2** {AI12-0440-1} A delay_statement cannot be executed by the environment task; consequently delay_statements cannot be executed as part of the elaboration of a library_item or the execution of the main subprogram. Such statements delay the environment task (see 10.2).

**NOTE 3** A delay_statement is an abort completion point and a potentially blocking operation, even if the task is not actually blocked.

**NOTE 4** There is no necessary relationship between System.Tick (the resolution of the clock of package Calendar) and Duration'Small (the small of type Duration).

**Ramification:** The inaccuracy of the delay_statement has no relation to System.Tick. In particular, it is possible that the clock used for the delay_statement is less accurate than Calendar.Clock.

We considered making Tick a run-time-determined quantity, to allow for easier configurability. However, this would not be upward compatible, and the desired configurability can be achieved using functionality defined in Annex D, “Real-Time Systems”.

**NOTE 5** Additional requirements associated with delay_statements are given in D.9, “Delay Accuracy”.

**Examples**

**Example of a relative delay statement:**

```
delay 3.0;  -- delay 3.0 seconds
```

**Example of a periodic task:**

```
declare
  use Ada.Calendar;
  Next_Time : Time := Clock + Period;
  -- Period is a global constant of type Duration
begin
  loop
    -- repeated every Period seconds
    delay until Next_Time;
    ...  -- perform some actions
    Next_Time := Next_Time + Period;
  end loop;
end;
```
9.6 Delay Statements, Duration, and Time

9.6.1 Formatting, Time Zones, and other operations for Time

Static Semantics

The following language-defined library packages exist:

package Ada.Calendar.Time_Zones

with Nonblocking, Global => in out synchronized is

-- Time zone manipulation:

type Time_Offset is range -28*60 .. 28*60;

Reason: We want to be able to specify the difference between any two arbitrary time zones. You might think that 1440 (24 hours) would be enough, but there are places (like Tonga, which is UTC+13hr) which are more than 12 hours different than UTC. Combined with summer time (known as daylight saving time in some parts of the world) – which switches opposite in the northern and southern hemispheres – and even greater differences are possible. We know of cases of a 26 hours difference, so we err on the safe side by selecting 28 hours as the limit.

Unknown_Zone_Error : exception;

function Local_Time_OffsetUTC_Time_Offset (Date : Time := Clock) return Time_Offset;

to renames Local_Time_Offset;

end Ada.Calendar.Time_Zones;

package Ada.Calendar.Arithmetic

with Nonblocking, Global => in out synchronized is

-- Arithmetic on days:
type Day_Count is range -366*(1+Year_Number'Last - Year_Number'First) .. 366*(1+Year_Number'Last - Year_Number'First);

subtype Leap_Seconds_Count is Integer range -2047 .. 2047;

Reason: The maximum number of leap seconds is likely to be much less than this, but we don't want to reach the limit too soon if the earth's behavior suddenly changes. We believe that the maximum number is 1612, based on the current rules, but that number is too weird to use here.

procedure Difference (Left, Right : in Time;
                      Days : out Day_Count;
                      Seconds : out Duration;
                      Leap_Seconds : out Leap_Seconds_Count);

function "+" (Left : Time; Right : Day_Count) return Time;
function "+" (Left : Day_Count; Right : Time) return Time;
function "-" (Left : Time; Right : Day_Count) return Time;
function "-" (Left, Right : Time) return Day_Count;

end Ada.Calendar.Arithmetic;

{AI12-0241-1} {AI12-0302-1}
with Ada.Calendar.Time_Zones;
package Ada.Calendar.Formatting
with Nonblocking, Global => in out synchronized is

-- Day of the week:

type Day_Name is (Monday, Tuesday, Wednesday, Thursday,
                  Friday, Saturday, Sunday);

function Day_of_Week (Date : Time) return Day_Name;

-- Hours:Minutes:Seconds access:

subtype Hour_Number is Natural range 0 .. 23;
subtype Minute_Number is Natural range 0 .. 59;
subtype Second_Number is Natural range 0 .. 59;
subtype Second_Duration is Day_Duration range 0.0 .. 1.0;

function Year       (Date : Time; Time_Zone : Time_Zones.Time_Offset := 0)
                      return Year_Number;
function Month      (Date : Time; Time_Zone : Time_Zones.Time_Offset := 0)
                      return Month_Number;
function Day        (Date : Time; Time_Zone : Time_Zones.Time_Offset := 0)
                      return Day_Number;
function Hour       (Date : Time; Time_Zone : Time_Zones.Time_Offset := 0)
                      return Hour_Number;
function Minute     (Date : Time; Time_Zone : Time_Zones.Time_Offset := 0)
                      return Minute_Number;
function Second     (Date : Time)
                      return Second_Number;
function Sub_Second (Date : Time)
                      return Second_Duration;
function Seconds_Of (Hour : Hour_Number;
                      Minute : Minute_Number;
                      Second : Second_Number := 0;
                      Sub_Second : Second_Duration := 0.0)
                      return Day_Duration;
procedure Split (Seconds : in Day_Duration;
    Hour : out Hour_Number;
    Minute : out Minute_Number;
    Second : out Second_Number;
    Sub Second : out Second_Duration);

function Time_Of (Year       : Year_Number;
    Month      : Month_Number;
    Day        : Day_Number;
    Hour       : Hour_Number;
    Minute     : Minute_Number;
    Second     : Second_Number;
    Sub Second : Second_Duration := 0.0;
    Leap Second: Boolean := False;
    Time Zone  : Time_Zones.Time_Offset := 0)
    return Time;

function Time_Of (Year       : Year_Number;
    Month      : Month_Number;
    Day        : Day_Number;
    Seconds    : Day_Duration := 0.0;
    Leap_Second: Boolean := False;
    Time_Zone  : Time_Zones.Time_Offset := 0)
    return Time;

procedure Split (Date       : in Time;
    Year       : out Year_Number;
    Month      : out Month_Number;
    Day        : out Day_Number;
    Hour       : out Hour_Number;
    Minute     : out Minute_Number;
    Second     : out Second_Number;
    Sub Second : out Second_Duration;
    Time_Zone  : in Time_Zones.Time_Offset := 0);

procedure Split (Date       : in Time;
    Year       : out Year_Number;
    Month      : out Month_Number;
    Day        : out Day_Number;
    Hour       : out Hour_Number;
    Minute     : out Minute_Number;
    Second     : out Second_Number;
    Sub Second : out Second_Duration;
    Leap_Second: out Boolean;
    Time_Zone  : in Time_Zones.Time_Offset := 0);

procedure Split (Date       : in Time;
    Year       : out Year_Number;
    Month      : out Month_Number;
    Day        : out Day_Number;
    Seconds    : out Day_Duration;
    Leap_Second: out Boolean;
    Time Zone   : in Time Zones.Time_Offset := 0);

-- Simple image and value:
function Image (Date : Time;
    Include_Time_Fraction : Boolean := False;
    Time Zone : Time Zones.Time_Offset := 0) return String;

function Local_Image (Date : Time;
    Include_Time_Fraction : Boolean := False)
    return String is
    (Image (Date, Include_Time_Fraction,
        Time Zones.Local_Time_Offset (Date)));

function Value (Date : String;
    Time Zone : Time Zones.Time_Offset := 0) return Time;

function Image (Elapsed Time : Duration;
    Include_Time_Fraction : Boolean := False) return String;

function Value (Elapsed Time : String) return Duration;
Type \texttt{Time_Offset} represents for a given locality at a given moment the number of minutes the local time is, at that moment, ahead (+) or behind (-) Coordinated Universal Time (abbreviated UTC). The Time_Offset for UTC is zero.

Function \texttt{Local\_Time\_Offset} returns, as a number of minutes, the difference between the implementation-defined time zone of Calendar and another time zone.

Procedure \texttt{Difference} returns the difference between \texttt{Left} and \texttt{Right}. Days is the number of days of difference, Seconds is the remainder seconds of difference excluding leap seconds, and Leap_Seconds is the number of leap seconds. If \texttt{Left} < \texttt{Right}, then Seconds <= 0.0, Days <= 0, and \texttt{Leap\_Seconds} <= 0. Otherwise, all values are nonnegative. The absolute value of Seconds is always less than 86 400.0. For the returned values, if Days = 0, then Seconds + Duration(Leap\_Seconds) = Calendar."-"(Left, Right).

Function \texttt{"+"} adds a number of days to a time value. Time\_Error is raised if the result is not representable as a value of type Time.

Function \texttt{"-"} subtracts a number of days from a time value. Time\_Error is raised if the result is not representable as a value of type Time.

Function \texttt{Day\_of\_Week} returns the day of the week for Time. This is based on the Year, Month, and Day values of Time.
function Year (Date : Time; 
          Time Zone : Time_Zones.Time_Offset := 0) 
          return Year_Number;

{AI95-00427-01} Returns the year for Date, as appropriate for the specified time zone offset.

function Month (Date : Time; 
             Time Zone : Time_Zones.Time_Offset := 0) 
             return Month_Number;

{AI95-00427-01} Returns the month for Date, as appropriate for the specified time zone offset.

function Day (Date : Time; 
             Time Zone : Time_Zones.Time_Offset := 0) 
             return Day_Number;

{AI95-00427-01} Returns the day number for Date, as appropriate for the specified time zone offset.

function Hour (Date : Time; 
              Time Zone : Time_Zones.Time_Offset := 0) 
              return Hour_Number;

{AI95-00351-01} Returns the hour for Date, as appropriate for the specified time zone offset.

function Minute (Date : Time; 
                Time Zone : Time_Zones.Time_Offset := 0) 
                return Minute_Number;

{AI95-00351-01} Returns the minute within the hour for Date, as appropriate for the specified time zone offset.

function Second (Date : Time) 
                return Second_Number;

{AI95-00351-01} Returns the second within the hour and minute for Date.

function Sub_Second (Date : Time) 
                  return Second_Duration;

{AI95-00351-01} Returns the fraction of second for Date (this has the same accuracy as Day_Duration). The value returned is always less than 1.0.

function Seconds_Of (Hour   : Hour_Number; 
                      Minute : Minute_Number; 
                      Second : Second_Number := 0; 
                      Sub_Second : Second_Duration := 0.0) 
                      return Day_Duration;

{AI95-00351-01} Returns a Day_Duration value for the combination of the given Hour, Minute, Second, and Sub_Second. This value can be used in Calendar.Time_Of as well as the argument to Calendar."+" and Calendar."-". If Seconds_Of is called with a Sub_Second value of 1.0, the value returned is equal to the value of Seconds_Of for the next second with a Sub_Second value of 0.0.

procedure Split (Seconds    : in Day_Duration; 
                Hour       : out Hour_Number; 
                Minute     : out Minute_Number; 
                Second     : out Second_Number; 
                Sub_Second : out Second_Duration); 

{AI95-00351-01} Splits Seconds into Hour, Minute, Second and Sub_Second in such a way that the resulting values all belong to their respective subtypes. The value returned in the Sub_Second parameter is always less than 1.0. If Seconds = 86400.0, Split propagates Time_Error.
Ramification: There is only one way to do the split which meets all of the requirements.

Reason: {AI05-0238-1} If Seconds = 86400.0, one of the returned values would have to be out of its defined range (either Sub_Second = 1.0 or Hour = 24 with the other value being 0). This doesn't seem worth breaking the invariants.

function Time_Of (Year       : Year_Number;
                Month      : Month_Number;
                Day        : Day_Number;
                Hour       : Hour_Number;
                Minute     : Minute_Number;
                Second     : Second_Number;
                Sub_Second : Second_Duration := 0.0;
                Leap_Second: Boolean := False;
                Time_Zone  : Time_Zones.Time_Offset := 0)
return Time;

{AI95-00351-01} {AI95-00427-01} If Leap_Second is False, returns a Time built from the date and time values, relative to the specified time zone offset. If Leap_Second is True, returns the Time that represents the time within the leap second that is one second later than the time specified by the other parameters. Time_Error is raised if the parameters do not form a proper date or time. If Time_Of is called with a Sub_Second value of 1.0, the value returned is equal to the value of Time_Of for the next second with a Sub_Second value of 0.0.

Discussion: Time_Error should be raised if Leap_Second is True, and the date and time values do not represent the second before a leap second. A leap second always occurs at midnight UTC, and is 23:59:60 UTC in ISO notation. So, if the time zone is UTC and Leap_Second is True, if any of Hour /= 23, Minute /= 59, or Second /= 59, then Time_Error should be raised. However, we do not say that, because other time zones will have different values where a leap second is allowed.

function Time_Of (Year       : Year_Number;
                Month      : Month_Number;
                Day        : Day_Number;
                Seconds    : Day_Duration := 0.0;
                Leap_Second: Boolean := False;
                Time_Zone  : Time_Zones.Time_Offset := 0)
return Time;

{AI95-00351-01} {AI95-00427-01} If Leap_Second is False, returns a Time built from the date and time values, relative to the specified time zone offset. If Leap_Second is True, returns the Time that represents the time within the leap second that is one second later than the time specified by the other parameters. Time_Error is raised if the parameters do not form a proper date or time. If Time_Of is called with a Seconds value of 86 400.0, the value returned is equal to the value of Time_Of for the next day with a Seconds value of 0.0.

procedure Split (Date       : in Time;
                Year       : out Year_Number;
                Month      : out Month_Number;
                Day        : out Day_Number;
                Hour       : out Hour_Number;
                Minute     : out Minute_Number;
                Second     : out Second_Number;
                Sub_Second : out Second_Duration;
                Leap_Second: out Boolean;
                Time_Zone  : in Time_Zones.Time_Offset := 0);

{AI95-00351-01} {AI95-00427-01} If Date does not represent a time within a leap second, splits Date into its constituent parts (Year, Month, Day, Hour, Minute, Second, Sub_Second), relative to the specified time zone offset, and sets Leap_Second to False. If Date represents a time within a leap second, set the constituent parts to values corresponding to a time one second earlier than that given by Date, relative to the specified time zone offset, and sets Leap_Seconds to True. The value returned in the Sub_Second parameter is always less than 1.0.
procedure Split (Date       : in Time;
Year       : out Year_Number;
Month      : out Month_Number;
Day        : out Day_Number;
Hour       : out Hour_Number;
Minute     : out Minute_Number;
Second     : out Second_Number;
Sub_Second : out Second_Duration;
Time_Zone  : in Time_Zones.Time_Offset := 0);

{AI95-00351-01} {AI95-00427-01} Splits Date into its constituent parts (Year, Month, Day, Hour, Minute, Second, Sub_Second), relative to the specified time zone offset. The value returned in the Sub_Second parameter is always less than 1.0.

procedure Split (Date       : in Time;
Year       : out Year_Number;
Month      : out Month_Number;
Day        : out Day_Number;
Seconds    : out Day_Duration;
Leap_Second: out Boolean;
Time_Zone  : in Time_Zones.Time_Offset := 0);

{AI95-00351-01} {AI95-00427-01} If Date does not represent a time within a leap second, splits Date into its constituent parts (Year, Month, Day, Seconds), relative to the specified time zone offset, and sets Leap_Second to False. If Date represents a time within a leap second, set the constituent parts to values corresponding to a time one second earlier than that given by Date, relative to the specified time zone offset, and sets Leap_Seconds to True. The value returned in the Seconds parameter is always less than 86_400.0.

function Image (Date : Time;
Include_Time_Fraction : Boolean := False;
Time_Zone  : Time_Zones.Time_Offset := 0) return String;

{AI95-00351-01} Returns a string form of the Date relative to the given Time_Zone. The format is "Year-Month-Day Hour:Minute:Second", where the Year is a 4-digit value, and all others are 2-digit values, of the functions defined in Calendar and Calendar.Formatting, including a leading zero, if needed. The separators between the values are a minus, another minus, a colon, and a single space between the Day and Hour. If Include_Time_Fraction is True, the integer part of Sub_Seconds*100 is suffixed to the string as a point followed by a 2-digit value.

Discussion: The Image provides a string in ISO 8601 format, the international standard time format. Alternative representations allowed in ISO 8601 are not supported here.

ISO 8601 allows 24:00:00 for midnight; and a seconds value of 60 for leap seconds. These are not allowed here (the routines mentioned above cannot produce those results).

Ramification: The fractional part is truncated, not rounded. It would be quite hard to define the result with proper rounding, as it can change all of the values of the image. Values can be rounded up by adding an appropriate constant (0.5 if Include_Time_Fraction is False, 0.005 otherwise) to the time before taking the image.

function Value (Date : String;
Time_Zone  : Time_Zones.Time_Offset := 0) return Time;

{AI95-00351-01} Returns a Time value for the image given as Date, relative to the given time zone. Constraint_Error is raised if the string is not formatted as described for Image, or the function cannot interpret the given string as a Time value.

Discussion: The intent is that the implementation enforce the same range rules on the string as the appropriate function Time_Of, except for the hour, so “cannot interpret the given string as a Time value” happens when one of the values is out of the required range. For example, "2005-08-31 24:00:000049" should raise Constraint_Error (the hour is out of range).
function Image (Elapsed_Time : Duration; Include_Time_Fraction : Boolean := False) return String;

{A195-00351-01} {A112-0445-1} Returns a string form of the Elapsed Time. The format is "Hour:Minute:Second", where all values are 2-digit values, including a leading zero, if necessary. The separators between the values are colons. If Include_Time_Fraction is True, the integer part of Sub_Seconds*100 is suffixed to the string as a point followed by a 2-digit value. If Elapsed_Time < 0.0, the result is Image (abs Elapsed_Time, Include_Time_Fraction) prefixed with a minus sign. If abs Elapsed_Time represents 100 hours or more, the result is implementation-defined.

Implementation defined: The result of Calendar.Formatting.Image if its argument represents more than 100 hours.

Implementation Note: This cannot be implemented (directly) by calling Calendar.Formatting.Split, since it may be out of the range of Day.Duration, and thus the number of hours may be out of the range of Hour_Number.
If a Duration value can represent more then 100 hours, the implementation will need to define a format for the return of Image.

function Value (Elapsed_Time : String) return Duration;

{A195-00351-01} Returns a Duration value for the image given as Elapsed_Time. Constraint_Error is raised if the string is not formatted as described for Image, or the function cannot interpret the given string as a Duration value.

Discussion: The intent is that the implementation enforce the same range rules on the string as the appropriate function Time_Of, except for the hour, so “cannot interpret the given string as a Time value” happens when one of the values is out of the required range. For example, "10:23:60" should raise Constraint_Error (the seconds value is out of range).

Implementation Advice

{A195-00351-01} An implementation should support leap seconds if the target system supports them. If leap seconds are not supported, Difference should return zero for Leap_Seconds, Split should return False for Leap_Second, and Time_Of should raise Time_Error if Leap_Second is True.

Implementation Advice: Leap seconds should be supported if the target system supports them. Otherwise, operations in Calendar.Formatting should return results consistent with no leap seconds.

Discussion: An implementation can always support leap seconds when the target system does not; indeed, this isn’t particularly hard (all that is required is a table of when leap seconds were inserted). As such, leap second support isn’t “impossible or impractical” in the sense of 1.1.3. However, for some purposes, it may be important to follow the target system’s lack of leap second support (if the target is a GPS satellite, which does not use leap seconds, leap second support would be a handicap to work around). Thus, this Implementation Advice should be read as giving permission to not support leap seconds on target systems that don’t support leap seconds. Implementers should use the needs of their customers to determine whether or not support leap seconds on such targets.

NOTE 1 {A195-00351-01} {A112-0336-1} {A112-0442-1} The implementation-defined time zone of package Calendar cannot, but need not, be the local time zone. Local_Time_OffsetUTC_Time_Offset always returns the difference relative to the implementation-defined time zone of package Calendar. If Local_Time_OffsetUTC_Time_Offset does not raise Unknown_Zone_Error, UTC time can be safely calculated (within the accuracy of the underlying time-base).

Discussion: The time in the time zone known as Greenwich Mean Time (GMT) is generally very close to UTC time; for most purposes they can be treated the same. GMT is the time based on the rotation of the Earth; UTC is the time based on atomic clocks, with leap seconds periodically inserted to realign with GMT (because most human activities depend on the rotation of the Earth). At any point in time, there will be a sub-second difference between GMT and UTC.

NOTE 2 {A195-00351-01} {A112-0336-1} Calling Split on the results of subtracting Duration(Local_Time_OffsetUTC_Time_Offset*60) from Clock provides the components (hours, minutes, and so on) of the UTC time. In the United States, for example, Local_Time_OffsetUTC_Time_Offset will generally be negative.

Discussion: This is an illustration to help specify the value of Local_Time_OffsetUTC_Time_Offset. A user should pass zeroUTC_Time_Offset as the Time_Zone parameter of Split, rather than trying to make the above calculation.
Extensions to Ada 95

91.b/2 \{AI95-00351-01\} \{AI95-00428-01\} Packages Calendar.Time.Zones, Calendar.Arithmetic, and Calendar.Formatting are new.

Inconsistencies With Ada 2005

91.c/3 \{AI05-0238-1\} Correction: Defined that Split for Seconds raises Time_Error for a value of exactly 86400.0, rather than breaking some invariant or raising some other exception. Ada 2005 left this unspecified; a program that depended on what some implementation does might break, but such a program is not portable anyway.

Wording Changes from Ada 2005

91.d/3 \{AI05-0119-1\} Correction: Clarified the sign of UTC_Time_Offset.

Inconsistencies With Ada 2012

91.e/5 \{AI12-0336-1\} Correction: Changed the definition of Time_Offset to be compatible with most compilers. Also added Local_Time_Offset and Local_Image to better describe the intent. A program that expects the Ada 2012 definition of Time_Offset would get incorrect answers. However, most compilers tested use the revised definition, so the likelihood of a program breaking is quite low. Additionally, the new definitions could cause a use clause conflict; see the introduction of Annex A for more on this topic.

9.7 Select Statements

[There are four forms of the select_statement. One form provides a selective wait for one or more select_alternatives. Two provide timed and conditional entry calls. The fourth provides asynchronous transfer of control.]

Syntax

select_statement ::= selective_accept | timed_entry_call | conditional_entry_call | asynchronous_select

Examples

Example of a select statement:

select
  accept Driver_Awake_Signal;
  or
  delay 30.0*Seconds;
  Stop_The_Train;
end select;

Extensions to Ada 83

4.a Asynchronous_select is new.

9.7.1 Selective Accept

[This form of the select_statement allows a combination of waiting for, and selecting from, one or more alternatives. The selection may depend on conditions associated with each alternative of the selective_accept.]

Syntax

selective_accept ::= select

[guard]
  select_alternative
{ or
  [guard]
  select_alternative }
[else
  sequence_of_statements ]
end select;

guard ::= when condition =>

select_alternative ::= 
  accept_alternative 
  | delay_alternative 
  | terminate_alternative

accept_alternative ::= 
  accept_statement [sequence_of_statements]

delay_alternative ::= 
  delay_statement [sequence_of_statements]

terminate_alternative ::= terminate;

A selective_accept shall contain at least one accept_alternative. In addition, it can contain:

• a terminate_alternative (only one); or
• one or more delay_alternatives; or
• an else part (the reserved word else followed by a sequence_of_statements).

These three possibilities are mutually exclusive.

Legality Rules

If a selective_accept contains more than one delay_alternative, then all shall be delay_relative_statements, or all shall be delay_until_statements for the same time type.

Reason: This simplifies the implementation and the description of the semantics.

Dynamic Semantics

A select_alternative is said to be open if it is not immediately preceded by a guard, or if the condition of its guard evaluates to True. It is said to be closed otherwise.

For the execution of a selective_accept, any guard conditions are evaluated; open alternatives are thus determined. For an open delay_alternative, the delay_expression is also evaluated. Similarly, for an open accept_alternative for an entry of a family, the entry_index is also evaluated. These evaluations are performed in an arbitrary order, except that a delay_expression or entry_index is not evaluated until after evaluating the corresponding condition, if any. Selection and execution of one open alternative, or of the else part, then completes the execution of the selective_accept; the rules for this selection are described below.

Open accept_alternatives are first considered. Selection of one such alternative takes place immediately if the corresponding entry already has queued calls. If several alternatives can thus be selected, one of them is selected according to the entry queuing policy in effect (see 9.5.3 and D.4). When such an alternative is selected, the selected call is removed from its entry queue and the handled_sequence_of_statements (if any) of the corresponding accept_statement is executed; after the rendezvous completes
any subsequent sequence_of_statements of the alternative is executed. If no selection is immediately possible (in the above sense) and there is no else part, the task blocks until an open alternative can be selected.

Selection of the other forms of alternative or of an else part is performed as follows:

- An open delay_alternative is selected when its expiration time is reached if no accept_alternative or other delay_alternative can be selected prior to the expiration time. If several delay_alternatives have this same expiration time, one of them is selected according to the queuing policy in effect (see D.4); the default queuing policy chooses arbitrarily among the delay_alternatives whose expiration time has passed.

- The else part is selected and its sequence_of_statements is executed if no accept_alternative can immediately be selected; in particular, if all alternatives are closed.

- \{AI05-0299-1\} \{AI12-0449-1\} An open terminate_alternative is selected if the conditions stated at the end of subclause clause 9.3 are satisfied.

Ramification: In the absence of a requeue_statement, the conditions stated are such that a terminate_alternative cannot be selected while there is a queued entry call for any entry of the task. In the presence of requeues from a task to one of its subtasks, it is possible that when a terminate_alternative of the subtask is selected, requeued calls (for closed entries only) might still be queued on some entry of the subtask. Tasking_Error will be propagated to such callers, as is usual when a task completes while queued callers remain.

The exception Program_Error is raised if all alternatives are closed and there is no else part.

NOTE \{AI12-0447-1\} A selective_accept can be allowed to have several open delay_alternatives. A selective_accept can be allowed to have several open accept_alternatives for the same entry.

Examples

task body Server is
        Current_Work_Item : Work_Item;
begin
        loop
            select
                accept Next_Work_Item(WI : in Work_Item) do
                    Current_Work_Item := WI;
                end;
                Process_Work_Item(Current_Work_Item);
            or
                accept Shut_Down;
                exit; -- Premature Shut down requested
            or
                terminate; -- Normal shutdown at end of scope
            end select;
        end loop;
end Server;

Wording Changes from Ada 83

The name of selective_wait was changed to selective_accept to better describe what is being waited for. We kept select_alternative as is, because selective_accept_alternative was too easily confused with accept_alternative.

9.7.2 Timed Entry Calls

[A timed_entry_call issues an entry call that is cancelled if the call (or a requeue-with-abort of the call) is not selected before the expiration time is reached. A procedure call may appear rather than an entry call for cases where the procedure can be implemented by an entry.]

9.7.1 Selective Accept

10 October 2023  548
Syntax

timed_entry_call ::= select
   entry_call_alternative
   or
   delay_alternative
end select;

\{AI95-00345-01\}  entry_call_alternative ::= procedure_or_entry_callentry_call_statement [sequence_of_statements]

\{AI95-00345-01\}  procedure_or_entry_call ::= procedure_call_statement | entry_call_statement

Legality Rules

\{AI95-00345-01\}  If a procedure call statement is used for a procedure or entry call, the
   procedure name or procedure prefix of the procedure call statement shall statically denote an entry
   renamed as a procedure or (a view of) a primitive subprogram of a limited interface whose first parameter
   is a controlling parameter (see 3.9.2).

   \textbf{Reason:} This would be a confusing way to call a procedure, so we only allow it when it is possible that the procedure
   is actually an entry. We could have allowed formal subprograms here, but we didn't because we'd have to allow all
   formal subprograms, and it would increase the difficulty of generic code sharing.

   We say “statically denotes” because an access-to-subprogram cannot be primitive, and we don't have anything like
   access-to-entry. So only names of entries or procedures are possible.

Static Semantics

\{AI95-00345-01\}  \{AI05-0291-1\}  If a procedure call statement is used for a procedure or entry call,
   and the procedure is implemented by an entry, then the procedure name, or procedure prefix and
   possibly the first parameter of the procedure call statement, determine the target object of the call and
   the entry to be called.

   \textbf{Discussion:} The above says “possibly the first parameter”, because Ada allows entries to be renamed and passed as
   formal subprograms. In those cases, the task or protected object is implicit in the name of the routine; otherwise the
   object is an explicit parameter to the call.

Dynamic Semantics

\{AI95-00345-01\}  For the execution of a timed_entry_call, the entry_name, procedure name, or
   procedure prefix, and any actual parameters are evaluated, as for a simple entry call (see 9.5.3) or
   procedure call (see 6.4). The expiration time (see 9.6) for the call is determined by evaluating the
   delay_expression of the delay_alternative. If the call is an entry call or a call on a procedure
   implemented by an entry, the entry call is then issued. Otherwise, the call proceeds as described in 6.4
   for a procedure call, followed by the sequence_of_statements of the entry_call_alternative;
   the sequence_of_statements of the delay_alternative is ignored.

   If the call is queued (including due to a requeue-with-abort), and not selected before the expiration time is
   reached, an attempt to cancel the call is made. If the call completes due to the cancellation, the optional
   sequence_of_statements of the delay_alternative is executed; if the entry call completes normally, the
   optional sequence_of_statements of the entry_call_alternative is executed.

\textbf{Ramification:} \{AI95-00345-01\}  The fact that the syntax calls for an entry_call_statement
   means that this fact is used in overload resolution. For example, if there is a procedure X and an entry X (both with no
   parameters), then "select X; ..." is legal, because overload resolution knows that the entry is the one that was meant.

This paragraph was deleted.
Examples

Example of a timed entry call:

```ada
select
Controller.Request(Medium)(Some_Item);
or
delay 45.0;
-- controller too busy, try something else
end select;
```

Wording Changes from Ada 83

7.a/3 \{AI05-0299-1\} This subclause comes before the one for Conditional Entry Calls, so we can define conditional entry calls in terms of timed entry calls.

Incompatibilities With Ada 95

7.b/3 \{AI95-00345-01\} \{AI05-0005-1\} A procedure call can be used as the `entry_call_alternative` in a timed or conditional entry call, if the procedure might actually be an entry. Since the fact that something is an entry could be used in resolving these calls in Ada 95, it is possible for timed or conditional entry calls that resolved in Ada 95 to be ambiguous in Ada 2005. That could happen if both an entry and procedure with the same name and profile exist, which should be rare.

9.7.3 Conditional Entry Calls

1/5 \{AI95-00345-01\} \{AI12-0439-1\} A conditional `entry_call` issues an entry call that is then cancelled if it is not selected immediately (or if a requeue-with-abort of the call is not selected immediately). A procedure call may appear rather than an entry call for cases where the procedure might be implemented by an entry.

1.a To be honest: In the case of an entry call on a protected object, it is OK if the entry is closed at the start of the corresponding protected action, so long as it opens and the call is selected before the end of that protected action (due to changes in the Count attribute).

Syntax

```ada
conditional_entry_call ::= 
select
  entry_call_alternative
else
  sequence_of_statements
end select;
```

Dynamic Semantics

3 The execution of a conditional `entry_call` is defined to be equivalent to the execution of a timed `entry_call` with a `delay_alternative` specifying an immediate expiration time and the same `sequence_of_statements` as given after the reserved word `else`.

4/5 NOTE \{AI12-0440-1\} A conditional `entry_call` can briefly increase the Count attribute of the entry, even if the conditional call is not selected.
Example of a conditional entry call:

```
{AI12-0178-1} procedure Spin(R : in out Resource) is -- see 9.4
  begin
    loop
      select
        R.Seize;
        return;
      else
        null; -- busy waiting
      end select;
    end loop;
  end;
```

Wording Changes from Ada 83

```
{AI05-0299-1} This subclause comes after the one for Timed Entry Calls, so we can define conditional entry calls in terms of timed entry calls. We do that so that an "expiration time" is defined for both, thereby simplifying the definition of what happens on a requeue-with-abort.
```

9.7.4 Asynchronous Transfer of Control

[An asynchronous select_statement provides asynchronous transfer of control upon completion of an entry call or the expiration of a delay.]

Syntax

```
asynchronous_select ::= select
  triggering_alternative
  then abort
  abortable_part
  end select;

triggering_alternative ::= triggering_statement [sequence_of_statements]

{AI95-00345-01} triggering_statement ::= procedure_or_entry_call

abortable_part ::= sequence_of_statements
```

Dynamic Semantics

```
{AI95-00345-01} For the execution of an asynchronous_select whose triggering_statement is a procedure_or_entry_call an entry_call_statement, the entry_name, procedure_name, or procedure_prefix, and actual parameters are evaluated as for a simple entry call (see 9.5.3) or procedure call (see 6.4). If the call is an entry call or a call on a procedure implemented by an entry, and the entry call is issued. If the entry call is queued (or requeued-with-abort), then the abortable_part is executed. [If the entry call is selected immediately, and never requeued-with-abort, then the abortable_part is never started.] If the call is on a procedure that is not implemented by an entry, the call proceeds as described in 6.4, followed by the sequence_of_statements of the triggering_alternative; the abortable_part is never started.

For the execution of an asynchronous_select whose triggering_statement is a delay_statement, the delay_expression is evaluated and the expiration time is determined, as for a normal delay_statement. If the expiration time has not already passed, the abortable_part is executed.
```
If the `abortable_part` completes and is left prior to completion of the `triggering_statement`, an attempt to cancel the `triggering_statement` is made. If the attempt to cancel succeeds (see 9.5.3 and 9.6), the asynchronous `select` is complete.

If the `triggering_statement` completes other than due to cancellation, the `abortable_part` is aborted (if started but not yet completed — see 9.8). If the `triggering_statement` completes normally, the optional sequence_of_statements of the `triggering_alternative` is executed after the `abortable_part` is left.

Discussion: We currently don't specify when the by-copy `[in] out` parameters are assigned back into the actuals. We considered requiring that to happen after the `abortable_part` is left. However, that doesn't seem useful enough to justify possibly overspecifying the implementation approach, since some of the parameters are passed by reference anyway.

In an earlier description, we required that the sequence_of_statements of the `triggering_alternative` execute after aborting the `abortable_part`, but before waiting for it to complete and finalize, to provide more rapid response to the triggering event in case the finalization was unbounded. However, various reviewers felt that this created unnecessary complexity in the description, and a potential for undesirable concurrency (and nondeterminism) within a single task. We have now reverted to simpler, more deterministic semantics, but anticipate that further discussion of this issue might be appropriate during subsequent reviews. One possibility is to leave this area implementation defined, so as to encourage experimentation. The user would then have to assume the worst about what kinds of actions are appropriate for the sequence_of_statements of the `triggering_alternative` to achieve portability.

Examples

Example of a main command loop for a command interpreter:

```ada
loop
  select
    Terminal.Wait_For_Interrupt;
    Put_Line("Interrupted");
  then abort
    -- This will be abandoned upon terminal interrupt
    Put_Line("-> ");
    Get_Line(Command, Last);
    Process_Command(Command(1..Last));
  end select;
end loop;
```

Example of a time-limited calculation:

```ada
{AI12-0442-1} select
  delay 5.0;
  Put_Line("Calculation does not converge");
then abort
  -- This calculation is expected to finish in 5.0 seconds;
  -- if not, it is assumed to diverge.
  Horribly_Complicated_Recursive_Function(X, Y);
end select;
```

Note that these examples presume that there are abort completion points (see 9.8) within the execution of the `abortable_part`.

9.8 Abort of a Task - Abort of a Sequence of Statements

[An abort_statement causes one or more tasks to become abnormal, thus preventing any further interaction with such tasks. The completion of the `triggering_statement` of an asynchronous `select` causes a sequence_of_statements to be aborted.]
Syntax

abort_statement ::= abort task_name {, task_name};

Name Resolution Rules

{AI12-0444-1} Each task_name is expected to be of any task type; each can be of a different task type. not all be of the same task type.

Dynamic Semantics

For the execution of an abort_statement, the given task_names are evaluated in an arbitrary order. Each named task is then aborted, which consists of making the task abnormal and aborting the execution of the corresponding task_body, unless it is already completed.

Ramification: {AI95-00114-01} Note that aborting those tasks is not defined to be an abort-deferred operation. Therefore, if one of the named tasks is the task executing the abort_statement, or if the task executing the abort_statement depends on one of the named tasks, then it is possible for the execution of the abort_statement to be aborted, thus leaving some of the tasks un aborted. This allows the implementation to use either a sequence of calls to an “abort task” run-time system primitive, or a single call to an “abort list of tasks” run-time system primitive.

When the execution of a construct is aborted (including that of a task_body or of a sequence_of_statements), the execution of every construct included within the aborted execution is also aborted, except for executions included within the execution of an abort-deferred operation; the execution of an abort-deferred operation continues to completion without being affected by the abort; the following are the abort-deferred operations:

- a protected action;
- waiting for an entry call to complete (after having initiated the attempt to cancel it — see below);
- waiting for the termination of dependent tasks;
- the execution of an Initialize procedure as the last step of the default initialization of a controlled object;
- the execution of a Finalize procedure as part of the finalization of a controlled object;
- an assignment operation to an object with a controlled part.

[The last three of these are discussed further in 7.6.]

Reason: Deferring abort during Initialize and finalization allows, for example, the result of an allocator performed in an Initialize operation to be assigned into an access object without being interrupted in the middle, which would cause storage leaks. For an object with several controlled parts, each individual Initialize is abort-deferred. Note that there is generally no semantic difference between making each Finalize abort-deferred, versus making a group of them abort-deferred, because if the task gets aborted, the first thing it will do is complete any remaining finalizations. Individual objects are finalized prior to an assignment operation (if nonlimited controlled) and as part of Unchecked_Dele allocation.

Ramification: Abort is deferred during the entire assignment operation to an object with a controlled part, even if only some subcomponents are controlled. Note that this says “assignment operation”, not “assignment_statement”. Explicit calls to Initialize, Finalize, or Adjust are not abort-deferred.

When a master is aborted, all tasks that depend on that master are aborted.

The order in which tasks become abnormal as the result of an abort_statement or the abort of a sequence_of_statements is not specified by the language.

If the execution of an entry call is aborted, an immediate attempt is made to cancel the entry call (see 9.5.3). If the execution of a construct is aborted at a time when the execution is blocked, other than for an entry call, at a point that is outside the execution of an abort-deferred operation, then the execution of the construct completes immediately. For an abort due to an abort_statement, these immediate effects occur before the execution of the abort_statement completes. Other than for these immediate effects, the
execution of a construct that is aborted does not necessarily complete before the abort_statement completes. However, the execution of the aborted construct completes no later than its next abort completion point (if any) that occurs outside of an abort-deferred operation; the following are abort completion points for an execution:

- the point where the execution initiates the activation of another task;
- the end of the activation of a task;
- {AI12-0119-1} a point within a parallel construct where a new logical thread of control is created;
- {AI12-0119-1} the end of a parallel construct;
- the start or end of the execution of an entry call, accept_statement, delay_statement, or abort_statement;

Ramification: Although the abort completion point doesn't occur until the end of the entry call or delay_statement, these operations might be cut short because an abort attempts to cancel them.

- the start of the execution of a select_statement, or of the sequence_of_statements of an exception_handler.

Reason: The start of an exception_handler is considered an abort completion point simply because it is easy for an implementation to check at such points.

Implementation Note: Implementations may of course check for abort more often than at each abort completion point; ideally, a fully preemptive implementation of abort will be provided. If preemptive abort is not supported in a given environment, then supporting the checking for abort as part of subprogram calls and loop iterations might be a useful option.

Bounded (Run-Time) Errors

{AI05-0264-1} {AI12-0445-1} An attempt to execute an asynchronous_select as part of the execution of an abort-deferred operation is a bounded error. Similarly, an attempt to create a task that depends on a master that is included entirely within the execution of an abort-deferred operation is a bounded error. In both cases, Program_Error is raised if the error is detected by the implementation; otherwise, the operations proceed as they would outside an abort-deferred operation, except that an abort of the abortable_part or the created task does not necessarily have an effect.

Reason: An asynchronous_select relies on an abort of the abortable_part to effect the asynchronous transfer of control. For an asynchronous_select within an abort-deferred operation, the abort might have no effect.

Creating a task dependent on a master included within an abort-deferred operation is considered an error, because such tasks could be aborted while the abort-deferred operation was still progressing, undermining the purpose of abort-deferral. Alternatively, we could say that such tasks are abort-deferred for their entire execution, but that seems too easy to abuse. Note that task creation is already a bounded error in protected actions, so this additional rule only applies to local task creation as part of Initialize, Finalize, or Adjust.

Erroneous Execution

If an assignment operation completes prematurely due to an abort, the assignment is said to be disrupted; the target of the assignment or its parts can become abnormal, and certain subsequent uses of the object can be erroneous, as explained in 13.9.1.

Wording Changes from Ada 83

{AI05-0299-1} This subclause has been rewritten to accommodate the concept of aborting the execution of a construct, rather than just of a task.


9.9 Task and Entry Attributes

Dynamic Semantics

For a prefix T that is of a task type [(after any implicit dereference)], the following attributes are defined:

T Callable  
Yields the value True when the task denoted by T is *callable*, and False otherwise; a task is callable unless it is completed or abnormal. The value of this attribute is of the predefined type Boolean.

T Terminated  
Yields the value True if the task denoted by T is terminated, and False otherwise. The value of this attribute is of the predefined type Boolean.

For a prefix E that denotes an entry of a task or protected unit, the following attribute is defined. This attribute is only allowed within the body of the task or protected unit, but excluding, in the case of an entry of a task unit, within any program unit that is, itself, inner to the body of the task unit.

E Count  
Yields the number of calls presently queued on the entry E of the current instance of the unit. The value of this attribute is of the type *universal_integer*.

NOTE 1  
For the Count attribute, the entry can be either a single entry or an entry of a family. The name of the entry or entry family can be either a *direct_name* or an expanded name.

NOTE 2  
Within task units, *byalgorithms* interrogating the attribute E Count should *take precautions* to allow for the increase of the value of this attribute for incoming entry calls, and its decrease, for example with timed_entry_calls. *Also, a conditional_entry_call can also* briefly increase this value, even if the conditional call is not accepted.

NOTE 3  
Within protected units, *byalgorithms* interrogating the attribute E Count in the *entry_barrier* for the entry E *should take precautions* to allow for the evaluation of the condition of the barrier both before and after queuing a given caller.

9.10 Shared Variables

Static Semantics

If two different objects, including nonoverlapping parts of the same object, are *independently addressable*, they can be manipulated concurrently by two different *logical threads of control*. Without synchronization, they are both subcomponents of the same full access object, and either is nonatomic (see C.6). Any two nonoverlapping objects are independently addressable if either object is specified as independently addressable (see C.6). Otherwise, two nonoverlapping objects are independently addressable except when they are both parts of a composite object for which a nonconfirming value is specified for any of the following representation aspects: (record) Layout, Component Size, Pack, Atomic, or Convention; in this case it is unspecified whether the parts are independently addressable. Normally, any two nonoverlapping objects are independently addressable. However, if packing, record layout, or Component Size is specified for a given composite object, then it is implementation defined whether or not two nonoverlapping parts of that composite object are independently addressable.

This paragraph was deleted. Implementation defined: Whether or not two nonoverlapping parts of a composite object are independently addressable, in the case where packing, record layout, or Component Size is specified for the object.

Implementation Note: Independent addressability is the only high level semantic effect of aspects pragmas Pack. If two objects are independently addressable, the implementation should allocate them in such a way that each can be written by the hardware without writing the other. For example, unless the user asks for it, it is generally not feasible to choose a bit-packed representation on a machine without an atomic bit field insertion.
instruction, because there might be tasks that update neighboring subcomponents concurrently, and locking operations on all subcomponents is generally not a good idea.

{AI05-0229-1} Even if `Packaging` or one of the other above-mentioned aspects is specified, subcomponents should still be updated independently if the hardware efficiently supports it.

**Ramification:** {AI05-0009-1} {AI05-0201-1} {AI12-0001-1} An atomic object (including atomic components) is always independently addressable from any other nonoverlapping object. Aspect specifications and representation items cannot change that fact. Any aspect specification or representation item which would prevent this from being true should be rejected, notwithstanding what this Reference Manual says elsewhere. Note, however, that the components of an atomic object are not necessarily atomic.

**Dynamic Semantics**

{AI12-0119-1} [Separate logical threads of control; tasks normally proceed independently and concurrently with one another. However, task interactions can be used to synchronize the actions of two or more logical threads of control to allow, for example, meaningful communication by the direct updating and reading of variables shared between them the tasks.] The actions of two different logical threads of control are synchronized in this sense when an action of one task-signals an action of the other task; an action A1 is defined to signal an action A2 under the following circumstances:

- If A1 and A2 are part of the execution of the same task, and the language rules require A1 to be performed before A2;
- If A1 is the action of an activator that initiates the activation of a task, and A2 is part of the execution of the task that is activated;
- If A1 is part of the activation of a task, and A2 is the action of waiting for completion of the activation;
- If A1 is part of the execution of a task, and A2 is the action of waiting for the termination of the task;
- If A1 is the termination of a task T, and A2 is either the evaluation of the expression `T'Terminated` that results in `True`, or a call to `Ada.Task_Identification.Is_Terminated` with an actual parameter that identifies T and a result of `True` (see C.7.1);
- If A1 is the action of issuing an entry call, and A2 is part of the corresponding execution of the appropriate `entry_body` or `accept_statement`.

**Ramification:** Evaluating the `entry_index` of an `accept_statement` is not synchronized with a corresponding entry call, nor is evaluating the entry barrier of an `entry_body`.

- If A1 is part of the execution of an `accept_statement` or `entry_body`, and A2 is the action of returning from the corresponding entry call;
- If A1 is part of the execution of a protected procedure body or `entry_body` for a given protected object, and A2 is part of a later execution of an `entry_body` for the same protected object;

**Reason:** The underlying principle here is that for one action to "signal" a second, the second action has to follow a potentially blocking operation, whose blocking is dependent on the first action in some way. Protected procedures are not potentially blocking, so they can only be "signalers", they cannot be signaled.

**Ramification:** Protected subprogram calls are not defined to signal one another, which means that such calls alone cannot be used to synchronize access to shared data outside of a protected object.

**Reason:** The point of this distinction is so that on multiprocessors with inconsistent caches, the caches only need to be refreshed at the beginning of an entry body, and forced out at the end of an entry body or protected procedure that leaves an entry open. Protected function calls, and protected subprogram calls for entryless protected objects do not require full cache consistency. Entryless protected objects are intended to be treated roughly like atomic objects — each operation is indivisible with respect to other operations (unless both are reads), but such operations cannot be used to synchronize access to other nonvolatile shared variables.

- If A1 signals some action that in turn signals A2.
Action A1 is defined to potentially signal action A2 if A1 signals A2, if action A1 and A2 occur as part of the execution of the same logical thread of control, and the language rules permit action A1 to precede action A2, or if action A1 potentially signals some action that in turn potentially signals A2.

Given an action of assigning to an object, and an action of reading or updating a part of the same object (or of a neighboring object if the two are not independently addressable), then the execution of the actions is erroneous unless the actions are sequential. Two actions are defined to be sequential if one of the following is true:

- One action signals the other;
- Both actions occur as part of the execution of the same logical thread of control;
  
  Reason: Any two actions of the same logical thread of control are sequential, even if one does not signal the other because they can be executed in an “arbitrary” (but necessarily equivalent to some “sequential”) order.

- Both actions occur as part of protected actions on the same protected object, and at least one of the actions is part of a call on an exclusive function of the protected object.
  
  Reason: Actions within protected actions do not always imply signaling, we have to mention them here explicitly to make sure that actions occurring within different protected actions of the same protected object are sequential with respect to one another (unless both are part of calls on nonexclusive functions).

Ramification: It doesn't matter whether or not the variable being assigned is actually a subcomponent of the protected object; globals can be safely updated from within the bodies of protected procedures, or exclusive protected functions.

Aspect, Atomic or aspect Atomic Components may also be specified to ensure that certain reads and updates are sequential — see C.6.

Ramification: If two actions are “sequential” it is known that their executions don't overlap in time, but it is not necessarily specified which occurs first. For example, all actions of a single logical thread of control are sequential, even though the exact order of execution is not fully specified for all constructs.

Discussion: Note that if two assignments to the same variable are sequential, but neither signals the other, then the program is not erroneous, but it is not specified which assignment ultimately prevails. Such a situation usually corresponds to a programming mistake, but in some (rare) cases, the order makes no difference, and for this reason this situation is not considered erroneous nor even a bounded error. In Ada 83, this was considered an “incorrect order dependence” if the “effect” of the program was affected, but “effect” was never fully defined. In Ada 95, this situation represents a potential nonportability, and a friendly compiler might want to warn the programmer about the situation, but it is not considered an error. An example where this would come up would be in gathering statistics as part of referencing some information, where the assignments associated with statistics gathering don't need to be ordered since they are just accumulating aggregate counts, sums, products, etc.

Two actions that are not sequential are defined to be concurrent actions.

Two actions are defined to conflict if one action assigns to an object, and the other action reads or assigns to a part of the same object (or of a neighboring object if the two are not independently addressable). The action comprising a call on a subprogram or an entry is defined to potentially conflict with another action if the Global aspect (or Global'Class aspect in the case of a dispatching call) of the called subprogram or entry is such that a conflicting action would be possible during the execution of the call. Similarly, two calls are considered to potentially conflict if they each have Global (or Global'Class in the case of a dispatching call) aspects such that conflicting actions would be possible during the execution of the calls. Finally, two actions that conflict are also considered to potentially conflict.
A synchronized object is an object of a task or protected type, an atomic object (see C.6), a suspension object (see D.10), or a synchronous barrier (see D.10.1). [Operations on such objects are necessarily sequential with respect to one another, and hence are never considered to conflict.]

Erroneous Execution

The execution of two concurrent actions is erroneous if the actions make conflicting uses of a shared variable (or neighboring variables that are not independently addressable).

Wording Changes from Ada 95

Corrigendum: Clarified that a task T2 can rely on values of variables that are updated by another task T1, if task T2 first verifies that T1'Terminated is True.

Wording Changes from Ada 2005

Correction: Revised the definition of independent addressability to exclude conforming representation clauses and to require that atomic and independent objects always have independent addressability. This should not change behavior that the user sees for any Ada program, so it is not an inconsistency.

Correction: Corrected the wording of AI95-00118-01 to actually say what was intended (as described above).

Wording Changes from Ada 2012

Added wording to support interaction of parallel constructs with tasks by changing various wording to talk about logical threads of control rather than purely about tasks.

Added wording to define potentially signalling actions and conflicting actions; these are used to define conflict policies.

9.10.1 Conflict Check Policies

This subclause determines what checks are performed relating to possible concurrent conflicting actions (see 9.10).

Syntax

The form of a pragma Conflict Check Policy is as follows:

```
pragma Conflict_Check_Policy (policy_identifier[, policy_identifier]);
```

A pragma Conflict Check Policy is allowed only immediately within a declarative_part, a package_specification, or as a configuration pragma.

Legality Rules

Each policy_identifier shall be one of No Parallel Conflict Checks, Known Parallel Conflict Checks, All Parallel Conflict Checks, No Tasking Conflict Checks, Known Tasking Conflict Checks, All Tasking Conflict Checks, or an implementation-defined conflict check policy. If two policy_identifiers are given, one shall include the word Parallel and one shall include the word Tasking. If only one policy_identifier is given, it shall not include the word Parallel or Tasking.

Implementation defined: Implementation-defined conflict check policies.

A pragma Conflict Check Policy given in a declarative_part or immediately within a package_specification applies from the place of the pragma to the end of the innermost enclosing declarative region. The region for a pragma Conflict Check Policy given as a configuration pragma is the declarative region for the entire compilation unit (or units) to which it applies.
If a pragma Conflict Check Policy applies to a generic instantiation, then the pragma Conflict Check Policy applies to the entire instance.

If multiple Conflict Check Policy pragmas apply to a given construct, the conflict check policy is determined by the one in the innermost enclosing region. If no Conflict Check Policy pragma applies to a construct, the policy is (All Parallel Conflict Checks, No Tasking Conflict Checks) (see below).

To be honest: The region mentioned in this rule is the region to which the policy pragma applies, and not the declarative region in which the policy pragma appears. This distinction matters when there are multiple policy pragmas in a single declarative region.

Certain potentially conflicting actions are disallowed according to which conflict check policies apply at the place where the action or actions occur, as follows:

No Parallel Conflict Checks
This policy imposes no restrictions on concurrent actions arising from parallel constructs.

No Tasking Conflict Checks
This policy imposes no restrictions on concurrent actions arising from tasking constructs.

Known Parallel Conflict Checks
If this policy applies to two concurrent actions appearing within parallel constructs, they are disallowed if they are known to denote the same object (see 6.4.1) with uses that conflict. For the purposes of this check, any parallel loop may be presumed to involve multiple concurrent iterations. Also, for the purposes of deciding whether two actions are concurrent, it is enough for the logical threads of control in which they occur to be concurrent at any point in their execution, unless all of the following are true:

- the shared object is volatile;
- the two logical threads of control are both known to also refer to a shared synchronized object; and
- each thread whose potentially conflicting action updates the shared volatile object, also updates this shared synchronized object.

Reason: To properly synchronize two actions to prevent concurrency, a thread that does an update of a volatile object must update a synchronized object afterwards to indicate it has completed its update, and the other thread needs to test the value of the synchronized object before it reads the updated volatile object. In a parallel construct, “signaling” cannot be used to prevent concurrency, since that generally requires some blocking, so testing the value of the synchronized object would probably need to use a busy-wait loop.

Known Tasking Conflict Checks
If this policy applies to two concurrent actions appearing within the same compilation unit, at least one of which appears within a task body but not within a parallel construct, they are disallowed if they are known to denote the same object (see 6.4.1) with uses that conflict, and neither potentially signals the other (see 9.10). For the purposes of this check, any named task type may be presumed to have multiple instances. Also, for the purposes of deciding whether two actions are concurrent, it is enough for the tasks in which they occur to be concurrent at any point in their execution, unless all of the following are true:

- the shared object is volatile;
- the two tasks are both known to also refer to a shared synchronized object; and
- each task whose potentially conflicting action updates the shared volatile object, also updates this shared synchronized object.

Reason: To properly synchronize two actions to prevent concurrency, a task that does an update of a nonvolatile object must use signaling via a synchronized object to indicate it has completed its update, and the other task needs to be signaled by this action on the synchronized object before it reads the updated nonvolatile object. In other words, to synchronize communication via a nonvolatile object, signaling must be used. To synchronize communication via a
volatile object, an update of a shared synchronized object followed by a read of the synchronized object in the other
task can be sufficient.

20/5

All Parallel Conflicts Checks

This policy includes the restrictions imposed by the Known Parallel Conflict Checks policy, and in addition disallows a parallel construct from reading or updating a variable that is global to the construct, unless it is a synchronized object, or unless the construct is a parallel loop, and the global variable is a part of a component of an array denoted by an indexed component with at least one index expression that statically denotes the loop parameter of the loop parameter specification or the chunk parameter of the parallel loop.

21/5

All Tasking Conflict Checks

This policy includes the restrictions imposed by the Known Tasking Conflict Checks policy, and in addition disallows a task body from reading or updating a variable that is global to the task body, unless it is a synchronized object.

22/5

No Conflict Checks, Known Conflict Checks, All Conflict Checks

These are shorthands for (No Parallel Conflict Checks, No Tasking Conflict Checks), (Known Parallel Conflict Checks, Known Tasking Conflict Checks), and (All Parallel Conflict Checks, All Tasking Conflict Checks), respectively.

Static Semantics

{AI12-0344-1} For a subprogram, the following language-defined representation aspect may be specified:

Parallel Calls

The Parallel Calls aspect is of type Boolean. The specified value shall be static. The Parallel Calls aspect of an inherited primitive subprogram is True if Parallel Calls is True either for the corresponding subprogram of the progenitor type or for any other inherited subprogram that it overrides. If not specified or inherited as True, the Parallel Calls aspect of a subprogram is False.

Specifying the Parallel Calls aspect to be True for a subprogram indicates that the subprogram can be safely called in parallel. Conflict checks (if required by the Conflict Check Policy in effect) are made on the subprogram assuming that multiple concurrent calls exist. Such checks can then be omitted on a call of the subprogram in a parallel iteration context.

Aspect Description for Parallel Calls: Specifies whether a given subprogram is expected to be called in parallel.

Implementation Permissions

{AI12-0267-1} {AI12-0298-1} When the conflict check policy Known Parallel Conflict Checks or All Parallel Conflict Checks applies, the implementation may disallow two concurrent actions appearing within parallel constructs if the implementation can prove they will at run-time denote the same object with uses that conflict. Similarly, when the conflict check policy Known Tasking Conflict Checks or All Tasking Conflict Checks applies, the implementation may disallow two concurrent actions, at least one of which appears within a task body but not within a parallel construct, if the implementation can prove they will at run-time denote the same object with uses that conflict.

Ramification: This permission allows additional enforcement in instance bodies (where Legality Rules aren't usually enforced), in subunits and their parents, and across compilation units, if the implementation wishes.

Extensions to Ada 2012

{AI12-0267-1} Conflict check policies (and the associated checks) are new.

{AI12-0344-1} Aspect Parallel Calls is new.
9.11 Example of Tasking and Synchronization

Examples

The following example defines a buffer protected object to smooth variations between the speed of output of a producing task and the speed of input of some consuming task. For instance, the producing task can have the following structure:

```ada
task Producer;
  task body Producer is
    Person : Person_Name; -- see 3.10.1
    Char : Character;
    begin
      ... -- simulate arrival of the next customer
      produce the next character Char
      Buffer.Append_Wait(Person)
      Write(Char);
      exit when Person = null
      Char = ASCII.EOT;
    end loop;
  end Producer;
```

The consuming task can have the following structure:

```ada
task Consumer;
  task body Consumer is
    Person : Person_Name;
    Char : Character;
    begin
      ... -- simulate serving a customer
      consume the character Char
      Buffer.Remove_First_Wait(Person)
      Read(Char);
      exit when Person = null
      Char = ASCII.EOT;
    end loop;
  end Consumer;
```

The buffer object contains an internal array pool of person names and characters managed in a round-robin fashion. The array pool has two indices, an In_Index denoting the index space for the next input person name character and an Out_Index denoting the index space for the next output person name character.

The Buffer is defined as an extension of the Synchronized_Queue interface (see 3.9.4), and as such promises to implement the abstraction defined by that interface. By doing so, the Buffer can be passed to the Transfer class-wide operation defined for objects of a type covered by Queue'Class.

```ada
type Person_Name_Array is array (Positive range <>) of Person_Name; -- see 3.10.1
protected Buffer is new Synchronized_Queue with
  entry Append_Wait(Person : in Person_Name);
  entry Remove_First_Wait(Person : out Person_Name);
  function Cur_Count return Natural;
  function Max_Count return Natural;
  procedure Append(Person : in Person_Name);
  procedure Remove_First(Person : out Person_Name);
private
  Pool : Person_Name_Array_String(1 .. 100);
  Count : Natural := 0;
  In_Index, Out_Index : Positive := 1;
end Buffer;
```
protected body Buffer is

entry Append_Wait(Person : in Person_Name) Write(C : in Character)
when Count < Pool'Length is
begin
  Append(Person); Pool(In_Index) := C;
  In_Index := (In_Index mod Pool'Length) + 1;
  Count := Count + 1;
end Append_Wait;

procedure Append(Person : in Person_Name) is
begin
  if Count = Pool'Length then
    raise Queue_Error with "Buffer Full"; -- see 11.3
  end if;
  Pool(In_Index) := Person;
  In_Index := (In_Index mod Pool'Length) + 1;
  Count := Count + 1;
end Append;

entry Remove_First_Wait(Person : out Person_Name) Read(C : out Character)
when Count > 0 is
begin
  Remove_First(Person); C := Pool(Out_Index);
  Out_Index := (Out_Index mod Pool'Length) + 1;
  Count := Count - 1;
end Remove_First_Wait;
end Buffer;

procedure Remove_First(Person : out Person_Name) is
begin
  if Count = 0 then
    raise Queue_Error with "Buffer Empty"; -- see 11.3
  end if;
  Person := Pool(Out_Index);
  Out_Index := (Out_Index mod Pool'Length) + 1;
  Count := Count - 1;
end Remove_First;

function Cur_Count return Natural is
begin
  return Buffer.Count;
end Cur_Count;

function Max_Count return Natural is
begin
  return Pool'Length;
end Max_Count;
end Buffer;
10 Program Structure and Compilation Issues

{AI05-0299-1} [The overall structure of programs and the facilities for separate compilation are described in this clause section. A program is a set of partitions, each of which may execute in a separate address space, possibly on a separate computer.

Term entry: program — set of partitions, each of which can execute in a separate address space, possibly on a separate computer

Term entry: partition — part of a program, which consists of a set of interdependent library units

Note: Each partition can run in a separate address space, possibly on a separate computer. A program can contain just one partition, or it can be distributed across multiple partitions, which can execute concurrently.

As explained below, a partition is constructed from library units. Syntactically, the declaration of a library unit is a library_item, as is the body of a library unit. An implementation may support a concept of a program library (or simply, a “library”), which contains library_items and their subunits. Library units may be organized into a hierarchy of children, grandchildren, and so on.]

{AI05-0299-1} This clause section has two subclauses: 10.1, “Separate Compilation” discusses compile-time issues related to separate compilation. 10.2, “Program Execution” discusses issues related to what is traditionally known as “link time” and “run time” — building and executing partitions.

Language Design Principles

We should avoid specifying details that are outside the domain of the language itself. The standard is intended (at least in part) to promote portability of Ada programs at the source level. It is not intended to standardize extra-language issues such as how one invokes the compiler (or other tools), how one's source is represented and organized, version management, the format of error messages, etc.

The rules of the language should be enforced even in the presence of separate compilation. Using separate compilation should not make a program less safe.

It should be possible to determine the legality of a compilation unit by looking only at the compilation unit itself and the compilation units upon which it depends semantically. As an example, it should be possible to analyze the legality of two compilation units in parallel if they do not depend semantically upon each other.

On the other hand, it may be necessary to look outside that set in order to generate code — this is generally true for generic instantiation and inlining, for example. Also on the other hand, it is generally necessary to look outside that set in order to check Post-Compilation Rules.

See also the “generic contract model” Language Design Principle of 12.3, “Generic Instantiation”.

Wording Changes from Ada 83

{AI05-0299-1} The clause section organization mentioned above is different from that of RM83.

10.1 Separate Compilation

[ A program unit is either a package, a task unit, a protected unit, a protected entry, a generic unit, or an explicitly declared subprogram other than an enumeration literal. Certain kinds of program units can be separately compiled. Alternatively, they can appear physically nested within other program units.

Term entry: program unit — language construct that is a package, a task unit, a protected unit, a protected entry, a generic unit, or an explicitly declared subprogram other than an enumeration literal

Note: Certain kinds of program units can be separately compiled. Alternatively, they can appear physically nested within other program units.

The text of a program can be submitted to the compiler in one or more compilations. Each compilation is a succession of compilation units. A compilation_unit contains either the declaration, the body, or a renaming of a program unit.] The representation for a compilation is implementation-defined.

Implementation defined: The representation for a compilation.
Ramification: Some implementations might choose to make a compilation be a source (text) file. Others might allow multiple source files to be automatically concatenated to form a single compilation. Others still may represent the source in a nontextual form such as a parse tree. Note that the RM95 does not even define the concept of a source file.

Note that a protected subprogram is a subprogram, and therefore a program unit. An instance of a generic unit is a program unit.

A protected entry is a program unit, but protected entries cannot be separately compiled.

Term entry: compilation unit — program unit that is separately compiled

Note: A compilation unit contains either the declaration, the body, or a renaming of a program unit.

A library unit is a separately compiled program unit, and is always a package, subprogram, or generic unit. Library units may have other (logically nested) library units as children, and may have other program units physically nested within them. A root library unit, together with its children and grandchildren and so on, form a subsystem.

Term entry: library unit — separately compiled program unit, which is a package, a subprogram, or a generic unit

Note: Library units can have other (logically nested) library units as children, and can have other program units physically nested within them. A root library unit, together with its children and grandchildren and so on, form a subsystem.

Implementation Permissions

An implementation may impose implementation-defined restrictions on compilations that contain multiple compilation units.

Implementation defined: Any restrictions on compilations that contain multiple compilation units.

Discussion: For example, an implementation might disallow a compilation that contains two versions of the same compilation unit, or that contains the declarations for library packages P1 and P2, where P1 precedes P2 in the compilation but P1 has a with_clause that mentions P2.

Wording Changes from Ada 83

The interactions between language issues and environmental issues are left open in Ada 95. The environment concept is new. In Ada 83, the concept of the program library, for example, appeared to be quite concrete, although the rules had no force, since implementations could get around them simply by defining various mappings from the concept of an Ada program library to whatever data structures were actually stored in support of separate compilation. Indeed, implementations were encouraged to do so.

In RM83, it was unclear which was the official definition of “program unit”. Definitions appeared in RM83-5, 6, 7, and 9, but not 12. Placing it here seems logical, since a program unit is sort of a potential compilation unit.

10.1.1 Compilation Units - Library Units

[A library_item is a compilation unit that is the declaration, body, or renaming of a library unit. Each library unit (except Standard) has a parent unit, which is a library package or generic library package.] A library unit is a child of its parent unit. The root library units are the children of the predefined library package Standard.

Ramification: Standard is a library unit.

Syntax

2

compilation ::= {compilation_unit}

3

compilation_unit ::= context_clause library_item | context_clause subunit

4

library_item ::= [private] library_unit_declaration | library_unit_body | [private] library_unit_renaming_declaration
library_unit_declaration ::= 
  subprogram_declaration | package_declaration 
  | generic_declaration | generic_instantiation

library_unit_renaming_declaration ::= 
  package_renaming_declaration 
  | generic_renaming_declaration 
  | subprogram_renaming_declaration

library_unit_body ::= subprogram_body | package_body

parent_unit_name ::= name

{AI95-00397-01} An overriding indicator is not allowed in a subprogram declaration, generic instantiation, or subprogram renaming declaration that declares a library unit.

Reason: All of the listed items syntactically include overriding indicator, but a library unit can never override anything. A majority of the ARG thought that allowing not overriding in that case would be confusing instead of helpful.

A library unit is a program unit that is declared by a library_item. When a program unit is a library unit, the prefix “library” is used to refer to it (or “generic library” if generic), as well as to its declaration and body, as in “library procedure”, “library package_body”, or “generic library package”. The term compilation unit is used to refer to a compilation_unit. When the meaning is clear from context, the term is also used to refer to the library_item of a compilation_unit or to the proper_body of a subunit [(that is, the compilation_unit without the context_clause and the separate (parent_unit_name))].

Discussion: In this example:

```
with Ada.Text_IO;
package P is
end P;
```

the term “compilation unit” can refer to this text: “with Ada.Text_IO; package P is ... end P;” or to this text: “package P is ... end P;”. We use this shorthand because it corresponds to common usage.

We like to use the word “unit” for declaration-plus-body things, and “item” for declaration or body separately (as in declarative_item). The terms “compilation_unit”, “compilation unit”, and “subunit” are exceptions to this rule. We considered changing “compilation_unit”, “compilation unit” to “compilation_item”, “compilation item”, respectively, but we decided not to.

The parent declaration of a library_item (and of the library unit) is the declaration denoted by the parent_unit_name, if any, of the defining_program_unit_name of the library_item. If there is no parent_unit_name, the parent declaration is the declaration of Standard, the library_item is a root library_item, and the library unit (renaming) is a root library unit (renaming). The declaration and body of Standard itself have no parent declaration. The parent unit of a library_item or library unit is the library unit declared by its parent declaration.

Discussion: The declaration and body of Standard are presumed to exist from the beginning of time, as it were. There is no way to actually write them, since there is no syntactic way to indicate lack of a parent. An attempt to compile a package Standard would result in Standard.Standard.

Reason: Library units (other than Standard) have “parent declarations” and “parent units”. Subunits have “parent bodies”. We didn't bother to define the other possibilities: parent body of a library unit, parent declaration of a subunit, parent unit of a subunit. These are not needed, and might get in the way of a correct definition of “child”.

[The children of a library unit occur immediately within the declarative region of the declaration of the library unit.] The ancestors of a library unit are itself, its parent, its parent's parent, and so on. [Standard is an ancestor of every library unit.] The descendant relation is the inverse of the ancestor relation.

Reason: These definitions are worded carefully to avoid defining subunits as children. Only library units can be children.

We use the unadorned term “ancestors” here to concisely define both “ancestor unit” and “ancestor declaration”.

Discussion: In this example:

```
with Ada.Text_IO;
package P is
end P;
```
A library_unit_declaration or a library_unit_renaming_declaration is private if the declaration is immediately preceded by the reserved word private; it is otherwise public. A library unit is private or public according to its declaration. The public descendants of a library unit are the library unit itself, and the public descendants of its public children. Its other descendants are private descendants.

Discussion: The first concept defined here is that a library_item is either public or private (not in relation to anything else — it's just a property of the library unit). The second concept is that a library_item is a public descendant or private descendant of a given ancestor. A given library_item can be a public descendant of one of its ancestors, but a private descendant of some other ancestor.

A subprogram declared by a subprogram_body (as opposed to a subprogram_declaration) is always public, since the syntax rules disallow the reserved word private on a body.

Note that a private library unit is a public descendant of itself, but a private descendant of its parent. This is because it is visible outside itself — its privateness means that it is not visible outside its parent.

Private children of Standard are legal, and follow the normal rules. It is intended that implementations might have some method for taking an existing environment, and treating it as a package to be “imported” into another environment, treating children of Standard in the imported environment as children of the imported package.

Ramification: Suppose we have a public library unit A, a private library unit A.B, and a public library unit A.B.C. A.B.C is a public descendant of itself and of A.B, but a private descendant of A; since A.B is private to A, we don't allow A.B.C to escape outside A either. This is similar to the situation that would occur with physical nesting, like this:

```ada
package A is
    private
    package B is
        package C is
            end C;
        private
        end B;
    end B;
end A;
```

Here, A.B.C is visible outside itself and outside A.B, but not outside A. (Note that this example is intended to illustrate the visibility of program units from the outside; the visibility within child units is not quite identical to that of physically nested units, since child units are nested after their parent's declaration.)

\{AI95-00217-06\} For each library package declaration in the environment, there is an implicit declaration of a limited view of that library package. The limited view of a package contains:

- \{AI95-00217-06\} \{AI05-0129-1\} \{AI05-0262-1\} For each nested package declaration occurring immediately within the visible part, a declaration of the limited view of that package, with the same defining program unit name.

- \{AI95-00217-06\} \{AI05-00326-01\} \{AI05-0108-1\} \{AI05-0129-1\} \{AI05-0262-1\} For each type declaration occurring immediately within the visible part that is not an incomplete type declaration, an incomplete view of the type with no discriminant_part; if the type_declaration is tagged, then the view is a tagged incomplete view.

Reason: \{AI05-0108-1\} The incomplete view of a type does not have a discriminant_part even if the type_declaration does have one. This is necessary because semantic analysis (and the associated dependence on with_clauses) would be necessary to determine the types of the discriminants.

No incomplete views of incomplete types are included in the limited view. The rules of 3.10.1 ensure that the completion of any visible incomplete type is declared in the same visible part, so such an incomplete view would simply be redundant.

Discussion: \{AI95-00217-06\} The implementation model of a limited view is that it can be determined solely from the syntax of the source of the unit, without any semantic analysis. That allows it to be created without the semantic dependences of a full unit, which is necessary for it to break mutual dependences of units.

Ramification: The limited view does not include package instances and their contents. Semantic analysis of a unit (and dependence on its with_clauses) would be needed to determine the contents of an instance.

The limited view of a library package declaration is private if that library package declaration is immediately preceded by the reserved word private.

[There is no syntax for declaring limited views of packages, because they are always implicit.] The implicit declaration of a limited view of a library package is not the declaration of a library unit (the
library package declaration is); nonetheless, it is a library item. The implicit declaration of the limited view of a library package forms an (implicit) compilation unit whose context clause is empty.

A library package declaration is the completion of the declaration of its limited view.

To be honest: This is notwithstanding the rule in 3.11.1 that says that implicit declarations don't have completions. Reason: This rule explains where to find the completions of the incomplete views defined by the limited view.

Legality Rules

The parent unit of a library item shall be a [library] package or generic [library] package.

If a defining program unit name of a given declaration or body has a parent unit name, then the given declaration or body shall be a library item. The body of a program unit shall be a library item if and only if the declaration of the program unit is a library item. In a library unit renaming declaration, the ([old]) name shall denote a library item.

Discussion: We could have allowed nested program units to be children of other program units; their semantics would make sense. We disallow them to keep things simpler and because they wouldn't be particularly useful.

{AI95-00217-06} A parent unit name [(which can be used within a defining program unit name of a library item and in the separate clause of a subunit)], and each of its prefixes, shall not denote a renaming declaration. [On the other hand, a name that denotes a library unit renaming declaration is allowed in a nonlimited with clause with clause and other places where the name of a library unit is allowed.]

If a library package is an instance of a generic package, then every child of the library package shall either be itself an instance or be a renaming of a library unit.

Discussion: A child of an instance of a given generic unit will often be an instance of a (generic) child of the given generic unit. This is not required, however.

Reason: Instances are forbidden from having noninstance children for two reasons:

1. We want all source code that can depend on information from the private part of a library unit to be inside the "subsystem" rooted at the library unit. If an instance of a generic unit were allowed to have a noninstance as a child, the source code of that child might depend on information from the private part of the generic unit, even though it is outside the subsystem rooted at the generic unit.

2. Disallowing noninstance children simplifies the description of the semantics of children of generic packages.

{AI05-0004-1} A child of a generic library package shall either be itself a generic unit or be a renaming of some other child of the same generic unit. The renaming of a child of a generic package shall occur only within the declarative region of the generic package.

A child of a parent generic package shall be instantiated or renamed only within the declarative region of the parent generic.

{AI95-00331-01} For each child declaration or renaming of a generic unit as a child of some parent generic package \( P \), there is a corresponding declaration \( C \) nested immediately within each instance of \( P \). For the purposes of this rule, if a child \( C \) itself has a child \( D \), each corresponding declaration for \( C \) has a corresponding child \( D \) of the parent. [The corresponding child within an instance is visible only within the scope of a with clause that mentions the (original) child generic unit.]

Implementation Note: Within the child, like anything nested in a generic unit, one can make up-level references to the current instance of its parent, and thereby gain access to the formal parameters of the parent, to the types declared in the parent, etc. This “nesting” model applies even within the generic formal part of the child, as does for a generic child of a nongeneric unit.

Ramification: Suppose \( P \) is a generic library package, and \( P.C \) is a generic child of \( P \). \( P.C \) can be instantiated inside the declarative region of \( P \). Outside \( P \), \( P.C \) can be mentioned only in a with clause. Conceptually, an instance \( I \) of \( P \) is a package that has a nested generic unit called \( I.C \). Mentioning \( P.C \) in a with clause allows \( I.C \) to be instantiated. \( I \) need not be a library unit, and the instantiation of \( I.C \) need not be a library unit. If \( I \) is a library unit, and an instance of \( I.C \) is a child of \( I \), then this instance has to be called something other than \( C \).
A library subprogram shall not override a primitive subprogram.

Reason: This prevents certain obscure anomalies. For example, if a library subprogram were to override a subprogram declared in its parent package, then in a compilation unit that depends indirectly on the library subprogram, the library subprogram could hide the overridden operation from all visibility, but the library subprogram itself would not be visible.

Note that even without this rule, such subprograms would be illegal for tagged types, because of the freezing rules.

The defining name of a function that is a compilation unit shall not be an operator symbol.

Reason: Since overloading is not permitted among compilation units, it seems unlikely that it would be useful to define one as an operator. Note that a subunit could be renamed within its parent to be an operator.

Static Semantics

A subprogram_renaming_declaration that is a library_unit_renaming_declaration is a renaming-as-declaration, not a renaming-as-body.

[There are two kinds of dependences among compilation units:

- {AI12-0445-1} The semantic dependences (see below) are the ones necessary to check the compile-time rules across compilation unit boundaries; a compilation unit depends semantically on the other compilation units necessary to determine its legality. The visibility rules are based on the semantic dependences.

- The elaboration dependences (see 10.2) determine the order of elaboration of library_items.]

Discussion: Don't confuse these kinds of dependences with the run-time dependences among tasks and masters defined in 9.3, “Task Dependence - Termination of Tasks”.

{AI95-00217-06} A library_item depends semantically upon its parent declaration. A subunit depends semantically on its own body. A library Unit_body depends semantically upon the corresponding library_unit_declaration, if any. The declaration of the limited view of a library package depends semantically upon the declaration of the limited view of its parent. The declaration of a library package depends semantically upon the declaration of its limited view. A compilation unit depends semantically upon each library_item mentioned in a with_clause of the compilation unit. In addition, if a given compilation unit contains an attribute_reference of a type defined in another compilation unit, then the given compilation unit depends semantically upon the other compilation unit. The semantic dependence relationship is transitive.

Discussion: The “if any” in the third sentence is necessary because library subprograms are not required to have a subprogram_declaration.

To be honest: If a given compilation unit contains a choice_parameter_specification, then the given compilation unit depends semantically upon the declaration of Ada.Exceptions.

If a given compilation unit contains a pragma with an argument of a type defined in another compilation unit, then the given compilation unit depends semantically upon the other compilation unit.

Discussion: For example, a compilation unit containing X'Address depends semantically upon the declaration of package System.

For the Address attribute, this fixes a hole in Ada 83. Note that in almost all cases, the dependence will need to exist due to with_clauses, even without this rule. Hence, the rule has very little effect on programmers.

Note that the semantic dependence does not have the same effect as a with_clause; in order to denote a declaration in one of those packages, a with_clause will generally be needed.

Note that no special rule is needed for an attribute_definition_clause, since an expression after use will require semantic dependence upon the compilation unit containing the type_declaration of interest.

Unlike a full view of a package, a limited view does not depend semantically on units mentioned in with clauses of the compilation unit that defines the package. Formally, this is achieved by saying that the limited view has an empty context clause. This is necessary so that they can be useful for their intended purpose: allowing mutual dependences between packages. The lack of semantic dependence limits the contents of a limited view to the items that can be determined solely from the syntax of the source of the package, without any semantic analysis. That allows it to be created without the semantic dependences of a full package.
Examples of library units:

```
package Rational_Numbers.IO is  -- public child of Rational_Numbers, see 7.1
   procedure Put(R : in Rational);
   procedure Get(R : out Rational);
end Rational_Numbers.IO;

private procedure Rational_Numbers.Reduce(R : in out Rational);  -- private child of Rational_Numbers
with Rational_Numbers.Reduce;  -- refer to a private child
package body Rational_Numbers is
   . . .
end Rational_Numbers;
```

**Examples**

```ada
package Rational_Numbers.IO is  -- public child of Rational_Numbers, see 7.1
   procedure Put(R : in Rational);
   procedure Get(R : out Rational);
end Rational_Numbers.IO;

private procedure Rational_Numbers.Reduce(R : in out Rational);  -- private child of Rational_Numbers
with Rational_Numbers.Reduce;  -- refer to a private child
package body Rational_Numbers is
   . . .
end Rational_Numbers;
```
with Rational_Numbers.IO; use Rational_Numbers;
with Ada.Text_IO; -- see A.10
procedure Main is -- a root library procedure
begin
  R := 5/3; -- construct a rational number, see 7.1
  Ada.Text_IO.Put("The answer is: ");
  IO.Put(R);
  Ada.Text_IO.New_Line;
end Main;

package Rational_IO renames Rational_Numbers.IO;
-- a library unit renaming declaration

Each of the above library_items can be submitted to the compiler separately.

Discussion: Example of a generic package with children:

generic
  type Element is private;
  with function Image(E : Element) return String;
package Generic_Bags is
  type Bag is limited private; -- A bag of Elements.
  procedure Add(B : in out Bag; E : Element);
  function Bag_Image(B : Bag) return String;
private
  type Bag is ...;
end Generic_Bags;

generic package Generic_Bags.Generic_Iterators is ...
  -- various additional operations on Bags.
  with procedure Use_Element(E : in Element);
  -- Called once per bag element.
  procedure Iterate(B : in Bag);
end Generic_Bags.Generic_Iterators;

A package that instantiates the above generic units:

with Generic_Bags;
with Generic_Bags.Generic_Iterators;
package My_Abstraction is
  type My_Type is ...;
  function Image(X : My_Type) return String;
package Bags_Of_My_Type is new Generic_Bags(My_Type, Image);
package Iterators_Of_Bags_Of_My_Type is new Bags_Of_My_Type.Generic_Iterators;
end My_Abstraction;

In the above example, Bags_Of_My_Type has a nested generic unit called Generic_Iterators. The second with_clause makes that nested unit visible.

Here we show how the generic body could depend on one of its own children:

with Generic_Bags.Generic_Iterators;
package body Generic_Bags is
  procedure Add(B : in out Bag; E : Element) is ... end Add;
  package Iters is new Generic_Iterators;
function Bag_Image(B : Bag) return String is
  Buffer : String(1..10_000);
  Last : Integer := 0;
begin
  if Last /= 0 then -- Insert a comma.
    Last := Last + 1;
    Buffer(Last) := ',';
  end if;
  Buffer(Last+1 .. Last+Im'Length) := Im;
  last := Last + Im'Length;
end Append_Image;
procedure Append_All is new Iters.Iterate(Append_Image);
begin
Append_All(B);
return Buffer(1..Last);
end Bag_Image;
end Generic_Bags;

Extensions to Ada 83

The syntax rule for library_item is modified to allow the reserved word private before a library_unit_declaration.

Children (other than children of Standard) are new in Ada 95.

Library unit renaming is new in Ada 95.

Wording Changes from Ada 83

Standard is considered a library unit in Ada 95. This simplifies the descriptions, since it implies that the parent of each library unit is a library unit. (Standard itself has no parent, of course.) As in Ada 83, the language does not define any way to recompile Standard, since the name given in the declaration of a library unit is always interpreted in relation to Standard. That is, an attempt to compile a package Standard would result in Standard.Standard.

Extensions to Ada 95

{AI95-00217-06} The concept of a limited view is new. Combined with limited_with_clauses (see 10.1.2), they facilitate construction of mutually recursive types in multiple packages.

Wording Changes from Ada 95

{AI95-00331-01} Clarified the wording so that a grandchild generic unit will work as expected.

Wording Changes from Ada 2005

{AI05-0108-1} {AI05-0129-1} Correction: Clarified the wording so that it is clear that limited views of types never have discriminants and never are of incomplete types.

10.1.2 Context Clauses - With Clauses

[A context_clause is used to specify the library_items whose names are needed within a compilation unit.]

Language Design Principles

The reader should be able to understand a context_clause without looking ahead. Similarly, when compiling a context_clause, the compiler should not have to look ahead at subsequent context_items, nor at the compilation unit to which the context_clause is attached. (We have not completely achieved this.)

{AI95-00217-06} A ripple effect occurs when the legality of a compilation unit could be affected by adding or removing an otherwise unneeded with_clause on some compilation unit on which the unit depends, directly or indirectly. We try to avoid ripple effects because they make understanding and maintenance more difficult. However, ripple effects can occur because of direct visibility (as in child units); this seems impossible to eliminate. The ripple effect for with_clauses is somewhat similar to the Beaujolais effect (see 8.4) for use_clauses, which we also try to avoid.

Discussion: {AI95-00217-06} A limited_with_clause makes a limited view of a unit visible.

Syntax

context_clause ::= {context_item}
context_item ::= with_clause | use_clause

{AI95-00217-06} {AI95-00262-01} with_clause ::= limited_with_clause | nonlimited_with_clause with library_unit_name {, library_unit_name};

limited_with_clause ::= limited [private] with library_unit_name {, library_unit_name};
nonlimited_with_clause ::= [private] with library_unit_name {, library_unit_name};

Discussion: {AI95-00217-06} A limited_with_clause makes a limited view of a unit visible.
4.b/2  \[AI95-00262-01\] A with_clause containing the reserved word private is called a private with_clause. It can be thought of as making items visible only in the private part, although it really makes items visible everywhere except the visible part. It can be used both for documentation purposes (to say that a unit is not used in the visible part), and to allow access to private units that otherwise would be prohibited.

Name Resolution Rules

5  The scope of a with_clause that appears on a library_unit_declaration or library_unit_renaming_- declaration consists of the entire declarative region of the declaration[, which includes all children and subunits]. The scope of a with_clause that appears on a body consists of the body[, which includes all subunits].

Discussion: \[AI95-00262-01\] Suppose a nonprivate with_clause of a public library unit mentions one of its private siblings. (This is only allowed on the body of the public library unit.) We considered making the scope of that with_clause not include the visible part of the public library unit. (This would only matter for a subprogram_body, since those are the only kinds of body that have a visible part, and only if the subprogram_body completes a subprogram_declaration, since otherwise the with_clause would be illegal.) We did not put in such a rule for two reasons: (1) It would complicate the wording of the rules, because we would have to split each with_clause into pieces, in order to correctly handle “with P, Q;” where P is public and Q is private. (2) The conformance rules prevent any problems. It doesn't matter if a type name in the spec of the body denotes the completion of a private_type_declaration.

5.b  A with_clause also affects visibility within subsequent use_clauses and pragmas of the same context_clause, even though those are not in the scope of the with_clause.

6/2  \[AI95-00217-06\] A library_item (and the corresponding library unit) is named mentioned in a with_clause if it is denoted by a library_unit_name or a prefix-in the with_clause. A library_item (and the corresponding library unit) is mentioned in a with_clause if it is named in the with_clause or if it is denoted by a prefix in the with_clause.

Discussion: With clauses control the visibility of declarations or renamings of library units. Mentions of a root library unit in a with_clause makes its declaration directly visible. Mentions of a nonroot library unit makes its declaration visible. See Clause 8 for details.

6.b/2  \[AI95-00114-01\] Note that this rule implies that “with A,B.C;” is almost equivalent to “with A, A.B, A.B.C;” The reason for making a with_clause apply to all the ancestor units is to avoid “visibility holes” — situations in which an inner program unit is visible while an outer one is not. Visibility holes would cause semantic complexity and implementation difficulty. (This is not exactly equivalent because the latter with_clause names A and A.B, while the previous one does not. Whether a unit is “named” does not have any effect on visibility, however, so it is equivalent for visibility purposes.)

[Outside its own declarative region, the declaration or renaming of a library unit can be visible only within the scope of a with_clause that mentions it. The visibility of the declaration or renaming of a library unit otherwise follows from its placement in the environment.]

Legality Rules

8/2  \[AI95-00262-01\] If a with_clause of a given compilation_unit mentions a private child of some library unit, then the given compilation_unit shall be one of either the declaration of a private descendant of that library unit or the body or subunit of a (public or private) descendant of that library unit.

9/2  \[AI95-00262-01\] the declaration, body, or subunit of a private descendant of that library unit;

10/2  \[AI95-00220-01\] \[AI95-00262-01\] the body or subunit of a public descendant of that library unit, but not a subprogram body acting as a subprogram declaration (see 10.1.4); or

11/2  \[AI95-00262-01\] the declaration of a public descendant of that library unit, in which case the with_clause shall include the reserved word private.

Reason: \[AI95-00262-01\] The purpose of this rule is to prevent a private child from being visible (or even semantically depended on) from outside the subsystem rooted at its parent. A private child can be semantically depended on without violating this principle if it is used in a private with_clause.

Discussion: This rule violates the one-pass context_clauses Language Design Principle. We rationalize this by saying that at least that Language Design Principle works for legal compilation units.
Example:

```ada
package A is end A;
package A.B is end A.B;
private package A.B.C is end A.B.C;
package A.B.C.D is end A.B.C.D;
with A.B.C; -- (1)
private package A.B.X is end A.B.X;
package A.B.Y is end A.B.Y;
with A.B.C; -- (2)
package body A.B.Y is end A.B.Y;
private with A.B.C; -- (3)
package A.B.Z is end A.B.Z;
```

{(AI95-00262-01) (1) is OK because it's a private child of A.B — it would be illegal if we made A.B.X a public child of A.B. (2) is OK because it's the body of a child of A.B. (3) is OK because it's a child of A.B, and it is a private with_clause. It would be illegal to say “with A.B.C;” on any library_item whose name does not start with “A.B”. Note that mentioning A.B.C.D in a with_clause automatically mentions A.B.C as well, so “with A.B.C.D;” is illegal in the same places as “with A.B.C;”.}

**To be honest:** {(AI05-0005-1) {(AI95-00262-01) For the purposes of this rule, if a subprogram_body has no preceding subprogram_declaration, the subprogram_body should be considered a declaration and not a body. Thus, it is illegal for such a subprogram_body to mention one of its siblings in a nonprivate with_clause if the sibling is a private library_unit.}

{(AI95-00262-01) {(AI05-0077-1) {(AI12-0261-1) {(AI12-0261-1) A name denoting a library_item (or the corresponding declaration for a child of a generic within an instance — see 10.1.1), if it is a library_item that is visible only due to being mentioned in one or more with_clauses of a unit U that include the reserved word private, shall appear only within:

- a private part;
- (AI12-0261-1) a body of a public descendant of U, but not within the subprogram_specification of a library_subprogram_body of a subprogram that is a public descendant of U;
- (AI12-0261-1) a private descendant of U or its body the unit on which one of these with_clauses appear; or
- a pragma within a context clause.}

**Ramification:** These rules apply only if all of the with_clauses that mention the name include the reserved word private. They do not apply if the name is mentioned in any with_clause that does not include private.

**Reason:** {(AI05-0077-1) These rules make the library_item visible anywhere that is not visible outside the subsystem rooted at the compilation_unit having the private with_clause, including private parts of packages nested in the visible part, private parts of child packages, the visible part of private children, and context clause pragmas like Elaborate_All.}

We considered having the scope of a private with_clause not include the visible part. However, that rule would mean that moving a declaration between the visible part and the private part could change its meaning from one legal interpretation to a different legal interpretation. For example:

```ada
package A is
  function B return Integer;
end A;
function B return Integer;
```
with A;
private with B;
package C is
    use A;
    V1 : Integer := B; -- (1)
private
    V2 : Integer := B; -- (2)
end C;

If we say that library subprogram B is not in scope in the visible part of C, then the B at (1) resolves to A.B, while (2) resolves to library unit B. Simply moving a declaration could silently change its meaning. With the legality rule defined above, the B at (1) is illegal. If the user really meant A.B, they still can say that.

\textit{Proof:} This is redundant because only such implicit declarations are visible in a \texttt{limited_with_clause}. See 10.1.6.

\textit{Reason:} We don't allow a \texttt{limited_with_clause} on a \texttt{library_unit_renaming_declaration} because it would be useless and therefore probably is a mistake. A renaming cannot appear in a \texttt{limited_with_clause} (by the rule prior to this one), and a renaming of a limited view cannot appear in a \texttt{nonlimited_with_clause} (because the name would not be within the scope of a \texttt{with_clause} denoting the package, see 8.5.3). Nor could it be the parent of another unit. That doesn't leave anywhere that the name of such a renaming could appear, so we simply make writing it illegal.

\textit{Ramification:} This applies to \texttt{nonlimited_with_clauses} found in the same \texttt{context_clause}, as well as \texttt{nonlimited_with_clauses} found on parent units.

\textit{Reason:} Such a \texttt{limited_with_clause} could have no effect, and would be confusing. If it is within the scope of a \texttt{nonlimited_with_clause} for the same package is inherited from a parent unit or given, or if such a clause is in the \texttt{context_clause}, the full view is available, which strictly provides more information than the limited view.

\textit{Ramification:} This applies to \texttt{use_clauses} found in the same \texttt{context_clause}, as well as \texttt{use_clauses} found in (or on) parent units.

\textit{Reason:} This prevents visibility issues, where whether an entity is an incomplete or full view depends on how the name of the entity is written. The \texttt{limited_with_clause} cannot be useful, as we must have the full view available in the parent in order for the \texttt{use_clause} to be legal.
NOTE {AI95-00217-06} A library_item mentioned in a nonlimited_with_clause of a compilation unit is visible within the compilation unit and hence acts just like an ordinary declaration. Thus, within a compilation unit that mentions its declaration, the name of a library package can be given in use_clauses and can be used to form expanded names, a library subprogram can be called, and instances of a generic library unit can be declared. If a child of a parent generic package is mentioned in a nonlimited_with_clause, then the corresponding declaration nested within each visible instance is visible within the compilation unit. Similarly, a library_item mentioned in a limited_with_clause of a compilation unit is visible within the compilation unit and thus can be used to form expanded names.

Ramification: The rules given for with_clauses are such that the same effect is obtained whether the name of a library unit is mentioned once or more than once by the applicable with_clauses, or even within a given with_clause.

If a with_clause mentions a library_unit_renaming_declaration, it only “mentions” the prefixes appearing explicitly in the with_clause (and the renamed view itself); the withClause is not defined to mention the ancestors of the renamed entity. Thus, if X renames Y.Z, then “with X;” does not make the declarations of Y or Z visible. Note that this does not cause the dreaded visibility holes mentioned above.

Examples

{AI12-0429-1} Examples of use of with clauses, limited with clauses, and private with clauses:

{AI95-00433-01} package Office is
end Office;

{AI95-00433-01} with Ada.Strings.Unbounded;
package Office.Locations is
  type Location is new Ada.Strings.Unbounded.Unbounded_String;
end Office.Locations;

{AI95-00433-01} limited with Office.Departments; -- types are incomplete
package Office.Employees is
  type Employee is private;
  function Dept_Of(Emp : Employee) return access Departments.Department;
  procedure Assign_Dept(Emp  : in out Employee; Dept : access Departments.Department);
...  
private
  type Employee is
  record
    Dept : access Departments.Department;
    Loc : Locations.Location;
  end record;
end Office.Employees;

{AI12-0178-1} limited with Office.Employees;
package Office.Departments is
  type Department is ...private;
  function Manager_Of(Dept : Department) return access Employees.Employee;
  procedure Assign_Manager(Dept : in out Department; Mgr : access Employees.Employee);
...  
end Office.Departments;

{AI95-00433-01} {AI12-0429-1} {AI12-0440-1} The limited_with_clause can be used to support mutually dependent abstractions that are split across multiple packages. In this case, an employee is assigned to a department, and a department has a manager who is an employee. If a with_clause with the reserved word private appears on one library unit and mentions a second library unit, it provides visibility to the second library unit, but restricts that visibility to the private part and body of the first unit. The compiler checks that no use is made of the second unit in the visible part of the first unit. The limited_with_clause may be used to support mutually dependent abstractions that are split across multiple packages. In this case, an employee is assigned to a department, and a department has a manager who is an employee. If a with_clause with the reserved word private appears on one library unit and mentions a second library unit, it provides visibility to the second library unit, but restricts that visibility to the
private part and body of the first unit. The compiler checks that no use is made of the second unit in the visible part of the first unit.

10.1.2

Extensions to Ada 83

32.a
The syntax rule for with_clause is modified to allow expanded name notation.

32.b
A use_clause in a context_clause may be for a package (or type) nested in a library package.

Wording Changes from Ada 83

32.c
The syntax rule for context_clause is modified to more closely reflect the semantics. The Ada 83 syntax rule implies that the use_clauses that appear immediately after a particular with_clause are somehow attached to that with_clause, which is not true. The new syntax allows a use_clause to appear first, but that is prevented by a textual rule that already exists in Ada 83.

32.d
The concept of “scope of a with_clause” (which is a region of text) replaces RM83's notion of “apply to” (a with_clause applies to a library_item). The visibility rules are interested in a region of text, not in a set of compilation units.

32.e
No need to define “apply to” for use_clauses. Their semantics are fully covered by the “scope (of a use_clause)” definition in 8.4.

Incompatibilities With Ada 95

32.f/2
\{AI95-00220-01\} Amendment Correction: A subprogram body acting as a declaration cannot with a private child unit. This would allow public export of types declared in private child packages, and thus cannot be allowed. This was allowed by mistake in Ada 95; a subprogram that does this will now be illegal.

Extensions to Ada 95

32.g/2
\{AI95-00217-06\} limited_with_clauses are new. They make a limited view of a package visible, where all of the types in the package are incomplete. They facilitate construction of mutually recursive types in multiple packages.

32.h/3
\{AI95-00262-01\}, \{AI05-0077-1\} The syntax rules for with_clause are modified to allow the reserved word private. Private with_clauses do not allow the use of their library_item in the visible part of their compilation_unit. They also allow using private units in more locations than in Ada 95.

Incompatibilities With Ada 2005

32.i/3
\{AI05-0040-1\} Correction: Added missing rule that a limited with clause cannot name an ancestor unit. This is incompatible if an Ada 2005 program does this, but as this is a new Ada 2005 feature and the unintentionally allowed capability is not useful, the incompatibility is very unlikely to occur in practice.

Wording Changes from Ada 2005

32.j/3
\{AI05-0077-1\} Correction: Fixed wording so that we are not checking whether something in a context_clause is “within the scope of” something, as context_clauses are never included in anything's scope. The intended meaning is unchanged, however.

32.k/3
\{AI05-0122-1\} Correction: Fixed wording so the rules for private with clauses also apply to "sprouted" generic child units.

Wording Changes from Ada 2012

32.l/5
\{AI12-0261-1\} Correction: Fixed wording so the privately withed units are visible in the subprogram specification of the body of a private descendant; otherwise, the private specification is legal but the completion is not.

10.1.3 Subunits of Compilation Units

Subunits are like child units, with these (important) differences: subunits support the separate compilation of bodies only (not declarations); the parent contains a body_stub to indicate the existence and place of each of its subunits; declarations appearing in the parent's body can be visible within the subunits.]
body_stub ::= 
  subprogram_body_stub | package_body_stub 
  | task_body_stub | protected_body_stub

{AI95-00218-03} {AI05-0267-1} subprogram_body_stub ::=  
  [overriding_indicator]  
  subprogram_specification is separate  
  [aspect_specification];

Discussion: Although this syntax allows a parent_unit_name, that is disallowed by 10.1.1, “Compilation Units - Library Units”.

{AI05-0267-1} package_body_stub ::=  
  [package body defining_identifier is separate  
  [aspect_specification];

{AI05-0267-1} task_body_stub ::=  
  [task body defining_identifier is separate  
  [aspect_specification];

{AI05-0267-1} protected_body_stub ::=  
  [protected body defining_identifier is separate  
  [aspect_specification];

subunit ::= separate (parent_unit_name) proper_body

Legality Rules

{AI95-00243-01} The parent body of a subunit is the body of the program unit denoted by its parent_unit_name. The term subunit is used to refer to a subunit and also to the proper_body of a subunit. The subunits of a program unit include any subunit that names that program unit as its parent, as well as any subunit that names such a subunit as its parent (recursively).

Reason: {AI95-00243-01} We want any rule that applies to a subunit to apply to a subunit of a subunit as well.

Term entry: subunit — body of a program unit that can be compiled separately from its enclosing program unit

The parent body of a subunit shall be present in the current environment, and shall contain a corresponding body_stub with the same defining_identifier as the subunit.

Discussion: This can't be a Name Resolution Rule, because a subunit is not a complete context.

{AI05-0004-1} A package_body_stub shall be the completion of a package_declaration or generic_package_declaration; a task_body_stub shall be the completion of a task_declaration; a protected_body_stub shall be the completion of a protected_declaration.

{AI12-0444-1} In contrast, a subprogram_body_stub can be defined without it being need not be the completion of a previous declaration, [in which case the _stub declares the subprogram]. If the _stub is a completion, it shall be the completion of a subprogram_declaration or generic_subprogram_declaration. The profile of a subprogram_body_stub that completes a declaration shall conform fully to that of the declaration.

Discussion: The part about subprogram_body_stubs echoes the corresponding rule for subprogram_bodies in 6.3, “Subprogram Bodies”.

A subunit that corresponds to a body_stub shall be of the same kind (package, subprogram, task, or protected) as the body_stub. The profile of a subprogram_body subunit shall be fully conformant to that of the corresponding body_stub.
A body_stub shall appear immediately within the declarative_part of a compilation unit body. This rule does not apply within an instance of a generic unit.

**Discussion:** This is a methodological restriction; that is, it is not necessary for the semantics of the language to make sense.

The defining_identifiers of all body_stubs that appear immediately within a particular declarative_part shall be distinct.

Post-Compilation Rules

For each body_stub, there shall be a subunit containing the corresponding proper_body.

NOTE The rules in 10.1.4, “The Compilation Process” say that a body_stub is equivalent to the corresponding proper_body. This implies:

- Visibility within a subunit is the visibility that would be obtained at the place of the corresponding body_stub (within the parent body) if the context_clause of the subunit were appended to that of the parent body.

  **Ramification:** Recursively. Note that this transformation might make the parent illegal; hence it is not a true equivalence, but applies only to visibility within the subunit.

- The effect of the elaboration of a body_stub is to elaborate the subunit.

  **Ramification:** The elaboration of a subunit is part of its parent body's elaboration, whereas the elaboration of a child unit is not part of its parent declaration's elaboration.

  **Ramification:** A library_item that is mentioned in a with_clause of a subunit can be hidden (from direct visibility) by a declaration (with the same identifier) given in the subunit. Moreover, such a library_item can even be hidden by a declaration given within the parent body since a library unit is declared in its parent's declarative region; this however does not affect the interpretation of the with_clauses themselves, since only library_items are visible or directly visible in with_clauses.

  The body of a protected operation cannot be a subunit. This follows from the syntax rules. The body of a protected unit can be a subunit.

**Examples**

{**AI12-0429-1**} Example that defines package Parent without subunits: The package Parent is first written without subunits:

```ada
package Parent is
  procedure Inner;
end Parent;

with Ada.Text_IO;
package body Parent is
  Variable : String := "Hello, there."
  procedure Inner is
    begin
      Ada.Text_IO.Put_Line(Variable);
    end Inner;
end Parent;
```

{**AI12-0429-1**} {**AI12-0440-1**} Example showing how the body of procedure Inner can be turned into a subunit by rewriting the package body as follows (with the declaration of Parent remaining the same): The body of procedure Inner may be turned into a subunit by rewriting the package body as follows (with the declaration of Parent remaining the same):

```ada
package body Parent is
  Variable : String := "Hello, there."
  procedure Inner is separate;
end Parent;

with Ada.Text_IO;
separate(Parent)
procedure Inner is
  begin
    Ada.Text_IO.Put_Line(Variable);
  end Inner;
```
Extensions to Ada 83

Subunits of the same ancestor library unit are no longer restricted to have distinct identifiers. Instead, we require only that the full expanded names be distinct.

Extensions to Ada 95

\{AI95-00218-03\} An overriding_indicator (see 8.3.1) is allowed on a subprogram stub.

Wording Changes from Ada 95

\{AI95-00243-01\} Clarified that a subunit of a subunit is still a subunit.

Extensions to Ada 2005

\{AI05-0267-1\} An optional aspect_specification can be used in a body_stub. This is described in 13.1.1.

10.1.4 The Compilation Process

Each compilation unit submitted to the compiler is compiled in the context of an environment declarative_part (or simply, an environment), which is a conceptual declarative_part that forms the outermost declarative region of the context of any compilation. At run time, an environment forms the declarative_part of the body of the environment task of a partition (see 10.2, “Program Execution”).

Ramification: At compile time, there is no particular construct that the declarative region is considered to be nested within — the environment is the universe.

To be honest: The environment is really just a portion of a declarative_part, since there might, for example, be bodies that do not yet exist.

\{AI12-0445-1\} The declarative_items of the environment are library_items appearing in an order such that there are no forward semantic dependences. Each included subunit occurs in place of the corresponding stub. The visibility rules apply as if the environment were the outermost declarative region, except that with_clauses are necessary to make declarations of library units visible (see 10.1.2).

\{AI95-00217-06\} The mechanisms for creating an environment and for adding and replacing compilation units within an environment are implementation defined. The mechanisms for adding a compilation unit mentioned in a limited_with_clause to an environment are implementation defined.

Implementation defined: The mechanisms for creating an environment and for adding and replacing compilation units.

Implementation defined: The mechanisms for adding a compilation unit mentioned in a limited_with_clause to an environment.

Ramification: The traditional model, used by most Ada 83 implementations, is that one places a compilation unit in the environment by compiling it. Other models are possible. For example, an implementation might define the environment to be a directory; that is, the compilation units in the environment are all the compilation units in the source files contained in the directory. In this model, the mechanism for replacing a compilation unit with a new one is simply to edit the source file containing that compilation unit.

Name Resolution Rules

\{8652/0032\} \{AI95-00192-01\} \{AI05-0264-1\} If a library_unit_body that is a subprogram_body is submitted to the compiler, it is interpreted only as a completion if a library_unit_declaration for a subprogram or a generic subprogram with the same defining_program_unit_name already exists in the environment for a subprogram other than an instance of a generic subprogram or for a generic subprogram (even if the profile of the body is not type conformant with that of the declaration); otherwise, the subprogram_body is interpreted as both the declaration and body of a library subprogram.

Ramification: The principle here is that a subprogram_body should be interpreted as only a completion if and only if it “might” be legal as the completion of some preexisting declaration, where “might” is defined in a way that does not require overload resolution to determine.
Hence, if the preexisting declaration is a subprogram_declaration or generic_subprogram_declaration, we treat the new subprogram_body as its completion, because it “might” be legal. If it turns out that the profiles don't fully conform, it's an error. In all other cases (the preexisting declaration is a package or a generic package, or an instance of a generic subprogram, or a renaming, or a “spec-less” subprogram, or in the case where there is no preexisting thing), the subprogram_body declares a new subprogram.

4.c

See also AI83-00266/09.

Legality Rules

5. When a compilation unit is compiled, all compilation units upon which it depends semantically shall already exist in the environment; the set of these compilation units shall be consistent in the sense that the new compilation unit shall not semantically depend (directly or indirectly) on two different versions of the same compilation unit, nor on an earlier version of itself.

5.a Discussion: For example, if package declarations A and B both say “with X;”, and the user compiles a compilation unit that says “with A, B;”, then the A and B have to be talking about the same version of X.

5.b Ramification: What it means to be a “different version” is not specified by the language. In some implementations, it means that the compilation unit has been recompiled. In others, it means that the source of the compilation unit has been edited in some significant way.

5.c Note that an implementation cannot require the existence of compilation units upon which the given one does not semantically depend. For example, an implementation is required to be able to compile a compilation unit that says “with A;” when A's body does not exist. It has to be able to detect errors without looking at A's body.

5.d/3 {AI05-0229-1} Similarly, the implementation has to be able to compile a call to a subprogram for which aspect pragmas have been specified without seeing the body of that subprogram — inlining would not be achieved in this case, but the call is still legal.

5.e/3 {AI95-00217-06} {AI05-0005-1} The consistency second rule applies to limited views as well as the full view of a compilation unit. That means that an implementation needs a way to enforce consistency of limited views, not just of full views.

Implementation Permissions

6/2 {AI95-00217-06} The implementation may require that a compilation unit be legal before it can be mentioned in a limited with_clause or it can be inserted into the environment.

7/3 {AI95-00214-01} {AI05-0229-1} When a compilation unit that declares or renames a library unit is added to the environment, the implementation may remove from the environment any preexisting library_item or subunit with the same full expanded name as the defining_program_unit_name. When a compilation unit that is a subunit or the body of a library unit is added to the environment, the implementation may remove from the environment any preexisting version of the same compilation unit.

When a compilation unit that contains a body_stub is added to the environment, the implementation may remove any preexisting library_item or subunit with the same full expanded name as the body_stub.

When a given compilation unit is removed from the environment, the implementation may also remove any compilation unit that depends semantically upon the given one. If the given compilation unit contains the body of a subprogram for which aspect pragmas are True, the implementation may also remove any compilation unit containing a call to that subprogram.

7.a/3 Ramification: {AI05-0005-1} The permissions given in this paragraph correspond to the traditional model, where compilation units enter the environment by being compiled into it, and the compiler checks their legality at that time. In an implementation model in which the environment consists of all source files in a given directory might not want to take advantage of these permissions. Compilation units would not be checked for legality as soon as they enter the environment; legality checking would happen later, when compilation units are compiled. In this model, compilation units might never be automatically removed from the environment; they would be removed when the user explicitly deletes a source file.

7.b Note that the rule is recursive: if the above permission is used to remove a compilation unit containing an inlined subprogram call, then compilation units that depend semantically upon the removed one may also be removed, and so on.

7.c Note that here we are talking about dependences among existing compilation units in the environment; it doesn't matter what with_clauses are attached to the new compilation unit that triggered all this.
An implementation may have other modes in which compilation units in addition to the ones mentioned above are removed. For example, an implementation might inline subprogram calls without an explicit pragma Inline. If so, it either has to have a mode in which that optimization is turned off, or it has to automatically regenerate code for the inlined calls without requiring the user to resubmit them to the compiler.

**Discussion:** \{8652/0108\} \{AI95-00077-01\} \{AI95-00114-01\} In the standard mode, implementations may only remove units from the environment for one of the reasons listed here, or in response to an explicit user command to modify the environment. It is not intended that the act of compiling a unit is one of the “mechanisms” for removing units other than those specified by this document.

\{AI95-00214-01\} These rules are intended to ensure that an implementation never need keep more than one compilation unit with any full expanded name. In particular, it is not necessary to be able to have a subunit and a child unit with the same name in the environment at one time.

**NOTE 1** The rules of the language are enforced across compilation and compilation unit boundaries, just as they are enforced within a single compilation unit.

**Ramification:** \{AI05-0299-1\} Note that Clause 1 requires an implementation to detect illegal compilation units at compile time.

**NOTE 2** \{AI12-0442-1\} An implementation may support a concept of a library, which contains library items. If multiple libraries are supported, the implementation can document how a single environment is constructed when a compilation unit is submitted to the compiler. Naming conflicts between different libraries can, for example, be resolved by treating each library as the root of a hierarchy of child library units.

**Implementation Note:** Alternately, naming conflicts could be resolved via some sort of hiding rule.

**Discussion:** For example, the implementation might support a command to import library Y into library X. If a root library unit called LU (that is, Standard.LU) exists in Y, then from the point of view of library X, it could be called Y.LU. X might contain library units that say, “with Y.LU;”.

**NOTE 3** A compilation unit containing an instantiation of a separately compiled generic unit does not semantically depend on the body of the generic unit. Therefore, replacing the generic body in the environment does not result in the removal of the compilation unit containing the instantiation.

**Implementation Note:** Therefore, implementations have to be prepared to automatically instantiate generic bodies at link-time, as needed. This might imply a complete automatic recompilation, but it is the intent of the language that generic bodies can be (re)instantiated without forcing all of the compilation units that semantically depend on the compilation unit containing the instantiation to be recompiled.

**Extensions to Ada 83**

\{AI95-00077-01\} \{AI95-00114-01\} Ada 83 allowed implementations to require that the body of a generic unit be available when the instantiation is compiled; that permission is dropped in Ada 95. This isn't really an extension (it doesn't allow Ada users to write anything that they couldn't in Ada 83), but there isn't a more appropriate category, and it does allow users more flexibility when developing programs.

**Wording Changes from Ada 95**

**Corrigendum:** The wording was clarified to ensure that a subprogram body is not considered a completion of an instance of a generic subprogram.

**AI95-00214-01** The permissions to remove a unit from the environment were clarified to ensure that it is never necessary to keep multiple (sub)units with the same full expanded name in the environment.

**AI95-00217-06** Units mentioned in a limited_with_clause were added to several rules; limited views have the same presence in the environment as the corresponding full views.

### 10.1.5 Pragmas and Program Units

\{AI12-0417-1\} [This subclause discusses pragmas related to program units, library units, and compilations.]

**Name Resolution Rules**

\{AI12-0417-1\} Certain pragmas are defined to be program unit pragmas. A name given as the argument of a program unit pragma shall resolve to denote the declarations or renamings of one or more program units that occur immediately within the declarative region or compilation in which the pragma immediately occurs, or it shall resolve to denote the declaration of the immediately enclosing program...
unit (if any), the pragma applies to the denoted program unit(s). If there are no names given as arguments, the pragma applies to the immediately enclosing program unit.

Ramification: The fact that this is a Name Resolution Rule means that the pragma will not apply to declarations from outer declarative regions.

Legality Rules

3/5 \{AI12-0417-1\} A program unit pragma shall appear in one of these places:

4/5 • At the place of a compilation_unit, in which case the pragma shall immediately follow in the same compilation (except for other pragmas) a library_unit_declaration that is a subprogram_declaration, generic_subprogram_declaration, or generic_instantiation, and the pragma shall have an argument that is a name denoting that declaration.

Ramification: The name has to denote the immediately preceding library_unit_declaration.

4.a/5 • \{8652/0033\} \{AI95-00136-01\} Immediately within the visible part declaration of a program unit and before any nested declaration (but not within a generic_formal_part), in which case the argument, if any, shall be a direct_name that denotes the immediately enclosing program unit declaration.

Ramification: The argument is optional in this case.

6/5 • At the place of a declaration other than the first, of a declarative_part or program_unit declaration, in which case the pragma shall have an argument, which shall be a direct_name that denotes one or more of the following (and nothing else): a subprogram_declaration, a generic_subprogram_declaration, or a generic_instantiation, of the same declarative_part or program_unit declaration.

Ramification: If you want to denote a subprogram_body that is not a completion, or a package_declaration, for example, you have to put the pragma inside.

7/5 \{AI05-0132-1\} \{AI12-0417-1\} Certain program unit pragmas are defined to be library_unit_pragmas. If a library_unit pragma applies to a program unit, the program unit shall be the name, if any, in a library_unit pragma that denote the declaration of a library unit.

Ramification: This, together with the rules for program_unit pragmas above, implies that if a library_unit pragma applies to a subprogram_declaration (and similar things), it has to appear immediately after the compilation_unit, whereas if the pragma applies to a package_declaration, a subprogram_body that is not a completion (and similar things), it has to appear inside, as the first declarative_item.

Paragraphs 2 through 7 were moved to Annex J, “Obsolescent Features”.

Static Semantics

7.1/5 \{8652/0034\} \{AI95-00041-01\} \{AI12-0417-1\} A library_unit pragma that applies to a generic_unit does not apply to its instances, unless a specific rule for the pragma specifies the contrary.

Post-Compilation Rules

8 Certain pragmas are defined to be configuration pragmas; they shall appear before the first compilation_unit of a compilation. [They are generally used to select a partition-wide or system-wide option.] The pragma applies to all compilation_units appearing in the compilation, unless there are none, in which case it applies to all future compilation_units compiled into the same environment.

Implementation Permissions

9/2 \{AI95-00212-01\} An implementation may require that configuration pragmas that select partition-wide or system-wide options be compiled place restrictions on configuration pragmas, so long as it allows them when the environment contains no library_items other than those of the predefined environment. In this
case, the implementation shall still accept configuration pragmas in individual compilations that confirm the initially selected partition-wide or system-wide options.

Implementation Advice

{8652/0034} {AI95-00041-01} {AI12-0417-1} **When applied to a generic unit, a program-unit pragma that is not a library unit pragma should apply to each instance of the generic unit for which there is not an overriding pragma applied directly to the instance.**

This paragraph was deleted. **Implementation Advice:** When applied to a generic unit, a program-unit pragma that is not a library-unit pragma should apply to each instance of the generic unit for which there is not an overriding pragma applied directly to the instance.

*Paragraph 10 was moved to Annex J, “Obsolescent Features”.*

Wording Changes from Ada 95

This paragraph was deleted. {8652/0033} {AI95-00136-01} {AI12-0417-1} **Corrigendum:** The wording was corrected to ensure that a program unit pragma cannot appear in private parts or generic formal parts.

This paragraph was deleted. {8652/0034} {AI95-00041-01} {AI12-0417-1} **Corrigendum:** The wording was clarified to explain the meaning of program unit and library unit pragmas in generic units.

This paragraph was deleted. {AI12-0417-1} **The Implementation Advice added by the Corrigendum was moved, as it was not in the normal order. (This changes the paragraph number.) It originally was directly after the new Static Semantics rule.**

{AI95-00212-01} **The permission to place restrictions was clarified to:**

- Ensure that it applies only to partition-wide configuration pragmas, not ones like Assertion Policy (see 11.4.2), which can be different in different units; and
- Ensure that confirming pragmas are always allowed.

Wording Changes from Ada 2005

This paragraph was deleted. {AI05-0132-1} {AI12-0417-1} **Correction:** A library unit pragma must apply directly to a library unit, even if no name is given in the pragma.

Wording Changes from Ada 2012

{AI12-0417-1} **The terms “program unit pragma” and “library unit pragma” were moved to Annex J, “Obsolescent Features” (specifically to J.15) as all of the pragmas that use these terms are now in that annex.**

### 10.1.6 Environment-Level Visibility Rules

[The normal visibility rules do not apply within a parent unit name or a context clause, nor within a pragma that appears at the place of a compilation unit. The special visibility rules for those contexts are given here.]

**Static Semantics**

{AI95-00217-06} {AI95-00312-01} **Within the parent unit name at the beginning of an explicit library item, and within a nonlimited with clause with clause,** the only declarations that are visible are those that are explicit library items of the environment, and the only declarations that are directly visible are those that are explicit root library items of the environment. **Within a limited with clause, the only declarations that are visible are those that are the implicit declaration of the limited view of a library package of the environment, and the only declarations that are directly visible are those that are the implicit declaration of the limited view of a root library package. Notwithstanding the rules of 4.1.3, an expanded name in a with clause may consist of a prefix that denotes a generic package and a selector name that denotes a child of that generic package.** [(The child is necessarily a generic unit; see 10.1.1.)]
2.a **Ramification:** In “`package P.Q.R is ... end P.Q.R;`”, this rule requires P to be a root library unit, and Q to be a library unit (because those are the things that are directly visible and visible). Note that visibility does not apply between the “`end`” and the “`;`”.

2.b Physically nested declarations are not visible at these places.

2.c Although Standard is visible at these places, it is impossible to name it, since it is not directly visible, and it has no parent.

2.c.1/2 *{AI95-00217-06} Only compilation units defining limited views can be mentioned in a limited_with_clause, while only compilation units defining full views (that is, the explicit declarations) can be mentioned in a nonlimited_with_clause. This resolves the conflict inherent in having two compilation units with the same defining name.*

2.d/2 *This paragraph was deleted. **Reason:** {AI95-00312-01} The “notwithstanding” part allows “with A.B;” where A is a generic library package and B is one of its (generic) children. This is necessary because it is not normally legal to use an expanded name to reach inside a generic package.*

3 Within a `use_clause` or `pragma` that is within a `context_clause`, each `library_item` mentioned in a previous `with_clause` of the same `context_clause` is visible, and each root `library_item` so mentioned is directly visible. In addition, within such a `use_clause`, if a given declaration is visible or directly visible, each declaration that occurs immediately within the given declaration’s visible part is also visible. No other declarations are visible or directly visible.

3.a **Discussion:** Note the word “same”. For example, if a `with_clause` on a declaration mentions X, this does not make X visible in `use_clauses` and `pragmas` that are on the body. The reason for this rule is the one-pass `context_clauses` Language Design Principle.

3.b Note that the second part of the rule does not mention `pragmas`.

4 Within the `parent_unit_name` of a subunit, `library_items` are visible as they are in the `parent_unit_name` of a `library_item`; in addition, the declaration corresponding to each `body_stub` in the environment is also visible.

4.a **Ramification:** For a subprogram without a separate `subprogram_declaration`, the `body_stub` itself is the declaration.

5 Within a `pragma` that appears at the place of a compilation unit, the immediately preceding `library_item` and each of its ancestors is visible. The ancestor root `library_item` is directly visible.

6/2 *{AI95-00312-01} Notwithstanding the rules of 4.1.3, an expanded name in a `with_clause`, a `pragma` in a `context_clause`, or a `pragma` that appears at the place of a compilation unit may consist of a prefix that denotes a generic package and a `selector_name` that denotes a child of that generic package. [(The child is necessarily a generic unit; see 10.1.1.)]*

6.a/2 **Reason:** This rule allows `with A.B;` and `pragma Elaborate(A.B);` where A is a generic library package and B is one of its (generic) children. This is necessary because it is not normally legal to use an expanded name to reach inside a generic package.

**Wording Changes from Ada 83**

6.b The special visibility rules that apply within a `parent_unit_name` or a `context_clause`, and within a `pragma` that appears at the place of a `compilation_unit` are clarified.

6.c Note that a `context_clause` is not part of any declarative region.

6.d We considered making the visibility rules within `parent_unit_names` and `context_clauses` follow from the context of compilation. However, this attempt failed for various reasons. For example, it would require `use_clauses` in `context_clauses` to be within the declarative region of Standard, which sounds suspiciously like a kludge. And we would still need a special rule to prevent seeing things (in our own `context_clause`) that were with-ed by our parent, etc.

**Wording Changes from Ada 95**

6.e/2 *{AI95-00217-06} Added separate visibility rules for limited `with_clauses`; the existing rules apply only to nonlimited `with_clauses.*

6.f/2 *{AI95-00312-01} Clarified that the name of a generic child unit may appear in a `pragma` in a `context_clause`.**
10.2 Program Execution

An Ada program consists of a set of partitions, which can execute in parallel with one another, possibly in a separate address space, and possibly on a separate computer.

Post-Compilation Rules

{AI12-0439-1} {AI12-0448-1} A partition is a program or part of a program that can be invoked from outside the Ada implementation. [For example, on many systems, a partition cannot be an executable file generated by the system linker.] The user can explicitly assign library units to a partition. The assignment is done in an implementation-defined manner. The compilation units included in a partition are those of the explicitly assigned library units, as well as other compilation units needed by those library units. The compilation units needed by a given compilation unit (the needed compilation units) are determined as follows (unless specified otherwise via an implementation-defined pragma, or by some other implementation-defined means):

Discussion: From a run-time point of view, an Ada 95 partition is identical to an Ada 83 program — implementations were always allowed to provide inter-program communication mechanisms. The additional semantics of partitions is that interfaces between them can be defined to obey normal language rules (as is done in Annex E, “Distributed Systems”), whereas interfaces between separate programs had no particular semantics.

Implementation defined: The manner of explicitly assigning library units to a partition.

Implementation defined: The implementation-defined means, if any, of specifying which compilation units are needed by a given compilation unit.

Discussion: There are no pragmas that “specify otherwise” defined by the core language. However, an implementation is allowed to provide such pragmas, and in fact Annex E, “Distributed Systems” defines some pragmas whose semantics includes reducing the set of compilation units described here.

Term entry: needed compilation unit — compilation unit that is necessary to produce an executable partition, because some entity declared or defined within the unit is used elsewhere in the partition

• {AI12-0448-1} A compilation unit is a needed compilation unit of needs itself;
• {AI12-0448-1} If a compilation unit is among the needed compilation units, then so are any compilation units upon which it depends semantically;
• {AI12-0448-1} If a library_unit_declaration is among the needed compilation units, then so is any corresponding library_unit_body;
• {AI95-00217-06} {AI12-0448-1} If a compilation unit with stubs is among the needed compilation units, then so are any corresponding subunits;
• {AI95-00217-06} {AI12-0448-1} If the (implicit) declaration of the limited view of a library package is among the needed compilation units, then so is the explicit declaration of the library package.

Discussion: Note that in the environment, the stubs are replaced with the corresponding proper_bodies.

• {AI95-00217-06} {AI12-0448-1} If the (implicit) declaration of the limited view of a library package is among the needed compilation units, then so is the explicit declaration of the library package.

Discussion: Note that a child unit is not included just because its parent is included — to include a child, mention it in a with_clause.

{AI95-00217-06} A package is included in a partition even if the only reference to it is in a limited with_clause. While this isn't strictly necessary (no objects of types imported from such a unit can be created), it ensures that all incomplete types are eventually completed, and is the least surprising option.

The user can optionally designate (in an implementation-defined manner) one subprogram as the main subprogram for the partition. A main subprogram, if specified, shall be a subprogram.

Discussion: This may seem superfluous, since it follows from the definition. But we would like to have every error message that might be generated (before run time) by an implementation correspond to some explicitly stated “shall” rule.
Of course, this does not mean that the “shall” rules correspond one-to-one with an implementation's error messages. For example, the rule that says overload resolution “shall” succeed in producing a single interpretation would correspond to many error messages in a good implementation — the implementation would want to explain to the user exactly why overload resolution failed. This is especially true for the syntax rules — they are considered part of overload resolution, but in most cases, one would expect an error message based on the particular syntax rule that was violated.

Each partition has an anonymous *environment task*, which is an implicit outermost task whose execution elaborates the *library_items* of the environment *declarative_part*, and then calls the main subprogram, if there is one. A partition’s execution is that of its tasks.

An implementation is allowed to support multiple concurrent executions of the same partition.

An implementation cannot require the user to specify, say, all of the library units to be included. It has to support, for example, perhaps the most typical case, where the user specifies just one library unit, the main program. The implementation has to do the work of tracking down all the other ones.

The environment task for a partition has the following structure:

```ada
task Environment_Task;

  task body Environment_Task is
    ... (1) -- The environment declarative_part
    ... (that is, the sequence of library_items) goes here.
    begin
      ... (2) -- Call the main subprogram, if there is one.
    end Environment_Task;
```

The name of the environment task is written in italics here to indicate that this task is anonymous.

The environment *declarative_part* at (1) is a sequence of *declarative_items* consisting of copies of the *library_items* included in the partition[]. The order of elaboration of *library_items* is the order in which they appear in the environment *declarative_part*:

- The order of all included *library_items* is such that there are no forward elaboration dependences.
a library_unit_body applies a pragma Elaborate_All to its own declaration, then the library_unit_body will depend on itself.

- {AI05-0229-1} {AI12-0417-1} Any included library_unit_declaration for which aspect pragma Elaborate_Body is True (including when a pragma Elaborate_Body applies) is immediately followed by its library_unit_body, if included.

  Discussion: This implies that the body of such a library unit shall not “with” any of its own children, or anything else that depends semantically upon the declaration of the library unit.

  Proof: {AI05-0229-1} {AI12-0417-1} Pragma Elaborate_Body sets aspect Elaborate_Body, see 10.2.1.

- All library_items declared pure occur before any that are not declared pure.

- All preelaborated library_items occur before any that are not preelaborated.

  Discussion: Normally, if two partitions contain the same compilation unit, they each contain a separate copy of that compilation unit. See Annex E, “Distributed Systems” for cases where two partitions share the same copy of something.

  There is no requirement that the main subprogram be elaborated last. In fact, it is possible to write a partition in which the main subprogram cannot be elaborated last.

  Ramification: This declarative_part has the properties required of all environments (see 10.1.4). However, the environment declarative_part of a partition will typically contain fewer compilation units than the environment declarative_part used at compile time — only the “needed” ones are included in the partition.

There shall be a total order of the library_items that obeys the above rules. The order is otherwise implementation defined.

  Discussion: {AI12-0417-1} The only way to violate this rule is to have Elaborate or Elaborate_All pragmas, or Elaborate Body aspects, that cause circular ordering requirements, thus preventing an order that has no forward elaboration dependences.

  Implementation defined: The order of elaboration of library_items.

  To be honest: {AI12-0005-1} Notwithstanding what the RM95 says elsewhere, each rule that requires a declaration to have a corresponding completion is considered to be a Post-Compilation Rule when the declaration is that of a library unit.

  Discussion: Such rules may be checked at “link time”, for example. Rules requiring the completion to have certain properties, on the other hand, are checked at compile time of the completion.

The full expanded names of the library units and subunits included in a given partition shall be distinct.

  Reason: This is a Post-Compilation Rule because making it a Legality Rule would violate the Language Design Principle labeled “legality determinable via semantic dependences”.

The sequence_of_statements of the environment task (see (2) above) consists of either:

- A call to the main subprogram, if the partition has one. If the main subprogram has parameters, they are passed, where the actuals come from is implementation defined. What happens to the result of a main function is also implementation defined.

  Implementation defined: Parameter passing and function return for the main subprogram.

  or:

- A null_statement, if there is no main subprogram.

  Discussion: For a passive partition, either there is no environment task, or its sequence_of_statements is an infinite loop. See E.1.

{AI12-0439-1} The mechanisms for building and running partitions are implementation defined. [These can might be combined into one operation, as, for example, in dynamic linking, or “load-and-go” systems.]

  Implementation defined: The mechanisms for building and running partitions.
Dynamic Semantics

25 The execution of a program consists of the execution of a set of partitions. Further details are implementation defined. The execution of a partition starts with the execution of its environment task, ends when the environment task terminates, and includes the executions of all tasks of the partition. [The execution of the (implicit) task_body of the environment task acts as a master for all other tasks created as part of the execution of the partition. When the environment task completes (normally or abnormally), it waits for the termination of all such tasks, and then finalizes any remaining objects of the partition.]

25.a Ramification: The “further details” mentioned above include, for example, program termination — it is implementation defined. There is no need to define it here; it's entirely up to the implementation whether it wants to consider the program as a whole to exist beyond the existence of individual partitions.

25.b Implementation defined: The details of program execution, including program termination.

25.c To be honest: The execution of the partition terminates (normally or abnormally) when the environment task terminates (normally or abnormally, respectively).

Bounded (Run-Time) Errors

26 Once the environment task has awaited the termination of all other tasks of the partition, any further attempt to create a task (during finalization) is a bounded error, and may result in the raising of Program_Error either upon creation or activation of the task. If such a task is activated, it is not specified whether the task is awaited prior to termination of the environment task.

Implementation Requirements

27 The implementation shall ensure that all compilation units included in a partition are consistent with one another, and are legal according to the rules of the language.

27.a Discussion: The consistency requirement implies that a partition cannot contain two versions of the same compilation unit. That is, a partition cannot contain two different library units with the same full expanded name, nor two different bodies for the same program unit. For example, suppose we compile the following:

27.b package A is -- Version 1.
   ... end A;
27.c with A;
   package B is
   end B;
27.d package A is -- Version 2.
   ... end A;
27.e with A;
   package C is
   end C;

27.f It would be wrong for a partition containing B and C to contain both versions of A. Typically, the implementation would require the use of Version 2 of A, which might require the recompilation of B. Alternatively, the implementation might automatically recompile B when the partition is built. A third alternative would be an incremental compiler that, when Version 2 of A is compiled, automatically patches the object code for B to reflect the changes to A (if there are any relevant changes — there might not be any).

27.g An implementation that supported fancy version management might allow the use of Version 1 in some circumstances. In no case can the implementation allow the use of both versions in the same partition (unless, of course, it can prove that the two versions are semantically identical).

27.h The core language says nothing about inter-partition consistency; see also Annex E, “Distributed Systems”.

Implementation Permissions

28/3 {AI05-0299-1} The kind of partition described in this subclause is known as an active partition. An implementation is allowed to support other kinds of partitions, with implementation-defined semantics.

28.a Implementation defined: The semantics of any nonactive partitions supported by the implementation.
**Discussion:** Annex E, “Distributed Systems” defines the concept of passive partitions; they may be thought of as a partition without an environment task, or as one with a particularly simple form of environment task, having an infinite loop rather than a call on a main subprogram as its sequence of statements.

An implementation may restrict the kinds of subprograms it supports as main subprograms. However, an implementation is required to support all main subprograms that are public parameterless library procedures.

**Ramification:** The implementation is required to support main subprograms that are procedures declared by generic instantiations, as well as those that are children of library units other than Standard. Generic units are, of course, not allowed to be main subprograms, since they are not subprograms.

Note that renamings are irrelevant to this rule. This rules says which subprograms (not views) have to be supported. The implementation can choose any way it wants for the user to indicate which subprogram should be the main subprogram. An implementation might allow any name of any view, including those declared by renamings. Another implementation might require it to be the original name. Another implementation still might use the name of the source file or some such thing.

If the environment task completes abnormally, the implementation may abort any dependent tasks.

**Reason:** If the implementation does not take advantage of this permission, the normal action takes place — the environment task awaits those tasks.

The possibility of aborting them is not shown in the Environment Task code above, because there is nowhere to put an exception_handler that can handle exceptions raised in both the environment declarative_part and the main subprogram, such that the dependent tasks can be aborted. If we put an exception_handler in the body of the environment task, then it won't handle exceptions that occur during elaboration of the environment declarative_part. If we were to move those things into a nested block_statement, with the exception_handler outside that, then the block_statement would await the library tasks we are trying to abort.

Furthermore, this is merely a permission, and is not fundamental to the model, so it is probably better to state it separately anyway.

Note that implementations (and tools like debuggers) can have modes that provide other behaviors in addition.

**NOTE 1 {AI12-0440-1}** An implementation can provide inter-partition communication mechanism(s) via special packages and pragmas. Standard pragmas for distribution and methods for specifying inter-partition communication are defined in Annex E, “Distributed Systems”. If no such mechanisms are provided, then each partition is isolated from all others, and behaves as a program in and of itself.

**Ramification:** Not providing such mechanisms is equivalent to disallowing multi-partition programs.

An implementation may provide mechanisms to facilitate checking the consistency of library units elaborated in different partitions; Annex E, “Distributed Systems” does so.

**NOTE 2 {AI12-0440-1}** Partitions are not required to run in separate address spaces. For example, an implementation can support dynamic linking via the partition concept.

**NOTE 3 {AI12-0417-1} {AI12-0449-1}** An order of elaboration of library_items that is consistent with the partial ordering defined above does not always ensure that each library_unit_body is elaborated before any other compilation unit whose elaboration necessitates that the library_unit_body be already elaborated. (In particular, there is no requirement that the body of a library unit be elaborated as soon as possible after the library_unit_declaration is elaborated, unless the pragmas or aspects in subclause 10.2.1 are used.)

**NOTE 4 {AI12-0442-1}** A partition (active or otherwise) does not necessarily need not have a main subprogram. In such a case, all the work done by the partition would be done by elaboration of various library_items, and by tasks created by that elaboration. Passive partitions, which cannot have main subprograms, are defined in Annex E, “Distributed Systems”.

**Ramification:** The environment task is the outermost semantic level defined by the language.

Standard has no private part. This prevents strange implementation-dependences involving private children of Standard having visibility upon Standard's private part. It doesn't matter where the body of Standard appears in the environment, since it doesn't do anything. See Annex A, “Predefined Language Environment”.

Note that elaboration dependence is carefully defined in such a way that if (say) the body of something doesn't exist yet, then there is no elaboration dependence upon the nonexistent body. (This follows from the fact that “needed by” is defined that way, and the elaboration dependences caused by a pragma Elaborate or Elaborate All are defined in terms of “needed by”.) This property allows us to use the environment concept both at compile time and at partition-construction time/run time.
Extensions to Ada 83

34.d The concept of partitions is new to Ada 95.

34.e A main subprogram is now optional. The language-defined restrictions on main subprograms are relaxed.

Wording Changes from Ada 83

34.f Ada 95 uses the term “main subprogram” instead of Ada 83’s “main program” (which was inherited from Pascal). This is done to avoid confusion — a main subprogram is a subprogram, not a program. The program as a whole is an entirely different thing.

Wording Changes from Ada 95

\{AI95-00256-01\} The mistaken use of “mentions” in the elaboration dependence rule was fixed.

\{AI95-00217-06\} \{AI12-0448-1\} The needed relationship was extended to include limited views.

10.2.1 Elaboration Control

\{AI12-0417-1\} [This subclause defines aspects and pragmas that help control the elaboration order of library_items.]

Language Design Principles

1.a The rules governing preelaboration are designed to allow it to be done largely by bulk initialization of statically allocated storage from information in a “load module” created by a linker. Some implementations may require run-time code to be executed in some cases, but we consider these cases rare enough that we need not further complicate the rules.

1.b It is important that programs be able to declare data structures that are link-time initialized with aggregates, string_literals, and concatenations thereof. It is important to be able to write link-time evaluated expressions involving the First, Last, and Length attributes of such data structures (including variables), because they might be initialized with positional aggregates or string_literals, and we don't want the user to have to count the elements. There is no corresponding need for accessing discriminants, since they can be initialized with a static constant, and then the constant can be referred to elsewhere. It is important to allow link-time initialized data structures involving discriminant-dependent components. It is important to be able to write link-time evaluated expressions involving pointers (both access values and addresses) to the above-mentioned data structures.

1.c The rules also ensure that no Elaboration_Check need be performed for calls on library-level subprograms declared within a preelaborated package. This is true also of the Elaboration_Check on task activation for library level task types declared in a preelaborated package. However, it is not true of the Elaboration_Check on instantiations.

1.d A static expression should never prevent a library unit from being preelaborable.

Syntax

\{AI12-0417-1\} The form of a pragma Preelaborate is as follows:

\{AI12-0417-1\} \texttt{pragma Preelaborate([library_unit_name]);}

\{AI12-0417-1\} A pragma Preelaborate is a library unit pragma.

\{AI95-00161-01\} \{AI12-0409-1\} The form of a pragma Preelaborable_Initialization is as follows:

\texttt{pragma Preelaborable_Initialization(direct_name)};

Paragraphs 2 through 4 were moved to Annex J, “Obsolescent Features”.

Legality Rules

5 An elaborable construct is preelaborable unless its elaboration performs any of the following actions:

\textbf{Ramification:} A preelaborable construct can be elaborated without using any information that is available only at run time. Note that we don't try to prevent exceptions in preelaborable constructs; if the implementation wishes to generate code to raise an exception, that's OK.
Because there is no flow of control and there are no calls (other than to predefined subprograms), these run-time properties can actually be detected at compile time. This is necessary in order to require compile-time enforcement of the rules.

- The execution of a statement other than a null_statement.
  
  **Ramification:** A preelaborable construct can contain labels and null_statements.

- `{AI12-0175-1}` A call to a subprogram other than:
  
  - a static function;
  
  - an instance of Unchecked Conversion (see 13.9);
  
  - a function declared in System.Storage_Elements (see 13.7.1); or

  **Ramification:** `{AI12-0175-1}` The parameters of any such function have to pass the preelaborability rules, so they typically have to be static expressions. The extra allowed functions are all forms of conversion that the compiler understands, so there should be little implementation burden. Note that such a call might raise an exception; preelaborable is not the same as elaborable with no code.

- The evaluation of a primary that is a name of an object, unless the name is a static expression, or statically denotes a discriminant of an enclosing type.
  
  **Ramification:** One can evaluate such a name, but not as a primary. For example, one can evaluate an attribute of the object. One can evaluate an attribute_reference, so long as it does not denote an object, and its prefix does not disobey any of these rules. For example, Obj'Access, Obj'Unchecked_Access, and Obj'Address are generally legal in preelaborated library units.

- `{AI95-00161-01}` `{AI05-0028-1}` The creation of an object [(including a component)] that is initialized by default, if its own type does not have preelaborable initialization. Similarly, a default-initialized object [(including a component)] of a descendant of a private type, private extension, controlled type, task type, or protected type with entry_declarations, similarly the evaluation of an extension_aggregate with an ancestor subtype_mark denoting a subtype of such a type.
  
  **Ramification:** One can declare these kinds of types, but one cannot create objects of those types.

- `{AI95-00161-01}` `{AI12-0232-1}` The elaboration of any elaborable construct that is not preelaborable.
  
  `{AI12-0232-1}` A generic declaration is preelaborable unless every instance would perform one of the above actions.
  
  **Ramification:** `{AI12-0232-1}` `{AI12-0417-1}` A generic declaration is preelaborable unless there is no instance that could be declared preelaborated. For instance, a generic package declaration that directly contains a variable initialized by a non-static function that is not a formal function is not preelaborable (and thus would be illegal if the Preelaborate aspect were applied to it).

- `{AI95-00403-01}` A generic body is preelaborable only if elaboration of a corresponding instance body would not perform any such actions, preserving that: the actual for each formal private type (or extension) is a private type (or extension), and the actual for each formal subprogram is a user-defined subprogram.

- `{AI95-000403-01}` `{AI12-0417-1}` the actual for each discriminated formal derived type, formal private type, (or formal private extension) declared within the formal part of the generic unit is a private type (or extension) that does not have preelaborable initialization, unless the pragma Preelaborable_Initialization aspect was specified for has been applied to the formal type:

- `{AI95-00403-01}` the actual for each formal type is nonstatic:
• \{AI95-00403-01\} the actual for each formal object is nonstatic; and
• \{AI95-00403-01\} the actual for each formal subprogram is a user-defined subprogram.

**Discussion**: \{AI95-00403-01\] This is an “assume-the-worst” rule. The elaboration of a generic unit doesn't perform any of the actions listed above, because its sole effect is to establish that the generic can from now on be instantiated. So the elaboration of the generic itself is not the interesting part when it comes to preelaboration rules. The interesting part is what happens when you elaborate “any instantiation” of the generic. For instance, declaring an object of a limited formal private type might well start tasks, call functions, and do all sorts of nonpreelaborable things. We prevent these situations by assuming that the actual parameters are as badly behaved as possible.

**Reason**: Without this rule about generics, we would have to forbid instantiations in preelaborated library units, which would significantly reduce their usefulness.

**Ramification**: In a generic body, we assume the worst about formal private types and extensions.

**Aspect Description for Preelaborate**: Code execution during elaboration is avoided for a given package.

**Discussion**: \{AI12-0417-1\] Rules for specifying a library unit aspect (like Preelaborate) are found in 13.1.1.

**The following rules specify which entities have preelaborable initialization, namely that the Preelaborable Initialization aspect of the entity is True**:  

- \{AI05-0028-1\} \{AI12-0409-1\} \{AI12-0444-1\] The partial view of a private type or private extension, a protected type without entry declarations, a generic formal private type, or a generic formal derived type, have preelaborable initialization if and only if the \pragmas Preelaborate aspect has been specified True for them. [A protected type with entry declarations or a task type never has preelaborable initialization.] The Preelaborable Initialization aspect of a partial view of a type may be specified as False, even if the full view of the type has preelaborable initialization. Similarly, a generic formal type may be specified with Preelaborable Initialization False, even if the actual type in an instance has preelaborable initialization.

- A component (including a discriminant) of a record or protected type has preelaborable initialization if its declaration includes a default expression whose execution does not perform any actions prohibited in preelaborable constructs as described above, or if its declaration does not include a default expression and its type has preelaborable initialization.

- \{AI05-0028-1\} \{AI05-0221-1\] A derived type has preelaborable initialization if its parent type has preelaborable initialization and (in the case of a derived record extension) if the noninherited
components all have preelaborable initialization. However, a user-defined controlled type with an
overriding Initialize procedure that is not a null procedure does not have preelaborable initialization.

- \{AI95-00161-01\} \{AI95-00345-01\} A view of a type has preelaborable initialization if it is an
elementary type, an array type whose component type has preelaborable initialization, a record
type whose components all have preelaborable initialization, or an interface type.

- \{AI95-00161-01\} \{AI12-0409-1\} The following attribute is defined for a nonformal composite subtype \$S\$
declared within the visible part of a package or a generic package, or a generic formal private subtype or
formal derived subtype: \{\texttt{pragma Preelaborable\_Initialization \texttt{specifies that a type has preelaborable}
initalization. This pragma shall appear in the visible part of a package or generic-package.

\texttt{S\_Preelaborable\_Initialization}

\{AI12-0409-1\} This attribute is of Boolean type, and its value reflects whether the type of \$S\$
has preelaborable initialization. The value of this attribute, the type-related
\texttt{Preelaborable\_Initialization} aspect, may be specified for any type for which the attribute is
defined. The value shall be specified by a static expression, unless the type is not a formal
type but is nevertheless declared within a generic package. In this latter case, the value
may also be specified by references to the Preelaborable Initialization attribute of one or more
formal types visible at the point of the declaration of the composite type, conjoined with \texttt{and}.

\textbf{Ramification:} \{AI12-0409-1\} “Formal types visible at the point of the declaration” includes all visible formal types,
including those that might have been declared in formal packages or in child packages.

\textbf{Aspect Description for Preelaborable\_Initialization:} Declares that a type has preelaborable initialization.

\{AI95-00161-01\} \{AI93-00345-01\} \{AI05-0028-1\} \{AI12-0409-1\} If the pragma appears in the first list
of \texttt{basic\_declarative\_items\_of\_a\_package\_specification}, then the direct name shall denote the first
subtype of a composite \texttt{private\_type,\_private\_extension,\_or\_protected\_type\_that\_is\_not\_an\_interface\_type\_and\_is
without entry\_declarations}, and the type shall be declared immediately within the same package as the
pragma. If the Preelaborable\_Initialization aspect is specified \texttt{True} for \texttt{pragma is applied to a private\_type}
or a private extension, the full view of the type shall have preelaborable initialization. If the aspect is
specified \texttt{True} for \texttt{pragma is applied to a protected\_type}, the protected type shall not have entries, and
each component of the protected type shall have preelaborable initialization. If the aspect is specified
\texttt{True} for a generic formal type, then in a \texttt{generic\_instantiation} the corresponding actual type shall have
preelaborable initialization. If the aspect definition includes one or more Preelaborable Initialization
attribute references, then the full view of the type shall have preelaborable initialization presuming the
types mentioned in the prefixes of the attribute references have preelaborable initialization. For any
other composite type, the aspect shall be specified statically \texttt{True} or \texttt{False} only if it is confirming that
shall have preelaborable initialization. In addition to the places where Legality Rules normally apply (see
12.3), these rules apply also in the private part of an instance of a generic unit.

\textbf{Reason:} \{AI05-0028-1\} \{AI12-0409-1\} The reason why we need to be allowed to specify the aspect \texttt{the pragma} for
private types, private extensions, and protected types is fairly clear: the properties of the full view determine whether
the type has preelaborable initialization or not; in order to preserve privacy we need a way to express on the partial
view that the full view is well-behaved. The reason why we need to be allowed to specify the aspect \texttt{the pragma} for
other composite types is more subtle: a nonnull override for Initialize might occur in the private part, even for a
nonprivate type; in order to preserve privacy, we need a way to express on a type declared in a visible part that the
private part does not contain any nasty override of Initialize.

\{AI95-00161-01\} \{AI12-0409-1\} If the \texttt{pragma appears in a generic\_formal\_part}, then the direct name
shall denote a generic formal private type or a generic formal derived type declared in the same
generic\_formal\_part as the pragma. In a \texttt{generic\_instantiation} the corresponding actual type shall have
preelaborable initialization.

\textbf{Ramification:} \{AI12-0409-1\} Not only do protected types with entry declarations and task types not have
preelaborable initialization, but they cannot have \texttt{pragma Preelaborable\_Initialization} aspect specified \texttt{True} for applied
to them.
In an implementation, a type declared in a preelaborated package should have the same representation in every elaboration of a given version of the package, whether the elaborations occur in distinct executions of the same program, or in executions of distinct programs or partitions that include the given version.

**Implementation Advice:** A type declared in a preelaborated package should have the same representation in every elaboration of a given version of the package.

```ada
pragma Pure((library_unit_name));
```

**Paragraphs 13 through 15 were moved to Annex J, “Obsolescent Features”**

**Static Semantics**

- **The form of a pragma Pure is as follows:**
  ```ada
  pragma Pure((library_unit_name));
  ```
  A pragma Pure is a library unit pragma.

- A pure program compilation unit is a preelaborable program compilation unit whose elaboration does not perform any of the following actions:
  - the elaboration of a variable declaration;
  - the evaluation of an allocator of an access-to-variable type; for the purposes of this rule, the partial view of a type is presumed to have nonvisible components whose default initialization evaluates such an allocator;
  - the elaboration of the declaration of a nonderived named access-to-variable type unless the Storage Size of the type has been specified by a static expression with value zero or is defined by the language to be zero;
  - the elaboration of the declaration of a nonderived named access-to-variable type unless the Storage Size of the type has been specified by a static expression with value zero or is defined by the language to be zero;
  - the elaboration of any program unit that is not pure.
A generic declaration is pure unless every instance would perform one of the above actions.

**Ramification:** A generic declaration is pure unless there is no instance that could be declared pure. For instance, a generic package declaration that directly contains a variable declaration is not pure (and thus would be illegal if aspect Pure is specified for it).

A generic body is pure only if elaboration of a corresponding instance body would not perform any such actions presuming any composite formal types have nonvisible components whose default initialization evaluates an allocator of an access-to-variable type.

The Storage Size for an anonymous access-to-variable type declared at library level in a library unit that is declared pure is defined to be zero.

**Ramification:** This makes allocators illegal for such types (see 4.8), making a storage pool unnecessary for these types. A storage pool would represent state.

Note that access discriminants and access parameters are never library-level, even when they are declared in a type or subprogram declared at library-level. That's because they have their own special accessibility rules (see 3.10.2).

This paragraph was deleted.

A pure library item is a preelaborable library item that does not contain the declaration of any variable or named access within a subprogram, generic subprogram, task unit, or protected unit.

When the library unit aspect Pure of a program unit is True, the `pragma Pure` is used to specify/declare that a library unit is said to be declared pure. When the Pure aspect is specified True for a library unit, namely that the Pure aspect of the library unit is True; all compilation units of the library unit are declared pure. In addition, the limited view of any library package is declared pure. The declaration and body of a declared pure library unit, and all subunits that are elaborated as part of elaborating the library unit, shall be pure. All `pragma Pure` applies to a library unit, then its compilation units of a declared pure library unit shall be pure, and they shall depend semantically only on compilation units of other library units that are declared pure library items. In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit. Furthermore, the full view of any partial view declared in the visible part of a declared pure the library unit that has any available stream attributes shall support external streaming (see 13.13.2).

This paragraph was deleted.

A declared-pure library unit is one to which a `pragma Pure` applies. Its declaration and body are also said to be declared pure.

**Discussion:** A declared-pure package is useful for defining types to be shared between partitions with no common address space.

**Reason:** Note that generic packages are not mentioned in the list of things that can contain variable declarations. Note that the Ada 95 rules for deferred constants make them allowable in library units that are declared pure; that isn't true of Ada 83's deferred constants.

**Ramification:** Anonymous access types (that is, access discriminants and access parameters) are allowed.

A limited view is not a library unit, so any rule that starts “declared pure library unit” does not apply to a limited view. In particular, the 3rd and last sentences never apply to limited views. However, a limited view is a library item, so rules that discuss “declared pure library items” do include limited views.

If a unit is not declared pure, the value of the Pure aspect for that unit is False.

**Reason:** Ada 95 didn't allow any access types as the primary reason for disallowing named access types is that an allocator has a side effect; the pool constitutes variable data. We considered somehow allowing allocator less access types. However, these (including access-to-subprogram types) would cause trouble for Annex E, “Distributed Systems”, because such types would allow access values in a shared passive partition to designate objects in an active partition, thus allowing inter-address space references. We decided to disallow such uses in the relatively rare cases where they cause problems, rather than making life harder for the majority of users. Types declared in a pure
package can be used in remote operations only if they are externally streamable. That simply means that there is a means to transport values of the type; that's automatically true for nonlimited types that don't have an access part. The only tricky part about this is to avoid privacy leakage; that was handled by ensuring that any private types (and private extensions) declared in a pure package that have available stream attributes (which include all nonlimited types by definition) have to be externally streamable. Furthermore, a named access to object type without a pool would be a new concept, adding complexity from the user's point of view. Finally, the prevention of allocators would have to be a runtime check, in order to avoid violations of the generic contract model.

Aspect Description for Pure: Side effects are avoided in the subprograms of a given package.

Errorneous Execution

{AI12-0076-1} Execution is erroneous if some operation (other than the initialization or finalization of the object) modifies the value of a constant object declared at library-level in a pure package.

Discussion: This could be accomplished via a self-referencing pointer or via squirrelling a writable pointer to a controlled object.

Implementation Permissions

{AI95-00366-01} {AI05-0219-1} If a library unit is declared pure, then the implementation is permitted to omit a call on a library-level subprogram of the library unit if the results are not needed after the call. In addition, the implementation may omit such a call on such a subprogram and simply reuse the results produced by an earlier call on the same subprogram, provided that none of the parameters nor any object accessible via access values from the parameters have any part that is of a type whose full type is an immutablyare of a limited type, and the addresses and values of all by-reference actual parameters, and the values of all by-copy-in actual parameters, and the values of all objects accessible via access values from the parameters, are the same as they were at the earlier call. [This permission applies even if the subprogram produces other side effects when called.]

Discussion: {AI95-00366-01} {AI05-0005-1} {AI05-0299-1} A declared-pure library_item has no variable state. Hence, a call on one of its (nonnested) subprograms cannot have side effects. Side effects are still possible via dispatching calls and via indirect calls through access-to-subprogram values. Other mechanisms that might be used to modify variable state include: the only possible side effects from such a call would be through machine code insertions, imported subprograms, and unchecked conversion to an access type declared within the subprogram; this list is not exhaustive and similar features. Thus, the permissions described in this subclause may apply to a subprogram whose execution has side effects. The compiler may omit a call to such a subprogram even if such side effects exist, so the writer of such a subprogram has to keep this in mind.

Syntax

{AI12-0417-1} The following pragmas are defined with the given forms:
The form of a pragma Elaborate, Elaborate_All, or Elaborate_Body is as follows:

Pragma Elaborate(library_unit_name{, library_unit_name});

Pragma Elaborate_All(library_unit_name{, library_unit_name});

This paragraph was deleted. {AI12-0417-1} 

Pragma Elaborate_Body((library_unit_name));

A pragma Elaborate or Elaborate_All is only allowed within a context_clause.

Ramification: “Within a context_clause” allows it to be the last item in the context_clause. It can't be first, because the name has to denote something mentioned earlier.

This paragraph was deleted. {AI12-0417-1} A pragma Elaborate_Body is a library unit pragma.

Discussion: Hence, a pragma Elaborate or Elaborate_All is not elaborated, not that it makes any practical difference.

Note that a pragma Elaborate or Elaborate_All is neither a program unit pragma, nor a library unit pragma.
Legality Rules

\{AI05-0229-1\} \{AI12-0417-1\} If the aspect pragma Elaborate_Body is True for a declaration [including when pragma Elaborate_Body applies], then the declaration requires a completion [(a body)].

**Proof:** \{AI05-0229-1\} \{AI12-0417-1\} Pragma Elaborate_Body sets the aspect (see below).

\{AI95-00217-06\} The library unit name of a pragma Elaborate or Elaborate_All shall denote a nonlimited view of a library unit.

**Reason:** These pragmas are intended to prevent elaboration check failures. But a limited view does not make anything visible that has an elaboration check, so the pragmas cannot do anything useful. Moreover, the pragmas would probably reintroduce the circularity that the limited_with_clause was intended to break. So we make such uses illegal.

Static Semantics

\{AI05-0229-1\} A pragma Elaborate specifies that the body of the named library unit is elaborated before the current library_item. A pragma Elaborate_All specifies that each library_item that is needed by the named library unit declaration is elaborated before the current library_item. A pragma Elaborate_Body specifies that the body of the library unit is elaborated immediately after its declaration.

**Proof:** The official statement of the semantics of these pragmas is given in 10.2.

\{AI05-0229-1\} A pragma Elaborate_Body sets the Elaborate_Body representation aspect of the library unit to which it applies to the value True. [If the Elaborate_Body aspect of a library unit is True, the body of the library unit is elaborated immediately after its declaration.]

**Proof:** The official statement of the semantics of this aspect is given in 10.2.

**Implementation Note:** \{AI12-0417-1\} The specification presence of the pragma Elaborate_Body aspect simplifies the removal of unnecessary Elaboration_Checks. For a subprogram declared immediately within a library unit for which the pragma Elaborate_Body aspect is specified as True, the only calls that can fail the Elaboration Check are those that occur in the library unit itself, between the declaration and body of the called subprogram; if there are no such calls (which can easily be detected at compile time if there are no stubs), then no Elaboration_Checks are needed for that subprogram. The same is true for Elaboration_Checks on task instantiations, and for library subprograms and generic units.

**Ramification:** The fact that the unit of elaboration is the library_item means that if a subprogram body is not a completion, it is impossible for any library_item to be elaborated between the declaration and the body of such a subprogram. Therefore, it is impossible for a call to such a subprogram to fail its Elaboration_Check.

**Discussion:** The visibility rules imply that each library_unit name of a pragma Elaborate or Elaborate_All has to denote a library unit mentioned by a previous with_clause of the same context_clause.

**Aspect Description for Elaborate_Body:** A given package will not have a body, and that body is elaborated immediately after the declaration.

**NOTE 1** \{AI12-0447-1\} A preelaborated library unit canis allowed to have nonpreelaborable children.

**Ramification:** \{8652/0035\} \{AI95-00002-01\} But generally not nonpreelaborated subunits. (Nonpreelaborated subunits of subprograms are allowed as discussed above.)

**NOTE 2** \{AI12-0447-1\} A library unit that is declared pure canis allowed to have impure children.

**Ramification:** \{8652/0035\} \{AI95-00002-01\} But generally not impure subunits. (Impure subunits of subprograms are allowed as discussed above.)

**Ramification:** Pragma Elaborate is mainly for closely related library units, such as when two package bodies 'with' each other's declarations. In such cases, Elaborate_All sometimes won't work.

Extensions to Ada 83

The concepts of preelaborability and purity are new to Ada 95. The Elaborate_All, Elaborate_Body, Preelaborate, and Pure pragmas are new to Ada 95.

Pragma Elaborate are allowed to be mixed with the other things in the context_clause — in Ada 83, they were required to appear last.
Incompatibilities With Ada 95

28.k/3 {AI05-0028-1} **Correction**: Corrected a serious unintended incompatibility with Ada 95 in the new preelaboration wording — explicit initialization of objects of types that don't have preelaborable initialization was not allowed. Ada 2012 switches back to the Ada 95 rule in these cases. This is unlikely to occur in practice, as it is unlikely that a compiler would have implemented the more restrictive rule (it would fail many ACATS tests if it did).

28.l/3 {AI05-0035-1} **Correction**: Added an assume-the-worst rule for generic bodies (else they would never be checked for purity) and added the boilerplate so that the entire generic specification is rechecked. Also fixed wording to have consistent handling for subunits for Pure and Preelaborate. An Ada 95 program could have depended on marking a generic pure that was not really pure, although this would defeat the purpose of the categorization and likely cause problems with distributed programs.

Extensions to Ada 2005

28.m/3 {AI05-0035-1} **Correction**: Adjusted wording so that a subunit can be pure (it is not a library item, but it is a compilation unit).

28.n/3 {AI05-0035-1} **Correction**: Adjusted wording so that the rules for access types only apply to nonderived types (derived types share their storage pool with their parent, so if the parent access type is legal, so is any derived type.)

28.o/5 {AI05-0229-1} {AI12-0417-1} Elaborate Body is now an aspect, so it can be specified by an aspect specification — although the pragmas is still preferred by the Reference Manual.

28.p/5 {AI05-0243-1} {AI12-0417-1} Pure and Preelaborate are now aspects, so they can be specified by an aspect specification — although the pragmas is still preferred by the Reference Manual.

Wording Changes from Ada 2005

28.q/3 {AI05-0034-1} **Correction**: Added wording so that a limited view is always treated as pure, no matter what categorization is used for the originating unit. This was undefined in Ada 2005.

28.r/3 {AI05-0028-1} {AI05-0221-1} **Correction**: Fixed minor issues with preelaborable initialization (PI): null Initialize procedures do not make a type non-PI; formal types with pragma PI can be assumed to have PI; formal extensions are assumed to have PI; all composite types can have pragma PI (so that the possibility of hidden Initialize routines can be handled); added discriminants of a derived type are not considered in calculating PI.
Clarified that the implementation permission to omit pure subprogram calls does not apply if any part of the parameters or any designated object has a part that is immutably limited. The old wording just said "limited type", which can change via visibility and thus isn't appropriate for dynamic semantics permissions.

Incompatibilities With Ada 2012

Added a rule that a generic declaration is not pure if no instance could be pure (for instance, because the generic declaration would elaborate a variable.) This was legal in Ada 2012, but of course no instance could have been declared pure. A similar rule (with a similar effect) was added for preelaborable generic declarations.

Added some intrinsic conversion functions to those allowed to be called during the elaboration of a preelaborated unit. This is necessary to allow a portable Address aspect in a preelaborated unit, important on small embedded systems.

Aspect Preelaborable Initialization is new; pragma Preelaborable Initialization is now obsolescent.

Corrigendum: Explicitly stated that modifying a library-level constant in a pure package is erroneous. We don't document this as inconsistent as implementations certainly can still do whatever they were previously doing (no change is required); moreover, this case (and many more) were erroneous in Ada 2005 and before, so we're just restoring the previous semantics.

Correction: Explicitly stated that the pure and preelaborate rules are recursive; that is, they apply to the contents of nested packages and generic packages.

The pragmas that set aspects (Pure, Preelaborate, Elaborate Body) are now obsolescent.
11 Exceptions

{AI05-0299-1} [This clause section defines the facilities for dealing with errors or other exceptional situations that arise during program execution.] An exception represents a kind of exceptional situation; an occurrence of such a situation (at run time) is called an exception occurrence. [To raise an exception is to abandon normal program execution so as to draw attention to the fact that the corresponding situation has arisen. Performing some actions in response to the arising of an exception is called handling the exception.]

To be honest: ...or handling the exception occurrence.

Ramification: For example, an exception End_Error might represent error situations in which an attempt is made to read beyond end-of-file. During the execution of a partition, there might be numerous occurrences of this exception.

To be honest: {AI12-0426-1} When the meaning is clear from the context, we sometimes use “occurrence” as a shorthand for “exception occurrence”.

Term entry: exception — kind of exceptional situation

Term entry: exception occurrence — run-time occurrence of an exceptional situation

{AI05-0043-1} {AI05-0258-1} [An exception_declaration declares a name for an exception. An exception can be raised explicitly (for example, initially either by a raise_statement) or implicitly (for example, by the failure of a language-defined check). When an exception arises, control can be transferred to a user-provided exception_handler at the end of a handled_sequence_of_statements, or it can be propagated to a dynamically enclosing execution.]

Wording Changes from Ada 83

We are more explicit about the difference between an exception and an occurrence of an exception. This is necessary because we now have a type (Exception_Occurrence) that represents exception occurrences, so the program can manipulate them. Furthermore, we say that when an exception is propagated, it is the same occurrence that is being propagated (as opposed to a new occurrence of the same exception). The same issue applies to a re-raise statement. In order to understand these semantics, we have to make this distinction.

Wording Changes from Ada 2005

{AI05-0043-1} Correction: Generalized the introductory description of how an exception can be raised so that it does not appear to cover all of the cases.

11.1 Exception Declarations

An exception_declaration declares a name for an exception.

Syntax

{AI05-0183-1} exception_declaration ::= defining_identifier_list : exception _ [aspect_specification];

Static Semantics

Each single exception_declaration declares a name for a different exception. If a generic unit includes an exception_declaration, the exception_declarations implicitly generated by different instantiations of the generic unit refer to distinct exceptions (but all have the same defining_identifier). The particular exception denoted by an exception name is determined at compilation time and is the same regardless of how many times the exception_declaration is elaborated.

Reason: We considered removing this requirement inside generic bodies, because it is an implementation burden for implementations that wish to share code among several instances. In the end, it was decided that it would introduce too much implementation dependency.
Ramification: Hence, if an exception_declaration occurs in a recursive subprogram, the exception name denotes the same exception for all invocations of the recursive subprogram. The reason for this rule is that we allow an exception occurrence to propagate out of its declaration's innermost containing master; if exceptions were created by their declarations like other entities, they would presumably be destroyed upon leaving the master; we would have to do something special to prevent them from propagating to places where they no longer exist.

Ramification: Exception identities are unique across all partitions of a program.

The predefined exceptions are the ones declared in the declaration of package Standard: Constraint_Error, Program_Error, Storage_Error, and Tasking_Error; one of them is raised when a language-defined check fails.

Ramification: The exceptions declared in the language-defined package IO_Exceptions, for example, are not predefined.

Dynamic Semantics

The elaboration of an exception_declaration has no effect.

The execution of any construct raises Storage_Error if there is insufficient storage for that execution. The amount of storage necessary for the execution of constructs is unspecified.

Ramification: Note that any execution whatsoever can raise Storage_Error. This allows much implementation freedom in storage management.

Examples

Examples of user-defined exception declarations:

Singular : exception;
Error : exception;
Overflow, Underflow : exception;

Inconsistencies With Ada 83

The exception Numeric_Error is now defined in the Obsolescent features Annex, as a rename of Constraint_Error. All checks that raise Numeric_Error in Ada 83 instead raise Constraint_Error in Ada 95. To increase upward compatibility, we also changed the rules to allow the same exception to be named more than once by a given handler. Thus, “when Constraint_Error | Numeric_Error =>” will remain legal in Ada 95, even though Constraint_Error and Numeric_Error now denote the same exception. However, it will not be legal to have separate handlers for Constraint_Error and Numeric_Error. This change is inconsistent in the rare case that an existing program explicitly raises Numeric_Error at a point where there is a handler for Constraint_Error; the exception will now be caught by that handler.

Wording Changes from Ada 83

We explicitly define elaboration for exception_declarations.

Extensions to Ada 2005

An optional aspect_specification can be used in a exception_declaration. This is described in 13.1.1.

11.2 Exception Handlers

[The response to one or more exceptions is specified by an exception_handler.]

Syntax

handled_sequence_of_statements ::= sequence_of_statements [exception exception_handler {exception_handler}]

exception_handler ::= when [choice_parameter_specification:] exception_choice {I exception_choice} =>
sequence_of_statements

choice_parameter_specification ::= defining_identifier

exception_choice ::= exception_name | others

To be honest: “Handler” is an abbreviation for “exception_handler”. 

{AI05-0299-1} Within this clause section, we sometimes abbreviate “exception_choice” to “choice”.

Legality Rules

{AI12-0022-1} An exception_name of an exception_choice shall denote an exception.

A choice with an exception_name covers the named exception. A choice with others covers all exceptions not named by previous choices of the same handled_sequence_of_statements. Two choices in different exception_handlers of the same handled_sequence_of_statements shall not cover the same exception.

Ramification: Two exception_choices of the same exception_handler may cover the same exception. For example, “when Ada.Text_IO.Data_Error | My_Seq.IO.Data_Error =>”. An others choice even covers exceptions that are not visible at the place of the handler. Since exception raising is a dynamic activity, it is entirely possible for an others handler to handle an exception that it could not have named.

A choice with others is allowed only for the last handler of a handled_sequence_of_statements and as the only choice of that handler.

An exception_name of a choice shall not denote an exception declared in a generic formal package.

Reason: This is because the compiler doesn't know the identity of such an exception, and thus can't enforce the coverage rules.

Static Semantics

A choice_parameter_specification declares a choice parameter, which is a constant object of type Exception_Occurrence (see 11.4.1). During the handling of an exception occurrence, the choice parameter, if any, of the handler represents the exception occurrence that is being handled.

Dynamic Semantics

The execution of a handled_sequence_of_statements consists of the execution of the sequence_of_statements. [The optional handlers are used to handle any exceptions that are propagated by the sequence_of_statements.]

Examples

Example of an exception handler:

{AI12-0178-1} begin
  Open(File, In_File, "input.txt");  -- see A.8.2
  exception
    when E : Name_Error =>
      Put("Cannot open input file : ");
      Put_Line(Ada.Exceptions.Exception_Message
        Exception_Message(E));  -- see 11.4.1
      raise;
  end;

Extensions to Ada 83

The syntax rule for exception_handler is modified to allow a choice_parameter_specification.

{AI95-00114-01} Different exception_choice choices of the same exception_handler may cover the same exception.

This allows for “when Numeric_Error | Constraint_Error =>” even though Numeric_Error is a rename of Constraint_Error. This also allows one to “with” two different I/O packages, and then write, for example, “when
Wording Changes from Ada 83

The syntax rule for `handled_sequence_of_statements` is new. These are now used in all the places where handlers are allowed. This obviates the need to explain (in Clauses Sections 5, 6, 7, and 9) what portions of the program are handled by the handlers. Note that there are more such cases in Ada 95.

The syntax rule for `choice_parameter_specification` is new.

11.3 Raise Statements and Raise Expressions

[A raise_statement raises an exception.]

Syntax

```
{AI95-00361-01} raise_statement ::= raise;

| raise exception_name [with string_expression]; raise [exception_name];

{AI12-0022-1} {AI12-0152-1} raise_expression ::= raise exception_name [with string_simple_expression]

{AI12-0152-1} If a raise_expression appears within the expression of one of the following contexts, the raise_expression shall appear within a pair of parentheses within the expression:

- object_declaration;
- modular_type_definition;
- floating_point_definition;
- ordinary_fixed_point_definition;
- decimal_fixed_point_definition;
- default_expression;
- ancestor_part.

Reason: Unlike conditional expressions, this doesn't say "immediately surrounded"; the only requirement is that it is somehow within a pair of parentheses that is part of the expression. We need this restriction in order that raise_expressions cannot be syntactically confused with immediately following constructs (such as aspect_specifications).

Discussion: We only need to require that a right parenthesis appear somewhere between the raise_expression and the surrounding context; that's all we need to specify in order to eliminate the ambiguities. Moreover, we don't care at all where the left parenthesis is (so long as it is legal, of course).

For instance, the following is illegal by this rule:

Obj : Boolean := Func_Call or else raise TBD_Error with Atomic;
```

as the "with Atomic" could be part of the raise_expression or part of the object declaration. Both of the following are legal:

```
Obj : Boolean := Func_Call or else (raise TBD_Error with Atomic);
Obj : Boolean := (Func_Call or else raise TBD_Error) with Atomic;
```

and if the with belongs to the raise_expression, then both of the following are legal:

```
Obj : Boolean := Func_Call or else (raise TBD_Error with Atomic);
Obj : Boolean := (Func_Call or else raise TBD_Error with Atomic);
```

This rule only requires parentheses for raise_expressions that are part of the "top-level" of an expression in one of the named contexts; the raise_expression is either the entire expression, or part of a chain of logical operations. In practice, the raise_expression will almost always be last in interesting top-level expressions; anything that follows it could never be executed, so that should be rare. Other contexts such as conditional expressions, qualified expressions, aggregates, and even function calls, provide the needed parentheses. All of the following are legal, no additional parens are needed:
Pre : Boolean := (if not Is_Valid(Param) then raise Not_Valid_Error);
A : A_Tagged := (Some_Tagged'raise TBD_Error with Comp => 'A');
B : Some_Array := (1, 2, 3, others => raise Not_Valid_Error);
C : Natural := Func (Val => raise TBD_Error);

Parentheses that are part of the context of the expression don’t count. For instance, the parentheses around the raise_expression are required in the following:

D : A_Tagged := ((raise TBD_Error with Comp => 'A'));

as ancestor_part is one of the contexts that triggers the rule.

This English-language rule could have been implemented instead by adding nonterminals initial_expression and initial_relation, which are the same as choice_expression and choice_relation except for the inclusion of membership in initial_relation. Then, initial_expression could be used in place of expression in all of the contexts noted. We did not do that because of the large amount of change required, both to the grammar and to language rules that refer to the grammar. A complete grammar is given in AI12-0152-1.

The use of a raise_expression is illegal in each of modular_type_definition, floating_point_definition, ordinary_fixed_point_definition, and decimal_fixed_point_definition as these uses are required to be static and a raise_expression is never static. We include these in this rule so that Ada text has an unambiguous syntax in these cases.

Legality Rules

\{AI12-0022-1\} \{AI12-0159-1\} The exception_name, if any, of a raise_statement or raise_expression shall denote an exception. A raise_statement with no exception_name (that is, a re-raise_statement) shall be within a handler, but not within a body enclosed by that handler.

Name Resolution Rules

\{AI95-00361-01\} \{AI12-0022-1\} \{AI12-0152-1\} The string_expression or string_simple_expression, if any, of a raise_statement or raise_expression, is expected to be of type String.

\{AI12-0022-1\} \{AI12-0159-1\} The expected type for a raise_expression shall be any single type.

Dynamic Semantics

\{AI95-00361-01\} \{AI12-0022-1\} \{AI12-0152-1\} To raise an exception is to raise a new occurrence of that exception, as explained in 11.4. For the execution of a raise_statement with an exception_name, the named exception is raised. Similarly, for the evaluation of a raise_expression, the named exception is raised. [In both of these cases, if a string_expression or string_simple_expression is present, the expression is evaluated and its value is associated with the exception occurrence.] For the execution of a re-raise_statement, the exception occurrence that caused transfer of control to the innermost enclosing handler is raised again.

Proof: \{AI95-00361-01\} The definition of Exceptions.Exception_Message includes a statement that the string is returned (see 11.4.1). We describe the use of the string here so that we don’t have an unexplained parameter in this subclause.

Implementation Note: For a re-raise_statement, the implementation does not create a new Exception_Occurrence, but instead propagates the same Exception_Occurrence value. This allows the original cause of the exception to be determined.

Term entry: raise an exception — abandon normal program execution so as to draw attention to the fact that the corresponding situation has arisen

NOTE \{AI12-0062-1\} \{AI12-0152-1\} \{AI12-0159-1\} If the evaluation of a string_expression or string_simple_expression raises an exception, that exception is propagated instead of the one denoted by the exception_name of the raise_statement or raise_expression.

Examples of raise statements:

\{AI95-00433-01\} raise Ada.IO_Exceptions.Name_Error; -- see A.13
raise Queue_Error with "Buffer Full"; -- see 9.11
11.3 Raise Statements and Raise Expressions

raise

-- re-raise the current exception

{AI12-0312-1} -- For an example of a raise expression, see the Streams Subsystem definitions in 13.13.1.

Wording Changes from Ada 83

8.a The fact that the name in a raise_statement has to denote an exception is not clear from RM83. Clearly that was the intent, since the italicized part of the syntax rules so indicate, but there was no explicit rule. RM83-1.5(11) doesn't seem to give the italicized parts of the syntax any force.

Extensions to Ada 95

{AI95-00361-01} The syntax of a raise_statement is extended to include a string message. This is more convenient than calling Exceptions.Exception_Message (exception_name,Identity,string_expression), and should encourage the use of message strings when raising exceptions.

Extensions to Ada 2012

{AI12-0022-1} {AI12-0152-1} {AI12-0159-1} Corrigendum: The raise_expression is new. This construct is necessary to allow conversion of existing specifications to use preconditions and predicates without changing the exceptions raised. It is considered important enough to be added to Ada 2012 rather than waiting for Ada 2022.

11.4 Exception Handling

[When an exception occurrence is raised, normal program execution is abandoned and control is transferred to an applicable exception_handler, if any. To handle an exception occurrence is to respond to the exceptional event. To propagate an exception occurrence is to raise it again in another context; that is, to fail to respond to the exceptional event in the present context.]

1.a Ramification: In other words, if the execution of a given construct raises an exception, but does not handle it, the exception is propagated to an enclosing execution (except in the case of a task_body).

1.b/1 Propagation involves re-raising the same exception occurrence (assuming the implementation has not taken advantage of the Implementation Permission of 11.3). For example, calling an entry of an uncallable task raises Tasking_Error; this is not propagation.

Dynamic Semantics

Within a given task, if the execution of construct a is defined by this document to consist (in part) of the execution of construct b, then while b is executing, the execution of a is said to dynamically enclose the execution of b. The innermost dynamically enclosing execution of a given execution is the dynamically enclosing execution that started most recently.

2.a To be honest: If the execution of a dynamically encloses that of b, then we also say that the execution of b is included in the execution of a.

2.b Ramification: Examples: The execution of an if_statement dynamically encloses the evaluation of the condition after the if (during that evaluation). (Recall that “execution” includes both “elaboration” and “evaluation”, as well as other executions.) The evaluation of a function call dynamically encloses the execution of the sequence_of_statements of the function body (during that execution). Note that, due to recursion, several simultaneous executions of the same construct can be occurring at once during the execution of a particular task.

2.c Dynamically enclosing is not defined across task boundaries; a task's execution does not include the execution of any other tasks.

2.d Dynamically enclosing is only defined for executions that are occurring at a given moment in time; if an if_statement is currently executing the sequence_of_statements after then, then the evaluation of the condition is no longer dynamically enclosed by the execution of the if_statement (or anything else).

3 When an exception occurrence is raised by the execution of a given construct, the rest of the execution of that construct is abandoned; that is, any portions of the execution that have not yet taken place are not performed. The construct is first completed, and then left, as explained in 7.6.1. Then:

• If the construct is a task_body, the exception does not propagate further;

4.a Ramification: When an exception is raised by the execution of a task_body, there is no dynamically enclosing execution, so the exception does not propagate any further. If the exception occurred during the activation of the task,
Then the activator raises Tasking_Error, as explained in 9.2, “Task Execution - Task Activation”, but we don’t define that as propagation; it’s a special rule. Otherwise (the exception occurred during the execution of the handled_sequence_of_statements of the task), the task silently disappears. Thus, abnormal termination of tasks is not always considered to be an error.

- If the construct is the sequence_of_statements of a handled_sequence_of_statements that has a handler with a choice covering the exception, the occurrence is handled by that handler;
- Otherwise, the occurrence is propagated to the innermost dynamically enclosing execution, which means that the occurrence is raised again in that context.

To be honest: As shorthands, we refer to the propagation of an exception, and the propagation by a construct, if the execution of the construct propagates an exception occurrence.

When an occurrence is handled by a given handler, the choice_parameter_specification, if any, is first elaborated, which creates the choice parameter and initializes it to the occurrence. Then, the sequence_of_statements of the handler is executed; this execution replaces the abandoned portion of the execution of the sequence_of_statements.

Ramification: This “replacement” semantics implies that the handler can do pretty much anything the abandoned sequence could do; for example, in a function, the handler can execute a return_statement that applies to the function.

Ramification: The rules for exceptions raised in library units, main subprograms and partitions follow from the normal rules, plus the semantics of the environment task described in Clause 10 (for example, the environment task of a partition elaborates library units and calls the main subprogram). If an exception is propagated by the main subprogram, it is propagated to the environment task, which then terminates abnormally, causing the partition to terminate abnormally. Although abnormal termination of tasks is not necessarily an error, abnormal termination of a partition due to an exception is an error.

Term entry: handle an exception — perform some actions in response to the arising of an exception

NOTE Exceptions raised in a declarative_part of a body are not handled by the handlers of the handled_sequence_of_statements of that body.

11.4.1 The Package Exceptions

Static Semantics

The following language-defined library package exists:

```ada
package Ada.Exceptions is
    type Exception_Id is private;
    withpragma Preelaborable_Initialization(Exception_Id);
    Null_Id : constant Exception_Id;
    function Exception_Name(Id : Exception_Id) return String;
    function Wide Exception Name(Id : Exception_Id) return Wide String;
    function Wide Wide Exception_Name(Id : Exception_Id) return Wide_Wide String;
    procedure Raise_Exception(E : in Exception_Id;
        Message : in String := "");
    procedure Reraise_Occurrence(X : in Exception_Occurrence);
    
    type Exception_Occurrence is limited private;
    withpragma Preelaborable_Initialization(Exception_Occurrence);
    type Exception_Occurrence_Access is access all Exception_Occurrence;
    Null_Occurrence : constant Exception_Occurrence;
    procedure Raise_Exception(E : in Exception_Id;
        Message : in String := "");
    procedure Reraise_Occurrence(X : in Exception_Occurrence);
```

NOTE {AI12-0451-1} Exceptions raised in a declarative_part of a body are not handled by the handlers of the handled_sequence_of_statements of that body.
Each distinct exception is represented by a distinct value of type Exception_Id. Null_Id does not represent any exception, and is the default initial value of type Exception_Id. Each occurrence of an exception is represented by a value of type Exception_Occurrence. Null_Occurrence does not represent any exception occurrence, and is the default initial value of type Exception_Occurrence.

For a prefix $E$ that denotes an exception, the following attribute is defined:

$E$.Identity $E$.Identity returns the unique identity of the exception. The type of this attribute is Exception_Id.

**Ramification:** In a distributed program, the identity is unique across an entire program, not just across a single partition. Exception propagation works properly across RPCs. An exception can be propagated from one partition to another, and then back to the first, where its identity is known.

Raise_Exception raises a new occurrence of the identified exception. In this case Exception_Message returns the Message parameter of Raise_Exception. For a raise_statement with an exception_name, Exception_Message returns implementation-defined information about the exception occurrence. Reraise_Occurrence reraises the specified exception occurrence.

Exception Message returns the message associated with the given Exception Occurrence. For an occurrence raised by a call to Raise Exception, the message is the Message parameter passed to Raise Exception. For the occurrence raised by a raise_statement or raise_expression with an exception name and a string_expression or string simple_expression, the message is the string_expression or string simple_expression. For the occurrence raised by a raise_statement or raise_expression with an exception name and without a string_expression or string simple_expression, the message is a string giving implementation-defined information about the exception occurrence. For an occurrence originally raised in some other manner (including by the failure of a language-defined check), the message is an unspecified string. In all cases, Exception Message returns a string with lower bound 1.
Implementation defined: The information returned by Exception_Message.

Discussion: \{AI05-0043-1\} There is Implementation Advice about the contents of this string for language-defined checks.

Ramification: Given an exception E, the raise_statement:

\[ \text{raise } E; \]

is equivalent to this call to Raise_Exception:

\[ \text{Raise_Exception(E'Identity, Message => implementation-defined-string);} \]

\{AI95-00361-01\} Similarly, the raise_statement:

\[ \text{raise } E \text{ with } \text{"some information";} \]

is equivalent to this call to Raise_Exception:

\[ \text{Raise_Exception(E'Identity, Message => "some information");} \]

\{AI95-00361-01\} Reraise_Occurrence reraises the specified exception occurrence.

Ramification: The following handler:

\[ \text{when others =>} \]
\[ \text{Cleanup;} \]
\[ \text{raise;} \]

is equivalent to this one:

\[ \text{when X : others =>} \]
\[ \text{Cleanup;} \]
\[ \text{Reraise_Occurrence(X);} \]

Exception_Identity returns the identity of the exception of the occurrence.

\{AI95-00400-01\} The Wide_Wide_Exception_Name, Exception_Name functions return the full expanded name of the exception, in upper case, starting with a root library unit. For an exception declared immediately within package Standard, the defining_identifier is returned. The result is implementation defined if the exception is declared within an unnamed block_statement.

Ramification: See the Implementation Permission below.

To be honest: This name, as well as each prefix of it, does not denote a renaming_declaration.

Implementation defined: The result of Exceptions.Wide_Wide_Exception_Name, Exceptions.Exception_Name for exception types declared within an unnamed block_statement.

Ramification: Note that we're talking about the name of the exception, not the name of the occurrence.

\{AI95-00400-01\} The Exception_Name functions (respectively, Wide_Exception_Name) return the same sequence of graphic characters as that defined for Wide_Wide_Exception_Name, if all the graphic characters are defined in Character (respectively, Wide_Character); otherwise, the sequence of characters is implementation defined, but no shorter than that returned by Wide_Wide_Exception_Name for the same value of the argument.

Implementation defined: The sequence of characters of the value returned by Exceptions.Exception_Name (respectively, Exceptions.Wide_Exception_Name) when some of the graphic characters of Exceptions.Wide_Exception_Name are not defined in Character (respectively, Wide_Character).

\{AI95-00378-01\} \{AI95-00417-01\} The string returned by the Exception_Name, Wide_Exception_Name, and Wide_Wide_Exception_Name functions has lower bound 1.

\{AI95-00378-01\} Exception_Information returns implementation-defined information about the exception occurrence. The returned string has lower bound 1.

Implementation defined: The information returned by Exception_Information.

\{AI95-00241-01\} \{AI95-00446-01\} Raise_Exception and Reraise_Occurrence have no effect in the case of Null_Id or Null_Occurrence. Raise_Exception and Exception_Name raise Constraint_Error for a Null_Id. Exception_Message, Exception_Name, and Exception_Information raise Constraint_Error for a Null_Occurrence. Exception_Identity applied to Null_Occurrence returns Null_Id, Exception_Message,
Exception_Identity, Exception_Name, and Exception_Information raise Constraint_Error for a Null_Id or Null_Occurrence.

Ramification: AI95-00241-01 Null_Occurrence can be tested for by comparing Exception_Identity(Occurrence) to Null_Id.

Discussion: AI95-00446-01 Raise Exception was changed so that it always raises an exception and thus can be a No Return procedure. A similar change was not made for Reraise Occurrence, as doing so was determined to be a significant incompatibility. It is not unusual to pass an Exception Occurrence to other code to delay raising it. If there was no exception, passing Null Occurrence works fine (nothing is raised). Moreover, as there is no test for Null Occurrence in Ada 95, this is the only way to write such code without using additional flags. Breaking this sort of code is unacceptable.

The Save_Occurrence procedure copies the Source to the Target. The Save_Occurrence function uses an allocator of type Exception_Occurrence_Access to create a new object, copies the Source to this new object, and returns an access value designating this new object; [the result may be deallocated using an instance of Unchecked_Deallocation.]

Ramification: It's OK to pass Null Occurrence to the Save_Occurrence subprograms; they don't raise an exception, but simply save the Null Occurrence.

AI95-00438-01 Write Exception Occurrence writes a representation of an exception occurrence to a stream; Read Exception Occurrence reconstructs an exception occurrence from a stream (including one written in a different partition).

Ramification: AI12-0005-1 These routines are used to define the stream attributes (see 13.13.2) for Exception_Occurrence.

The identity of the exception, as well as the Exception_Name and Exception_Message, have to be preserved across partitions.

The string returned by Exception_Name or Exception_Message on the result of calling the Read attribute on a given stream has to be the same as the value returned by calling the corresponding function on the exception occurrence that was written into the stream with the Write attribute. The string returned by Exception_Information need not be the same, since it is implementation defined anyway.

Reason: This is important for supporting writing exception occurrences to external files for post-mortem analysis, as well as propagating exceptions across remote subprogram calls in a distributed system (see E.4).

Implementation Requirements

AI95-00438-01 The implementation of the Write attribute (see 13.13.2) of Exception_Occurrence shall support writing a representation of an exception occurrence to a stream; the implementation of the Read attribute of Exception_Occurrence shall support reconstructing an exception occurrence from a stream (including one written in a different partition).

Ramification: The identity of the exception, as well as the Exception_Name and Exception_Message, have to be preserved across partitions.

The string returned by Exception_Name or Exception_Message on the result of calling the Read attribute on a given stream has to be the same as the value returned by calling the corresponding function on the exception occurrence that was written into the stream with the Write attribute. The string returned by Exception_Information need not be the same, since it is implementation defined anyway.

Reason: This is important for supporting writing exception occurrences to external files for post-mortem analysis, as well as propagating exceptions across remote subprogram calls in a distributed system (see E.4).

Paragraph 16 was deleted.

Implementation Permissions

An implementation of Exception_Name in a space-constrained environment may return the defining_identifier instead of the full expanded name.
The string returned by Exception_Message may be truncated (to no less than 200 characters) by the Save_Occurrence procedure [not the function], the Reraise_Occurrence procedure, and the re-raise statement.

**Reason:** The reason for allowing truncation is to ease implementations. The reason for choosing the number 200 is that this is the minimum source line length that implementations have to support, and this feature seems vaguely related since it's usually a “one-liner”. Note that an implementation is allowed to do this truncation even if it supports arbitrarily long lines.

**Implementation Advice**

Exception_Message (by default) and Exception_Information should produce information useful for debugging. Exception_Message should be short (about one line), whereas Exception_Information can be long. Exception_Message should not include the Exception_Name. Exception_Information should include both the Exception_Name and the Exception_Message.

**Implementation Advice:** Exception_Information should provide information useful for debugging, and should include the Exception_Name and Exception_Message.

**Implementation Advice:** Exception_Message by default should be short, provide information useful for debugging, and should not include the Exception_Name.

**Reason:** It may seem strange to define two subprograms whose semantics is implementation defined. The idea is that a program can print out debugging/error-logging information in a portable way. The program is portable in the sense that it will work in any implementation; it might print out different information, but the presumption is that the information printed out is appropriate for debugging/error analysis on that system.

**Implementation Note:** As an example, Exception_Information might include information identifying the location where the exception occurred, and, for predefined exceptions, the specific kind of language-defined check that failed. There is an implementation trade-off here, between how much information is represented in an Exception_Occurrence, and how much can be passed through a re-raise.

The string returned should be in a form suitable for printing to an error log file. This means that it might need to contain line-termination control characters with implementation-defined I/O semantics. The string should neither start nor end with a newline.

If an implementation chooses to provide additional functionality related to exceptions and their occurrences, it should do so by providing one or more children of Ada.Exceptions.

Note that exceptions behave as if declared at library level; there is no “natural scope” for an exception; an exception always exists. Hence, there is no harm in saving an exception occurrence in a data structure, and re-raising it later. The re-raise has to occur as part of the same program execution, so saving an exception occurrence in a file, reading it back in from a different program execution, and then re-raising it is not required to work. This is similar to I/O of access types. Note that it is possible to use RPC to propagate exceptions across partitions.

Here's one way to implement Exception_Occurrence in the private part of the package. Using this method, an implementation need store only the actual number of characters in exception messages. If the user always uses small messages, then exception occurrences can be small. If the user never uses messages, then exception occurrences can be smaller still:

```ada
type Exception_Occurrence(Message_Length : Natural := 200) is
  limited record
  Id : Exception_Id;
  Message : String(1..Message_Length);
end record;
```

At the point where an exception is raised, an Exception_Occurrence can be allocated on the stack with exactly the right amount of space for the message — none for an empty message. This is just like declaring a constrained object of the type:

```ada
Temp : Exception_Occurrence(10); -- for a 10-character message
```

After finding the appropriate handler, the stack can be cut back, and the Temp copied to the right place. This is similar to returning an unknown-sized object from a function. It is not necessary to allocate the maximum possible size for every Exception_Occurrence. If, however, the user declares an Exception_Occurrence object, the discriminant will be permanently set to 200. The Save_Occurrence procedure would then truncate the Exception_Message. Thus, nothing is lost until the user tries to save the occurrence. If the user is willing to pay the cost of heap allocation, the Save_Occurrence function can be used instead.

Note that any arbitrary-sized implementation-defined Exception_Information can be handled in a similar way. For example, if the Exception_Occurrence includes a stack traceback, a discriminant can control the number of stack
frames stored. The traceback would be truncated or entirely deleted by the Save_Occurrence procedure — as the implementation sees fit.

If the internal representation involves pointers to data structures that might disappear, it would behoove the implementation to implement it as a controlled type, so that assignment can either copy the data structures or else null out the pointers. Alternatively, if the data structures being pointed at are in a task control block, the implementation could keep a unique sequence number for each task, so it could tell when a task's data structures no longer exist.

Using the above method, heap space is never allocated unless the user calls the Save_Occurrence function.

An alternative implementation would be to store the message strings on the heap when the exception is raised. (It could be the global heap, or it could be a special heap just for this purpose — it doesn't matter.) This representation would be used only for choice parameters. For normal user-defined exception occurrences, the Save_Occurrence procedure would copy the message string into the occurrence itself, truncating as necessary. Thus, in this implementation, Exception_Occurrence would be implemented as a variant record:

```ada
type Exception_Occurrence_Kind is (Normal, As_Choice_Param);

type Exception_Occurrence(Kind : Exception_Occurrence_Kind := Normal) is
  limited record
  case Kind is
    when Normal =>
      . . . -- space for 200 characters
    when As_Choice_Param =>
      . . . -- pointer to heap string
  end case;
end record;
```

Exception_Occurrences created by the run-time system during exception raising would be As_Choice_Param. User-declared ones would be Normal — the user cannot see the discriminant, and so cannot set it to As_Choice_Param. The strings in the heap would be freed upon completion of the handler.

This alternative implementation corresponds to a heap-based implementation of functions returning unknown-sized results.

One possible implementation of Reraise_Occurrence is as follows:

```ada
procedure Reraise_Occurrence(X : in Exception_Occurrence) is
begin
  Raise_Exception(Identity(X), Exception_Message(X));
end Reraise_Occurrence;
```

However, some implementations may wish to retain more information across a re-raise — a stack traceback, for example.

**Ramification:** Note that Exception_Occurrence is a definite subtype. Hence, values of type Exception_Occurrence may be written to an error log for later analysis, or may be passed to subprograms for immediate error analysis.

This paragraph was deleted. Implementation Note: If an implementation chooses to have a mode in which it supports non-Latin-1 characters in identifiers, then it needs to define what the above functions return in the case where the name of an exception contains such a character.

NOTE UTF-8 encoding (see A.4.11) can be used to represent non-ASCII characters in exception messages.

Extensions to Ada 83

The Identity attribute of exceptions is new, as is the package Exceptions.

**Inconsistencies With Ada 95**

**Amendment Correction:** Exception_Identity of an Exception_Occurrence now is defined to return Null_Id for Null_Occurrence, rather than raising Constraint_Error. This provides a simple way to test for Null_Occurrence. We expect that programs that need Constraint_Error raised will be very rare; they can be easily fixed by explicitly testing for Null_Id or by using Exception_Name instead.

**Amendment Correction:** We now define the lower bound of the string returned from [Wide_Wide_]Exception_Name, Exception_Message, and Exception_Information. This makes working with the returned string easier, and is consistent with many other string-returning functions in Ada. This is technically an inconsistency: if a program depended on some other lower bound for the string returned from one of these functions, it could fail when compiled with Ada 2005. Such code is not portable even between Ada 95 implementations, so it should be very rare.

**Amendment Correction:** Raise_Exception now raises Constraint_Error if passed Null_Id. This means that it always raises an exception, and thus we can apply pragma No_Return to it. We expect that programs that call Raise_Exception with Null_Id will be rare, and programs that do that and expect no exception to be raised will be rarer; such programs can be easily fixed by explicitly testing for Null_Id before calling Raise_Exception.
Incompatibilities With Ada 95

- AI95-00400-01, AI95-00438-01, AI05-0005-1: Functions `Wide_Exception_Name` and `Write_Exception_Occurrence` are newly added to Exceptions. If Exceptions is referenced in a `use_clause`, and an entity `E` with the same `defining_identifier` as a new entity in Exceptions is defined in a package that is also referenced in a `use_clause`, the entity `E` may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 95

- AI95-00362-01: The package Exceptions is preelaborated, and types `Exception_Id` and `Exception_Occurrence` have preelaborable initialization, allowing this package to be used in preelaborated units.

Wording Changes from Ada 95

- AI95-00361-01: The meaning of `Exception_Message` is reworded to reflect that the string can come from a `raise_statement` as well as a call of `Raise_Exception`.

- AI95-00400-01: Added `Wide_Exception_Name` and `Wide_Wide_Exception_Name` because identifiers can now contain characters outside of Latin-1.

Wording Changes from Ada 2005

- AI05-0043-1: Correction: Added explicit wording that the exception message for language-defined checks is unspecified. The old wording appeared inclusive, but it was not.

11.4.2 Pragmas Assert and Assertion_Policy

- AI95-00286-01, AI05-0274-1: Pragma `Assert` is used to assert the truth of a boolean expression at any point within a sequence of declarations or statements. Pragma `Assertion_Policy` is used to control whether such assertions are to be ignored by the implementation, checked at run time, or handled in some implementation-defined manner.

- AI05-0274-1, AI12-0265-1: Assert pragmas, subtype predicates (see 3.2.4), preconditions and postconditions (see 6.1.1), and type invariants (see 7.3.2), and default initial conditions (see 7.3.3) are collectively referred to as assertions; their boolean expressions are referred to as assertion expressions.

**Term entry: assertion** — boolean expression that is expected to be True at run time at certain specified places

**Note:** Certain pragmas and aspects define various kinds of assertions.

- AI05-0274-1: Pragma `Assertion_Policy` is used to control whether assertions are to be ignored by the implementation, checked at run time, or handled in some implementation-defined manner.

**Syntax**

- AI95-00286-01: The form of a `pragma Assert` is as follows:

```
pragma Assert([Check =>] boolean_expression[, [Message =>] string_expression]);
```

A `pragma Assert` is allowed at the place where a declarative item or a statement is allowed.

- AI95-00286-01: The form of a `pragma Assertion_Policy` is as follows:

```
pragma Assertion_Policy(policy_identifier);
```

- AI05-0290-1: `pragma Assertion_Policy` is allowed only immediately within a declarative_part, immediately within a package_specification, or as a configuration pragma.
Name Resolution Rules

8/2 \{AI95-00286-01\} The expected type for the boolean expression of a pragma Assert is any boolean type.
The expected type for the string expression of a pragma Assert is type String.

8.a/2 Reason: We allow any boolean type to be like if_statements and other conditionals; we only allow String for the
message in order to match raise_statements.

Legality Rules

9/5 \{AI95-00286-01\} \{AI05-0290-1\} \{AI12-0265-1\} \{AI12-0396-1\} The assertion aspect mark of a
pragma Assertion_Policy shall identify an assertion aspect, namely be one of Assert, Static_Predicate,
Dynamic_Predicate, Pre, Pre'Class, Post, Post'Class, Type_Invariant, Type_Invariant'Class,
Default Initial Condition, or some implementation-defined (assertion) implementation-defined aspect mark. The policy identifier of a pragma Assertion_Policy shall be either Check, Ignore, or
some implementation-defined identifier.

9.a/3 Implementation defined: Implementation-defined policy identifiers and assertion aspect marks allowed in a
pragma Assertion_Policy.

9.b/5 To be honest: \{AI12-0396-1\} “Assert” is considered an “assertion aspect” for the purposes of this rule, even though
there is no sort of entity that has an Assert aspect. It can only be specified using an Assert pragma, and applies to a
particular point in the execution of a logical thread of control.

Static Semantics

10/3 \{AI95-00286-01\} \{AI05-0290-1\} A pragma Assertion_Policy determines for each assertion aspect
named in the pragma argument associations whether assertions of the given aspect are to be enforced
by a runtime check. The policy identifier Check requires that assertion expressions of the given aspect be
checked that they evaluate to True at the points specified for the given aspect; the policy identifier Ignore
requires that the assertion expression not be evaluated at these points, and the runtime checks not be
performed. [Note that for subtype predicate aspects (see 3.2.4), even when the applicable Assertion Policy is Ignore, the predicate will still be evaluated as part of membership tests and Valid
attribute references, and if static, will still have an effect on loop iteration over the subtype, and the selection of case_statement_alternatives and variants.]
A configuration pragma that specifies the assertion policy in effect for the compilation units to which it applies. Different policies may apply to
different compilation units within the same partition. The default assertion policy is implementation-defined.

10.1/3 \{AI05-0290-1\} If no assertion aspect marks are specified in the pragma, the specified policy applies to
all assertion aspects.

10.2/5 \{AI05-0290-1\} \{AI12-0396-1\} A pragma Assertion_Policy applies to the named assertion aspects in a
specific region, and applies to all assertion expressions associated with those aspects specified in that
region. A pragma Assertion_Policy given in a declarative part or immediately within a
package_specification applies from the place of the pragma to the end of the innermost enclosing
declarative region. The region for a pragma Assertion_Policy given as a configuration pragma is the
declarative region for the entire compilation unit (or units) to which it applies.

10.3/3 \{AI05-0290-1\} If a pragma Assertion_Policy applies to a generic instantiation, then the pragma
Assertion_Policy applies to the entire instance.

10.4/3 \{AI05-0290-1\} If multiple Assertion_Policy pragmas apply to a given construct for a given assertion
aspect, the assertion policy is determined by the one in the innermost enclosing region of a pragma
Assertion_Policy specifying a policy for the assertion aspect. If no such Assertion_Policy pragma exists, the policy is implementation defined.

Implementation defined: The default assertion policy.

{AI95-00286-01} The following language-defined library package exists:

{AI12-0414-1} package Ada.Assertions is
    withpragma Pure is Ada.Assertions;
    Assertion_Error: exception;
    procedure Assert(Check: in Boolean);  
    procedure Assert(Check: in Boolean; Message: in String);
end Ada.Assertions;

{AI95-00286-01} {AI05-0290-1} A compilation unit containing a check for an assertion (including a pragma Assert) has a semantic dependence on the Assertions library unit.

This paragraph was deleted. {AI95-00286-01} {AI05-0290-1} The assertion policy that applies to a generic unit also applies to all its instances.

Dynamic Semantics

{AI95-00286-01} {AI05-0290-1} An assertion policy specifies how a pragma Assert is interpreted by the implementation. If the assertion policy is Ignore at the point of a pragma Assert, the pragma is ignored. If performing checks is required by the Assert assertion policy in effect at the place point of a pragma Assert, the elaboration of the pragma consists of evaluating the boolean expression, and if the result is False, evaluating the Message argument, if any, and raising the exception Assertions.Assertion_Error, with a message if the Message argument is provided.

{AI95-00286-01} Calling the procedure Assertions.Assert without a Message parameter is equivalent to:

    if Check = False then
        raise Ada.Assertions.Assertion_Error;
    end if;

{AI95-00286-01} Calling the procedure Assertions.Assert with a Message parameter is equivalent to:

    if Check = False then
        raise Ada.Assertions.Assertion_Error with Message;
    end if;

{AI95-00286-01} The procedures Assertions.Assert have these effects independently of the assertion policy in effect.

Bounded (Run-Time) Errors

{AI05-0274-1} {AI12-0439-1} It is a bounded error to invoke a potentially blocking operation (see 9.5.1) during the evaluation of an assertion expression associated with a call on, or return from, a protected operation. If the bounded error is detected, Program_Error is raised. If not detected, execution proceeds normally, but if it is invoked within a protected action, it can might result in deadlock or a (nested) protected action.

Implementation Requirements

{AI12-0179-1} {AI12-0265-1} Any postcondition expression, type invariant expression, or default initial condition expression occurring in the specification of a language-defined unit is enabled (see 6.1.1, 7.3.2, and 7.3.3).

Ramification: The Assertion_Policy does not have an effect on such postconditions, invariants, and default initial conditions. This has no execution impact since such assertions shouldn’t fail anyway (see the next rule).
The evaluation of any such postcondition, type invariant, or default initial condition expression shall either yield True or propagate an exception from a raise expression that appears within the assertion expression.

Ramification: In other words, evaluating such an assertion expression will not return a result of False, nor will it propagate an exception other than by evaluating a raise_expression which is syntactically all or part of the assertion expression.

To be honest: Evaluation of any expression might raise Storage_Error.

Reason: This allows the Reference Manual to express semantic requirements as postconditions, invariants, or default initial conditions (which are invariably clearer than English prose would be) while keeping it clear that failing the assertion check (or any other run time check) is not conforming behavior.

Any precondition expression occurring in the specification of a language-defined unit is enabled (see 6.1.1) unless suppressed (see 11.5). Similarly, any predicate checks for a subtype occurring in the specification of a language-defined unit are enabled (see 3.2.4) unless suppressed.

Reason: This allows the Reference Manual to express runtime requirements on the client of a language-defined unit as preconditions or predicates (which are clearer than English prose would be). Some such requirements can be suppressed with pragma Suppress. Ada 2012 and earlier versions did not provide a mechanism to suppress such code.

Assertion_Error may be declared by renaming an implementation-defined exception from another package.

Reason: This permission is intended to allow implementations which had an implementation-defined Assert pragma to continue to use their originally defined exception. Without this permission, such an implementation would be incorrect, as Exception_Name would return the wrong name.

Implementations may define their own assertion policies.

If the result of a function call in an assertion is not used, it is permitted to omit the function call. [This permission applies even if the function has side effects.]

An implementation may disallow the specification of an assertion expression if the evaluation of the expression has a side effect such that an immediate reevaluation of the expression can produce a different value. Similarly, an implementation may disallow the specification of an assertion expression that is checked as part of a call on or return from a callable entity C if the evaluation of the expression has a side effect such that the evaluation of some other assertion expression associated with the same call of (or return from) C can produce a different value than it would if the first expression had not been evaluated.

Ramification: This allows an implementation to reject such assertions. To maximize portability, assertions should not include expressions that contain these sorts of side effects.

Discussion: The intended effect of the second part of the rule (the part starting with “Similarly”) is that an evaluation of the involved assertion expressions (subtype predicates, type invariants, preconditions and postconditions) in any order yields identical results.

The rule is intended to apply to all of the assertion expressions that are evaluated at the start of call (and similarly for the assertion expressions that are evaluated during the return from a call), but not other assertions actually given in the body, nor between the assertions checked at the start and end of the call. Specifically, a side effect that alters a variable in a function called from a precondition expression that changes the result of a postcondition expression of the same subprogram does not trigger these rules unless it also changes the value of a reevaluation of the precondition expression.

Language Design Principles

Our intent is that any assertion expression that violates this Implementation Permission is considered pathological. We definitely want compilers to be able to assume that if you evaluate an assertion expression once and it is True, you don't need to evaluate it again if all you are doing in the meantime is evaluating assertion expressions. We
were unable to find wording that had this effect that didn't throw out important other cases (logging, memo functions), so we settled for a strong warning that compilers can reject such pathologies. Perhaps in a future version of Ada we'll be able to tighten this up.

NOTE {AI95-00286-01} {AI12-0442-1} {AI12-0447-1} Normally, the boolean expression in a pragma Assert should not call functions that have significant side effects when the result of the expression is True, so that the particular assertion policy in effect will not affect normal operation of the program.

Extensions to Ada 95

{AI95-00286-01} Pragmas Assert and Assertion_Policy, and package Assertions are new.

Incompatibilities With Ada 2005

{AI05-0274-1} There now is an Implementation Permission to reject an assertion expression that calls a function that has a side effect such that an immediate reevaluation of the expression could produce a different value. This means that a pragma Assert that works in Ada 2005 might be illegal in Ada 2012 in the unlikely event that the compiler detected such an error. This should be unlikely to occur in practice and it is considered a good thing, as the original expression was tricky and probably was not portable (as order of evaluation is unspecified within an expression). Moreover, no compiler is required to reject such expressions, so there is no need for any compiler to change behavior.

Extensions to Ada 2005

{AI12-0290-1} Assertion_Policy pragmas are now allowed in more places and can specify behavior for individual kinds of assertions.

Wording Changes from Ada 2012

{AI12-0112-1} Added wording that preconditions and predicates given on language-defined units are always checked unless suppressed (that is, they act like language-defined checks). This is not considered an inconsistency, since there are no such preconditions or predicates in Ada 2012.

{AI12-0265-1} Correction: Added wording that postconditions, type invariants, and default initial conditions given on language-defined units cannot fail. This is not considered an inconsistency, since there are no such postconditions, invariants, or default initial conditions in Ada 2012.

{AI12-0265-1} Added default initial conditions to the kinds of assertions (see 7.3.3).

{AI12-0396-1} Correction: Added a definition of assertion aspects, used in some freezing rules (see 13.14).

11.4.3 Example of Exception Handling

Examples

{AI12-0440-1} Exception handling can be used to separate the detection of an error from the response to that error:

```ada
package File_System is
  type Data_Type is ...;
  type File_Handle is limited private;
  File_Not_Found : exception;
  procedure Open(F : in out File_Handle; Name : String);
    -- raises File_Not_Found if named file does not exist
  End_Of_File : exception;
  procedure Read(F : in out File_Handle; Data : out Data_Type);
    -- raises End_Of_File if the file is not open
private
  ...;
end File_System;

Reason: {AI12-0178-1} The first ... provides a place for Close to be declared, and the second ... provides a place for File_Handle to be completed.
```

{AI12-0178-1} package_body File_System is
  ...;
```
Reason: {AI12-0178-1} This ... provides a place for File_Exists and the body of Close to be declared.

{AI95-00433-01} {AI12-0178-1} package_body File_System is
procedures

procedure Open(F : in out File_Handle; Name : String) is
begin
    if File_Exists(Name) then
        ...
    else
        raise Exceptions.Raise_Exception(File_Not_Found with "Identity,
                "File not found: " & Name & ".");
    end if;
end Open;

procedure Read(F : in out File_Handle; Data : out Data_Type) is
begin
    if F.Current_Position <= F.Last_Position then
        ...
    else
        raise End_Of_File;
    end if;
end Read;

end File_System;

{AI12-0178-1} with Ada.Text_IO;
with Ada.Exceptions;
with File_System;
use File_System;
use Ada;

procedure Main is
    Verbosity_Desired : Boolean := ...;
begin
    ... -- call operations in File_System
exception
    when End_Of_File =>
        Close(Some_File);
    when Not_Found_Error : File_Not_Found =>
        Text_IO.Put_Line(Exceptions.Exception_Message(Not_Found_Error));
    when The_Error : others =>
        Text_IO.Put_Line("Unknown error:");
        if Verbosity_Desired then
            Text_IO.Put_Line(Exceptions.Exception_Information(The_Error));
        else
            Text_IO.Put_Line(Exceptions.Exception_Name(The_Error));
            Text_IO.Put_Line(Exceptions.Exception_Message(The_Error));
        end if;
        raise;
end Main;

{AI12-00440-1} In the above example, the File_System package contains information about detecting
certain exceptional situations, but it does not specify how to handle those situations. Procedure Main
specifies how to handle them; other clients of File_System can have different handlers, even though
the exceptional situations arise from the same basic causes.

Wording Changes from Ada 83

11.5 Suppressing Checks

{AI95-00224-01} Checking pragmas give instructions to an implementation on handling language-
defined checks. A pragma Suppress gives permission to an implementation to omit certain language-
defined checks, while a pragma Unsuppress revokes the permission to omit checks.
Term entry: suppress a check — assert that the check cannot fail, and request that the compiler optimize by disabling the check.

Note: The compiler is not required to honor this request. Suppressing checks that can fail can cause a program to behave in arbitrary ways.

A language-defined check (or simply, a “check”) is one of the situations defined by this document that requires a check to be made at run time to determine whether some condition is true. A check fails when the condition being checked is False, causing an exception to be raised.

Discussion: All such checks are defined under “Dynamic Semantics” in clauses and subclauses throughout the standard.

Term entry: check — test made during execution to determine whether a language rule has been violated.

Syntax

The forms of checking pragmas are as follows:

- **pragma Suppress**(identifier[, On => name]);
- **pragma Unsuppress**(identifier);
- **pragma Suppress** is allowed only immediately within a declarative_part, immediately within a package_specification, or as a configuration pragma.

Legality Rules

The identifier shall be the name of a check. The name (if present) shall statically denote some entity.

This paragraph was deleted.

For a **pragma Suppress** that is immediately within a package_specification and includes a name, the name shall denote an entity (or several overloaded subprograms) declared immediately within the package_specification.

Static Semantics

A checking pragma applies to the named check in a specific region, and applies to all entities in that region. A checking pragma given in a declarative_part or immediately within a package_specification applies from the place of the pragma to the end of the innermost enclosing declarative region. The region for a checking pragma given as a configuration pragma is the declarative region for the entire compilation unit (or units) to which it applies.

If a checking pragma applies to a generic instantiation, then the checking pragma also applies to the entire instance.

If a checking pragma applies to a call to a subprogram that has a **pragma Inline** applied to it, then the checking pragma also applies to the inlined subprogram body.

Ramification: This means that a Suppress pragma that occurs in a scope enclosing the declaration of a generic unit but not also enclosing the declaration of a given instance of that generic unit will not apply to constructs within the given instance.

A **pragma Suppress** gives permission to an implementation to omit the named check (or every check in the case of All_Checks) for any entities to which it applies, from the place of the pragma to the end of the innermost enclosing declarative region, or, if the pragma is given in a package_specification and includes a name, to the end of the scope of the named entity. If the pragma includes a name, the permission applies only to checks performed on the named entity, or, for a subtype, on objects and values of its type. Otherwise, the permission applies to all entities. If permission has been given to suppress a given check, the check is said to be suppressed.

Ramification: A check is suppressed even if the implementation chooses not to actually generate better code. This allows the implementation to raise Program_Error, for example, if the erroneousness is detected.
A `pragma Unsuppress` revokes the permission to omit the named check (or every check in the case of All_Checks) given by any `pragma Suppress` that applies at the point of the `pragma Unsuppress`. The permission is revoked for the region to which the `pragma Unsuppress` applies. If there is no such permission at the point of a `pragma Unsuppress`, then the `pragma` has no effect. A later `pragma Suppress` can renew the permission.

The following are the language-defined checks:

- **Access_Check**
  - When evaluating a dereference (explicit or implicit), check that the value of the name is not null. When converting to a subtype that excludes null, check that the converted value is not null. When passing an actual parameter to a formal access parameter, check that the value of the actual parameter is not null. When evaluating a discriminant association for an access discriminant, check that the value of the discriminant is not null.

- **Discriminant_Check**
  - Check that the discriminants of a composite value have the values imposed by a discriminant constraint. Also, when accessing a record component, check that it exists for the current discriminant values.

- **Division_Check**
  - Check that the second operand is not zero for the operations /, rem, and mod.

- **Index_Check**
  - Check that the bounds of an array value are equal to the corresponding bounds of an index constraint. Also, when accessing a component of an array object, check for each dimension that the given index value belongs to the range defined by the bounds of the array object. Also, when accessing a slice of an array object, check that the given discrete range is compatible with the range defined by the bounds of the array object.

- **Length_Check**
  - Check that two arrays have matching components, in the case of array subtype conversions, and logical operators for arrays of boolean components.

- **Overflow_Check**
  - Check that a scalar value is within the base range of its type, in cases where the implementation chooses to raise an exception instead of returning the correct mathematical result.

- **Range_Check**
  - Check that a scalar value satisfies a range constraint. Also, for the elaboration of a subtype indication, check that the constraint (if present) is compatible with the subtype denoted by the subtype mark. Also, for an aggregate, check that an index or discriminant value belongs to the corresponding subtype. Also, check that when the result of an operation yields an array, the value of each component belongs to the component subtype. Also, for the attributes Value, Wide_Value, and Wide_Wide_Value, check that the given string has the appropriate syntax and value for the base subtype of the prefix of the attribute reference.

- **Tag_Check**
  - Check that operand tags in a dispatching call are all equal. Check for the correct tag on tagged type conversions, for an assignment_statement, and when returning a tagged limited object from a function.

- **Constraint_Error**
  - When converting to a subtype that excludes null, check that the converted value is not null. When passing an actual parameter to a formal access parameter, check that the value of the actual parameter is not null. When evaluating a discriminant association for an access discriminant, check that the value of the discriminant is not null.
\{AI95-00280\} **Accessibility Check**  
Check the accessibility level of an entity or view.

\{AI95-00280\} **Allocation Check**  
For an allocator, check that the master of any tasks to be created by the allocator is not yet completed or some dependents have not yet terminated, and that the finalization of the collection has not started.

**Elaboration Check**  
When a subprogram or protected entry is called, a task activation is accomplished, or a generic instantiation is elaborated, check that the body of the corresponding unit has already been elaborated.

\{AI95-00280\} \{AI12-0309-1\} **Program Error Check**  
Other language-defined checks that raise Program_Error: that subtypes with predicates are not used to index an array in a generic unit; that the maximum number of chunks is greater than zero; that the default value of an out parameter is convertible; that there is no misuse of functions in a generic with a class-wide actual type; that there are not colliding External_Tag values; that there is no misuse of operations of unchecked union types.  
**Accessibility Check** — Check the accessibility level of an entity or view.

\{AI12-0309-1\} [The following check corresponds to situations in which the exception Storage_Error is raised upon failure of a language-defined check.]

**Storage Check**  
Check that evaluation of an allocator does not require more space than is available for a storage pool. Check that the space available for a task or subprogram has not been exceeded.

**Reason:** We considered splitting this out into three categories: Pool Check (for allocators), Stack Check (for stack usage), and Heap Check (for implicit use of the heap — use of the heap other than through an allocator). Storage Check would then represent the union of these three. However, there seems to be no compelling reason to do this, given that it is not feasible to split Storage_Error.

- \{AI12-0309-1\} [The following check corresponds to situations in which the exception Tasking_Error is raised upon failure of a language-defined check.]

- \{AI12-0112-1\} \{AI12-0311-1\} [The following checks correspond to situations in which the exception Assertion_Error is raised upon failure of a language-defined check:] For a language-defined unit $U$ associated with one of these checks in the list below, the check refers to performance of checks associated with the Pre, StaticPredicate, and DynamicPredicate aspects associated with any entity declared in a descendant of $U$, or in an instance of a generic unit which is, or is declared in, a descendant of $U$. Each check is associated with one or more units:

\{AI12-0311-1\} **Calendar Assertion Check**  
Calendar.

\{AI12-0311-1\} **Characters Assertion Check**  
Characters, Wide_Characters, and Wide_Wide_Characters.

\{AI12-0112-1\} \{AI12-0311-1\} **Containers Assertion Check**  
Containers.

\{AI12-0311-1\} **Interfaces Assertion Check**  
Interfaces.
11.5 Suppressing Checks

### Ramification:

Any unit $U$ is a descendant of itself.

### Reason:

One could use pragma Assertion_Policy to eliminate such checks, but that would require recompiling the language-defined packages (the assertion policy that determines whether the assertion checks are made is that used to compile the unit). In addition, we do not want to specify the behavior of language-defined operations if the precondition fails; that is different than the usual behavior of Assertion_Policy. By using Suppress for this purpose, we make it clear that a failed check that is suppressed means erroneous execution.

### To be honest:

The preceding rule about an instance of a generic where the generic is declared in $U$ really extends recursively to handle the case of a generic package $G1$ which declares another generic package $G1.G2$, which declares another generic package $G1.G2.G3$, and so on. So if $G1$ is declared in some predefined unit $U$ then, for purposes of defining these checks, Some_Instance_Of_G1.G2 is also considered to be declared in $U$.

### Discussion:

We don’t want to say that assertions are suppressed, because we don’t want the potential failure of an assertion to cause erroneous execution (see below). Thus they are excluded from the suppression part of the above rule and then handled with an implicit Ignore policy.

### Erroneous Execution

If a given check has been suppressed, and the corresponding error situation occurs, the execution of the program is erroneous. Similarly, if a precondition check has been suppressed and the evaluation of the precondition would have raised an exception, execution is erroneous.

### Implementation Permissions

An implementation is allowed to place restrictions on checking pragmas, subject only to the requirement that pragma Unsuppress shall allow any check names supported by pragma Suppress pragmas. An implementation is allowed to add additional check names, with implementation-defined semantics. When Overflow_Check has been suppressed, an implementation may also suppress an unspecified subset of the Range_Checks.
This paragraph was deleted. **Reason:** {AI95-00224-01} The permission to restrict is given so the implementation can give an error message when the requested suppression is nonsense, such as suppressing a Range_Check on a task type. It would be verbose and pointless to list all the cases of nonsensical language-defined checks in the standard, and since the list of checks is open ended, we can’t list the restrictions for implementation-defined checks anyway.

**Implementation defined:** Implementation-defined check names.

**Discussion:** For Overflow_Check, the intention is that the implementation will suppress any Range_Checks that are implemented in the same manner as Overflow_Checks (unless they are free).

{AI95-00224-01} An implementation may support an additional parameter on **pragma Unsuppress** similar to the one allowed for **pragma Suppress** (see J.10). The meaning of such a parameter is implementation-defined.

**Implementation defined:** Existence and meaning of second parameter of **pragma Unsuppress**.

**Implementation Advice**

The implementation should minimize the code executed for checks that have been suppressed.

**Implementation Advice:** Code executed for checks that have been suppressed should be minimized.

**Implementation Note:** However, if a given check comes for free (for example, the hardware automatically performs the check in parallel with doing useful work) or nearly free (for example, the check is a tiny portion of an expensive run-time system call), the implementation should not bother to suppress the check. Similarly, if the implementation detects the failure at compile time and provides a warning message, there is no need to actually suppress the check.

**NOTE 1** {AI12-0442-1} There is no guarantee that a suppressed check is actually removed; hence a **pragma Suppress** is useful only to improve should be used only for efficiency reasons.

**NOTE 2** {AI95-00224-01} It is possible to give both a **pragma Suppress** and Unsuppress for the same check immediately within the same declarative part. In that case, the last **pragma** given determines whether or not the check is suppressed. Similarly, it is possible to resuppress a check which has been unsuppressed by giving a **pragma Suppress** in an inner declarative region.

**Examples**

{AI95-00224-01} Examples of suppressing and unsuppressing checks:

`pragma Suppress(Index_Check);`  
`pragma Unsuppress(Overflow_Check);Range_Check);`  
`pragma Suppress(Index_Check, On => Table);`

**Extensions to Ada 83**

A **pragma Suppress** is allowed as a configuration pragma. A **pragma Suppress** without a name is allowed in a **package_specification**.

Additional check names are added. We allow implementations to define their own checks.

**Wording Changes from Ada 83**

We define the checks in a distributed manner. Therefore, the long list of what checks apply to what is merely a NOTE.

We have removed the detailed rules about what is allowed in a **pragma Suppress**, and allow implementations to invent their own. The RM83 rules weren’t quite right, and such a change is necessary anyway in the presence of implementation-defined checks.

We make it clear that the difference between a Range_Check and an Overflow_Check is fuzzy. This was true in Ada 83, given RM83-11.6, but it was not clear. We considered removing Overflow_Check from the language or making it obsolete, just as we did for Numeric_Error. However, we kept it for upward compatibility, and because it may be useful on machines where range checking costs more than overflow checking, but overflow checking still costs something. Different compilers will suppress different checks when asked to suppress Overflow_Check — the nonuniformity in this case is not harmful, and removing it would have a serious impact on optimizers.

Under Access_Check, dereferences cover the cases of **selected_component**, **indexed_component**, slice, and attribute that are listed in RM83, as well as the new **explicit_dereference**, which was included in selected_component in RM83.

**Extensions to Ada 95**

{AI95-00224-01} **Pragma Unsuppress** is new.
11.5 Suppressing Checks

11.6 Exceptions and Optimization

[AI05-0299-1] The effect of a checking pragma no longer applies inside an inlined subprogram body. While this could change the behavior of a program that depends on a check being suppressed in an inlined body, such a program is erroneous and thus no behavior can be depended upon anyway. It's also likely to be very rare. We make this change so that inlining has no effect on the meaning of the subprogram body (since inlining is never required), this is necessary in order to be able to reason about the body), and so that assertion policies and suppress work the same way for inlining.

Wording Changes from Ada 2012

31.a/5 [AI12-0244-1] Correction: Range_Check is defined to include checks associated with the Value and related attributes.

11.6 Exceptions and Optimization

[AI05-0299-1] [ This subclause gives permission to the implementation to perform certain “optimizations” that do not necessarily preserve the canonical semantics.]

Dynamic Semantics

2/3 [AI05-0299-1] The rest of this Reference Manual (outside this subclause) defines the canonical semantics of the language. [The canonical semantics of a given (legal) program determines a set of possible external effects that can result from the execution of the program with given inputs.]

2.a Ramification: Note that the canonical semantics is a set of possible behaviors, since some reordering, parallelism, and nondeterminism is allowed by the canonical semantics.

2.b/3 Discussion: [AI05-0299-1] The following parts of the canonical semantics are of particular interest to the reader of this subclause:

2.c Behavior in the presence of abnormal objects and objects with invalid representations (see 13.9.1).

2.d Various actions that are defined to occur in an arbitrary order.

2.e Behavior in the presence of a misuse of Unchecked_Deallocation, Unchecked_Access, or imported or exported entity (see Clause 13).

3/3 [AI05-0299-1] [As explained in 1.1.3, “Conformity of an Implementation”, the external effect of a program is defined in terms of its interactions with its external environment. Hence, the implementation can perform any internal actions whatsoever, in any order or in parallel, so long as the external effect of
the execution of the program is one that is allowed by the canonical semantics, or by the rules of this
subclauseclause.]

**Ramification:** Note that an optimization can change the external effect of the program, so long as the changed external
effect is an external effect that is allowed by the semantics. Note that the canonical semantics of an erroneous
execution allows any external effect whatsoever. Hence, if the implementation can prove that program execution will
be erroneous in certain circumstances, there need not be any constraints on the machine code executed in those
circumstances.

*Implementation Permissions*

The following additional permissions are granted to the implementation:

- **{AI12-0444-1}** An implementation can omit raising need not always raise an exception when a
language-defined check fails. Instead, the operation that failed the check can simply yield an
undefined result. The exception is required to be raised by the implementation only if, in the
absence of raising it, the value of this undefined result would have some effect on the external
interactions of the program. In determining this, the implementation shall not presume that an
undefined result has a value that belongs to its subtype, nor even to the base range of its type, if
scalar. [Having removed the raise of the exception, the canonical semantics will in general allow
the implementation to omit the code for the check, and some or all of the operation itself.]

**Ramification:** Even without this permission, an implementation can always remove a check if it cannot possibly fail.

**Reason:** We express the permission in terms of removing the raise, rather than the operation or the check, as it
minimizes the disturbance to the canonical semantics (thereby simplifying reasoning). By allowing the implementation
to omit the raise, it thereby does not need to "look" at what happens in the exception handler to decide whether the
optimization is allowed.

**Discussion:** The implementation can also omit checks if they cannot possibly fail, or if they could only fail in
erroreneous executions. This follows from the canonical semantics.

**Implementation Note:** This permission is intended to allow normal "dead code removal" optimizations, even if some
of the removed code might have failed some language-defined check. However, one may not eliminate the raise of an
exception if subsequent code presumes in some way that the check succeeded. For example:

```ada
if X * Y > Integer'Last
  Put_Line("X * Y overflowed");
end if;
exception
  when others =>
    Put_Line("X * Y overflowed");
```

If X*Y does overflow, you may not remove the raise of the exception if the code that does the comparison against
Integer'Last presumes that it is comparing it with an in-range Integer value, and hence always yields False.

As another example where a raise may not be eliminated:

```ada
subtype Str10 is String(1..10);
type P10 is access Str10;
X : P10 := null;
begin
  if X.all'Last = 10 then
    Put_Line("Oops");
  end if;
```

In the above code, it would be wrong to eliminate the raise of Constraint_Error on the "X.all" (since X is null), if the
code to evaluate 'Last always yields 10 by presuming that X.all belongs to the subtype Str10, without even "looking".

- **{AI105-0229-1} {AI12-0445-1}** If an exception is raised due to the failure of a language-defined
check, then upon reaching the corresponding exception_handler (or the termination of the task, if
none), the external interactions that have occurred have not raised somewhere within the execution of the sequence_of_statements with the handler (or the
task_body), possibly earlier (or later if the interactions are independent of the result of the
checked operation) than that defined by the canonical semantics, but not within the execution of
some abort-deferred operation or independent subprogram that does not dynamically enclose the
execution of the construct whose check failed. An independent subprogram is one that is defined
outside the library unit containing the construct whose check failed, and for which the has no
Inline aspect is Falsepragma applied to it. Any assignment that occurred outside of such abort-
deferred operations or independent subprograms can be disrupted by the raising of the exception, causing the object or its parts to become abnormal, and certain subsequent uses of the object to be erroneous, as explained in 13.9.1.

6.a  **Reason:** We allow such variables to become abnormal so that assignments (other than to atomic variables) can be disrupted due to “imprecise” exceptions or instruction scheduling, and so that assignments can be reordered so long as the correct results are produced in the end if no language-defined checks fail.

6.b  **Ramification:** If a check fails, no result dependent on the check may be incorporated in an external interaction. In other words, there is no permission to output meaningless results due to postponing a check.

6.c  **Discussion:** We believe it is important to state the extra permission to reorder actions in terms of what the programmer can expect at run time, rather than in terms of what the implementation can assume, or what transformations the implementation can perform. Otherwise, how can the programmer write reliable programs?

6.d/3  

\{AI05-0299-1\} This subclause has two conflicting goals: to allow as much optimization as possible, and to make program execution as predictable as possible (to ease the writing of reliable programs). The rules given above represent a compromise.

6.e  Consider the two extremes:

6.f/3  

\{AI05-0299-1\} The extreme conservative rule would be to delete this subclause entirely. The semantics of Ada would be the canonical semantics. This achieves the best predictability. It sounds like a disaster from the efficiency point of view, but in practice, implementations would provide modes in which less predictability but more efficiency would be achieved. Such a mode could even be the out-of-the-box mode. In practice, implementers would provide a compromise based on their customer's needs. Therefore, we view this as one viable alternative.

6.g  The extreme liberal rule would be “the language does not specify the execution of a program once a language-defined check has failed; such execution can be unpredictable”. This achieves the best efficiency. It sounds like a disaster from the predictability point of view, but in practice it might not be so bad. A user would have to assume that exception handlers for exceptions raised by language-defined checks are not portable. They would have to isolate such code (like all nonportable code), and would have to find out, for each implementation of interest, what behaviors can be expected. In practice, implementations would tend to avoid going so far as to punish their customers too much in terms of predictability.

6.h/3  

\{AI05-0299-1\} The most important thing about this subclause is that users understand what they can expect at run time, and implementers understand what optimizations are allowed. Any solution that makes this subclause contain rules that can interpreted in more than one way is unacceptable.

6.i  We have chosen a compromise between the extreme conservative and extreme liberal rules. The current rule essentially allows arbitrary optimizations within a library unit and inlined subprograms reachable from it, but disallow semantics-disrupting optimizations across library units in the absence of inlined subprograms. This allows a library unit to be debugged, and then reused with some confidence that the abstraction it manages cannot be broken by bugs outside the library unit.

7/3  **NOTE:** \{AI05-0299-1\} The permissions granted by this subclause can have an effect on the semantics of a program only if the program fails a language-defined check.

Wording Changes from Ada 83

7.a  RM83-11.6 was unclear. It has been completely rewritten here; we hope this version is clearer. Here's what happened to each paragraph of RM83-11.6:

7.b  • Paragraphs 1 and 2 contain no semantics; they are merely pointing out that anything goes if the canonical semantics is preserved. We have similar introductory paragraphs, but we have tried to clarify that these are not granting any “extra” permission beyond what the rest of the document allows.

7.c  • Paragraphs 3 and 4 are reflected in the “extra permission to reorder actions”. Note that this permission now allows the reordering of assignments in many cases.

7.d  • Paragraph 5 is moved to 4.5, “Operators and Expression Evaluation”, where operator association is discussed. Hence, this is no longer an “extra permission” but is part of the canonical semantics.

7.e  • Paragraph 6 now follows from the general permission to store out-of-range values for unconstrained subtypes. Note that the parameters and results of all the predefined operators of a type are of the unconstrained subtype of the type.

7.f  • Paragraph 7 is reflected in the “extra permission to avoid raising exceptions”.

7.g/5  

\{AI05-0299-1\} \{AI12-0005-1\} We moved subclauses 11.5, “Suppressing Checks” (which was numbered 11.7) from after 11.6 to before 11.6, in order to preserve the famous number “11.6” (given the changes to earlier subclauses in Clause 11).
12  Generic Units

A generic unit is a program unit that is either a generic subprogram or a generic package. A generic unit is a template, which can be parameterized, and from which corresponding (nongeneric) subprograms or packages can be obtained. The resulting program units are said to be instances of the original generic unit.

Term entry: generic unit — template for a (nongeneric) program unit
Note 1: The template can be parameterized by objects, types, subprograms, and packages.
Note 2: Generic units can be used to perform the role that macros sometimes play in other languages.

Term entry: generic instance — nongeneric unit created by the instantiation of a generic unit

A generic unit is declared by a generic_declaration. This form of declaration has a generic_formal_part declaring any generic formal parameters. An instance of a generic unit is obtained as the result of a generic_instantiation with appropriate generic actual parameters for the generic formal parameters. An instance of a generic subprogram is a subprogram. An instance of a generic package is a package.

Generic units are templates. As templates they do not have the properties that are specific to their nongeneric counterparts. For example, a generic subprogram can be instantiated but it cannot be called. In contrast, an instance of a generic subprogram is a (nongeneric) subprogram; hence, this instance can be called but it cannot be used to produce further instances.

12.1 Generic Declarations

A generic_declaration declares a generic unit, which is either a generic subprogram or a generic package. A generic_declaration includes a generic_formal_part declaring any generic formal parameters. A generic formal parameter can be an object; alternatively (unlike a parameter of a subprogram), it can be a type, a subprogram, or a package.

Syntax

generic_declaration ::= generic_subprogram_declaration | generic_package_declaration

{AI05-0183-1} generic_subprogram_declaration ::= generic_formal_part subprogram_specification

[aspect_specification];

generic_package_declaration ::= generic_formal_part package_specification;

Ramification: {AI05-0183-1} No syntax change is needed here to allow an aspect_specification; a generic package can have an aspect_specification because a package_specification allows an aspect_specification.

generic_formal_part ::= generic {generic_formal_parameter_declaration | use_clause}

generic_formal_parameter_declaration ::= formal_object_declaration

| formal_type_declaration

| formal_subprogram_declaration

| formal_package_declaration

The only form of subtype_indication allowed within a generic_formal_part is a subtype_mark [(that is, the subtype_indication shall not include an explicit constraint)]. The defining name of a generic subprogram shall be an identifier [(not an operator_symbol)].
Reason: The reason for forbidding constraints in subtype indications is that it simplifies the elaboration of generic declarations (since there is nothing to evaluate), and that it simplifies the matching rules, and makes them more checkable at compile time.

Static Semantics

{AI95-00434-01} A generic_declaration declares a generic unit — a generic package, generic procedure, or generic function, as appropriate.

An entity is a generic formal entity if it is declared by a generic_formal_parameter_declaration. “Generic formal”, or simply “formal”, is used as a prefix in referring to objects, subtypes (and types), functions, procedures and packages, that are generic formal entities, as well as to their respective declarations. [Examples: “generic formal procedure” or a “formal integer type declaration”.

Ramification: Aspect specifications (see 13.1.1) given in a generic formal part can only use declarations given in the formal part, and not those in the visible part of the generic unit.

Dynamic Semantics

The elaboration of a generic_declaration has no effect.

NOTE 1 Outside a generic unit a name that denotes the generic_declaration denotes the generic unit. In contrast, within the declarative region of the generic unit, a name that denotes the generic_declaration denotes the current instance.

Proof: This is stated officially as part of the “current instance” rule in 8.6, “The Context of Overload Resolution”. See also 12.3, “Generic Instantiation”.

NOTE 2 Within a generic subprogram_body, the name of this program unit acts as the name of a subprogram. Hence this name can be overloaded, and it can appear in a recursive call of the current instance. For the same reason, this name cannot appear after the reserved word new in a (recursive) generic_instantiation.

NOTE 3 {AI12-0447-1} A default_expression or default_name appearing in a generic_formal_part is not evaluated during elaboration of the generic_formal_part; instead, it is evaluated when used. However, the usual visibility rules apply to any name used in a default, with name resolution performed based on the location of the name within the generic_formal_part; the denoted declaration therefore has to be visible at the place of the expression.)

Examples

Examples of generic formal parts:

```
geometric -- parameterless

generic
    Size : Natural; -- formal object

generic
    Length : Integer := 200; -- formal object with a default expression
    Area : Integer := Length*Length; -- formal object with a default expression

generic
    type Item is private;
    type Index is <>;
    type Row is array(Index range <>) of Item; -- formal type
    with function "<(X, Y : Item) return Boolean; -- formal subprogram
```

Examples of generic declarations declaring generic subprograms Exchange and Squaring:

```
geometric
    type Elem is private;
    procedure Exchange(U, V : in out Elem);

{AI12-0178-1} geometric
    type Item is <>;
    with function "***(U, V : Item) return Item is <>;
    function Squaring(X : Item) return Item;
```
Example of a generic declaration declaring a generic package:

```
generic
  type Item is private;
  type Vector is array (Positive range <>) of Item;
  with function Sum (X, Y : Item) return Item;
package On_Vectors is
  function Sum (A, B : Vector) return Vector;
  function Sigma(A : Vector) return Item;
  Length_Error : exception;
end On_Vectors;
```

Extensions to Ada 83

The syntax rule for `generic_formal_parameter_declaration` is modified to allow the reserved words `tagged` and `abstract`, to allow formal derived types, and to allow formal packages.

Use clauses are allowed in `generic_formal_parts`. This is necessary in order to allow a `use_clause` within a formal part to provide direct visibility of declarations within a generic formal package.

Wording Changes from Ada 83

{AI05-0299-1} The syntax for `generic_formal_parameter_declaration` and `formal_type_definition` is split up into more named categories. The rules for these categories are moved to the appropriate clauses and subclauses. The names of the categories are changed to be more intuitive and uniform. For example, we changed `generic_parameter_declaration` to `generic_formal_parameter_declaration`, because the thing it declares is a generic formal, not a generic. In the others, we abbreviate “generic formal” to just “formal”. We can't do that for `generic_formal_parameter_declaration`, because of confusion with normal formal parameters of subprograms.

Extensions to Ada 2005

{AI05-0183-1} An optional `aspect_specification` can be used in a `generic_subprogram_declaration` (as well as a `generic_package_declaration`). This is described in 13.1.1.

Wording Changes from Ada 2012

{AI12-0371-1} Defined a formal part as a declaration list, so that the visibility of entities in aspect specifications is properly defined.

12.2 Generic Bodies

The body of a generic unit (a `generic body`) [is a template for the instance bodies. The syntax of a generic body is identical to that of a nongeneric body].

Ramification: We also use terms like “generic function body” and “nongeneric package body”.

Dynamic Semantics

The elaboration of a generic body has no other effect than to establish that the generic unit can from then on be instantiated without failing the Elaboration_Check. If the generic body is a child of a generic package, then its elaboration establishes that each corresponding declaration nested in an instance of the parent (see 10.1.1) can from then on be instantiated without failing the Elaboration_Check.

NOTE The syntax of generic subprograms implies that a generic subprogram body is always the completion of a declaration.

Examples

Example of a generic procedure body:

```
procedure Exchange (U, V : in out Elem) is -- see 12.1
  T : Elem; -- the generic formal type
begin
  T := U;
  U := V;
  V := T;
end Exchange;
```
Example of a generic function body:

```ada
function Squaring(X : Item) return Item is -- see 12.1
begin
  return X*X;  -- the formal operator "*"
end Squaring;
```

Example of a generic package body:

```ada
package body On_Vectors is -- see 12.1
function Sum(A, B : Vector) return Vector is
  Result : Vector(A'Range); -- the formal type Vector
  Bias   : constant Integer := B'First - A'First;
begin
  if A'Length /= B'Length then
    raise Length_Error;
  end if;
  for N in A'Range loop
    Result(N) := Sum(A(N), B(N + Bias)); -- the formal function Sum
  end loop;
  return Result;
end Sum;

function Sigma(A : Vector) return Item is
  Total : Item := A(A'First); -- the formal type Item
begin
  for N in A'First + 1 .. A'Last loop
    Total := Sum(Total, A(N)); -- the formal function Sum
  end loop;
  return Total;
end Sigma;
end On_Vectors;
```

12.3 Generic Instantiation

[ An instance of a generic unit is declared by a generic_instantiation.]

Language Design Principles

1.a/5 \{AI12-0300-1\} The legality of an instance should be determinable without looking at the generic body. Likewise, the legality of a generic body should be determinable without looking at any instances. Thus, the generic_declaration forms a contract between the body and the instances; if each obeys the rules with respect to the generic_declaration, then no legality problems will arise. This is really a special case of the “legality determinable via semantic dependences” Language Design Principle (see Clause 10), given that a generic_instantiation does not depend semantically upon the generic body, nor vice-versa.

1.b Run-time issues are another story. For example, whether parameter passing is by copy or by reference is determined in part by the properties of the generic actuals, and thus cannot be determined at compile time of the generic body. Similarly, the contract model does not apply to Post-Compilation Rules.

Syntax

2/3 \{AI95-00218-03\} \{AI05-0183-1\} generic_instantiation ::= 
  package defining_program_unit_name is 
    new generic_package_name [generic_actual_part]
    [aspect_specification]; 
  [overriding_indicator]
  procedure defining_program_unit_name is 
    new generic_procedure_name [generic_actual_part]
    [aspect_specification]; 
  [overriding_indicator]
  function defining_designator is 
    new generic_function_name [generic_actual_part]
[aspect_specification]:

generic_actual_part ::=  
  (generic_association {, generic_association})

generic_association ::=  
  [generic_formal_parameter_selector_name =>] explicit_generic_actual_parameter

explicit_generic_actual_parameter ::= expression | variable_name  
  | subprogram_name | entry_name | subtype_mark  
  | package_instance_name

A generic_association is named or positional according to whether or not the generic_formal_parameter_selector_name is specified. Any positional associations shall precede any named associations.

\{AI05-0004-1\} \{AI12-0205-1\} The generic actual parameter is either the explicit_generic_actual_parameter given in a generic_association for each formal, or the corresponding default_expression, default_subtype_mark, or default_name if no generic_association is given for the formal. When the meaning is clear from context, the term “generic actual”, or simply “actual”, is used as a synonym for “generic actual parameter” and also for the view denoted by one, or the value of one.

Ramification: \{AI12-0205-1\} Any matching or other Legality Rules that apply to a generic actual are applied to any default_expression, default_subtype_mark, or default_name that are used as an actual.

Legality Rules

In a generic_instantiation for a particular kind of program unit [(package, procedure, or function)], the name shall denote a generic unit of the corresponding kind [(generic package, generic procedure, or generic function, respectively)].

\{AI05-0118-1\} The generic_formal_parameter_selector_name of a named generic_association shall denote a generic_formal_parameter_declaration of the generic unit being instantiated. If two or more formal subprograms have the same defining name, then named associations are not allowed for the corresponding actuals.

\{AI05-0118-1\} The generic_formal_parameter_declaration for a positional generic_association is the parameter with the corresponding position in the generic_formal_part of the generic unit being instantiated.

\{AI12-0205-1\} A generic_instantiation shall contain at most one generic_association for each formal. Each formal without an association shall have a default_expression, default_subtype_mark, or subprogram_default.

\{AI12-0418-1\} In a generic unit, Legality Rules are enforced at compile time of the generic_declaration and generic body, given the properties of the formals. In the visible part and formal part of an instance, Legality Rules are enforced at compile time of the generic_instantiation, given the properties of the actuals. In other parts of an instance, Legality Rules are not enforced; this rule does not apply when a given rule explicitly specifies otherwise.

Reason: \{AI95-00114-01\} Since rules are checked using the properties of the formals, and since these properties do not always carry over to the actuals, we need to check the rules again in the visible part of the instance. For example, only if a tagged type is limited may an extension of it have limited components in the record_extension_part. A formal tagged limited type is limited, but the actual might be nonlimited. Hence any rule that requires a tagged type to be limited runs into this problem. Such rules are rare; in most cases, the rules for matching of formals and actuals guarantee that if the rule is obeyed in the generic unit, then it has to be obeyed in the instance.
11.1/3 {AI05-0005-1} Ada 2012 addendum: Such Legality Rules are not as rare as the authors of Ada 95 hoped; there are more than 30 of them known at this point. They are indexed under “generic contract issue” and are associated with the boilerplate “In addition to the places where Legality Rules normally apply...”. Indeed, there is only one known rule where rechecking in the specification is needed and where rechecking in the private part is not wanted (it is in 3.4, but even it needs rechecking when tagged types are involved).

11.b Ramification: The “properties” of the formals are determined without knowing anything about the actuals:

11.c/1 • {8652/0095} {AI95-00034-01} A formal derived subtype is constrained if and only if the ancestor subtype is constrained. A formal array type is constrained if and only if the declarations say so. A formal private type is constrained if it does not have a discriminant part. Other formal subtypes are unconstrained, even though they might be constrained in an instance.

11.d • A formal subtype can be indefinite, even though the copy might be definite in an instance.

11.e • A formal object of mode in is not a static constant; in an instance, the copy is static if the actual is.

11.f • A formal subtype is not static, even though the actual might be.

11.g • Formal types are specific, even though the actual can be class-wide.

11.h • The subtype of a formal object of mode in out is not static. (This covers the case of A183-00878.)

11.i • The subtype of a formal parameter of a formal subprogram does not provide an applicable index constraint.

11.j/3 • {AI05-0239-1} The profile of a formal subprogram is not subtype conformant subtype-conformant with any other profile.

11.k • A generic formal function is not static.

11.l {AI95-00034-01} The corrections made by the Corrigendum added a number of such rules, and the Amendment added many more. There doesn't seem to be much value in repeating all of these rules here (as of this writing, there are roughly 33 such rules). As noted below, all such rules are indexed in the AARM.

11.m Ramification: The exceptions to the above rule about when legality rules are enforced fall into these categories:

11.n • Some rules are checked in the generic declaration, and then again in both the visible and private parts of the instance:

11.o • The parent type of a record extension has to be specific (see 3.9.1). This rule is not checked in the instance body.

11.p/3 • {AI95-00402-01} {AI05-0093-1} A type with an access discriminant with a default_expression has to be immutably limited. In the generic body, the definition of immutably limited is adjusted in an assume-the-worst manner (thus the rule is checked that way) a descendant of an explicitly limited record type declared with limited, or be a task or protected type. This rule is irrelevant in the instance body.

11.q • In the declaration of a record extension, if the parent type is nonlimited, then each of the components of the record_extension_part have to be nonlimited (see 3.9.1). In the generic body, this rule is checked in an assume-the-worst manner.

11.r • A preelaborated library unit has to be preelaborable (see 10.2.1). In the generic body, this rule is checked in an assume-the-worst manner.

11.r.1/2 {AI95-00402-01} The rules requiring “reasonable” values for static expressions are ignored when the expected type for the expression is a descendant of a generic formal type other than a generic formal derived type, and do not apply in an instance.

11.s For the accessibility rules, the formals have nothing to say about the property in question. Like the above rules, these rules are checked in the generic declaration, and then again in both the visible and private parts of the instance. In the generic body, we have explicit rules that essentially assume the worst (in the cases of type extensions and access-to-subprogram types), and we have runtime checks (in the case of access-to-object types). See 3.9.1, 3.10.2, and 4.6.

11.t We considered runtime checks for access-to-subprogram types as well. However, this would present difficulties for implementations that share generic bodies.

11.u • The rules requiring “reasonable” values for static expressions are ignored when the expected type for the expression is a descendant of a generic formal type other than a generic formal derived type, and do not apply in an instance.

11.v • The rule forbidding two explicit homographs in the same declarative region does not apply in an instance of a generic unit, except that it does apply in the declaration of a record extension that appears in the visible part of an instance.

11.w • Some rules do not apply at all in an instance, not even in the visible part:

11.x • Body_stubs are not normally allowed to be multiply nested, but they can be in instances.

11.y Each rule that is an exception is marked with “generic contract issue;” look that up in the index to find them all.
Ramification: The Legality Rules are the ones labeled Legality Rules. We are talking about all Legality Rules in the entire language here. Note that, with some exceptions, the legality of a generic unit is checked even if there are no instantiations of the generic unit.

Ramification: [AI05-0299-1] [AI12-0005-1] The Legality Rules are described here, and the overloading rules were described earlier in this subclause. Presumably, every Static Semantic Item is included indirectly by one of those. Thus, we have covered all the compile-time rules of the language. There is no need to say anything special about the Post-Compilation Rules or the Dynamic Semantic Items.

Discussion: Here is an example illustrating how this rule is checked: “In the declaration of a record extension, if the parent type is nonlimited, then each of the components of the record_extension_part shall be nonlimited.”

```
generic
  type Parent is tagged private;
  type Comp is limited private;
package G1 is
  type Extension is new Parent with
    record
      C : Comp; -- Illegal!
    end record;
end G1;
```

The parent type is nonlimited, and the component type is limited, which is illegal. It doesn't matter that one could imagine writing an instantiation with the actual for Comp being nonlimited — we never get to the instance, because the generic itself is illegal.

On the other hand:

```
generic
  type Parent is tagged limited private; -- Parent is limited.
  type Comp is limited private;
package G2 is
  type Extension is new Parent with
    record
      C : Comp; -- OK.
    end record;
end G2;
```

```
type Limited_Tagged is tagged limited null record;
type Non_Limited_Tagged is tagged null record;
type Non_Limited_Untagged is null record;
package Good_1 is new G2(Parent => Limited_Tagged,
  Comp => Non_Limited_Untagged);
package Good_2 is new G2(Parent => Non_Limited_Tagged,
  Comp => Non_Limited_Untagged);
package Bad is new G2(Parent => Non_Limited_Tagged,
  Comp => Limited_Untagged); -- Illegal!
```

The first instantiation is legal, because in the instance the parent is limited, so the rule is not violated. Likewise, in the second instantiation, the rule is not violated in the instance. However, in the Bad instance, the parent type is nonlimited, and the component type is limited, so this instantiation is illegal.

Static Semantics

A generic_instantiation declares an instance; it is equivalent to the instance declaration (a package_declaration or subprogram_declaration) immediately followed by the instance body, both at the place of the instantiation.

Ramification: The declaration and the body of the instance are not “implicit” in the technical sense, even though you can't see them in the program text. Nor are declarations within an instance “implicit” (unless they are implicit by other rules). This is necessary because implicit declarations have special semantics that should not be attached to instances. For a generic subprogram, the profile of a generic_instantiation is that of the instance declaration, by the stated equivalence.

Ramification: The visible and private parts of a package instance are defined in 7.1, “Package Specifications and Declarations” and 12.7, “Formal Packages”. The visible and private parts of a subprogram instance are defined in 8.2, “Scope of Declarations”.

The instance is a copy of the text of the template. [Each use of a formal parameter becomes (in the copy) a use of the actual, as explained below.] An instance of a generic package is a package, that of a generic procedure is a procedure, and that of a generic function is a function.
Ramification: An instance is a package or subprogram (because we say so), even though it contains a copy of the generic_formal_part, and therefore doesn't look like one. This is strange, but it's OK, since the syntax rules are overloading rules, and therefore do not apply in an instance.

Discussion: We use a macro-expansion model, with some explicitly-stated exceptions (see below). The main exception is that the interpretation of each construct in a generic unit (especially including the denotation of each name) is determined when the declaration and body of the generic unit (as opposed to the instance) are compiled, and in each instance this interpretation is (a copy of) the template interpretation. In other words, if a construct is interpreted as a name denoting a declaration D, then in an instance, the copy of the construct will still be a name, and will still denote D (or a copy of D). From an implementation point of view, overload resolution is performed on the template, and not on each copy.

We describe the substitution of generic actual parameters by saying (in most cases) that the copy of each generic formal parameter declares a view of the actual. Suppose a name in a generic unit denotes a generic_formal_parameter_declaration. The copy of that name in an instance will denote the copy of that generic_formal_parameter_declaration in the instance. Since the generic_formal_parameter_declaration in the instance declares a view of the actual, the name will denote a view of the actual.

Another property of the copy (for example, staticness, categories, to which types belong) are recalculated for each instance; this is implied by the fact that it's a copy.

Although the generic_formal_part is included in an instance, the declarations in the generic_formal_part are only visible outside the instance in the case of a generic formal package whose formal_package_actual_part includes one or more <> indicators — see 12.7.

The interpretation of each construct within a generic declaration or body is determined using the overload rules when that generic declaration or body is compiled. In an instance, the interpretation of each (copied) construct is the same, except in the case of a name that denotes the generic_declaration or some declaration within the generic unit; the corresponding copy in the instance then denotes the corresponding copy of the denoted declaration. The overloading rules do not apply in the instance.

Ramification: See 8.6, “The Context of Overload Resolution” for definitions of “interpretation” and “overloading rule”.

Even the generic_formal_parameterclarations have corresponding declarations in the instance, which declare views of the actuals.

Although the declarations in the instance are copies of those in the generic unit, they often have quite different properties, as explained below. For example a constant declaration in the generic unit might declare a nonstatic constant, whereas the copy of that declaration might declare a static constant. This can happen when the staticness depends on some generic formal.

This rule is partly a ramification of the “current instance” rule in 8.6, “The Context of Overload Resolution”. Note that that rule doesn't cover the generic_formal_part.

Although the overloading rules are not observed in the instance, they are, of course, observed in the generic instantiation in order to determine the interpretation of the constituents of the generic instantiation.

Since children are considered to occur within their parent's declarative region, the above rule applies to a name that denotes a child of a generic unit, or a declaration inside such a child.

Since the Syntax Rules are overloading rules, it is possible (legal) to violate them in an instance. For example, it is possible for an instance body to occur in a package_specification, even though the Syntax Rules forbid bodies in package_specifications.

In an instance, a generic_formal_parameter_declaration declares a view whose properties are identical to those of the actual, except whenas specified otherwise (in particular, see 6.1.1, “Preconditions and Postconditions”, in 12.4, “Formal Objects”, and 12.6, “Formal Subprograms”). Similarly, for a declaration within a generic_formal_parameter_declaration, the corresponding declaration in an instance declares a view whose properties are identical to the corresponding declaration within the declaration of the actual.

Ramification: In an instance, there are no “properties” of types and subtypes that come from the formal. The primitive operations of the type come from the formal, but these are declarations in their own right, and are therefore handled separately.

Note that certain properties that come from the actuals are irrelevant in the instance. For example, if an actual type is of a class deeper in the derived-type hierarchy than the formal, it is impossible to call the additional operations of the
deeper class in the instance, because any such call would have to be a copy of some corresponding call in the generic unit, which would have been illegal. However, it is sometimes possible to reach into the specification of the instance from outside, and notice such properties. For example, one could pass an object declared in the instance specification to one of the additional operations of the deeper type.

{AI95-00114-01} A formal_type_declaration can contain discriminant_specifications, a formal_subprogram_declaration can contain parameter_specifications, formal_parameter_specification, and a formal_package_declaration can contain many kinds of declarations. These are all inside the generic unit, and have corresponding declarations in the instance.

This rule implies, for example, that if a subtype in a generic unit is a subtype of a generic formal subtype, then the corresponding subtype in the instance is a subtype of the corresponding actual subtype.

For a generic_instantiation, if a generic actual is a static ([scalar or string]) subtype, then each use of the corresponding formal parameter within the specification of the instance is considered to be static. (See AI83-00409.)

Similarly, if a generic actual is a static expression and the corresponding formal parameter has a static ([scalar or string]) subtype, then each use of the formal parameter in the specification of the instance is considered to be static. (See AI83-00505.)

If a primitive subprogram of a type derived from a generic formal derived tagged type is not overriding (that is, it is a new subprogram), it is possible for the copy of that subprogram in an instance to override a subprogram inherited from the actual. For example:

```ada
{AI12-0005-1} generic
  type Formal is new T1 with private;
package G is
  type Derived_From_Formal is new Formal with record ... end record;
  procedure Foo(X : in Derived_From_Formal); -- Does not override anything.
end G;
type T2 is new T1 with record ... end record;
procedure Foo(X : in T2);
package Inst is new G(Formal => T2);
```

In the instance Inst, the declaration of Foo for Derived_From_Formal overrides the Foo inherited from T2.

Implementation Note: {8652/0009} {AI95-00137-01} For formal types, an implementation that shares the code among multiple instances of the same generic unit needs to beware that things like parameter passing mechanisms (by-copy vs. by-reference) and aspect_clause_representation_clauses are determined by the actual.

Reason: {AI12-0407-1} In particular, we allow differences for aspects that can be specified on generic formal parameters. For instance, Pre (see 6.1.1) can be specified on generic formal subprograms to be added to the Pre of the actual.

Implicit declarations are also copied, and a name that denotes an implicit declaration in the generic denotes the corresponding copy in the instance. However, for a type declared within the visible part of the generic, a whole new set of primitive subprograms is implicitly declared for use outside the instance, and may differ from the copied set if the properties of the type in some way depend on the properties of some actual type specified in the instantiation. For example, if the type in the generic is derived from a formal private type, then in the instance the type will inherit subprograms from the corresponding actual type.

These new implicit declarations occur immediately after the type declaration in the instance, and override the copied ones. The copied ones can be called only from within the instance; the new ones can be called only from outside the instance, although for tagged types, the body of a new one can be executed by a call to an old one.]

Proof: This rule is stated officially in 8.3, “Visibility”.

Ramification: The new ones follow from the class(es) of the formal types. For example, for a type T derived from a generic formal private type, if the actual is Integer, then the copy of T in the instance has a "+'" primitive operator, which can be called from outside the instance (assuming T is declared in the visible part of the instance).

AI83-00398.

{AI95-00442-01} Since an actual type is always in the category class determined for the formal, the new subprograms hide all of the copied ones, except for a declaration of "/=" that corresponds to an explicit declaration of "=". Such "/=" operators are special, because unlike other implicit declarations of primitive subprograms, they do not appear by virtue of the class, but because of an explicit declaration of "=". If the declaration of "=" is implicit (and therefore overridden in the instance), then a corresponding implicitly declared "/=" is also overridden. But if the declaration of "=" is
explicit (and therefore not overridden in the instance), then a corresponding implicitly declared "/=" is not overridden either, even though it's implicit.

Note that the copied ones can be called from inside the instance, even though they are hidden from all visibility, because the names are resolved in the generic unit — visibility is irrelevant for calls in the instance.

[In the visible part of an instance, an explicit declaration overrides an implicit declaration if they are homographs, as described in 8.3.] On the other hand, an explicit declaration in the private part of an instance overrides an implicit declaration in the instance, only if the corresponding explicit declaration in the generic overrides a corresponding implicit declaration in the generic. Corresponding rules apply to the other kinds of overriding described in 8.3.

Ramification: For example:

```ada
type Ancestor is tagged null record;
generic
  type Formal is new Ancestor with private;
package G is
  type T is new Formal with null record;
  procedure P(X : in T); -- (1)
  private
  procedure Q(X : in T); -- (2)
end G;

type Actual is new Ancestor with null record;
procedure P(X : in Actual);
procedure Q(X : in Actual);
package Instance is new G(Formal => Actual);
```

In the instance, the copy of P at (1) overrides Actual's P, whereas the copy of Q at (2) does not override anything; in implementation terms, it occupies a separate slot in the type descriptor.

Reason: {AI12-0347-1} The reason for this rule is so a programmer writing a generic instantiation need not look at the private part of the generic in order to determine which subprograms will be overridden.

Post-Compilation Rules

Recursive generic instantiation is not allowed in the following sense: if a given generic unit includes an instantiation of a second generic unit, then the instance generated by this instantiation shall not include an instance of the first generic unit [(whether this instance is generated directly, or indirectly by intermediate instantiations)].

Discussion: Note that this rule is not a violation of the generic contract model, because it is not a Legality Rule. Some implementations may be able to check this rule at compile time, but that requires access to all the bodies, so we allow implementations to check the rule at link time.

Dynamic Semantics

For the elaboration of a generic instantiation, each generic association is first evaluated. If a default is used, an implicit generic association is assumed for this rule. These evaluations are done in an arbitrary order, except that the evaluation for a default actual takes place after the evaluation for another actual if the default includes a name that denotes the other one. Finally, the instance declaration and body are elaborated.

Ramification: Note that if the evaluation of a default depends on some side effect of some other evaluation, the order is still arbitrary.

For the evaluation of a generic association the generic actual parameter is evaluated. Additional actions are performed in the case of a formal object of mode in (see 12.4).

To be honest: Actually, the actual is evaluated only if evaluation is defined for that kind of construct — we don't actually “evaluate” subtype marks.

NOTE If a formal type is not tagged, then the type is treated as an untagged type within the generic body. Deriving from such a type in a generic body is permitted; the new type does not get a new tag value, even if the actual is tagged. Overriding operations for such a derived type cannot be dispatched to from outside the instance.
Ramification: If two overloaded subprograms declared in a generic package specification differ only by the (formal)
type of their parameters and results, then there exist legal instantiations for which all calls of these subprograms from
outside the instance are ambiguous. For example:

```ada
generic
  type A is <>;
  type B is private;
package G is
  function Next(X : A) return A;
  function Next(X : B) return B;
end G;
package P is new G(A => Boolean, B => Boolean);
-- All calls of P:Next are ambiguous.
```

Ramification: The following example illustrates some of the subtleties of the substitution of formals and actuals:

```ada
{AI12-0005-1} generic
  type T1 is private;
  -- A predefined "=" operator is implicitly declared here:
  -- function "="(Left, Right : T1) return Boolean;
  -- Call this "=".
...
package G is
  subtype S1 is T1; -- So we can get our hands on the type from
  -- outside an instance.
  type T2 is new T1;
  -- An inherited "=" operator is implicitly declared here:
  -- function "="(Left, Right : T2) return Boolean;
  -- Call this "=".
  T1_Obj : T1 := ...;  
  Bool1 : Boolean := T1_Obj = T1_Obj;
  T2_Obj : T2 := ...;  
  Bool2 : Boolean := T2_Obj = T2_Obj;
end G;
...
{AI12-0005-1} package P is
  type My_Int is new Integer;
  -- A predefined "=" operator is implicitly declared here:
  -- function "="(Left, Right : My_Int) return Boolean;
  -- Call this "=".
  function "="(X, Y : My_Int) return Boolean;
  -- Call this "=".
  -- "=" is hidden from all visibility by "=".
  -- Nonetheless, "=" can "reemerge" in certain circumstances.
end P;
use P;
...
package I is new G(T1 => My_Int, ...); -- "=" is declared in I (see below).
use I;
  Another_T1_Obj : S1 := 13; -- Can't denote T1, but S1 will do.
  Bool1 : Boolean := Another_T1_Obj = Another_T1_Obj;
  Another_T2_Obj : T2 := 45;
  Bool2 : Boolean := Another_T2_Obj = Another_T2_Obj;
  Double : T2 := T2_Obj + Another_T2_Obj;
In the instance I, there is a copy of "=" (call it "="), and "=" (call it "="). The "=" and "=" declare views of the
predefined "=" of My_Int (that is, "="). In the initialization of Bool1 and Bool2 in the generic unit G, the names "="
denote "=" and "=" respectively. Therefore, the copies of these names in the instances denote "=" and "=" respectively. Thus, the initialization of I.Boo1 and I.Boo2 call the predefined equality operator of My_Int; they
will not call "=".
The declarations "=" and "=" are hidden from all visibility. This prevents them from being called from outside the
instance.
The declaration of Boo1 calls "=".
The instance I also contains implicit declarations of the primitive operators of T2, such as "=" (call it "=") and "=".
These operations cannot be called from within the instance, but the declaration of Boo2 calls "=".
```
Examples

Examples of generic instantiations (see 12.1):

```ada
{AI12-0178-1} procedure Swap is new Exchange(Elem => Integer);
procedure Swap is new Exchange(Character);  -- Swap is overloaded
function Square is new Squaring(Integer);  -- "*" of Integer used by default
function Square is new Squaring(Item => Matrix, "*" => Matrix Product);
function Square is new Squaring(Matrix, Matrix Product);  -- same as previous
package Int_Vectors is new On_Vectors(Integer, Table, "+");
```

Examples of uses of instantiated units:

```ada
Swap(A, B);
A := Square(A);
```

```
T : Table(1 .. 5) := (10, 20, 30, 40, 50);
N : Integer := Int_Vectors.Sigma(T);  -- 150  
-- (see 12.2.2, "Generic Bodies" for the body of Sigma)
```

use Int_Vectors;

```
M : Integer := Sigma(T);  -- 150
```

Inconsistencies With Ada 83

29.a
In Ada 83, all explicit actuals are evaluated before all defaults, and the defaults are evaluated in the order of the formal declarations. This ordering requirement is relaxed in Ada 95.

Incompatibilities With Ada 83

29.b
We have attempted to remove every violation of the contract model. Any remaining contract model violations should be considered bugs in the RM95. The unfortunate property of reverting to the predefined operators of the actual types is retained for upward compatibility. (Note that fixing this would require subtype conformance rules.) However, tagged types do not revert in this sense.

Extensions to Ada 83

29.c
The syntax rule for `explicit_generic_actual_parameter` is modified to allow a `package_instance_name`.

Wording Changes from Ada 83

29.d
The fact that named associations cannot be used for two formal subprograms with the same defining name is moved to AARM-only material, because it is a ramification of other rules, and because it is not of interest to the average user.

29.e
The rule that “An explicit `explicit_generic_actual_parameter` shall not be supplied more than once for a given `generic_formal_parameter`” seems to be missing from RM83, although it was clearly the intent.

29.f
In the explanation that the instance is a copy of the template, we have left out RM83-12.3(5)'s “apart from the generic formal part”, because it seems that things in the formal part still need to exist in instances. This is particularly true for generic formal packages, where you're sometimes allowed to reach in and denote the formals of the formal package from outside it. This simplifies the explanation of what each name in an instance denotes: there are just two cases: the declaration can be inside or outside (where inside needs to include the generic unit itself). Note that the RM83 approach of listing many cases (see RM 83-12.5(5-14)) would have become even more unwieldy with the addition of generic formal packages, and the declarations that occur therein.

29.g
We have corrected the definition of the elaboration of a `generic_instantiation` (RM83-12.3(17)); we don't elaborate entities, and the instance is not “implicit”.

29.h
In RM83, there is a rule saying the formal and actual shall match, and then there is much text defining what it means to match. Here, we simply state all the latter text as rules. For example, “A formal foo is matched by an actual greenish bar” becomes “For a formal foo, the actual shall be a greenish bar”. This is necessary to split the Name Resolution Rules from the Legality Rules. Besides, there's really no need to define the concept of matching for generic parameters.

Extensions to Ada 95

29.i
The rule that “An `overriding_indicator` (see 8.3.1) is allowed on a subprogram instantiation.”

Extensions to Ada 2005

29.j
An optional `aspect_specification` can be used in a `generic_instantiation`. This is described in 13.1.1.
12.4 Formal Objects

[ A generic formal object can be used to pass a value or variable to a generic unit. ]

Language Design Principles

A generic formal object of mode in is like a constant initialized to the value of the explicit_generic_actual_parameter.

A generic formal object of mode in out is like a renaming of the explicit_generic_actual_parameter.

Syntax

\{AI95-00423-01\} \{AI95-0005-1\} \{AI05-0183-1\}
formal_object_declaration ::= 
  defining_identifier_list : mode [null_exclusion] subtype_mark [:= default_expression]
  | defining_identifier_list : mode access_definition [:= default_expression]
    | [aspect_specification];

Name Resolution Rules

The expected type for the default_expression, if any, of a formal object is the type of the formal object.

For a generic formal object of mode in, the expected type for the actual is the type of the formal.

\{AI95-00423-01\} For a generic formal object of mode in out, the type of the actual shall resolve to the type determined by the subtype_mark, or for a formal_object_declaration with an access_definition, to a specific anonymous access type. If the anonymous access type is an access-to-object type, the type of the actual shall have the same designated type as that of the access_definition. If the anonymous access type is an access-to-subprogram type, the type of the actual shall have a designated profile which is type conformant with that of the access_definition of the formal.

Reason: See the corresponding rule for object_renaming_declarations for a discussion of the reason for this rule.

Legality Rules

If a generic formal object has a default_expression, then the mode shall be in [(either explicitly or by default)]; otherwise, its mode shall be either in or in out.

Ramification: Mode out is not allowed for generic formal objects.

For a generic formal object of mode in, the actual shall be an expression. For a generic formal object of mode in out, the actual shall be a name that denotes a variable for which renaming is allowed (see 8.5.1).

To be honest: The part of this that requires an expression or name is a Name Resolution Rule, but that's too pedantic to worry about. (The part about denoting a variable, and renaming being allowed, is most certainly not a Name Resolution Rule.)

\{AI95-00287-01\} \{AI95-00423-01\} In the case where the type of the formal is defined by an access_definition, the type of the actual and the type of the formal. The type of a generic formal object of mode in shall be nonlimited.

\bullet \{AI95-00423-01\} shall both be access-to-object types with statically matching designated subtypes and with both or neither being access-to-constant types; or

8.2/2 • `{AI95-00423-01}` shall both be access-to-subprogram types with subtype conformant designated profiles.

8.3/5 `{AI95-00423-01}` `{AI12-0287-1}` For a formal_object_declaration of mode in out with a null exclusion or an access definition that has a null exclusion, the subtype of the actual matching the formal_object_declaration shall exclude null. In addition, if the actual matching the formal_object_declaration statically denotes the generic formal object of mode in out of another generic unit G, and the instantiation containing the actual occurs within the body of G or within the body of a generic unit declared within the declarative region of G, then the declaration of the formal object of G shall have a null exclusion. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

8.4/5 • `{AI12-0287-1}` if the actual matching the formal_object_declaration denotes the generic formal object of another generic unit G, and the instantiation containing the actual occurs within the body of G or within the body of a generic unit declared within the declarative region of G, then the declaration of the formal object of G shall have a null exclusion;

8.5/5 • `{AI12-0287-1}` otherwise, the subtype of the actual matching the formal_object_declaration shall exclude null. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

Reason: `{AI95-00287-01}` `{AI95-00423-01}` `{AI12-0287-1}` This rule prevents “lying”. Null must never be the value of an object with an explicit null exclusion. The “in addition” part first bullet is an assume-the-worst rule which prevents trouble in generic bodies (including bodies of child units) when the subtype of the formal object of mode in out excludes null implicitly. Since a generic formal object of mode in is like a constant initialized to the value of the actual, the runtime check performed by the initialization is enough to prevent lying; thus we don't need a Legality Rule for such objects. Since a generic formal object is like a constant of mode in initialized to the value of the actual, a limited type would not make sense, since initializing a constant is not allowed for a limited type. That is, generic formal objects of mode in are passed by copy, and limited types are not supposed to be copied.

Static Semantics

9/2 `{AI95-00255-01}` `{AI95-00423-01}` A formal_object_declaration declares a generic formal object. The default mode is in. For a formal object of mode in, the nominal subtype is the one denoted by the subtype_mark or access_definition in the declaration of the formal. For a formal object of mode in out, its type is determined by the subtype_mark or access_definition in the declaration; its nominal subtype is nonstatic, even if the subtype_mark denotes a static subtype; for a composite type, its nominal subtype is unconstrained if the first subtype of the type is unconstrained, even if the subtype_mark denotes a constrained subtype.

Reason: `{AI95-00255-01}` We require that the subtype is unconstrained because a formal in out acts like a renaming, and thus the given subtype is ignored for purposes of matching; any value of the type can be passed. Thus we can assume only that the object is constrained if the first subtype is constrained (and thus there can be no unconstrained subtypes for the type). If we didn't do this, it would be possible to rename or take Access of components that could disappear due to an assignment to the whole object.

Discussion: `{AI95-00423-01}` The two “even if” clauses are OK even though they don't mention access_definitions; an access subtype can neither be a static subtype nor be a composite type.

10/2 `{AI95-00269-01}` In an instance, a formal_object_declaration of mode in is a full constant declaration and declares a new stand-alone constant object whose initialization expression is the actual, whereas a formal_object_declaration of mode in out declares a view whose properties are identical to those of the actual.

Ramification: `{AI95-00287-01}` These rules imply that generic formal objects of mode in are passed by copy (or are built-in-place for a limited type), whereas generic formal objects of mode in out are passed by reference.

Initialization and finalization happen for the constant declared by a formal_object_declaration of mode in as for any constant; see 3.3.1, “Object Declarations” and 7.6, “Assignment and Finalization”.

In an instance, the subtype of a generic formal object of mode in is as for the equivalent constant. In an instance, the subtype of a generic formal object of mode in out is the subtype of the corresponding generic actual.
Dynamic Semantics

For the evaluation of a generic_association for a formal object of mode in, a constant object is created, the value of the actual parameter is converted to the nominal subtype of the formal object, and assigned to the object[, including any value adjustment — see 7.6].

Ramification: This includes evaluating the actual and doing a subtype conversion, which might raise an exception.
Discussion: The rule for evaluating a generic_association for a formal object of mode in out is covered by the general Dynamic Semantics rule in 12.3.

NOTE The constraints that apply to a generic formal object of mode in out are those of the corresponding generic actual parameter (not those implied by the subtype_mark that appears in the formal_object_declaration). Therefore, to avoid confusion, it is recommended that the name of a first subtype be used for the declaration of such a formal object.

Ramification: Constraint checks are done at instantiation time for formal objects of mode in, but not for formal objects of mode in out.

Extensions to Ada 83

In Ada 83, it is forbidden to pass a (nongeneric) formal parameter of mode out, or a subcomponent thereof, to a generic formal object of mode in out. This restriction is removed in Ada 95.

Wording Changes from Ada 83

We make “mode” explicit in the syntax. RM83 refers to the mode without saying what it is. This is also more uniform with the way (nongeneric) formal parameters are defined.

We considered allowing mode out in Ada 95, for uniformity with (nongeneric) formal parameters. The semantics would be identical for modes in out and out. (Note that generic formal objects of mode in out are passed by reference. Note that for (nongeneric) formal parameters that are allowed to be passed by reference, the semantics of in out and out is the same. The difference might serve as documentation. The same would be true for generic formal objects, if out were allowed, so it would be consistent.) We decided not to make this change, because it does not produce any important benefit, and any change has some cost.

Extensions to Ada 95

{AI95-00287-01} A generic formal in object can have a limited type. The actual for such an object must be built-in-place via a function_call or aggregate, see 7.5.

{AI95-00423-01} A generic formal object can have a null_exclusion or an anonymous access type.

Wording Changes from Ada 95

{AI95-00255-01} Clarified that the nominal subtype of a composite formal in out object is unconstrained if the first subtype of the type is unconstrained.

{AI95-00269-01} Clarified that a formal in object can be static when referenced from outside of the instance (by declaring such an object to be a full constant declaration).

Extensions to Ada 2005

{AI05-0183-1} An optional aspect_specification can be used in a formal_object_declaration. This is described in 13.1.1.

Extensions to Ada 2012

{AI12-0287-1} Correction: The Legality Rule for matching null exclusions only applies to formal objects with mode in out. (In mode formal objects have a run-time check to avoid problems.) This is an extension as some instantiations that were illegal in original Ada 2012 are now legal.

12.5 Formal Types

{AI95-00442-01} [A generic formal subtype can be used to pass to a generic unit a subtype whose type is in a certain category class of types.]

Reason: We considered having intermediate syntactic categories formal_integer_type_definition, formal_real_type_definition, and formal_fixed_point_definition, to be more uniform with the syntax rules for non-
generic-formal types. However, that would make the rules for formal types slightly more complicated, and it would cause confusion, since formal_discrete_type_definition would not fit into the scheme very well.

Syntax

\[
\begin{align*}
\{AI05-0213-1\} & \text{ formal_type_declaration ::=} \\
& \quad \text{ formal_complete_type_declaration} \\
& \quad | \text{ formal_incomplete_type_declaration} \text{type defining_identifier[discriminant_part] is formal_type definition;} \\
\{AI05-0183-1\} \{AI12-0205-1\} & \text{ formal_complete_type_declaration ::=} \\
& \quad \text{ type defining_identifier[discriminant_part] is formal_type definition} \\
& \quad | \text{ or use default subtype_mark} \text{[aspect_specification];} \\
\{AI05-0213-1\} \{AI12-0205-1\} & \text{ formal_incomplete_type_declaration ::=} \\
& \quad \text{ type defining_identifier[discriminant_part] [is tagged]} \\
& \quad | \text{ or use default subtype_mark;} \\
\{AI95-00251-01\} & \text{ formal_type_definition ::=} \\
& \quad \text{ formal_private_type_definition} \\
& \quad | \text{ formal_derived_type_definition} \\
& \quad | \text{ formal_discrete_type_definition} \\
& \quad | \text{ formal_signed_integer_type_definition} \\
& \quad | \text{ formal_modular_type_definition} \\
& \quad | \text{ formal_floating_point_definition} \\
& \quad | \text{ formal_ordinary_fixed_point_definition} \\
& \quad | \text{ formal_decimal_fixed_point_definition} \\
& \quad | \text{ formal_array_type_definition} \\
& \quad | \text{ formal_access_type_definition} \\
& \quad | \text{ formal_interface_type_definition} \\
\end{align*}
\]

Legality Rules

For a generic formal subtype, the actual shall be a subtype_mark; it denotes the (generic) actual subtype.

Ramification: When we say simply “formal” or “actual” (for a generic formal that denotes a subtype) we're talking about the subtype, not the type, since a name that denotes a formal_type_declaration denotes a subtype, and the corresponding actual also denotes a subtype.

Static Semantics

A formal_type_declaration declares a (generic) formal type, and its first subtype, the (generic) formal subtype.

Ramification: A subtype (other than the first subtype) of a generic formal type is not a generic formal subtype.

Reason: This rule is clearer with the flat syntax rule for formal_type_definition given above. Adding formal_integer_type_definition and others would make this rule harder to state clearly.
We use “category” rather than “class” above, because the requirement that classes are closed under derivation is not important here. Moreover, there are interesting categories that are not closed under derivation. For instance, limited and interface are categories that do not form classes.

Legality Rules

The actual type shall be in the category class determined for the formal.

Ramification: AI95-00442-01 For example, if the category class determined for the formal is the category class of all discrete types, then the actual has to be discrete.

AI95-00442-01 Note that this rule does not require the actual to belong to every category class to which the formal belongs. For example, formal private types are in the category class of composite types, but the actual need not be composite. Furthermore, one can imagine an infinite number of category classes that just arbitrary sets of types that obey the closed under derivation rule, and are therefore technically classes (even though we don't give them names, since they are uninteresting). We don't want this rule to apply to those category classes.

AI95-00114-01 AI95-00442-01 “Limited” is not an “interesting” category class, but “nonlimited” is; it is legal to pass a nonlimited type to a limited formal type, but not the other way around. The reserved word limited really represents a category class containing both limited and nonlimited types. “Private” is not a category for this purpose class; a generic formal private type accepts both private and nonprivate actual types.

AI95-00442-01 It is legal to pass a class-wide subtype as the actual if it is in the right category class, so long as the formal has unknown discriminants.

AI12-0205-1 The default subtype mark, if any, shall denote a subtype which is allowed as an actual subtype for the formal type.

Ramification: AI12-0205-1 This rule is observed at compile time of the generic declaration, and is consistent with the handling of the default name of a formal subprogram. This means that a type declared outside of the generic declaration cannot be used as the default subtype mark for a formal type that depends on any other formal type.

Static Semantics

The formal type also belongs to each category class that contains the determined category class. The primitive subprograms of the type are as for any type in the determined category class. For a formal type other than a formal derived type, these are the predefined operators of the type. For an elementary formal type, the predefined operators are implicitly declared immediately after the declaration of the formal type. For a composite formal type, the predefined operators are implicitly declared either immediately after the declaration of the formal type, or later immediately within the declarative region in which the type is declared in its immediate scope according to the rules of 7.3.1; they are implicitly declared immediately after the declaration of the formal type. In an instance, the copy of such an implicit declaration declares a view of the predefined operator of the actual type, even if this operator has been overridden for the actual type and even if it is never declared for the actual type, unless the actual type is an untagged record type, in which case it declares a view of the primitive (equality) operator. [The rules specific to formal derived types are given in 12.5.1.]

Ramification: AI95-00442-01 All properties of the type are as for any type in the category class. Some examples: The primitive operations available are as defined by the language for each category class. The form of constraint applicable to a formal type in a subtype indication depends on the category class of the type as for a nonformal type. The formal type is tagged if and only if it is declared as a tagged private type, or as a type derived from a (visibly) tagged type. (Note that the actual type might be tagged even if the formal type is not.)

AI12-0413-1 If the primitive equality operator of the (actual) untagged record type is declared abstract, then Program_Error will be raised if the equality operator of the formal type is in fact invoked within an instance of a generic body (see 4.5.2). If the operator is invoked within an instance of the generic spec, the instance is illegal.
Reason: \{AI05-0029-1\} The somewhat cryptic phrase “even if it is never declared” is intended to deal with the following oddity:

```ada
package Q is
  type T is limited private;
  type T is range 1 .. 10;
private
generic
  type A is array (Positive range <>) of T;
package Q.G is
  A1, A2 : A (1 .. 1);
private
  B : Boolean := A1 = A2;
end Q.G;
end Q;
end
```

An “=” is available for the formal type `A` in the private part of `Q.G`. However, no “=” operator is ever declared for type `C`, because its component type `Q.T` is limited. Still, in the instance `I` the name “=” declares a view of the “=” for `C` which exists-but-is-never-declared.

**NOTE 1** Generic formal types, like all types, are not named. Instead, a name can denote a generic formal subtype. Within a generic unit, a generic formal type is considered as being distinct from all other (formal or nonformal) types.

**Proof:** This follows from the fact that each `formal_type_declaration` declares a type.

**NOTE 2** A discriminant part is allowed only for certain kinds of types, and therefore only for certain kinds of generic formal types. See 3.7.

**Ramification:** \{AI12-0005-1\} The term “formal floating point type” refers to a type defined by a `formal_floating_point_definition`. It does not include a formal derived type whose ancestor is a `floating_point_type`. Similar terminology applies to the other kinds of `formal_type_definition`.

**Examples**

```ada
type Item is private;
type Buffer (Length : Natural) is limited private;
type Enum is (<>);
type Int is range <>;
type Angle is delta <>;
type Mass is digits <>;
type Table is array (Enum) of Item;
```

**Example of a generic formal part declaring a formal integer type:**

```ada
generic
  type Rank is range <>;
First : => Rank := Rank'First;
Second : => Rank := First + 1;  -- the operator "+" of the type Rank
```

Wording Changes from Ada 83

RM83 has separate sections “Generic Formal Xs” and “Matching Rules for Formal Xs” (for various X’s) with most of the text redundant between the two. We have combined the two in order to reduce the redundancy. In RM83, there is no “Matching Rules for Formal Types” section; nor is there a “Generic Formal Y Types” section (for Y = Private, Scalar, Array, and Access). This causes, for example, the duplication across all the “Matching Rules for Y Types” sections of the rule that the actual passed to a formal type shall be a subtype; the new organization avoids that problem.

The matching rules are stated more concisely.

We no longer consider the multiplying operators that deliver a result of type `universal_fixed` to be predefined for the various types; there is only one of each in package Standard. Therefore, we need not mention them here as RM83 had to.
12.5.1 Formal Private and Derived Types

{AI95-00442-01} {AI05-0213-1} {AI12-0445-1} [In its most general form, the category determined for a formal private type is all types, but the category can be restricted to only nonlimited types or to only tagged types; can be either limited or nonlimited, and either tagged or untagged; no more specific class is known for such a type. Similarly, the category for a formal incomplete type is all types but the category can be restricted to only tagged types; unlike other formal types, the actual type can be incompletely defined and not ready does not need to be able to be frozen (see 13.14). The category determined for a formal derived type is the derivation class rooted at the ancestor type.]

Proof: {AI95-00442-01} {AI05-0213-1} The first two rules are given normatively below, and the third second rule is given normatively in 12.5; they are repeated here to give a capsule summary of what this subclause is about.

Ramification: {AI05-0213-1} Since the actual of a formal incomplete type does not need to be able to be frozen, the actual can be an incomplete type or a partial view before its completion.

Syntax

formal_private_type_definition ::= [[abstract] [tagged] [limited] private

formal_derived_type_definition ::= __[abstract] [limited | synchronized] new subtype_mark [and interface_list] with private

Legality Rules

If a generic formal type declaration has a known_discriminant_part, then it shall not include a default_expression for a discriminant.
4.a | **Ramification:** Consequently, a generic formal subtype with a known_discriminant_part is an indefinite subtype, so the declaration of a stand-alone variable has to provide a constraint on such a subtype, either explicitly, or by its initial value.

5.a | **Reason:** We use the term “ancestor” here instead of “parent” because the actual can be any descendant of the ancestor, not necessarily a direct descendant.

5.b/3 | **AI95-00419-01** | **AI05-0005-1** | **AI95-00049-01** | We require the ancestor type to be limited when **limited** appears so that we avoid oddities like integer types. Normally, **limited** means “match anything” for a generic formal, but it was felt that allowing limited elemental types to be declared was just too weird. Integer still matches a formal limited private type; it is only a problem when the type is known to be elementary. Note that the progenitors are required to be limited by rules in 3.9.4, thus that part of the rule is redundant.

5.c/2 | **AI95-00443-01** | We require that **synchronized** appear if the ancestor or any of the progenitors are synchronized, so that property is explicitly given in the program text — it is not automatically inherited from the ancestors. However, it can be given even if neither the ancestor nor the progenitors are synchronized.

5.1/5 | **AI95-00251-01** | **AI95-00401-01** | **AI95-00443-01** | **AI05-0087-1** | **AI12-0036-1** | **AI12-00442-1** | The actual type for a formal derived type shall be a descendant of [the ancestor type and] every progenitor of the formal type. **If the formal type is nonlimited, the actual type shall be nonlimited.** The actual type for a formal derived type shall be tagged if and only if the formal derived type is a private extension. **If the reserved word **synchronized** appears in the declaration of the formal derived type, the actual type shall be a synchronized tagged type.**

5.d/2 | **Proof:** The actual type has to be a descendant of the ancestor type, in order that it be in the correct class. Thus, that part of the rule is redundant.

5.e/3 | **Discussion:** **AI05-0005-1** | For a nonformal private extension, we require the partial view to be synchronized if the full view is synchronized tagged. This does not apply to a formal private extension — it is OK if the formal is not synchronized. Any attempt to extend the formal type will be rechecked in the instance, where the rule disallowing extending a synchronized noninterface type will be enforced. This is consistent with the “no hidden interfaces” rule also applying only to nonformal private extensions, as well as the rule that a limited nonformal private extension implies a limited full type. Formal private extensions are exempted from all these rules to enable the construction of generics that can be used with the widest possible range of types. In particular, an indefinite tagged limited formal private type can match any “concrete” actual tagged type.

5.f/3 | **AI05-0087-1** | A type (including formal types) derived from a limited interface could be nonlimited; we do not want a limited type derived from such an interface to match a nonlimited formal derived type. Otherwise, we could assign limited objects. Thus, we have to explicitly ban this case.

5.g/5 | **AI12-0036-1** | **AI12-0005-1** | If we allowed actual types whose kind differs from that that differ from the kind of the formal derived type, we could allow type conversions that would not be allowed outside of the generic. That would be particularly problematical if the actual is a tagged type with extension components; we could have created an object of the type that is missing those components by converting from the ancestor type to a formal derived type that is not an extension.

6.5/ | **AI05-0213-1** | **AI12-00442-1** | If the formal subtype is definite, then the actual subtype shall also be definite. **If the formal type is nonlimited, the actual type shall be nonlimited.**

6.a | **Ramification:** On the other hand, for an indefinite formal subtype, the actual can be either definite or indefinite.

6.b/5 | **Discussion:** **AI12-00442-1** | The rule about nonlimited formals applies to both private and derived formal types.
A formal incomplete type declaration declares a formal incomplete type. The only view of a formal incomplete type is an incomplete view. [Thus, a formal incomplete type is subject to the same usage restrictions as any other incomplete type — see 3.10.1.]

For a generic formal derived type with no discriminant_part, the actual subtype shall be statically compatible with the ancestor subtype. Furthermore:

- If the ancestor subtype is constrained, the actual subtype shall be constrained, and shall be statically compatible with the ancestor.
  
  Ramification: In other words, any constraint on the ancestor subtype is considered part of the “contract”. Predicates are also considered part of the contract for any subtype, via the static compatibility requirement.

- If the ancestor subtype is an unconstrained access or composite subtype, the actual subtype shall be unconstrained.
  
  Reason: This rule ensures that if a composite constraint is allowed on the formal, one is also allowed on the actual. If the ancestor subtype is an unconstrained scalar subtype, the actual is allowed to be constrained, since a scalar constraint does not cause further constraints to be illegal.

- If the ancestor subtype is an unconstrained discriminated subtype, then the actual shall have the same number of discriminants, and each discriminant of the actual shall correspond to a discriminant of the ancestor, in the sense of 3.7.
  
  Reason: This ensures that if a discriminant constraint is given on the formal subtype, the corresponding constraint in the instance will make sense, without additional runtime checks. This is not necessary for arrays, since the bounds cannot be overridden in a type extension. An unknown_discriminant_part may be used to relax these matching requirements.

- If the ancestor subtype is an access subtype, the actual subtype shall exclude null if and only if the ancestor subtype excludes null.
  
  Reason: We require that the “excludes null” property match, because it would be difficult to write a correct generic for a formal access type without knowing this property. Many typical algorithms and techniques will not work for a subtype that excludes null (setting an unused component to null, default-initialized objects, and so on). We want this sort of requirement to be reflected in the contract of the generic.

The declaration of a formal derived type shall not have a known_discriminant_part. For a generic formal private or incomplete type with a known_discriminant_part:

- The actual type shall be a type with the same number of discriminants.

- The actual subtype shall be unconstrained.

- The subtype of each discriminant of the actual type shall statically match the subtype of the corresponding discriminant of the formal type.

  Reason: We considered defining the first and third rule to be called “subtype conformance” for discriminant_parts. We rejected that idea, because it would require implicit (inherited) discriminant_parts, which seemed like too much mechanism.

[For a generic formal type with an unknown_discriminant_part, the actual may, but need not, have discriminants, though that is not required, and may be definite or indefinite.]

When enforcing Legality Rules, for the purposes of determining within a generic body whether a type is unconstrained in any partial view, a discriminated subtype is considered to have a constrained partial view if it is a descendant of an untagged generic formal private or derived type.

### Static Semantics

The category_class determined for a formal private type is as follows:

<table>
<thead>
<tr>
<th>Type Definition</th>
<th>Determined CategoryClass</th>
</tr>
</thead>
<tbody>
<tr>
<td>limited private</td>
<td>the category_class of all types</td>
</tr>
</tbody>
</table>
private

tagged limited private

tagged private

[The presence of the reserved word abstract determines whether the actual type may be abstract.]

A formal private or derived type is a private or derived type, respectively. A formal derived tagged type is a private extension. [A formal private or derived type is abstract if the reserved word abstract appears in its declaration.]

For a formal derived type, the characteristics if the ancestor type is a composite type that is not an array type, the formal type inherits components from the ancestor type (including components, but excluding discriminants if there is a new discriminant part is not specified), predefined operators, and inherited user-defined primitive subprograms are determined by its ancestor type and its progenitor types (if any), in the same way that those of a derived type are determined by those of its parent type and its progenitor types defined by a derived type declaration (see 3.4 and 7.3.1). In an instance, the copy of such an implicit declaration of a primitive subprogram of a formal derived type declares a view of the corresponding primitive subprogram of the ancestor or progenitor of the formal derived type, even if this primitive has been overridden for the actual type and even if it is never declared for the actual type. When the ancestor or progenitor of the formal derived type is itself a formal type, the copy of the implicit declaration declares a view of the corresponding copied operation of the ancestor or progenitor. [In the case of a formal private extension, however, the tag of the formal type is that of the actual type, so if the tag in a call is statically determined to be that of the formal type, the body executed will be that corresponding to the actual type.]

The above rule defining the properties of primitive subprograms in an instance applies even if the subprogram has been overridden or hidden for the actual type. This rule is necessary for untagged types, because their primitive subprograms might have been overridden by operations that are not subtype conformant subtype conformant with the operations defined for the class. For tagged types, the rule still applies, but the primitive subprograms will dispatch to the appropriate implementation based on the type and tag of the operands. Even for tagged types, the formal parameter names and default expressions are determined by those of the primitive subprograms of the specified ancestor type (or progenitor type, for subprograms inherited from an interface type).

The availability of stream attributes is not formally a characteristic of a type, but it is still determined by the ancestor type for a formal derived type in the same way as the characteristics are. Availability is rechecked in the instance specification.

In an instance, the implicitly composed and additive aspects (see 13.1.1) of a formal type are those of the actual; for a nonoverridable aspect, a formal derived type inherits the aspect if the ancestor or any progenitor has the aspect, according to the rules given in 13.1.

For a prefix S that denotes a formal indefinite subtype, the following attribute is defined:

S'Define yields True if the actual subtype corresponding to S is definite; otherwise, it yields False. The value of this attribute is of the predefined type Boolean.

Whether an actual subtype is definite or indefinite may have a major effect on the algorithm used in a generic. For example, in a generic I/O package, whether to use fixed-length or
variable-length records could depend on whether the actual is definite or indefinite. This attribute is essentially a replacement for the Constrained attribute, which is now considered obsolete.

Dynamic Semantics

\{AI95-00158-01\} \{AI05-0071-1\} \textit{In the case where a formal type basis tagged with unknown discriminants, and the actual type is a class-wide type }T\textit{Class:}

\begin{itemize}
  \item \{AI95-00158-01\} For the purposes of defining the primitive operations of the formal type, each of the primitive operations of the actual type is considered to be a subprogram (with an intrinsic calling convention — see 6.3.1) whose body consists of a dispatching call upon the corresponding operation of }T\textit{, with its formal parameters as the actual parameters. If it is a function, the result of the dispatching call is returned.}
  \item \{AI95-00158-01\} If the corresponding operation of }T\textit{ has no controlling formal parameters, then the controlling tag value is determined by the context of the call, according to the rules for tag-indeterminate calls (see 3.9.2 and 5.2). In the case where the tag would be statically determined to be that of the formal type, the call raises Program\_Error. If such a function is renamed, any call on the renaming raises Program\_Error.
\end{itemize}

\textbf{Discussion:} As it states in 6.3.1, the convention of an inherited subprogram of a generic formal tagged type with unknown discriminants is intrinsic.

In the case of a corresponding primitive of }T\textit{ with no controlling formal parameters, the context of the call provides the controlling tag value for the dispatch. If no tag is provided by context, Program\_Error is raised rather than resorting to a nondispatching call. For example:

\begin{verbatim}
generic
    type NT(<>) is new T with private;
    -- Assume }T\textit{ has operation "function Empty return }T;\textit;"
package G is
    procedure Test(X : in out NT);
end G;
package body G is
    procedure Test(X : in out NT) is
        X := Empty;  -- Dispatching based on X'Tag takes place if actual is class-wide.
        declare
            Y : NT := Empty;
            -- If actual is class-wide, this raises Program\_Error
            -- as there is no tag provided by context.
            begin
                X := Y;  -- We never get this far.
            end;
        end Test;
end G;
end G;
type T1 is new T with null record;
package I is new G(T1'Class);
\end{verbatim}

\textbf{NOTE 1} \{AI95-00442-01\} \{AI12-0442-1\} In accordance with the general rule that the actual type shall belong to the category class determined for the formal (see 12.5, “Formal Types”):

\begin{itemize}
  \item \{AI12-0442-1\} If the formal type is nonlimited, then so shall be the actual;
  \item \{AI12-0442-1\} For a formal derived type, the actual shall be in the class rooted at the ancestor subtype.
\end{itemize}

\textbf{NOTE 2} The actual type can be abstract only if the formal type is abstract (see 3.9.3).

\textbf{Reason:} This is necessary to avoid contract model problems, since one or more of its primitive subprograms are abstract; it is forbidden to create objects of the type, or to declare functions returning the type.

\textbf{Ramification:} On the other hand, it is OK to pass a nonabstract actual to an abstract formal — abstract on the formal indicates that the actual might be abstract.

\textbf{NOTE 3} \{AI12-0447-1\} If the formal has a discriminant\_part, the actual can be either definite or indefinite. Otherwise, the actual can only be definite.

\textit{Incompatibilities With Ada 83}

Ada 83 does not have unknown\_discriminant\_parts, so it allows indefinite subtypes to be passed to definite formals, and applies a legality rule to the instance body. This is a contract model violation. Ada 95 disallows such cases at the
The check for discriminant subtype matching is changed from a runtime check to a compile-time check.

**Extensions to Ada 95**

- {AI95-00250-01} {AI95-00419-01} {AI95-00443-01} A generic formal derived type can include progenitors (interfaces) as well as a primary ancestor. It also may include limited to indicate that it is a limited type, and synchronized to indicate that it is a synchronized type.

**Wording Changes from Ada 95**

- {8652/0038} {AI95-00202-01} **Corrigendum:** Corrected wording to define the operations that are inherited when the ancestor of a formal type is itself a formal type to avoid anomalies.
- {AI95-00158-01} Added a semantic description of the meaning of operations of an actual class-wide type, as such a type does not have primitive operations of its own.
- {AI95-00231-01} Added a matching rule for access subtypes that exclude null.
- {AI95-00233-01} The wording for the declaration of implicit operations is corrected to be consistent with 7.3.1 as modified by Corrigendum 1.
- {AI95-00442-01} We change to “determines a category” as that is the new terminology (it avoids confusion, since not all interesting properties form a class).

**Incompatibilities With Ada 2005**

- {AI05-0087-1} **Correction:** Added wording to prevent a limited type from being passed to a nonlimited formal derived type. While this was allowed, it would break the contract for the limited type, so hopefully no programs actually depend on that.

**Extensions to Ada 2005**

- {AI05-0213-1} Formal incomplete types are a new kind of generic formal; these can be instantiated with incomplete types and unfrozen private types.

**Wording Changes from Ada 2005**

- {AI05-0029-1} **Correction:** Updated the wording to acknowledge the possibility of operations that are never declared for an actual type but still can be used inside of a generic unit.
- {AI05-0071-1} **Correction:** Fixed hole that failed to define what happened for "" in an untagged private type whose actual is class-wide.
- {AI05-0110-1} **Correction:** Revised the wording for inheritance of characteristics and operations of formal derived types to be reuse the rules as defined for derived types; this should eliminate holes in the wording which have plagued us since Ada 95 was defined (it has been "corrected" four previous times).
- {AI05-0237-1} **Correction:** Added missing rule for the ancestors of formal derived types. The added rule would formally be incompatible, but since it would be impossible to instantiate any such generic, this cannot happen outside of test suites and thus is not documented as an incompatibility.

**Incompatibilities With Ada 2012**

- {AI12-0036-1} **Corrigendum:** Added a requirement that a tagged type only match a formal derived type that is a private extension. This is necessary to prevent type conversions that would not be allowed outside of the generic. We expect that this will be rare, as it only can happen if the formal derived type does not accurately describe the actual type; in most such cases, extension will be desired and a private extension used so that is allowed.
- {AI12-0351-1} **Correction:** The predicates of an ancestor subtype are considered part of the contract for a formal derived type, even if the ancestor subtype is unconstrained. This means, for instance, if the ancestor subtype is a subtype of Float with a predicate, then an actual subtype with a different predicate is illegal in Ada 2022 while it would have been allowed in Ada 2012. Cases like this are quite unlikely and will be detected at compile-time if they occur.

**Wording Changes from Ada 2012**

- {AI12-0095-1} **Corrigendum:** The assume the worst rule for determining within a generic body whether a type is unconstrained in any partial view was moved here. While AI05-0041-1 added it to 3.10.2, it's also needed (at least) in 4.6 and 6.4.1. Thus, it was moved here so that it applies generally.
12.5.2 Formal Scalar Types

{AI95-00442-01} A formal scalar type is one defined by any of the formal_type_definitions in this subclause. [The category_class determined for a formal scalar type is the category of all discrete, signed integer, modular, floating point, ordinary fixed point, or decimal types.]

Proof: {AI95-00442-01} The second rule follows from the rule in 12.5 that says that the category is determined by the one given in the name of the syntax production. The effect of the rule is repeated here to give a capsule summary of what this subclause is about.

Ramification: {AI95-00442-01} The “category of a type” includes any classes that the type belongs to.

Syntax

formal_discrete_type_definition ::= (<>)
formal_signed_integer_type_definition ::= range <>
formal_modular_type_definition ::= mod <>
formal_floating_point_definition ::= digits <>
formal_ordinary_fixed_point_definition ::= delta <>
formal_decimal_fixed_point_definition ::= delta <> digits <>

Legality Rules

The actual type for a formal scalar type shall not be a nonstandard numeric type.

Reason: This restriction is necessary because nonstandard numeric types have some number of restrictions on their use, which could cause contract model problems in a generic body. Note that nonstandard numeric types can be passed to formal derived and formal private subtypes, assuming they obey all the other rules, and assuming the implementation allows it (being nonstandard means the implementation might disallow anything).

NOTE {AI12-0442-1} The actual shall be in the class of types implied by the syntactic category of the formal_type_definition (see 12.5, “Formal Types”). For example, the actual for a formal_modular_type_definition shall be a modular type.

Wording Changes from Ada 95

{AI95-00442-01} We change to “determines a category” as that is the new terminology (it avoids confusion, since not all interesting properties form a class).

12.5.3 Formal Array Types

{AI95-00442-01} [The category_class determined for a formal array type is the category_class of all array types.]

Proof: {AI95-00442-01} This rule follows from the rule in 12.5 that says that the category is determined by the one given in the name of the syntax production. The effect of the rule is repeated here to give a capsule summary of what this subclause is about.

Syntax

formal_array_type_definition ::= array_type_definition

Legality Rules

The only form of discrete_subtype_definition that is allowed within the declaration of a generic formal (constrained) array subtype is a subtype_mark.

Reason: The reason is the same as for forbidding constraints in subtype_indications (see 12.1).

For a formal array subtype, the actual subtype shall satisfy the following conditions:
The formal array type and the actual array type shall have the same dimensionality; the formal subtype and the actual subtype shall be either both constrained or both unconstrained.

For each index position, the index types shall be the same, and the index subtypes (if unconstrained), or the index ranges (if constrained), shall statically match (see 4.9.1).

The component subtypes of the formal and actual array types shall statically match.

If the formal type has aliased components, then so shall the actual.

**Ramification:** On the other hand, if the formal's components are not aliased, then the actual's components can be either aliased or not.

### Examples

#### Example of formal array types:

```ada
generic
  type Item is private;
  type Index is <>;
  type Vector is array (Index range <>) of Item;
  type Table is array (Index) of Item;
package P is
  ...;
end P;
```

```
-- and the types

  type Mix is array (Color range <>) of Boolean;
  type Option is array (Color) of Boolean;
```

-- then Mix can match Vector and Option can match Table

```ada
package R is new P(Item => Boolean, Index => Color, Vector => Mix, Table => Option);
```

-- Note that Mix cannot match Table and Option cannot match Vector

### Incompatibilities With Ada 83

The check for matching of component subtypes and index subtypes or index ranges is changed from a runtime check to a compile-time check. The Ada 83 rule that “If the component type is not a scalar type, then the component subtypes shall be either both constrained or both unconstrained” is removed, since it is subsumed by static matching. Likewise, the rules requiring that component types be the same is subsumed.

### Wording Changes from Ada 95

{A195-00442-01} We change to “determines a category” as that is the new terminology (it avoids confusion, since not all interesting properties form a class).

## 12.5.4 Formal Access Types

{A195-00442-01} [The category class determined for a formal access type is the category class of all access types.]

### Proof: {A195-00442-01}

This rule follows from the rule in 12.5 that says that the category is determined by the one given in the name of the syntax production. The effect of the rule is repeated here to give a capsule summary of what this subclause is about.

### Syntax

```
formal_access_type_definition ::= access_type_definition
```

### Legality Rules

For a formal access-to-object type, the designated subtypes of the formal and actual types shall statically match.
{AI95-00231-01} If and only if the `general_access_modifier constant` applies to the formal, the actual shall be an access-to-constant type. If the `general_access_modifier all` applies to the formal, then the actual shall be a general access-to-variable type (see 3.10). **If and only if the formal subtype excludes null, the actual subtype shall exclude null.**

**Ramification:** If no `_modifier` applies to the formal, then the actual type may be either a pool-specific or a general access-to-variable type.

**Reason:** {AI95-00025-01} Matching an access-to-variable to a formal access-to-constant type cannot be allowed. If it were allowed, it would be possible to create an access-to-variable value designating a constant.

{AI95-00231-01} We require that the “excludes null” property match, because it would be difficult to write a correct generic for a formal access type without knowing this property. Many typical algorithms and techniques will not work for a subtype that excludes null (setting an unused component to `null`, default-initialized objects, and so on). Even Ada.Unchecked DEALLOCATION would fail for a subtype that excludes null. Most generics would end up with comments saying that they are not intended to work for subtypes that exclude null. We would rather that this sort of requirement be reflected in the contract of the generic.

{AI05-0239-1} {AI05-0288-1} For a formal access-to-subprogram subtype, the designated profiles of the formal and the actual shall be **subtype conformant** and the calling convention of the actual shall be **protected** if and only if that of the formal is **protected**.

**Reason:** {AI05-0288-1} We considered requiring subtype conformance here, but mode conformance is more flexible, given that there is no way in general to specify the convention of the formal.

### Examples

**Example of formal access types:**

```ada
-- the formal types of the generic package
generic
    type Node is private;
    type Link is access Node;
package P is
   end P;
-- can be matched by the actual types
type Car;
type Car_Name is access Car;
type Car is record
    Pred, Succ : Car_Name;
    Number : License_Number;
    Owner : Person;
end record;
-- in the following generic instantiation
package R is new P(Node => Car, Link => Car_Name);
```

### Incompatibilities With Ada 83

The check for matching of designated subtypes is changed from a runtime check to a compile-time check. The Ada 83 rule that “If the designated type is other than a scalar type, then the designated subtypes shall be either both constrained or both unconstrained” is removed, since it is subsumed by static matching.

### Extensions to Ada 83

Formal access-to-subprogram subtypes and formal general access types are new concepts.

### Wording Changes from Ada 95

{AI95-00231-01} Added a matching rule for subtypes that exclude null.

{AI95-00442-01} We change to “determines a category” as that is the new terminology (it avoids confusion, since not all interesting properties form a class).
12.5.4 Formal Access Types

Incompatibilities With Ada 2005

{A105-0288-1} **Correction:** Matching of formal access-to-subprogram types now uses subtype conformance rather than mode conformance, which is needed to plug a hole. This could cause some instantiations legal in Ada 95 and Ada 2005 to be rejected in Ada 2012. We believe that formal access-to-subprogram types occur rarely, and actuals that are not subtype conformant are rarer still, so this should not happen often. (In addition, one popular compiler has a bug that causes such instances to be rejected, so no code compiled with that compiler could have an incompatibility.)

12.5.5 Formal Interface Types

{A195-00251-01} {A195-00442-01} [The category determined for a formal interface type is the category of all interface types.]

**Proof:** {A195-00442-01} This rule follows from the rule in 12.5 that says that the category is determined by the one given in the name of the syntax production. The effect of the rule is repeated here to give a capsule summary of what this subclause is about.

**Ramification:** Here we're taking advantage of our switch in terminology from “determined class” to “determined category”: by saying “category” rather than “class”, we require that any actual type be an interface type, not just some type derived from an interface type.

**Syntax**

{A195-00251-01} formal_interface_type_definition ::= interface_type_definition

**Legality Rules**

{A195-00251} {A195-00401} The actual type shall be a descendant of every progenitor of the formal type.

{A195-00345} The actual type shall be a limited, task, protected, or synchronized interface if and only if the formal type is also, respectively, a limited, task, protected, or synchronized interface.

**Discussion:** We require the kind of interface type to match exactly because without that it is almost impossible to properly implement the interface.

**Examples**

{A112-0429-1} {A112-0442-1} **Example of the use of a generic with a formal interface type, to establish a standard interface that all tasks will implement so they can be managed appropriately by an application-specific scheduler:**

{A195-00433-01} type Root_Work_Item is tagged private;

{A195-00433-01} generic
type Managed_Task is task interface;
type Work_Item<> is new Root_Work_Item with private;
package Server_Manager is
task type Server is new Managed_Task with
entry Start(Data : in out Work_Item);
end Server;
end Server_Manager;

{A195-00433-01} {A112-0429-1} **This generic allows an application to establish a standard interface that all tasks need to implement so they can be managed appropriately by an application-specific scheduler.**

**Extensions to Ada 95**

{A195-00251-01} {A195-00345-01} {A195-00401-01} {A195-00442-01} The formal interface type is new.

12.6 Formal Subprograms

[ Formal subprograms can be used to pass callable entities to a generic unit.]
Language Design Principles

Generic formal subprograms are like renames of the explicit_generic_actual_parameter.

Syntax

\{AI95-00260-02\} \texttt{formal\_subprogram\_declaration ::= formal\_concrete\_subprogram\_declaration | formal\_abstract\_subprogram\_declaration with subprogram\_specification [is subprogram\_default];}

\{AI95-00260-02\} \{AI05-0183-1\} \texttt{formal\_concrete\_subprogram\_declaration ::= with subprogram\_specification [is subprogram\_default];}

\{AI95-00260-02\} \{AI05-0183-1\} \texttt{formal\_abstract\_subprogram\_declaration ::= with subprogram\_specification is abstract [subprogram\_default];}

\{AI95-00348-01\} \texttt{subprogram\_default ::= default\_name | <> | null}

\texttt{default\_name ::= name}

\{AI95-00260-02\} \{AI95-00348-01\} \texttt{A subprogram\_default of null shall not be specified for a formal function or for a formal\_abstract\_subprogram\_declaration.}

\textbf{Reason}: There are no null functions because the return value has to be constructed somehow. We don't allow null for abstract formal procedures, as the operation is dispatching. It doesn't seem appropriate (or useful) to say that the implementation of something is null in the formal type and all possible descendants of that type. This also would define a dispatching operation that doesn't correspond to a slot in the tag of the controlling type, which would be a new concept. Finally, additional rules would be needed to define the meaning of a dispatching null procedure (for instance, the convention of such a subprogram should be intrinsic, but that's not what the language says). It doesn't seem worth the effort.

Name Resolution Rules

The expected profile for the default\_name, if any, is that of the formal subprogram.

\textbf{Ramification}: \{AI05-0299-1\} This rule, unlike others in this subclause, is observed at compile time of the generic\_declaration.

The evaluation of the default\_name takes place during the elaboration of each instantiation that uses the default, as defined in 12.3, “Generic Instantiation”.

For a generic formal subprogram, the expected profile for the actual is that of the formal subprogram.

Legality Rules

\{AI05-0239-1\} The profiles of the formal and any named default shall be \texttt{mode\_conformant}.\texttt{mode\_conformant}.

\textbf{Ramification}: \{AI05-0299-1\} This rule, unlike others in this subclause, is checked at compile time of the generic\_declaration.

\{AI05-0239-1\} The profiles of the formal and actual shall be \texttt{mode\_conformant}.\texttt{mode\_conformant}.

\{AI95-00423-01\} \texttt{For a parameter or result subtype of a formal\_subprogram\_declaration that has an explicit null\_exclusion;}

- \texttt{\{AI12-0183-1\} \{AI12-0287-1\} if the actual matching the formal\_subprogram\_declaration statically denotes a generic\_formal\_subprogram\_object of another generic unit G, and the instantiation containing the actual that\_occurs within the body of a generic unit G or within the body of a generic unit declared within the declarative region of the generic unit G, then the corresponding parameter or result type of the formal\_subprogram\_object of G shall have a null\_exclusion;
• otherwise, the subtype of the corresponding parameter or result type of the actual matching the formal subprogram declaration shall exclude null. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

**Reason:** This rule prevents “lying.” Null must never be the value of a parameter or result with an explicit null exclusion. The first bullet is an assume-the-worst rule which prevents trouble in generic bodies (including bodies of child generics) when the formal subtype excludes null implicitly.

{AI12-0204-1} If the named default, if any, is a prefixed view, the prefix of that view shall denote an object for which renaming is allowed (see 8.5.1). Similarly, if the actual subprogram in an instantiation is a prefixed view, the prefix of that view shall denote an object for which renaming is allowed.

**Reason:** {AI12-0204-1} The prefix in such a case is essentially renamed at the point of the instantiation and passed to any calls of the formal subprogram in the generic. If the prefix isn't legal to rename, that doesn't make sense (and allowing it might end up passing a nonexistent object to some calls).

{AI95-00260-02} {AI05-0296-1} If a formal parameter of a formal abstract subprogram declaration is of a specific tagged type \( T \) or of an anonymous access type designating a specific tagged type \( T \), \( T \) is called a controlling type of the formal abstract subprogram declaration. Similarly, if the result of a formal abstract subprogram declaration for a function is of a specific tagged type \( T \) or of an anonymous access type designating a specific tagged type \( T \), \( T \) is called a controlling type of the formal abstract subprogram declaration. A formal abstract subprogram declaration shall have exactly one controlling type, and that type shall not be incomplete.

**Ramification:** The specific tagged type could be any of a formal tagged private type, a formal derived type, a formal interface type, or a normal tagged type. While the last case doesn't seem to be very useful, there isn't any good reason for disallowing it. This rule ensures that the operation is a dispatching operation of some type, and that we unambiguously know what that type is.

We informally call a subprogram declared by a formal abstract subprogram declaration an abstract formal subprogram, but we do not use this term in normative wording. (We do use it often in these notes.)

{AI95-00260-02} {AI12-0165-1} The actual subprogram for a formal abstract subprogram declaration shall be: a dispatching operation of the controlling type or of the actual type corresponding to the controlling type.

• a dispatching operation of the controlling type; or

• if the controlling type is a formal type, and the actual type corresponding to that formal type is a specific type \( T \), a dispatching operation of type \( T \); or

• if the controlling type is a formal type, and the actual type is a class-wide type \( T \)\(^\text{'Class} \), an implicitly declared subprogram corresponding to a primitive operation of type \( T \) (see Static Semantics below).

**To be honest:** We mean the controlling type of the formal abstract subprogram declaration, of course. Saying that gets unwieldy and redundant (so says at least one reviewer, anyway).

**Ramification:** {AI12-0165-1} This means that the actual is a primitive operation of the controlling type, an abstract formal subprogram, or the implicitly available primitive operation for a class-wide type.

{AI12-0165-1} {AI12-0005-1} An explicit class-wide operation cannot be used for the actual of a formal abstract subprogram. Such an operation is never primitive (only specific types have primitive subprograms).

{AI12-0165-1} This means that the actual is either a primitive operation of the controlling type, or an abstract formal subprogram. Also note that this prevents the controlling type from being class-wide (with one exception explained below), as only specific types have primitive operations (and a formal subprogram eventually has to have an actual that is a primitive of some type). This could happen in a case like:

```
generic
  type T<> is tagged private;
  with procedure P00 (Ob) : in T is abstract;
package P ...;
```

package New_P is new P (Something'Class, Some_Proc);
If Some_Proc is an explicit class-wide operation, the instantiation here is always illegal, because Some_Proc is not a primitive operation of Something'Class (there are no such operations). That's good, because we want calls to Foo always to be dispatching calls.

However, if Some_Proc is a primitive operation of type Something, then the instantiation is legal; the actual is the implicitly generated subprogram described in Static Semantics below. This is not a problem, since the rules given in 12.5.1 explain how this routine dispatches even though its parameter is class-wide.

We allow this special case because it is possible for a class-wide operation to be primitive inside of an instance, and the contract model does not allow us to make such cases illegal. As such, it seems inconsistent to not allow the same in explicit instantiations.

Specifically, since it is possible for a formal tagged type to be instantiated with a class-wide type, it is possible for the (real) controlling type to be class-wide as in the following unusual case:

```ada
generic
  type NT<> is new T with private;
  -- Presume that T has the following primitive operation:
  with procedure Bar (Obj : in T);
package Gr ...
end Gr;
package body Gr is
  package New_P2 is new P (NT, Foo => Bar);
end Gr;
package New_Gr is new Gr (Something'Class);
```

The instantiation of New_P2 is legal, since Bar is a dispatching operation of the actual type of the controlling type of the abstract formal subprogram Foo. Again, this is not a problem, since the rules given in 12.5.1 explain how this routine dispatches even though its parameter is class-wide.

Note that this legality rule never needs to be rechecked in an instance (that contains a nested instantiation). The rule only talks about the actual type of the instantiation; it does not require looking further; if the actual type is in fact a formal type, we do not intend looking at the actual for that formal.

**Static Semantics**

A formal_subprogram_declaration declares a generic formal subprogram. The types of the formal parameters and result, if any, of the formal subprogram are those determined by the subtype_marks given in the formal_subprogram_declaration; however, independent of the particular subtypes that are denoted by the subtype_marks, the nominal subtypes of the formal parameters and result, if any, are defined to be nonstatic, and unconstrained if of an array type [no applicable index constraint is provided in a call on a formal subprogram]). In an instance, a formal_subprogram_declaration declares a view of the actual. The profile of this view takes its subtypes and calling convention from the original profile of the actual entity, while taking the formal parameter names and default_expressions from the profile given in the formal_subprogram_declaration. The view is a function or procedure, never an entry.

**Discussion:** This rule is intended to be the same as the one for renamings-as-declarations, where the formal_subprogram_declaration is analogous to a renaming-as-declaration, and the actual is analogous to the renamed view.

**Reason:** This gives the same capabilities to formal subprograms as those that primitive operations of the formal type have when the actual type is class-wide. We do not want to discourage the use of explicit declarations for (formal) subprograms!
If a generic unit has a subprogram_default specified by a box, and the corresponding actual parameter is omitted, then it is equivalent to an explicit actual parameter that is a usage name identical to the defining name of the formal.

Reason: This is necessary to trigger all of the dispatching operation rules. It otherwise would not be considered a dispatching operation, as formal subprograms are never primitive operations.

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:

Examples of generic formal subprograms:
-- given the generic procedure declaration

generic
  with procedure Action (X : in Item);
procedure Iterate(Seq : in Item_Sequence);
-- and the procedure
procedure Put_Item(X : in Item);
-- the following instantiation is possible
procedure Put_List is new Iterate(Action => Put_Item);

Extensions to Ada 95

{AI95-00260-02} The formal abstract subprogram declaration is new. It allows the passing of dispatching operations to generic units.

{AI95-00348-01} The formal subprogram default of null is new. It allows the default of a generic procedure to do nothing, such as for passing a debugging routine.

Wording Changes from Ada 95

{AI95-00423-01} Added matching rules for null exclusions.

Incompatibilities With Ada 2005

{AI05-0296-1} It is now illegal to declare a formal abstract subprogram whose controlling type is incomplete. It was never intended to allow that, and such a type would have to come from outside of the generic unit in Ada 2005, so it is unlikely to be useful. Moreover, a dispatching call on the subprogram is likely to fail in many implementations. So it is very unlikely that any code will need to be changed because of this new rule.

Extensions to Ada 2005

{AI05-0071-1} {AI05-0131-1} Correction: Added construction of implicit subprograms for primitives of class-wide actual types, to make it possible to import subprograms via formal subprograms as well as by implicit primitive operations of a formal type. (This is a Correction as it is very important for the usability of indefinite containers when instantiated with class-wide types; thus we want Ada 2005 implementations to support it.)

{AI05-0183-1} An optional aspect specification can be used in a formal_concrete_subprogram_declaration and a formal_abstract_subprogram_declaration. This is described in 13.1.1.

Incompatibilities With Ada 2012

{AI12-0204-1} Correction: Added a rule to ensure that for an actual subprogram that is a prefixed view, the prefix continues to exist during the life of the instantiation. If the prefix is a subcomponent that depends on discriminants, Ada 2005 and 2012 would have allowed the prefix while Ada 2022 would not. Without this change, explicit forms (renaming the object and then using that in instantiations) would be safer than directly using the prefixed view; that's inconsistent with other kinds of actual subprograms.

Extensions to Ada 2012

{AI12-0165-1} Correction: We now allow the actual for a formal abstract subprogram declaration to be an implicitly declared subprogram for a class-wide type. The rules already required a compiler to be able to construct this subprogram for use in an instantiation that occurs inside of a generic unit, so it made no sense to prevent it from being used explicitly as well (in the same way that the previous extension allows them to be used for other kinds of formal subprograms).

Wording Changes from Ada 2012

{AI12-0287-1} Correction: Added wording to ensure that the object subject to a Legality Rule can be determined at compile-time. The alternative being nonsense, we treat this as a wording change.

12.7 Formal Packages

[ Formal packages can be used to pass packages to a generic unit. The formal_package_declaration declares that the formal package is an instance of a given generic package. Upon instantiation, the actual package has to be an instance of that generic package.]
Syntax

```
{AI05-0183-1} formal_package_declaration ::=  
  with package defining_identifier is new generic_package_name formal_package_actual_part  
  [aspect_specification];
```

```
{AI95-00317-01} formal_package_actual_part ::=  
  ([others => <>] <>)  
  | [generic_actual_part]  
  | {formal_package_association {, formal_package_association} [, others => <>]}(<>)[generic_actual_part]
```

```
{AI95-00317-01} formal_package_association ::=  
  generic_association  
  | generic_formal_parameter_selector_name => <>
```

Legality Rules

The `generic_package_name` shall denote a generic package (the *template* for the formal package); the formal package is an instance of the template.

```
{AI05-0025-1} The generic_formal_parameter_selector_name of a formal_package_association shall  
  denote a generic_formal_parameter_declaration of the template. If two or more formal subprograms  
  of the template have the same defining name, then named associations are not allowed for the corresponding  
  actuals.
```

```
{AI95-00398-01} A formal_package_actual_part shall contain at most one  
  formal_package_association for each formal parameter. If the formal_package_actual_part does not  
  include “others => <>”, each formal parameter without an association shall have a default_expression or  
  subprogram_default.
```

```
{AI05-0200-1} The rules for matching between formal_package_associations and the generic formals of  
  the template are as follows:
```

- If all of the formal_package_associations are given by generic associations, the  
  explicit generic_actual_parameters of the formal_package_associations shall be legal for an  
  instantiation of the template.

- `{AI05-0200-1}` If a formal_package_association for a formal type \( T \) of the template is given by  
  `<>`, then the formal_package_association for any other generic_formal_parameter_declaration  
  of the template that mentions \( T \) directly or indirectly shall also be given by `<>` as well.

```
Discussion: `{AI05-0200-1}` The above rule is simple to state, though it does not reflect the fact that the formal package  
  functions like an instantiation of a special kind, where each box association for a  
  generic_formal_parameter_declaration \( F \) is replaced with a new entity \( F' \) that has the same characteristics as \( F \); if \( F \) is  
  a formal discrete type then \( F' \) is a discrete type, if \( F \) is a formal subprogram then \( F' \) is a subprogram with a similar  
  signature, etc. In practice this is achieved by making the association into a copy of the declaration of the generic  
  formal.
```

```
{AI95-00317-01} The actual shall be an instance of the template. If the formal_package_actual_part is  
  `<>` or `(others => <>), then the actual may be any instance of the template; otherwise, certain of the  
  actual_parameters each actual parameter of the actual instance shall match the corresponding actual  
  parameters parameter of the formal package, determined [((whether the actual parameter is given explicitly  
  or by default)], as follows:
```
• \{\textit{AI95-00317-01}\} If the \textit{formal\_package\_actual\_part} includes \textit{generic\_associations} as well as associations with \texttt{<>}, then only the actual parameters specified explicitly with \textit{generic\_associations} are required to match;

• \{\textit{AI95-00317-01}\} Otherwise, all actual parameters shall match[, whether any actual parameter is given explicitly or by default].

\{\textit{AI95-00317-01}\} The rules for matching of actual parameters between the actual instance and the \textit{formal\_package} are as follows:

• \{\textit{AI95-00317-01}\} For a formal object of mode \texttt{in\_}, the actuals match if they are static expressions with the same value, or if they statically denote the same constant, or if they are both the literal \texttt{null}.

  \textit{Reason:} We can't simply require full conformance between the two actual parameter expressions, because the two expressions are being evaluated at different times.

• For a formal subtype, the actuals match if they denote statically matching subtypes.

• For other kinds of formals, the actuals match if they statically denote the same entity.

\{\textit{8652/0039}\} \{\textit{AI95-00213-01}\} For the purposes of matching, any actual parameter that is the name of a formal object of mode \texttt{in} is replaced by the formal object's actual expression (recursively).

\textit{Static Semantics}

A \textit{formal\_package\_declaration} declares a generic formal package.

\{\textit{AI95-00317-01}\} The visible part of a formal package includes the first list of \textit{basic\_declarative\_items} of the \textit{package\_specification}. In addition, for each actual parameter that is not required to match, a copy of the declaration of the corresponding formal parameter of the template is included in the visible part of the formal package. If the copied declaration is for a formal type, copies of the implicit declarations of the primitive subprograms of the formal type are also included in the visible part of the \textit{formal\_package}. If the \textit{formal\_package\_actual\_part} is (<>), it also includes the \textit{generic\_formal\_part} of the template for the formal package.

\textit{Ramification:} \{\textit{AI95-00317-01}\} If the \textit{formal\_package\_actual\_part} is (<>), then the declarations that occur immediately within the \textit{generic\_formal\_part} of the template for the formal package are visible outside the formal package, and can be denoted by expanded names outside the formal package. \text{\textit{If only some of the actual parameters are given by <>}, then the declaration corresponding to those parameters (but not the others) are made visible.}

\textit{Reason:} \{\textit{AI05-0005-I}\} We always want either the actuals or the formals of an instance to be \texttt{nameable} at least one of outside, but never both. If both were \texttt{nameable} from outside, one would get some funny anomalies since they denote the same entity, but, in the case of types at least, they might have different and inconsistent sets of primitive operators due to predefined operator “reemergence”. Formal derived types exacerbate the difference. We want the implicit declarations of the \textit{generic\_formal\_part} as well as the explicit declarations, so we get operations on the formal types.

\textit{Ramification:} A generic formal package is a package, and is an instance. Hence, it is possible to pass a generic formal package as an actual to another generic formal package.

\{\textit{AI95-00317-01}\} \textit{For the purposes of matching, if the actual instance A is itself a formal package, then the actual parameters of A are those specified explicitly or implicitly in the \textit{formal\_package\_actual\_part} for A, plus, for those not specified, the copies of the formal parameters of the template included in the visible part of A.}
Examples

Example of a generic package with formal package parameters:

```ada
with Ada.Containers.Ordered_Maps;  -- see A.18.6
generic
with package Mapping_1 is new Ada.Containers.Ordered_Maps(<>);
with package Mapping_2 is new Ada.Containers.Ordered_Maps
(Key_Type => Mapping_1.Element_Type,
others => <>);
package Ordered_Join is
   -- Provide a "join" between two mappings
   subtype Key_Type is Mapping_1.Key_Type;
   subtype Element_Type is Mapping_2.Element_Type;
   function Lookup(Key : Key_Type) return Element_Type;
end Ordered_Join;
```

Example of an instantiation of a package with formal packages:

```ada
with Ada.Containers.Ordered_Maps;
package Symbol_Package is
   subtype Key_String is String(1..5);
   type String_Id is ...
   subtype String_Info is ...
   package String_Table is new Ada.Containers.Ordered_Maps
   (Key_Type => Key_String,
   Element_Type => String_Id);
   package Symbol_Table is new Ada.Containers.Ordered_Maps
   (Key_Type => String_Id,
   Element_Type => Symbol_Info);
   package String_Info is new Ordered_Join(Mapping_1 => String_Table,
   Mapping_2 => Symbol_Table);
   Apple_Info : constant Symbol_Info := String_Info.Lookup("Apple");
end Symbol_Package;
```

Extensions to Ada 93

Formal packages are new to Ada 95.

Extensions to Ada 95

It's now allowed to mix actuals of a formal package that are specified with those that are not specified.

Wording Changes from Ada 95

Corrigendum: Corrected the description of formal package matching to say that formal parameters are always replaced by their actual parameters (recursively). This matches the actual practice of compilers, as the ACATS has always required this behavior.

The description of which operations are visible in a formal package has been clarified. We also specify how matching is done when the actual is a formal package.

Incompatibilities With Ada 2005

Correction: Added missing rules for parameters of generic formal package that parallel those in 12.3, as well as some specific to <> parameters. These are technically incompatibilities because generic formal package parameters that Ada 95 and Ada 2005 would have considered legal now have to be rejected. But this should not be an issue in practice as such formal parameters could not have matched any actual generics. And it is quite likely that implementations already enforce some of these rules.
12.8 Example of a Generic Package

The following example provides a possible formulation of stacks by means of a generic package. The size of each stack and the type of the stack elements are provided as generic formal parameters.

This paragraph was deleted.

```ada
generic
  Size : Positive;
package Stack is
  type Item is private;
  procedure Push(E : in Item);
  procedure Pop (E : out Item);
  Overflow, Underflow : exception;
end Stack;
package body Stack is
  type Table is array (Positive range <>) of Item;
  Space : Table(1 .. Size);
  Index : Natural := 0;
  procedure Push(E : in Item) is
    begin
      if Index >= Size then
        raise Overflow;
      end if;
      Index := Index + 1;
      Space(Index) := E;
    end Push;
  procedure Pop(E : out Item) is
    begin
      if Index = 0 then
        raise Underflow;
      end if;
      E := Space(Index);
      Index := Index - 1;
    end Pop;
end Stack;

Instances of this generic package can be obtained as follows:

package Stack_Int is new Stack(Size => 200, Item => Integer);
package Stack_Bool is new Stack(100, Boolean);

Thereafter, the procedures of the instantiated packages can be called as follows:

Stack_Int.Push(N);
Stack_Bool.Push(True);
```
Alternatively, a generic formulation of the type Stack can be given as follows (package body omitted):

```ada
generic
type Item is private;
package On_Stacks is
type Stack(Size : Positive) is limited private;
procedure Push(S : in out Stack; E : in Item);
procedure Pop (S : in out Stack; E : out Item);
Overflow, Underflow : exception;
private
type Table is array (Positive range <>) of Item;
type Stack(Size : Positive) is
  record
    Space : Table(1 .. Size);
    Index : Natural := 0;
  end record;
end On_Stacks;
```

In order to use such a package, an instance has to be created and thereafter stacks of the corresponding type can be declared:

```ada
declare
  package Stack_Real is new On_Stacks(Real); use Stack_Real;
  S : Stack(100);
begin
  ...
  Push(S, 2.54);
  ...
end;
```
13 Representation Issues

{8652/0009} {AI95-00137-01} {AI05-0299-1} [This clause describes features for querying and controlling certain aspects of entities and for interfacing to hardware.]

Wording Changes from Ada 83

{AI05-0299-1} The subclauses of this clause have been reorganized. This was necessary to preserve a logical order, given the new Ada 95 semantics given in this section.

13.1 Operational and Representation Aspects

{8652/0009} {AI95-00137-01} {AI05-0295-1} {AI22-0018-1} [Representation and operational items can be used to specify aspects of entities.] Two kinds of aspects of entities can be specified: aspects of representation and operational aspects. Representation aspects affect how the types and other entities of the language are to be mapped onto the underlying machine. Operational aspects determine other properties of entities. When not specified otherwise, an aspect is defined to be an operational aspect.

Term entry: operational aspect — aspect that indicates a logical property of an entity, such as the precondition of a subprogram, or the procedure used to write a given type of object to a stream

Term entry: representation aspect — aspect that indicates how an entity is mapped onto the underlying hardware, for example the size or alignment of an object

{AI05-0183-1} {AI05-0295-1} [Either kind of aspect of an entity may be specified by means of an aspect specification (see 13.1.1), which is an optional element of most kinds of declarations and applies to the entity or entities being declared. Aspects may also be specified by certain other constructs occurring subsequent to the declaration of the affected entity: a representation aspect value may be specified by means of a representation item and an operational aspect value may be specified by means of an operational item.]

{8652/0009} {AI95-00137-01} There are six kinds of representation items: attribute_definition_clauses for representation attributes, enumeration_representation_clauses, record_representation_clauses, component_clauses, and representation_enums.

[Representation items specify how the types and other entities of the language are to be mapped onto the underlying machine. They can be provided to give more efficient representation or to interface with features that are outside the domain of the language (for example, peripheral hardware). Representation items also specify other specifiable properties of entities. A representation item applies to an entity identified by a local_name, which denotes an entity declared local to the current declarative region, or a library unit declared immediately preceding a representation pragma in a compilation.]

{8652/0009} {AI95-00137-01} An operational item is an attribute_definition_clause for an operational attribute.

{8652/0009} {AI95-00137-01} [An operational item or a representation item applies to an entity identified by a local_name, which denotes an entity declared local to the current declarative region, or a library unit declared immediately preceding a representation pragma in a compilation.]
Confirming the value of an aspect with an operational or representation item should never change the semantics of the aspect. Thus Size = 8 (for example) means the same thing whether it was specified with a representation item or whether the compiler chose this value by default.

Term entry: aspect — specifiable property of an entity

Note: An aspect can be specified by an aspect specification on the declaration of the entity. Some aspects can be queried via attributes.

Syntax

```
aspect_clause representation_clause ::= attribute_definition_clause
   | enumeration_representation_clause
   | record_representation_clause
   | at_clause

local_name ::= direct_name
   | direct_name'attribute_designator
   | library_unit_name
```

A representation pragma is allowed only at places where an aspect_clause a representation_clause or compilation_unit is allowed.

Name Resolution Rules

```
5/1 {8652/0009} {AI95-00137-01} In an operational item or a representation item, if the local_name is a direct_name, then it shall resolve to denote a declaration (or, in the case of a pragma, one or more declarations) that occurs immediately within the same declarative region as the representation_item. If the local_name has an attribute_designator, then it shall resolve to denote an implementation-defined component (see 13.5.1) or a class-wide type implicitly declared immediately within the same declarative region as the representation_item. A local_name that is a library_unit_name (only permitted in a representation pragma) shall resolve to denote the library_item that immediately precedes (except for other pragmas) the representation pragma.
```

Reason: {8652/0009} {AI95-00137-01} This is a Name Resolution Rule, because we don't want an operational item or a representation item for X to be ambiguous just because there's another X declared in an outer declarative region. It doesn't make much difference, since most operational or representation items are for types or subtypes, and type and subtype names can't be overloaded.

Ramification: {8652/0009} {AI95-00137-01} The visibility rules imply that the declaration has to occur before the operational or representation item.

Legality Rules

```
6/1 {8652/0009} {AI95-00137-01} The local_name of an aspect_clause a representation_clause or representation pragma shall statically denote an entity (or, in the case of a pragma, one or more entities) declared immediately preceding it in a compilation, or within the same declarative_part, package_specification, task_definition, protected_definition, or record_definition as the representation_or operational item. If a local_name denotes a [local] callable entity, it may do so through a [local] subprogram_renaming_declaration [(as a way to resolve ambiguity in the presence of overloading)]; otherwise, the local_name shall not denote a renaming_declaration.
```

Ramification: The “statically denote” part implies that it is impossible to specify the representation of an object that is not a stand-alone object, except in the case of a representation item like pragma Atomic that is allowed inside a component_list (in which case the representation item specifies the representation of components of all objects of the type). It also prevents the problem of renamings of things like “P.all” (where P is an access-to-subprogram value) or “E(I)” (where E is an entry family).
The part about where the denoted entity has to have been declared appears twice — once as a Name Resolution Rule, and once as a Legality Rule. Suppose P renames Q, and we have a representation item in a declarative_part whose local_name is P. The fact that the representation item has to appear in the same declarative_part as P is a Name Resolution Rule, whereas the fact that the representation item has to appear in the same declarative_part as Q is a Legality Rule. This is subtle, but it seems like the least confusing set of rules.

**Discussion:** A separate Legality Rule applies for component_clauses. See 13.5.1, “Record Representation Clauses”.

**AI95-00291-02** {AI12-0445-1} The representation of an object consists of a certain number of bits (the size of the object). For an object of an elementary type, these are the bits that are normally read or updated by the machine code when loading, storing, or operating-on the value of the object. For an object of a composite type, these are the bits reserved for this object, and include bits occupied by subcomponents of the object. If this includes some padding bits, when the size of an object is greater than that of its subtype, the additional bits are padding bits. For an elementary object, these padding bits are considered to be part of the representation of the object, rather than being gaps between objects, if these bits are normally read and updated along with the others. For a composite object, it is unspecified whether padding bits are not be read or updated in any given composite operation, depending on the implementation.

**To be honest:** {AI95-00291-02} Discontiguous representations are allowed, but the ones we're interested in here are generally contiguous sequences of bits. For a discontiguous representation, the size doesn't necessarily describe the “footprint” of the object in memory (that is, the amount of space taken in the address space for the object).

**Discussion:** {AI95-00291-02} In the case of composite objects, we want the implementation to have the flexibility to either do operations component-by-component, or with a block operation covering all of the bits. We carefully avoid giving a preference in the wording. There is no requirement for the choice to be documented, either, as the implementation can make that choice based on many factors, and could make a different choice for different operations on the same object.

**AI95-00291-02** In the case of a properly aligned, contiguous object whose size is a multiple of the storage unit size, no other bits should be read or updated as part of operating on the object. We don't say this normatively because it would be difficult to normatively define “properly aligned” or “contiguous”.

**Ramification:** Two objects with the same value do not necessarily have the same representation. For example, an implementation might represent False as zero and True as any odd value. Similarly, two objects (of the same type) with the same sequence of bits do not necessarily have the same value. For example, an implementation might use a biased representation in some cases but not others:

```ada
{AI05-0229-1} subtype S is Integer range 1..256;

{AI05-0229-1} type A is array(Natural range 1..4) of S
with Pack;

pragma Pack(1);
X : S := 3;
Y : A := (1, 2, 3, 4);
```

The implementation might use a biased-by-1 representation for the array elements, but not for X. X and Y(3) have the same value, but different representation: the representation of X is a sequence of (say) 32 bits: 0...011, whereas the representation of Y(3) is a sequence of 8 bits: 0000001 (assuming a two’s complement representation).

Such tricks are not required, but are allowed.

**Discussion:** The value of any padding bits is not specified by the language, though for a numeric type, it will be much harder to properly implement the predefined operations if the padding bits are not either all zero, or a sign extension.

**Ramification:** {AI05-0229-1} For example, suppose S'Size = 2, and an object X is of subtype S. If the machine code typically uses a 32-bit load instruction to load the value of X, then X'Size should be 32, even though 30 bits of the value are just zeros or sign-extension bits. On the other hand, if the machine code typically masks out those 30 bits, then X'Size should be 2. Usually, such masking only happens for components of a composite type for which Packing, Component_Size, or record layout is specified.

**Note:** However, that the formal parameter of an instance of Unchecked_Conversion is a special case. Its Size is required to be the same as that of its subtype.

**Note:** That we don't generally talk about the representation of a value. A value is considered to be an amorphous blob without any particular representation. An object is considered to be more concrete.

**AI05-0112-1** {AI05-0295-1} {AI12-0396-1} {AI12-0407-1} A representation item directly specifies a representation aspect of representation of the entity denoted by the local_name, except in the case of a type-related representation item, whose local_name shall denote a first subtype, and which
directly specifies an aspect of the subtype's type. A representation item that names a subtype is either subtype-specific (Size, Object_Size, and Alignment clauses) or type-related (all others). [Subtype-specific aspects may differ for different subtypes of the same type.]

8.a/5

This paragraph was deleted. To be honest: {AI12-0407-1} Type-related and subtype-specific are defined likewise for the corresponding aspects of representation.

8.b

To be honest: Some representation items directly specify more than one aspect.

8.c/3

Discussion: {AI05-0229-1} For example, a pragma Export (see J.15.5) specifies the convention of an entity, and also specifies that it is exported. Such items are obsolescent, directly specifying the associated aspects is preferred.

8.d

Ramification: Each specifiable attribute constitutes a separate aspect. An enumeration_representation_clause specifies the coding aspect. A record_representation_clause (without the mod_clause) specifies the record layout aspect. Each representation pragma specifies a separate aspect.

8.e

Reason: We don't need to say that an at_clause or a mod_clause specify separate aspects, because these are equivalent to attribute_definition_clauses. See J.7, “At Clauses”, and J.8, “Mod Clauses”.

8.e.1/3

{AI05-0112-1} We give a default naming for representation aspects of representation pragmas so we don't have to do that for every pragma. Operational and representation attributes are given a default naming in 13.3. We don't want any anonymous aspects; that would make other rules more difficult to write and understand.

8.f

Ramification: The following representation items are type-related:

8.g

• enumeration_representation_clause

8.h

• record_representation_clause

8.i

• Component_Size clause

8.j/1

• This paragraph was deleted. {AI95-00137-01} External_Tag_clause

8.k

• Small clause

8.l

• Bit_Order clause

8.m

• Storage_Pool clause

8.n

• Storage_Size clause

8.o/2

• {8652/0009} {AI95-00137-01} {AI95-00270-01} Stream_Size_clause

8.p/5

• {8652/0009} {AI95-00137-01} {AI12-0005-1} pragma Unchecked_Union

8.q/1

• This paragraph was deleted. {8652/0009} {AI95-00137-01} Input_clause

8.r/1

• This paragraph was deleted. {8652/0009} {AI95-00137-01} Output_clause

8.s

• Machine_Radix clause

8.t

• pragma Pack

8.u

• pragmas Import, Export, and Convention (when applied to a type)

8.v/3

• {AI05-0009-1} pragmas Atomic, Independent, and Volatile (when applied to a type)

8.w/3

• {AI05-0009-1} pragmas Atomic_Components, Independent_Components, and Volatile_Components (when applied to an array type)

8.x

• pragma Discard_Names (when applied to an enumeration or tagged type)

8.x.1/5

• {AI12-0005-1} pragmas Priority and Interrupt_Priority (when applied to a task or protected type)

8.x.2/5

• {AI12-0005-1} pragma CPU (when applied to a task or protected type)

8.x.3/5

• {AI12-0005-1} pragma Dispatching_Domain

8.x.4/5

• {AI12-0005-1} pragma Relative_Deadline (when applied to a task or protected type)

8.y

The following representation items are subtype-specific:

8.z

• Alignment clause (when applied to a first subtype)

8.z.1/5

• {AI12-0396-1} Object_Size_clause

8.aa

• Size clause (when applied to a first subtype)

8.bb

The following representation items do not apply to subtypes, so they are neither type-related nor subtype-specific:

8.cc

• Address clause (applies to objects and program units)

8.dd

• Alignment clause (when applied to an object)

8.ee

• Size clause (when applied to an object)
• {AI95-00414-01} **pragma Inline** (applies to subprograms) 8.8f/2
• pragmas Import, Export, and Convention (when applied to anything other than a type) 8.9g
• pragmas Atomic and Volatile (when applied to an object or a component) 8.hh
• {AI05-0009-1} pragmas Atomic_Components, Independent_Components, and Volatile_Components (when applied to an array object) 8.ii/3
• pragma Discard_Names (when applied to an exception) 8.jj
• pragma Asynchronous (applies to procedures) 8.kk
• {AI95-00414-01} **pragma No_Return** (applies to subprograms) 8.ii/2
• {AI12-0005-1} pragmas Attach_Handler and Interrupt_Handler (apply to protected units) 8.ii.1/5
• {AI12-0005-1} pragmas Priority and Interrupt_Priority (when applied to a subprogram) 8.ii.2/5
• {AI12-0005-1} **pragma CPU** (when applied to a subprogram) 8.ii.3/5
• {AI12-0005-1} **pragma Relative_Deadline** (when applied to a subprogram) 8.ii.4/5
}{AI05-0229-1} {AI12-0005-1} **While an aspect specification is not a representation item, a similar categorization applies to the aspect that corresponds to each of these representation items. In addition, there are representation-aspects that do not have associated representation items.**

{AI12-0005-1} **The following representation aspects that do not have associated representation items are type-related:** 8.mm/5

- aspect Default_Value
- aspect Default_Component_Value
- aspect Exclusive_Functions
- aspects Link_Name and External_Name (when applied to a type)
- aspect Max_Entry_Queue_Length (when applied to a task or protected type)

{AI12-0005-1} **There are no subtype-specific representation aspects that do not have associated representation items.** 8.mm.7/5

{AI12-0005-1} **The following representation aspects that do not have associated representation items also do not apply to subtypes, so they are neither type-related nor subtype-specific:** 8.mm.8/5

- aspect Static (applies to expression functions)
- aspect Synchronization (applies to procedures)
- aspects Link_Name and External_Name (when applied to anything other than a type)
- aspect Max_Entry_Queue_Length (when applied to an entry)

{8652/0009} {AI95-00137-01} {AI05-0183-1} **An operational item directly specifies an operational aspect of the entitytype of the subtype denoted by the local name, except in the case of a type-related operational item, whose local name shall denote a first subtype, and which directly specifies an aspect of the type of the subtype. The local name of an operational item shall denote a first subtype. An operational item that names a subtype is type-related.**

**Ramification:** {8652/0009} {AI95-00137-01} **The following operational items are type-related:** 8.nn/1

- **External_Tag clause** 8.oo/1
- Read clause 8.pp/1
- Write clause 8.qq/1
- Input clause 8.rr/1
- Output clause 8.ss/1

{AI12-0407-1} **Aspects that can be specified for types and subtypes are also classified into type-related or subtype-specific aspects. Representation aspects that can be specified for types and subtypes are considered type-related unless specified otherwise. In contrast, the classification of operational aspects are given with the definition of the aspect. Type-related aspects have the same value for all subtypes of (a view of) a type[, while subtype-specific aspects may differ for different subtypes of the same type].**

**Discussion:** We talk about “type-related aspects”, which of course include both type-related representation aspects and type-related operational aspects. Aspects Size, Object_Size, and Alignment are subtype-specific, as that is specified above. All other representation aspects are either type-related or not specifiable for a type or subtype. Unlike
A representation item or operational item that directly specifies an aspect of an entity shall appear before the entity is frozen (see 13.14). A representation item that directly specifies an aspect of a subtype or type shall appear after the type is completely defined (see 3.11.1) and before the subtype or type is frozen (see 13.14). If a representation item or aspect_specification is given that directly specifies an aspect of an entity, then it is illegal to give another representation item or aspect_specification that directly specifies the same aspect of the entity.

**Ramification:** {8652/0009} {AI95-00137-01} {AI12-0222-1} The fact that a representation item (or operational item, see next paragraph) that directly specifies an aspect of an entity is required to appear before the entity is frozen prevents changing the representation of an entity after using the entity in ways that require the representation to be known.

**Reason:** {AI12-0116-1} {AI12-0396-1} {AI12-0417-1} If a representation item, operational item, library unit pragma (see J.15), or aspect_specification is given that directly specifies an aspect of an entity, then it is illegal to give another representation item, operational item, library unit pragma, or aspect_specification that directly specifies the same aspect of the entity.

**Ramification:** Unlike representation items, operational items can be specified on partial views. Since they don't affect the representation, the full declaration need not be known to determine their legality.
and type T is a by-reference type or defines one or more by-reference primitives that are inherited by these descendants.

**Ramification:** {8652/0009} {AI95-00137-01} {AI05-0295-1} On the other hand, subtype-specific representation aspects may be specified for the first subtype of such a type, as can operational aspects.

**Reason:** {AI05-0229-1} {AI05-0295-1} {AI12-0109-1} {AI12-0376-1} {AI12-0427-1} The reason for forbidding specification of type-related representation aspects on untagged types is because a change of representation is impossible when passing by reference (to an inherited subprogram). (A by-reference object cannot be copied to change its representation.) The reason for forbidding specification of type-related representation aspects on untagged types with by-reference primitives is that access parameters, access results, and aliased parameters cannot be converted as part of invoking an inherited subprogram if the representation of the designated types might be different.

**Discussion:** {AI12-0109-1} “By-reference type” usually cannot be used in Legality Rules, as it is privacy breaking. Our use here is privacy breaking, but we’re stuck with it for compatibility reasons. Since representation aspects cannot be specified on partial views, privacy violations only can happen when a type includes a component of a private type. In that case, whether these rules are triggered depends on the full type of the private type — which is clearly privacy breaking.

**AI05-00117-01**

{8652/0009} {AI95-00137-01} {8652/0011} {AI95-00117-01} {AI95-00326-01} {AI05-0295-1} {AI12-0036-1} {AI12-0409-1} If a type-related aspect is defined for the partial view of a type, then it has the same definition for the full view of the type, except for certain Boolean-valued operational aspects where the language specifies that the partial view can have the value False even when the full view has the value True. Type-related aspects cannot be specified for them unless they are tagged (in which case only the extension part is affected in any case).

**Operational and representation aspects of a partial view are the same for all views of a type as those of the full view.** Specification of a type-related representation aspect is not allowed for a descendant of a generic formal untagged type.

**Ramification:** {8652/0009} {AI95-00137-01} {AI05-0295-1} Specifying representation aspects is allowed for types whose subcomponent types or index subtypes are generic formal types. Specifying operational aspects and subtype-related representation aspects are allowed on descendants of generic formal types.

**Reason:** {AI05-0295-1} Since it is not known whether a formal type has user-defined primitive subprograms, specifying type-related representation aspects for them is not allowed, unless they are tagged (in which case only the extension part is affected in any case).

**AI12-0396-1** Different views of an entity can have different representation and operational aspects. Most type-related aspects are the same for all views of a type; but specific aspects may have different rules. Similarly, different views of an object can have different representation aspects. For instance, an actual object passed by reference and the associated formal parameter may have different values for Alignment even though the formal parameter is merely a view of the actual object. This is necessary to maintain the language design principle that Alignments are always known at compile time.

**Discussion:** {AI12-0409-1} For type-related aspects, the aspect of the partial view (if any) and full view have to be the same, with an exception for certain Boolean-valued aspects. The exception is intended for aspect Preclarable Initialization, where it would be wildly incompatible (as well as unfriendly) to require the (possibly implicit) state of the full view to be repeated explicitly on the partial view. Aspect Nonblocking has a similar rule for similar reasons, though it is a subtype-specific aspect.

**Proof:** {AI12-0396-1} The syntax of incomplete_type_declarations and formal_incomplete_type_declarations do not allow for an aspect_specification. The prefix of an attribute_reference cannot name an incomplete type (see 3.10.1).
so no attribute_definition_clause can be used with an incomplete type. Similarly, the local_name of a representation pragma cannot name an incomplete type, so no such pragmas can be used with an incomplete type.

The specification of a representation item that specifies the Size aspect for a given subtype, or the size or storage place for an object (including a component) of a given subtype, shall allow for enough storage space to accommodate any value of the subtype.

The specification of certain language-defined aspects is not required to be supported by all implementations; in such an implementation, the specification for such an aspect if a specification of a representation or operational aspect item that is not supported by the implementation, it is illegal; or raises an exception at run time.

Ramification: There is an Implementation Permission below that allows an implementation to put restrictions on any representation aspect; this rule applies if that permission is used for an aspect. This rule only applies to an operational aspect if the aspect explicitly allows the aspect to not be supported.

A type_declaration is illegal if it has one or more progenitors, and a nonconfirming value was specified for a representation aspect of item applies to an ancestor, and this representation item conflicts with the representation of some other ancestor. The cases that cause conflicts are implementation defined.

Implementation defined: The cases that cause conflicts between the representation of the ancestors of a type declaration.

Reason: This rule is needed because it may be the case that only the combination of types in a type declaration causes a conflict. Thus it is not possible, in general, to reject the original representation item or aspect_specification. For instance:

```
package Pkg1 is
  type Ifc is interface;
  type T is tagged record
    Fld : Integer;
  end record;
  for T use record
    Fld at 0 range 0 .. Integer'Size - 1;
  end record;
end Pkg1;
```

Assume the implementation uses a single tag with a default offset of zero, and that it allows the use of nondefault locations for the tag (by putting a component other than the tag into the default location). Clearly, this package will be accepted by the implementation. However, other declarations could cause trouble. For instance, the implementation could reject:

```
with Pkg1;
package Pkg2 is
  type NewT is new Pkg1.T and Pkg1.If. with null record;
end Pkg2;
```

because the declarations of T and Ifc have a conflict in their representation items. This is clearly necessary (it’s hard to imagine how Ifc.Class could work with the tag at a location other than the one it is expecting without introducing distributed overhead).

Conflicts will usually involve implementation-defined attributes (for specifying the location of the tag, for instance), although the example above shows that doesn’t have to be the case. For this reason, we didn’t try to specify exactly what causes a conflict; it will depend on the implementation’s implementation model and what representation aspects items it allows to be changed.

Implementation Note: An implementation can only use this rule to reject type_declarations where one of its ancestors had a nonconfirming representation value specified in a representation aspect item. An implementation must ensure that the default representations of ancestors cannot conflict.

When specifying an aspect that denotes a subprogram, the profile of the subprogram shall be mode conformant with the one required for the aspect, and the convention shall be Ada. Additional requirements are defined for particular aspects.

Reason: As well as applying to aspect_specifications, this rule applies to attribute_definition_clauses for those aspects that have associated attributes.

This rule implies, for example, that if one writes:
type T is ...
with Read => R;

R has to be a procedure with two parameters with the appropriate subtypes and modes as shown in 13.13.2.

13.1

Static Semantics

{AI12-0059-1} If two subtypes statically match, then their subtype-specific aspects (for example, Size and Alignment) are the same.

Reason: {AI05-0295-1} {AI12-0059-1} This is necessary because we allow (for example) conversion between access types whose designated subtypes statically match. Note that most aspects (including the subtype-specific aspects Size and Alignment) may not be specified for a nonfirst subtype. The only language-defined exceptions to this rule are the Object_Size, Static_Predicate, and Dynamic_Predicate aspects; it is illegal to specify an aspect (including a subtype-specific one) for a nonfirst subtype.

Consider, for example:

{AI12-0005-1} package P1 is
  subtype S1 is Integer range 0..2**16-1
  with Size => +
  -- for S1/Size use 16; -- Illegal!
  -- S1/Size would be 16 by default.
  type A1 is access all S1;
X1: A1;
end P1;

{AI12-0005-1} package P2 is
  subtype S2 is Integer range 0..2**16-1
  with Size => +
  -- for S2/Size use 32; -- Illegal!
  type A2 is access all S2;
X2: A2;
end P2;

{AI05-0229-1} procedure Q is
  use P1, P2;
  type Array1 is array (Integer range <>) of aliased S1
  with Pack+;
  pragma Pack(Array1);
  Obj1: Array1(1..100);
  type Array2 is array (Integer range <>) of aliased S2
  with Pack+;
  pragma Pack(Array2);
  Obj2: Array2(1..100);
begin
X1 := Obj2(17)'Unchecked_Access;
X2 := Obj1(17)'Unchecked_Access;
end Q;

Loads and stores through X1 would read and write 16 bits, but X1 points to a 32-bit location. Depending on the endianness of the machine, loads might load the wrong 16 bits. Stores would fail to zero the other half in any case.

Loads and stores through X2 would read and write 32 bits, but X2 points to a 16-bit location. Thus, adjacent memory locations would be trashed.

Hence, the above is illegal. Furthermore, the compiler is forbidden from choosing different Sizes by default, for the same reason.

{AI12-0059-1} The same issues apply to Alignment. Similar issues apply to Object_Size, Static_Predicate, and Dynamic_Predicate, but the chosen solution is different: explicit rules in 4.9.1 that ensure that the aspects are the same if specified.

{AI12-0059-1} The above static matching rule combined with the definition of static matching in 4.9.1 (after updating to add Object_Size) does not cause incompatibilities in existing Ada 2012 code that does not mention Object_Size. But it does constrain the implementation-defined value of Object_Size when it is not specified for a subtype; the above rule applies even in that case. (The effects noted in the example above would occur otherwise.)

{AI12-0059-1} We need this rule even though static matching explicitly excludes confirming values of Object_Size. That's because a general access type can designate any aliased object whose subtype statically matches the designated subtype. Since the Object_Size of a subtype determines the number of bits allocated for an aliased object of the subtype, if we allowed different Object_Sizes for statically matching subtypes, we'd be allowing the access type to designate objects with differing numbers of bits. That isn't going to work.
A derived type inherits each type-related representation aspect of a parent type that was directly specified before the declaration of the derived type, or (in the case where the parent is derived) that was inherited by the parent type from the grandparent type, and can be overridden by aspect specifications or operational items that occur at a point before or after the inheritance takes place.

**Ramiﬁcation:** As with representation items, if an operational item for the parent appears after the derived type declaration, then inheritance does not happen for that operational item.

**Discussion:** Currently, only untagged types inherit operational aspects. Inheritance from tagged types causes problems, as the different views can have different visibility on operational items — potentially leading to operational items that depend on the view. We want aspects to be the same for all views. Untagged types don’t have this problem as plain private types don’t have ancestors, and thus can’t inherit anything. In addition, it seems unlikely that we’ll need inheritance for tagged types, as usually we’ll want to incorporate the parent’s operation into a new one that also handles any extension components. We considered writing this rule that way, but rejected it as that could be too speciﬁc for future operational aspects. (After all, that is precisely the problem that caused us to introduce “operational aspects” in the ﬁrst place.)

**AI12-0396-1** When a type-related operational aspect is inherited, the rules for inheritance depend on the nature of the aspect (see 13.1.1). Unless otherwise speciﬁed for a given aspect, these rules are as follows:

- For an operational aspect that is a value, the inherited aspect has the same value;
- For an operational aspect that is a name:

  - if the name denotes one or more primitive subprograms of the type, the inherited aspect is a name that denotes the corresponding primitive subprogram(s) of the derived type;

**Discussion:** A primitive subprogram that is declared after the end of the enclosing declaration list of a derived type (in particular, in the private part of a package if the derived type is declared in the package’s visible part).
is not the “corresponding primitive subprogram” in the sense of this rule. In a case like this, the corresponding primitive subprogram is actually the inherited subprogram. This doesn’t make a difference for tagged types, because of the “dispatching” semantics used, which means a call on the inherited subprogram actually “reaches” the body of the overriding. But for untagged types, overriding an inherited subprogram of an untagged derived type in the private part is “too late” to have an effect on external uses of the primitive, since non-visible overridings are not generally reachable, and a call that only “sees” the inherited subprogram goes to the body of the parent’s operation, effectively ignoring the private overriding. This same rule applies to aspects that denote an inherited subprogram of an untagged derived type — the private overriding is effectively ignored.

- otherwise, the inherited aspect is a name that denotes the same entity or entities as the original aspect;

- AII2-0396-1 AII2-0423-1 For an operational aspect that is an identifier specific to the aspect, the inherited aspect is the same identifier;

- AII2-0396-1 AII2-0423-1 For an operational aspect that is an expression or an aggregate, the inherited aspect is a corresponding expression or aggregate where each name, value, and identifier follows these same rules for inheritance.

AII95-00444-01 AII12-0419-1 When an aspect that is a subprogram is inherited, the derived type inherits the aspect in the same way that a derived type inherits a user-defined primitive subprogram from its parent (see 3.4).

**Reason:** This defines the parameter names and types, and the needed implicit conversions.

Each aspect of representation of an entity is as follows:

- If the aspect is specified for the entity, meaning that it is either directly specified or inherited, then that aspect of the entity is as specified, except in the case of Storage_Size, which specifies a minimum.

  **Ramification:** This rule implies that queries of the aspect return the specified value. For example, if the user writes “for X’Sz...e use 32;”, then a query of X’Sz will return 32.

- If an aspect of representation of an entity is not specified, it is chosen by default in an unspecified manner.

  **Ramification:** 8652/0009 AII95-00137-01 AII05-0295-1 Note that specifying a representation aspectitem can affect the semantics of the entity.

  The rules forbid things like “for S’Base...alignment use ...” and “for S’Base...record ...”.

  **Discussion:** The intent is that implementations will represent the components of a composite value in the same way for all subtypes of a given composite type. Hence, Component_Size and record layout are type-related aspects.

  **Ramification:** AII05-0083-1 As noted previously, in the case of an object, the entity mentioned in this text is a specific view of an object. That means that only references to the same view of an object that has a specified value for a representation aspect R necessarily have that value for the aspect R. The value of the aspect R for a different view of that object is unspecified. In particular, this means that the representation values for by-reference parameters is not the same as those of the underlying object.

8652/0040 AII95-00108-01 AII12-0396-1 If an operational aspect is specified for an entity (meaning that it is either directly specified or, if type-related or subtype-specific, inherited), then that aspect of the entity is as specified. Otherwise, the aspect of the entity has the default value for that aspect. For aspects that are neither type-related nor subtype-specific, the terms “specified” and “directly specified” are equivalent.

**Proof:** AII2-0396-1 Aspect inheritance is only defined for types and subtypes.

AII95-00291-02 AII05-0295-1 AII12-0396-1 An aspect specification or a representation item that specifies an aspect of representation aspect that would have been chosen in the absence of the aspect specification or representation item is said to be confirming. The aspect value specified in this case is said to be a confirming representation aspect value. Other values of the aspect are said to be nonconfirming, as are the aspect specifications and representation items that specified them. Similarly,
an aspect specification or operational item that specifies an operational aspect to be the same as the definition it would have by default is said to be confirming; otherwise it is nonconfirming.

Discussion: {AI12-0005-1} As noted at the beginning of this subclause, we have a Language Design Principle that confirming aspects do not change the semantics. However, it is not a Language Design Principle principle that one can always specify a confirming aspect. Some aspects can never be confirmed. For instance, the default implementation of a stream-oriented attribute cannot be confirmed, as any subprogram that can be specified is not the same as the default subprogram, and thus is nonconfirming. Whether the effect is the same is not relevant for this purpose: it would be very difficult to formally define what it means to have the same effect. (Note that one can name any implementation for a stream-oriented attribute by using the associated attribute but specifying that by name would violate the circular aspect definition rule.) This is true for any implicitly composed aspect. Similarly, aspect Default Value cannot be confirmed as the default is that there is no default value; any value that can be specified is not that.

Dynamic Semantics

Ramification: {AI05-0299-1} Elaboration of representation pragmas is covered by the general rules for pragmas in 2.8 Section 2.

Implementation Permissions

Implementation defined: The interpretation of each aspect of representation aspect.

Implementation defined: Any restrictions placed upon the specification of representation aspects. A recommended level of support is defined specified for the specification of representation aspects and related features in each subclause. These recommendations are changed to requirements for implementations that support the Systems Programming Annex (see C.2, “Required Representation Support”).

Implementation Advice

The recommended level of support for the specification of all representation aspects is qualified as follows:

• {AI95-00291-02} {AI05-0295-1} A confirming specification for a representation aspect item should be supported.

To be honest: {AI05-0295-1} A confirming representation aspect value item might not be possible for some entities. For instance, consider an unconstrained array. The size of such a type is implementation-defined, and might not actually be a representable value, or might not be static.

• {AI05-0295-1} {AI12-0444-1} An implementation is not required to support the specification for a representation aspect that contains items containing nonstatic expressions, unless except that an implementation should support a representation item for a given entity if each nonstatic expression in the representation item is a name that statically denotes a constant declared before the entity.

Reason: This is to avoid the following sort of thing:

{AI12-0005-1} X : Integer := F(...)

with Address => Y;
Y : Address := G(...);
for X'Address use Y;

In the above, we have to evaluate the initialization expression for X before we know where to put the result. This seems like an unreasonable implementation burden.
The above code should instead be written like this:

```ada
{AI12-0005-1} Y : constant Address := G(...);
X : Integer := F(...)
with Address =>

for Address use Y;
```

This allows the expression “Y” to be safely evaluated before X is created.

An implementation can support other nonstatic expressions if it wants to. Expressions of type Address are hardly ever static, but their value might be known at compile time anyway in many cases.

- `{AI12-0059-1} {AI12-0444-1}` An implementation is not required to support a specification for the `Object_Size` or `Size` for a given composite subtype, nor the size or storage place for an object (including a component) of a given composite subtype, unless the constraints on the subtype and its composite subcomponents (if any) are all static constraints.

  **Reason:** `{AI12-0059-1}` We don't want to require that `Object_Size` or `Size` be supported on types that might have a representation not completely specified at compile time, or are represented discontinuously, or are represented differently for different constraints.

- `{AI95-00291-02} {AI05-0295-1} {AI12-0444-1}` An implementation is not required to support specifying a nonconfirming representation aspect value if it can cause an aliased object or an object of a by-reference type to be allocated at a nonaddressable location or, when the alignment attribute of the subtype of such an object is nonzero, at an address that is not an integral multiple of that alignment. An aliased component, or a component whose type is by-reference, should always be allocated at an addressable location.

  **Reason:** The intent is that access types, type `System.Address`, and the pointer used for a by-reference parameter should be implementable as a single machine address — bit-field pointers should not be required. (There is no requirement that this implementation be used — we just want to make sure it's feasible.)

  **Implementation Note:** `{AI95-00291-02}` We want subprograms to be able to assume the properties of the types of their parameters inside of subprograms. While many objects can be copied to allow this (and thus do not need limitations), aliased or by-reference objects cannot be copied (their memory location is part of their identity).

  **Thus Note that** the above rule does not apply to types that merely allow by-reference parameter passing; for such types, a copy typically needs to be made at the call site when a bit-aligned component is passed as a parameter.

- `{AI95-00291-02} {AI05-0295-1} {AI12-0444-1}` An implementation is not required to support specifying a nonconfirming representation aspect value if it can cause an aliased object of an elementary type to have a size other than that which would have been chosen by default.

  **Reason:** Since all bits of elementary objects participate in operations, aliased objects must not have a different size than that assumed by users of the access type.

- `{AI95-00291-02} {AI05-0295-1} {AI12-0444-1}` An implementation is not required to support specifying a nonconfirming representation aspect value if it can cause an aliased object of a composite type, or an object whose type is by-reference, to have a size smaller than that which would have been chosen by default.

  **Reason:** Unlike elementary objects, there is no requirement that all bits of a composite object participate in operations. Thus, as long as the object is the same or larger in size than that expected by the access type, all is well.

  **Ramification:** This rule presumes that the implementation allocates an object of a size specified to be larger than the default size in such a way that access of the default size suffices to correctly read and write the value of the object.

- `{AI95-00291-02} {AI05-0295-1} {AI12-0444-1}` An implementation is not required to support specifying a nonconfirming subtype-specific representation aspect value for item specifying an aspect of representation of an indefinite or abstract subtype.

  **Reason:** `{AI05-0295-1}` Representation aspects are often not well-defined for such types.

  **Ramification:** `{AI95-00291-02} {AI05-0229-1}` A type with the Pack aspect specified A pragma Pack will typically not be packed so tightly as to disobey the above rules. A Component Size clause or record representation clause will typically be illegal if it disobeys the above rules. Atomic components have similar restrictions (see C.6, “Shared Variable Control”).

---

677 16 October 2023  Operational and Representation Aspects 13.1
For purposes of these rules, the determination of whether specifying a representation aspect value for an object of a type can cause an object to have some property is based solely on the properties of the type itself, not on any available information about how the type is used. In particular, it presumes that minimally aligned objects of this type cannot be declared at some point.

Implementation Advice: The recommended level of support for all representation items should be followed.

NOTE  {AI05-0229-1} Aspects that can be specified are defined throughout this document, and are summarized in K.1.

Incompatibilities With Ada 83

It is now illegal for a representation item to cause a derived by-reference type to have a different record layout from its parent. This is necessary for by-reference parameter passing to be feasible. This only affects programs that specify the representation of types derived from types containing tasks; most by-reference types are new to Ada 95. For example, if A1 is an array of tasks, and A2 is derived from A1, it is illegal to apply a pragma Pack to A2.

Extensions to Ada 83

Ada 95 allows additional aspect_clause_representation_clause for objects.

Wording Changes from Ada 83

The syntax rule for type_representation_clause is removed; the right-hand side of that rule is moved up to where it was used, in aspect_clause_representation_clause. There are two references to “type representation clause” in RM83, both in Section 13; these have been reworded. Also, the representation_clause has been renamed the aspect_clause to reflect that it can be used to control more than just representation aspects.

We have defined a new term “representation item”, which includes all_representation_clause_representation_clauses and representation pragmas, as well as component_clauses. This is convenient because the rules are almost identical for all of them. We have also defined the new terms “operational item” and “operational aspects” in order to conveniently handle new types of specifiable and permitted entities.

All of the forcing occurrence stuff has been moved into its own subclause (see 13.14), and rewritten to use the term “freezing”.

RM83-13.1(10) requires implementation-defined restrictions on representation items to be enforced at compile time. However, that is impossible in some cases. If the user specifies a junk (nonstatic) address in an address clause, and the implementation chooses to detect the error (for example, using hardware memory management with protected pages), then it's clearly going to be a run-time error. It seems silly to call that “semantics” rather than “a restriction”.

RM83-13.1(10) tries to pretend that representation_clauses don't affect the semantics of the program. One counter-example is the Small clause. Ada 95 has more counter-examples. We have noted the opposite above.

Some of the more stringent requirements are moved to C.2, “Required Representation Support”.

Extensions to Ada 95

Amendment Correction: Confirming representation items are defined, and the recommended level of support is now that they always be supported.

Wording Changes from Ada 95

Added operational items in order to eliminate unnecessary restrictions and permissions on stream attributes. As part of this, representation_clause was renamed to aspect_clause.

Added wording to say that the partial and full views have the same operational and representation aspects. Ada 2005 extends this to cover all views, including the incomplete view.

Changed operational items to have inheritance specified for each such aspect.

Added wording to allow the rejection of types with progenitors that have conflicting representation items.

The description of the representation of an object was clarified (with great difficulty reaching agreement). Added wording to say that representation items on aliased and by-reference objects never need be supported if they would not be implementable without distributed overhead even if other recommended level of support says otherwise. This wording matches the rules with reality.
Added wording so that inheritance depends on whether operational items are visible rather than whether they occur before the declaration (we don't want to look into private parts). Also limited limited operational inheritance to untagged types to avoid anomalies with private extensions (this is not incompatible, no existing operational attribute used this capability). Also added wording to clearly define that subprogram inheritance works like derivation of subprograms.

**Incompatibilities With Ada 2005**

*Correction:* Specifying a language-defined aspect for a generic formal parameter is no longer allowed. Most aspects could not be specified on these anymore; moreover, this was not allowed in Ada 83, so it is unlikely that compilers are supporting this as a capability (and it is not likely that they have a consistent definition of what it means if it is allowed). Thus, we expect this to occur rarely in existing programs. **Note:** This correction is repealed in Ada 2022, as a number of aspects are allowed on formals in that later language version.

**Wording Changes from Ada 2005**

*Correction:* Defined that overriding of nonconfirming representation aspect only happens for a nonconfirming representation item. This prevents a derived type from being considered to have only a confirming representation item when the value would be nonconfirming if given on a type that does not inherit any aspects of representation. This change just eliminates a wording confusion and ought not change any behavior.

*Correction:* Defined a default naming for representation aspects that are representation pragmas.

*Added text ensuring that the rules for representational and operational items also apply appropriately to aspect specifications; generalized operational aspects so that they can be defined for entities other than types. Any extensions are documented elsewhere.*

*Correction:* Rewrote many rules to be in terms of "specifying a representation aspect" rather than use of a "representation item". This better separates how an aspect is specified from what rules apply to the value of the aspect.

**Incompatibilities With Ada 2012**

*Corrigendum:* Added a rule that makes it illegal to specify a representation value after a type is derived from an untagged by-reference type. This restriction is incompatible, but since the implementation would have had to copy an object that does not allow copying in order to change the representation for any implicit or explicit conversion between the original and the derived type, it is unlikely that any program could exist without running into internal compiler errors or bogus results.

*Corrigendum:* Added a rule preventing self-referencing representation or operational aspects. This is technically incompatible, but since the similar representation or operational item has been illegal since they've existed, and they don't make any sense, it's unlikely that any implementation accepted them or that they appear in any program.

*Correction:* Added a rule preventing giving a representation aspect on a partial view. Since this has always been prohibited for other kinds of representation items, it's unlikely that any implementation accepted them or that they appear in any program.

**Extensions to Ada 2012**

*Correction:* It is now allowed to specify type-related representation aspects for an untagged derived type that has primitive operations, so long as the type is not a by-reference type.

*Corrigendum:* Clarified that an aspect (any aspect) can be specified only once for an entity, no matter what means of specifying it are used. **We did not document this as an incompatibility as only aspects that are neither operational nor representation could change behavior and there is no known implementation of these new aspects that allows multiple definitions.**

*Added wording changes to support Object Size.*

*Correction:* Clarified that many of these rules only make sense for type-related aspects.

*Correction:* Clarified how inheritance works for operational aspects that are not values.

*Move the general requirements for aspects that are subprograms here from 13.3.*

**Wording Changes from Ada 2022**

*Corrigendum:* Clarified that any aspect not explicitly defined as a representation aspect is an operational aspect.
13.1.1 Aspect Specifications

{AI05-0183-1} [Certain representation or operational aspects of an entity may be specified as part of its declaration using an aspect specification, rather than using a separate representation or operational item.] The declaration with the aspect specification is termed the associated declaration.

Syntax

{AI05-0183-1} aspect_specification ::= 
   with aspect_mark [=> aspect_definition] .
   aspect_mark [=> aspect_definition] .

{AI05-0183-1} aspect_mark ::= aspect_identifier[’Class]

Language Design Principles

{AI05-0183-1} {AI05-0267-1} The aspect specification is an optional element in most kinds of declarations. Here is a list of all kinds of declarations and an indication of whether or not they allow aspect clauses, and in some cases a short discussion of why (* = allowed, NO = not allowed). Kinds of declarations with no indication are followed by their subdivisions (which have indications).

4.a/3

{AI12-0005-1} {AI12-0061-1} {AI12-0079-3} {AI12-0395-1} {AI12-0398-1} basic_declaration
   type_declaration
   full_type_declaration
   type_declaration_syntax*
   task_type_declaration*
   protected_type_declaration*
   incomplete_type_declaration -- NO
   -- Incomplete types do not have aspects by definition, type aspects cannot be read by an attribute or specified by attribute_definition_clause.
   -- (the attribute name is illegal), so it would not make sense to allow specifying them this in another way.
   private_type_declaration*
   private_extension_declaration*
   subtype_declaration*
   object_declaration
   object_declaration_syntax*
   single_task_declaration*
   single_protected_declaration*
   number_declaration -- NO
   iterated_component_association -- NO
   subprogram_declaration*
   abstract_subprogram_declaration*
   null_procedure_declaration*
   expression_function_declaration*
   package_declaration* -- via package_specification
   renaming_declaration*
   -- There are no language-defined aspects that may be specified
   -- on renames, but implementations might support some.
   exception_declaration*
   generic_declaration
   generic_subprogram_declaration*
   generic_package_declaration* -- via package_specification
   generic_instantiation*
   enumeration_literal_specification -- NO
   -- The syntax would be ambiguous if this was supported directly.
   discriminantSpecification*
   -- There are no language-defined aspects that may be specified
--- on discriminants, but implementations might support some. --- NO

component_declaration* NO

loop_parameter_specification -- NO

chunk_specification -- NO - the enclosing construct has an aspect_specification

iterator_specification -- NO

iterator_parameter_specification -- NO

parameter_specification*

-- There are no language-defined aspects that may be specified

-- on parameters, but implementations might support some. --- NO

subprogram_body* -- - but language-defined aspects only if there is no explicit specification

entry_declaration*

entry_index_specification*

-- There are no language-defined aspects that may be specified

-- on an entry index, but implementations might support some. --- NO

subprogram_body_stub* -- - but language-defined aspects only if there is no explicit specification

generic_formal_parameter_declaration* NO

-- There are no language-defined aspects that may be specified

-- on generic formals, but implementations might support some.

formal_object_declaration*

formal_type_declaration

formal_complete_type_declaration* NO - see incomplete_type_declaration above*

formal_subprogram_declaration

formal_concrete_subprogram_declaration*

formal_abstract_subprogram_declaration*

formal_package_declaration* NO

extended_return_object_declaration*

-- There are no language-defined aspects that may be specified

-- on return objects, but implementations might support some extended_return_statement --- NO

{AI12-0005-1} {AI12-0169-1} -- 4.d/5

We also allow aspect_specifications on all kinds of bodies, but there are no language-defined aspects

-- that may be specified on a body. These are allowed for implementation-defined aspects.

-- See above for subprogram bodies and stubs (as these can be declarations).

package_body*

task_body*

protected_body*

entry_body*

package_body_stub*

task_body_stub*

protected_body_stub*

{AI05-0267-1} Syntactically, aspect_specifications generally are located at the end of declarations. When a declaration is all in one piece such as a null_procedure_declaration, object_declaration, or generic_instantiation the aspect_specification goes at the end of the declaration; it is then more visible and less likely to interfere with the layout of the rest of the structure. However, we make an exception for program units (other than subprogram specifications) and bodies, in which the aspect_specification goes before the IS. In these cases, the entity could be large and could contain other declarations that also have aspect specifications, so it is better to put the aspect_specification toward the top of the declaration. (Some aspects – such as Pure – also affect the legality of the contents of a unit, so it would be annoying to only see those after reading the entire unit.)

4.d/3

{AI105-0183-1} {AI112-0212-1} An aspect_mark identifies an aspect of the entity defined by the associated declaration (the associated entity); the aspect denotes an object, a value, an expression, an aggregate, a subprogram, or some other kind of entity. If the aspect_mark identifies:

- an aspect that denotes an object, the aspect_definition shall be a name. The expected type for the name is the type of the identified aspect of the associated entity;

- an aspect that is a value or an expression, the aspect_definition shall be an expression. The expected type for the expression is the type of the identified aspect of the associated entity;
The usage names in an aspect_definition associated with a declaration \{ are not resolved at the point of the associated declaration, but rather\} are resolved at the end of the immediately enclosing declaration list, or in the case of the declaration of a library unit, at the end of the visible part of the entity.

\begin{itemize}
\item \{AI12-0212-1\} an aspect that is an aggregate, the aspect definition shall be an expression that is an aggregate, with the form of the aggregate determined by the identified aspect;
\begin{itemize}
\item Ramification: \{AI12-0212-1\} The only requirement here is that the expression is syntactically an aggregate; there is no requirement that it resolve to some particular type or even that it should resolve like an aggregate. Each aspect that uses an aggregate is responsible for specifying how the choice(s), component(s), and other contents of the aggregate are resolved and interpreted.
\end{itemize}
\item an aspect that denotes a subprogram, the aspect_definition shall be a name; the expected profile for the name is the profile required for the aspect of the associated entity;
\item an aspect that denotes some other kind of entity, the aspect_definition shall be a name, and the name shall resolve to denote an entity of the appropriate kind;
\item an aspect that is given by an identifier specific to the aspect, the aspect_definition shall be an identifier, and the identifier shall be one of the identifiers specific to the identified aspect.
\end{itemize}

\begin{itemize}
\item \{AI05-0183-1\} \{AI12-0373-1\} \{AI12-0427-1\} The usage names in an aspect_definition associated with a declaration \{ are not resolved at the point of the associated declaration, but rather\} are resolved at the end of the immediately enclosing declaration list, or in the case of the declaration of a library unit, at the end of the visible part of the entity.
\begin{itemize}
\item Ramification: If an aspect_definition is not associated with a declaration (instead being part of a statement or expression), then it is resolved when the associated construct is resolved.
\end{itemize}
\item \{AI05-0183-1\} \{AI12-0180-1\} \{AI12-0220-1\} If the associated declaration is for a subprogram, or entry, or access-to-subprogram_type, the names of the formal parameters are directly visible within the aspect_definition, as are certain attributes, as specified elsewhere in this document for the identified aspect. If the associated declaration is a type_declaration, within the aspect_definition the names of any visible_components, protected_subprograms, and entries are directly visible, and the name of the first subtype denotes the current instance of the type (see 8.6). If the associated declaration is a subtype_definition, within the aspect_definition the name of the new subtype denotes the current instance of the subtype.
\end{itemize}

Legality Rules

\begin{itemize}
\item \{AI05-0183-1\} If the first freezing point of the associated entity comes before the end of the immediately enclosing declaration list, then each usage name in the aspect_definition shall resolve to the same entity at the first freezing point as it does at the end of the immediately enclosing declaration list.
\item \{AI12-0181-1\} \{AI12-0396-1\} An expression or name that causes freezing of an entity shall not occur within an aspect_specification that specifies a representation or operational aspect of that entity.
\begin{itemize}
\item Reason: \{AI12-0181-1\} \{AI12-0396-1\} The rule prevents an aspect of an entity from depending (directly or indirectly) on properties of the entity itself.
\item Implementation Note: \{AI12-0396-1\} This check needs to be deferred at least to the freezing of the entity (as the aspect_definition is not resolved until then), and might be accomplished during the freezing of the aspect_definition (since it is closely related). Keep in mind that multiple other entities could be involved.
\end{itemize}
\item \{AI05-0183-1\} At most one occurrence of each aspect_mark is allowed within a single aspect_specification. The aspect identified by the aspect_mark shall be an aspect that can be specified for the associated entity (or view of the entity defined by the associated declaration).
\begin{itemize}
\item Ramification: \{AI12-0016-1\} \{AI12-0005-1\} \{AI12-0396-1\} This rule prevents multiple specifications in the same aspect_specification. Rules in 13.1 prevent multiple specifications in different aspect_specifications (on different views of the same type, for instance), or between operational or representation items and an aspect_specification, even for aspects that are neither operational nor representation aspects.
\end{itemize}
\item \{AI05-0183-1\} The aspect_definition associated with a given aspect_mark may be omitted only when the aspect_mark identifies an aspect of a boolean type, in which case it is equivalent to the aspect_definition being specified as True.
\end{itemize}
If the aspect mark includes 'Class, then the associated entity shall be a tagged type or a primitive subprogram of a tagged type.

Unless otherwise specified for a specific aspect, all language-defined aspect cannot be specified on a renaming declaration or, a generic formal parameter declaration, a subunit, a package body, a task body, a protected body, or a body stub other than a subprogram body stub.

Discussion: Implementation-defined aspects can be allowed on these, of course; the implementation will need to define the semantics. In addition, the language does not define default aspect matching rules for generic forms; only the handful of aspects allowed on forms have such rules. Therefore, the implementation will need to define actual type matching rules for any aspects allowed on formal types; there are no default matching rules defined by the language.

Unless specified otherwise, a language-defined aspect shall not be specified in an aspect specification given on a subprogram body or subprogram body stub that is a completion of a program unit, subprogram or generic subprogram or another declaration.

Reason: Most language-defined aspects (for example, preconditions) are intended to be available to callers, and specifying them on a body that has a separate declaration hides them from callers. Specific language-defined aspects may allow this, but they have to do so explicitly (by defining an alternative Legality Rule), and provide any needed rules about visibility. Note that this rule does not apply to implementation-defined aspects, so implementers need to carefully define whether such aspects can be applied to bodies and stubs, and what happens if they are specified on both the declaration and body of a unit.

If an aspect of a derived type is inherited from an ancestor type and has the boolean value True, the inherited value shall not be overridden to have the value False for the derived type, unless otherwise specified in this document.

Reason: Most boolean-valued language-defined aspects are associated with a representation pragma. The existing rules for such pragmas assume that the aspect cannot be removed. For instance, if a type is declared to be Atomic, then all descendants of that are also Atomic. This rule ensures that remains the case when using the aspect notation instead of pragmas.

Discussion: This definition leaves holes for Boolean aspects that can be specified on non-first subtypes. Such aspects (for instance, Nonblocking) must have their own rules (that is, "otherwise specify" rules) that define the effects of inheriting from subtypes (both first subtypes and nonfirst subtypes).

If a given aspect is type-related and inherited, then within an aspect definition for the aspect, if a name resolves to denote multiple visible subprograms, all or none of the denoted subprograms shall be primitives of the associated type.

Reason: This is necessary because the inheritance rules for names denoting primitive subprograms are different from those for names denoting other entities — see 13.1.

Certain type-related aspects are defined to be nonoverridable; all such aspects are specified using an aspect definition that is a name. All such aspects are inherited by derived types according to the rules given in 13.1. Any legality rule associated with a nonoverridable aspect is re-checked for the derived type, if the derived type is not abstract. Certain type-related and subtype-specific aspects are defined to be additive; such aspects are not inherited, but they can apply to the types derived from, or the subtypes based on, the original type or subtype, as defined for each such aspect. Finally, certain type-related aspects are implicitly composed; such aspects are not inherited, but rather a default implementation for a derived type is provided, as defined for each such aspect, based on that of its parent type, presuming the aspect for the parent type is available where the derived type is declared, plus those of any new components added as part of a type extension.

For a nonoverridable aspect of a type that denotes one or more subprograms with a parameter or result of type or access, all of the denoted subprograms shall be primitive for the type.
same restriction applies to elements that denote subprograms within a nonoverridable aspect that is in the form of an aggregate.

**Reason:** \{AI22-0002-1\} Nonoverridable aspects can only be confirmed on inheritance, and a name that denotes a nonprimitive subprogram continues to denote the original subprogram, thus there would be an inherited reference to a subprogram that operates on the parent type rather than the derived type. An example of an aspect that has elements that denote subprograms is the Aggregate aspect.

\[AI12-0138-1\] \{AI12-0206-1\} \{AI12-0211-1\} \{AI12-0396-1\} \{AI22-0002-1\] If a nonoverridable aspect is directly specified for a type \(T\), then any explicit specification of that aspect for any other descendant of \(T\) (other than \(T\) itself) shall be confirming. In the case of an aspect whose value is a name, this means that the specified name shall match the inherited aspect in the sense that it, meaning that the specified name shall denote the same declarations as would the inherited name. Similarly, for an aspect that is an expression or an aggregate, confirming means the defining expression is fully conformant (see 6.3.1) with the defining expression for the inherited aspect, with the added rule that an identifier that is specific to the aspect is the same as the corresponding identifier in the inherited aspect.

\[AI12-0138-1\] \{AI12-0396-1\} \{AI22-0002-1\] If a full type has a partial view, and a given nonoverridable aspect is allowed for both the full view and the partial view, then the given aspect for the partial view and the full view shall be the same: the aspect shall be directly specified only on the partial view; if the full type inherits the aspect, then a matching definition shall be specified (directly or by inheritance) for the partial view.

**Ramification:** In order to enforce these rules without breaking privacy, we cannot allow a private type that could have a particular overridable aspect to have a hidden definition of that aspect. There is no problem if the private type does not allow the aspect (as the aspect could not be specified on descendants in that case).

\[AI12-0211-1\] \{AI22-0002-1\] If a type inherits a nonoverridable aspect from multiple ancestors, the value of the aspect inherited from any given ancestor shall be confirming of the values inherited from all other ancestors.

**Reason:** \{AI12-0005-1\} \{AI12-0211-1\] If more than one progenitor of a type \(T\) specifies a nonoverridable aspect, they all have to specify the same or matching values for that aspect. Otherwise, we'd have two different values for the aspect that depend on which progenitor we inherit from.

\[AI12-0138-1\] \{AI12-0211-1\} \{AI22-0002-1\] In addition to the places where Legality Rules normally apply (see 12.3), these rules about nonoverridable aspects also apply in the private part of an instance of a generic unit.

\[AI12-0138-1\] \{AI12-0206-1\} \{AI12-0256-1\} \{AI12-0373-1\} \{AI12-0437-1\] [The Default_Iterator, Iterator_Element, Implicit Dereference, Constant Indexing, and Variable Indexing aspects are nonoverridable.]

**Discussion:** We don't need an assume-the-worst rule for most nonoverridable aspects as they only work on tagged types and deriving from formal tagged types is not allowed in generic bodies. In the case of Implicit Dereference, a derivation in a generic body does not cause problems (the ancestor necessarily cannot have the aspect, else specifying the aspect would be illegal), as there could be no place with visibility on both aspects. In the case of Max_Entry_Queue_Length, it is only allowed on task and protected types, and on entries, and there are not formal versions of any of those things. In the case of No_Controlled_Parts, we defined an assume-the-worst rule with the aspect.

\[AI12-0437-1\] A list of all nonoverridable aspects can be found in the index, under “nonoverridable aspect”.

---

**Static Semantics**

\[AI05-0183-1\] Depending on which aspect is identified by the aspect mark, an aspect definition specifies:

- a name that denotes a subprogram, object, or other kind of entity;
• {AI12-0427-1} an expression (other than an aggregate), which is either evaluated to produce a single value, or which (as in a precondition) is to be evaluated at particular points during later execution; or

• {AI12-0427-1} an identifier specific to the aspect; or

• {AI12-0427-1} an aggregate, which is positional or named, and is composed of elements of any of these four kinds of constructs.

{AI05-0183-1} The identified aspect of the associated entity, or in some cases, the view of the entity defined by the declaration, is as specified by the aspect definition (or by the default of True when boolean). Whether an aspect specification applies to an entity or only to the particular view of the entity defined by the declaration is determined by the aspect mark and the kind of entity. The following aspects are view specific:

• An aspect specified on an object_declaration;

• An aspect specified on a subprogram_declaration;

• An aspect specified on a renaming_declaration.

{AI05-0183-1} All other aspect specifications are associated with the entity, and apply to all views of the entity, unless otherwise specified in this document.

{AI05-0183-1} {AI12-0106-1} If the aspect mark includes 'Class (a class-wide aspect), then, unless specified otherwise for a particular class-wide aspect:

• if the associated entity is a tagged type, the specification applies to all descendants of the type;

• if the associated entity is a primitive subprogram of a tagged type T, the specification applies to the corresponding primitive subprogram of all descendants of T.

{AI05-0183-1} {AI05-0229-1} All specifiable operational and representation attributes may be specified with an aspect specification instead of an attribute_definition_clause (see 13.3).

Ramification: The name of the aspect is the same as that of the attribute (see 13.3), so the aspect mark is the attribute_designator of the attribute.

{AI12-0005-1} Unless specified otherwise, all of the requirements for specifying a particular aspect with an attribute_definition_clause also apply to an aspect specification for the aspect. These are enforced at the freezing point of the entity. For example, when specifying the Size aspect of a subtype, the expression has to be a static expression with an integer type and a nonnegative value, all of the recommended level of support requirements apply if Annex C is supported (see C.2), and so on.

{AI05-0229-1} {AI12-0154-1} {AI12-0417-1} Some aspects are defined to be library unit aspects. Library unit aspects are:

Any aspect specified by a representation pragma or library unit pragma that has a local_name as its single argument may be specified by an aspect specification, with the entity being the local name. The aspect definition is expected to be of type Boolean. The expression specifying a library unit aspect shall be static. Library unit aspects are defined for all program units, but shall be specified only for library units. Notwithstanding what this document says elsewhere, the expression of a library unit aspect that can be specified by a library unit pragma is resolved and evaluated at the point where it occurs in the aspect specification, rather than the first freezing point of the associated unit/package.

Ramification: The name of the aspect is the same as that of the pragma (see 13.1), so the aspect mark is the name of the pragma.

{AI05-0229-1} In addition, other operational and representation aspects not associated with specifiable attributes or representation pragmas may be specified, as specified elsewhere in this document.
If an aspect of a derived type is inherited from an ancestor type and has the boolean value True, the inherited value shall not be overridden to have the value False for the derived type, unless otherwise specified in this document.

Reason: Some rules only apply when an aspect has been specified (for instance, an indexable type is one that has aspect Variable_Indexing specified). In order to prevent privacy breaking, this can only be true when the specification of the aspect is visible. In particular, if the Variable_Indexing aspect is specified on the full view of a private type, the private type is not considered an indexable type.

Alternative legality and semantics rules may apply for particular aspects, as specified elsewhere in this document.

Dynamic Semantics

At the freezing point of the associated entity, the aspect specification is elaborated. When appearing in a construct other than a declaration, an aspect specification is elaborated as part of the execution of the construct. The elaboration of the aspect specification consists of the elaboration of each aspect definition in an arbitrary order. The elaboration of an aspect definition includes the evaluation of any the name or expression that is part of the aspect definition, if any, unless the part is itself an expression. If the corresponding aspect (or part thereof) represents an expression (as in a precondition), the elaboration of that part has no effect; the expression is evaluated later at points within the execution as specified elsewhere in this document for the particular aspect.

Implementation Permissions

Implementations may support implementation-defined aspects. The aspect specification for an implementation-defined aspect may use an implementation-defined syntax for the aspect definition, and may follow implementation-defined legality and semantics rules.

Discussion: The intent is to allow implementations to support aspects that are defined, for example, by a subtype indication rather than an expression or a name. We chose not to try to enumerate all possible aspect definition syntaxes, but to give implementations maximum freedom. Unrecognized aspects are illegal, whether or not they use custom syntax, so this freedom does not reduce portability.

Implementation defined: Implementation-defined aspects, including the syntax for specifying such aspects and the legality rules for such aspects.

An implementation may ignore the specification of an unrecognized aspect; if an implementation chooses to ignore such an aspect specification (as opposed to rejecting it), then it has no effect on the semantics of the program except for possibly (and this is not required) the rejection of syntax errors within the aspect definition.

Discussion: Identifying the textual end of an aspect definition for an unrecognized aspect may be challenging, particularly if the syntax for the unrecognized aspect's aspect definition is implementation-defined. It is not specified how an implementation might accomplish this. Note that an implementation is never required to be able to do this; if an aspect definition for an unrecognized aspect is problematic in any way, then it can always be rejected (as opposed to being ignored).

Extensions to Ada 2005

Aspect specifications are new.

Inconsistencies With Ada 2012

Correction: Names of protected subprograms and entries are now directly visible in an aspect of a type declaration. This was always intended to be the case, but it was omitted from the Reference Manual by an editing error. In the unlikely case that a parameterless protected function has the same name and type as an entity used in a type
invariant expression, the meaning would change from the outside entity which would now be hidden by the protected function. It is much more likely that a conflict (itself rather unlikely) would cause a resolution failure.

**Incompatibilities With Ada 2012**

\{AI12-0154-1\} Corrigendum: Added a clarification that aspects that correspond to library unit pragmas are resolved and evaluated immediately. However, this would have required retroactive enforcement of such aspects, which is a new capability not available from the associated pragma, and moreover no known Ada 2012 implementation has ever allowed late evaluation of such aspects. As such, there should be no practical incompatibility.

\{AI12-0005-1\} \{AI12-0220-1\} Parameters of access-to-subprogram types are now visible in aspect specifications. This can be incompatible if some entity with the same name as a parameter is used in an existing aspect specification. We believe that all such aspects require either static expressions or a subprogram that is statically denoted; since a parameter can be neither of these and hides everything else, all such cases will be caught at compile-time. In addition, we expect such cases to be very rare.

**Extensions to Ada 2012**

\{AI12-0212-1\} An aspect can be an unresolved aggregate, these can be used to specify a list of entities, or to set a group of different but related properties with a single aspect.

\{AI12-0355-2\} Aspect specifications can appear in, and apply to, constructs other than declarations.

\{AI12-0389-1\} An unrecognized aspect specification can be ignored.

**Wording Changes from Ada 2012**

\{AI12-0105-1\} Corrigendum: Clarified the wording so that the restriction against language-defined aspects on subprogram completions includes completions that are expressions functions and null procedures.


\{AI12-0138-1\} Corrigendum: Added a definition of nonoverridable aspects. This is necessary to prevent generic contract problems with formal derived types.

\{AI12-0194-1\} Correction: Added entry_body to the list of entities that don't allow any language-defined aspects. This was an oversight in AI12-0169-1 which allowed aspect_specifications on an entry_body in the first place.

\{AI12-0206-1\} Correction: Extended the definition of nonoverridable aspects to cover most kinds of aspects.

\{AI12-0211-1\} Correction: Added a rule so that the a nonoverridable aspect has to be the same for every ancestor of a type.

\{AI12-0355-2\} \{AI12-0427-1\} Clarified when elaboration and resolution of aspect_specifications not associated with a declaration occur.

\{AI12-0380-1\} \{AI12-0407-1\} Revises the rules about entities that cannot have specified language-defined aspects. The body portion of the rule was changed to a general prohibition on specifying language-defined aspects on completions (this allows specifying aspects on bodies that act as a declaration, and eliminates the list of entities, which was a maintenance nightmare). Then the remaining entities (renamings and generic formal parameters) were revised to allow specific aspects, since Nonblocking (see 9.5), as well as Pre and Post, are now allowed on generic formal parameters.

\{AI12-0373-1\} Added the missing definition for resolution of entities found in aspects of library units.

\{AI12-0396-1\} Correction: Defined confirming for nonoverridable aspects that are expressions or aggregates.

\{AI12-0419-1\} Added a description of additive and implicitly composed aspects in order to explain the different inheritance mechanisms used by existing aspects.

**Incompatibilities With Ada 2022**

\{AI22-0002-1\} Corrigendum: If a nonoverridable aspect is specified by a subprogram that is not primitive, and the associated type is never derived, the program was legal in Ada 2022 but now is illegal. (If the type was derived, it was unclear what would happen; the subprogram would have parameters and/or results of the wrong type.)

### 13.2 Packed Types

Pragma Pac

\{AI05-0229-1\} The Pack aspect having the value True, pragma Pack specifies that storage minimization should be the main criterion when selecting the representation of a composite type.]
Paragraphs 2 through 4 were moved to Annex J, “Obsolescent Features”.

Language Design Principles

1.a/4 {AI12-0001-1} If the default representation already uses minimal storage for a particular type, aspect Pack might not cause any representation change. It follows that aspect Pack should always be allowed, even when it has no effect on representation.

1.b/4 As a consequence, the chosen representation for a packed type may change during program maintenance even if the type is unchanged (in particular, if other representation aspects change on a part of the type). This is different than the behavior of most other representation aspects, whose properties remain guaranteed no matter what changes are made to other aspects.

Therefore, aspect Pack should not be used to achieve a representation required by external criteria. For instance, setting Component_Size to 1 should be preferred over using aspect Pack to ensure an array of bits. If future maintenance would make the array components aliased, independent, or atomic, the program would become illegal if Component_Size is used (immediately identifying a problem) while the aspect Pack version would simply change representations (probably causing a hard-to-find bug).

Syntax

{AI05-0229-1} The form of a pragma Pack is as follows:

```
pragma Pack(first_subtype_local_name);
```

Legality Rules

{AI05-0229-1} The first_subtype_local_name of a pragma Pack shall denote a composite subtype.

Static Semantics

{AI05-0229-1} For a full type declaration of a composite type, the following language-defined representation aspect may be specified: A pragma Pack specifies the packing aspect of representation; the type (or the extension part) is said to be packed. For a type extension, the parent part is packed as for the parent type, and a pragma Pack causes packing only of the extension part.

5.1/3 Pack

The type of aspect Pack is Boolean. When aspect Pack is True for a type, the type (or the extension part) is said to be packed. For a type extension, the parent part is packed as for the parent type, and specifying Pack causes packing only of the extension part.

5.a/3 Aspect Description for Pack: Minimize storage when laying out records and arrays.

5.2/3 If directly specified, the aspect_definition shall be a static expression. If not specified (including by inheritance), the aspect is False.

5.b/3 Ramification: {AI05-0229-1} The only high level semantic effect of specifying the pragma Pack aspect is potential loss of independent addressability (see 9.10, “Shared Variables”).

Implementation Advice

6 If a type is packed, then the implementation should try to minimize storage allocated to objects of the type, possibly at the expense of speed of accessing components, subject to reasonable complexity in addressing calculations.

6.a.1/2 Implementation Advice: Storage allocated to objects of a packed type should be minimized.

6.a/3 Ramification: {AI05-0229-1} Specifying the pragma Pack aspect is for gaining space efficiency, possibly at the expense of time. If more explicit control over representation is desired, then a record_representation_clause, a Component_Size clause, or a Size clause should be used instead of, or in addition to, the pragma Pack aspect.

6.1/4 This paragraph was deleted. {AI95-00291-02} {AI12-0001-1} If a packed type has a component that is not of a by-reference type and has no aliased part, then such a component need not be aligned according to the Alignment of its subtype; in particular it need not be allocated on a storage element boundary.

7/3 {AI05-0229-1} The recommended level of support for the pragma Pack aspect is:
• \{AI12-0001-1\} Any component of a packed type that is of a by-reference type, that is specified as independently addressable, or that contains an aliased part, shall be aligned according to the alignment of its subtype.

  **Ramification:** This also applies to atomic components. "Atomic" implies "specified as independently addressable", so we don't need to mention atomic here.

  Other components do not have to respect the alignment of the subtype when packed; in many cases, the Recommended Level of Support will require the alignment to be ignored.

• \{AI12-0001-1\} \{AI12-0444-1\} For a packed record type, the components should be packed as tightly as possible subject to the above alignment requirements, the Sizes of the component subtypes, and subject to any record_representation_clause that applies to the type; the implementation is allowed to reorder components or cross aligned word boundaries to improve the packing. A component whose Size is greater than the word size may be allocated an integral number of words.

  **Ramification:** The implementation can always allocate an integral number of words for a component that will not fit in a word. The rule also allows small component sizes to be rounded up if such rounding does not waste space. For example, if Storage_Unit = 8, then a component of size 8 is probably more efficient than a component of size 7 plus a 1-bit gap (assuming the gap is needed anyway).

• \{AI05-0009-1\} \{AI12-0001-1\} For a packed array type, if the component subtype's Size of the component subtype is less than or equal to the word size, and Component_Size is not specified for the type, Component_Size should be less than or equal to the Size of the component subtype, rounded up to the nearest factor of the word size, unless this would violate the above alignment requirements.

  This paragraph was deleted. **Ramification:** \{AI12-0001-1\} If a component subtype is aliased, its Size will generally be a multiple of Storage_Unit, so it probably won't get packed very tightly.

  **Implementation Advice:** The recommended level of support for the pragma Pack aspect should be followed.

**Wording Changes from Ada 95**

\{AI95-00291-02\} \{AI05-0229-1\} Added clarification that the pragma Pack aspect can ignore alignment requirements on types that don't have by-reference or aliased parts. This was always intended, but there was no wording to that effect.

**Extensions to Ada 2005**

\{AI05-0229-1\} Aspect Pack is new; pragma Pack is now obsolescent.

**Wording Changes from Ada 2005**

\{AI05-0009-1\} **Correction:** Fixed so that the presence or absence of a confirming Component_Size representation clause does not change the meaning of the Pack aspect.

**Wording Changes from Ada 2012**

\{AI12-0001-1\} **Corrigendum:** Fixed so that the Recommended Level of Support does not require packing of components for which such packing would violate other representation items or aspects. This is not incompatible, as either such Pack aspects were treated as illegal or the Recommended Level of Support was ignored as impractical, neither of which would change the behavior of any working programs. (Other behavior cannot be justified from the Reference Manual.)

### 13.3 Operational and Representation Attributes

\{8652/0009\} \{AI95-00137-01\} [ The values of certain implementation-dependent characteristics can be obtained by interrogating appropriate operational or representation attributes. Some of these attributes are specifiable via an attribute_definition_clause.]

---

689 16 October 2023 Packed Types 13.2
Language Design Principles

1.a In general, the meaning of a given attribute should not depend on whether the attribute was specified via an attribute_definition_clause, or chosen by default by the implementation.

Syntax

2 attribute_definition_clause ::= for local_name'attribute_designator use expression; | for local_name'attribute_designator use name;

Name Resolution Rules

3 For an attribute_definition_clause that specifies an attribute that denotes a value, the form with an expression shall be used. Otherwise, the form with a name shall be used.

4 For an attribute_definition_clause that specifies an attribute that denotes a value or an object, the expected type for the expression or name is that of the attribute. For an attribute_definition_clause that specifies an attribute that denotes a subprogram, the expected profile for the name is the profile required for the attribute. For an attribute_definition_clause that specifies an attribute that denotes some other kind of entity, the name shall resolve to denote an entity of the appropriate kind.

Ramification: For example, the Size attribute is of type universal_integer. Therefore, the expected type for Y in “for X'Size use Y;” is universal_integer, which means that Y can be of any integer type.

Discussion: For attributes that denote subprograms, the required profile is indicated separately for the individual attributes.

Ramification: For an attribute_definition_clause with a name, the name need not statically denote the entity it denotes. For example, the following kinds of things are allowed:

for Some_Access_Type'Storage_Pool use Storage_Pool_Array(I); for Some_Type'Read use Subprogram_Pointer.all;

Legality Rules

5/3 \{8652/0009\} \{AI95-00137-01\} \{AI05-0183-1\} An attribute_designator is allowed in an attribute_definition_clause only if this Reference Manual explicitly allows it, or for an implementation-defined attribute if the implementation allows it. Each specifiable attribute constitutes an operational aspect or aspect of representation; the name of the aspect is that of the attribute.

Discussion: For each specifiable attribute, we generally say something like, “The ... attribute may be specified for ... via an attribute_definition_clause.”

The above wording allows for T'Class'Alignment, T'Class'Size, T'Class'Input, and T'Class'Output to be specifiable.

A specifiable attribute is not necessarily specifiable for all entities for which it is defined. For example, one is allowed to ask T'Component_Size for an array subtype T, but “for T'Component_Size use ...” is only allowed if T is a first subtype, because Component_Size is a type-related aspect.

This paragraph was deleted.\{AI12-0427-1\} For an attribute_definition_clause that specifies an attribute that denotes a subprogram, the profile shall be mode conformant with the one required for the attribute, and the convention shall be Ada. Additional requirements are defined for particular attributes.

6/5 \{AI95-00270-01\} A Size clause is an attribute_definition_clause whose attribute_designator is Size. Similar definitions apply to the other specifiable attributes.

To be honest: An attribute_definition_clause is type-related or subtype-specific if the attribute_designator denotes a type-related or subtype-specific attribute, respectively.

13.3 Operational and Representation Attributes 16 October 2023 690
A storage element is an addressable element of storage in the machine. A word is the largest amount of storage that can be conveniently and efficiently manipulated by the hardware, given the implementation's run-time model. A word consists of an integral number of storage elements.

Discussion: A storage element is not intended to be a single bit, unless the machine can efficiently address individual bits.

Ramification: For example, on a machine with 8-bit storage elements, if there exist 32-bit integer registers, with a full set of arithmetic and logical instructions to manipulate those registers, a word ought to be 4 storage elements — that is, 32 bits.

Discussion: The “given the implementation's run-time model” part is intended to imply that, for example, on an 80386 running MS-DOS, the word might be 16 bits, even though the hardware can support 32 bits.

A word is what ACID refers to as a “natural hardware boundary”.

Storage elements may, but need not be, independently addressable (see 9.10, “Shared Variables”). Words are expected to be independently addressable.

{AI95-00133-01} {AI05-0092-1} A machine scalar is an amount of storage that can be conveniently and efficiently loaded, stored, or operated upon by the hardware. Machine scalars consist of an integral number of storage elements. The set of machine scalars is implementation defined, but includes must include at least the storage element and the word. Machine scalars are used to interpret component clauses when the nondefault bit ordering applies.

Implementation defined: The set of machine scalars.

Ramification: {AI05-0092-1} A single storage element is a machine scalar in all Ada implementations. Similarly, a word is a machine scalar in all implementations (although it might be the same as a storage element). An implementation may define other machine scalars that make sense on the target (a half-word, for instance).

{8652/0009} {AI95-00137-01} {AI05-0191-1} {AI12-0059-1} The following representation attributes are defined: Address, Alignment, Size, Object Size, Storage Size, and Component Size. Has Same Storage, and Overlaps Storage. The following attributes are defined:

For a prefix X that denotes an object, program unit, or label:

X'Address Denotes the address of the first of the storage elements allocated to X. For a program unit or label, this value refers to the machine code associated with the corresponding body or statement. The value of this attribute is of type System.Address.

Ramification: Here, the “first of the storage elements” is intended to mean the one with the lowest address; the endianness of the machine doesn't matter.

{AI05-0095-1} The prefix of X'Address shall not statically denote a subprogram that has convention Intrinsic. X'Address raises Program_Error if X denotes a subprogram that has convention Intrinsic.

Address may be specified for stand-alone objects and for program units via an attribute_definition_clause.

Ramification: Address is not allowed for enumeration literals, predefined operators, derived task types, or derived protected types, since they are not program units.

Address is not allowed for intrinsic subprograms, either. That can be checked statically unless the prefix is a generic formal subprogram and the attribute reference is in the body of a generic unit. We define that case to raise Program_Error, in order that the compiler does not have to build a wrapper for intrinsic subprograms.

The validity of a given address depends on the run-time model; thus, in order to use Address clauses correctly, one needs intimate knowledge of the run-time model.

{AI05-0229-1} If the Address of an object is specified, any explicit or implicit initialization takes place as usual, unless the pragma Import aspect is also specified for the object (in which case any necessary initialization is presumably done in the foreign language).

Any compilation unit containing an attribute_reference of a given type depends semantically on the declaration of the package in which the type is declared, even if not mentioned in an applicable with_clause — see 10.1.1. In this case, it means that if a compilation unit contains X'Address, then it depends on the declaration of System. Otherwise, the fact
that the value of Address is of a type in System wouldn't make sense; it would violate the “legality determinable via semantic dependences” Language Design Principle.

AI83-00305 — If X is a task type, then within the body of X, X denotes the current task object; thus, X'Address denotes the object's address.

Interrupt entries and their addresses are described in J.7.1, “Interrupt Entries”.

If X is not allocated on a storage element boundary, X'Address points at the first of the storage elements that contains any part of X. This is important for the definition of the Position attribute to be sensible.

**Aspect Description for Address:** Machine address of an entity.

**Erroneous Execution**

{AI05-0009-1} If an Address is specified, it is the programmer's responsibility to ensure that the address is valid and appropriate for the entity and its use; otherwise, program execution is erroneous.

**Discussion:** “Appropriate for the entity and its use” covers cases such as misaligned addresses, read-only code addresses for variable data objects (and nonexecutable data addresses for code units), and addresses which would force objects that are supposed to be independently addressable to not be. Such addresses may be “valid” as they designate locations that are accessible to the program, but the program execution is still erroneous (meaning that implementations do not have to worry about these cases).

**Implementation Advice**

For an array X, X'Address should point at the first component of the array, and not at the array bounds.

**Implementation Advice:** For an array X, X'Address should point at the first component of the array rather than the array bounds.

**Ramification:** On the other hand, we have no advice to offer about discriminants and tag fields; whether or not the address points at them is not specified by the language. If discriminants are stored separately, then the Position of a discriminant might be negative, or might raise an exception.

The recommended level of support for the Address attribute is:

- X'Address should produce a useful result if X is an object that is aliased or of a by-reference type, or is an entity whose Address has been specified.

  **Reason:** Aliased objects are the ones for which the Unchecked_Access attribute is allowed; hence, these have to be allocated on an addressable boundary anyway. Similar considerations apply to objects of a by-reference type.

- An implementation need not go to any trouble to make Address work in other cases. For example, if an object X is not aliased and not of a by-reference type, and the implementation chooses to store it in a register, X'Address might return System.Null_Address (assuming registers are not addressable). For a subprogram whose calling convention is Intrinsic, or for a package, the implementation need not generate an out-of-line piece of code for it.

- An implementation should support Address clauses for imported subprograms.

  **This paragraph was deleted** {AI95-00291-02} Objects (including subcomponents) that are aliased or of a by-reference type should be allocated on storage element boundaries.

  **Reason:** This is necessary for the Address attribute to be useful (since First_Bit and Last_Bit apply only to components). Implementations generally need to do this anyway, for tasking to work properly.

- If the Address of an object is specified, or it is imported or exported, then the implementation should not perform optimizations based on assumptions of no aliases.

  **Implementation Advice:** The recommended level of support for the Address attribute should be followed.

**NOTE 1** The specification of a link name with the Link_Name aspect in a pragma Export (see B.1) for a subprogram or object is an alternative to explicit specification of its link-time address, allowing a link-time directive to place the subprogram or object within memory.

**NOTE 2** The rules for the Size attribute imply, for an aliased object X, that if X'Size = Storage_Unit, then X'Address points at a storage element containing all of the bits of X, and only the bits of X.

**Wording Changes from Ada 83**

The intended meaning of the various attributes, and their attribute_definition_clauses, is more explicit.
The address_clause has been renamed to at_clause and moved to Annex J, “Obsolescent Features”. One can use an Address clause (“for T'Address use ...”) instead.

The attributes defined in RM83-13.7.3 are moved to Annex G, A.5.3, and A.5.4.

Wording Changes from Ada 2005

{AI05-0183-1} Defined that the names of aspects are the same as the name of the attribute; that gives a name to use in aspect specifications (see 13.1.1).

Language Design Principles

By default, the Alignment of a subtype should reflect the “natural” alignment for objects of the subtype on the machine. The Alignment, whether specified or default, should be known at compile time, even though Addresses are generally not known at compile time. (The generated code should never need to check at run time the number of zero bits at the end of an address to determine an alignment).

There are two symmetric purposes of Alignment clauses, depending on whether or not the implementation has control over object allocation. If the implementation allocates an object, the implementation should ensure that the Address and Alignment are consistent with each other. If something outside the implementation allocates an object, the implementation should be allowed to assume that the Address and Alignment are consistent, but should not assume stricter alignments than that.

Static Semantics

{AI95-00291-02} For a prefix X that denotes a subtype or object:

21.b

X'Alignment

21.c

The value of this attribute is of type universal_integer, and nonnegative; zero means that the object is not necessarily aligned on a storage element boundary. If X'Alignment is not zero, then X is aligned on a storage unit boundary and X'Address of an object that is allocated under control of the implementation is an integral multiple of X'Alignment the Alignment of the object (that is, the Address modulo the Alignment is zero). The offset of a record component is a multiple of the Alignment of the component. For an object that is not allocated under control of the implementation (that is, one that is imported, that is allocated by a user-defined allocator, whose Address has been specified, or is designated by an access value returned by an instance of Unchecked_Conversion), the implementation may assume that the Address is an integral multiple of its Alignment. The implementation shall not assume a stricter alignment.

This paragraph was deleted.

24.b

Alignment may be specified for first subtypes and [stand-alone] objects via an attribute_definition_clause; the expression of such a clause shall be static, and its value nonnegative. If the Alignment of a subtype is specified, then the Alignment of an object of the subtype is at least as strict, unless the object's Alignment is also specified. The Alignment of an object created by an allocator is that of the designated subtype.

Aspect Description for Alignment (object):

25.a/3

Alignment of an object.
For every subtype \( S \):

\[ S'\text{Alignment} \]

The value of this attribute is of type `universal_integer`, and nonnegative.

For an object \( X \) of subtype \( S \), if \( S'\text{Alignment} \) is not zero, then \( X'\text{Alignment} \) is a nonzero integral multiple of \( S'\text{Alignment} \) unless specified otherwise by a representation item.

Alignment may be specified for first subtypes via an `attribute_definition_clause`; the expression of such a clause shall be static, and its value nonnegative.

Aspect Description for Alignment (subtype): Alignment of a subtype.

Program execution is erroneous if an Address clause is given that conflicts with the Alignment.

Ramification: The user has to either give an Alignment clause also, or else know what Alignment the implementation will choose by default.

If the Alignment is specified for an object that is not allocated under control of the implementation, execution is erroneous if the object is not aligned according to its Alignment.

For any tagged specific subtype \( S \), \( S'\text{Class'Alignment} \) should equal \( S'\text{Alignment} \).

Reason: A tagged object should never be less aligned than the alignment of the type of its view, so for a class-wide type \( T'\text{Class} \), the alignment should be no greater than that of any type covered by \( T'\text{Class} \). If the implementation only supports alignments that are required by the recommended level of support (and this is most likely), then the alignment of any covered type has to be the same or greater than that of \( T \) — which leaves the only reasonable value of \( T'\text{Class'Alignment} \) being \( T'\text{Alignment} \). Thus we recommend this, but don't require it so that in the unlikely case that the implementation does support smaller alignments for covered types, it can select a smaller value for \( T'\text{Class'Alignment} \).

Implementation Advice: For any tagged specific subtype \( S \), \( S'\text{Class'Alignment} \) should equal \( S'\text{Alignment} \).

The recommended level of support for the Alignment attribute for subtypes is:

- An implementation should support an Alignment clause for a discrete type, fixed point type, record type, or array type, specifying an Alignment value that is zero or a power of two.
- An implementation is not required to support an Alignment clause for a signed integer type specifying an Alignment greater than the largest Alignment value that is ever chosen by default by the implementation for any signed integer type.
- An implementation is not required to support an Alignment clause that can cause which could enable the creation of an object of an elementary type that which cannot be easily loaded and stored by available machine instructions.
- An implementation is not required to support a nonconfirming Alignment clause that can cause which could enable the creation of an object of a derived tagged type that which is not a multiple of the Alignment of the parent type. An implementation is not required to support a nonconfirming Alignment specified for a derived untagged by-reference type.
The recommended level of support for the Alignment attribute for objects is:

- For stand-alone library-level objects of statically constrained subtypes, the implementation should support all Alignments supported by the target linker. For example, page alignment is likely to be supported for such objects, but not for subtypes.

- For other objects, an implementation should at least support the alignments supported for their subtype, subject to the following:
- An implementation is not required to support Alignments specified for objects of a by-reference type or for objects of types containing aliased subcomponents if the specified Alignment is not a multiple of the Alignment of the subtype of the object.

Implementation Advice: The recommended level of support for the Alignment attribute should be followed.

NOTE 3 Alignment is a subtype-specific attribute.

NOTE 4 The Alignment of a composite object is always equal to the least common multiple of the Alignments of its components, or a multiple thereof.

NOTE 5 A component_clause, Component_Size clause, or specifying the pragma Pack aspect as True can override a specified Alignment.

Discussion: Most objects are allocated by the implementation; for these, the implementation obeys the Alignment. The implementation is of course allowed to make an object more aligned than its Alignment requires — an object whose Alignment is 4 might just happen to land at an address that's a multiple of 4096. For formal parameters, the implementation might want to force an Alignment stricter than the parameter's subtype. For example, on some systems, it is customary to always align parameters to 4 storage elements. Hence, one might initially assume that the implementation could evilly make all Alignments 1 by default, even though integers, say, are normally aligned on a 4-storage-element boundary. However, the implementation cannot get away with that — if the Alignment is 1, the generated code cannot assume an Alignment of 4, at least not for objects allocated outside the control of the implementation.

Of course implementations can assume anything they can prove, but typically an implementation will be unable to prove much about the alignment of, say, an imported object. Furthermore, the information about where an address “came from” can be lost to the compiler due to separate compilation.

Specifying an Alignment of 0 in an attribute_definition_clause does not require the implementation to do anything (except return 0 when the Alignment is queried). However, it might be taken as advice on some implementations.

If the machine has no particular natural alignments, then all subtype Alignments will probably be 1 by default.

It is an error for an Address clause to disobey the object’s Alignment. The error cannot be detected at compile time, in general, because the Address is not necessarily known at compile time (and is almost certainly not static). We do not require a runtime check, since efficiency seems paramount here, and Address clauses are treading on thin ice anyway. Hence, this misuse of Address clauses is just like any other misuse of Address clauses — it’s erroneous.
A type extension can have a stricter Alignment than its parent. This can happen, for example, if the Alignment of the parent is 4, but the extension contains a component with Alignment 8. The Alignment of a class-wide type or object will have to be the maximum possible Alignment of any extension.

The recommended level of support for the Alignment attribute is intended to reflect a minimum useful set of capabilities. An implementation can assume that all Alignments are multiples of each other — 1, 2, 4, and 8 might be the only supported Alignments for subtypes. An Alignment of 3 or 6 is unlikely to be useful. For objects that can be allocated statically, we recommend that the implementation support larger alignments, such as 4096. We do not recommend such large alignments for subtypes, because the maximum subtype alignment will also have to be used as the alignment of stack frames, heap objects, and class-wide objects. Similarly, we do not recommend such large alignments for stack-allocated objects.

If the maximum default Alignment is 8 (say, Long_Float'Alignment = 8), then the implementation can refuse to accept stricter alignments for subtypes. This simplifies the generated code, since the compiler can align the stack and class-wide types to this maximum without a substantial waste of space (or time).

Note that the recommended level of support takes into account interactions between Size and Alignment. For example, on a 32-bit machine with 8-bit storage elements, where load and store instructions have to be aligned according to the size of the thing being loaded or stored, the implementation might accept an Alignment of 1 if the Size is 8, but might reject an Alignment of 1 if the Size is 32. On a machine where unaligned loads and stores are merely inefficient (as opposed to causing hardware traps), we would expect an Alignment of 1 to be supported for any Size.

**Wording Changes from Ada 83**

{AI12-0005-1} The nonnegative part is missing from RM83 (for mod_clauses, known in Ada 83 as alignment_clauses, which are an obsolete version of Alignment clauses).

**Static Semantics**

For a prefix X that denotes an object:

X'Size Denotes the size in bits of the representation of the object. The value of this attribute is of the type universal_integer.

**Ramification:** Note that Size is in bits even if Machine_Radix is 10. Each decimal digit (and the sign) is presumably represented as some number of bits.

Size may be specified for [stand-alone] objects via an attribute_definition_clause; the expression of such a clause shall be static and its value nonnegative.

**Aspect Description for Size (object):** Size in bits of an object.

**Implementation Advice**

{AI95-00051-02} The size of an array object should not include its bounds.

**Implementation Advice:** The Size of an array object should not include its bounds.

{AI95-00051-02} {AI95-00291-02} {AI12-0445-1} The recommended level of support for the Size attribute of objects is the same as for subtypes (see below), except that only a confirming Size clause is required to be supported for an aliased elementary object.

• This paragraph was deleted. {AI95-00051-02} A Size clause should be supported for an object if the specified Size is at least as large as its subtype's Size, and corresponds to a size in storage elements that is a multiple of the object's Alignment (if the Alignment is nonzero).

**Static Semantics**

For every subtype S:

S'Size If S is definite, denotes the size [(in bits)] that the implementation would choose for the following objects of subtype S:

• A record component of subtype S when the record type is packed.

• The formal parameter of an instance of Unchecked_Conversion that converts from subtype S to some other subtype.
If S is indefinite, the meaning is implementation defined. The value of this attribute is of the type universal_integer. The Size of an object is at least as large as that of its subtype, unless the object's Size is determined by a Size clause, a component_clause, or a Component_Size clause. Size may be specified for first subtypes via an attribute_definition_clause; the expression of such a clause shall be static and its value nonnegative.

Implementation defined: The meaning of Size for indefinite subtypes.

Reason: The effects of specifying the Size of a subtype are:

- Unchecked_Conversion works in a predictable manner.
- A composite type cannot be packed so tightly as to override the specified Size of a component's subtype.
- Assuming the Implementation Advice is obeyed, if the specified Size allows independent addressability, then the Size of certain objects of the subtype should be equal to the subtype's Size. This applies to stand-alone objects and to components (unless a component_clause or a Component_Size clause applies).

Implementation Advice: If the Size of a subtype is nonconfirming and allows for efficient independent addressability (see 9.10) on the target architecture, then the Object_Size of the following objects of the subtype should have the same value in the absence of an explicit specification of a different value equal the Size of the subtype:

- Aliased objects (including components).
- Unaliased components, unless the Size of the component is determined by a component_clause or Component_Size clause.

Ramification: The Size of a large unconstrained subtype (e.g. String'Size) is likely to raise Constraint_Error, since it is a nonstatic expression of type universal_integer that might overflow the largest signed integer type. There is no requirement that the largest integer type be able to represent the size in bits of the largest possible object.
Implementation Note: On the other hand, if one writes, “for S2'Size use 5;” then stand-alone objects of subtype S2 will typically have their Size rounded up to ensure independent addressability.

Note that “for S'Size use 32;” does not cause things like formal parameters to have Size = 32 — the implementation is allowed to make all parameters be at least 64 bits, for example.

Note that “for S2'Size use 5;” requires record components whose subtype is S2 to be exactly 5 bits if the record type is packed. The same is not true of array components; their Size may be rounded up to the nearest factor of the word size.

Implementation Note: On most machines, arrays don't contain gaps between elementary components; if the Component_Size is greater than the Size of the component subtype, the extra bits are generally considered part of each component, rather than gaps between components. On the other hand, a record might contain gaps between elementary components, depending on what sorts of loads, stores, and masking operations are generally done by the generated code.

Implementation Note: On most machines, arrays don't contain gaps between elementary components; if the Component_Size is greater than the Size of the component subtype, the extra bits are generally considered part of each component, rather than gaps between components. On the other hand, a record might contain gaps between elementary components, depending on what sorts of loads, stores, and masking operations are generally done by the generated code.

A Size clause on a composite subtype should not affect the internal layout of components.

The recommended level of support for the Size attribute of subtypes is:

• The Size (if not specified) of a static discrete or fixed point subtype should be the number of bits necessary to represent each value belonging to the subtype using an unbiased representation, leaving space for a sign bit only if the subtype contains negative values. If such a subtype is a first subtype, then an implementation should support a specified Size for it that reflects this representation.

Implementation Note: This applies to static enumeration subtypes, using the internal codes used to represent the values.

For a two's-complement machine, this implies that for a static signed integer subtype S, if all values of S are in the range 0..2^–1, or all values of S are in the range –2^–1..2^–1, for some n less than or equal to the word size, then S'Size should be <= the smallest such n. For a one's-complement machine, it is the same except that in the second range, the lower bound “–2^n” is replaced by “–2^(n+1)”.

If an integer subtype (whether signed or unsigned) contains no negative values, the Size should not include space for a sign bit. Typically, the implementation will choose to make the Size of a subtype be exactly the smallest such n. However, it might, for example, choose a biased representation, in which case it could choose a smaller value.

On most machines, it is in general not a good idea to pack (parts of) multiple stand-alone objects into the same storage element, because (1) it usually doesn't save much space, and (2) it requires locking to prevent tasks from interfering with each other, since separate stand-alone objects are independently addressable. Therefore, if S'Size = 2 on a machine with 8-bit storage elements, the size of a stand-alone object of subtype S will probably not be 2. It might, for example, be 8, 16 or 32, depending on the availability and efficiency of various machine instructions. The same applies to components of composite types, unless Packing, Component_Size, or record layout is specified.

For an unconstrained discriminated object, if the implementation allocates the maximum possible size, then the Size attribute should return that maximum possible size.

Ramification: The Size of an object X is not usually the same as that of its subtype S. If X is a stand-alone object or a parameter, for example, most implementations will round X'Size up to a storage element boundary, or more, so X'Size might be greater than S'Size. On the other hand, X'Size cannot be less than S'Size, even if the implementation can prove, for example, that the range of values actually taken on by X during execution is smaller than the range of S.

For example, if S is a first integer subtype whose range is 0..3, S'Size will be probably be 2 bits, and components of packed composite types of this subtype will be 2 bits (assuming Storage_Unit is a multiple of 2), but stand-alone
objects and parameters will probably not have a size of 2 bits; they might be rounded up to 32 bits, for example. On the other hand, Unchecked_Conversion will use the 2-bit size, even when converting a stand-alone object, as one would expect.

Another reason for making the Size of an object bigger than its subtype's Size is to support the run-time detection of uninitialized variables. The implementation might add an extra value to a discrete subtype that represents the uninitialized state, and check for this value on use. In some cases, the extra value will require an extra bit in the representation of the object. Such detection is not required by the language. If it is provided, the implementation has to be able to turn it off. For example, if the programmer gives a record_representation_clause or Component_Size clause that makes a component too small to allow the extra bit, then the implementation will not be able to perform the checking (not using this method, anyway).

The fact that the size of an object is not necessarily the same as its subtype can be confusing:

```ada
type Device_Register is range 0..2**8 - 1;
for Device_Register'Size use 8; -- Confusing!
My_Device : Device_Register;
for My_Device'Address use To_Address(16#FF00#);
```

{AI12-0005-1} The programmer might think that My_Device'Size is 8, and that My_Device'Address points at an 8-bit location. However, this is not guaranteed to be true. In Ada 83 (and in Ada 95), My_Device'Size might well be 32, and My_Device'Address might well point at the high-order 8 bits of the 32-bit object, which are always all zero bits. If My_Device'Address is passed to an assembly language subprogram, based on the programmer's assumption, the program will not work properly.

**Reason:** It is not reasonable to require that an implementation allocate exactly 8 bits to all objects of subtype Device_Register. For example, in many run-time models, stand-alone objects and parameters are always aligned to a word boundary. Such run-time models are generally based on hardware considerations that are beyond the control of the implementer. (It is reasonable to require that an implementation allocate exactly 8 bits to all components of subtype Device_Register, if packed.)

**Ramification:** The correct way to write the above code is like this:

```ada
type Device_Register is range 0..2**8 - 1;
My_Device : Device_Register;
for My_Device'Address use To_Address(16#FF00#);
```

If the implementation cannot accept 8-bit stand-alone objects, then this will be illegal. However, on a machine where an 8-bit device register exists, the implementation will probably be able to accept 8-bit stand-alone objects. Therefore, My_Device'Size will be 8, and My_Device'Address will point at those 8 bits, as desired.

If an object of subtype Device_Register is passed to a foreign language subprogram, it will be passed according to that subprogram's conventions. Most foreign language implementations have similar run-time model restrictions. For example, when passing to a C function, where the argument is of the C type char* (that is, pointer to char), the C compiler will generally expect a full word value, either on the stack, or in a register. It will not expect a single byte. Thus, Size clauses for subtypes really have nothing to do with passing parameters to foreign language subprograms.

- For a subtype implemented with levels of indirection, the Size should include the size of the pointers, but not the size of what they point at.

**Ramification:** For example, if a task object is represented as a pointer to some information (including a task stack), then the size of the object should be the size of the pointer. The Storage_Size, on the other hand, should include the size of the stack.

- {AI95-00051-02} An implementation should support a Size clause for a discrete type, fixed point type, record type, or array type, subject to the following:

- {AI95-00051-02} {AI12-0444-1} An implementation is not required to need not support a Size clause for a signed integer type specifying a Size greater than that of the largest signed integer type supported by the implementation in the absence of a size clause (that is, when the size is chosen by default). A corresponding limitation may be imposed for modular integer types, fixed point types, enumeration types, record types, and array types.

**Discussion:** {AI95-00051-02} Note that the “corresponding limitation” for a record or array type implies that an implementation may impose some reasonable maximum size for records and arrays (e.g. 2**32 bits), which is an upper bound (“capacity” limit) on the size, whether chosen by default or by being specified by the user. The largest size supported for records need not be the same as the largest size supported for arrays.
Ramification: AI05-0155-1 Only Size clauses with a size greater than or equal to the Size that would be chosen by default may be safely presumed to be supported on nonstatic elementary subtypes. Implementations may choose to support smaller sizes, but only if the Size allows any value of the subtype to be represented, for any possible value of the bounds.

- A195-00291-02 A nonconfirming size clause for the first subtype of a derived untagged by-reference type is not required to need be supported.

Implementation Advice: The recommended level of support for the Size attribute should be followed.

Ramification: AI95-00291-02 There is no recommendation to support any nonconfirming Size clauses for types not mentioned above. Remember that 13.1 requires support for confirming Size clauses for all types.

NOTE 6 Size is a subtype-specific attribute.

NOTE 7 AI05-0229-1 A component_clause or Component_Size clause can override a specified Size. Aspect pragma Pack cannot.

Inconsistencies With Ada 83

We specify the meaning of Size in much more detail than Ada 83. This is not technically an inconsistency, but it is in practice, as most Ada 83 compilers use a different definition for Size than is required here. This should have been documented more explicitly during the Ada 9X process.

Wording Changes from Ada 83

The requirement for a nonnegative value in a Size clause was not in RM83, but it's hard to see how it would make sense. For uniformity, we forbid negative sizes, rather than letting implementations define their meaning.

Static Semantics

For every subtype S:

S'Object_Size

If S is definite, denotes the size (in bits) of a stand-alone aliased object, or a component of subtype S in the absence of an aspect specification or representation item that specifies the size of the object or component. If S is indefinite, the meaning is implementation-defined. The value of this attribute is of the type universal integer. If not specified otherwise, the Object Size of a subtype is at least as large as the Size of the subtype. Object Size may be specified via an attribute_definition_clause; the expression of such a clause shall be static and its value nonnegative. All aliased objects with nominal subtype S have the size S'Object Size. In the absence of an explicit specification, the Object Size of a subtype S defined by a subtype_indication without a constraint, is that of the value of the Object Size of the subtype denoted by the subtype mark of the subtype_indication, at the point of this definition.

Implementation defined: The meaning of Object Size for indefinite subtypes.

Implementation Advice

If S is a definite first subtype and S'Object_Size is not specified, S'Object_Size should be the smallest multiple of the storage element size larger than or equal to S'Size that is consistent with the alignment of S.

Implementation Advice: If S is a definite first subtype for which Object_Size is not specified, S'Object_Size should be the smallest multiple of the storage element size larger than or equal to S'Size that is consistent with the alignment of S.

Reason: Many implementations “round up” allocations to the nearest multiple of the alignment. For instance, this example appears in the GNAT documentation:

[Given] a record containing an integer and a character:
type Rec is record
  I : Integer;
  C : Character;
end record;

will have a size of 40 (that is Rec'Size will be 40). The alignment will be 4, because of the integer field, and so the default size of record objects for this type will be 64 (8 bytes).

We purposely used the vague phrase “consistent with the alignment of S” so that implementations that do not round up allocations (just using padding to provide alignment) are not required to do any rounding up.

{AI12-0059-1} If X denotes an object (including a component) of subtype S, X'Size should equal S'Object_Size, unless:

- X'Size is specified; or
- X is a nonaliased stand-alone object; or
- The size of X is determined by a component_clause or Component_Size clause; or
- The type containing component X is packed.

Implementation Advice: The Size of most objects of a subtype should equal the Object_Size of the subtype.

{AI12-0059-1} An Object_Size clause on a composite type should not affect the internal layout of components.

Implementation Advice: An Object_Size clause on a composite type should not affect the internal layout of components.

{AI12-0059-1} The recommended level of support for the Object_Size attribute of subtypes is:

- If S is a static signed integer subtype, the implementation should support the specification of S'Object_Size to match the size of any signed integer base subtype provided by the implementation that is no smaller than S'Size. Corresponding support is expected for modular integer subtypes, fixed point subtypes, and enumeration subtypes.
  
  Ramification: The intent is that a compiler need support only those Object Sizes for integer subtypes that it might select for an integer type declaration. Similarly for the other kinds of subtypes listed.

- If S is an array or record subtype with static constraints and S is not a first subtype of a derived untagged by-reference type, the implementation should support the specification of S'Object_Size to be any multiple of the storage element size that is consistent with the alignment of S, that is no smaller than S'Size, and that is no larger than that of the largest composite subtype supported by the implementation.

  Discussion: Any extra bits required this way will be padding bits. Unlike elementary objects, padding bits can be considered part of composite objects.

- If S is some other subtype, only confirming specifications of Object_Size are required to be supported.

  Implementation Advice: The recommended level of support for the Object_Size attribute should be followed.

Static Semantics

For a prefix T that denotes a task object [(after any implicit dereference)]:

T'Storage_Size

{AI05-0229-1} Denotes the number of storage elements reserved for the task. The value of this attribute is of the type universal_integer. The Storage_Size includes the size of the task's stack, if any. The language does not specify whether or not it includes other storage associated with the task (such as the “task control block” used by some implementations.) If the aspect pragma Storage_Size is specified for the type of the object given, the value of the Storage_Size attribute is at least the value determined by the aspect specified in the pragma.

Ramification: The value of this attribute is never negative, since it is impossible to “reserve” a negative number of storage elements.
If the implementation chooses to allocate an initial amount of storage, and then increase this as needed, the Storage_Size cannot include the additional amounts (assuming the allocation of the additional amounts can raise Storage_Error); this is inherent in the meaning of “reserved”.

The implementation is allowed to allocate different amounts of storage for different tasks of the same subtype. Storage_Size is also defined for access subtypes — see 13.11.

{AI95-0229-1} [Aspect A pragma] Storage_Size specifies the amount of storage to be reserved for the execution of a task.

Paragraphs 62 through 65 were moved to Annex J, “Obsolescent Features”.

Syntax

{AI05-0229-1} The form of a pragma Storage_Size is as follows:

\[\text{pragma Storage_Size}(\text{expression});\]

{AI05-0229-1} A pragma Storage_Size is allowed only immediately within a task_definition.

Name Resolution Rules

{AI05-0229-1} The expression of a pragma Storage_Size is expected to be of any integer type.

Static Semantics

{AI05-0229-1} {AI05-0269-1} For a task_type (including the anonymous_type of a single_task_declaration), the following language-defined representation aspect may be specified:

\[\text{Storage_Size}\]

The Storage_Size aspect is an expression, which shall be of any integer type.

To be honest: This definition somewhat conflicts with the “automatic” one for the obsolescent attribute Storage_Size (which can be specified). The only difference is where the given expression is evaluated. We intend for the above definition to supersede that “automatic” definition for this attribute.

Ramification: Note that the value of the Storage_Size aspect is an expression; it is not the value of an expression. The expression is evaluated for each object of the type (see below).

Aspect Description for Storage_Size (task): Size in storage elements reserved for a task type or single task object.

Legality Rules

{AI05-0229-1} The Storage_Size aspect shall not be specified for a task_interface_type.

Dynamic Semantics

When a task object is created, the expression (if any) associated with the Storage_Size aspect of its type A pragma Storage_Size is elaborated when an object of the type defined by the immediately enclosing task_definition is created. For the elaboration of a pragma Storage_Size, the expression is evaluated; the Storage_Size attribute of the newly created task object is at least the value of the expression.

Ramification: The implementation is allowed to round up a specified Storage_Size amount. For example, if the implementation always allocates in chunks of 4096 bytes, the number 200 might be rounded up to 4096. Also, if the user specifies a negative number, the implementation has to normalize this to 0, or perhaps to a positive number.

If the Storage_Size aspect is not specified for the type of the task object, the value of the Storage_Size attribute is unspecified.

At the point of task object creation, or upon task activation, Storage_Error is raised if there is insufficient free storage to accommodate the requested Storage_Size.

Static Semantics

For a prefix X that denotes an array subtype or array object [(after any implicit dereference)]:

13.3 Operational and Representation Attributes
X'Component_Size

Denotes the size in bits of components of the type of X. The value of this attribute is of type universal_integer.

Component_Size may be specified for array types via an attribute_definition_clause; the expression of such a clause shall be static, and its value nonnegative.

Implementation Note: The intent is that the value of X'Component_Size is always nonnegative. If the array is stored “backwards” in memory (which might be caused by an implementation-defined pragma), X'Component_Size is still positive.

Ramification: For an array object A, A'Component_Size = A(I)'Size for any index I.

Aspect Description for Component_Size: Size in bits of a component of an array type.

Implementation Advice

The recommended level of support for the Component_Size attribute is:

- \{AI12-0444-1\} An implementation is not required to support specified Component_Sizes that are less than the Size of the component subtype.
- \{AI05-0229-1\} An implementation should support specified Component_Sizes that are factors and multiples of the word size. For such Component_Sizes, the array should contain no gaps between components. For other Component_Sizes (if supported), the array should contain no gaps between components when Packing is also specified; the implementation should forbid this combination in cases where it cannot support a no-gaps representation.

Ramification: \{AI05-0229-1\} For example, if Storage_Unit = 8, and Word_Size = 32, then the user is allowed to specify a Component_Size of 1, 2, 4, 8, 16, and 32, with no gaps. In addition, \(n\times32\) is allowed for positive integers \(n\), again with no gaps. If the implementation accepts Component_Size = 3, then it might allocate 10 components per word, with a 2-bit gap at the end of each word (unless Packing is also specified), or it might not have any internal gaps at all. (There can be gaps at either end of the array.)

Implementation Advice: The recommended level of support for the Component_Size attribute should be followed.

Static Semantics

\{AI05-0191-1\} For a prefix X that denotes an object:

X'Has_Same_Storage

\{AI05-0191-1\} X'Has_Same_Storage denotes a function with the following specification:

function X'Has_Same_Storage (Arg : any_type) return Boolean

\{AI05-0191-1\} \{AI05-0264-1\} \{AI12-0077-1\} The actual parameter shall be a name that denotes an object. The object denoted by the actual parameter can be of any type. This function evaluates the names of the objects involved, \(V\), and returns True if the representation of the object denoted by the actual parameter occupies exactly the same bits as the representation of the object denoted by \(X\) and the objects occupy at least one bit, otherwise, it returns False.

Discussion: Has_Same_Storage means that, if the representation is contiguous, the objects sit at the same address and occupy the same length of memory.

\{AI05-0191-1\} For a prefix X that denotes an object:

X'Overlaps_Storage

\{AI05-0191-1\} X'Overlaps_Storage denotes a function with the following specification:

function X'Overlaps_Storage (Arg : any_type) return Boolean

\{AI05-0191-1\} \{AI05-0264-1\} \{AI12-0077-1\} The actual parameter shall be a name that denotes an object. The object denoted by the actual parameter can be of any type. This function evaluates the names of the objects involved and returns True if the representation of the object denoted by
the actual parameter shares at least one bit with the representation of the object denoted by \( X \); otherwise, it returns False.

### NOTE 8
\( \{ A105-0191-1 \} \) \( X'\text{Has_Same_Storage}(Y) \) implies \( X'\text{Overlaps_Storage}(Y) \).

### NOTE 9
\( \{ A105-0191-1 \} \) \( X'\text{Has_Same_Storage}(Y) \) and \( X'\text{Overlaps_Storage}(Y) \) are not considered to be reads of \( X \) and \( Y \).

### Static Semantics

\( \{ 8652/0009 \} \) \( \{ A195-00137-01 \} \) \( \{ A105-0183-1 \} \) The following type-related operational attribute is defined: \( \text{External_Tag} \).

For every subtype \( S \) of a tagged type \( T \) (specific or class-wide), the following attribute is defined:

\[ S'\text{External_Tag} \]

This denotes an external string representation for \( S'Tag \); it is of the predefined type \( \text{String} \). \( S'\text{External_Tag} \) may be specified for a specific tagged type via an \( \text{attribute_definition_clause} \); the expression of such a clause shall be static. The default external tag representation is implementation defined. See \( 4.9.2 \) and \( 13.13.2 \). The value of \( \text{External_Tag} \) is never inherited; the default value is always used unless a new value is directly specified for a type.

### Implementation defined:
The default external representation for a type tag.

### Aspect Description for \( \text{External_Tag} \):
Unique identifier for a tagged type in streams.

### Dynamic Semantics

\( \{ A105-0113-1 \} \) If a user-specified external tag \( S'\text{External_Tag} \) is the same as \( T'\text{External_Tag} \) for some other tagged type declared by a different declaration in the partition, Program_Error is raised by the elaboration of the \( \text{attribute_definition_clause} \).

### Ramification:
This rule does not depend on the visibility of the other tagged type, but it does depend on the existence of the other tagged type. The other tagged type could have the default external tag or a user-specified external tag.

This rule allows the same declaration to be elaborated multiple times. In that case, different types could have the same external tag. If that happens, \( \text{Internal_Tag} \) would return some unspecified tag, and \( \text{Descendant_Tag} \) probably would return the intended tag (using the given ancestor to determine which type is intended). However, in some cases (such as multiple instantiations of a derived tagged type declared in a generic body), Tag_Error might be raised by \( \text{Descendant_Tag} \) if multiple types are identified.

Note that while there is a race condition inherent in this definition (which \( \text{attribute_definition_clause} \) raises Program_Error depends on the order of elaboration), it doesn't matter as a program with two such clauses is simply wrong. Two types that both come from the same declaration are allowed, as noted previously.

### Implementation Requirements

In an implementation, the default external tag for each specific tagged type declared in a partition shall be distinct, so long as the type is declared outside an instance of a generic body. If the compilation unit in which a given tagged type is declared, and all compilation units on which it semantically depends, are the same in two different partitions, then the external tag for the type shall be the same in the two partitions. What it means for a compilation unit to be the same in two different partitions is implementation defined. At a minimum, if the compilation unit is not recompiled between building the two different partitions that include it, the compilation unit is considered the same in the two partitions.

### Implementation defined:
What determines whether a compilation unit is the same in two different partitions.

### Reason:
These requirements are important because external tags are used for input/output of class-wide types. These requirements ensure that what is written by one program can be read back by some other program so long as they share the same declaration for the type (and everything it depends on).

The user may specify the external tag if (s)he wishes its value to be stable even across changes to the compilation unit in which the type is declared (or changes in some unit on which it depends).
We use a String rather than a Stream_Element_Array Storage_Array to represent an external tag for portability.

**Ramification:** Note that the characters of an external tag need not all be graphic characters. In other words, the external tag can be a sequence of arbitrary 8-bit bytes.

**Implementation Permissions**

If a user-specified external tag S'External_Tag is the same as T'External_Tag for some other tagged type declared by a different declaration in the partition, the partition may be rejected.

**Ramification:** This is, in general, a post-compilation check. This permission is intended for implementations that do link-time construction of the external tag lookup table; implementations that dynamically construct the table will likely prefer to raise Program_Error upon elaboration of the problem construct. We don't want this check to require any implementation complexity, as it will be very rare that there would be a problem.

**NOTE 10** The following language-defined attributes are specifiable, at least for some of the kinds of entities to which they apply: Address, Size, Component_Size, Alignment, Bit_Order, Component_Size, External_Tag, Input, Machine_Radix, Output, Read, Size, Small, Bit_Order, Storage_Pool, Storage_Size, Stream_Size, and Write, Output, Read, Input, and Machine_Radix.

**NOTE 11** It follows from the general rules in 13.1 that if one writes “for X'Size use Y;” then the X'Size attribute_reference will return Y (assuming the implementation allows the Size clause). The same is true for all of the specifiable attributes except Storage_Size.

**Ramification:** An implementation may specify that an implementation-defined attribute is specifiable for certain entities. This follows from the fact that the semantics of implementation-defined attributes is implementation defined. An implementation is not allowed to make a language-defined attribute specifiable if it isn't.

**Examples of attribute definition clauses:**

```ada
Byte : constant := 8;
Page : constant := 2**12;

type Medium is range 0 .. 65_000;
for Medium'Size use 2*Byte;
for Medium'Alignment use 2;
Device_Register : Medium;
for Device_Register'Size use Medium'Size;
for Device_Register'Address use
System.Storage_Elements.To_Address(16#FFFF_0020#);

type Short is delta 0.01 range -100.0 .. 100.0;
for Short'Size use 15;
for Car_Name'Storage_Size use -- specify access type's storage pool size
2000*(Car'Size/System.Storage_Unit) +1); -- approximately 2000 cars

{AI95-00441-01} function My_Input(My_Read(Stream : not null access Ada.Streams.Root_Stream_Type'Class)) return T;
for T'Input use My_InputMy_Read; -- see 13.13.2
```

**Extensions to Ada 83**

The syntax rule for length_clause is replaced with the new syntax rule for attribute_definition_clause, and it is modified to allow a name (as well as an expression).

**Wording Changes from Ada 83**

The syntax rule for attribute_definition_clause now requires that the prefix of the attribute be a local_name; in Ada 83 this rule was stated in the text.
Ada 83, the relationship between a `aspect_clause` specifying a certain aspect and an attribute that queried that aspect was unclear. In Ada 95, they are the same, except for certain explicit exceptions.

**Wording Changes from Ada 95**

- **Corrigendum:** Added wording to specify for each attribute whether it is an operational or representation attribute.
- **Corrigendum:** Added wording to specify that `External_Tag` is never inherited.
- **Corrigendum:** Adjusted the Recommended Level of Support for Alignment to eliminate nonsense requirements and to ensure that useful capabilities are required.
- **Corrigendum:** Added wording to specify that for each attribute whether it is an operational or representation attribute.
- **Corrigendum:** Added wording to specify that `External_Tag` is never inherited.
- **Corrigendum:** Adjusted the Recommended Level of Support for Size to eliminate nonsense requirements and to ensure that useful capabilities are required. Also eliminated any dependence on whether an aspect was specified (a confirming representation item should not affect the semantics).
- **Corrigendum:** Added the definition of machine scalar.
- **Corrigendum:** Removed the requirement that specified alignments for a composite type cannot override those for their components, because it was never intended to apply to components whose location was specified with a representation item. Moreover, it causes a difference in legality when a confirming alignment is specified for one of the composite types.
- **Corrigendum:** Removed recommended level of support rules about types with by-reference and aliased parts, because there are now blanket rules covering all recommended level of support rules.
- **Corrigendum:** Split the definition of Alignment for subtypes and for objects. This simplified the wording and eliminated confusion about which rules applied to objects, which applied to subtypes, and which applied to both.

**Inconsistencies With Ada 2005**

- **Correction:** An address attribute with a prefix of a generic formal subprogram whose actual parameter has convention Intrinsic now raises Program_Error. Since it is unlikely that such an attribute would have done anything useful (a subprogram with convention Intrinsic is not expected to have a normal subprogram body), it is highly unlikely that any existing programs would notice the difference, and any that do probably are buggy.
- **Correction:** User-specified external tags that conflict with other external tags raise Program_Error (or are optionally illegal). This was legal and did not raise an exception in the past, although the effects were not defined. So while a program might depend on such behavior, the results were not portable (even to different versions of the same implementation). Such programs should be rare.

**Incompatibilities With Ada 2005**

- **Correction:** An address attribute with a prefix of a subprogram with convention Intrinsic is now illegal. Such attributes are very unlikely to have provided a useful answer (the intended meaning of convention Intrinsic is that there is no actual subprogram body for the operation), so this is highly unlikely to affect any existing programs unless they have a hidden bug.

**Extensions to Ada 2005**

- **Attributes Has_Same_Storage and Overlaps_Storage are new.**
- **Aspect Storage_Size is new; `pragma` Storage_Size is now obsolescent, joining attribute Storage_Size for task types.**

**Wording Changes from Ada 2005**

- **Correction:** Improved the description of erroneous execution for address clauses to make it clear that specifying an address inappropriate for the entity will lead to erroneous execution.
- **Correction:** Added Implementation Advice for the alignment of class-wide types.

**Extensions to Ada 2012**

- **Attribute Object_Size is new.**

**Wording Changes from Ada 2012**

- **Corrigendum:** Clarified the behavior of Has_Same_Storage when 'Size = 0.
13.4 Enumeration Representation Clauses

[An enumeration_representation_clause specifies the internal codes for enumeration literals.]

Syntax

\[
\text{enumeration_representation_clause} ::= \\
\text{for first_subtype_local_name use enumeration_aggregate;}
\]

\[
\text{enumeration_aggregate} ::= \text{array_aggregate}
\]

Name Resolution Rules

The enumeration_aggregate shall be written as a one-dimensional array_aggregate, for which the index subtype is the unconstrained subtype of the enumeration type, and each component expression is expected to be of any integer type.

Ramification: The “full coverage rules” for aggregates applies. An others is not allowed — there is no applicable index constraint in this context.

Legality Rules

The first_subtype_local_name of an enumeration_representation_clause shall denote an enumeration subtype.

Ramification: As for all type-related representation items, the local_name is required to denote a first subtype.

\{AI95-00287-01\} Each component of the array_aggregate shall be given by an expression rather than a <>. The expressions given in the array_aggregate shall be static, and shall specify distinct integer codes for each value of the enumeration type; the associated integer codes shall satisfy the predefined ordering relation of the type.

Reason: Each value of the enumeration type has to be given an internal code, even if the first subtype of the enumeration type is constrained to only a subrange (this is only possible if the enumeration type is a derived type). This “full coverage” requirement is important because one may refer to Enum'Base'First and Enum'Base'Last, which need to have defined representations.

Static Semantics

An enumeration_representation_clause specifies the coding aspect of representation. The coding consists of the internal code for each enumeration literal, that is, the integral value used internally to represent each literal.

Aspect Description for Coding: Internal representation of enumeration literals. Specified by an enumeration_representation_clause, not by an aspect_specification.

Implementation Requirements

For nonboolean enumeration types, if the coding is not specified for the type, then for each value of the type, the internal code shall be equal to its position number.

Reason: This default representation is already used by all known Ada compilers for nonboolean enumeration types. Therefore, we make it a requirement so users can depend on it, rather than feeling obliged to supply for every enumeration type an enumeration representation clause that is equivalent to this default rule.

Discussion: For boolean types, it is relatively common to use all ones for True, and all zeros for False, since some hardware supports that directly. Of course, for a one-bit Boolean object (like in a packed array), False is presumably zero and True is presumably one (choosing the reverse would be extremely unfriendly!).

Implementation Advice

The recommended level of support for enumeration_representation_clauses is:
• \{AI12-0444-1\} An implementation should support at least the internal codes in the range System.Min_Int .. System.Max_Int. An implementation \textit{is not required} to support \textit{enumeration_representation_clauses} for boolean types.

\textbf{Ramification:} The implementation may support numbers outside the above range, such as numbers greater than System.Max_Int. See AI83-00564.

\textbf{Reason:} The benefits of specifying the internal coding of a boolean type do not outweigh the implementation costs. Consider, for example, the implementation of the logical operators on a packed array of boolean with strange internal codes. It's implementable, but not worth it.

\textbf{Implementation Advice:} The recommended level of support for \textit{enumeration_representation_clauses} should be followed.

\textbf{Static Semantics}

\textbf{AI12-0237-1} For every discrete subtype S, the following attributes are defined:

\textbf{S'Enum_Rep}

\textit{S'Enum_Rep denotes a function with the following specification:}

\texttt{function S'Enum_Rep (Arg : S'Base) return universal_integer}

This function returns the representation value of the value of Arg, as a value of type \textit{universal_integer}. The \textit{representation value} is the internal code specified in an \textit{enumeration_representation_clause}, if any, for the type corresponding to the value of Arg, and otherwise is the position number of the value.

\textbf{S'Enum_Val}

\textit{S'Enum_Val denotes a function with the following specification:}

\texttt{function S'Enum_Val (Arg : universal_integer) return S'Base}

This function returns a value of the type of S whose representation value equals the value of Arg. For the evaluation of a call on \textit{S'Enum_Val}, if there is no value in the base range of its type with the given representation value, \textit{Constraint Error} is raised.

\textbf{Reason:} We define these on all discrete types so that they can be used inside of a generic unit on a subtype of a generic formal discrete type. They're not useful on integer types (they have the same effect as \textit{S'Pos} and \textit{S'Val}).

\textbf{Note:} \{8652/0009\} \{AI95-00137-01\} \{AI05-0299-1\} \{AI12-0237-1\} \{AI12-0442-1\} Attribute \textit{Enum_RepUnchecked_Conversion} can\textbf{may} be used to query the internal codes used for an enumeration type; \textit{attribute \textit{Enum_Val}} can\textbf{may} be used to convert from an internal code to an enumeration value. The \textit{other} attributes of the type, such as Succ, Pred, and Pos, are unaffected by \textit{ enumeration_representation_clause}. For example, Pos always returns the position number, not the internal integer code that \textit{was} might have been specified in \textit{an enumeration_representation_clause}.

\textbf{Discussion:} Suppose the enumeration type in question is derived:

\texttt{type T1 is (Red, Green, Blue);} \\
\texttt{subtype S1 is T1 range Red .. Green;} \\
\texttt{type S2 is new S1;} \\
\texttt{for S2 use (Red => 10, Green => 20, Blue => 30);} \\
\texttt{for I in S2'Base loop} \\
\texttt{... -- When I equals Blue, the internal code is 30.} \\
\texttt{end loop;}

We considered allowing or requiring \texttt{for S2'Base use ...} in cases like this, but it didn't seem worth the trouble.

\textbf{Examples}

\textbf{AI12-0312-1} \textit{Examples: Example of an enumeration representation {'}{}\textit{clauses}-clause:}

\texttt{type Mix_Code is (ADD, SUB, MUL, LDA, STA, STZ);} \\
\texttt{for Mix_Code use} \\
\texttt{(ADD => 1, SUB => 2, MUL => 3, LDA => 8, STA => 24, STZ =>33)};
13.5 Record Layout

The \(\textit{record} \) layout aspect of representation consists of the \textit{storage places} for some or all components, that is, storage place attributes of the components. The layout can be specified with a \textit{record_representation_clause}.

### 13.5.1 Record Representation Clauses

\[\text{A record_representation_clause} \text{ specifies the storage representation of records and record extensions, that is, the order, position, and size of components (including discriminants, if any).}\]

\textit{Language Design Principles}

\[\text{AI95-00114-01} \] \textit{It should be feasible for an implementation to use negative offsets in the representation of composite types. However, no implementation should be forced to support negative offsets. Therefore, in the interest of uniformity, negative offsets should be disallowed in record_representation_clauses.}

\textit{Syntax}

\[\text{AI12-0213-1} \] \textit{record_representation_clause} ::= 
\quad for \textit{first_subtype_local_name} use 
\quad record [\textit{mod_clause}] 
\quad \{\textit{component_clause}\} 
\quad end record [\textit{local_name}];

\textit{component_clause} ::= 
\quad \textit{component_local_name} \textit{at position range} \textit{first_bit} .. \textit{last_bit};

\textit{position} ::= \textit{static_expression}

\textit{first_bit} ::= \textit{static_simple_expression}
last_bit ::= static_simple_expression

Reason: First_bit and last_bit need to be simple_expression instead of expression for the same reason as in range (see 3.5, “Scalar Types”).

{AI12-0213-1} If a local_name appears at the end of the record_representation_clause, it shall repeat the first_subtype_local_name.

Name Resolution Rules

Each position, first_bit, and last_bit is expected to be of any integer type.

Ramification: These need not have the same integer type.

Legality Rules

{AI95-00436-01} The first_subtype_local_name of a record_representation_clause shall denote a specific nonlimited record or record extension subtype.

Ramification: As for all type-related representation items, the local_name is required to denote a first subtype.

If the component_local_name is a direct_name, the local_name shall denote a component of the type. For a record extension, the component shall not be inherited, and shall not be a discriminant that corresponds to a discriminant of the parent type. If the component_local_name has an attribute_designator, the direct_name of the local_name shall denote either the declaration of the type or a component of the type, and the attribute_designator shall denote an implementation-defined implicit component of the type.

The position, first_bit, and last_bit shall be static expressions. The value of position and first_bit shall be nonnegative. The value of last_bit shall be no less than first_bit – 1.

Ramification: A component_clause such as “X at 4 range 0..–1;” is allowed if X can fit in zero bits.

{AI95-00133-01} If the nondefault bit ordering applies to the type, then either:

- the value of last_bit shall be less than the size of the largest machine scalar; or
- the value of first_bit shall be zero and the value of last_bit + 1 shall be a multiple of System.Storage_Unit.

At most one component_clause is allowed for each component of the type, including for each discriminant (component_clauses may be given for some, all, or none of the components). Storage places within a component_list shall not overlap, unless they are for components in distinct variants of the same variant_part.

A name that denotes a component of a type is not allowed within a record_representation_clause for the type, except as the component_local_name of a component_clause.

Reason: It might seem strange to make the record_representation_clause part of the declarative region, and then disallow mentions of the components within almost all of the record_representation_clause. The alternative would be to treat the component_local_name like a formal parameter name in a subprogram call (in terms of visibility). However, this rule would imply slightly different semantics, because (given the actual rule) the components can hide other declarations. This was the rule in Ada 83, and we see no reason to change it. The following, for example, was and is illegal:

```ada
type T is record
   X : Integer;
end record;
X : constant := 31; -- Same defining name as the component.
for T use
   record
      X at 0 range 0..X; -- Illegal!
   end record;
```

The component X hides the named number X throughout the record_representation_clause.
Static Semantics

\{AI95-00133-01\} A record_representation_clause (without the mod_clause) specifies the layout. The storage place attributes (see 13.5.2) are taken from the values of the position, first_bit, and last_bit expressions after normalizing those values so that first_bit is less than Storage_Unit.

Aspect Description for Layout (record): Layout of record components. Specified by a record_representation_clause, not by an aspect_specification.

Aspect Description for Record layout: See Layout.

\{AI95-00133-01\} If the default bit ordering applies to the type, the position, first_bit, and last_bit of each component_clause directly specify the position and size of the corresponding component.

\{AI95-00133-01\} \{AI05-0264-1\} If the nondefault bit ordering applies to the type, then the layout is determined as follows:

- the component_clauses for which the value of last_bit is greater than or equal to the size of the largest machine scalar directly specify the position and size of the corresponding component;

- for other component_clauses, all of the components having the same value of position are considered to be part of a single machine scalar, located at that position; this machine scalar has a size which is the smallest machine scalar size larger than the largest last_bit for all component_clauses at that position; the first_bit and last_bit of each component_clause are then interpreted as bit offsets in this machine scalar.

This paragraph was deleted

Ramification: \{AI95-00133-01\} For example, if Storage_Unit is 8, then “C at 0 range 24..31;” defines C_Position = 3, C_First_Bit = 0, and C_Last_Bit = 7. This is true of machines with either bit ordering.

A component_clause also determines the value of the Size attribute of the component, since this attribute is related to First_Bit and Last_Bit.

[A record_representation_clause for a record extension does not override the layout of the parent part;] if the layout was specified for the parent type, it is inherited by the record extension.

Implementation Permissions

An implementation may generate implementation-defined components (for example, one containing the offset of another component). An implementation may generate names that denote such implementation-defined components; such names shall be implementation-defined attribute References. An implementation may allow such implementation-defined names to be used in record_representation_clauses. An implementation can restrict such component_clauses in any manner it sees fit.

Implementation defined: Implementation-defined components.

Ramification: Of course, since the semantics of implementation-defined attributes is implementation defined, the implementation need not support these names in all situations. They might be purely for the purpose of component_clauses, for example. The visibility rules for such names are up to the implementation.

We do not allow such component names to be normal identifiers — that would constitute blanket permission to do all kinds of evil things.

Discussion: Such implementation-defined components are known in the vernacular as “dope”. Their main purpose is for storing offsets of components that depend on discriminants.

If a record_representation_clause is given for an untagged derived type, the storage place attributes for all of the components of the derived type may differ from those of the corresponding components of the parent type, even for components whose storage place is not specified explicitly in the record_representation_clause.

Reason: This is clearly necessary, since the whole record may need to be laid out differently.

Implementation Advice

The recommended level of support for record_representation_clauses is:
• \{AI95-00133-01\} An implementation should support machine scalars that correspond to all of the integer, floating point, and address formats supported by the machine.

• An implementation should support storage places that can be extracted with a load, mask, shift sequence of machine code, and set with a load, shift, mask, store sequence, given the available machine instructions and run-time model.

• A storage place should be supported if its size is equal to the Size of the component subtype, and it starts and ends on a boundary that obeys the Alignment of the component subtype.

• \{AI95-00133-01\} For if the default bit ordering applies to the declaration of a given type, then for a component with a subtype whose subtype's Size is less than the word size, any storage place that does not cross an aligned word boundary should be supported.

  **Reason:** The above recommendations are sufficient to define interfaces to most interesting hardware. This causes less implementation burden than the definition in ACID, which requires arbitrary bit alignments of arbitrarily large components. Since the ACID definition is neither enforced by the ACVC, nor supported by all implementations, it seems OK for us to weaken it.

• An implementation may reserve a storage place for the tag field of a tagged type, and disallow other components from overlapping that place.

  **Ramification:** Similar permission for other dope is not granted.

• \{AI12-0444-1\} An implementation is not required to support a component_clause for a component of an extension part if the storage place is not after the storage places of all components of the parent type, whether or not those storage places had been specified.

  **Reason:** These restrictions are probably necessary if block equality operations are to be feasible for class-wide types. For block comparison to work, the implementation typically has to fill in any gaps with zero (or one) bits. If a "gap" in the parent type is filled in with a component in a type extension, then this won't work when a class-wide object is passed by reference, as is required.

  **Implementation Advice:** The recommended level of support for record_representation_clause should be followed.

NOTE If no component_clause is given for a component, then the choice of the storage place for the component is left to the implementation. If component_clauses are given for all components, the record_representation_clause completely specifies the representation of the type and will be obeyed exactly by the implementation.

• Ramification: The visibility rules prevent the name of a component of the type from appearing in a record_representation_clause at any place except for the component_local_name of a component_clause. However, since the record_representation_clause is part of the declarative region of the type declaration, the component names hide outer homographs throughout.

• \{8652/0009\} \{AI95-00137-01\} A record_representation_clause cannot be given for a protected type, even though protected types, like record types, have components. The primary reason for this rule is that there is likely to be too much dope in a protected type — entry queues, bit maps for barrier values, etc. In order to control the representation of the user-defined components, simply declare a record type, give it a record_representation_clause, and give the protected type one component whose type is the record type. Alternatively, if the protected object is protecting something like a device register, it makes more sense to keep the thing being protected outside the protected object (possibly with a pointer to it in the protected object), in order to keep implementation-defined components out of the way.

**Examples**

Example of specifying the layout of a record type:

```
Word : constant := 4;  -- storage element is byte, 4 bytes per word

type State is (A,M,W,P);
type Mode is (Fix, Dec, Exp, Signif);

{AI12-0178-1} type Byte_Mask is array (0..7) of Boolean with Component_Size => 1;
type State_Mask is array (State) of Boolean with Component_Size => 1;
type Mode_Mask is array (Mode) of Boolean with Component_Size => 1;
```
type Program_Status_Word is
record
  System_Mask      : Byte_Mask;
  Protection_Key   : Integer range 0 .. 3;
  Machine_State    : State_Mask;
  Interrupt_Cause  : Interruption_Code;
  I1c              : Integer range 0 .. 3;
  Cc               : Integer range 0 .. 3;
  Program_Mask     : Mode_Mask;
  Inst_Address     : Address;
end record;

for Program_Status_Word use
record
  System_Mask      at 0*Word range 0 .. 7;
  Protection_Key   at 0*Word range 10 .. 11; -- bits 8,9 unused
  Machine_State    at 0*Word range 12 .. 15;
  Interrupt_Cause  at 0*Word range 16 .. 31;
  I1c              at 1*Word range 0 .. 1; -- second word
  Cc               at 1*Word range 2 .. 3;
  Program_Mask     at 1*Word range 4 .. 7;
  Inst_Address     at 1*Word range 8 .. 31;
end record;

for Program_Status_Word'Size use 8*System.Storage_Unit;
for Program_Status_Word'Alignment use 8;

{AI12-0452-1} The record_representation_clause defines the record layout. The Size clause guarantees that (at least) eight storage elements are used for objects of the type. The Alignment clause guarantees that aliased, imported, or exported objects of the type will have addresses divisible by eight.

NOTE 2 {AI12-0452-1} Note on the example: The record_representation_clause defines the record layout. The Size clause guarantees that (at least) eight storage elements are used for objects of the type. The Alignment clause guarantees that aliased, imported, or exported objects of the type will have addresses divisible by eight.

Wording Changes from Ada 83
The alignment_clause has been renamed to mod_clause and moved to Annex J, “Obsolescent Features”.
We have clarified that implementation-defined component names have to be in the form of an attribute_reference of a component or of the first subtype itself; surely Ada 83 did not intend to allow arbitrary identifiers.
The RM83-13.4(7) wording incorrectly allows components in nonvariant records to overlap. We have corrected that oversight.

Incompatibilities With Ada 95
{AI95-00133-01} Amendment Correction: The meaning of a record_representation_clause for the nondefault bit order is now clearly defined. Thus, such clauses can be portably written. In order to do that though, the equivalence of bit 1 in word 1 to bit 9 in word 0 (for a machine with Storage_Unit = 8) had to be dropped for the nondefault bit order. Any record_representation_clauses which depends on that equivalence will break (although such code would imply a noncontiguous representation for a component, and it seems unlikely that compilers were supporting that anyway).

Extensions to Ada 95
{AI95-00436-01} Amendment Correction: The undocumented (and likely unintentional) incompatibility with Ada 83 caused by not allowing record_representation_clauses on limited record types is removed.

Extensions to Ada 2012
{AI12-0213-1} The local_name following end record is new.

13.5.2 Storage Place Attributes

Static Semantics
For a component C of a composite, non-array object R, the storage place attributes are defined:
Ramification: The storage place attributes are not (individually) specifiable, but the user may control their values by giving a record_representation_clause.

\[\text{R.C'Position} \{/\text{AI95-00133-01}\}\]

If the nondefault bit ordering applies to the composite type, and if a component_clause specifies the placement of C, denotes the value given for the position of the component_clause; otherwise, denotesDenotes the same value as R.C'Address – R'Address. The value of this attribute is of the type universal_integer.

Ramification: {AI95-00133-01} Thus, for the default bit order, R.C'Position is the offset of C in storage elements from the beginning of the object, where the first storage element of an object is numbered zero. R'Address + R.C'Position = R.C'Address. For record extensions, the offset is not measured from the beginning of the extension part, but from the beginning of the whole object, as usual.

In “R.C'Address – R'Address”, the "−" operator is the one in System.Storage_Elements that takes two Addresses and returns a Storage_Offset.

\[\text{R.C'First_Bit} \{/\text{AI95-00133-01}\}\]

If the nondefault bit ordering applies to the composite type, and if a component_clause specifies the placement of C, denotes the value given for the first_bit of the component_clause; otherwise, denotesDenotes the offset, from the start of the first of the storage elements occupied by C, of the first bit occupied by C. This offset is measured in bits. The first bit of a storage element is numbered zero. The value of this attribute is of the type universal_integer.

\[\text{R.C'Last_Bit} \{/\text{AI95-00133-01}\}\]

If the nondefault bit ordering applies to the composite type, and if a component_clause specifies the placement of C, denotes the value given for the last_bit of the component_clause; otherwise, denotesDenotes the offset, from the start of the first of the storage elements occupied by C, of the last bit occupied by C. This offset is measured in bits. The value of this attribute is of the type universal_integer.

Ramification: {AI95-00114-01} The ordering of bits in a storage element is is-defined in 13.5.3, “Bit Ordering”.

R.C'Size = R.C'Last_Bit – R.C'First_Bit + 1. (Unless the implementation chooses an indirection representation.)

If a component_clause applies to a component, then that component will be at the same relative storage place in all objects of the type. Otherwise, there is no such requirement.

Implementation Advice

If a component is represented using some form of pointer (such as an offset) to the actual data of the component, and this data is contiguous with the rest of the object, then the storage place attributes should reflect the place of the actual data, not the pointer. If a component is allocated discontinuously from the rest of the object, then a warning should be generated upon reference to one of its storage place attributes.

Reason: For discontinuous components, these attributes make no sense. For example, an implementation might allocate dynamic-sized components on the heap. For another example, an implementation might allocate the discriminants separately from the other components, so that multiple objects of the same subtype can share discriminants. Such representations cannot happen if there is a component_clause for that component.

Implementation Advice: If a component is represented using a pointer to the actual data of the component which is contiguous with the rest of the object, then the storage place attributes should reflect the place of the actual data. If a component is allocated discontinuously from the rest of the object, then a warning should be generated upon reference to one of its storage place attributes.

Incompatibilities With Ada 95

\[\text{AI95-00133-01}\] Amendment Correction: The meaning of the storage place attributes for the nondefault bit order is now clearly defined, and can be different than that given by strictly following the Ada 95 wording. Any code which depends on the original Ada 95 values for a type using the nondefault bit order where they are different will break.
13.5.3 Bit Ordering

[The Bit_Order attribute specifies the interpretation of the storage place attributes.]

**Reason:** The intention is to provide uniformity in the interpretation of storage places across implementations on a particular machine by allowing the user to specify the Bit_Order. It is not intended to fully support data interoperability across different machines, although it can be used for that purpose in some situations.

\[\text{AI95-00114-01} \] We can't require all implementations on a given machine to use the same bit ordering by default; if the user cares, a `pragma Bit_Order attribute_definition_clause` can be used to force all implementations to use the same bit ordering.

**Static Semantics**

A bit ordering is a method of interpreting the meaning of the storage place attributes. High_Order_First [(known in the vernacular as “big endian”) means that the first bit of a storage element (bit 0) is the most significant bit (interpreting the sequence of bits that represent a component as an unsigned integer value). Low_Order_First [(known in the vernacular as “little endian”) means the opposite: the first bit is the least significant.

\[\text{AI12-0373-1} \] For every specific record subtype S, the following `representation` attribute is defined:

\[
S \text{'Bit_Order}
\]

Denotes the bit ordering for the type of S. The value of this attribute is of type `System.Bit_Order`. Bit_Order may be specified for specific record types via an `attribute_definition_clause`; the expression of such a clause shall be static.

**Aspect Description for Bit_Order:** Order of bit numbering in a `record_representation_clause`.

If Word_Size = Storage_Unit, the default bit ordering is implementation defined. If Word_Size > Storage_Unit, the default bit ordering is the same as the ordering of storage elements in a word, when interpreted as an integer.

**Implementation defined:** If Word_Size = Storage_Unit, the default bit ordering.

**Ramification:** Consider machines whose Word_Size = 32, and whose Storage_Unit = 8. Assume the default bit ordering applies. On a machine with big-endian addresses, the most significant storage element of an integer is at the address of the integer. Therefore, bit zero of a storage element is the most significant bit. On a machine with little-endian addresses, the least significant storage element of an integer is at the address of the integer. Therefore, bit zero of a storage element is the least significant bit.

The storage place attributes of a component of a type are interpreted according to the bit ordering of the type.

**Ramification:** This implies that the interpretation of the position, first_bit, and last_bit of a component_clause of a `record_representation_clause` obey the bit ordering given in a representation item.

**Implementation Advice**

The recommended level of support for the nondefault bit ordering is:

- \[\text{AI95-00133-01} \] The `Word_Size = Storage_Unit`, then the implementation should support the nondefault bit ordering in addition to the default bit ordering.

**Ramification:** \[\text{AI95-00133-01} \] The `Word_Size = Storage_Unit`, the implementation should support both bit orderings. We don't push for support of the nondefault bit ordering when Word_Size > Storage_Unit, except for upward compatibility with a preexisting implementation whose Ada 83 bit order did not correspond to the required Ada 95 default bit order, because implementations are required to support storage positions that cross storage element boundaries when Word_Size > Storage_Unit but the definition of the storage place attributes for the nondefault bit order ensures that such storage positions will not be split into two or three pieces. Thus, there is no significant implementation burden to supporting the nondefault bit order, given that the set of machine scalars is implementation-defined if the nondefault bit ordering is used, which could be onerous to support. However, if `Word_Size = Storage_Unit`, there might not be a natural bit ordering, but the splitting problem need not occur.

**Implementation Advice:** The recommended level of support for the nondefault bit ordering should be followed.
13.5.3 Bit Ordering

NOTE {AI95-00133-01} Bit Order clauses make it possible to write record_representation_clause that can be ported between machines having different bit ordering. They do not guarantee transparent exchange of data between such machines.

Extensions to Ada 83

The Bit_Order attribute is new to Ada 95.

Wording Changes from Ada 95

{AI95-00133-01} We now suggest that all implementations support the nondefault bit order.

13.6 Change of Representation

{AI05-0229-1} {AI12-0445-1} A type_conversion (see 4.6) can be used to convert between two different representations of the same array or record. To convert an array from one representation to another, two array types need to be declared with matching component subtypes, and convertible index types are required. If one type has Packing specified and the other does not, then explicit conversion can be used to pack or unpack an array.

{AI12-0425-1} To convert an untagged record from one representation to another, two record types with a common ancestor type are required to be declared, with no inherited subprograms. Distinct representations can then be specified for the record types, and explicit conversion between the types can be used to effect a change in representation.

Ramification: {AI12-0425-1} The language does not allow implicit copying of by-reference types, so it also does not allow different representations of related by-reference types. Similarly, language rules prevent related tagged types from having different representations of the parent part. Therefore, this technique cannot be used does not work if the first type is an untagged type with user-defined primitive subprograms. It does not work at all for tagged or by-reference types.

Examples

Example of change of representation:

```ada
-- Packed_Descriptor and Descriptor are two different types
-- with identical characteristics, apart from their
-- representation

type Descriptor is
  record
    -- components of a descriptor
  end record;

type Packed_Descriptor is new Descriptor;

for Packed_Descriptor use
  record
    -- component clauses for some or for all components
  end record;

-- Change of representation can now be accomplished by explicit type conversions:

D : Descriptor;
P : Packed_Descriptor;
P := Packed_Descriptor(D);  -- pack D
D := Descriptor(P);         -- unpack P
```

13.7 The Package System

[For each implementation there is a library package called System which includes the definitions of certain configuration-dependent characteristics.]
The following language-defined library package exists:

Implementation defined: The contents of the visible part of package System and its language-defined children.

{AI95-00362-01} {AI12-0414-1} package System is
withpragma Pure Preelaborate is(System);


type Name is implementation-defined enumeration-type;
System_Name : constant Name := implementation-defined;

-- System-Dependent Named Numbers:
Min_Int : constant := root_integer'First;
Max_Int : constant := root_integer'Last;
Max_Binary_Modulus : constant := implementation-defined;
Max_Nonbinary_Modulus : constant := implementation-defined;
Max_Base_Digits : constant := root_real'Digits;
Max_Digits : constant := implementation-defined;
Max_Mantissa : constant := implementation-defined;
Fine_Delta : constant := implementation-defined;
Tick : constant := implementation-defined;

-- Storage-related Declarations:
type Address is implementation-defined;
Null_Address : constant Address;
Storage_Unit : constant := implementation-defined;
Word_Size : constant := implementation-defined * Storage_Unit;
Memory_Size : constant := implementation-defined;

{AI05-0229-1} -- Address Comparison:
function "<" (Left, Right : Address) return Boolean
with Convention => Intrinsic;

function "<=" (Left, Right : Address) return Boolean
with Convention => Intrinsic;

function ">" (Left, Right : Address) return Boolean
with Convention => Intrinsic;

function ">=" (Left, Right : Address) return Boolean
with Convention => Intrinsic;

function ">=" (Left, Right : Address) return Boolean
with Convention => Intrinsic;

function "/=" (Left, Right : Address) return Boolean;
-- "/=" is implicitly defined

withpragma Convention(Intrinsic, "/=");
and so on for all language-defined subprograms in this package

{AI95-00221-01} -- Other System-Dependent Declarations:
type Bit_Order is (High_Order_First, Low_Order_First);
Default_Bit_Order : constant Bit_Order := implementation-defined;

-- Priority-related declarations (see D.1):
subtype Any_Priority is Integer range implementation-defined;
subtype Priority is Any_Priority range Any_Priority'First .. Any_Priority'Last;
subtype Interrupt_Priority is Any_Priority range Priority'Last+1 .. Any_Priority'Last;

Default_Priority : constant Priority := (Priority'First + Priority'Last)/2;

private
... -- not specified by the language
end System;

Name is an enumeration subtype. Values of type Name are the names of alternative machine configurations handled by the implementation. System_Name represents the current machine configuration.
The named numbers Fine_Delta and Tick are of the type \textit{universal_real}; the others are of the type \textit{universal_integer}.

The meanings of the named numbers are:

- \texttt{Min_Int} The smallest (most negative) value allowed for the expressions of a \textit{signed_integer_type}-definition.
- \texttt{Max_Int} The largest (most positive) value allowed for the expressions of a \textit{signed_integer_type}-definition.
- \texttt{Max_Binary_Modulus} A power of two such that it, and all lesser positive powers of two, are allowed as the modulus of a \textit{modular_type_definition}.
- \texttt{Max_Nonbinary_Modulus} A value such that it, and all lesser positive integers, are allowed as the modulus of a \textit{modular_type_definition}.

\textbf{Ramification:} There is no requirement that \texttt{Max_Nonbinary_Modulus} be less than or equal to \texttt{Max_Binary_Modulus}, although that's what makes most sense. On a typical 32-bit machine, for example, \texttt{Max_Binary_Modulus} will be $2^{32}$ and \texttt{Max_Nonbinary_Modulus} will be $2^{31}$, because supporting nonbinary moduli in above $2^{31}$ causes implementation difficulties.

- \texttt{Max_Base_Digits} The largest value allowed for the requested decimal precision in a \textit{floating_point_definition}.
- \texttt{Max_Digits} The largest value allowed for the requested decimal precision in a \textit{floating_point_definition} that has no \textit{real_range_specification}. \texttt{Max_Digits} is less than or equal to \texttt{Max_Base_Digits}.

- \texttt{Max_Mantissa} The largest possible number of binary digits in the mantissa of machine numbers of a user-defined ordinary fixed point type. (The mantissa is defined in Annex G.)

- \texttt{Fine_Delta} The smallest delta allowed in an \textit{ordinary_fixed_point_definition} that has the \textit{real_range_specification \texttt{range} \texttt{–1.0 .. 1.0}.}

- \texttt{Tick} A period in seconds approximating the real time interval during which the value of Calendar.Clock remains constant.

\textbf{Ramification:} There is no required relationship between System.Tick and Duration'Small, other than the one described here.

- The inaccuracy of the \texttt{delay_statement} has no relation to Tick. In particular, it is possible that the clock used for the \texttt{delay_statement} is less accurate than Calendar.Clock.

- We considered making Tick a run-time-determined quantity, to allow for easier configurability. However, this would not be upward compatible, and the desired configurability can be achieved using functionality defined in Annex D, “Real-Time Systems”.

- \texttt{Storage_Unit} The number of bits per storage element.

- \texttt{Word_Size} The number of bits per word.

- \texttt{Memory_Size} An implementation-defined value [that is intended to reflect the memory size of the configuration in storage elements.]

\textbf{Discussion:} It is unspecified whether this refers to the size of the address space, the amount of physical memory on the machine, or perhaps some other interpretation of “memory size”. In any case, the value has to be given by a static expression, even though the amount of memory on many modern machines is a dynamic quantity in several ways. Thus, \texttt{Memory_Size} is not very useful.
Address is of a definite, nonlimited type with preelaborable initialization (see 10.2.1). Address represents machine addresses capable of addressing individual storage elements. Null_Address is an address that is distinct from the address of any object or program unit.

**Ramification:** The implementation has to ensure that there is at least one address that nothing will be allocated to; Null_Address will be one such address.

**Ramification:** Address is the type of the result of the attribute Address.

**Reason:** Address is required to be nonlimited and definite because it is important to be able to assign addresses, and to declare uninitialized address variables.

**Ramification:** If System_Address is defined as a private type (as suggested below), it might be necessary to add the pragma Preelaborable_Initialization aspect to the declarationspecification of Address in order that it have preelaborable initialization as required.

Default_Bit_Order shall be a static constant. See 13.5.3 for an explanation of Bit_Order and Default_Bit_Order.

### Implementation Permissions

An implementation may add additional implementation-defined declarations to package System and its children. Package System may be declared pure.

**Ramification:** The declarations in package System and its children can be implicit. For example, since Address is not limited, the predefined "=" and "/=" operations are probably sufficient. However, the implementation is not required to use the predefined "/=".

### Implementation Advice

Address should be of a private type.

**Reason:** This promotes uniformity by avoiding having implementation-defined predefined operations for the type. We don't require it, because implementations may want to stick with what they have.

**Implementation Advice:** Type System.Address should be a private type.

**Implementation Note:** It is not necessary for Address to be able to point at individual bits within a storage element. Nor is it necessary for it to be able to point at machine registers. It is intended as a memory address that matches the hardware's notion of an address.

The representation of the null value of a general access type should be the same as that of Null_Address; instantiations of Unchecked_Conversion should work accordingly. If the implementation supports interfaces to other languages, the representation of the null value of a general access type should be the same as in those other languages, if appropriate.

Note that the children of the Interfaces package will generally provide foreign-language-specific null values where appropriate. See UI-0065 regarding Null_Address.

NOTE There are also some language-defined child packages of System defined elsewhere.

### Extensions to Ada 83

The declarations Max_Binary_Modulus, Max_Nonbinary_Modulus, Max_Base_Digits, Null_Address, Word_Size, Bit_Order, Default.Bit_Order, Any_Priority, Interrupt_Priority, and Default_Priority are added to System in Ada 95. The presence of ordering operators for type Address is also guaranteed (the existence of these depends on the definition of Address in an Ada 83 implementation). We do not list these as incompatibilities, as the contents of System can vary between implementations anyway; thus a program that depends on the contents of System (by using use System; for example) is already at risk of being incompatible when moved between Ada implementations.

### Wording Changes from Ada 83

Much of the content of System is standardized, to provide more uniformity across implementations. Implementations can still add their own declarations to System, but are encouraged to do so via children of System.

Some of the named numbers are defined more explicitly in terms of the standard numeric types.

The pragmas System_Name, Storage_Unit, and Memory_Size are no longer defined by the language. However, the corresponding declarations in package System still exist. Existing implementations may continue to support the three pragmas as implementation-defined pragmas, if they so desire.
Priority semantics, including subtype Priority, have been moved to the Real Time Annex.

### Extensions to Ada 95

- **AI05-00161-01** **Amendment Correction:** Type Address is defined to have preelaborable initialization, so that it can be used without restriction in preelaborated units. (If Address is defined to be a private type, as suggested by the Implementation Advice, in Ada 95 it cannot be used in some contexts in a preelaborated units. This is an unnecessary portability issue.)

- **AI05-00221-01** **Amendment Correction:** Default_Bit_Order is now a static constant.

- **AI05-00362-01** **Amendment Correction:** Package System is now Pure, so it can be portably used in more places. (Ada 95 allowed it to be Pure, but did not require that.)

### 13.7.1 The Package System.Storage_Elements

#### Static Semantics

The following language-defined library package exists:

```ada
with Pure; pragma Pure(System.Storage_Elements);
package System.Storage_Elements is
  type Storage_Offset is range implementation-defined;
  subtype Storage_Count is Storage_Offset range 0..Storage_Offset'Last;
  type Storage_Element is mod implementation-defined;
  for Storage_Element'Size use Storage_Unit;
  type Storage_Array is array (Storage_Offset range <>) of aliased Storage_Element;
  for Storage_Array'Component_Size use Storage_Unit;

  -- Address Arithmetic:

  {AI05-0229-1} function ""(Left : Address; Right : Storage_Offset)
      return Address
    with Convention => Intrinsic;
  function ""(Left : Storage_Offset; Right : Address)
      return Address
    with Convention => Intrinsic;
  function "-"(Left : Address; Right : Storage_Offset)
      return Address
    with Convention => Intrinsic;
  function "-"(Left, Right : Address)
      return Storage_Offset
    with Convention => Intrinsic;

  {AI05-0229-1} function "mod"(Left : Address; Right : Storage_Offset)
      return Storage_Offset
    with Convention => Intrinsic;

  -- Conversion to/from integers:

  {AI05-0229-1} type Integer_Address is implementation-defined;
  function To_Address(Value : Integer_Address) return Address
    with Convention => Intrinsic;
  function To_Integer(Value : Address) return Integer_Address
    with Convention => Intrinsic;

  {AI05-0229-1} pragma Convention(Intrinsic, ""),
    and so on for all language-defined subprograms declared in this package.
end System.Storage_Elements;
```

**Reason:** {AI05-0229-1} The Convention `pragma Convention` imply that the attribute Access is not allowed for those operations.

The `mod` function is needed so that the definition of Alignment makes sense.

**Implementation defined:** The range of `System.Storage_Offset`, the modulus of `System.Storage_Element`, and the declaration of `System.Storage_Elements.Integer_Address`.

---

13.7 The Package System
Storage_Element represents a storage element. Storage_Offset represents an offset in storage elements. Storage_Count represents a number of storage elements. Storage_Array represents a contiguous sequence of storage elements.

Reason: The index subtype of Storage_Array is Storage_Offset because we wish to allow maximum flexibility. Most Storage_Arrays will probably have a lower bound of 0 or 1, but other lower bounds, including negative ones, make sense in some situations.

This paragraph was deleted. Note that there are some language defined subprograms that fill part of a Storage_Array, and return the index of the last element filled as a Storage_Offset. The Read procedures in Streams (see 13.13.1), Streams.Stream_IO (see A.12.1), and System.RPC (see E.5) behave in this manner. These will raise Constraint_Error if the resulting Last value is not in Storage_Offset. This implies that the Storage_Array passed to these subprograms should not have a lower bound of Storage_Offset'First, because then a read of 0 elements would always raise Constraint_Error. A better choice of lower bound is 1.

Integer_Address is a [(signed or modular)] integer subtype. To_Address and To_Integer convert back and forth between this type and Address.

Implementation Requirements

Storage_Offset'Last shall be greater than or equal to Integer'Last or the largest possible storage offset, whichever is smaller. Storage_Offset'First shall be <= (–Storage_Offset'Last).

Implementation Permissions

{AI95-00362-01} Package System.Storage_Elements may be declared pure.

Paragraph 15 was deleted.

Implementation Advice

Operations in System and its children should reflect the target environment semantics as closely as is reasonable. For example, on most machines, it makes sense for address arithmetic to “wrap around”. Operations that do not make sense should raise Program_Error.

Implementation Advice: Operations in System and its children should reflect the target environment; operations that do not make sense should raise Program_Error.

Discussion: For example, on a segmented architecture, X < Y might raise Program_Error if X and Y do not point at the same segment (assuming segments are unordered). Similarly, on a segmented architecture, the conversions between Integer_Address and Address might not make sense for some values, and so might raise Program_Error.

Reason: We considered making Storage_Element a private type. However, it is better to declare it as a modular type in the visible part, since code that uses it is already low level, and might as well have access to the underlying representation. We also considered allowing Storage_Element to be any integer type, signed integer or modular, but it is better to have uniformity across implementations in this regard, and viewing storage elements as unsigned seemed to make the most sense.

Implementation Note: To_Address is intended for use in Address clauses. Implementations should overload To_Address if appropriate. For example, on a segmented architecture, it might make sense to have a record type representing a segment/offset pair, and have a To_Address conversion that converts from that record type to type Address.

Extensions to Ada 95

{AI95-00362-01} Package System.Storage_Elements is now Pure, so it can be portably used in more places. (Ada 95 allowed it to be Pure, but did not require that.)

13.7.2 The Package System.Address_To_Access_Conversions

Static Semantics

The following language-defined generic library package exists:
generic
  type Object(<>) is limited private;
package System.Address_To_Access_Conversions is
  withpragma Preelaborate, Nonblocking, Global => in out synchronized
  is (Address => System.Address_To_Access_Conversions);
end System.Address_To_Access_Conversions;

The To_Pointer and To_Address subprograms convert back and forth between values of types Object_Pointer and Address. To_Pointer(X'Address) is equal to X'Unchecked_Access for any X that allows Unchecked_Access. To_Pointer(Null_Address) returns null. For other addresses, the behavior is unspecified. To_Address(null) returns Null_Address (for null of the appropriate type). To_Address(Y), where Y /= null, returns Y.all'Address.

Discussion: The programmer should ensure that the address passed to To_Pointer is either Null_Address, or the address of an object of type Object. (If Object is not a not-by-reference type, the object ought to be aliased; recall that the Address attribute is not required to provide a useful result for other objects.) Otherwise, the behavior of the program is unspecified; it might raise an exception or crash, for example.

Reason: Unspecified is almost the same thing as erroneous; they both allow arbitrarily bad behavior. We don't say erroneous here, because the implementation might allow the address passed to To_Pointer to point at some memory that just happens to “look like” an object of type Object. That's not necessarily an error; it's just not portable. However, if the actual type passed to Object is (for example) an array type, the programmer would need to be aware of any dote that the implementation expects to exist, when passing an address that did not come from the Address attribute of an object of type Object.

One might wonder why To_Pointer and To_Address are any better than unchecked conversions. The answer is that Address does not necessarily have the same representation as an access type. For example, an access value might point at the bounds of an array when an address would point at the first element. Or an access value might be an offset in words from someplace, whereas an address might be an offset in bytes from the beginning of memory.

Implementation Permissions

An implementation may place restrictions on instantiations of Address_To_Access_Conversions.

Ramification: For example, if the hardware requires aligned loads and stores, then dereferencing an access value that is not properly aligned might raise an exception.

For another example, if the implementation has chosen to use negative component offsets (from an access value), it might not be possible to preserve the semantics, since negative offsets from the Address are not allowed. (The Address attribute always points at “the first of the storage elements...”.) Note that while the implementation knows how to convert an access value into an address, it might not be able to do the reverse. To avoid generic contract model violations, the restriction might have to be detected at run time in some cases.

13.8 Machine Code Insertions

[ A machine code insertion can be achieved by a call to a subprogram whose sequence_of_statements contains code_statements. ]

Syntax

code_statement ::= qualified_expression;

A code_statement is only allowed in the handled_sequence_of_statements of a subprogram_body. If a subprogram_body contains any code_statements, then within this subprogram_body the only allowed form of statement is a code_statement (labeled or not), the only allowed declarative_
items are use_clauses, and no exception_handler is allowed (comments and pragmas are allowed as usual).

Name Resolution Rules

The qualified_expression is expected to be of any type.

Legality Rules


Ramification: This includes types declared in children of System.Machine_Code.

A code_statement shall appear only within the scope of a with_clause that mentions package System.Machine_Code.

Ramification: Note that this is not a note; without this rule, it would be possible to write machine code in compilation units which depend on System.Machine_Code only indirectly.

Static Semantics

The contents of the library package System.Machine_Code (if provided) are implementation defined. The meaning of code_statements is implementation defined. [Typically, each qualified_expression represents a machine instruction or assembly directive.]

Discussion: For example, an instruction might be a record with an Op_Code component and other components for the operands.


Implementation Permissions

An implementation may place restrictions on code_statements. An implementation is not required to provide package System.Machine_Code.

NOTE 1 {AI12-0440-1} An implementation can provide implementation-defined pragmas specifying register conventions and calling conventions.

NOTE 2 {AI95-00318-02} Machine code functions are exempt from the rule that a return_statement is required. In fact, return_statements are forbidden, since only code_statements are allowed.

Discussion: The idea is that the author of a machine code subprogram knows the calling conventions, and refers to parameters and results accordingly. The implementation should document where to put the result of a machine code function, for example, “Scalar results are returned in register 0”.

NOTE 3 Intrinsic subprograms (see 6.3.1, “Conformance Rules”) can also be used to achieve machine code insertions. Interface to assembly language can be achieved using the features in Annex B, “Interface to Other Languages”.

Examples

Example of a code statement:

{AI05-0229-1} M : Mask;

 procedure Set_Mask
  -- with Inline; pragma Inline(Set_Mask);  
  procedure Set_Mask is
   begin
    SI_Format'(Code => SSM, B => M'Base_Reg, D => M'Disp);
    -- Base_Reg and Disp are implementation-defined attributes
   end Set_Mask;

Extensions to Ada 83

Machine code functions are allowed in Ada 95; in Ada 83, only procedures were allowed.
Wording Changes from Ada 83

14.9 Unchecked Type Conversions

[An unchecked type conversion can be achieved by a call to an instance of the generic function Unchecked_Conversion.]

Static Semantics

The syntax for code_statement is changed to say “qualified_expression” instead of “subtype_mark'record_aggregate”. Requiring the type of each instruction to be a record type is overspecification.

Dynamic Semantics

The following language-defined generic library function exists:

```ada
{AI05-0229-1} {AI12-0241-1} generic
  type Source<> is limited private;
type Target<> is limited private;
  function Ada.Unchecked_Conversion(S : Source) return Target
  with Pure, Nonblocking, Convention => Intrinsic;
  pragma Convention(Intrinsic, Ada.Unchecked_Conversion);
  pragma Pure(Ada.Unchecked_Conversion);

Reason: {AI05-0229-1} The aspect pragma Convention implies that the attribute Access is not allowed for instances of Unchecked_Conversion.
```

Implementation defined: The result of unchecked conversion for instances with scalar result types whose result is not defined by the language.

Implementation defined: The effect of unchecked conversion for instances with nonscalar result types whose effect is not defined by the language.

Reason: {AI95-00426-01} Note the difference between these sentences; the first only says that the bits returned are implementation defined, while the latter allows any effect. The difference is because scalar objects should never be abnormal unless their assignment was disrupted or if they are a subcomponent of an abnormal composite object. Neither exception applies to instances of Unchecked_Conversion.

Ramification: {AI95-00426-01} Whenever unchecked conversions are used, it is the programmer's responsibility to ensure that these conversions maintain the properties that are guaranteed by the language for objects of the target type. For nonscalar types, this requires the user to understand the underlying run-time model of the implementation. The execution of a program that violates these properties by means of unchecked conversions is implementation defined.

Ramification: {AI95-00426-01} Otherwise, if the result type is scalar, the result of the function is implementation defined, and can have an invalid representation (see 13.9.1). If the result type is nonscalar, the effect is implementation defined; in particular, the result can be abnormal (see 13.9.1).

```ada
3.a/3
Reason: {AI05-0229-1} The aspect pragma Convention implies that the attribute Access is not allowed for instances of Unchecked_Conversion.
```

```
3/5
{AI05-0229-1} {AI12-0241-1} generic
  type Source<> is limited private;
type Target<> is limited private;
  function Ada.Unchecked_Conversion(S : Source) return Target
  with Pure, Nonblocking, Convention => Intrinsic;
  pragma Convention(Intrinsic, Ada.Unchecked_Conversion);
  pragma Pure(Ada.Unchecked_Conversion);

3.a/3
Reason: {AI05-0229-1} The aspect pragma Convention implies that the attribute Access is not allowed for instances of Unchecked_Conversion.
```

```
3/5
{AI05-0229-1} {AI12-0241-1} generic
  type Source<> is limited private;
type Target<> is limited private;
  function Ada.Unchecked_Conversion(S : Source) return Target
  with Pure, Nonblocking, Convention => Intrinsic;
  pragma Convention(Intrinsic, Ada.Unchecked_Conversion);
  pragma Pure(Ada.Unchecked_Conversion);

3.a/3
Reason: {AI05-0229-1} The aspect pragma Convention implies that the attribute Access is not allowed for instances of Unchecked_Conversion.
```

```
3/5
{AI05-0229-1} {AI12-0241-1} generic
  type Source<> is limited private;
type Target<> is limited private;
  function Ada.Unchecked_Conversion(S : Source) return Target
  with Pure, Nonblocking, Convention => Intrinsic;
  pragma Convention(Intrinsic, Ada.Unchecked_Conversion);
  pragma Pure(Ada.Unchecked_Conversion);

3.a/3
Reason: {AI05-0229-1} The aspect pragma Convention implies that the attribute Access is not allowed for instances of Unchecked_Conversion.
```
type is erroneous. Properties of scalar types can be checked by using the Valid attribute (see 13.9.2); programs can avoid violating properties of the type (and erroneous execution) by careful use of this attribute.

An instance of Unchecked_Conversion can be applied to an object of a private type, assuming the implementation allows it.

Implementation Permissions

An implementation may return the result of an unchecked conversion by reference, if the Source type is not a by-copy type. [In this case, the result of the unchecked conversion represents simply a different (read-only) view of the operand of the conversion.]

Ramification: In other words, the result object of a call on an instance of Unchecked_Conversion can occupy the same storage as the formal parameter S.

An implementation may place restrictions on Unchecked_Conversion.

Ramification: For example, an instantiation of Unchecked_Conversion for types for which unchecked conversion doesn't make sense may be disallowed.

Implementation Advice

{AI95-00051-02} Since the Size of an array object generally does not include its bounds, hence, the bounds should not be part of the converted data.

Implementation Advice: Since the Size of an array object generally does not include its bounds, the bounds should not be part of the converted data in an instance of Unchecked_Conversion.

Ramification: On the other hand, we have no advice to offer about discriminants and tag fields.

The implementation should not generate unnecessary runtime checks to ensure that the representation of S is a representation of the target type. It should take advantage of the permission to return by reference when possible. Restrictions on unchecked conversions should be avoided unless required by the target environment.

Implementation Advice: There should not be unnecessary runtime checks on the result of an Unchecked_Conversion; the result should be returned by reference when possible. Restrictions on Unchecked_Conversion should be avoided.

Implementation Note: As an example of an unnecessary runtime check, consider a record type with gaps between components. The compiler might assume that such gaps are always zero bits. If a value is produced that does not obey that assumption, then the program might misbehave. The implementation should not generate extra code to check for zero bits (except, perhaps, in a special error-checking mode).

The recommended level of support for unchecked conversions is:

- {AI05-0299-1} Unchecked conversions should be supported and should be reversible in the cases where this subclause defines the result. To enable meaningful use of unchecked conversion, a contiguous representation should be used for elementary subtypes, for statically constrained array subtypes whose component subtype is one of the subtypes described in this paragraph, and for record subtypes without discriminants whose component subtypes are described in this paragraph.

Implementation Advice: The recommended level of support for Unchecked Conversion should be followed.

Wording Changes from Ada 95

{AI95-00051-02} The implementation advice about the size of array objects was moved to 13.3 so that all of the advice about Size is in one place.

{AI95-00426-01} Clarified that the result of Unchecked_Conversion for scalar types can be invalid, but not abnormal.

Wording Changes from Ada 2005

{AI05-0078-1} Correction: Relaxed the alignment requirement slightly, giving a defined result in more cases.
13.9.1 Data Validity

Certain actions that can potentially lead to erroneous execution are not directly erroneous, but instead can cause objects to become abnormal. Subsequent uses of abnormal objects can be erroneous.

A scalar object can have an invalid representation, which means that the object's representation does not represent any value of the object's subtype. The primary cause of invalid representations is uninitialized variables.

Abnormal objects and invalid representations are explained in this subclause.

Dynamic Semantics

When an object is first created, and any explicit or default initializations have been performed, the object and all of its parts are in the normal state. Subsequent operations generally leave them normal. However, an object or part of an object can become abnormal in the following ways:

- An assignment to the object is disrupted due to an abort (see 9.8) or due to the failure of a language-defined check (see 11.6).
- The object is not scalar, and is passed to an in out or out parameter of an imported procedure, the Read procedure of an instance of Sequential_IO, Direct_IO, or Storage_IO, or the stream attribute T'Read or language-defined input procedure, if after return from the procedure the representation of the parameter does not represent a value of the parameter's subtype.
- The object is the return object of a function call of a nonscalar type, and the function is an imported function, an instance of Unchecked_Conversion, or the stream attribute T'Input, if after return from the function the representation of the return object does not represent a value of the function's subtype.

Discussion: We explicitly list the routines involved in order to avoid future arguments. All possibilities are listed.

We did not include Stream_IO.Read in the list above. A Stream_Element should include all possible bit patterns, and thus it cannot be invalid. Therefore, the parameter will always represent a value of its subtype. By omitting this routine, we make it possible to write arbitrary I/O operations without any possibility of abnormal objects.

{AI95-00426-01} For an imported object, it is the programmer's responsibility to ensure that the object remains in a normal state.

Proof: This follows (and echos) the standard rule of interfacing; the programmer must ensure that Ada semantics are followed (see B.1).

Whether or not an object actually becomes abnormal in these cases is not specified. An abnormal object becomes normal again upon successful completion of an assignment to the object as a whole.

Erroneous Execution

It is erroneous to evaluate a primary that is a name denoting an abnormal object, or to evaluate a prefix that denotes an abnormal object.

This paragraph was deleted. Ramification: {AI95-00114-01} Although a composite object with no subcomponents of an access type, and with static constraints all the way down cannot become abnormal, a scalar subcomponent of such an object can become abnormal.

The in out or out parameter case does not apply to scalars; bad scalars are merely invalid representations, rather than abnormal, in this case.

Reason: {AI95-00114-01} The reason we allow access objects, and objects containing subcomponents of an access type, to become abnormal is because the correctness of an access value cannot necessarily be determined merely by looking at the bits of the object. The reason we allow scalar objects to become abnormal is that we wish to allow the compiler to optimize assuming that the value of a scalar object belongs to the object's subtype, if the compiler can prove that the object is initialized with a value that belongs to the subtype. The reason we allow composite objects to
become abnormal if some constraints are nonstatic—is that such object might be represented with implicit levels of
indirection; if those are corrupted, then even assigning into a component of the object, or simply asking for its Address,
might have an unpredictable effect. The same is true if the discriminants have been destroyed.

Bounded (Run-Time) Errors

If the representation of a scalar object does not represent a value of the object's subtype (perhaps because
the object was not initialized), the object is said to have an invalid representation. It is a bounded error to
evaluate the value of such an object. If the error is detected, either Constraint_Error or Program_Error is
raised. Otherwise, execution continues using the invalid representation. The rules of the language outside
this subclause assume that all objects have valid representations. The semantics of operations on invalid
representations are as follows:

Discussion: The AARM is more explicit about what happens when the value of the case expression is an invalid
representation.

Ramification: [AI95-00426-01] This includes the result object of functions, including the result of
Unchecked_Conversion, T'Input, and imported functions.

- If the representation of the object represents a value of the object's type, the value of the type is
  used.

- If the representation of the object does not represent a value of the object's type, the semantics of
  operations on such representations is implementation-defined, but does not by itself lead to
  erroneous or unpredictable execution, or to other objects becoming abnormal.

Implementation Note: [AI95-00426-01] This means that the implementation must take care not to use an invalid
representation in a way that might cause erroneous execution. For instance, the exception mandated for
case statements must be raised. Array indexing must not cause memory outside of the array to be written (and
usually, not read either). These cases and similar cases may require explicit checks by the implementation.

Erroneous Execution

{AI95-00167-01} {AI05-0279-1} A call to an imported function or an instance of Unchecked_Conversion
is erroneous if the result is scalar, and the result object has an invalid representation, and the result is used
other than as the expression of an assignment_statement or an object_declaration, as the object_name
of an object_renaming_declaration, or as the prefix of a Valid attribute. If such a result object is used as
the source of an assignment, and the assigned value is an invalid representation for the target of the
assignment, then any use of the target object prior to a further assignment to the target object, other than
as the prefix of a Valid attribute reference, is erroneous.

Ramification: [AI95-00167-01] In a typical implementation, every bit pattern that fits in an object of a signed
integer subtype will represent a value of the type, if not of the subtype. However, for an enumeration or floating point
type, as well as some modular types, there are typically bit patterns that do not represent any value of the type. In such
cases, the implementation ought to define the semantics of operations on the invalid representations in the obvious
manner (assuming the bounded error is not detected): a given representation should be equal to itself, a representation
that is in between the internal codes of two enumeration literals should behave accordingly when passed to comparison
operators and membership tests, etc. We considered requiring such sensible behavior, but it resulted in too much
arcane verbiage, and since implementations have little incentive to behave irrationally, such verbiage is not important
to have.

{AI95-00167-01} If a stand-alone scalar object is initialized to a an in-range value, then the implementation can take
advantage of the fact that the use of any out-of-range value has to be erroneous abnormal. Such an out-of-range value
can be produced only by things like unchecked conversion, imported functions input, and abnormal values caused by
disruption of an assignment due to abort or to failure of a language-defined check. This depends on out-of-range values
being checked before assignment (that is, checks are not optimized away unless they are proven redundant).

Consider the following example:

{AI95-00167-01} type My_Int is range 0..99;
function Safe_Convert is new Unchecked_Conversion(My_Int, Integer);
function Unsafe_Convert is new Unchecked_Conversion(My_Int, Positive);
X : Positive := Safe_Convert(0); -- Raises Constraint_Error.
Y : Positive := Unsafe_Convert(0); -- Bounded Error, may be invalid.
B : Boolean := Y'Valid; -- OK, B = False.
Z : Positive := Y+1; -- Erroneous to use Y'Invalid.
The call to Unsafe Convert is a bounded error, which might raise Constraint Error, Program Error, or return an invalid value. Moreover, if an exception is not raised, most uses of that invalid value (including the use of Y) cause erroneous execution. The call to Safe_Convert is not erroneous. The result object is an object of subtype Integer containing the value 0. The assignment to X is required to do a constraint check; the fact that the conversion is unchecked does not obviate the need for subsequent checks required by the language rules.

The reason for delaying erroneous execution until the object is used is so that the invalid representation can be tested for validity using the Valid attribute (see 13.9.2) without causing execution to become erroneous. Note that this delay does not imply an exception will not be raised; an implementation could treat both conversions in the example in the same way and raise Constraint Error.

The rules are defined in terms of the result object, and thus the name used to reference that object is irrelevant. That is why we don't need any special rules to describe what happens when the function result is renamed.

Implementation Note: If an implementation wants to have a “friendly” mode, it might always assign an uninitialized scalar a default initial value that is outside the object's subtype (if there is one), and check for this value on some or all reads of the object, so as to help detect references to uninitialized scalars. Alternatively, an implementation might want to provide an “unsafe” mode where it presumed even uninitialized scalars were always within their subtype.

The above rules imply that it is a bounded error to apply a predefined operator to an object with a scalar subcomponent having an invalid representation, since this implies reading the value of each subcomponent. Either Program Error or Constraint Error is raised, or some result is produced, which if composite, might have a corresponding scalar subcomponent still with an invalid representation.

The above mentioned Unchecked..., Unchecked_Deallocation, Unchecked_Access, or Unchecked_Conversion.

Clarified the definition of objects that can become abnormal; made sure that all of the possibilities are included.

Correction: Common programming techniques such as squirreling away an access to a controlled object during initialization and using a self-referencing discriminant (the so-called “Rosen trick”) no longer are

NOTE Objects can become abnormal due to other kinds of actions that directly update the object's representation; such actions are generally considered directly erroneous, however.

In order to reduce the amount of erroneousness, we separate the concept of an undefined value into objects with invalid representation (scalars only) and abnormal objects.

Reading an object with an invalid representation is a bounded error rather than erroneous; reading an abnormal object is still erroneous. In fact, the only safe thing to do to an abnormal object is to assign to the object as a whole.

The description of erroneous execution for Unchecked Conversion and imported objects was tightened up so that using the Valid attribute to test such a value is not erroneous.
immediately erroneous if the object is declared constant, so these techniques can be used portably and safely.
Practically, these techniques already worked as compilers did not take much advantage of this rule, so the impact of
this change will be slight.

Correction: The description of erroneous execution for Unchecked_Conversion and imported objects
was adjusted to clarify that renaming such an object is not, by itself, erroneous.

13.9.2 The Valid Attribute

The Valid attribute can be used to check the validity of data produced by unchecked conversion, input,
interface to foreign languages, and the like.

Static Semantics

For a prefix X that denotes a scalar object [(after any implicit dereference)], the following attribute is
defined:

\[
\text{X'Valid} \quad \text{Yields True if and only if the object denoted by X is normal,}
\text{and has a valid representation, and then, if the preceding conditions hold, the value of X also}
\text{satisfies the predicate of the nominal subtype of X evaluates to True.}
\]

The value of this attribute is of the predefined type Boolean.

Ramification: Having checked that X'Valid is True, it is safe to read the value of X without fear of erroneous
execution caused by abnormality, or a bounded error caused by an invalid representation. Such a read will produce a
value in the subtype of X.

NOTE 1 Invalid data can be created in the following cases (not counting erroneous or unpredictable execution):

- an uninitialized scalar object,
- the result of an unchecked conversion,
- input,
- interface to another language (including machine code),
- aborting an assignment,
- disrupting an assignment due to the failure of a language-defined check (see 11.6), and
- use of an object whose Address has been specified.

NOTE 2 Determining whether X is normal and has a valid representation as part of the
evaluation of X'Valid is not considered to include an evaluation of a read of X, hence, it is not an error to check the validity
of an object that is invalid or abnormal. Determining whether X satisfies the predicates of its nominal subtype cannot
include an evaluation of X, but only after it has been determined that X has a valid representation invalid data.

NOTE 3 The Valid attribute can be used to check the result of calling an instance of
Unchecked_Conversion (or any other operation that can return invalid values). However, an exception handler is still
useful because implementations are permitted to raise Constraint_Error or Program_Error if they
detect the use of an invalid representation (see 13.9.1).

Ramification: If X is of an enumeration type with a representation clause, then X'Valid checks that the value of X
when viewed as an integer is one of the specified internal codes.

Reason: Valid is defined only for scalar objects because the implementation and description burden would be too high
for other types. For example, given a typical run-time model, it is impossible to check the validity of an access value.
The same applies to composite types implemented with internal pointers. One can check the validity of a composite
object by checking the validity of each of its scalar subcomponents. The user should ensure that any composite types
that need to be checked for validity are represented in a way that does not involve implementation-defined
components, or gaps between components. Furthermore, such types should not contain access subcomponents.

This paragraph was deleted.

Note that one can safely check the validity of a composite object with an
abnormal value only if the constraints on the object and all of its subcomponents are static. Otherwise, evaluation of
the prefix of the attribute_reference causes erroneous execution (see 4.1).
X'Valid is new in Ada 95.

Wording Changes from Ada 95

\[AI95-00426-01\] Added a note explaining that handlers for Constraint Error and Program Error are needed in the general case of testing for validity. (An implementation could document cases where these are not necessary, but there is no language requirement.)

Wording Changes from Ada 2005

\[AI05-0153-3\] The validity check now also includes a check of the predicate aspects (see 3.2.4), if any, of the subtype of the object.

Wording Changes from Ada 2012

\[AI12-0071-1\] Corrigendum: Updated wording of the attributes X'Valid to use the new term "satisfies the predicates" (see 3.2.4). Also updated the notes to make sense when evaluating predicates and testing validity of volatile objects.

13.10 Unchecked Access Value Creation

[The attribute Unchecked_Access is used to create access values in an unsafe manner — the programmer is responsible for preventing “dangling references”.]

Static Semantics

The following attribute is defined for a prefix X that denotes an aliased view of an object:

X'Unchecked_Access

All rules and semantics that apply to X'Access (see 3.10.2) apply also to X'Unchecked_Access, except that, for the purposes of accessibility rules and checks, it is as if X were declared immediately within a library package.

Ramification: \[AI05-0005-1\] We say “rules and semantics” here so that library-level accessibility applies to the value created by X'Unchecked Access as well as to the checks needed for the attribute itself. This means that any anonymous access values that inherit the accessibility of this attribute (such as access parameters) also act as if they have library-level accessibility. We don't want the "real" accessibility of the created value re-emerging at a later point — that would create hard-to-understand bugs.

NOTE 1 \[AI12-0449-1\] This attribute is provided to support the situation where a local object is to be inserted into a global linked data structure, when the programmer knows that it will always be removed from the data structure prior to exiting the object's scope. The Access attribute would be illegal in this case (see 3.10.23-10.2, “Operations of Access Types”).

Ramification: The expected type for X'Unchecked_Access is as for X'Access.

If an attribute_reference with Unchecked_Access is used as the actual parameter for an access parameter, an Accessibility_Check can never fail on that access parameter.

NOTE 2 There is no Unchecked_Access attribute for subprograms.

Reason: \[AI95-00254-01\] Such an attribute would allow unsafe “downward closures”, where an access value designating a more nested subprogram is passed to a less nested subprogram. (Anonymous access-to-subprogram parameters provide safe “downward closures”.) This requires some means of reconstructing the global environment for the more nested subprogram, so that it can do up-level references to objects. The two methods of implementing up-level references are displays and static links. If unsafe downward closures were supported, each access-to-subprogram value would have to carry the static link or display with it. We don't want to require the space and time overhead of requiring the extra information for all access-to-subprogram types, especially as including it would make interfacing to other languages (like C) harder. In the case of displays, this was judged to be infeasible, and we don't want to disrupt implementations by forcing them to use static links if they already use displays.

If desired, an instance of Unchecked_Conversion can be used to create an access value of a global access-to-subprogram type that designates a local subprogram. The semantics of using such a value are not specified by the language. In particular, it is not specified what happens if such subprograms make up-level references; even if the frame being referenced still exists, the up-level reference might go awry if the representation of a value of a global access-to-subprogram type doesn't include a static link.
13.11 Storage Management

[ Each access-to-object type has an associated storage pool. The storage allocated by an allocator comes from the pool; instances of Unchecked_Deallocation return storage to the pool. Several access types can share the same pool.]

{AI95-00435-01} [A storage pool is a variable of a type in the class rooted at Root_Storage_Pool, which is an abstract limited controlled type. By default, the implementation chooses a standard storage pool for each access-to-object type. The user may define new pool types, and may override the choice of pool for an access-to-object type by specifying Storage_Pool for the type.]

**Ramification:** By default, the implementation might choose to have a single global storage pool, which is used (by default) by all access types, which might mean that storage is reclaimed automatically only upon partition completion. Alternatively, it might choose to create a new pool at each accessibility level, which might mean that storage is reclaimed for an access type when leaving the appropriate scope. Other schemes are possible.

**Term entry:** storage pool object — object associated with one or more access types from which the storage for objects created by allocators of the access type(s) is obtained

**Note:** Some storage pools can be partitioned into subpools in order to support finer-grained storage management.

**Legalities Rules**

If Storage_Pool is specified for a given access type, Storage_Size shall not be specified for it.

**Reason:** The Storage_Pool determines the Storage_Size; hence it would not make sense to specify both. Note that this rule is simplified by the fact that the aspects in question cannot be specified for derived types, nor for nonfirst subtypes, so we don't have to worry about whether, say, Storage_Pool on a derived type overrides Storage_Size on the parent type. For the same reason, “specified” means the same thing as “directly specified” here.

**Static Semantics**

The following language-defined library package exists:

{AI12-0235-1} with Ada.Finalization;
with System.Storage_Elements;
package System.Storage_Pools with Pure, Nonblocking => False is
pragma Preelaborate(System.Storage_Pools);

{AI95-00161-01} {AI12-0399-1} type Root_Storage_Pool is abstract new Ada.Finalization.Limited_Controlled with private;
withpragma Preelaborable_Initialization(Root_Storage_Pool);

procedure Allocate(
  Pool : in out Root_Storage_Pool;
  Storage_Address : out Address;
  Size_In_Storage_Elements : in Storage_Elements.Storage_Count;
  Alignment : in Storage_Elements.Storage_Count) is abstract;

procedure Deallocate(
  Pool : in out Root_Storage_Pool;
  Storage_Address : in Address;
  Size_In_Storage_Elements : in Storage_Elements.Storage_Count;
  Alignment : in Storage_Elements.Storage_Count) is abstract;

function Storage_Size(Pool : Root_Storage_Pool) return Storage_Elements.Storage_Count is abstract;

private
  -- not specified by the language
end System.Storage_Pools;

**Reason:** The Alignment parameter is provided to Deallocate because some allocation strategies require it. If it is not needed, it can be ignored.

A storage pool type (or pool type) is a descendant of Root_Storage_Pool. The elements of a storage pool are the objects allocated in the pool by allocators.
Discussion: In most cases, an element corresponds to a single memory block allocated by Allocate. However, in some cases the implementation may choose to associate more than one memory block with a given pool element.

For every access-to-object subtype \( S \), the following representation attributes are defined:

**S'_storage_pool**

Denotes the storage pool of the type of \( S \). The type of this attribute is Root_Storage_Pool'Class.

**S'storage_size**

Yields the result of calling \( \text{Storage_Size}(S'\text{storage_pool}) \), which is intended to be a measure of the number of storage elements reserved for the pool. The type of this attribute is \( \text{universal_integer} \).

Ramification: Storage_Size is also defined for task subtypes and objects — see 13.3.

Storage_Size is not a measure of how much un-allocated space is left in the pool. That is, it includes both allocated and unallocated space. Implementations and users may provide a Storage_Available function for their pools, if so desired.

For every access-to-object subtype \( S \), the following representation attributes are defined:

**S'_storage_pool**

Denotes the storage pool of the type of \( S \). The type of this attribute is Root_Storage_Pool'Class.

**S'storage_size**

Yields the result of calling \( \text{Storage_Size}(S'\text{storage_pool}) \), which is intended to be a measure of the number of storage elements reserved for the pool. The type of this attribute is \( \text{universal_integer} \).

Ramification: Storage_Size is also defined for task subtypes and objects — see 13.3.

Storage_Size is not a measure of how much un-allocated space is left in the pool. That is, it includes both allocated and unallocated space. Implementations and users may provide a Storage_Available function for their pools, if so desired.

For every access-to-object subtype \( S \), the following representation attributes are defined:

**S'_storage_pool**

Denotes the storage pool of the type of \( S \). The type of this attribute is Root_Storage_Pool'Class.

**S'storage_size**

Yields the result of calling \( \text{Storage_Size}(S'\text{storage_pool}) \), which is intended to be a measure of the number of storage elements reserved for the pool. The type of this attribute is \( \text{universal_integer} \).

Ramification: Storage_Size is also defined for task subtypes and objects — see 13.3.

Storage_Size is not a measure of how much un-allocated space is left in the pool. That is, it includes both allocated and unallocated space. Implementations and users may provide a Storage_Available function for their pools, if so desired.

For every access-to-object subtype \( S \), the following representation attributes are defined:

**S'_storage_pool**

Denotes the storage pool of the type of \( S \). The type of this attribute is Root_Storage_Pool'Class.

**S'storage_size**

Yields the result of calling \( \text{Storage_Size}(S'\text{storage_pool}) \), which is intended to be a measure of the number of storage elements reserved for the pool. The type of this attribute is \( \text{universal_integer} \).

Ramification: Storage_Size is also defined for task subtypes and objects — see 13.3.

Storage_Size is not a measure of how much un-allocated space is left in the pool. That is, it includes both allocated and unallocated space. Implementations and users may provide a Storage_Available function for their pools, if so desired.

For every access-to-object subtype \( S \), the following representation attributes are defined:

**S'_storage_pool**

Denotes the storage pool of the type of \( S \). The type of this attribute is Root_Storage_Pool'Class.

**S'storage_size**

Yields the result of calling \( \text{Storage_Size}(S'\text{storage_pool}) \), which is intended to be a measure of the number of storage elements reserved for the pool. The type of this attribute is \( \text{universal_integer} \).

Ramification: Storage_Size is also defined for task subtypes and objects — see 13.3.

Storage_Size is not a measure of how much un-allocated space is left in the pool. That is, it includes both allocated and unallocated space. Implementations and users may provide a Storage_Available function for their pools, if so desired.

For every access-to-object subtype \( S \), the following representation attributes are defined:

**S'_storage_pool**

Denotes the storage pool of the type of \( S \). The type of this attribute is Root_Storage_Pool'Class.

**S'storage_size**

Yields the result of calling \( \text{Storage_Size}(S'\text{storage_pool}) \), which is intended to be a measure of the number of storage elements reserved for the pool. The type of this attribute is \( \text{universal_integer} \).

Ramification: Storage_Size is also defined for task subtypes and objects — see 13.3.

Storage_Size is not a measure of how much un-allocated space is left in the pool. That is, it includes both allocated and unallocated space. Implementations and users may provide a Storage_Available function for their pools, if so desired.

For every access-to-object subtype \( S \), the following representation attributes are defined:

**S'_storage_pool**

Denotes the storage pool of the type of \( S \). The type of this attribute is Root_Storage_Pool'Class.

**S'storage_size**

Yields the result of calling \( \text{Storage_Size}(S'\text{storage_pool}) \), which is intended to be a measure of the number of storage elements reserved for the pool. The type of this attribute is \( \text{universal_integer} \).

Ramification: Storage_Size is also defined for task subtypes and objects — see 13.3.

Storage_Size is not a measure of how much un-allocated space is left in the pool. That is, it includes both allocated and unallocated space. Implementations and users may provide a Storage_Available function for their pools, if so desired.
This paragraph was deleted.

Implementation defined: The manner of choosing a storage pool for an access type when Storage_Pool is not specified for the type.

Discussion: The manner of choosing a storage pool is covered by a Documentation Requirement below, so it is not summarized here.

Implementation defined: Whether or not the implementation provides user-accessible names for the standard pool type(s).

To be honest: [AI12-0005-1] pragma Default_Storage_Pool (see 13.11.3) can be used to specify a specific pool (or none at all) to be used with access types declared in a particular declaration list, rather than a standard storage pool.

{AI12-0005-1} Although there is no language-defined user-accessible name for the standard pool type(s), the default use of a standard pool may be indicated using the identifier Standard in the pragma Default_Storage_Pool.

Ramification: [AI95-00230-01] An anonymous access type has no pool. An access-to-object type defined by a derived_type_definition inherits its pool from its parent type, so all access-to-object types in the same derivation class share the same pool. Hence the “defined by an access_to_object_definition” wording above.

There is no requirement that all storage pools be implemented using a contiguous block of memory (although each allocation returns a pointer to a contiguous block of memory).

{AI12-0319-1} {AI12-0424-1} The type(s) of the standard pool(s), and the primitive Allocate, Deallocate, and Storage_Size subprograms for the standard pool(s) are nonblocking. Concurrent invocations of these subprograms do not conflict with one another (see 9.10) when applied to standard storage pools.

Reason: We need to specify that the type is nonblocking so that an instance of Unchecked_Deallocation is nonblocking if the object type is nonblocking (as the type is used in the contract). Ada 95 did not declare standard allocation/deallocation as potentially blocking, so these things can be used in protected types, and we want that to remain true (with static checking).

{AI12-0043-1} {AI12-0319-1} If Storage_Size is specified for an access type T, an implementation-defined pool P is used for the type. Then the Storage_Size of this pool is at least that requested, and the storage for P is reclaimed when the master containing the declaration of the access type is left. If the implementation cannot satisfy the request, Storage_Error is raised at the freezing point of type T. The storage pool P is used only for allocators returning type T or other access types specified to use T's Storage_Pool. Storage_Error is raised by an allocator returning such a type if the storage space of P is exhausted (additional memory is not allocated), the attribute_definition_clause. If neither Storage_Pool nor Storage_Size are specified, then the meaning of Storage_Size is implementation defined. The type of P, and the primitive Allocate, Deallocate, and Storage_Size subprograms of P are nonblocking.

{AI12-0043-1} If neither Storage_Pool nor Storage_Size are specified, then the meaning of Storage_Size is implementation defined.

Implementation defined: The meaning of Storage_Size when neither the Storage_Size nor the Storage_Pool is specified for an access type.

Ramification: The Storage_Size function and attribute will return the actual size, rather than the requested size. Comments about rounding up, zero, and negative on task Storage_Size apply here, as well. See also A183-00557, A183-00558, and A183-00608.

The expression in a Storage_Size clause need not be static.

The reclamation happens after the master is finalized.

Implementation Note: For a pool allocated on the stack, normal stack cut-back can accomplish the reclamation. For a library-level pool, normal partition termination actions can accomplish the reclamation.

If Storage_Pool is specified for an access type, then the specified pool is used.

The effect of calling Allocate and Deallocate for a standard storage pool directly (rather than implicitly via an allocator or an instance of Unchecked_Deallocation) is unspecified.

Ramification: For example, an allocator might put the pool element on a finalization list. If the user directly Deallocates it, instead of calling an instance of Unchecked_Deallocation, then the implementation would probably try to finalize the object upon master completion, which would be bad news. Therefore, the implementation should define such situations as erroneous.
Erroneous Execution

If Storage_Pool is specified for an access type, then if Allocate can satisfy the request, it should allocate a contiguous block of memory, and return the address of the first storage element in Storage_Address. The block should contain Size_In_Storage_Elements storage elements, and should be aligned according to Alignment. The allocated storage should not be used for any other purpose while the pool element remains in existence. If the request cannot be satisfied, then Allocate should propagate an exception [(such as Storage_Error)]. If Allocate behaves in any other manner, then the program execution is erroneous.

Implementation Requirements

\{AI05-0107-1\} \{AI05-0262-1\} The Allocate procedure of a user-defined storage pool object P may be called by the implementation only to allocate storage for a type T whose pool is P, only at the following points:

- During the execution of an allocator of type T;
  
  Ramification: This includes during the evaluation of the initializing expression such as an aggregate; this is important if the initializing expression is built-in-place. We need to allow allocation to be deferred until the size of the object is known.

- During the execution of a return statement for a function whose result is built-in-place in the result of an allocator of type T;
  
  Reason: We need this bullet as well as the preceding one in order that exceptions that propagate from such a call to Allocate can be handled within the return statement. We don't want to require the generation of special handling code in this unusual case, as it would add overhead to most return statements of composite types.

- During the execution of an assignment operation with a target of an allocated object of type T with a part that has an unconstrained discriminated subtype with defaults.
  
  Reason: We allow Allocate to be called during assignment of objects with mutable parts so that mutable objects can be implemented with reallocation on assignment. (Unfortunately, the term “mutable” is only defined in the AARM, so we have to use the long-winded wording shown here.)

Discussion: Of course, explicit calls to Allocate are also allowed and are not bound by any of the rules found here.

\{AI05-0107-1\} \{AI05-0116-1\} \{AI05-0193-1\} \{AI05-0262-1\} \{AI05-0269-1\} For each of the calls of Allocate described above, P (equivalent to T's Storage Pool) is passed as the Pool parameter. The Size_In_Storage_Elements parameter indicates the number of storage elements to be allocated, and is no more than D'Max_Size_In_Storage_Elements, where D is the designated subtype of T. The Alignment parameter is a nonzero integral multiple of D'Alignment if D is a specific type, and otherwise is a nonzero integral multiple of the alignment of the specific type identified by the tag of the object being created; it is unspecified if there is no such value. The Alignment parameter is no more than D'Max_Alignment_For_Allocation. The result returned in the Storage_Address parameter is used as the address of the allocated storage, which is a contiguous block of memory of Size_In_Storage_Elements storage elements. [Any exception propagated by Allocate is propagated by the construct that contained the call.]

Ramification: Note that the implementation does not turn other exceptions into Storage_Error.

“Nonzero integral multiple” of an alignment includes the alignment value itself, of course. The value is unspecified if the alignment of the specific type is zero.

\{AI05-0107-1\} \{AI12-0445-1\} The number of calls to Allocate that will be used to implement an allocator for any particular type is unspecified. The number of calls to Deallocate that will be used to implement an instance of Unchecked_Deallocation (see 13.11.2) for any particular object is the same as the number of Allocate calls for that object.

Reason: This supports objects that are allocated in one or more parts. The second sentence prevents extra or missing calls to Deallocate.
To be honest: \{AI05-0005-1\} The number of calls to Deallocate from all sources for an object always will be the same as the number of calls to Allocate from all sources for that object. However, in unusual cases, not all of those Deallocate calls may be made by an instance of Unchecked Deallocation. Specifically, in the unusual case of assigning to an object of a mutable variant record type such that the variant changes, some of the Deallocate calls may be made by the assignment (as may some of the Allocate calls).

Ramification: We do not define the relative order of multiple calls used to deallocate the same object — that is, if the allocator allocated two pieces \(x\) and \(y\), then an instance of Unchecked_Deallocation might deallocate \(x\) and then \(y\), or it might deallocate \(y\) and then \(x\).

\{AI05-0107-1\} The Deallocate procedure of a user-defined storage pool object \(P\) may be called by the implementation to deallocate storage for a type \(T\) whose pool is \(P\) only at the places when an Allocate call is allowed for \(P\), during the execution of an instance of Unchecked_Deallocation for \(T\), or as part of the finalization of the collection of \(T\). For such a call of Deallocate, \(P\) (equivalent to \(T\Storage_Pool\)) is passed as the Pool parameter. The value of the Storage_Address parameter for a call to Deallocate is the value returned in the Storage_Address parameter of the corresponding successful call to Allocate. The values of the Size_In_Storage_Elements and Alignment parameters are the same values passed to the corresponding Allocate call. Any exception propagated by Deallocate is propagated by the construct that contained the call.

Reason: We allow Deallocate to be called anywhere that Allocate is, in order to allow the recovery of storage from failed allocations (that is, those that raise exceptions); from extended return statements that exit via a goto, exit, or locally handled exception; and from objects that are deallocated when they are assigned. In each of these cases, we would have a storage leak if the implementation did not recover the storage (there is no way for the programmer to do it). We do not require such recovery, however, as it could be a serious performance drag on these operations.

Documentation Requirements

\{AI12-0445-1\} An implementation shall document the set of values that a user-defined Allocate procedure \texttt{hasneneeds} to accept for the Alignment parameter. An implementation shall document how the standard storage pool is chosen, and how storage is allocated by standard storage pools.

This paragraph was deleted. Implementation defined: Implementation-defined aspects of storage pools.

Documentation Requirement: The set of values that a user-defined Allocate procedure needs to accept for the Alignment parameter. How the standard storage pool is chosen, and how storage is allocated by standard storage pools.

Implementation Advice

An implementation should document any cases in which it dynamically allocates heap storage for a purpose other than the evaluation of an allocator.

Implementation Advice: Any cases in which heap storage is dynamically allocated other than as part of the evaluation of an allocator should be documented.

Reason: This is “Implementation Advice” because the term “heap storage” is not formally definable; therefore, it is not testable whether the implementation obeys this advice.

A default (implementation-provided) storage pool for an access-to-constant type should not have overhead to support deallocation of individual objects.

Implementation Advice: A default storage pool for an access-to-constant type should not have overhead to support deallocation of individual objects.

Ramification: Unchecked_Deallocation is not defined for such types. If the access-to-constant type is library-level, then no deallocation (other than at partition completion) will ever be necessary, so if the size needed by an allocator of the type is known at link-time, then the allocation should be performed statically. If, in addition, the initial value of the designated object is known at compile time, the object can be allocated to read-only memory.

Implementation Note: If the Storage_Size for an access type is specified, the storage pool should consist of a contiguous block of memory, possibly allocated on the stack. The pool should contain approximately this number of storage elements. These storage elements should be reserved at the place of the Storage_Size clause, so that allocators cannot raise Storage_Error due to running out of pool space until the appropriate number of storage elements has been used up. This approximate (possibly rounded-up) value should be used as a maximum; the implementation should not increase the size of the pool on the fly. If the Storage_Size for an access type is specified as zero, then the pool should not take up any storage space, and any allocator for the type should raise Storage_Error.
24.c Ramification: Note that most of this is approximate, and so cannot be (portably) tested. That's why we make it an Implementation Note. There is no particular number of allocations that is guaranteed to succeed, and there is no particular number of allocations that is guaranteed to fail.

25/2 The storage pool used for an allocator of an anonymous access type should be determined as follows:

- If the allocator is defining a coextension (see 3.10.2) of an object being created by an outer allocator, then the storage pool used for the outer allocator should also be used for the coextension;
- For other access discriminants and access parameters, the storage pool should be created at the point of the allocator, and be reclaimed when the allocated object becomes inaccessible;
- If the allocator defines the result of a function with an access result, the storage pool is determined as though the allocator were in place of the call of the function. If the call is the operand of a type conversion, the storage pool is that of the target access type of the conversion. If the call is itself defining the result of a function with an access result, this rule is applied recursively;
- Otherwise, a default storage pool should be created at the point where the anonymous access type is elaborated; such a storage pool may have no mechanism for the need not support deallocation of individual objects.

25.1/2 Implementation Advice: Usually, a storage pool for an access discriminant or access parameter should be created at the point of an allocator, and be reclaimed when the designated object becomes inaccessible. For other anonymous access types, the pool should be created at the point where the type is elaborated and may have no mechanism for the need not support deallocation of individual objects.

25.2/2 Implementation Note: For access parameters and access discriminants, Normally the "storage pool" for an anonymous access type would not normally exist as a separate entity. Instead, the designated object of the allocator would be allocated, in the case of an access parameter, as a local aliased variable at the call site, and in the case of an access discriminant, contiguous with the object containing the discriminant. This is similar to the way storage for aggregates is typically managed.

25.3/3 For other sorts of anonymous access types, this implementation is not possible in general, as the accessibility of the anonymous access type is that of its declaration, while the allocator could be more nested. In this case, a "real" storage pool is required. Note, however, that this storage pool need not support (separate) deallocation, as it is not possible to instantiate Unchecked Deallocate with an anonymous access type. (If deallocation is needed, the object should be allocated for a named access type and converted.) Thus, deallocation only need happen when the object is defined a coextension (see 3.10.2) of an anonymous access type should be

25.4/5 If the allocator defines the result of a function with an access result, the storage pool is determined as though the allocator were in place of the call of the function. If the call is the operand of a type conversion, the storage pool is that of the target access type of the conversion. If the call is itself defining the result of a function with an access result, this rule is applied recursively;

26/5 A user-defined storage pool type can be obtained by extending the Root_Storage_Pool type, and overriding the primitive subprograms Allocate, Deallocate, and Storage_Size. A user-defined storage pool can then be obtained by declaring an object of the type extension. The user can override Initialize and Finalize if there is any desire for nontrivial initialization and finalization for a user-defined pool type. For example, Finalize can reclaim blocks of storage that are allocated separately from the pool object itself.

NOTE 1 A user-defined storage pool type can be obtained by extending the Root_Storage_Pool type, and overriding the primitive subprograms Allocate, Deallocate, and Storage_Size. A user-defined storage pool can then be obtained by declaring an object of the type extension. The user can override Initialize and Finalize if there is any desire for nontrivial initialization and finalization for a user-defined pool type. For example, Finalize can reclaim blocks of storage that are allocated separately from the pool object itself.

NOTE 2 The writer of the user-defined allocation and deallocation procedures, and users of allocators for the associated access type, are responsible for dealing with any interactions with tasks. In particular:
- If the allocators are used in different tasks, they require mutual exclusion.
- If they are used inside protected objects, they cannot block.

NOTE 3 The primitives Allocate, Deallocate, and Storage_Size are declared as abstract (see 3.9.3), and therefore they have to be overridden when a new (nonabstract) storage pool type is declared.

Ramification: Note that the Storage_Pool attribute denotes an object, rather than a value, which is somewhat unusual for attributes.

The calls to Allocate, Deallocate, and Storage_Size are dispatching calls — this follows from the fact that the actual parameter for Pool is T'Storage_Pool, which is of type Root_Storage_Pool'Class. In many cases (including all cases in
which Storage_Pool is not specified), the compiler can determine the tag statically. However, it is possible to construct cases where it cannot.

All access types in the same derivation class share the same pool, whether implementation defined or user defined. This is necessary because we allow type conversions among them (even if they are pool-specific), and we want pool-specific access values to always designate an element of the right pool.

**Implementation Note:** If an access type has a standard storage pool, then the implementation doesn't actually have to follow the pool interface described here, since this would be semantically invisible. For example, the allocator could conceivably be implemented with inline code.

### Examples

To associate an access type with a storage pool object, the user first declares a pool object of some type derived from Root_Storage_Pool. Then, the user defines its Storage_Pool attribute, as follows:

```ada
Pool_Object : Some_Storage_Pool_Type;

type T is access Designated;
for T'Storage_Pool use Pool_Object;
```

{AFI2-0440-1} Another access type may be added to an existing storage pool, via:

```ada
for T2'Storage_Pool use T'Storage_Pool;
```

The semantics of this is implementation defined for a standard storage pool.

**Reason:** For example, the implementation is allowed to choose a storage pool for T that takes advantage of the fact that T is of a certain size. If T2 is not of that size, then the above will probably not work.

{AI05-0111-3} {AFI2-0440-1} As usual, a derivative of Root_Storage_Pool may define additional operations. For example, consider the presumption that Mark_Release_Pool_Type defined in 13.11.6, that has two additional operations, Mark and Release, the following is a possible use:

```ada
{8652/0041} {AI95-00066-01} {AI05-0111-3} type Mark_Release_Pool_Type
(Pool_Size : Storage_Elements.Storage_Count;
 Block_Size : Storage_Elements.Storage_Count)
    is new Subpools.Root_Storage_Pool_With_Subpools Root_Storage_Pool with
    limited private;
    -- As defined in package MR Pool, see 13.11.6
...
{AI05-0111-3} {AI12-0178-1} Our_Pool : Mark_Release_Pool_Type (Pool_Size => 2000,
    Block_Size => 100);
My_Mark : Subpool_Handle Our_Pool.Subpool_Handle;  -- As declared in See 13.11.6

{AI05-0111-3} type Acc is access ...;
for Acc'Storage_Pool use Our_PoolMR_Pool;
...
{AI05-0111-3} My_Mark := Mark(Our_PoolMR_Pool);
...  -- Allocate objects using “new (My_Mark)Designated(...)”.
Release(My_MarkMR_Pool);  -- Finalize objects and reclaimReclaim the storage.
```

### Extensions to Ada 83

User-defined storage pools are new to Ada 95.

### Wording Changes from Ada 83

{AI05-0005-1} {AI05-0190-1} Ada 83 originally introduced the concept called a “collection”, which is similar to what we call a storage pool. All access types in the same derivation class share the same collection. In Ada 95 introduces the storage pool, which is similar in that all access types in the same derivation class share the same storage pool, but other (unrelated) access types can also share the same storage pool, either by default, or as specified by the user. A collection was an amorphous grouping of objects (mainly used to describe finalization of access types); a storage pool is a more concrete concept — hence the different name.

RM83 states the erroneousness of reading or updating deallocated objects incorrectly by missing various cases.
13.11 Storage Management

### Incompatibilities With Ada 95

#### {AI95-00035-01} Amendment Correction: Storage pools (and Storage Size) are not defined for access-to-subprogram types. The original Ada 95 wording defined the attributes, but said nothing about their values. If a program uses attributes Storage Pool or Storage Size on an access-to-subprogram type, it will need to be corrected for Ada 2005. That's a good thing, as such a use is a bug — the concepts never were defined for such types.

#### Extensions to Ada 95

#### {AI95-00161-01} Amendment Correction: Added pragma Preelaborable Initialization to type Root Storage Pool, so that extensions of it can be used to declare default-initialized objects in preelaborated units.

#### Wording Changes from Ada 95

#### {8652/0009} {AI95-00137-01} Corrigendum: Added wording to specify that these are representation attributes.

#### {AI95-00230-01} Added wording to clarify that an allocator shares the pool with the outer allocator.

#### Wording Changes from Ada 2005

#### {AI05-0051-1} Correction: Added the missing definition of the storage pool of an allocator for an anonymous access result type.

#### {AI05-0107-1} Correction: Clarified when an implementation is allowed to call Allocate and Deallocate, and the requirements on such calls.

#### {AI05-0111-3} Added wording to support subpools and refer to the subpool example, see 13.11.4.

#### {AI05-0116-1} Correction: Added wording to specify that the alignment for an allocator with a class-wide designated type comes from the specific type that is allocated.

#### {AI05-0193-1} Added wording to allow larger alignments for calls to Allocate made by allocators, up to Max Alignment For Allocation. This eases implementation in some cases.

#### Extensions to Ada 2012

#### {AI12-0235-1} Package System.Storage_Pools now has Pure categorization, so it can be mentioned for any package. Note that this does not allow storage pool objects to be shared between partitions, as these necessarily must be variables; however, this does allow a storage pool type to be shared.

#### Wording Changes from Ada 2012

#### {AI12-0043-1} Corrigendum: Tightened up the description of the implementation-defined pool used when Storage Size is specified. This is not intended to change any implementation.

#### {AI12-0319-1} {AI12-0424-1} Specified that the standard pool(s), and the pool(s) used to implement a specified Storage Size, are nonblocking and support concurrent use. This was always true (which is why this is not documented as an incompatibility), but it never was explicitly stated before. In the past, the absence of wording defining something to be potentially blocking determined if blocking was not allowed. Similarly, the absence of a statement that allocation was not allowed in multiple tasks implied that it was allowed.

### 13.11.1 Storage Allocation Attributes

#### The Max_Size_In_Storage.Elements Attribute

#### {AI05-0193-1} [The Max_Size_In_Storage.Elements and Max Alignment For Allocation attributes may be attributes is useful in writing user-defined pool types.]

#### Static Semantics

#### {AI05-0193-1} For every subtype S, the following attributes are attribute is defined:

#### S'Max_Size_In_Storage.Elements

#### {AI95-00256-01} {AI95-00416-01} {AI05-0193-1} {AI12-0439-1} Denotes the maximum value for Size_In_Storage.Elements that could be requested by the implementation via Allocate for an access type whose designated subtype is S. For a type with access discriminants, if the implementation allocates space for a coextension in the same pool as that
of the object having the access discriminant, then this accounts for any calls on Allocate that could be performed to provide space for such coextensions. The value of this attribute is of type universal_integer.

**Ramification:** If S is an unconstrained array subtype, or an unconstrained subtype with discriminants, S'Max_Size_In_Storage_Elements might be very large.

**S'Max_Alignment_For_Allocation**

\[\text{AI05-0193-1} \quad \text{AI12-0439-1}\] Denotes the maximum value for Alignment that can be requested by the implementation via Allocate for an access type whose designated subtype is S. The value of this attribute is of type universal_integer.

\[\text{AI05-0193-1} \quad \text{AI12-0439-1}\] For a type with access discriminants, if the implementation allocates space for a coextension in the same pool as that of the object having the access discriminant, then these attributes account for any calls on Allocate that can be performed to provide space for such coextensions.

**Reason:** \[\text{AI05-0193-1}\] The values of these attributes should reflect only the calls that might be made to the pool specified for an access type with designated type S. Thus, if the coextensions would normally be allocated from a different pool than the one used for the main object (that is, the Implementation Advice of 13.11 for determining the pool of an anonymous access discriminant is not followed), then these attributes should not reflect any calls on Allocate used to allocate the coextensions.

**Ramification:** \[\text{AI05-0193-1}\] Coextensions of coextensions of this type (and so on) are included in the values of these attributes if they are allocated from the same pool.

**Wording Changes from Ada 95**

\[\text{AI95-00256-01}\] Corrected the wording so that a fortune-telling compiler that can see the future execution of the program is not required.

**Extensions to Ada 2005**

\[\text{AI05-0193-1}\] The Max_Alignment_For_Allocation attribute is new.

### 13.11.2 Unchecked Storage Deallocation

[Unchecked storage deallocation of an object designated by a value of an access type is achieved by a call to an instance of the generic procedure Unchecked_Deallocation.]

**Static Semantics**

The following language-defined generic library procedure exists:

\[\text{AI05-0229-1} \quad \text{AI12-0241-1} \quad \text{AI12-0302-1} \quad \text{AI12-0319-1}\] \textit{generic}

\textit{type} Object<> is limited private;

\textit{type} Name is access Object;

\textit{procedure} Ada.Unchecked_Deallocation(\textit{in out} Name)

\textit{with} Preelaborate, Nonblocking,

\textit{Global => in out Name.Storage_Pool},

\textit{Convention => Intrinsic};

pragma Convention(Intrinsic, Ada.Unchecked_Deallocation);

pragma Preelaborate(Ada.Unchecked_Deallocation);

**Reason:** \[\text{AI05-0229-1}\] The aspect pragma Convention implies that the attribute Access is not allowed for instances of Unchecked_Deallocation.

**Legality Rules**

\[\text{AI05-0157-1}\] A call on an instance of Unchecked_Deallocation is illegal if the actual access type of the instance is a type for which the Storage_Size has been specified by a static expression with value zero or is defined by the language to be zero. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.
Discussion: This rule is the same as the rule for allocators. We could have left the last sentence out, as a call to Unchecked_Deallocation cannot occur in a specification as it is a procedure call, but we left it for consistency and to avoid future maintenance hazards.

Dynamic Semantics

Given an instance of Unchecked_Deallocation declared as follows:

```
procedure Free is
  new Ada.Unchecked_Deallocation(
    object_subtype_name, access_to_variable_subtype_name);
```

Procedure Free has the following effect:

1. After executing Free(X), the value of X is null.
2. Free(X), when X is already equal to null, has no effect.
3. Free(X), when X is not equal to null first performs finalization of the object designated by X (and any coextensions of the object — see 3.10.2), as described in 7.6.17.6. It then deallocates the storage occupied by the object designated by X (and any coextensions). If the storage pool is a user-defined object, then the storage is deallocated by calling Deallocate as described in 13.11, passing access_to_variable_subtype_name.Storage_Pool as the Pool parameter. Storage_Address is the value returned in the Storage_Address parameter of the corresponding Allocate call. Size_In_Storage_Elements and Alignment are the same values passed to the corresponding Allocate call. There is one exception: if the object being freed contains tasks, it is unspecified whether the object is deallocated.

Ramification: Free calls only the specified Deallocate procedure to do deallocation. For any given object deallocation, the number of calls to Free (usually one) will be equal to the number of Allocate calls it took to allocate the object. We do not define the relative order of multiple calls used to deallocate the same object — that is, if the allocator allocated two pieces x and y, then Free might deallocate x and then y, or it might deallocate y and then x.

Bounded (Run-Time) Errors

It is a bounded error to free a discriminated, unterminated task object. The possible consequences are:

Reason: This is an error because the task might refer to its discriminants, and the discriminants might be deallocated by freeing the task object.

- No exception is raised.
- Program_Error or Tasking_Error is raised at the point of the deallocation.
- Program_Error or Tasking_Error is raised in the task the next time it references any of the discriminants.

Implementation Note: This last case presumes an implementation where the task references its discriminants indirectly, and the pointer is nulled out when the task object is deallocated.

In the first two cases, the storage for the discriminants (and for any enclosing object if it is designated by an access discriminant of the task) is not reclaimed prior to task termination.

Ramification: The storage might never be reclaimed.

Discussion: These can result from use of Unchecked_Deallocation, Unchecked_Deallocate_Subpool, and attribute Unchecked_Access. Bad results from Unchecked_Conversion and from stream-oriented attributes are abnormal by 13.9.1, which is stronger and thus takes precedence.
If a dangling reference is dereferenced (implicitly or explicitly), execution is erroneous (see below). If there is no explicit or implicit dereference, then it is a bounded error to evaluate an expression whose result is a dangling reference. If the error is detected, either Constraint_Error or Program_Error is raised. Otherwise, execution proceeds normally, but with the possibility that the access value designates some other existing object.

**Reason:** If a dangling reference is compared with another access value, a result of either True or False is allowed. We need to allow this so that simple implementations of access values (for instance, as a bare address) can work if the memory in question is reused. (The formal definition of access equality is that it returns True if both access values designate the same object; that can never be True if one of the values is a dangling reference, and the other is not, but both values could refer to the same memory.) Membership tests that do not involve an implicit dereference generally do not depend on the access value at all.

We allow Constraint_Error to be raised here so that dangling reference and null pointer checks can be combined into a single check. If different exceptions are required, then the checks have to be made separately - but there's little semantic difference (neither designate a usable object).

**Ramification:** If a dangling reference is assigned into an object, including being passed to a formal parameter, that object also contains a dangling reference afterwards.

**Discussion:** For equality and membership operations on composite types, this applies to any parts that are access types, as these operations are created based on the operations of the components (which triggers the bounded error). For other operations on composite types, the bounded error is not triggered. For instance, an assignment of a composite object with a subcomponent that is a dangling reference has to work normally; no exception can be raised, but the target object will have a subcomponent that is a dangling references, and a (direct) use of that subcomponent is again a bounded error. This is similar to the way that assignments of invalid subcomponents are handled (see 13.9.1).

---

**Erroneous Execution**

Evaluating a name that denotes a nonexistent object, or a protected subprogram or subprogram renaming whose associated object (if any) is nonexistent, is erroneous. The execution of a call to an instance of Unchecked_Deallocation is erroneous if the object was created other than by an allocator for an access type whose pool is Name'Storage_Pool.

**Reason:** The part about a protected subprogram is intended to cover the case of an access-to-protected-subprogram where the associated object has been deallocated. The part about a subprogram renaming is intended to cover the case of a renaming of a prefixed view where the prefix object has been deallocated, or the case of a renaming of an entry or protected subprogram where the associated task or protected object has been deallocated.

**Ramification:** This text does not cover the case of a name that contains a null access value, as null does not denote an object (rather than denoting a nonexistent object).

**Implementation Advice**

For a standard storage pool, Free should actually reclaim the storage.

**Implementation Advice:** For a standard storage pool, an instance of Unchecked_Deallocation should actually reclaim the storage.

**Ramification:** This is not a testable property, since we do not know how much storage is used by a given pool element, nor whether fragmentation can occur.

A call on an instance of Unchecked_Deallocation with a nonnull access value should raise Program_Error if the actual access type of the instance is a type for which the Storage_Size has been specified to be zero or is defined by the language to be zero.

**Implementation Advice:** A call on an instance of Unchecked_Deallocation with a nonnull access value should raise Program_Error if the actual access type of the instance is a type for which the Storage_Size has been specified to be zero or is defined by the language to be zero.

**Discussion:** If the call is not illegal (as in a generic body), we recommend that it raise Program_Error. Since the execution of this call is erroneous (any allocator from the pool will have raised Storage_Error, so the nonnull access value must have been allocated from a different pool or be a stack-allocated object), we can't require any behavior — anything at all would be a legitimate implementation.

**NOTE 1** The rules here that refer to Free apply to any instance of Unchecked_Deallocation.
NOTE 2 Unchecked_Deallocation cannot be instantiated for an access-to-constant type. This is implied by the rules of 12.5.4.

Wording Changes from Ada 95

{AI05-00416-01} The rules for coextensions are clarified (mainly by adding that term). In theory, this reflects no change from Ada 95 (coextensions existed in Ada 95, they just didn't have a name).

Wording Changes from Ada 2005

{AI05-0033-1} Correction: Added a rule that using an access-to-protected-subprogram is erroneous if the associated object no longer exists. It is hard to imagine an alternative meaning here, and this has no effect on correct programs.

{AI05-0107-1} Correction: Moved the requirements on an implementation-generated call to Deallocate to 13.11, in order to put all of the rules associated with implementation-generated calls to Allocate and Deallocate together.

{AI05-0157-1} Correction: Added wording so that calling an instance of Unchecked_Deallocation is treated similarly to allocators for access types where allocators would be banned.

Inconsistencies With Ada 2012

{AI12-0148-1} Corrigendum: Defined a "dangling reference", and specified that a dangling reference might designate some other existing object. This allows simple implementations of access values and reuse of object memory after deallocation. In prior versions of Ada, "=" between a dangling reference and an access to an existing object has to return False, even if the existing object and the object designated by the dangling reference are allocated in the same memory. A program that depended upon that could break with this revised rule. However, as a practical matter, almost all Ada implementations use simple implementations of access types that do not meet that requirement. So such a program would not work (consistently) on most Ada implementations; thus the change shouldn't break any existing programs - it just aligns the Standard with actual practice.

{AI12-0148-1} A side effect of this change is to allow an Ada implementation to detect dangling references in more places. This does not require any Ada implementation to change, and if the implementation does change, it just means that errors will be detected earlier.

Wording Changes from Ada 2012

{AI12-0148-1} Corrigendum: Clarified that deallocated objects cease to exist after finalization but before Deallocate is called. This is necessary to prevent erroneous execution from being triggered by the rules in 13.11 in the time between the end of finalization and the end of the call to the instance of Unchecked_Deallocation.

13.11.3 Default Storage Pools Pragma Controlled

{AI05-0229-1} {AI12-0003-1} [Pragma and aspect Default_Storage_Pool specify the storage pool that will be used in the absence of an explicit specification of a storage pool or storage size for an access type.][Pragma Controlled is used to prevent any automatic reclamation of storage (garbage collection) for the objects created by allocators of a given access type.]

Syntax

{AI05-00190-1} {AI05-0229-1} The form of a pragma Default_Storage_Pool Controlled is as follows:

{AI05-00190-1} {AI05-0229-1} pragma Default_Storage_Pool (storage_pool_indicator); pragma Controlled(first_subtype_local_name);

Discussion: {AI05-0229-1} Not to be confused with type Finalization.Controlled.

{AI05-0190-1} {AI12-0003-1} storage_pool_indicator ::= storage_pool_name | null | Standard

{AI05-0190-1} A pragma Default_Storage_Pool is allowed immediately within the visible part of a packageSpecification, immediately within a declarative_part, or as a configuration pragma.

Name Resolution Rules

{AI05-0190-1} The storage_pool_name is expected to be of type Root_Storage_Pool'Class.
Legality Rules

\{AI05-0190-1\} \{AI05-0229-1\} The _storage pool name_ shall denote a variable. The _first subtype local name_ of a pragma _Controlled_ shall denote a nonderived access subtype.

\{AI12-0003-1\} The _Standard storage pool indicator_ is an identifier specific to a pragma (see 2.8) and does not denote any declaration. If the _storage pool indicator_ is _Standard_, then there shall not be a declaration with _defining identifier_ _Standard_ that is immediately visible at the point of the pragma, other than _package Standard itself_.

**Reason:** We considered having the _Standard storage pool indicator_ resolve to _package Standard_ rather than being an identifier specific to a pragma. That would eliminate the need for a special check. But it would be bizarre to have something that could resolve to either an object or a (single) package, and resolving to _package Standard_ would imply that the standard pool is an object declared in that package. A storage pool object must be a variable (see 13.11), yet preelaborable packages depend on _package Standard_, which would require implementers to implement the standard storage pool with _Prelaborable Initialization_, which is an unnecessary restriction.

No declaration of _Standard_ can ever be use-visible, as the language-defined nonoverloadable definition of _Standard_ will hide any use-visible declarations. Thus we need only concern ourselves with eliminating any possible confusion with regard to immediately visible declarations with the _defining identifier_ _Standard_.

\{AI05-0190-1\} \{AI12-0003-1\} If the _pragma_ is used as a configuration _pragma_, the _storage pool indicator_ shall be either _null_ or _Standard_, and it defines the _default pool_ to be the given _storage pool indicator null_ within all applicable compilation units (see 10.1.5), except within the immediate scope of another _pragma Default Storage Pool_. Otherwise, [the _pragma_ occurs immediately within a sequence of declarations, and] it defines the _default pool_ within the immediate scope of the _pragma_ to be the given _storage pool indicator_ _null_ or the pool denoted by the _storage pool name_, except within the immediate scope of a later pragma _Default Storage Pool_. [Thus, an inner _pragma_ overrides an outer one.]

\{AI05-0190-1\} \{AI05-0262-1\} A _pragma_ _Default Storage Pool_ shall not be used as a configuration _pragma_ that applies to a _compilation unit_ that is within the immediate scope of another _pragma Default Storage Pool_.

**Reason:** This is to prevent confusion in cases like this:

```
package Parent is
  -- _pragma Default Storage Pool(...);
  ...
end Parent;

pragma Default Storage Pool(...); -- Illegal!
package Parent.Child is
  ...
end Parent.Child;
```

where the _Default Storage Pool_ on _Parent.Child_ would not (if it were legal) override the one in _Parent_.

Static Semantics

\{AI05-0190-1\} \{AI05-0229-1\} \{AI12-0003-1\} The language-defined aspect _Default Storage Pool_ may be specified for a generic instance; it defines the _default pool_ for access types within an instance. The _expected type_ for the _Default Storage Pool_ aspect is _Root Storage Pool'Class_. The _aspect definition_ must be a _name_ that denotes a variable. This aspect overrides any _Default Storage Pool_ _pragma_ that might apply to the _generic unit_; if the _aspect_ is not specified, the _default pool_ of the _instance_ is that defined for the _generic unit_. A _pragma Controlled_ is a _representation pragma_ that specifies the _controlled aspect of representation_.

\{AI12-0003-1\} The _Default Storage Pool_ aspect may be specified as _Standard_, which is an _identifier specific to an aspect_ (see 13.1.1) and defines the _default pool_ to be _Standard_. In this case, there shall not be a declaration with _defining identifier_ _Standard_ that is immediately visible at the point of the _aspect specification_, other than _package Standard itself_.

**Reason:**

5.2/5 {AI12-0003-1} {AI12-0445-1} Otherwise, the expected type for the Default Storage Pool aspect is Root Storage.Pool'Class and the aspect definition shall be a name that denotes a variable. This aspect overrides any Default Storage Pool pragma that applies to the generic unit; if the aspect is not specified, the default pool of the instance is that defined for the generic unit.

5.3/4 {AI12-0136-1} The effect of specifying the aspect Default Storage Pool on an instance of a language-defined generic unit is implementation-defined.

5.4/1/4 Implementation defined: The effect of specifying aspect Default Storage Pool on an instance of a language-defined generic unit.

6.1/3, 6.2/4 {AI05-0190-1} {AI05-0229-1} For nonderived access types declared in places where the default pool is defined by the pragma or aspect, their Storage Pool or Storage Size attribute is determined as follows, unless Storage Pool or Storage Size is specified for the type:

- Garbage collection is a process that automatically reclaims storage, or moves objects to a different address, while the objects still exist.
- If the default pool is null, the Storage Size attribute is defined by the language to be zero. [Therefore, an allocator for such a type is illegal.]
- If the default pool is neither null nor Standard, the Storage Pool attribute is that pool.

6.3/4 {AI05-0190-1} {AI12-0003-1} Otherwise (including when the default pool is specified as Standard), there is no default pool; the standard storage pool is used for the type as described in 13.11.

6.6/3 Ramification: {AI05-0190-1} {AI05-0229-1} Default Storage Pool is the only way to specify the storage pool for an anonymous access type; storage reclamation upon leaving a master is not considered garbage collection.

6.b/3 Note that coextensions should be allocated in the same pool (or on the stack) as the outer object (see 13.11); the Storage Pool of the access discriminant (and hence the Default Storage Pool) is supposed to be ignored for coextensions. This matches the required finalization point for coextensions.

6.b.3/1 The default storage pool for an allocator that occurs within an instance of a generic is defined by the Default Storage Pool aspect of the instantiation (if specified), or by the Default Storage Pool pragma that applied to the generic; the Default Storage Pool pragma that applies to the instantiation is irrelevant.

6.b.2/3 It is possible to specify the Default Storage Pool aspect for an instantiation such that allocations will fail. For example, the generic unit might be expecting a pool that supports certain sizes and alignments, and the one on the instance might be more restrictive. It is the programmer's responsibility to get this right.

6.b.3/3 The semantics of the Default Storage Pool aspect are similar to passing a pool object as a generic formal, and putting pragma Default Storage Pool at the top of the generic's visible part, specifying that formal.

6.c/3 Reason: {AI05-0229-1} Programs that will be damaged by automatic storage reclamation are just as likely to be damaged by having objects moved to different locations in memory. A pragma Controlled should turn off both flavors of garbage collection.

6.d/3 Implementation Note: {AI05-0229-1} If garbage collection reclaims the storage of a controlled object, it should first finalize it. Finalization is not done when moving an object; any self-relative pointers will have to be updated by the garbage collector. If an implementation provides garbage collection for a storage pool containing controlled objects (see 7.6), then it should provide a means for deferring garbage collection of those controlled objects.

6.e/3 Reason: {AI05-0229-1} This allows the manager of a resource released by a Finalize operation to defer garbage collection during its critical regions; it is up to the author of the Finalize operation to do so. Garbage collection, at least in some systems, can happen asynchronously with respect to normal user code. Note that it is not enough to defer garbage collection during Initialize, Adjust, and Finalize, because the resource in question might be used in other situations as well. For example:

```ada
with Ada.Finalization;
package P is
  type My_Controlled is new Ada.Finalization.Limited_Controlled with private;
  procedure Finalize(Object : in out My_Controlled);
  type My_Controlled_Access is access My_Controlled;
  procedure Non_Reentrant;
```

### 13.11.3 Default Storage Pools
package body P is
  X : Integer := 0;
  A : array (Integer range 1..10) of Integer;
procedure Non_Reentrant is
  X := X + 1;
  A(X) := ...
end Non_Reentrant;
procedure Finalize (Object : in out My_Controlled) is
  begin
    Non_Reentrant;
  end Finalize;
end P;

with P; use P;
procedure Main is
  begin
   ...
  end Main;

It is the user's responsibility to protect against this sort of thing, and the implementation's responsibility to provide the necessary operations.

We do not give these operations names, nor explain their exact semantics, because different implementations of garbage collection might have different needs, and because garbage collection is not supported by most Ada implementations, so portability is not important here. Another reason not to turn off garbage collection during each entire Finalize operation is that it would create a serial bottleneck; it might be only part of the Finalize operation that conflicts with some other resource. It is the intention that the mechanisms provided be finer-grained than pragma Controlled.

This paragraph was deleted.  

If a pragma Controlled is specified for an access type with a standard storage pool, then garbage collection is not performed for objects in that pool.

Ramification:  
If Controlled is not specified, the implementation may, but need not, perform garbage collection. If Storage_Pool is specified, then a pragma Controlled for that type is ignored.

Reason:  
Controlled means that implementation-provided garbage collection is turned off; if the Storage_Pool is specified, the pool controls whether garbage collection is done.

Implementation Permissions

An object created by an allocator that is passed as the actual parameter to an access parameter may be allocated on the stack, and automatically reclaimed, regardless of the default pool. An implementation need not support garbage collection, in which case, a pragma Controlled has no effect.

Discussion:  
This matches the required finalization point for such an allocated object.

NOTE  
Default Storage Pool can may be used with restrictions No Coextensions and No Access Parameter Allocators (see H.4) to ensure that all allocators use the default pool.

Wording Changes from Ada 83

Ada 83 used the term “automatic storage reclamation” to refer to what is known traditionally as “garbage collection”. Because of the existence of storage pools (see 13.11), we need to distinguish this from the storage reclamation that might happen upon leaving a master. Therefore, we now use the term “garbage collection” in its normal computer-science sense. This has the additional advantage of making our terminology more accessible to people outside the Ada world.
Incompatibilities With Ada 2005

9.b/3 {AI05-0229-1} Pragma Controlled has been dropped from Ada, as it has no effect in any known Ada implementations and it seems to promise capabilities not expected in Ada implementations. This is usually not an incompatibility, as the pragma merely becomes unrecognized (with a warning) and can be implemented as an implementation-defined pragma if desired. However, it is incompatible if it is (now) implemented as an implementation-defined pragma, someone used this pragma in a unit, and they also used restriction No_Implementation_Prags on that unit. In that case, the pragma would now violate the restriction; but use of this pragma (which does nothing) should be very rare, so this is not a significant issue.

Extensions to Ada 2005

9.c/4 {AI05-0190-1} {AI12-0005-1} The pragma Default_Storage_Pool and aspect Default_Storage_Pool are new.

Wording Changes from Ada 2005

9.d/3 {AI05-0229-1} The entire discussion of garbage collection (and especially that of controlled objects) is deleted. Ada 2012 provides subpools (see 13.11.4) for storage management of objects, including controlled objects, a mechanism which is much more predictable than garbage collection. Note that no version of Ada allows early finalization of controlled objects (other than via the use of Unchecked_Deallocation or Unchecked_Deallocate_Subpool), so that garbage collection of such objects would be ineffective in the standard mode anyway.

Extensions to Ada 2012

9.e/4 {AI05-0003-1} Corrigendum: The storage_pool_indicator Standard is new.

Wording Changes from Ada 2012

9.f/4 {AI12-0136-1} Corrigendum: We now explicitly say that the behavior of language-defined generic units when given the Default_Storage_Pool aspect is implementation-defined. Portable code cannot rely on such a package using a particular pool implementation.

13.11.4 Storage Subpools

1/3 {AI05-0111-3} This subclause defines a package to support the partitioning of a storage pool into subpools. A subpool may be specified as the default to be used for allocation from the associated storage pool, or a particular subpool may be specified as part of an allocator (see 4.8).

Static Semantics

2/3 {AI12-0302-1} The following language-defined library package exists:

{AI12-0356-1} {AI12-0399-1} type Root_Storage_Pool_With_Subpools is abstract new Root_Storage_Pool with private

{AI12-0356-1} {AI12-0399-1} type Root_Subpool is abstract tagged limited private

{AI12-0356-1} {AI12-0399-1} type Subpool_Handle is access all Root_Subpool'Class;

{AI05-0252-1} -- The following operations are intended for pool implementers:

{AI12-0356-1} {AI12-0399-1} function Create_Subpool (Pool : in out Root_Storage_Pool_With_Subpools)

{AI12-0356-1} {AI12-0399-1} return not null Subpool_Handle is abstract;

{AI12-0356-1} {AI12-0399-1} procedure Set_Pool_of_Subpool (Subpool : not null Subpool_Handle)

{AI12-0356-1} {AI12-0399-1} return access Root_Storage_Pool_With_Subpools'Class;

{AI12-0302-1} procedure Set_Pool_of_Subpool (Subpool : not null Subpool_Handle;

{AI12-0302-1} To : in out Root_Storage_Pool_With_Subpools'Class)

{AI12-0302-1} with Global => overriding in out Subpool;
{AI12-0302-1}  

procedure Allocate_From_Subpool (  
   Pool : in out Root_Storage_Pool_With_Subpools;  
   Size_In_Storage_Elements : in Storage_Elements.Storage_Count;  
   Alignment : in Storage_Elements.Storage_Count;  
   Subpool : in not null Subpool_Handle) is abstract  
with Pre'Class => Pool of Subpool(Subpool) = Pool'Access,  
       Global => overriding in out Subpool;  

procedure Deallocate_Subpool (  
   Pool : in out Root_Storage_Pool_With_Subpools;  
   Subpool : in out Subpool_Handle) is abstract  
with Pre'Class => Pool of Subpool(Subpool) = Pool'Access;  

{AI05-0298-1}  

function Default_Subpool_for_Pool (  
   Pool : in out Root_Storage_Pool_With_Subpools)  
return not null Subpool_Handle;  

overriding  

procedure Allocate (  
   Pool : in out Root_Storage_Pool_With_Subpools;  
   Size_In_Storage_Elements : in Storage_Elements.Storage_Count;  
   Alignment : in Storage_Elements.Storage_Count);  

overriding  

procedure Deallocate (  
   Pool : in out Root_Storage_Pool_With_Subpools;  
   Size_In_Storage_Elements : in Storage_Elements.Storage_Count;  
   Alignment : in Storage_Elements.Storage_Count) is null;  

{AI05-0298-1}  

overriding  

function Storage_Size (Pool : Root_Storage_Pool_With_Subpools)  
return Storage_Elements.Storage_Count  
is (Storage_Elements.Storage_Count'Last);  

private  
   ... -- not specified by the language  
end System.Storage_Pools.Subpools;  

{AI05-0111-3}  

A subpool is a separately reclaimable portion of a storage pool, identified by an object of type Subpool_Handle (a subpool handle). A subpool handle also identifies the enclosing storage pool, a storage pool that supports subpools, which is a storage pool whose type is descended from Root_Storage_Pool_With_Subpools. A subpool is created by calling Create_Subpool or a similar constructor; the constructor returns the subpool handle.

{AI05-0111-3}  

Each subpool belongs to a single storage pool [[which will always be a pool that supports subpools]]. An access to the pool that a subpool belongs to can be obtained by calling Pool of Subpool with the subpool handle. Set Pool of Subpool causes the subpool of the subpool handle to belong to the given pool; this is intended to be called from subpool constructors like Create_Subpool.] Set Pool of Subpool propagates Program_Error if the subpool already belongs to a pool. If Set Pool of Subpool has not yet been called for a subpool, Pool of Subpool returns null.

Discussion: Pool of Subpool and Set Pool of Subpool are provided by the Ada implementation and typically will not be overridden by the pool implementer.

{AI05-0111-3}  

When an allocator for a type whose storage pool supports subpools is evaluated, a call is made on Allocate From Subpool passing in a Subpool Handle, in addition to the parameters as defined
for calls on Allocate (see 13.11). The subpool designated by the subpool handle name is used, if specified in an allocator. Otherwise, Default Subpool for Pool of the Pool is used to provide a subpool handle. All requirements on the Allocate procedure also apply to Allocate_from_Subpool.

Discussion: Deallocate_Subpool is expected to do whatever is needed to deallocate all of the objects contained in the subpool, it is called from Unchecked_Deallocate_Subpool (see 13.11.5).

Typically, the pool implementer will not override Allocate. In the canonical definition of the language, it will never be called for a pool that supports subpools (there is an Implementation Permission below that allows it to be called in certain rare cases).

**Legality Rules**

\{AI05-0111-3\} If a storage pool that supports subpools is specified as the Storage Pool for an access type, the access type is called a "subpool access type." A subpool access type shall be a pool-specific access type.

\{AI05-0111-3\} \{AI05-0252-1\} The accessibility level of a subpool access type shall not be statically deeper than that of the storage pool object. If the specified storage pool object is a storage pool that supports subpools, then the name that denotes the object shall not denote part of a formal parameter, nor shall it denote part of a dereference of a value of a non-library-level general access type. In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

**Dynamic Semantics**

\{AI05-0111-3\} \{AI05-0252-1\} When an access type with a specified storage pool is frozen (see 13.14), if the tag of the storage pool object identifies a storage pool that supports subpools, the following checks are made:

- the name used to specify the storage pool object does not denote part of a formal parameter nor part of a dereference of a value of a non-library-level general access type; and
- the accessibility level of the access type is not deeper than that of the storage pool object.

\{AI05-0252-1\} Program_Error is raised if either of these checks fail.

**Reason:** This check (and its static counterpart) ensures that the type of the allocated objects exists at least as long as the storage pool object, so that the subpools are finalized (which finalizes any remaining allocated objects) before the type of the objects ceases to exist. The access type itself (and the associated collection) will cease to exist before the storage pool ceases to exist.

We also disallow the use of formal parameters and dereferences of non-library-level general access types when specifying a storage pool object if it supports subpools, because the "apparent" accessibility level is potentially deeper than that of the underlying object. Neither of these cases is very likely to occur in practice.

\{AI05-0111-3\} A call to Subpools.Allocate(P, Addr, Size, Align) does the following:

\{AI05-0111-3\} An allocator that allocates in a subpool raises Program_Error if the allocated object has task parts.

**Reason:** This is to ease implementation. We envision relaxing this restriction in a future version of Ada, once implementation experience has been gained. At this time, we are unable to come up with a set of rules for task termination that is both useful, and surely feasible to implement.

\{AI05-0111-3\} Unless overridden, Default Subpool for Pool propagates Program_Error.
Erroneous Execution

\{AI12-0142-1\} If \texttt{Allocate From Subpool} does not meet one or more of the requirements on the \texttt{Allocate} procedure as given in the Erroneous Execution rules of 13.11, then the program execution is erroneous.

Implementation Permissions

\{AI05-0111-3\} When an allocator for a type whose storage pool is of type \texttt{Root Storage Pool'Class} is evaluated, but supports subpools, the implementation may call \texttt{Allocate} rather than \texttt{Allocate From Subpool}. [This will have the same effect, so long as \texttt{Allocate} has not been overridden.]

\textbf{Reason:} This ensures either of two implementation models are possible for an allocator with no subpool specification. Note that the "supports subpools" property is not known at compile time for a pool of the class-wide type.

- The implementation can dispatch to \texttt{Storage_Pools.Allocate}. If the pool supports subpools, this will call \texttt{Allocate From Subpool} with the default subpool so long as \texttt{Allocate} has not been overridden.
- The implementation can declare \texttt{Allocate From Subpool} as a primitive of \texttt{Root_Storage_Pool} in the private part of Storage Pools. This means that the \texttt{Allocate From Subpool} for \texttt{Root Storage Pool With Subpools} overrides that private one. The implementation can thus call the private one, which will call \texttt{Allocate} for non-subpool-supporting pools. The effect of this implementation does not change if \texttt{Allocate} is overridden for a pool that supports subpools.

\textbf{NOTE 1} \{AI05-0111-3\} \{AI12-0442-1\} \{AI12-0447-1\} A user-defined storage pool type that supports subpools can be implemented by extending the \texttt{Root Storage Pool With Subpools} type, and overriding the primitive subprograms \texttt{Create Subpool}, \texttt{Allocate From Subpool}, and \texttt{Deallocate Subpool}. \texttt{Create Subpool} is expected to call \texttt{Set_Pool_Of_Subpool} before returning the subpool handle. To make use of such a pool, a user can use it to define the Storage Pool attribute of one or more access types, and then invoke \texttt{Create Subpool} to obtain subpool handles associated with the pool.

\textbf{NOTE 2} \{AI05-0111-3\} \{AI12-0440-1\} A user-defined storage pool type that supports subpools can define additional subpool constructors similar to \texttt{Create Subpool} (these typically will have additional parameters).

\textbf{NOTE 3} \{AI05-0111-3\} \{AI12-0442-1\} The pool implementor should override Default Subpool For Pool if they want the pool to support a default subpool for the pool. The implementor can override \texttt{Deallocate} if individual object reclamation is to be supported, and can override \texttt{Storage Size} if there is some limit on the total size of the storage pool. The implementor can override \texttt{Initialize} and \texttt{Finalize} if there is any need for nontrivial initialization and finalization for the pool as a whole. For example, \texttt{Finalize} might reclaim blocks of storage that are allocated over and above the space occupied by the pool object itself. The pool implementor should extend the \texttt{Root Subpool} type as necessary to carry additional information with each subpool provided by \texttt{Create Subpool}.

 Extensions to Ada 2005

\{AI05-0111-3\} \{AI05-0252-1\} Subpools and the package \texttt{System.Storage_Pools.Subpools} are new.

 Wording Changes from Ada 2012

\{AI12-0142-1\} \textbf{Corrigendum:} Clarified that an incorrect implementation of \texttt{Allocate From Subpool} causes execution to become erroneous. The wording already said that the requirements of \texttt{Allocate} apply to \texttt{Allocate From Subpool}, so we’re just confirming the consequences of violating those requirements also apply.

\{AI12-0145-1\} \textbf{Corrigendum:} Clarified that \texttt{Pool Of Subpool} returns \texttt{null} if \texttt{Set Pool Of Subpool} has not been called. As that can be inferred from the definition, and all known existing implementations return \texttt{null} in this case, we document this as a wording change rather than a possible inconsistency.

\subsection*{13.11.5 Subpool Reclamation}

\{AI05-0111-3\} A subpool may be explicitly deallocated using \texttt{Unchecked Deallocate Subpool}.

\textbf{Static Semantics}

\{AI05-0111-3\} The following language-defined library procedure exists:

\begin{verbatim}
with Global => in out all;
\end{verbatim}
### Discussion:

{AI12-0005-1} {AI12-0302-1} The Global specification for this routine needs to account for the dispatching call to the user-defined Deallocate_Subpool routine. We can’t use the Dispatching aspect (see H.7.1) as that requires a statically named object (we have a function call here), so we have to use in out all in order to allow the user-defined subprogram to do anything it needs to do.

{AI05-0111-3} If Subpool is null, a call on Unchecked_Deallocate_Subpool has no effect. Otherwise, the subpool is finalized, and Subpool is set to null.

{AI05-0111-3} {AI12-0331-1} Finalization of a subpool has the following effects in the given order:

1. The subpool no longer belongs to any pool;
2. Any of the objects allocated from the subpool that still exist are finalized in an arbitrary order;
3. {AI12-0148-1} All of the objects allocated from the subpool cease to exist;
4. The following [dispatching] call is then made:
   ```ada```
   ```
   Deallocate_Subpool(Pool_of_Subpool(Subpool).all, Subpool);
   ```
   ```ada```
5. {AI12-0331-1} The subpool ceases to belong to any pool.

{AI05-0111-3} Finalization of a Root_Storage_Pool_With_Subpools object finalizes all subpools that belong to that pool that have not yet been finalized.

#### Extensions to Ada 2005

{AI05-0111-3} Unchecked_Deallocate_Subpool is new.

#### Wording Changes from Ada 2012

{AI12-0148-1} Corrigendum: Added missing wording to state that the objects cease to exist after the completion of finalization. This is formally an inconsistency (it would be possible to depend on the fact that objects finalized by Unchecked_Deallocate_Subpool still exist), but that violates every sane expectation for a procedure called "Deallocate" something.

{AI12-0331-1} Clarified that the steps of deallocating a subpool occur in a specific order. This shouldn’t change any implementation; no implementation is going to finalize deallocated objects or implement Unchecked_Deallocate_Subpool so it is certain to raise Constraint_Error.

### 13.11.6 Storage Subpool Example

#### Examples

{AI05-0111-3} The following example is a simple but complete implementation of the classic Mark/Release pool using subpools:

```ada```
```language-ada
with System.Storage_Pools.Subpools;
with System.Storage_Elements;
with Ada.Unchecked_Deallocate_Subpool;
package MR_Pool is
```
use System.Storage_Pools;
-- For uses of Subpools.
use System.Storage_Elements;
-- For uses of Storage_Count and Storage_Array.
-- Mark and Release work in a stack fashion, and allocations are not allowed
-- from a subpool other than the one at the top of the stack. This is also
-- the default pool.
subtype Subpool_Handle is Subpools.Subpool_Handle;

type Mark_Release_Pool_Type (Pool_Size : Storage_Count) is new
Subpools.Root_Storage_Pool_With_Subpools with private;

function Mark (Pool : in out Mark_Release_Pool_Type)
return not null Subpool_Handle;

procedure Release (Subpool : in out Subpool_Handle)
renames Ada.Unchecked_Deallocate_Subpool;

private

{AI05-0298-1} {AI12-0134-1} subtype MR_Subpool is new Subpools.Root_Subpool with record
Start : Storage_Count;
end record;

subsubtype Subpool_Indexes is Positive range 1 .. 10;
type Subpool_Array is array (Subpool_Indexes) of aliased MR_Subpool;

{AI05-0298-1} {AI05-0298-1} type Mark_Release_Pool_Type (Pool_Size : Storage_Count) is new
Subpools.Root_Storage_Pool_With_Subpools with record
Storage : Storage_Array (0 .. Pool_Size - 1);
Next_Allocation : Storage_Count := 0;
Markers : Subpool_Array;
Current_Pool : Subpool_Indexes := 1;
end record;

{AI05-0298-1} overriding
function Create_Subpool (Pool : in out Mark_Release_Pool_Type)
return not null Subpool_Handle;

function Mark (Pool : in out Mark_Release_Pool_Type)
return not null Subpool_Handle renames Create_Subpool;

overriding
procedure Allocate_From_Subpool (
Pool : in out Mark_Release_Pool_Type;
Storage_Address : out System.Address;
Size_In_Storage_Elements : in Storage_Count;
Alignment : in Storage_Count;
Subpool : not null Subpool_Handle);

overriding
procedure Deallocate_Subpool (
Pool : in out Mark_Release_Pool_Type;
Subpool : in out Subpool_Handle);

{AI05-0298-1} overriding
function Default_Subpool for Pool (Pool : in out Mark_Release_Pool_Type)
return not null Subpool_Handle;

overriding
procedure Initialize (Pool : in out Mark_Release_Pool_Type);
-- We don't need Finalize.
end MR_Pool;

package body MR_Pool is

{AI05-0298-1} use type Subpool_Handle;
procedure Initialize (Pool : in out Mark_Release_Pool_Type) is
  begin
    Pool.Markers(1).Start := 1;
    Subpools.Set_Pool_of_Subpool
      (Pool.Markers(1)'Unchecked_Access, Pool);
  end Initialize;

function Create_Subpool (Pool : in out Mark_Release_Pool_Type)
  return not null Subpool_Handle is
begin
  if Pool.Current_Pool = Subpool_Indexes'Last then
    raise Storage_Error; -- No more subpools.
  end if;

  Result := constant not null Subpool_Handle :=
  do
    Subpools.Set_Pool_of_Subpool (Result, Pool);
  end do;
end Create_Subpool;

procedure Deallocate_Subpool (Pool : in out Mark_Release_Pool_Type;
                              Subpool : in out Subpool_Handle) is
begin
  if Subpool /= Pool.Markers(Pool.Current_Pool)'Unchecked_Access then
    raise Program_Error; -- Only the last marked subpool can be released.
  end if;
  if Pool.Current_Pool /= 1 then
  else
    -- Reinitialize the default subpool:
    Pool.Next_Allocation := 1;
    Subpools.Set_Pool_of_Subpool
      (Pool.Markers(1)'Unchecked_Access, Pool);
  end if;
end Deallocate_Subpool;

function Default_Subpool_for_Pool (Pool : in out Mark_Release_Pool_Type)
  return not null Subpool_Handle is
begin
end Default_Subpool_for_Pool;

procedure Allocate_From_Subpool (Pool : in out Mark_Release_Pool_Type;
                                  Storage_Address : out System.Address;
                                  Size_In_Storage_Elements : in Storage_Count;
                                  Alignment : in Storage_Count;
                                  Subpool : not null Subpool_Handle) is
begin
  if Subpool /= Pool.Markers(Pool.Current_Pool)'Unchecked_Access then
    raise Program_Error; -- Only the last marked subpool can be used for allocations.
  end if;
if Alignment > Pool.Storage'Alignment then
  raise Program_Error;
end if;
-- Check for the maximum supported alignment, which is the alignment of the storage area:

else if Alignment > Pool.Storage'Alignment then
  raise Program_Error; -- Correct the alignment if necessary:
  Pool.Next_Allocation := Pool.Next_Allocation + ((-Pool.Next_Allocation) mod Alignment);
  if Pool.Next_Allocation + Size_In_Storage_Elements > Pool.Pool_Size then
    raise Storage_Error; -- Out of space.
  end if;
  Storage_Address := Pool.Storage (Pool.Next_Allocation)'Address;
  Pool.Next_Allocation := Pool.Next_Allocation + Size_In_Storage_Elements;
end Allocate_From_Subpool;
end MR_Pool;
A restriction may impose requirements on some or all of the units comprising the partition. Unless otherwise specified for a particular restriction, such a requirement applies to all of the units comprising the partition and is enforced via a post-compilation check.

Ramification: In this latter case, there is no post-compilation check needed for the requirement.

For the purpose of checking whether a partition contains constructs that violate any restriction (unless specified otherwise for a particular restriction):

Generic instances are logically expanded at the point of instantiation;

If an object of a type is declared or allocated and not explicitly initialized, then all expressions appearing in the definition for the type and any of its ancestors are presumed to be used;

A default_expression for a formal parameter or a generic formal object is considered to be used if and only if the corresponding actual parameter is not provided in a given call or instantiation.

Implementation Permissions

An implementation may provide implementation-defined restrictions; the identifier for an implementation-defined restriction shall differ from those of the language-defined restrictions.

Implementation defined: Implementation-defined restrictions allowed in a pragma Restrictions.

An implementation may place limitations on the values of the expression that are supported, and limitations on the supported combinations of restrictions. The consequences of violating such limitations are implementation defined.

Implementation defined: The consequences of violating limitations on Restrictions pragmas.

Ramification: Such limitations may be enforced at compile time or at run time. Alternatively, the implementation is allowed to declare violations of the restrictions to be erroneous, and not enforce them at all.

An implementation is permitted to omit restriction checks for code that is recognized at compile time to be unreachable and for which no code is generated.

Whenever enforcement of a restriction is not required prior to execution, an implementation may nevertheless enforce the restriction prior to execution of a partition to which the restriction applies, provided that every execution of the partition would violate the restriction.

The form of a pragma Profile is as follows:

`pragma Profile (profile_identifier, profile pragma_argument_association);`

The profile identifier shall be the name of a usage profile. The semantics of any profile pragma_argument_associations are defined by the usage profile specified by the profile identifier.
13.12 Static Semantics

{AI95-00249-01} {AI05-0246-1} A profile is equivalent to the set of configuration pragmas that is defined for each usage profile.

Post-Compilation Rules

{AI95-00249-01} A pragma Profile is a configuration pragma. There may be more than one pragma Profile for a partition.

Implementation Permissions

{AI05-0269-1} An implementation may provide implementation-defined usage profiles; the identifier for an implementation-defined usage profile shall differ from those of the language-defined usage profiles.

Implementation defined: Implementation-defined usage profiles allowed in a pragma Profile.

NOTE 1 {AI95-00347-01} Restrictions intended to facilitate the construction of efficient tasking run-time systems are defined in D.7. Restrictions intended for use when constructing high integrity systems Safety and security-related restrictions are defined in H.4.

NOTE 2 An implementation has to enforce the restrictions in cases where enforcement is required, even if it chooses not to take advantage of the restrictions in terms of efficiency.

Discussion: It is not the intent that an implementation will support a different run-time system for every possible combination of restrictions. An implementation might support only two run-time systems, and document a set of restrictions that is sufficient to allow use of the more efficient and safe one.

Extensions to Ada 83

Pragma Restrictions is new to Ada 95.

Extensions to Ada 95

{AI95-00249-01} {AI05-0246-1} Pragma Profile is new; it was moved here by Ada 2012 and renamed to a "usage profile" but was otherwise unchanged.

Wording Changes from Ada 95

{8652/0042} {AI95-00130-01} Corrigendum: Corrected the wording so that restrictions are checked inside of generic instantiations and in default expressions. Since not making these checks would violate the purpose of restrictions, we are not documenting this as an incompatibility.

{8652/0043} {AI95-00190-01} Corrigendum: Added a permission that restrictions can be enforced at compile-time. While this is technically incompatible, documenting it as such would be unnecessarily alarming - there should not be any programs depending on the runtime failure of restrictions.

{AI95-00381-01} The syntax of a restriction parameter argument has been defined to better support restriction No Dependence (see 13.12.1).

Wording Changes from Ada 2005

{AI05-0013-1} Correction: When restrictions are checked has been clarified.

13.12.1 Language-Defined Restrictions and Profiles

Language-Defined Restrictions

Static Semantics

{AI95-00257-01} The following restriction identifiers are language defined (additional restrictions are defined in the Specialized Needs Annexes):

{AI05-0241-1} No Implementation Aspect Specifications. There are no implementation-defined aspects specified by an aspect specification. This restriction applies only to the current compilation or environment, not the entire partition.
Discussion: {AI05-0241-1} This restriction (as well as others below) applies only to the current compilation, because it is likely that the runtime (and possibly user-written low-level code) will need to use implementation-defined aspects. But a partition-wide restriction applies everywhere, including the runtime.

{AI95-00257-01} {AI22-0004-1} No Implementation Attributes

There are no implementation-defined attributes. There are no implementation-defined extensions to the definition of any language-defined attribute (see 4.1.4). This restriction applies only to the current compilation or environment, not the entire partition.

Discussion: {AI05-0241-1} This restriction (as well as No Implementation Pragmas) only applies to the current compilation, because it is likely that the runtime (and possibly user-written low-level code) will need to use implementation-defined entities. But a partition-wide restriction applies everywhere, including the runtime.

{AI05-0246-1} {AI05-0269-1} No Implementation Identifiers

There are no usage names that denote declarations with implementation-defined identifiers that occur within language-defined packages or instances of language-defined generic packages. Such identifiers can arise as follows:

- The following language-defined packages and generic packages allow implementation-defined identifiers:
  - package System (see 13.7);
  - package Standard (see A.1);
  - package Ada.Command_Line (see A.15);
  - package Interfaces.C (see B.3);
  - package Interfaces.C.Strings (see B.3.1);
  - package Interfaces.C.Pointers (see B.3.2);
  - package Interfaces.COBOL (see B.4);
  - package Interfaces.Fortran (see B.5);

- The following language-defined packages contain only implementation-defined identifiers:
  - package System.Machine_Code (see 13.8);
  - package Ada.Directories.Information (see A.16);
  - nested Implementation packages of the Queue containers (see A.18.28-31);
  - package Interfaces (see B.2);
  - package Ada.Interrupts.Names (see C.3.2).

For package Standard, Standard.Long_Integer and Standard.Long_Float are considered language-defined identifiers, but identifiers such as Standard.Short.Short_Integer are considered implementation-defined.

This restriction applies only to the current compilation or environment, not the entire partition.

{AI95-00257-01} No Implementation Pragmas There are no implementation-defined pragmas or pragma arguments. This restriction applies only to the current compilation or environment, not the entire partition.

{AI05-0242-1} No Implementation Units

There is no mention in the context clause of any implementation-defined descendants of packages Ada, Interfaces, or System. This restriction applies only to the current compilation or environment, not the entire partition.
No Obsolescent Features

There is no use of language features defined in Annex J. It is implementation defined whether implementation-defined if uses of the renamings of J.1 and of the pragmas of J.15 are detected by this restriction. This restriction applies only to the current compilation or environment, not the entire partition.

Reason: A user could compile a rename like

```ada
with Ada.Text_IO;
package Text_IO renames Ada.Text_IO;
```

Such a rename must not be disallowed by this restriction, nor should the compilation of such a rename be restricted by an implementation. Many implementations implement the renamings of J.1 by compiling them normally; we do not want to require implementations to use a special mechanism to implement these renamings.

The pragmas have the same functionality as the corresponding aspect (unlike the typical obsolescent feature), and rejecting them could be a significant portability problem for existing code.

The following restriction parameter identifiers are language defined:

| No_Dependence | Specifies a library unit on which there are no semantic dependences. |
| No_Specification_of_Aspect | Identifies an aspect for which no aspect specification, attribute definition clause, or pragma is given. |
| No_Use_Of_Attribute | Identifies an attribute for which no attribute reference or attribute definition clause is given. |
| No_Use_Of_Pragma | Identifies a pragma which is not to be used. |
| No_Unrecognized_Aspects | There are no aspect specifications having an unrecognized aspect identifier. This restriction applies only to the current compilation or environment, not the entire partition. |
| No_Unrecognized_Pragmas | There are no pragmas having an unrecognized pragma identifier. This restriction applies only to the current compilation or environment, not the entire partition. |

Legality Rules

The restriction parameter argument of a No_Dependence restriction shall be a name; the name shall have the form of a full expanded name of a library unit, but can be a name that has no corresponding need not denote a unit currently present in the environment.

Ramification: This name is not resolved.

The restriction parameter argument of a No_Specification_of_Aspect restriction shall be an identifier; this is an identifier specific to a pragma (see 2.8) and does not denote any declaration.

Ramification: This restriction parameter argument is not resolved as it is an identifier specific to a pragma. As for No_Dependence, there is no check that the aspect identifier is meaningful; it might refer to an implementation-defined aspect on one implementation, but nothing at all on another implementation.

The restriction parameter argument of a No_Use_Of_Attribute restriction shall be an identifier or one of the reserved words Access, Delta, Digits, Mod, or Range; this is an identifier specific to a pragma.  

Ramification: This restriction parameter argument is not resolved as it is an identifier specific to a pragma.
**13.12.1 Language-Defined Restrictions and Profiles**

7.3/3 **Ramification:** This restriction parameter argument is not resolved as it is an identifier specific to a pragma. There is no check that the attribute identifier refers to a known attribute_designator; it might refer to an implementation-defined attribute on one implementation, but nothing at all on another implementation.

7.3/3 **{AI05-0272-1}** The restriction parameter argument of a No_Use_Of_Pragma restriction shall be an identifier or the reserved word Interface; this is an identifier specific to a pragma.

7.3/3 **Ramification:** This restriction parameter argument is not resolved as it is an identifier specific to a pragma. There is no check that the attribute identifier refers to a known attribute_designator; it might refer to an implementation-defined attribute on one implementation, but nothing at all on another implementation.

---

8/3 **{AI95-00381-01} {AI05-0241-1}** No compilation unit included in the partition shall depend semantically on the library unit identified by the name of a No_Dependence restriction.

8.a/5 **Ramification:** {AI12-0005-1} There is no requirement that the library unit actually exist. One possible use of the pragma is to prevent the use of implementation-defined units; when the program is ported to a different compiler, it is perfectly reasonable that no unit with the name exist.

---

**9/3** **{AI05-0246-1}** The following profile_identifier is language defined:

**9/3** **{AI05-0246-1}** No Implementation Extensions

---

11/3 **{AI05-0246-1}** For usage profile No Implementation Extensions, there shall be no profile pragma_argument_associations.

12/3 **{AI05-0246-1}** The No Implementation Extensions usage profile is equivalent to the following restrictions:

---

13/3 **{AI05-0246-1}** No Implementation Aspect Specifications, No Implementation Attributes, No Implementation Identifiers, No Implementation Pragmas, No Implementation Units.

---

**13.13 Streams**

A stream is a sequence of elements comprising values from possibly different types and allowing sequential access to these values. A stream type is a type in the class whose root type is

---

13.12.1 Language-Defined Restrictions and Profiles
Streams.Root_Stream_Type. A stream type may be implemented in various ways, such as an external sequential file, an internal buffer, or a network channel.

**Discussion:** A stream element will often be the same size as a storage element, but that is not required.

**Term entry:** stream — sequence of elements that can be used, along with the stream-oriented attributes, to support marshalling and unmarshalling of values of most types

**Extensions to Ada 83**

Streams are new in Ada 95.

### 13.13.1 The Streams Subsystem

The abstract type `Root_Stream_Type` is the root type of the class of stream types. The types in this class represent different kinds of streams. A new stream type is defined by extending the root type (or some other stream type), overriding the Read and Write operations, and optionally defining additional primitive subprograms, according to the requirements of the particular kind of stream. The predefined stream-oriented attributes like `T'Read` and `T'Write` make dispatching calls on the Read and Write procedures of the `Root_Stream_Type`. (User-defined `T'Read` and `T'Write` attributes can also make such calls, or can call the Read and Write attributes of other types.)

{AI12-0293-1} The library package `Ada.Streams` has the following declaration:

```ada
package Ada.Streams is
  with pragma Pure, Nonblocking => False is (Streams);

  type Root_Stream_Type is abstract tagged limited private;
  with pragma Preelaborable_Initialization(Root_Stream_Type);

  type Stream_Element is mod implementation-defined;
  subtype Stream_Element_Offset is range implementation-defined;
  type Stream_Element_Count is Stream_Element_Offset range 0..Stream_Element_Offset'Last;
  type Stream_Element_Array is array(Stream_Element_Offset range <>) of aliased Stream_Element;

  procedure Read(
    Stream : in out Root_Stream_Type;
    Item   : out Stream_Element_Array;
    Last   : out Stream_Element_Offset) is abstract;

  procedure Write(
    Stream : in out Root_Stream_Type;
    Item   : in Stream_Element_Array) is abstract;

  private
    ... -- not specified by the language
end Ada.Streams;
```

**Reason:** {AI12-0241-1} This package must allow blocking (Nonblocking => False) for compatibility. The purpose of this package is to provide a template for overriding user-defined routines; and such routines can only allow blocking if the root type does so. Users can still declare their overriding routines nonblocking if they wish.

{AI95-00181-01} The Read operation transfers `Item'Length` stream elements from the specified stream to fill the array `Item`. Elements are transferred until `Item'Length` elements have been transferred, or until the end of the stream is reached. If any elements are transferred, the index of the last stream element transferred is returned in `Last`. Otherwise, `Item'First - 1` is returned in `Last`. `Last` is less than `Item'Last` only if the end of the stream is reached.

The Write operation appends `Item` to the specified stream.
Discussion: \{AI95-00114-01\} The index subtype of Stream Element Array is Stream Element Offset because we wish to allow maximum flexibility. Most Stream Element Arrays will probably have a lower bound of 0 or 1, but other lower bounds, including negative ones, make sense in some situations.

\{AI95-00114-01\} \{AI05-0005-1\} Note that there are some language-defined subprograms that fill part of a Stream Element Array, and return the index of the last element filled as a Stream Element Offset. The Read procedures declared here, Streams.Stream.IO (see A.12.1), and System.RPC (see E.5) behave in this manner. These will raise Constraint_Error if the resulting Last value is not in Stream Element Offset. This implies that the Stream Element Array passed to these subprograms should not have a lower bound of Stream Element Offset'First, because then a read of 0 elements would always raise Constraint_Error. A better choice of lower bound is 0 or 1.

\{AI12-0293-1\} Three additional packages provide stream implementations that do not make use of any file operations. These packages provide the same operations, with Streams.Storage providing an abstract interface, and two child packages providing implementations of that interface. The difference is that for Streams.Storage.Bounded, the maximum storage is bounded.

\{AI12-0293-1\} The library package Ada.Streams.Storage has the following declaration:

```ada
package Ada.Streams.Storage
with Pure, Nonblocking is
  type Storage_Stream_Type is abstract new Root_Stream_Type with private;
  function Element_Count (Stream : Storage_Stream_Type) return Stream_Element_Count is abstract;
  procedure Clear (Stream : in out Storage_Stream_Type) is abstract;
private
  ... -- not specified by the language end Ada.Streams.Storage;
```

\{AI12-0293-1\} The library package Ada.Streams.Storage.Unbounded has the following declaration:

```ada
package Ada.Streams.Storage.Unbounded
with Prelaborated, Nonblocking, Global => in out synchronized is
  type Stream_Type is new Storage_Stream_Type with private with Default_Initial_Condition => Element_Count (Stream_Type) = 0;
  overriding procedure Read (Stream : in out Stream_Type;
  Item   : out Stream_Element_Array;
  Last   : out Stream_Element_Offset)
with Post =>
    (declare
      Num_Read : constant Stream_Element_Count :=
        Stream_Element_Count'Min (Element_Count(Stream)'Old, Item'Length);
    begin
      Last = Num_Read + Item'First - 1 and
      Element_Count (Stream) =
        Element_Count (Stream)'Old - Num_Read);
```

Discussion: Num_Read is the number of elements read; this is the minimum of Item'Length and the number of available elements. Last then is determined by that, and the Element_Count decreases by the number of elements read.

```ada
  overriding procedure Write (Stream : in out Stream_Type;
  Item   : in Stream_Element_Array)
with Post =>
    Element_Count (Stream) =
      Element_Count (Stream)'Old + Item'Length;
```

```ada
  overriding function Element_Count (Stream : Stream_Type) return Stream_Element_Count;
```
```ada
overriding
procedure Clear (Stream : in out Stream_Type)
with Post => Element_Count (Stream) = 0;
private
... -- not specified by the language
end Ada.Streams.Storage.Unbounded;

{AI12-0293-1} The library package Ada.Streams.Storage.Bounded has the following declaration:

```ada
package Ada.Streams.Storage.Bounded
with Pure, Nonblocking is
  type Stream_Type (Max_Elements : Stream_Element_Count)
    is new Storage.Stream_Type with private
    with Default_Initial_Condition =>
      Element_Count (Stream_Type) = 0;
overriding
procedure Read (
  Stream : in out Stream_Type;
  Item   : out Stream_Element_Array;
  Last   : out Stream_Element_Offset)
with Post =>
  declare
    Num_Read : constant Stream_Element_Count :=
      Stream_Element_Count'Min
        (Element_Count(Stream)'Old, Item'Length);
  begin
    Last = Num_Read + Item'First - 1 and
    Element_Count (Stream) =
      Element_Count (Stream)'Old - Num_Read;
overriding
procedure Write (
  Stream : in out Stream_Type;
  Item   : in Stream_Element_Array)
with Pre =>
  Element_Count (Stream) + Item'Length <= Stream.Max_Elements
or else raise Constraint_Error),
Post =>
  Element_Count (Stream) =
  Element_Count (Stream)'Old + Item'Length;
overriding
function Element_Count (Stream : Stream_Type)
  return Stream_Element_Count
with Post => Element_Count'Result <= Stream.Max_Elements;
overriding
procedure Clear (Stream : in out Stream_Type)
with Post => Element_Count (Stream) = 0;
private
... -- not specified by the language
end Ada.Streams.Storage.Bounded;

{AI12-0293-1} The Element_Count functions return the number of stream elements that are available for reading from the given stream.

{AI12-0293-1} The Read and Write procedures behave as described for package Ada.Streams above. Stream elements are read in FIFO (first-in, first-out) order; stream elements are available for reading immediately after they are written.

{AI12-0293-1} The Clear procedures remove any available stream elements from the given stream.

Implementation Permissions

{8652/0044} {AI95-00181-01} {AI12-0444-1} If Stream_Element_Size is not a multiple of System.Storage_Unit, then the components of Stream_Element_Array will need not be aliased.
Ramification: {AI95-00114-01} If the Stream Element'Size is less than the size of System.Storage.Unit, then components of Stream Element Array need not be aliased. This is necessary as the components of type Stream Element size might not be addressable on the target architecture.

Implementation Advice

Implementation Advice: Streams.Storage.Bounded.Stream_Type objects should be implemented without implicit pointers or dynamic allocation.

Reason: The Streams.Storage.Bounded package is provided in order to make available an alternative to the Streams.Storage.Unbounded package which gives more predictable memory usage.

NOTE 1 See A.12.1, “The Package Streams.Stream_IO” for an example of extending type Root_Stream_Type.

NOTE 2 {AI95-00227-01} If the end of stream has been reached, and Item'First is Stream_Element_Offset'First, Read will raise Constraint_Error.

Ramification: Thus, Stream_Element_Arrays should start at 0 or 1, not Stream_Element_Offset'First.

Extensions to Ada 95

Amendment Correction: Added pragma Preelaborable. Initialization to type Root_Stream_Type.

Wording Changes from Ada 95

Corrigendum: Stream elements are aliased presuming that makes sense.

Fixed the wording for Read to properly define the result in Last when no stream elements are transferred.

Extensions to Ada 2012

Package Ada.Streams.Storage and its children are new.

13.13.2 Stream-Oriented Attributes

The type-related operational attributes Write, Read, Output, and Input attributes convert values to a stream of elements and reconstruct values from a stream.

Static Semantics

For every subtype S of an elementary type T, the following representation attribute is defined:

S'Stream_Size

Denotes the number of bits read from or written to a stream by the default implementations of S'Write and S'Read occupied in a stream by items of subtype S. Hence, the number of stream elements required per item of elementary type T is:

T'Stream_Size / Ada.Streams.Stream_Element'Size

The value of this attribute is of type universal_integer and is a multiple of Stream_Element'Size.

Stream Size may be specified for first subtypes via an attribute definition clause; the expression of such a clause shall be static, nonnegative, and a multiple of Stream_Element'Size.

Aspect Description for Stream Size: Size in bits used to represent elementary objects in a stream.

Discussion: Stream Size is a type-related attribute (see 13.1).

Ramification: {AI05-0194-1} The value of S'Stream_Size is unaffected by the presence or absence of any attribute definition clauses or aspect specifications specifying the Read or Write attributes of any ancestor of S. S'Stream Size is defined in terms of the behavior of the default implementations of S'Read and S'Write even if those default implementations are overridden.
If not specified, the value of Stream_Size for an elementary type should be the number of bits that corresponds to the minimum number of stream elements required by the first subtype of the type, rounded up to the nearest factor or multiple of the word size that is also a multiple of the stream element size.

**Implementation Advice:** If not specified, the value of Stream_Size for an elementary type should be the number of bits that corresponds to the minimum number of stream elements required by the first subtype of the type, rounded up to the nearest factor or multiple of the word size that is also a multiple of the stream element size.

**Reason:** [AI95-00270-01] This is Implementation Advice because we want to allow implementations to remain compatible with their Ada 95 implementations, which may have a different handling of the number of stream elements. Users can always specify Stream_Size if they need a specific number of stream elements.

The recommended level of support for the Stream_Size attribute is:

- **AI95-00270-01** A Stream_Size clause should be supported for a discrete or fixed point type T if the specified Stream_Size is a multiple of Stream_Element'Size and is no less than the size of the first subtype of T, and no greater than the size of the largest type of the same elementary class (signed integer, modular integer, enumeration, ordinary fixed point, or decimal fixed point).

**Implementation Advice:** The recommended level of support for the Stream_Size attribute should be followed.

**Ramification:** There are no requirements beyond supporting confirming Stream_Size clauses for floating point and access types. Floating point and access types usually only have a handful of defined formats, streaming anything else makes no sense for them.

For discrete and fixed point types, this may require support for sizes other than the “natural” ones. For instance, on a typical machine with 32-bit integers and a Stream_Element'Size of 8, setting Stream_Size to 24 must be supported. This is required as such formats can be useful for interoperability with unusual machines, and there is no difficulty with the implementation (drop extra bits on output, sign extend on input).

For every subtype S of a specific type T, the following attributes are defined.

**S'Write**

S'Write denotes a procedure with the following specification:

```
{AI95-00441-01} procedure S'Write(
  Stream : not null access Ada.Streams.Root_Stream_Type'Class;
  Item : in T)
```

S'Write writes the value of Item to Stream.

**S'Read**

S'Read denotes a procedure with the following specification:

```
{AI95-00441-01} procedure S'Read(
  Stream : not null access Ada.Streams.Root_Stream_Type'Class;
  Item : out T)
```

S'Read reads the value of Item from Stream.

This paragraph was deleted. For an untagged derived type T types, the Write (resp. Read) attribute is attributes are inherited according to the rules given as specified in 13.1 if the attribute is [specified and'] available for the parent type at the point where T is declared. For a tagged derived type, these attributes are not inherited, but rather, otherwise, the default implementations of these attributes are used. The default implementations of Write and Read attributes execute as follows:

**Proof:** [AI05-0192-1] [AI12-0419-1] The inheritance rules of 13.1 say that only specified or inherited aspects are inherited; we mention it again here as a clarification.

**AI95-00444-01** The default implementations of the Write and Read attributes, where available, execute as follows:

- **AI95-00040** [AI95-00108-01] [AI95-00444-01] [AI05-0192-1] [AI12-0419-1] For nonderived elementary types, Read reads (and Write writes) the...
number of stream elements implied by the Stream_Size for the type \( T \); the representation in terms of those stream elements is implementation defined. For nonderived composite types, the Write or Read attribute for each component (excluding those, if any, that are not components of the nominal type of the object) is called in a canonical order, which The canonical order of components is last dimension varying fastest for an array (unless the convention of the array is Fortran, in which case it is first dimension varying fastest), and positional aggregate order for a record. Bounds are not included in the stream if \( T \) is an array type. If \( T \) is a discriminated type, discriminants are included only if they have defaults. If \( T \) is a tagged type, the tag is not included. For type extensions, the Write or Read attribute for the parent type is called, followed by the Write or Read attribute of each component of the extension part, in canonical order. For a limited type extension, if the attribute of the parent or any progenitor type of \( T \) is available anywhere within the immediate scope of \( T \) has been directly specified and the attribute of the parent or any ancestor type of the type of any of the extension components is not available at the freezing point of \( T \), then which are of a limited type has not been specified, the attribute of \( T \) shall be directly specified.

Implementation defined: The contents of the stream elements read and written representation used by the Read and Write attributes of elementary types in terms of stream elements.

\[\{\text{AI12-0419-1}\}\]

For type extensions, the Write or Read attribute for the parent type is called, followed by the Write or Read attribute of each component of the extension part, in canonical order. For a limited type extension, if the attribute of the parent type or any progenitor type of \( T \) is available anywhere within the immediate scope of \( T \), and the attribute of the parent type or the type of any of the extension components is not available at the freezing point of \( T \), then the attribute of \( T \) shall be directly specified. For untagged derived types, the Write (resp. Read) attribute invokes the corresponding attribute of the parent type, if the attribute is available for the parent type.

Implementation Note: \[\{\text{AI12-0419-1}\}\] The default implementation of a stream-oriented attribute might not be well-defined in cases where the attribute is never available anywhere in the scope of the type. In such cases, the attribute cannot be called and is defined (far below) to raise Program_Error.

\[\{\text{AI05-0023-1}\}\] \[\{\text{AI05-0264-1}\}\] \[\{\text{AI12-0419-1}\}\] If \( T \) is a discriminated type and its discriminants have defaults, then S'Read first reads the discriminants from the stream without modifying Item. S'Read then creates an object of type \( T \) constrained by these discriminants. The value of this object is then converted to the subtype of Item and is assigned to Item. Finally, the Read attribute for each nondiscriminant component of Item is called in canonical order as described above. Normal default initialization and finalization take place for the created object.

Reason: A discriminant with a default value is treated simply as a component of the object. On the other hand, an array bound or a discriminant without a default value, is treated as “descriptor” or “dope” that must be provided in order to create the object and thus is logically separate from the regular components. Such “descriptor” data are written by 'Output and produced as part of the delivered result by the 'Input function, but they are not written by 'Write nor read by 'Read. A tag is like a discriminant without a default.

\[\{\text{AI95-00108-01}\}\] \[\{\text{AI95-00195-01}\}\] For limited type extensions, we must have a definition of 'Read and 'Write if the parent type has one, as it is possible to make a dispatching call through the attributes. The rule is designed to automatically do the right thing in as many cases as possible.

\[\{\text{AI95-00251-01}\}\] Similarly, a type that has a progenitor with an available attribute must also have that attribute, for the same reason.

\[\{\text{AI05-0023-1}\}\] The semantics of S'Read for a discriminated type with defaults involves an anonymous object so that the point of required initialization and finalization is well-defined, especially for objects that change shape and have controlled components. The creation of this anonymous object often can be omitted (see the Implementation Permissions below).

Ramification: \[\{\text{AI95-00195-01}\}\] For a composite object, the subprogram denoted by the Write or Read attribute of each component is called, whether it is the default or is user-specified. Implementations are allowed to optimize these calls (see below), presuming the properties of the attributes are preserved.

\[\{\text{AI95-00270-01}\}\] \[\{\text{AI05-0264-1}\}\] \[\{\text{AI12-0419-1}\}\] Constraint Error is raised by the predefined Write attribute if the value of the elementary item is outside the range of values representable using Stream_Size.
For a signed integer type, an enumeration type, or a fixed point type, the range is unsigned only if the integer code for the lower bound of the first subtype is nonnegative, and a (symmetric) signed range that covers all values of the first subtype would require more than Stream_Size bits; otherwise, the range is signed.

For every subtype S'Class of a class-wide type T'Class:

S'Class'Write

S'Class'Write denotes a procedure with the following specification:

```ada
procedure S'Class'Write(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class;
    Item   : in T'Class)
```

Dispatches to the subprogram denoted by the Write attribute of the specific type identified by the tag of Item.

S'Class'Read

S'Class'Read denotes a procedure with the following specification:

```ada
procedure S'Class'Read(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class;
    Item   : out T'Class)
```

Dispatches to the subprogram denoted by the Read attribute of the specific type identified by the tag of Item.

Reason: It is necessary to have class-wide versions of Read and Write in order to avoid generic contract model violations; in a generic, we don't necessarily know at compile time whether a given type is specific or class-wide.

Implementation Advice

{AI95-00270-01} If a stream element is the same size as a storage element, then the normal in-memory representation should be used by Read and Write for scalar objects. Otherwise, Read and Write should use the smallest number of stream elements needed to represent all values in the base range of the scalar type.

Paragraph 17 was deleted.

Static Semantics

For every subtype S of a specific type T, the following attributes are defined.

S'Output

S'Output denotes a procedure with the following specification:

```ada
procedure S'Output(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class;
    Item   : in T)
```

S'Output writes the value of Item to Stream, including any bounds or discriminants.

Ramification: Note that the bounds are included even for an array type whose first subtype is constrained.

S'Input

S'Input denotes a function with the following specification:

```ada
function S'Input(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class)
```

S'Input reads and returns one value from Stream, using any bounds or discriminants written by a corresponding S'Output to determine how much to read.

{8652/0040} {AI95-00108-01} {AI95-00444-01} {AI05-0192-1} {AI12-0419-1} For an untagged derived type T, types, the default implementation of the Output (resp. and Input) attribute is attributes of the parent type are invokes the corresponding attribute of the parent type inherited according to the rules given as specified in 13.1 if the attribute is [specified and] available for the parent type at the point where T is declared. For any other type a tagged derived type, these attributes are not inherited, but rather...
otherwise, the default implementations of these attributes of the Output and Input attributes, where
available, execute as follows. The default implementations of Output and Input attributes execute
as follows. Unless overridden by an attribute_definition_clause, these subprograms execute as follows:

**Proof:** [AI05-0109-1] [AI12-0419-1] See the note following the inheritance rules for the Write attribute, above.

25.13.2 Stream-Oriented Attributes

25.13.2.1 The default implementations of the Output and Input attributes, where
available, execute as follows:

- **[AI05-0269-1]** If `T` is an array type, S'Output first writes the bounds, and S'Input first reads the
  bounds. If `T` has discriminants without defaults, S'Output first writes the discriminants (using the
  Write attribute of the discriminant type S'Write for each), and S'Input first reads the discriminants
  (using the Read attribute of the discriminant type S'Read for each).

- **[AI95-00195-01] [AI05-0023-1]** S'Output then calls S'Write to write the value of Item to the
  stream. S'Input then creates an object of type `T`, (with the bounds or (when without defaults) the
  discriminants, if any, taken from the stream), passes it to S'Read, and returns the
  value of the object. If `T` has discriminants, then this object is unconstrained if and only the
discriminants have defaults. Normal default initialization and finalization take place for this
object (see 3.3.1, 7.6, and 7.6.1).

- **[AI95-00251-01]** If `T` is an abstract type, then S'Input is an abstract function.

**Ramification:** For an abstract type `T`, S'Input can be called in a dispatching call, or passed to an abstract formal
subprogram. But it cannot be used in nondispatching contexts, because we don't allow objects of abstract types to exist.
The designation of this function as abstract has no impact on descendants of `T`, as T'Input is not inherited for tagged
types, but rather recreated (and the default implementation of T'Input calls T'Read, not the parent type's T'Input). Note
that T'Input cannot be specified in this case, as any function with the proper profile is necessarily abstract, and
specifying abstract subprograms in an attribute_definition_clause is illegal.

For every subtype S'Class of a class-wide type T'Class:

S'Class'Output denotes a procedure with the following specification:

- **[AI95-00441-01]** procedure S'Class'Output(
  Stream : not null access Ada.Streams.Root_Stream_Type'Class;
  Item : in T'Class)

  **[AI95-00344-01]** First writes the external tag of Item to Stream (by calling
  String'Output(Stream, Tags.External_Tag(Item'Tag)) — see 3.9) and then dispatches to the
  subprogram denoted by the Output attribute of the specific type identified by the tag. Tag_Error is raised if the tag of Item identifies a type declared at an accessibility level deeper
  than that of S.

  **Reason:** [AI95-00344-01] We raise Tag_Error here for nested types as such a type cannot be successfully read with
  S'Class'Input, and it doesn't make sense to allow writing a value that cannot be read.

S'Class'Input denotes a function with the following specification:

- **[AI95-00441-01]** function S'Class'Input(
  Stream : not null access Ada.Streams.Root_Stream_Type'Class)

  return T'Class

  **[AI95-00279-01] [AI95-00344-01] [AI05-0109-1] [AI12-0439-1]** First reads the external
tag from Stream and determines the corresponding internal tag (by calling
Tags.Descendant_Tag(Stream, Item'Tag) which
  can raise Tag_Error — see 3.9) and then dispatches to the subprogram denoted by the Input attribute of the
  specific type identified by the internal tag; returns that result. If the specific type
  identified by the internal tag is not covered by T'Class or is abstract, Constraint_Error is
  raised.

  **Ramification:** [AI05-0109-1] Descendant_Tag will ensure that the tag it returns is covered by T'Class; Tag_Error will be raised if it would not cover T'Class.

---

13.13.2 Stream-Oriented Attributes
In the default implementation of Read and Input for a composite type, for each scalar component that is a discriminant or that has an implicit initial value whose component_declaration includes a default_expression, a check is made that the value returned by Read for the component belongs to its subtype. Constraint_Error is raised if this check fails. For other scalar components, no check is made. For each component that is of an access type, if the implementation can detect that the value returned by Read for the component is not a value of its subtype, Constraint_Error is raised. If the value is not a value of its subtype and this error is not detected, the component has an abnormal value, and erroneous execution can result (see 13.9.1). In the default implementation of Read for a composite type with defaulted discriminants, if the actual parameter of Read is constrained, a check is made that the discriminants read from the stream are equal to those of the actual parameter. Constraint_Error is raised if this check fails.

Reason: The check for scalar components that have an implicit initial value is to preserve our Language Design Principle that all objects that have an implicit initial value do not become "deinitialized".

Ramification: A scalar component can have an implicit initial value if it has a default_expression, if the component's type has the Default_Value aspect specified, or if the component is that of an array type that has the Default_Component_Value aspect specified.

To be honest: An implementation should always be able to detect the error for a null value read into a component of an access subtype with a null exclusion; the "if the implementation can detect" is intended to cover nonnull access values.

It is unspecified at which point and in which order these checks are performed. In particular, if Constraint_Error is raised due to the failure of one of these checks, it is unspecified how many stream elements have been read from the stream.

In the default implementation of Read and Input for a type, End_Error is raised if the end of the stream is reached before the reading of a value of the type is completed.

The Nonblocking aspect is statically True and the Global aspect is null for the default implementations of stream-oriented attributes for elementary types. For the default implementations of stream-oriented attributes for composite types, the value of the Nonblocking aspect is that of the first subtype, and the Global aspect defaults to that of the first subtype. A default implementation of a stream-oriented attribute that has the Nonblocking aspect statically True is considered a nonblocking region. The aspect Dispatching (see H.7.1) is Read(Stream) for the default implementations of the stream-oriented attributes Read, Read'Class, Input, and Input'Class; the aspect Dispatching is Write(Stream) for the default implementations of the stream-oriented attributes Write, Write'Class, Output, and Output'Class.

Ramification: If the default implementation of a stream-oriented attribute A for a composite type would call other stream-oriented attribute(s) whose Global aspect was not allowed by the Global aspect of A, then the Legality Rules of 6.1.2 are violated and the type declaration is illegal. If the stream-oriented attribute A is overridden, then the default implementation is not created and this check is not made. A similar ramification applies to the Nonblocking aspect of default implementation of a stream-oriented attribute.

The stream-oriented attributes may be specified for any type via an attribute_definition_clause. [Alternatively, each of the specific stream-oriented attributes may be specified using an aspect specification on any type declaration, with the aspect name being the corresponding attribute name.] Each of the class-wide stream-oriented attributes may be specified using an aspect specification for a tagged type T using the name of the stream-oriented attribute followed by 'Class; such class-wide aspects do not apply to other descendants of T. If not directly specified, a default implementation of a stream-oriented attribute is implicitly composed for a nonlimited type, and for certain limited types, as defined above. The subprogram name given in such a clause shall statically denote a subprogram that is not a denotable abstract subprogram. Furthermore, if a stream-oriented attribute is specified for an interface type by an attribute_definition_clause, the subprogram name given in the.
clause shall statically denote a null procedure. All nonlimited types have default implementations for these operations. An attribute_reference for one of these attributes is illegal if the type is limited, unless the attribute has been specified by an attribute_definition_clause or [(for a type extension)] the attribute has been specified for an ancestor type. For an attribute_definition_clause specifying one of these attributes, the subtype of the Item parameter shall be the base subtype if scalar, and the first subtype otherwise. The same rule applies to the result of the Input function.

38.a.1/2

This paragraph was deleted. Discussion: [8652/0040] {AI95-00108-01} {AI95-00195-01} "Specified" includes inherited attributes, and default implementations are never inherited. So, for untagged limited types, the second part of the attribute_reference rule has the same meaning as the first part. However, tagged types never inherit attributes, so the second rule is needed so that the default implementations for the attributes can be called when those are constructed from a directly specified ancestor.

Proof: {AI12-0121-1} 13.1.1 says that all operational attributes can be specified with an aspect specification.

38.a.2/4

Aspect Description for Read’Class: Procedure to read a value from a stream for the class-wide type associated with a given type.

38.a.3/4

Aspect Description for Write’Class: Procedure to write a value to a stream for the class-wide type associated with a given type.

38.a.5/4

Aspect Description for Input’Class: Function to read a value from a stream for the class-wide type associated with a given type, including any bounds and discriminants.

38.a.6/4

Aspect Description for Output’Class: Procedure to write a value to a stream for the class-wide type associated with a given type, including any bounds and discriminants.

38.1/4

{AI12-0121-1} The subprogram name given in such an attribute_definition_clause or aspect_specification shall statically denote a subprogram that is not an abstract subprogram. Furthermore, if a specific stream-oriented attribute is specified for an interface type, the subprogram name given in the attribute_definition_clause or aspect_specification shall statically denote a null procedure.

38.b/2

Discussion: [AI95-00251-01] Stream attributes (other than Input) are always null procedures for interface types (they have no components). We need to allow explicit setting of the Read and Write attributes in order that the class-wide attributes like Int’Class’Input can be made available. (In that case, any descendant of the interface type would require available attributes.) But we don’t allow any concrete implementation because these don’t participate in extensions (unless the interface is the parent type). If we didn’t ban concrete implementations, the order of declaration of a pair of interfaces would become significant. For example, if Int1 and Int2 are interfaces with concrete implementations of ‘Read, then the following declarations would have different implementations for ‘Read:

```ada
type Con1 is new Int1 and Int2 with null record;
type Con2 is new Int2 and Int1 with null record;
```

This would violate our design principle that the order of the specification of the interfaces in a derived_type_definition doesn’t matter.

38.c/2

Ramification: The Input attribute cannot be specified for an interface. As it is a function, a null procedure is impossible; a concrete function is not possible anyway as any function returning an abstract type must be abstract. And we don’t allow specifying stream attributes to be abstract subprograms. This has no impact, as the availability of Int’Class’Input (where Int is a limited interface) depends on whether Int’Read (not Int’Input) is specified. There is no reason to allow Int’Output to be specified, either, but there is equally no reason to disallow it, so we don’t have a special rule for that.

38.d/2

Discussion: {AI95-00195-01} Limited types generally do not have default implementations of the stream-oriented attributes. The rules defining when a stream-oriented attribute is available (see below) determine when an attribute of a limited type is in fact well defined and usable. The rules are designed to maximize the number of cases in which the attributes are usable. For instance, when the language provides a default implementation of an attribute for a limited type based on a specified attribute for the parent type, we want to be able to call that attribute.

38.e/2

Discussion: [AI95-000195-01] Limited types generally do not have default implementations of the stream-oriented attributes. The rules defining when a stream-oriented attribute is available (see below) determine when an attribute of a limited type is in fact well defined and usable. The rules are designed to maximize the number of cases in which the attributes are usable. For instance, when the language provides a default implementation of an attribute for a limited type based on a specified attribute for the parent type, we want to be able to call that attribute.

38.f/2

Aspect Description for Read: Procedure to read a value from a stream for a given type.

38.g/3

Aspect Description for Write: Procedure to write a value to a stream for a given type.

38.h/3

Aspect Description for Input: Function to read a value from a stream for a given type, including any bounds and discriminants.

38.i/3

Aspect Description for Output: Procedure to write a value to a stream for a given type, including any bounds and discriminants.
A stream-oriented attribute for a subtype of a specific type \( T \) is available at places where one of the following conditions is true:

- \( T \) is nonlimited.
- The attribute designator is Read (resp. Write) and \( T \) is a limited record extension, and the attribute Read (resp. Write) is available for the parent type of \( T \) and for the types of all of the extension components.
  
  **Reason:** In this case, the language provides a well-defined default implementation, which we want to be able to call.

- \{AI12-0419-1\} \( T \) is a limited untagged derived type, and the attribute is available as inherited for the parent type.
  
  **Reason:** {AI12-0419-1} Again, the language provides a default implementation, which Attributes are only inherited for untagged derived types, and surely we want to be able to call inherited attributes.

- The attribute designator is Input (resp. Output), and \( T \) is a limited type, and the attribute Read (resp. Write) is available for \( T \).
  
  **Reason:** The default implementation of Input and Output are based on Read and Write; so if the implementation of Read or Write is good, so is the matching implementation of Input or Output.

- \{AI12-0419-1\} The attribute has been specified via an attribute definition clause or aspect specification, and the attribute definition clause or aspect specification is visible.
  
  **Reason:** We always want to allow calling a specified attribute. But we don't want availability to break privacy. Therefore, only attributes whose specification can be seen count. Yes, we defined the visibility of an attribute definition clause (see 8.3).

A stream-oriented attribute for a subtype of a class-wide type \( T \)Class is available at places where one of the following conditions is true:

- \( T \) is nonlimited;
- \{AI12-0419-1\} the attribute has been specified via an attribute definition clause or aspect specification, and the attribute definition clause or aspect specification is visible; or
- the corresponding attribute of \( T \) is available, provided that if \( T \) has a partial view, the corresponding attribute is available at the end of the visible part where \( T \) is declared.
  
  **Reason:** The rules are stricter for class-wide attributes because (for the default implementation) we must ensure that any specific attribute that might ever be dispatched to is available. Because we require specification of attributes for extensions of limited parent types with available attributes, we can in fact know this. Otherwise, we would not be able to use default class-wide attributes with limited types, a significant limitation.

An attribute reference for one of the stream-oriented attributes is illegal unless the attribute is available at the place of the attribute reference. Furthermore, an attribute reference for \( T \)Input is illegal if \( T \) is an abstract type. In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

**Discussion:** Stream attributes always exist. It is illegal to call them in some cases. Having the attributes not be defined for some limited types would seem to be a cleaner solution, but it would lead to contract model problems for limited private types.

\( T \)Input is available for abstract types so that \( T \)Class'Input is available. But we certainly don't want to allow calls that could create an object of an abstract type. Remember that \( T \)Class is never abstract, so the above legality rule doesn't apply to it. We don't have to discuss whether the attribute is specified, as it cannot be: any function returning the type would have to be abstract, and we do not allow specifying an attribute with an abstract subprogram.

**To be honest:** {AI12-0030-1} “These rules apply” refers to just this paragraph and not to the rest of the rules in this section. This rule probably should have been a Legality Rule, but the word “illegal” should key the reader that this is a Legality Rule, no matter under what text heading it occurs.

Unless available for inherited from a parent type, if any, for an untagged type having a task, protected, or explicitly limited record part, the default implementation of each of the Read, Write, Input, and Output attributes raises Program_Error and performs no other action.
It might seem that there is no need to specify the behavior of the default implementation of a streaming attribute of, for example, a task type because there is no way that it can be invoked. It is possible, however, to construct an example where such a stream attribute can be invoked. This involves using a formal untagged limited derived type for which some streaming attribute is available (because it was explicitly specified for the ancestor type) and a corresponding actual type for which the attribute is unspecified (because the derivation occurred in a place where the attribute is never available for the parent type before the aspect was specified for the ancestor type and the specification was therefore not inherited).

In the parameter and result profiles for the default implementations of the stream-oriented attributes, the subtype of the Item parameter is the base subtype of T if T is a scalar type, and the first subtype otherwise. The same rule applies to the result of the Input attribute.

For an attribute definition clause or aspect specification specifying one of these attributes, the subtype of the Item parameter shall be the first subtype or the base subtype if scalar, and the first subtype if not scalar otherwise. The same rule applies to the result of the Input function.

This is to simplify implementation.

The view of the type at the point of the attribute definition clause determines whether the first subtype or base subtype is allowed. Thus, for a scalar type with a partial view (which is never scalar), whether the first subtype or the base subtype is allowed is determined by whether the attribute definition clause occurs before or after the full definition of the scalar type. For the same reason, the base subtype is never allowed for an attribute specified via an aspect specification on the partial view.

A type is said to support external streaming if Read and Write attributes are provided for sending values of such a type between active partitions, with Write marshalling the representation, and Read unmarshalling the representation. A limited type supports external streaming only if it has available Read and Write attributes. A type with a part that is of a nonremote access type supports external streaming only if that access type or the type of some part that includes the access type component, has Read and Write attributes that have been specified via an attribute definition clause, and that attribute definition clause is visible. [An anonymous access type does not support external streaming.] All other types (including remote access types, see E.2.2) support external streaming.

A limited type with a part that is of a nonremote access type needs to satisfy both rules.

If the internal tag returned by Descendant_Tag to T'Class'Input identifies a type that is not library-level and whose tag has not been created, or does not exist in the partition at the time of the call, execution is erroneous.

The definition of Descendant_Tag prevents such a tag from being provided to T'Class'Input if T is a library-level type. However, this rule is needed for nested tagged types.

For every subtype S of a language-defined nonlimited specific type T, the output generated by S'Output or S'Write shall be readable by S'Input or S'Read, respectively. This rule applies across partitions if the implementation conforms to the Distributed Systems Annex.

If Constraint_Error is raised during a call to Read because of failure of one the above checks, the implementation shall ensure that the discriminants of the actual parameter of Read are not modified.
Implementation Permissions

The number of calls performed by the predefined implementation of the stream-oriented attributes on the Read and Write operations of the stream type is unspecified. An implementation may take advantage of this permission to perform internal buffering. However, all the calls on the Read and Write operations of the stream type **must** take place before this invocation returns. An explicit invocation is one appearing explicitly in the program text, possibly through a generic instantiation (see 12.3).

If \( T \) is a discriminated type and its discriminants have defaults, then in two cases an execution of the default implementation of \( S'\text{Read} \) is not required to create an anonymous object of type \( T \): If the discriminant values that are read in are equal to the corresponding discriminant values of \( \text{Item} \), then **creation of a new object of type \( T \) may be bypassed** and \( \text{Item} \) may be used instead. If they are not equal and \( \text{Item} \) is a constrained variable, then **Constraint_Error** may be raised at that point, before any further values are read from the stream and before the object of type \( T \) is created.

A default implementation of \( S'\text{Input} \) that calls the default implementation of \( S'\text{Read} \) may create a constrained anonymous object with discriminants that match those in the stream.

**Implementation Note:** This allows the combined executions of \( S'\text{Input} \) and \( S'\text{Read} \) to create one object of type \( T \) instead of two. If this option is exercised, then:

- The discriminants are read from the stream by \( S'\text{Input} \), not \( S'\text{Read} \).
- \( S'\text{Input} \) declares an object of type \( T \) constrained by the discriminants read from the stream, not an unconstrained object.
- The discriminant values that \( S'\text{Read} \) would normally have read from the stream are read from \( \text{Item} \) instead.
- The permissions of the preceding paragraph then apply and no object of type \( T \) need be created by the execution of \( S'\text{Read} \).

**NOTE 1** For a definite subtype \( S \) of a type \( T \), only \( T'\text{Write} \) and \( T'\text{Read} \) are necessary to pass an arbitrary value of the subtype through a stream. For an indefinite subtype \( S \) of a type \( T \), \( T'\text{Output} \) and \( T'\text{Input} \) will normally be necessary, since \( T'\text{Write} \) and \( T'\text{Read} \) do not pass bounds, discriminants, or tags.

**NOTE 2** User-specified attributes of \( S'\text{Class} \) are not inherited by other class-wide types descended from \( S \).

### Examples

**Example of user-defined Write attribute:**

```ada
procedure My_Write(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class;
    Item : My_Integer'Base);
for My_Integer'Write use My_Write;
```

**Discussion:** Example of network input/output using input output attributes:

```ada
with Ada.Streams; use Ada.Streams;
generic
type Msg_Type<> is private;
package Network_IO is
    -- Connect/Disconnect are used to establish the stream
    procedure Connect(...);
    procedure Disconnect(...);
    -- Send/Receive transfer messages across the network
    procedure Send(X : in Msg_Type);
    function Receive return Msg_Type;
private
type Network_Stream is new Root_Stream_Type with ...
procedure Read(...); -- define Read/Write for Network_Stream
procedure Write(...);
end Network_IO;
```
package body Network_IO is

Current_Stream : aliased Network_Stream := null;
.
procedure Connect(...) is ...
procedure Disconnect(...) is ...

procedure Send(X : in Msg_Type) is
begin
  Msg_Type'Output(Current_Stream'Access, X);
end Send;

function Receive return Msg_Type is
begin
  return Msg_Type'Input(Current_Stream'Access);
end Receive;

end Network_IO;

Inconsistencies With Ada 95

{8652/0040} {AI95-00108-01} Corrigendum: Clarified how the default implementation for stream attributes is determined (eliminating conflicting language). The new wording provides that attributes for type extensions are created by composing the parent's attribute with those for the extension components if any. If a program was written assuming that the extension components were not included in the stream (as in original Ada 95), it would fail to work in the language as corrected by the Corrigendum.

{AI95-00195-01} Amendment Correction: Explicitly provided a permission that the number of calls to the underlying stream Read and Write operations may differ from the number determined by the canonical operations. If Ada 95 code somehow depended on the number of calls to Read or Write, it could fail with an Ada 2005 implementation. Such code is likely to be very rare; moreover, such code is really wrong, as the permission applies to Ada 95 as well.

Extensions to Ada 95

{8652/0040} {AI95-00108-01} {AI95-00195-01} {AI95-00444-01} Corrigendum: Limited types may have default constructed attributes if all of the parent and (for extensions) extension components have available attributes. Ada 2005 adds the notion of availability to patch up some holes in the Corrigendum model.

Wording Changes from Ada 95

{8652/0009} {AI95-00137-01} Corrigendum: Added wording to specify that these are operational attributes.

{8652/0045} {AI95-00132-01} Corrigendum: Clarified that End_Error is raised by the default implementation of Read and Input if the end of the stream is reached. (The result could have been abnormal without this clarification, thus this is not an inconsistency, as the programmer could not have depended on the previous behavior.)

{AI95-00195-01} Clarified that the default implementation of S'Input does normal initialization on the object that it passes to S'Read.

{AI95-00195-01} Explicitly stated that what is read from a stream when a required check fails is unspecified.

{AI95-00251-01} Defined availability and default implementations for types with progenitors.

{AI95-00279-01} Specified that Constraint_Error is raised if the internal tag retrieved for S'Class is for some type not covered by S'Class or is abstract. We also explicitly state that the program is erroneous if the tag has not been created or does not currently exist in the partition. (Ada 95 did not specify what happened in these cases; it's very unlikely to have provided some useful result, so this is not considered an inconsistency.)

{AI95-00344-01} Added wording to support nested type extensions. S'Input and S'Output always raise Tag_Error for such extensions, and such extensions were not permitted in Ada 95, so this is neither an extension nor an incompatibility.

{AI95-00366-01} Defined supports external streaming to put all of the rules about “good” stream attributes in one place. This is used for distribution and for defining pragma Pure.

{AI95-00441-01} Added the not null qualifier to the first parameter of all of the stream attributes, so that the semantics doesn't change between Ada 95 and Ada 2005. This change is compatible, because mode conformance is required for subprograms specified as stream attributes, and null exclusions are not considered for mode conformance.

{AI95-00444-01} Improved the wording to make it clear that we don't define the default implementations of attributes that cannot be called (that is, aren't “available”). Also clarified when inheritance takes place.
Incompatibilities With Ada 2005

{AI05-0039-1} **Correction:** Added a requirement that stream attributes be specified by a static subprogram name rather than a dynamic expression. Expressions cannot provide any useful functionality because of the freezing rules, and the possibility of them complicates implementations. Only pathological programs should be affected.

Extensions to Ada 2005

{AI05-0007-1} **Correction:** Stream attributes for scalar types can be specified with subprograms that take the first subtype as well as the base type. This eliminates confusion about which subtype is appropriate for attributes specified for partial views whose full type is a scalar type. It also eliminates a common user error (forgetting 'Base).

Wording Changes from Ada 2005

{AI05-0023-1} **Correction:** Corrected the definition of the default version S'Read and S'Input to be well-defined if S is a discriminated type with defaulted discriminants and some components require initialization and/or finalizations.

{AI05-0065-1} **Correction:** Defined remote access types to support external streaming, since that is their purpose.

{AI05-0109-1} **Correction:** Removed a misleading phrase which implies that Constraint_Error is raised for internal tags of the wrong type, when Tag_Error should be raised for such tags.

{AI05-0139-2} Clarified that arrays with convention Fortran are written in column-major order, rather than row-major order. This is necessary in order that streaming of Fortran arrays is efficient.

{AI05-0192-1} **Correction:** Clarified that the profile of an inherited stream attribute is as defined for an inherited primitive subprogram, while the default implementation of the same attribute might have a different profile.

{AI05-0194-1} **Correction:** Clarified that Stream_Size has no effect on and is not effected by user-defined stream attributes.

Inconsistencies With Ada 2012

{AI12-0419-1} The switch from inheritance to “implicitly composed” aspects means that there exists an exceedingly unlikely case where Ada 2022 code will raise Constraint_Error where Ada 2012 code would not. That case requires deriving a constrained untagged composite type C from an unconstrained parent type P, using a type conversion to P of the Input attribute of C, and streaming in a value that violates the constraints of C. Simply using the Input attribute of P instead of that of C will restore the Ada 2012 behavior.

Extensions to Ada 2012

{AI12-0106-1} **Corrigendum:** Defined how to specify a class-wide stream-oriented attribute using an aspect_specification. It was always intended that this was possible, but the method was not clear, as a class-wide type never has an explicit declaration.

Wording Changes from Ada 2012

{AI12-0030-1} **Corrigendum:** Defined the runtime effect of stream attributes for untagged limited types, as there is a weird corner case where they can be called. We don't specify this as an inconsistency, as it doesn't make semantic sense to stream a task, and nothing useful could have been done with that, so it should not exist in any programs.

{AI12-0106-1} **Corrigendum:** Clarified that the same Legality Rules apply when a stream-oriented attribute is specified via an aspect_specification as applied when it is specified via an attribute_definition_clause.

{AI12-0064-2} {AI12-0396-1} Added the definition of Nonblocking (see 9.5) and Global (see 6.1.2) for stream-oriented attributes.

{AI12-0419-1} **Corrigendum:** Revised to define composition of stream-oriented attributes for untagged derived types in order to avoid using inheritance for these attributes/aspects.

13.14 Freezing Rules

{AI05-0299-1} [This subclause defines a place in the program text where each declared entity becomes “frozen”. A use of an entity, such as a reference to it by name, or (for a type) an expression of the type, causes freezing of the entity in some contexts, as described below. The Legality Rules forbid certain kinds of uses of an entity in the region of text where it is frozen.]

**Reason:** This concept has two purposes: a compile-time one and a run-time one.
The compile-time purpose of the freezing rules comes from the fact that the evaluation of static expressions depends on overload resolution, and overload resolution sometimes depends on the value of a static expression. (The dependence of static evaluation upon overload resolution is obvious. The dependence in the other direction is more subtle. There are three rules that require static expressions in contexts that can appear in declarative places: The expression in an attribute_designator shall be static. In a record aggregate, variant-controlling discriminants shall be static. In an array aggregate with more than one named association, the choices shall be static. The compiler needs to know the value of these expressions in order to perform overload resolution and legality checking.) We wish to allow a compiler to evaluate static expressions when it sees them in a single pass over the compilation_unit. The freezing rules ensure that.

The run-time purpose of the freezing rules is called the “linear elaboration model”. This means that declarations are elaborated in the order in which they appear in the program text, and later elaborations can depend on the results of earlier ones. The elaboration of the declarations of certain entities requires run-time information about the implementation details of other entities. The freezing rules ensure that this information has been calculated by the time it is used. For example, suppose the initial value of a constant is the result of a function call that takes a parameter of type \( T \). In order to pass that parameter, the size of type \( T \) has to be known. If \( T \) is composite, that size might be known only at run time.

(Note that in these discussions, words like “before” and “after” generally refer to places in the program text, as opposed to times at run time.)

**Discussion:** The “implementation details” we’re talking about above are:

- For a tagged type, the implementations of all the primitive subprograms of the type — that is (in the canonical implementation model), the contents of the type descriptor, which contains pointers to the code for each primitive subprogram.
- For a type, the full type declaration of any parts (including the type itself) that are private.
- For a deferred constant, the full constant declaration, which gives the constant's value. (Since this information necessarily comes after the constant's type and subtype are fully known, there's no need to worry about its type or subtype.)
- For any entity, representation information specified by the user via representation items. Most representation items are for types or subtypes; however, various other kinds of entities, such as objects and subprograms, are possible.

{AI05-0005-1} Similar issues arise for incomplete types. However, we do not use freezing to prevent premature access there; incomplete types have different, more severe, restrictions. Similar issues also arise for subprograms, protected operations, tasks and generic units. However, we do not use freezing to prevent premature access for those there either; 3.11 prevents problems with run-time Elaboration Checks. Even so, freezing is used for these entities to prevent giving representation items too late (that is, after uses that require representation information, such as calls).

**Language Design Principles**

An evaluable construct should freeze anything that's needed to evaluate it.

However, if the construct is not evaluated where it appears, let it cause freezing later, when it is evaluated. This is the case for default_expressions and default_names. (Formal parameters, generic formal parameters, and components can have default_expressions or default_names.)

The compiler should be allowed to evaluate static expressions without knowledge of their context. (I.e. there should not be any special rules for static expressions that happen to occur in a context that requires a static expression.)

Compilers should be allowed to evaluate static expressions (and record the results) using the run-time representation of the type. For example, suppose Color'Pos(Red) = 1, but the internal code for Red is 37. If the value of a static expression is Red, some compilers might store 1 in their symbol table, and other compilers might store 37. Either compiler design should be feasible.

Compilers should never be required to detect erroneousness or exceptions at compile time (although it's very nice if they do). This implies that we should not require code-generation for a nonstatic expression of type \( T \) too early, even if we can prove that that expression will be erroneous, or will raise an exception.

Here's an example (modified from AI83-00039, Example 3):
type T is
  record
    ...
  end record;
function F return T;
function G(X : T) return Boolean;
Y : Boolean := G(F); -- doesn't force T in Ada 83
for T use
  record
    ...
  end record;

AI83-00039 says this is legal. Of course, it raises Program_Error because the function bodies aren't elaborated yet. A one-pass compiler has to generate code for an expression of type T before it knows the representation of T. Here's a similar example, which AI83-00039 also says is legal:

package P is
  type T is private;
  function F return T;
  function G(X : T) return Boolean;
Y : Boolean := G(F); -- doesn't force T in Ada 83
private
  type T is
    record
      ...
    end record;
end P;

If T's size were dynamic, that size would be stored in some compiler-generated dope; this dope would be initialized at the place of the full type declaration. However, the generated code for the function calls would most likely allocate a temp of the size specified by the dope before checking for Program_Error. That dope would contain uninitialized junk, resulting in disaster. To avoid doing that, the compiler would have to determine, at compile time, that the expression will raise Program_Error.

This is silly. If we're going to require compilers to detect the exception at compile time, we might as well formulate the rule as a legality rule.

Compilers should not be required to generate code to load the value of a variable before the address of the variable has been determined.

After an entity has been frozen, no further requirements may be placed on its representation (such as by a representation item or a full_type_declaration).

The freezing of an entity occurs at one or more places (freezing points) in the program text where the representation for the entity has to be fully determined. Each entity is frozen from its first freezing point to the end of the program text (given the ordering of compilation units defined in 10.1.4).

Ramification: The “representation” for a subprogram includes its calling convention and means for referencing the subprogram body, either a “link-name” or specified address. It does not include the code for the subprogram body itself, nor its address if a link-name is used to reference the body.

This subclause also defines a place in the program text where the profile of each declared callable entity becomes frozen. A use of a callable entity causes freezing of its profile in some contexts, as described below. At the place where the profile of a callable entity becomes frozen, the entity itself becomes frozen.

The end of a declarative_part, protected_body, or a declaration of a library package or generic library package, causes freezing of each entity and profile declared within it, as well as the entity itself in the case of the declaration of a library unit except for incomplete types. A noninstance proper_body, body_stub, or entry_body, noninstance body other than a rename as body, causes freezing of each entity and profile declared before it within the same declarative_part that is not an incomplete type; it only causes freezing of an incomplete type if the body is within the immediate scope of the incomplete type.

Discussion: This is worded carefully to handle nested packages and private types. Entities declared in a nested package_specification will be frozen by some containing construct.

An incomplete type declared in the private part of a library package_specification can be completed in the body. For other incomplete types (and in the bodies of library packages), the completion of the type will be frozen at the end of the package or declarative_part, and that will freeze the incomplete view as well.
3.1/5 \{AI05-0017-1\} \{AI12-0155-1\} The reason we have to worry about freezing of incomplete types is to prevent premature uses of the types in dispatching calls. Such uses may need access to the tag of the type, and the type has to be frozen to know where the tag is stored.

3.3/3 \{AI05-0029-1\} The part about bodies does not say immediately within. A renaming-as-body does not have this property. Nor does \texttt{an imported body pragma Import}.

3.4/5 \{AI12-0300-1\} The reason bodies cause freezing is because we want proper_bodies and body_stubs to be interchangeable — one should be able to move a proper_body to a subunit, and vice versa, without changing the semantics. Clearly, anything that should cause freezing should do so even if it’s inside a proper_body. However, if we make it a body_stub, then the compiler can’t see that thing that should cause freezing. So we make body_stubs cause freezing, just in case they contain something that should cause freezing. But that means we need to do the same for proper_bodies.

3.e Another reason for bodies to cause freezing, there could be an added implementation burden if an entity declared in an enclosing declarative_part is frozen within a nested body, since some compilers look at bodies after looking at the containing declarative_part.

3.6/4 \{AI05-0177-1\} \{AI12-0103-1\} Note that “body” includes null procedure declarations and expression_function_declarations (even when those are used as completions), as well as generic_instantiations and renames-as-bodies do not necessarily cause freezing: each have their own specific rules. \texttt{entry_body} (see 3.11.1). These all cause freezing, along with proper_bodies and body_stubs.

3.9/5 \{AI12-0103-1\} \{AI12-0005-1\} Note that the rule about proper bodies \texttt{causing being} freezing only applies in declarative_parts. All of the kinds of bodies (see 3.11.1 — keep in mind the difference from bodys) that are allowed in a package specification have their own freezing rules, so they don’t need to be covered by the above rule.

4/1 \{8652/0046\} \{AI95-00106-01\} A construct that (explicitly or implicitly) references an entity can cause the \texttt{freezing} of the entity, as defined by subsequent paragraphs. At the place where a construct causes freezing, each name, \texttt{expression}, \texttt{implicit dereference}, \texttt{expression}, [or range] within the construct causes freezing.

4.a \textbf{Ramification:} Note that in the sense of this paragraph, a subtype_mark “references” the denoted subtype, but not the type.

5/3 \{AI05-0213-1\} The occurrence of a generic_instantiation causes freezing, except that a name which is a generic actual parameter whose corresponding generic formal parameter is a formal incomplete type (see 12.5.1) does not cause freezing. In addition, if, also, if a parameter of the instantiation is defaulted, the default_expression or default_name for that parameter causes freezing.

5.a/3 \textbf{Ramification:} \{AI05-0213-1\} Thus, an actual parameter corresponding to a formal incomplete type parameter may denote an incomplete or private type which is not completely defined at the point of the generic_instantiation.

5.1/4 \{AI12-0103-1\} \{AI12-0157-1\} At the occurrence of an expression_function_declaration that is a completion, the return expression of the expression function causes freezing.

5.b/4 \textbf{Reason:} \{AI12-0103-1\} This rule prevents calls through access values to an expression that might have unfrozen parts. Typically, elaboration checks and other freezing rules prevent this, but in this case the completion is elaborated and since this is not a body it does not by itself freeze anything that precedes it.

5.2/4 \{AI12-0132-1\} \{AI12-0157-1\} At the occurrence of a renames-as-body whose callable_entity name denotes an expression function, the return expression of the expression function causes freezing.

6 \textbf{Reason:} The occurrence of an object_declaration that has no corresponding completion causes freezing.

6.a \textbf{Ramification:} Note that this does not include a formal_object_declaration.

7 \textbf{Reason:} The declaration of a record extension causes freezing of the parent subtype.

7.a \textbf{Ramification:} This combined with another rule specifying that primitive subprogram declarations shall precede freezing ensures that all descendants of a tagged type implement all of its dispatching operations.

7.b/2 \{AI95-00251-01\} The declaration of a private extension does not cause freezing. The freezing is deferred until the full type declaration, which will necessarily be for a record extension, task, or protected type (the latter only for a limited private extension derived from an interface).

7.1/2 \{AI95-00251-01\} The declaration of a record extension, interface type, task unit, or protected unit causes freezing of any progenitor types specified in the declaration.
Reason: This rule has the same purpose as the one above: ensuring that all descendants of an interface tagged type implement all of its dispatching operations. As with the previous rule, a private extension does not freeze its progenitors; the full type declaration (which must have the same progenitors) will do that.

Ramification: An interface type can be a parent as well as a progenitor; these rules are similar so that the location of an interface in a record extension does not have an effect on the freezing of the interface type.

- {AI05-0183-1} {AI12-0396-1} {AI12-0407-1} {AI12-0439-1} At the freezing point of the entity associated with an aspect specification, any static expressions or names within the aspect specification cause freezing, as do expressions or names in aspect definitions for representation aspects, or operational aspects that have a corresponding operational attribute. Similarly, if an aspect definition for an operational aspect, other than an assertion aspect, can affect the Name Resolution, Static Semantics, or Legality Rules of a subsequent construct, then any expressions or names within the aspect definition cause freezing at the freezing point of the associated entity. Any static expressions within an aspect specification also cause freezing at the end of the immediately enclosing declaration list. For the purposes of this rule, if there is no declared entity associated with an aspect specification, the freezing point is considered to occur immediately following the aspect specification.

- {8652/0046} {AI95-00106-01} {AI05-0177-1} {AI05-0183-1} {AI05-0157-1} A static expression (other than within an aspect specification) causes freezing where it occurs. An object name or a nonstatic expression causes freezing where it occurs, unless the name or expression is part of a default_expression, a default_name, the return expression of an expression function, an aspect specification, or a per-object expression of a component's constraint, in which case, the freezing occurs later as part of another construct or at the freezing point of an associated entity.

- {8652/0046} {AI95-00106-01} {AI05-0019-1} An implicit call freezes the same entities and profiles that would be frozen by an explicit call. This is true even if the implicit call is removed via implementation permissions.

- {8652/0046} {AI95-00106-01} If an expression is implicitly converted to a type or subtype T, then at the place where the expression causes freezing, T is frozen.

The following rules define which entities are frozen at the place where a construct causes freezing:

- {AI12-0367-1} At the place where an expression causes freezing, the type of the expression is frozen, unless the expression is an enumeration literal used as a discrete_choice of the array_aggregate of an enumeration_representation_clause or as the aspect_definition of a specification for aspect Default_Value.

Reason: We considered making enumeration literals never cause freezing, which would be more upward compatible, but examples like the variant record aggregate (Discrim => Red, ...) caused us to change our mind. Furthermore, an enumeration literal is a static expression, so the implementation should be allowed to represent it using its representation.

- {AI12-0367-1} We exclude uses of enumeration literals that are used in part for setting the representation of the type (aspect Default_Value is defined to be a representation aspect) so we don’t freeze the type while determining its representation.

Ramification: The following pathological example was legal in Ada 83, but is illegal in Ada 95:

```
package P1 is
  type T is private;
package P2 is
  type Composite(D : Boolean) is
    record
      case D is
        when False => Cf : Integer;
        when True  => Ct : T;
      end case;
    end record;
  end P2;
  X : Boolean := P2."=( (False,1), (False,1) );
private
  type T is array(1..Func_Call) of Integer;
end;
```
In Ada 95, the declaration of X freezes Composite (because it contains an expression of that type), which in turn freezes T (even though Ct does not exist in this particular case). But type T is not completely defined at that point, violating the rule that a type shall be completely defined before it is frozen. In Ada 83, on the other hand, there is no occurrence of the name T, hence no forcing occurrence of T.

At the place where a function call causes freezing, the profile of the function is frozen. Furthermore, if a parameter of the call is defaulted, the default expression for that parameter causes freezing. If the function call is to an expression function, the return expression of the expression function causes freezing.

Reason: This is the important rule for profile freezing: a call freezes the profile. That's because generating the call will need to know how the parameters are passed, and that will require knowing details of the types. Other uses of subprograms do not need to know about the parameters, and thus only freeze the subprogram, and not the profile.

Note that we don't need to consider procedure or entry calls, since a body freezes everything that precedes it, and the end of a declarative part freezes everything in the declarative part.

Ramification: Freezing of the return expression of an expression function only needs to be considered when the expression function is in the same compilation unit and there are no intervening bodies; the end of a declarative part or library package freezes everything in it, and a body freezes everything declared before it.

At the place where a generic instantiation causes freezing of a callable entity, the profile of that entity is frozen unless the formal subprogram corresponding to the callable entity has a parameter or result of a formal untagged incomplete type; if the callable entity is an expression function, the return expression of the expression function causes freezing.

Reason: Elaboration of the generic might call the actual for one of its formal subprograms, so we need to know the profile and (for an expression function) expression.

At the place where a use of the Access or Unchecked Access attribute whose prefix denotes an expression function causes freezing, the return expression of the expression function causes freezing.

Reason: This is needed to avoid calls to unfrozen expressions. Consider:

```ada
package Pack is
  type Flub is range 0 .. 100;
  function Foo (A : in Natural) return Natural is
    [A + Flub'Size]; -- The expression is not frozen.
  end Foo;

  type Bar is access function Foo (A : in Natural) return Natural;
  end Bar;

  P : Bar := Foo'Access; -- (A)
  Val : Natural := P.all[5]; -- (B)
end Pack;
```

If point (A) did not freeze the expression of Foo (which freezes Flub), then the call at point (B) would be depending on the aspects of the unfrozen type Flub. That would be bad.

At the place where a name causes freezing, the entity denoted by the name is frozen, unless the name is a prefix of an expanded name; at the place where an object name causes freezing, the nominal subtype associated with the name is frozen.

Ramification: This only matters in the presence of deferred constants or access types; an object_declaration other than a deferred_constant_declaration causes freezing of the nominal subtype, plus all component junk.

Discussion: This rule ensures that X.D freezes the same entities that X.all.D does. Note that an implicit dereference is neither a name nor expression by itself, so it isn't covered by other rules.

[ At the place where a range causes freezing, the type of the range is frozen.]
Proof: This is consequence of the facts that expressions freeze their type, and the Range attribute is defined to be equivalent to a pair of expressions separated by "..".

- At the place where an allocator causes freezing, the designated subtype of its type is frozen. If the type of the allocator is a derived type, then all ancestor types are also frozen.

Ramification: Allocators also freeze the named subtype, as a consequence of other rules.

The ancestor types are frozen to prevent things like this:

```
type Pool_Ptr is access System.Storage_Pools.Root_Storage_Pool'Class;
function F return Pool_Ptr;
package P is
  type A1 is access Boolean;
  type A2 is new A1;
  type A3 is new A2;
  X : A3 := new Boolean; -- Don't know what pool yet!
  for A1'Storage_Pool use F.all;
end P;
```

This is necessary because derived access types share their parent's pool.

- {AI05-0019-1} At the place where a profile callable entity is frozen, each subtype of the corresponding profile is frozen. If the corresponding callable entity is a member of an entry family, the index subtype of the family is frozen.

At the place where a function call causes freezing, if a parameter of the call is defaulted, the default_expression for that parameter causes freezing.

This paragraph was deleted. Discussion: We don't worry about freezing for procedure calls or entry calls, since a body freezes everything that precedes it, and the end of a declarative part freezes everything in the declarative part.

- {AI12-0186-1} At the place where a subtype is frozen, its type is frozen. At the place where a type is frozen, any expressions or names within the full type definition cause freezing, other than those that occur within an access_type_definition or an access_definition; the first subtype, and any component subtypes, index subtypes, and parent subtype of the type are frozen as well. For a specific tagged type, the corresponding class-wide type is frozen as well. For a class-wide type, the corresponding specific type is frozen as well.

Ramification: Freezing a type needs to freeze its first subtype in order to preserve the property that the subtype-specific aspects of statically matching subtypes are the same.

Freezing an access type does not freeze its designated subtype.

- {AI95-00341-01} {AI05-0019-1} At the place where a specific tagged type is frozen, the primitive subprograms of the type are frozen. At the place where a type is frozen, any subprogram named in an attribute_definition_clause for the type is frozen.

Reason: We have a language design principle that all of the details of a specific tagged type are known at its freezing point. But that is only true if the primitive subprograms are frozen at this point as well. Late changes of Import and address clauses violate the principle.

Implementation Note: This rule means that no implicit call to Initialize or Adjust can freeze a subprogram (the type and thus subprograms would have been frozen at worst at the same point).

Discussion: {AI05-0019-1} The second sentence is the rule that makes it possible to check that only subprograms with convention Ada are specified in attribute_definition_clauses without jumping through hoops.

- {AI12-0396-1} At the place where a construct causes freezing, if the construct includes a check associated with some assertion aspect [(independent of whether the check is enabled)], or depends on the definition of some operational aspect as part of its Dynamic Semantics, any names or expressions in the aspect_definition for the aspect cause freezing.

Ramification: Aspects such as Constant Indexing cause freezing when they are used — the name in a Constant Indexing would cause freezing when a generalized_indexing that makes use of it causes freezing.

Notwithstanding the rest of this subclause, freezing an incomplete view has no effect.
In contrast, freezing a partial view does have an effect (the completion of the view is frozen and the program is illegal if it hasn't occurred yet).

**Legality Rules**

16. **The explicit declaration of a primitive subprogram of a tagged type shall occur before the type is frozen (see 3.9.2).**

   **Reason:** This rule is needed because (1) we don't want people dispatching to things that haven't been declared yet, and (2) we want to allow tagged type descriptors to be static (allocated statically, and initialized to link-time-known symbols). Suppose T2 inherits primitive P from T1, and then overrides P. Suppose P is called before the declaration of the overriding P. What should it dispatch to? If the answer is the new P, we've violated the first principle above. If the answer is the old P, we've violated the second principle. (A call to the new one necessarily raises Program_Error, but that's beside the point.)

16.b Note that a call upon a dispatching operation of type T will freeze T.

16.c We considered applying this rule to all derived types, for uniformity. However, that would be upward incompatible, so we rejected the idea. As in Ada 83, for an untagged type, the above call upon P will call the old P (which is arguably confusing).

16.d/3

   **To be honest:** {AI95-00222-1} This rule only applies to "original" declarations and not to the completion of a primitive subprogram, even though a completion is technically an explicit declaration, and it may declare a primitive subprogram.

17. **[A type shall be completely defined before it is frozen (see 3.11.1 and 7.3).]**

18. **[The completion of a deferred constant declaration shall occur before the constant is frozen (see 7.4).]**

18.a/5

   **This paragraph was deleted**

   **Proof:** {AI95-00114-01} {AI93-0299-1} {AI12-0181-1} The above Legality Rules are stated "officially" in the referenced subclauses/ clauses.

19. **{8652/0009} {AI95-00137-01}**

   **[An operational or A] representation item that directly specifies an aspect of an entity shall appear before the entity is frozen (see 13.1).]

19.a/1

   **Discussion:** {8652/0009} {AI95-00137-01} From RM83-13.1(7). The wording here forbids freezing within the \_clause itself, which was not true of the Ada 83 wording. The wording of this rule is carefully written to work properly for type-related representation items. For example, an enumeration._representation_clause is illegal after the type is frozen, even though the _clause refers to the first subtype.

19.a/1/5

   **This paragraph was deleted** {AI95-00114-01} {AI12-0181-1} The above Legality Rule is stated for types and subtypes in 13.1, but the rule here covers all other entities as well.

19.b/5

   **Proof:** {AI95-00114-01} {AI12-0181-1} The above Legality Rules are stated "officially" in the referenced subclauses. The above Legality Rules are stated "officially" in the referenced clauses.

19.c

   **Discussion:** Here's an example that illustrates when freezing occurs in the presence of defaults:

19.d

   type T is ...;
   function F return T;
   type R is
       record
           C : T := F;
           D : Boolean := F = F;
       end record;

   X : R;

19.e

   Since the elaboration of R's declaration does not allocate component C, there is no need to freeze C's subtype at that place. Similarly, since the elaboration of R does not evaluate the default_expression "F = F", there is no need to freeze the types involved at that point. However, the declaration of X does need to freeze these things. Note that even if component C did not exist, the elaboration of the declaration of X would still need information about T — even though D is not of type T, its default_expression requires that information.

19.f

   **Ramification:** Although we define freezing in terms of the program text as a whole (i.e. after applying the rules of Clause 10), the freezing rules actually have no effect beyond compilation unit boundaries.

19.g

   **Reason:** That is important, because Clause 10 allows some implementation definedness in the order of things, and we don't want the freezing rules to be implementation defined.

19.h

   **Ramification:** These rules also have no effect in statements — they only apply within a single declarative_part, package_specification, task_definition, protected_definition, or protected_body.

19.i

   **Implementation Note:** An implementation may choose to generate code for default_expressions and default_names in line at the place of use. Alternatively, an implementation may choose to generate thunks (subprograms implicitly
generated by the compiler) for evaluation of defaults. Thunk generation cannot, in general, be done at the place of the declaration that includes the default. Instead, they can be generated at the first freezing point of the type(s) involved. (It is impossible to write a purely one-pass Ada compiler, for various reasons. This is one of them — the compiler needs to store a representation of defaults in its symbol table, and then walk that representation later, no earlier than the first freezing point.)

In implementation terms, the linear elaboration model can be thought of as preventing uninitialized dope. For example, the implementation might generate dope to contain the size of a private type. This dope is initialized at the place where the type becomes completely defined. It cannot be initialized earlier, because of the order-of-elaboration rules. The freezing rules prevent elaboration of earlier declarations from accessing the size dope for a private type before it is initialized.

\{AI05-0299-1\} 2.8 overrides the freezing rules in the case of unrecognized pragmas; similarly 13.1.1 overrides the freezing rules in the case of an unrecognized aspect.

\{8652/0009\} \{AI95-00137-01\} An aspect_clause A representation_clause for an entity should most certainly not be a freezing point for the entity.

**Dynamic Semantics**

\{AI95-00279-01\} The tag (see 3.9) of a tagged type T is created at the point where T is frozen.

**Incompatibilities With Ada 83**

RM83 defines a forcing occurrence of a type as follows: “A forcing occurrence is any occurrence [of the name of the type, subtypes of the type, or types or subtypes with subcomponents of the type] other than in a type or subtype declaration, a subprogram specification, an entry declaration, a deferred constant declaration, a pragma, or a representation_clause for the type itself. In any case, an occurrence within an expression is always forcing.”

It seems like the wording allows things like this:

\begin{verbatim}
  type A is array(Integer range 1..10) of Boolean;
  subtype S is Integer range A'Range;
  -- not forcing for A
\end{verbatim}

Occurrences within pragmas can cause freezing in Ada 95. (Since such pragmas are ignored in Ada 83, this will probably fix more bugs than it causes.)

**Extensions to Ada 83**

In Ada 95, generic_formal_parameter_declarations do not normally freeze the entities from which they are defined. For example:

\begin{verbatim}
package Outer is
  type T is tagged limited private;
  generic
    type T2 is new T with private; -- Does not freeze T
    -- in Ada 95.
  package Inner is
    ...;
  end Inner;
private
  type T is ...;
end Outer;
\end{verbatim}

This is important for the usability of generics. The above example uses the Ada 95 feature of formal derived types. Examples using the kinds of formal parameters already allowed in Ada 83 are well known. See, for example, comments 83-00627 and 83-00688. The extensive use expected for formal derived types makes this issue even more compelling than described by those comments. Unfortunately, we are unable to solve the problem that explicit_generic_actual_parameters cause freezing, even though a package equivalent to the instance would not cause freezing. This is primarily because such an equivalent package would have its body in the body of the containing program unit, whereas an instance has its body right there.

**Wording Changes from Ada 83**

The concept of freezing is based on Ada 83’s concept of “forcing occurrences”. The first freezing point of an entity corresponds roughly to the place of the first forcing occurrence, in Ada 83 terms. The reason for changing the terminology is that the new rules do not refer to any particular “occurrence” of a name of an entity. Instead, we refer to “uses” of an entity, which are sometimes implicit.

In Ada 83, forcing occurrences were used only in rules about representation_clauses. We have expanded the concept to cover private types, because the rules stated in RM83-7.4.1(4) are almost identical to the forcing occurrence rules.
The Ada 83 rules are changed in Ada 95 for the following reasons:

- The Ada 83 rules do not work right for subtype-specific aspects. In an earlier version of Ada 9X, we considered allowing representation items to apply to subtypes other than the first subtype. This was part of the reason for changing the Ada 83 rules. However, now that we have dropped that functionality, we still need the rules to be different from the Ada 83 rules.

- The Ada 83 rules do not achieve the intended effect. In Ada 83, either with or without the AIs, it is possible to force the compiler to generate code that references uninitialized dope, or force it to detect erroneousness and exception raising at compile time.

- It was a goal of Ada 83 to avoid uninitialized access values. However, in the case of deferred constants, this goal was not achieved.

- The Ada 83 rules are not only too weak — they are also too strong. They allow loopholes (as described above), but they also prevent certain kinds of default expressions that are harmless, and certain kinds of generic declarations that are both harmless and very useful.

- Ada 83 had a case where an aspect_clause, representation_clause had a strong effect on the semantics of the program — ‘Small. This caused certain semantic anomalies. There are more cases in Ada 95, because the attribute_definition_clause, attribute_representation_clause has been generalized.

### Incompatibilities With Ada 95

- Various freezing rules were added to fix holes in the rules. Most importantly, implicit calls are now freezing, which make some representation clauses illegal in Ada 2005 that were legal (but dubious) in Ada 95.
- Amendment Correction: Similarly, the primitive subprograms of a specific tagged type are frozen when the type is frozen, preventing dubious convention changes (and address clauses) after the freezing point. In both cases, the code is dubious and the workaround is easy.

### Wording Changes from Ada 95

- Added wording to specify that both operational and representation attributes must be specified before the type is frozen.
- Added wording that declaring a specific descendant of an interface type freezes the interface type.
- Added wording that defines when a tag is created for a type (at the freezing point of the type). This is used to specify checking for uncreated tags (see 3.9).

### Incompatibilities With Ada 2005

- Separated the freezing of the profile from the rest of a subprogram, in order to reduce the impact of the Ada 95 incompatibility noted above. (The effects were much more limiting than expected.)

### Wording Changes from Ada 2005

- Reworded so that incomplete types with a deferred completion aren't prematurely frozen.
- Added freezing rules for expression functions; these are frozen at the point of call, not the point of declaration, like default expressions.
- Added freezing rules for aspect_specifications; these are frozen at the freezing point of the associated entity, not the point of declaration.
- Added freezing rules for formal incomplete types; the corresponding actual is not frozen.

### Wording Changes from Ada 2012

- Clarified when and what an expression_function_declaration that is a completion or that is the target of a renames-as-body freezes. This is formally an incompatibility, but as all known implementations freeze expression functions more aggressively than allowed by either the old or new wording, practically this will be an extension.
- This was an unintentional change caused by the Technical Corrigendum 1 oversimplifying wording.
- Clarified that the implicit body created by an instance doesn't have any freezing effect. Incompatibility change caused by the Technical Corrigendum 1 oversimplifying wording.
- Clarified that incomplete types do not freeze in any case. The known case where incomplete freezing was necessary has been plugged with a new Legality Rules (see 3.10.1). This matches the original intent (see Language Design Principles above) and eliminates whack-a-mole trying to allow such freezing without it having (almost) any effects.
- Clarified that the subtype names in an access type are not frozen at the point of the type declaration. This has always been true (there is an Ada 95-era AARM note that says so) but it didn’t follow from the
actual wording. Since the ACATS requires the AARM note to be true, no compiler could actually get this wrong, so no incompatibility is possible.

\{AI12-0367-1\} Correction: Added a freezing exclusion for enumeration literals in the expression of a Default_Value aspect; otherwise, one could not set a default value for an enumeration type.

\{AI12-0373-1\} Added missing definition of freezing of library units.

\{AI12-0396-1\} Correction: Improved and clarified the freezing rules for aspect specifications; these now depend on the kind of aspect.
The Standard Libraries
Annex A
(normative)
Predefined Language Environment

[ This Annex contains the specifications of library units that shall be provided by every implementation. There are three root library units: Ada, Interfaces, and System; other library units are children of these:]

\{8652/0047\} \{AI95-00081-01\} \{AI95-00424-01\} \{AI05-0001-1\} \{AI05-0049-1\} \{AI05-
0111-3\} \{AI05-0136-1\} \{AI05-0137-1\} \{AI05-0166-1\} \{AI05-0168-1\} \{AI12-0021-1\} \{AI12-0208-1\}
\{AI12-0234-1\} \{AI12-0254-1\} \{AI12-0293-1\} \{AI12-0321-1\}

---

Instantiations — A.15
Ada — A.2

---

Assertions — 11.4.2
Asynchronous_Task_Control — D.11
Calendar — 9.6
Arithmetic — 9.6.1
Formatting — 9.6.1
Time_Zones — 9.6.1
Characters — A.3.1
Conversions — A.3.4
Handling — A.3.2
Latin_1 — A.3.3
Command_Line — A.15
Complex_Text_IO — G.1.3
Containers — A.18.1

---

Bounded_Doubly_Linked_Lists — A.18.20
Bounded_Hashed_Maps — A.18.21
Bounded_Hashed_Sets — A.18.23
Bounded_Indefinite_Holders — A.18.32
Bounded_Multiway_Trees — A.18.25
Bounded_Ordered_Maps — A.18.22
Bounded_Ordered_Sets — A.18.24
Bounded_Priority_Queue — A.18.31
Bounded_Synchronized_Queue — A.18.29
Bounded_Vectors — A.18.19
Doubly_Linked_Lists — A.18.3
Generic_Array_Sort — A.18.26
Generic_Constrained_Array — A.18.26
Generic_Sort — A.18.26
Hashed_Maps — A.18.5
Hashed_Sets — A.18.8
Indefinite_Doubly_Linked_Lists — A.18.12
Indefinite_Hashed_Maps — A.18.13
Indefinite_Hashed_Sets — A.18.15
Indefinite_Multiway_Trees — A.18.17
Indefinite_Ordered_Maps — A.18.14
Indefinite_Ordered_Sets — A.18.16
Indefinite_Vectors — A.18.11

---

Multiway_Trees — A.18.10
Ordered_Maps — A.18.6
Ordered_Sets — A.18.9
Synchronized_Queue_Interfaces — A.18.27
Unbounded_Priority_Queue — A.18.30
Unbounded_Synchronized_Queue — A.18.28
Vectors — A.18.2

---

Standard (...continued)

---

Dispatching — D.2.1
EDF — D.2.6
Non_Preemptive — D.2.4
Round_Robin — D.2.5
Dynamic_Priorities — D.5.1
Environment_Variables — A.17

---

Exceptions — 11.4.1
Execution_Time — D.14
A.4.7
Wide_Equal_Case_Insensitive
—— A.4.7
Wide_Hash — A.4.7
Wide_Hash_Case_Insensitive — A.4.7
Wide_Wide_Bounded — A.4.8
Wide_Wide_Equal_Case_Insensitive
—— A.4.8
Wide_Wide_Hash — A.4.8
Wide_Wide_Hash_Case_Insensitive
—— A.4.8
Wide_Wide_Maps — A.4.8
Wide_Wide_Constants — A.4.8
Wide_Wide_Unbounded — A.4.8
Wide_Wide_Equal_Case_Insensitive
—— A.4.8
Wide_Wide_Hash — A.4.8
Wide_Wide_Hash_Case_Insensitive
—— A.4.8
Wide_Wide_Characters — A.3.1
Handling — A.3.6
Wide_Wide_Command_Line — A.15.1
Wide_Wide_Directories — A.16.2
Wide_Wide_Environment_Variables — A.17.1
Unbounded_IO — A.10.12
Unchecked_Conversion — 13.9
Unchecked_Deallocate_Subpool — 13.11.5
Unchecked_Deallocation — 13.11.2
Wide_Characters — A.3.1
Handling — A.3.5
Wide_Command_Line — A.15.1
Wide_Directories — A.16.2
Wide_Environment_Variables — A.17.1
String (.continued)

Ada (.continued)

Strings (.continued)

Wide_Wide_Equal_Case_Insensitive
—— A.4.8
Wide_Wide_Fixed — A.4.8
Wide_Wide_Equal_Case_Insensitive
—— A.4.8
Wide_Wide_Hash — A.4.8
Wide_Wide_Hash_Case_Insensitive
—— A.4.8
Wide_Wide_Hash — A.4.8
Wide_Wide_Hash_Case_Insensitive
—— A.4.8
Wide_Wide_Maps — A.4.8
Wide_Wide_Constants — A.4.8
Wide_Wide_Unbounded — A.4.8
Wide_Wide_Equal_Case_Insensitive
—— A.4.8
Wide_Wide_Hash — A.4.8
Wide_Wide_Hash_Case_Insensitive
—— A.4.8
Synchronous_Barriers — D.10.1
Synchronous_Task_Control — D.10
EDF — D.10
Standard (.continued)

Ada (.continued)

Tags — 3.9
Generic_Dispatching_Constructor — 3.9
Task_Attributes — C.7.2
Task_Identification — C.7.1
Task_Termination — C.7.3
Standard (.continued)

Ada (.continued)

Text_IO — A.10.1
Bounded_IO — A.10.11
Complex_IO — G.1.3
Editing — F.3.3
Text_Streams — A.12.2
Unbounded_IO — A.10.12
Unchecked_Conversion — 13.9
Unchecked_Deallocate_Subpool — 13.11.5
Unchecked_Deallocation — 13.11.2
Wide_Characters — A.3.1
Handling — A.3.5
Wide_Command_Line — A.15.1
Wide_Directories — A.16.2
Wide_Environment_Variables — A.17.1
String (.continued)

Ada (.continued)

Strings (.continued)

Wide_Wide_Equal_Case_Insensitive
—— A.4.8
Wide_Wide_Fixed — A.4.8
Wide_Wide_Equal_Case_Insensitive
—— A.4.8
Wide_Wide_Hash — A.4.8
Wide_Wide_Hash_Case_Insensitive
—— A.4.8
Wide_Wide_Hash — A.4.8
Wide_Wide_Hash_Case_Insensitive
—— A.4.8
Wide_Wide_Maps — A.4.8
Wide_Wide_Constants — A.4.8
Wide_Wide_Unbounded — A.4.8
Wide_Wide_Equal_Case_Insensitive
—— A.4.8
Wide_Wide_Hash — A.4.8
Wide_Wide_Hash_Case_Insensitive
—— A.4.8
Synchronous_Barriers — D.10.1
Synchronous_Task_Control — D.10
EDF — D.10
Standard (.continued)

Ada (.continued)

Tags — 3.9
Generic_Dispatching_Constructor — 3.9
Task_Attributes — C.7.2
Task_Identification — C.7.1
Task_Termination — C.7.3
Standard (.continued)

Ada (.continued)

Text_IO — A.10.1
Bounded_IO — A.10.11
Complex_IO — G.1.3
Editing — F.3.3
Text_Streams — A.12.2
Unbounded_IO — A.10.12
Unchecked_Conversion — 13.9
Unchecked_Deallocate_Subpool — 13.11.5
Unchecked_Deallocation — 13.11.2
Wide_Characters — A.3.1
Handling — A.3.5
Wide_Command_Line — A.15.1
Wide_Directories — A.16.2
Wide_Environment_Variables — A.17.1
String (.continued)

Ada (.continued)

Strings (.continued)
Subpools — 13.11.4

2.a
Discussion: In running text, we generally leave out the “Ada.” when referring to a child of Ada.

2.b
Reason: We had no strict rule for which of Ada, Interfaces, or System should be the parent of a given library unit. However, we have tried to place as many things as possible under Ada, except that interfacing is a separate category, and we have tried to place library units whose use is highly nonportable under System.

Implementation Requirements

3/5
\{AI95-00434-01\} \{AI12-0052-1\} \{AI12-0114-1\} \{AI12-0200-1\} \{AI12-0439-1\} The implementation shall ensure that each language-defined subprogram is reentrant in the sense that concurrent calls on any two (possibly the same) language-defined subprograms perform as specified, so long as all pairs of objects (one from each call) that are either denoted by parameters that could be passed by reference, or are designated by parameters of an access type, denote nonoverlapping objects.

3.a.1/4
Ramification: \{AI12-0052-1\} \{AI12-0114-1\} So long as the parameters are disjoint, concurrent calls on the same language-defined subprogram, and concurrent calls on two different language-defined subprograms are required to work. But concurrent calls operating on overlapping objects (be they of the same or different language-defined subprograms) are not required to work (being an erroneous use of shared variables) unless both subprograms are required to pass the associated parameter by-copy.

3.a
For example, simultaneous calls to Text_IO.Put will work properly, so long as they are going to different two objects. On the other hand, simultaneous output to the same file constitutes erroneous use of shared variables.

3.b
To be honest: Here, “language defined subprogram” means a language defined library subprogram, a subprogram declared in the visible part of a language defined library package, an instance of a language defined generic library subprogram, or a subprogram declared in the visible part of an instance of a language defined generic library package.

3.b.1/4
Ramification: \{AI12-0052-1\} This rule applies to all language-defined subprograms, including those defined in packages that manage some global state (like environment variables or the current directory). Unless specified above, such subprograms need to work when the explicit parameters are not overlapping; in particular, the existence of the global state is not considered.

3.c/4
\{AI12-0052-1\} The rule implies that any data local to the private part or body of the package (including global state as described above) has to be somehow protected against simultaneous access.

3.1/4
\{AI12-0052-1\} \{AI12-0159-1\} For the purpose of determining whether concurrent calls on text input-output subprograms are required to perform as specified above, when calling a subprogram within Text_IO or its children that implicitly operates on one of the default input-output files, the subprogram is considered to have a parameter of Current_Input or Current_Output (as appropriate).

3.2/3
\{AI05-0048-1\} If a descendant of a language-defined tagged type is declared, the implementation shall ensure that each inherited language-defined subprogram behaves as described in this Reference Manual. In particular, overriding a language-defined subprogram shall not alter the effect of any inherited language-defined subprogram.

3.d/3
Reason: This means that internally the implementation must not do redispaching unless it is required by the Standard. So when we say that some subprogram Bar is equivalent to Foo, overriding Foo for a derived type doesn't change the semantics of Bar, and in particular it means that Bar may no longer be equivalent to Foo. The word “equivalent” is always a bit of a lie anyway.

Implementation Permissions

4
The implementation may restrict the replacement of language-defined compilation units. The implementation may restrict children of language-defined library units (other than Standard).

4.a
Ramification: For example, the implementation may say, “you cannot compile a library unit called System” or “you cannot compile a child of package System” or “if you compile a library unit called System, it has to be a package, and it has to contain at least the following declarations: ...”.

4.b/5
Ramification: \{AI12-0112-1\} Implementations are of course allowed to make changes to the specifications of language-defined units, so long as those changes are semantically neutral (that is, no program could change legality or effect because of the changes). In particular, an implementation can with additional units (especially implementation-defined units) so long as those units do not change the elaboration of the language-defined unit.
Similarly, an implementation can add postconditions to language-defined subprograms, so long as those postconditions always evaluate to True. This is useful if the implementation can use those postconditions for optimization.

Wording Changes from Ada 83

Many of Ada 83’s language-defined library units are now children of Ada or System. For upward compatibility, these are renamed as root library units (see J.1).

The order and lettering of the annexes has been changed.

Wording Changes from Ada 95

{8652/0047} {AI95-00081-01} Corrigendum: Units missing from the list of predefined units were added.

{AI95-00424-01} Added new units to the list of predefined units.

Wording Changes from Ada 2005

{AI05-0048-1} Correction: Added wording to ban redispatching unless it is explicitly required, in order to safeguard portability when overriding language-defined routines.

{AI05-0060-1} {AI05-0206-1} Correction: Added a permission to omit pragma Remote_Types from language-defined units if Annex E is not supported. This was later removed, as a better method of supporting the reason is now available. Note that this requires all implementations to provide minimal support for the Remote_Types categorization even if Annex E is not supported; being unable to compile language-defined units is not allowed.

{AI05-0001-1} {AI05-0049-1} {AI05-0113-1} {AI05-0136-1} {AI05-0137-1} {AI05-0166-1} {AI05-0168-1} Added various new units to the list of predefined units.

Incompatibilities With Ada 2012

{AI12-0005-1} When a new entity \( E \) is added to a package \( P \) that is used in client code, use clause conflicts are possible. Specifically, if \( P \) is referenced in a use_clause, and an entity \( F \) with the same defining identifier as \( E \) is defined in some other package that is also referenced in a use_clause, the user-defined entity \( F \) may no longer be use-visible, resulting in errors. This is an incompatibility when the new entity is added to a language-defined package. Note that use clause conflicts are rare and easily fixed by using an expanded name.

Wording Changes from Ada 2012

{AI12-0052-1} {AI12-0114-1} {AI12-0159-1} Correction: The rules requiring concurrent access of language-defined subprograms were expanded to include implicit Text_IO objects, overlapping objects designated by parameters of an access type, and simultaneous calls on different language-defined subprograms. While this might change behavior of some programs, it would do so by eliminating erroneous execution, so we don’t consider this an inconsistency.

{AI12-0200-1} Correction: The rules requiring concurrent access of language-defined subprograms were clarified further.

{AI12-0201-1} {AI12-0208-1} {AI12-0234-1} {AI12-0254-1} {AI12-0293-1} {AI12-0321-1} {AI12-0340-1} Added various new units to the list of predefined units.

A.1 The Package Standard

{AI05-0299-1} This subclause outlines the specification of the package Standard containing all predefined identifiers in the language. The corresponding package body is not specified by the language.

The operators that are predefined for the types declared in the package Standard are given in comments since they are implicitly declared. Italics are used for pseudo-names of anonymous types (such as root_real) and for undefined information (such as implementation-defined).

Ramification: All of the predefined operators are of convention Intrinsic.

Static Semantics

The library package Standard has the following declaration:

Implementation defined: The names and characteristics of the numeric subtypes declared in the visible part of package Standard.
The specification of each operator for the type Integer is obtained by replacing Integer by the name of the type root_integer, or for any additional predefined integer type, is obtained by replacing Integer by the name of the type.

The integer type root_integer and the corresponding universal type are predefined.

The predefined relational operators for this type are as follows:

- The predefined logical operators and the predefined logical negation operator are as follows:

The floating point type root_real and the corresponding universal type are predefined.

The integer type root_integer and the corresponding universal integer are predefined.

The predefined operators for type Integer are as follows:

- The specification of each operator for the type
- root_integer, or for any additional predefined integer
type, is obtained by replacing Integer by the name of the type
- in the specification of the corresponding operator of the type
- Integer. The right operand of the exponentiation operator
- remains as subtype Natural.

The predefined operators for this type are as follows:

- The floating point type root_real and their predefined.

The corresponding universal type universal_real are predefined.

The predefined operators for this type are as follows:
-- function "+" (Right : Float) return Float;
-- function "-" (Right : Float) return Float;
-- function "abs" (Right : Float) return Float;
-- function "+" (Left, Right : Float) return Float;
-- function "+" (Left, Right : Float) return Float;
-- function "+" (Left, Right : Float) return Float;
-- function "+" (Left, Right : Float) return Float;
-- function "+" (Left : Float; Right : Integer'Base) return Float;
-- The specification of each operator for the type root_real, or for
-- any additional predefined floating point type, is obtained by
-- replacing Float by the name of the type in the specification of the
-- corresponding operator of the type Float.
-- In addition, the following operators are predefined for the root
-- numeric types:
function "*" (Left : root_integer; Right : root_real)
return root_real;
function "*" (Left : root_real; Right : root_integer)
return root_real;
function "/" (Left : root_real; Right : root_integer)
return root_real;
-- The type universal_fixed is predefined.
-- The only multiplying operators defined between
-- fixed point types are
function "+" (Left : universal_fixed; Right : universal_fixed)
return universal_fixed;
function "+" (Left : universal_fixed; Right : universal_fixed)
return universal_fixed;

{AI95-00230-01} -- The type universal_access is predefined.
function "+" (Left, Right: universal_access) return Boolean;
function "+" (Left, Right: universal_access) return Boolean;

35/3

-- The declaration of type Character is based on the standard ISO 8859-1 character set.
-- They are indicated in italics in this definition. See 3.5.2.

**type** Character is
(nul, soh, stx, etx, cot, enq, ack, bel, -0 (16#00h) .. 7 (16#07h)
bs, ht, lf, vt, ff, cr, so, si, -8 (16#08h) .. 15 (16#0Fh)
dle, dc1, dc2, dc3, dc4, nak, syn, etb, -16 (16#10h) .. 23 (16#17h)
can, em, sub, esc, fs, gs, rs, us, -24 (16#18h) .. 31 (16#1Fh)
'0' .. '9', 'a' .. 'z', '{', '|', '}', '~', 'p' .. 't', 'u' .. 'z', -32 (16#20h) .. 39 (16#27h)
'ü', 'v', 'w', 'x', 'y', 'z', '{', '|', '}', '~', -40 (16#28h) .. 47 (16#2Fh)

There are no character literals corresponding to the positions for control characters.

-- The predefined operators for the type Character are the same as for any enumeration type.

36.1/5

-- The declaration of type Wide_Character is based on the standard ISO/IEC 10646-2020/201202 BMP character set.
-- See: The first 256 positions have the same contents as type Character. See 3.5.2.

**type** Wide_Character is (nul, soh ... Hex 0000FFFEFE, Hex 0000FFFEFEFE);
The declaration of type Wide_Wide_Character is based on the full ISO/IEC 10646:2020/2011 character set. The first 65536 positions have the same contents as type Wide_Character. See 3.5.2.

```ada
type Wide_Wide_Character is (nul, soh ... Hex 7FFFFFFE, Hex 7FFFFFFF);
for Wide_Wide_Character'Size use 32;
package ASCII is ... end ASCII; -- Obsolescent; see J.5
```

Predefined string types:

```ada
type String is array(Positive range <>) of Character
  with Pack;
pragma Pack(String);
-- The predefined operators for this type are as follows:
-- function "=" (Left, Right: String) return Boolean;
-- function "/=" (Left, Right: String) return Boolean;
-- function "+=" (Left, Right: String) return Boolean;
-- function ">=" (Left, Right: String) return Boolean;
-- function ">" (Left: String; Right: String) return String;
-- function "+" (Left: Character; Right: String) return String;
-- function "+" (Left: String; Right: Character) return String;
```

```ada
type Wide_String is array(Positive range <>) of Wide_Character
  with Pack;
pragma Pack(Wide_String);
-- The predefined operators for this type correspond to those for String.
```

```ada
type Wide_Wide_String is array(Positive range <>) of Wide_Wide_Character
  with Pack;
pragma Pack (Wide_Wide_String);
{AI95-00285-01} -- The predefined operators for this type correspond to those for String.
```

```ada
type Duration is delta implementation-defined range implementation-defined;
  -- The predefined operators for the type Duration are the same as for
  -- any fixed point type.
  -- The predefined exceptions:
Constraint_Error: exception;
Program_Error : exception;
Storage_Error : exception;
Tasking_Error : exception;
end Standard;
```

Standard has no private part.

Reason: This is important for portability. All library packages are children of Standard, and if Standard had a private part then it would be visible to all of them.
Dynamic Semantics

Elaboration of the body of Standard has no effect.

Discussion: Note that the language does not define where this body appears in the environment declarative_part — see 10, “Program Structure and Compilation Issues”.

Implementation Permissions

An implementation may provide additional predefined integer types and additional predefined floating point types. Some or not all of these types may be anonymous.

To be honest: An implementation may add representation items to package Standard, for example to specify the internal codes of type Boolean, or the Small of type Duration.

Implementation Advice

If an implementation provides additional named predefined integer types, then the names should end with “Integer” as in “Long_Integer”. If an implementation provides additional named predefined floating point types, then the names should end with “Float” as in “Long_Float”.

NOTE 1 Certain aspects of the predefined entities cannot be completely described in the language itself. For example, although the enumeration type Boolean can be written showing the two enumeration literals False and True, the short-circuit control forms cannot be expressed in the language.

NOTE 2 As explained in 8.1, “Declarative Region” and 10.1.4, “The Compilation Process”, the declarative region of the package Standard encloses every library unit and consequently the main subprogram; the declaration of every library unit is assumed to occur within this declarative region. Library items are assumed to be ordered in such a way that there are no forward semantic dependences. However, as explained in 8.3, “Visibility”, the only library units that are visible within a given compilation unit are the library units named by all with_clauses that apply to the given unit, and moreover, within the declarative region of a given library unit, that library unit itself.

NOTE 3 If all block statements of a program are named, then the name of each program unit can always be written as an expanded name starting with Standard (unless Standard is itself hidden). The name of a library unit cannot be a homograph of a name (such as Integer) that is already declared in Standard.

NOTE 4 The exception Standard.Numeric_Error is defined in J.6.

Discussion: The declaration of Natural needs to appear between the declaration of Integer and the (implicit) declaration of the "**" operator for Integer, because a formal parameter of "**" is of subtype Natural. This would be impossible in normal code, because the implicit declarations for a type occur immediately after the type declaration, with no possibility of intervening explicit declarations. But we're in Standard, and Standard is somewhat magic anyway.

Using Natural as the subtype of the formal of "**" seems natural; it would be silly to have a textual rule about Constraint_Error being raised when there is a perfectly good subtype that means just that. Furthermore, by not using Integer for that formal, it helps remind the reader that the exponent remains Natural even when the left operand is replaced with the derivative of Integer. It doesn't logically imply that, but it's still useful as a reminder.

In any case, declaring these general-purpose subtypes of Integer close to Integer seems more readable than declaring them much later.

Extensions to Ada 83

Package Standard is declared to be pure.

Discussion: The introduction of the types Wide_Character and Wide_String is not an Ada 95 extension to Ada 83, since ISO WG9 has approved these as an authorized extension of the original Ada 83 standard that is part of that standard.

Wording Changes from Ada 83

Numeric_Error is made obsolescent.

The declarations of Natural and Positive are moved to just after the declaration of Integer, so that "**" can refer to Natural without a forward reference. There's no real need to move Positive, too — it just came along for the ride.
Extensions to Ada 95

{AI95-00285-01} Types Wide_Character and Wide_String are new.

**Discussion:** The inconsistencies associated with these types are documented in 3.5.2 and 3.6.3.

{AI95-00230-01} Type universal_access and the equality operations for it are new.

Wording Changes from Ada 95

{8652/0028} {AI95-00145-01} **Corrigendum:** Corrected the parameter type for the Boolean operators declared in Standard.

Wording Changes from Ada 2005

{AI05-0181-1} **Correction:** Since soft_hyphen (position 173) is defined to be nongraphic, gave it a name.

**Discussion:** The inconsistencies associated with this change are documented in 3.5.

A.2 The Package Ada

**Static Semantics**

The following language-defined library package exists:

{AI12-0414-1} package Ada is
with pragma Pure is (Ada);
end Ada;

{AI12-0414-1} Ada serves as the parent of most of the other language-defined library units; its declaration is empty (except for the pragma Pure).

**Legality Rules**

In the standard mode, it is illegal to compile a child of package Ada.

**Reason:** The intention is that mentioning, say, Ada.Text_IO in a with_clause is guaranteed (at least in the standard mode) to refer to the standard version of Ada.Text_IO. The user can compile a root library unit Text_IO that has no relation to the standard version of Text_IO.

**Ramification:** Note that Ada can have non-language-defined grandchildren, assuming the implementation allows it. Also, packages System and Interfaces can have children, assuming the implementation allows it.

**Implementation Note:** An implementation will typically support a nonstandard mode in which compiling the language defined library units is allowed. Whether or not this mode is made available to users is up to the implementer.

An implementation could theoretically have private children of Ada, since that would be semantically neutral. However, a programmer cannot compile such a library unit.

**Extensions to Ada 83**

{AI05-0299-1} This subclause is new to Ada 95.

A.3 Character Handling

{AI95-00285-01} {AI05-0243-1} {AI05-0299-1} This subclause presents the packages related to character processing: an empty declared pure package Characters and child packages Characters.Handling and Characters.Latin_1. The package Characters.Handling provides classification and conversion functions for Character data, and some simple functions for dealing with Wide_Character and Wide_Wide_Character data. The child package Characters.Latin_1 declares a set of constants initialized to values of type Character.

**Extensions to Ada 83**

{AI05-0299-1} This subclause is new to Ada 95.
The library package Characters has the following declaration:

```ada
package Ada.Characters is
with pragma Pure is (Characters);
end Ada.Characters;
```

The library package Wide_Characters has the following declaration:

```ada
package Ada.Wide_Characters is
with pragma Pure is (Wide_Characters);
end Ada.Wide_Characters;
```

The library package Wide_Wide_Characters has the following declaration:

```ada
package Ada.Wide_Wide_Characters is
with pragma Pure is (Wide_Wide_Characters);
end Ada.Wide_Wide_Characters;
```

Implementation Advice

If an implementation chooses to provide implementation-defined operations on Wide_Character or Wide_String (such as case mapping, classification, collating and sorting, etc.) it should do so by providing child units of Wide_Characters. Similarly if it chooses to provide implementation-defined operations on Wide_Wide_Character or Wide_Wide_String it should do so by providing child units of Wide_Wide_Characters.

Implementation Advice: Implementation-defined operations on Wide_Character, Wide_String, Wide_Wide_Character, and Wide_Wide_String should be child units of Wide_Characters or Wide_Wide_Characters.

The packages Wide_Characters and Wide_Wide_Characters are new.

The library package Characters.Handling has the following declaration:

```ada
package Ada.Characters.Handling is
with pragma Pure Preelaborate is (Handling);
```

Extensions to Ada 95

The packages Wide_Characters and Wide_Wide_Characters are new.
--Character classification functions

[A12-0004-1]  {AI12-0185-1}  function Is_Control (Item : in Character) return Boolean;
  function Is_Graphic (Item : in Character) return Boolean;
  function Is_Letter (Item : in Character) return Boolean;
  function Is_Lower (Item : in Character) return Boolean;
  function Is_Upper (Item : in Character) return Boolean;
  function Is_Digit (Item : in Character) return Boolean;
  function Is_Decimal_Digit (Item : in Character) return Boolean;

renames Is_Digit;

function Is_Hexadecimal_Digit (Item : in Character) return Boolean;
function Is_Alphanumeric (Item : in Character) return Boolean;
function Is_Special (Item : in Character) return Boolean;
function Is_Other_Format (Item : in Character) return Boolean;
function Is_Punctuation_Connector (Item : in Character) return Boolean;
function Is_Space (Item : in Character) return Boolean;
function Is_NFKC (Item : in Character) return Boolean;

--Conversion functions for Character and String

function To_Lower (Item : in Character) return Character;
function To_Upper (Item : in Character) return Character;
function To_Basic (Item : in Character) return Character;
function To_Lower (Item : in String) return String;
function To_Upper (Item : in String) return String;
function To_Basic (Item : in String) return String;

--Classifications of and conversions between Character and ISO 646

subtype ISO_646 is
  Character range Character'Val(0) .. Character'Val(127);

function Is_ISO_646 (Item : in Character) return Boolean;
function To_ISO_646 (Item : in String) return Boolean;
function To_ISO_646 (Item : in Character;
  Substitute : in ISO_646 := ' ')
  return ISO_646;

function To_ISO_646 (Item : in String;
  Substitute : in ISO_646 := ' ')
  return String;

{AI95-00285-01}  {AI95-00395-01}  -- The functions Is_Character, Is_String, To_Character, To_String,
To_Wide_Character, Classifications of and conversions between Wide_Character and Character.
-- and To_Wide_String are obsolete; see J.14.

Paraphrages 14 through 18 were deleted.

{AI95-00395-01}  --function To_Character (Item : in Wide_Character) return Boolean;

{AI95-00395-01}  --function To_String (Item : in String) return Boolean;

{AI95-00395-01}  --function To_Character (Item : in Wide_Character;
  Substitute : in Character := ' ')

  return Character;

{AI95-00395-01}  --function To_String (Item : in String;
  Substitute : in Character := ' ')

  return String;

{AI95-00395-01}  --function To_Wide_Character (Item : in Character) return
Wide_Character;

{AI95-00395-01}  --function To_Wide_String (Item : in String) return
Wide_String;

end Ada.Characters.Handling;

Discussion:  [AI95-00395-01] The with clause for Ada.Characters.Conversions is needed for the definition of the
obsolete functions (see J.14). It would be odd to put this clause into J.14 as it was not present in Ada 95, and
with clauses are semantically neutral to clients anyway.
In the description below for each function that returns a Boolean result, the effect is described in terms of
the conditions under which the value True is returned. If these conditions are not met, then the function
returns False.

Each of the following classification functions has a formal Character parameter, Item, and returns a
Boolean result.

**Is_Control**  
True if Item is a control character. A *control character* is a character whose position is in one
of the ranges 0..31 or 127..159.

**Is_Graphic**  
True if Item is a graphic character. A *graphic character* is a character whose position is in
one of the ranges 32..126 or 160..255.

**Is_Letter**  
True if Item is a letter. A *letter* is a character that is in one of the ranges 'A'..'Z' or 'a'..'z', or
whose position is in one of the ranges 192..214, 216..246, or 248..255.

**Is_Lower**  
True if Item is a lower-case letter. A *lower-case letter* is a character that is in the range 'a'..'z',
or whose position is in one of the ranges 223..246 or 248..255.

**Is_Upper**  
True if Item is an upper-case letter. An *upper-case letter* is a character that is in the range
'A'..'Z' or whose position is in one of the ranges 192..214 or 216..222.

**Is_Basic**  
True if Item is a basic letter. A *basic letter* is a character that is in one of the ranges 'A'..'Z'
and 'a'..'z', or that is one of the following: 'Æ', 'æ', 'Ð', 'ð', 'Þ', 'þ', or 'ß'.

**Is_Digit**  
True if Item is a decimal digit. A *decimal digit* is a character in the range '0'..'9'.

**Is_Decimal_Digit**  
A renaming of Is_Digit.

**Is_Hexadecimal_Digit**  
True if Item is a hexadecimal digit. A *hexadecimal digit* is a character that is either a decimal
digit or that is in one of the ranges 'A'..'F' or 'a'..'f'.

**Is_Alphanumeric**  
True if Item is an alphanumeric character. An *alphanumeric character* is a character that is
either a letter or a decimal digit.

**Is_Special**  
True if Item is a special graphic character. A *special graphic character* is a graphic character
that is not alphanumeric.
Each of the names To_Lower, To_Upper, and To_Basic refers to two functions: one that converts from Character to Character, and the other that converts from String to String. The result of each Character-to-Character function is described below, in terms of the conversion applied to Item, its formal Character parameter. The result of each String-to-String conversion is obtained by applying to each element of the function's String parameter the corresponding Character-to-Character conversion; the result is the null String if the value of the formal parameter is the null String. The lower bound of the result String is 1.

To_Lower    Returns the corresponding lower-case value for Item if Is_Upper(Item), and returns Item otherwise.

To_Upper    Returns the corresponding upper-case value for Item if Is_Lower(Item) and Item has an upper-case form, and returns Item otherwise. The lower case letters 'ß' and 'ÿ' do not have upper case forms.

To_Basic    Returns the letter corresponding to Item but with no diacritical mark, if Item is a letter but not a basic letter; returns Item otherwise.

The following set of functions test for membership in the ISO 646 character range, or convert between ISO 646 and Character.

Is_ISO_646
The function whose formal parameter, Item, is of type Character returns True if Item is in the subtype ISO_646.

Is_ISO_646
The function whose formal parameter, Item, is of type String returns True if Is_ISO_646(Item(I)) is True for each I in Item'Range.

To_ISO_646
The function whose first formal parameter, Item, is of type Character returns Item if Is_ISO_646(Item), and returns the Substitute ISO_646 character otherwise.

To_ISO_646
The function whose first formal parameter, Item, is of type String returns the String whose Range is 1..Item'Length and each of whose elements is given by To_ISO_646 of the corresponding element in Item.

Paragraphs 42 through 49 were deleted.

The following set of functions test Wide_Character values for membership in Character, or convert between corresponding characters of Wide_Character and Character.

Is_Character
Returns True if Wide_Character'Pos(Item) <= Character'Pos(Character'Last).

Is_String
Returns True if Is_Character(Item(I)) is True for each I in Item'Range.

To_Character
Returns the Character corresponding to Item if Is_Character(Item), and returns the Substitute Character otherwise.

To_String
Returns the String whose range is 1..Item'Length and each of whose elements is given by To_Character of the corresponding element in Item.
A.3.2 The Package Characters.Handling

\{AI95-00285-01\} \{AI95-00395-01\} To_Wide_Character

Returns the Wide_Character X such that Character'Pos(Item) = Wide_Character'Pos(X).

\{AI95-00285-01\} \{AI95-00395-01\} To_Wide_String

Returns the Wide_String whose range is 1..Item'Length and each of whose elements is given by To_Wide_Character of the corresponding element in Item.

Implementation Advice

\{AI95-00285-01\} \{AI95-00395-01\} If an implementation provides a localized definition of Character or Wide_Character, then the effects of the subprograms in Characters.Handling should reflect the localizations. See also 3.5.2.

NOTE 1 A basic letter is a letter without a diacritical mark.

NOTE 2 Except for the hexadecimal digits, basic letters, and ISO_646 characters, the categories identified in the classification functions form a strict hierarchy:

- Control characters
- Graphic characters
  - Alphanumeric characters
    - Letters
      - Upper-case letters
      - Lower-case letters
    - Decimal digits
  - Special graphic characters

Ramification: Thus each Character value is either a control character or a graphic character but not both; each graphic character is either an alphanumeric or special graphic but not both; each alphanumeric is either a letter or decimal digit but not both; each letter is either upper case or lower case but not both.

NOTE 3 \{AI05-0114-1\} There are certain characters which are defined to be lower case letters by ISO 10646 and are therefore allowed in identifiers, but are not considered lower case letters by Ada.Characters.Handling.

Reason: This is to maintain runtime compatibility with the Ada 95 definitions of these functions. We don't list the exact characters involved because they're likely to change in future character set standards; the list for ISO 10646:2011 can be found in AI05-0114-1.

Ramification: No version of Characters.Handling is intended to do portable (Ada-version independent) manipulation of Ada identifiers. The classification given by Wide_Characters.Handling will be correct for the current implementation for Ada 2012 identifiers, but it might not be correct for a different implementation or version of Ada.

Extensions to Ada 95

\{AI95-00362-01\} Characters.Handling is now Pure, so it can be used in pure units.

Incompatibilities With Ada 2005

\{AI05-0185-1\} Added additional classification routines so that Characters.Handling has all of the routines available in Wide_Characters.Handling. If Characters.Handling is referenced in a use_clause, and an entity E with a defining_identifier that is the same as one of the new functions is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Wording Changes from Ada 95

\{AI95-00285-01\} \{AI95-00395-01\} The conversion functions are made obsolescent; a more complete set is available in Characters.Conversions — see A.3.4.

\{AI95-00285-01\} \{AI05-0248-1\} We no longer talk about localized character sets; these are a nonstandard mode, which is none of our business.

Wording Changes from Ada 2005

\{AI05-0114-1\} Correction: Added a note to clarify that these functions don't have any relationship to the characters allowed in identifiers.
A.3.3 The Package Characters.Latin_1

The package Characters.Latin_1 declares constants for characters in ISO 8859-1.

**Reason:** The constants for the ISO 646 characters could have been declared as renamings of objects declared in package ASCII, as opposed to explicit constants. The main reason for explicit constants was for consistency of style with the upper-half constants, and to avoid emphasizing the package ASCII.

**Static Semantics**

The library package Characters.Latin_1 has the following declaration:

```ada
package Ada.Characters.Latin_1 is
  with pragma Pure (Latin_1);
  -- Control characters:
  NUL : constant Character := Character'Val(0);
  SOH : constant Character := Character'Val(1);
  STX : constant Character := Character'Val(2);
  ETX : constant Character := Character'Val(3);
  EOT : constant Character := Character'Val(4);
  ENQ : constant Character := Character'Val(5);
  ACK : constant Character := Character'Val(6);
  BEL : constant Character := Character'Val(7);
  BS  : constant Character := Character'Val(8);
  HT  : constant Character := Character'Val(9);
  LF  : constant Character := Character'Val(10);
  VT  : constant Character := Character'Val(11);
  FF  : constant Character := Character'Val(12);
  CR  : constant Character := Character'Val(13);
  SO  : constant Character := Character'Val(14);
  SI  : constant Character := Character'Val(15);
  DLE : constant Character := Character'Val(16);
  DC1 : constant Character := Character'Val(17);
  DC2 : constant Character := Character'Val(18);
  DC3 : constant Character := Character'Val(19);
  DC4 : constant Character := Character'Val(20);
  NAK : constant Character := Character'Val(21);
  SYN : constant Character := Character'Val(22);
  ETB : constant Character := Character'Val(23);
  CAN : constant Character := Character'Val(24);
  EM  : constant Character := Character'Val(25);
  SUB : constant Character := Character'Val(26);
  ESC : constant Character := Character'Val(27);
  FS  : constant Character := Character'Val(28);
  GS  : constant Character := Character'Val(29);
  RS  : constant Character := Character'Val(30);
  US  : constant Character := Character'Val(31);
```


7
8

-- ISO 646 graphic characters:
Space
Exclamation
Quotation
Number_Sign
Dollar_Sign
Percent_Sign
Ampersand
Apostrophe
Left_Parenthesis
Right_Parenthesis
Asterisk
Plus_Sign
Comma
Hyphen
Minus_Sign
Full_Stop
Solidus

:
:
:
:
:
:
:
:
:
:
:
:
:
:
:
:
:

constant Character := ' ';
constant Character := '!';
constant Character := '"';
constant Character := '#';
constant Character := '$';
constant Character := '%';
constant Character := '&';
constant Character := ''';
constant Character := '(';
constant Character := ')';
constant Character := '*';
constant Character := '+';
constant Character := ',';
constant Character := '-';
Character renames Hyphen;
constant Character := '.';
constant Character := '/';

9

-- Decimal digits '0' though '9' are at positions 48 through 57

10

Colon
Semicolon
Less_Than_Sign
Equals_Sign
Greater_Than_Sign
Question
Commercial_At

11

-- Letters 'A' through 'Z' are at positions 65 through 90

12

Left_Square_Bracket
Reverse_Solidus
Right_Square_Bracket
Circumflex
Low_Line

:
:
:
:
:

constant
constant
constant
constant
constant

13

Grave
LC_A
LC_B
LC_C
LC_D
LC_E
LC_F
LC_G
LC_H
LC_I
LC_J
LC_K
LC_L
LC_M
LC_N
LC_O

:
:
:
:
:
:
:
:
:
:
:
:
:
:
:
:

14

LC_P
LC_Q
LC_R
LC_S
LC_T
LC_U
LC_V
LC_W
LC_X
LC_Y
LC_Z
Left_Curly_Bracket
Vertical_Line
Right_Curly_Bracket
Tilde
DEL

:
:
:
:
:
:
:
:
:
:
:
:
:
:
:
:

:
:
:
:
:
:
:

A.3.3 The Package Characters.Latin_1

-- Character'Val(32)
-- Character'Val(33)
-- Character'Val(34)
-- Character'Val(35)
-- Character'Val(36)
-- Character'Val(37)
-- Character'Val(38)
-- Character'Val(39)
-- Character'Val(40)
-- Character'Val(41)
-- Character'Val(42)
-- Character'Val(43)
-- Character'Val(44)
-- Character'Val(45)
-- Character'Val(46)
-- Character'Val(47)

:=
:=
:=
:=
:=
:=
:=

':';
';';
'<';
'=';
'>';
'?';
'@';

-- Character'Val(58)
-- Character'Val(59)
-- Character'Val(60)
-- Character'Val(61)
-- Character'Val(62)
-- Character'Val(63)
-- Character'Val(64)

Character
Character
Character
Character
Character

:=
:=
:=
:=
:=

'[';
'\';
']';
'^';
'_';

-- Character'Val(91)
-- Character'Val(92)
-- Character'Val(93)
-- Character'Val(94)
-- Character'Val(95)

constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant

Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character

:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=

'`';
'a';
'b';
'c';
'd';
'e';
'f';
'g';
'h';
'i';
'j';
'k';
'l';
'm';
'n';
'o';

-- Character'Val(96)
-- Character'Val(97)
-- Character'Val(98)
-- Character'Val(99)
-- Character'Val(100)
-- Character'Val(101)
-- Character'Val(102)
-- Character'Val(103)
-- Character'Val(104)
-- Character'Val(105)
-- Character'Val(106)
-- Character'Val(107)
-- Character'Val(108)
-- Character'Val(109)
-- Character'Val(110)
-- Character'Val(111)

constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant
constant

Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character
Character

:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=
:=

'p'; -- Character'Val(112)
'q'; -- Character'Val(113)
'r'; -- Character'Val(114)
's'; -- Character'Val(115)
't'; -- Character'Val(116)
'u'; -- Character'Val(117)
'v'; -- Character'Val(118)
'w'; -- Character'Val(119)
'x'; -- Character'Val(120)
'y'; -- Character'Val(121)
'z'; -- Character'Val(122)
'{'; -- Character'Val(123)
'|'; -- Character'Val(124)
'}'; -- Character'Val(125)
'~'; -- Character'Val(126)
Character'Val(127);

constant
constant
constant
constant
constant
constant
constant

Character
Character
Character
Character
Character
Character
Character

16 October 2023

804


-- ISO 6429 control characters:

- Reserved_128 : constant Character := Character'Val(128);
- Reserved_129 : constant Character := Character'Val(129);
- BPH : constant Character := Character'Val(130);
- NBH : constant Character := Character'Val(131);
- Reserved_132 : constant Character := Character'Val(132);
- NEL : constant Character := Character'Val(133);
- SSA : constant Character := Character'Val(134);
- ESA : constant Character := Character'Val(135);
- HTS : constant Character := Character'Val(136);
- HTJ : constant Character := Character'Val(137);
- VTS : constant Character := Character'Val(138);
- FLD : constant Character := Character'Val(139);
- PLU : constant Character := Character'Val(140);
- RI : constant Character := Character'Val(141);
- SS2 : constant Character := Character'Val(142);
- SS3 : constant Character := Character'Val(143);
- DCS : constant Character := Character'Val(144);
- PU1 : constant Character := Character'Val(145);
- PU2 : constant Character := Character'Val(146);
- STS : constant Character := Character'Val(147);
- CCH : constant Character := Character'Val(148);
- MW : constant Character := Character'Val(149);
- SPA : constant Character := Character'Val(150);
- EPA : constant Character := Character'Val(151);
- SOS : constant Character := Character'Val(152);
- Reserved_153 : constant Character := Character'Val(153);
- SCI : constant Character := Character'Val(154);
- CSI : constant Character := Character'Val(155);
- ST : constant Character := Character'Val(156);
- OSC : constant Character := Character'Val(157);
- PM : constant Character := Character'Val(158);
- APC : constant Character := Character'Val(159);

-- Other graphic characters:

- No_Break_Space : constant Character := ' '; -- Character'Val(160)
- Inverted_Exclamation : constant Character := '¡'; -- Character'Val(161)
- Cent_Sign : constant Character := '¢'; -- Character'Val(162)
- Pound_Sign : constant Character := '£'; -- Character'Val(163)
- Currency_Sign : constant Character := '€'; -- Character'Val(164)
- Yen_Sign : constant Character := '¥'; -- Character'Val(165)
- Broken_Bar : constant Character := '¦'; -- Character'Val(166)
- Section_Sign : constant Character := '§'; -- Character'Val(167)
- Diaeresis : constant Character := '¨'; -- Character'Val(168)
- Copyright_Sign : constant Character := '©'; -- Character'Val(169)
- Feminine_Ordinal_Indicator : constant Character := 'ª'; -- Character'Val(170)
- Left_Angle_Quotation : constant Character := '«'; -- Character'Val(171)
- Not_Sign : constant Character := '¬'; -- Character'Val(172)
- Registered_Trade_Mark_Sign : constant Character := '®'; -- Character'Val(174)
- Macron : constant Character := '¯'; -- Character'Val(175)
A.3.3  The Package Characters.Latin_1
-- Character positions 224 (16#E0#) .. 239 (16#EF#):

LC_A_Grave : constant Character := 'à'; -- Character'Val(224)
LC_A_Acute : constant Character := 'á'; -- Character'Val(225)
LC_A_Circumflex : constant Character := 'â'; -- Character'Val(226)
LC_A_Tilde : constant Character := 'ã'; -- Character'Val(227)
LC_A_Diaeresis : constant Character := 'ä'; -- Character'Val(228)
LC_A_Ring : constant Character := 'å'; -- Character'Val(229)
LC_AE_Diphthong : constant Character := 'æ'; -- Character'Val(230)
LC_C_Cedilla : constant Character := 'ç'; -- Character'Val(231)
LC_E_Grave : constant Character := 'è'; -- Character'Val(232)
LC_E_Acute : constant Character := 'é'; -- Character'Val(233)
LC_E_Circumflex : constant Character := 'ê'; -- Character'Val(234)
LC_E_Diaeresis : constant Character := 'ë'; -- Character'Val(235)
LC_I_Grave : constant Character := 'ì'; -- Character'Val(236)
LC_I_Acute : constant Character := 'í'; -- Character'Val(237)
LC_I_Circumflex : constant Character := 'î'; -- Character'Val(238)
LC_I_Diaeresis : constant Character := 'ï'; -- Character'Val(239)

-- Character positions 240 (16#F0#) .. 255 (16#FF#):

LC_Icelandic_Eth : constant Character := 'ð'; -- Character'Val(240)
LC_N_Tilde : constant Character := 'ñ'; -- Character'Val(241)
LC_O_Grave : constant Character := 'ò'; -- Character'Val(242)
LC_O_Acute : constant Character := 'ó'; -- Character'Val(243)
LC_O_Circumflex : constant Character := 'ô'; -- Character'Val(244)
LC_O_Tilde : constant Character := 'õ'; -- Character'Val(245)
LC_O_Diaeresis : constant Character := 'ö'; -- Character'Val(246)
Division_Sign : constant Character := '÷'; -- Character'Val(247)
LC_O_Oblique_Stroke : constant Character := 'ø'; -- Character'Val(248)
LC_U_Grave : constant Character := 'ù'; -- Character'Val(249)
LC_U_Acute : constant Character := 'ú'; -- Character'Val(250)
LC_U_Circumflex : constant Character := 'û'; -- Character'Val(251)
LC_U_Diaeresis : constant Character := 'ü'; -- Character'Val(252)
LC_Y_Acute : constant Character := 'ý'; -- Character'Val(253)
LC_Icelandic_Thorn : constant Character := 'þ'; -- Character'Val(254)
LC_Y_Diaeresis : constant Character := 'ÿ'; -- Character'Val(255)

end Ada.Characters.Latin_1;

Implementation Permissions

An implementation may provide additional packages as children of Ada.Characters, to declare names for the symbols of the local character set or other character sets.

Wording Changes from Ada 2005

{AI05-0181-1} Correction: Soft_Hyphen is not a graphic character, and thus a character literal for it is illegal. So we have to use the position value. This makes no semantic change to users of the constant.

A.3.4 The Package Characters.Conversions

Static Semantics

{AI95-00395-01} The library package Characters.Conversions has the following declaration:

{AI12-0414-1} package Ada.Characters.Conversions is
withpragma Pure is (Conversions);

function Is_Character (Item : in Wide_Character) return Boolean;
function Is_String (Item : in Wide_String) return Boolean;
function Is_Character (Item : in Wide_Wide_Character) return Boolean;
function Is_Wide_Character (Item : in Wide_Wide_Character) return Boolean;
function Is_Wide_String (Item : in Wide_Wide_String) return Boolean;

end Ada.Characters.Conversions;
function To_Wide_Character (Item : in Character) return Wide_Character;
function To_Wide_String  (Item : in String)  return Wide_String;
function To_Wide_Wide_Character (Item : in Character)
    return Wide_Wide_Character;
function To_Wide_Wide_String (Item : in String)
    return Wide_Wide_String;
function To_Wide_Wide_Character (Item : in Wide_Character)
    return Wide_Wide_Character;
function To_Wide_Wide_String (Item : in Wide_String)
    return Wide_Wide_String;
function To_Character (Item       : in Wide_Character;
    Substitute : in Character := ' ') return Character;
function To_String    (Item       : in Wide_String;
    Substitute : in Character := ' ') return String;
function To_Character (Item : in Wide_Wide_Character;
    Substitute : in Character := ' ') return Character;
function To_String    (Item : in Wide_Wide_String;
    Substitute : in Character := ' ') return String;
function To_Wide_Character (Item : in Wide_Wide_Character;
    Substitute : in Wide_Character := ' ') return Wide_Character;
function To_Wide_String (Item : in Wide_Wide_String;
    Substitute : in Wide_Character := ' ') return Wide_String;

end Ada.Characters.Conversions;

{AI95-00395-01} The functions in package Characters.Conversions test Wide_Wide_Character or
Wide_Character values for membership in Wide_Character or Character, or convert between
corresponding characters of Wide_Character, Wide_Character, and Character.

function Is_Character (Item : in Wide_Character) return Boolean;
{AI95-00395-01} Returns True if Wide_Character'Pos(Item) <= Character'Pos(Character'Last).

function Is_Character (Item : in Wide_Wide_Character) return Boolean;
{AI95-00395-01} Returns True if Is_Character(Item(I)) is True for each I in Item'Range.

function Is_Wide_Character (Item : in Wide_Wide_Character) return Boolean;
{AI95-00395-01} Returns True if Wide_Wide_Character'Pos(Item) <=
Wide_Character'Pos(Wide_Character'Last).

function Is_String (Item : in Wide_String) return Boolean;
function Is_String (Item : in Wide_Wide_String) return Boolean;
{AI95-00395-01} Returns True if Is_Character(Item(I)) is True for each I in Item'Range.

function Is_Wide_String (Item : in Wide_String) return Boolean;
{AI95-00395-01} Returns True if Is_Wide_Character(Item(I)) is True for each I in Item'Range.

function To_Character (Item : in Wide_Character;
    Substitute : in Character := ' ') return Character;
function To_Character (Item : in Wide_Character;
    Substitute : in Character := ' ') return Character;
{AI95-00395-01} Returns the Character corresponding to Item if Is_Chara
ter(Item), and returns
the Substitute Character otherwise.

function To_Wide_Character (Item : in Character) return Wide_Character;
The package `Characters.Conversions` is new, replacing functions previously found in `Characters.Handling`.

## A.3.5 The Package `Wide_Characters.Handling`

The `Wide_Characters.Handling` package provides operations for classifying `Wide_Characters` and case folding for `Wide_Characters`. 
Static Semantics

{AI05-0185-1} The library package Wide_Characters.Handling has the following declaration:

```ada
package Ada.Wide_Characters.Handling is
  withpragma Pure is (Handling);

  function Character_Set_Version return String;
  function Is_Control (Item : Wide_Character) return Boolean;
  function Is_Letter (Item : Wide_Character) return Boolean;
  function Is_Lower (Item : Wide_Character) return Boolean;
  function Is_Upper (Item : Wide_Character) return Boolean;

  function Is_Basic (Item : Wide_Character) return Boolean;
  function Is_Digit (Item : Wide_Character) return Boolean;
  function Is_Decimal_Digit (Item : Wide_Character) return Boolean;
  function Is_Hexadecimal_Digit (Item : Wide_Character) return Boolean;
  function Is_Alphanumeric (Item : Wide_Character) return Boolean;
  function Is_Special (Item : Wide_Character) return Boolean;
  function Is_Line_Terminator (Item : Wide_Character) return Boolean;
  function Is_Mark (Item : Wide_Character) return Boolean;
  function Is_Other_Format (Item : Wide_Character) return Boolean;
  function Is_Punctuation_Connector (Item : Wide_Character) return Boolean;
  function Is_Space (Item : Wide_Character) return Boolean;

  function Is_NFKC (Item : Wide_Character) return Boolean;
  function Is_Graphic (Item : Wide_Character) return Boolean;

  function To_Lower (Item : Wide_Character) return Wide_Character;
  function To_Upper (Item : Wide_Character) return Wide_Character;

  function To_Basic (Item : Wide_Character) return Wide_Character;

  function To_Lower (Item : Wide_String) return Wide_String;
  function To_Upper (Item : Wide_String) return Wide_String;

  function To_Basic (Item : Wide_String) return Wide_String;

end Ada.Wide_Characters.Handling;
```

{AI05-0185-1} The subprograms defined in Wide_Characters.Handling are locale independent.

```ada
function Character_Set_Version return String;

function Is_Control (Item : Wide_Character) return Boolean;

function Is_Basic (Item : Wide_Character) return Boolean;
renames Is_Digit;
```

```ada
function Is_Decimal_Digit (Item : Wide_Character) return Boolean;
function Is_Hexadecimal_Digit (Item : Wide_Character) return Boolean;
function Is_Alphanumeric (Item : Wide_Character) return Boolean;
function Is_Special (Item : Wide_Character) return Boolean;
function Is_Line_Terminator (Item : Wide_Character) return Boolean;
function Is_Mark (Item : Wide_Character) return Boolean;
function Is_Other_Format (Item : Wide_Character) return Boolean;
function Is_Punctuation_Connector (Item : Wide_Character) return Boolean;
function Is_Space (Item : Wide_Character) return Boolean;
```

```ada
function Is_NFKC (Item : Wide_Character) return Boolean;
function Is_Graphic (Item : Wide_Character) return Boolean;
```

```ada
function To_Lower (Item : Wide_Character) return Wide_Character;
function To_Upper (Item : Wide_Character) return Wide_Character;
```

```ada
function To_Basic (Item : Wide_Character) return Wide_Character;
function To_Lower (Item : Wide_String) return Wide_String;
function To_Upper (Item : Wide_String) return Wide_String;
function To_Basic (Item : Wide_String) return Wide_String;
```

```
end Ada.Wide_Characters.Handling;
```

{AI05-0185-1} The subprograms defined in Wide_Characters.Handling are locale independent.

```ada
function Character_Set_Version return String;

function Is_Control (Item : Wide_Character) return Boolean;

function Is_Basic (Item : Wide_Character) return Boolean;
renames Is_Digit;
```

```ada
function Is_Decimal_Digit (Item : Wide_Character) return Boolean;
function Is_Hexadecimal_Digit (Item : Wide_Character) return Boolean;
function Is_Alphanumeric (Item : Wide_Character) return Boolean;
function Is_Special (Item : Wide_Character) return Boolean;
function Is_Line_Terminator (Item : Wide_Character) return Boolean;
function Is_Mark (Item : Wide_Character) return Boolean;
function Is_Other_Format (Item : Wide_Character) return Boolean;
function Is_Punctuation_Connector (Item : Wide_Character) return Boolean;
function Is_Space (Item : Wide_Character) return Boolean;
```

```ada
function Is_NFKC (Item : Wide_Character) return Boolean;
function Is_Graphic (Item : Wide_Character) return Boolean;
```

```ada
function To_Lower (Item : Wide_Character) return Wide_Character;
function To_Upper (Item : Wide_Character) return Wide_Character;
```

```ada
function To_Basic (Item : Wide_Character) return Wide_Character;
function To_Lower (Item : Wide_String) return Wide_String;
function To_Upper (Item : Wide_String) return Wide_String;
function To_Basic (Item : Wide_String) return Wide_String;
```

```
end Ada.Wide_Characters.Handling;
```
function Is_Upper (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as letter_uppercase; otherwise returns False.

function Is_Basic (Item : Wide_Character) return Boolean;

{AI12-0260-1} {AI12-0450-1} Returns True if the Wide_Character designated by Item has no Decomposition Mapping in the code charts of ISO/IEC 10646:2020; otherwise returns False.

Implementation Note: Decomposition Mapping is defined in Clause 33 of ISO/IEC 10646:2020. Machine-readable (and normative!) versions of this can be found as Character Decomposition Mapping, described in file http://www.unicode.org/Public/UCD/latest/ucd/UnicodeData.txt, field 5 (which is the 6th item, Unicode counts from zero).

function Is_Digit (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as number_decimal; otherwise returns False.

function Is_Hexadecimal_Digit (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as number_decimal, or is in the range 'A' .. 'F' or 'a' .. 'f'; otherwise returns False.

function Is_Alphabetic (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as letter_uppercase, letter_lowercase, letter_titlecase, letter_modifier, letter_other, number_letter, or number_decimal; otherwise returns False.

function Is_Special (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as graphic_character, but not categorized as letter_uppercase, letter_lowercase, letter_titlecase, letter_modifier, letter_other, number_letter, or number_decimal; otherwise returns False.

function Is_Line_Terminator (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as separator_line or separator_paragraph, or if Item is a conventional line terminator character (Line_Feed, Line_Tabulation, Form_Feed, Carriage_Return, Next_Line); otherwise returns False.

function Is_Mark (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as mark_non_spacing or mark_spacing_combining; otherwise returns False.

function Is_Other_Format (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as other_format; otherwise returns False.

function Is_Punctuation_Connector (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as punctuation_connector; otherwise returns False.

function Is_Space (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as separator_space; otherwise returns False.
function Is_NFKC (Item : Wide_Character) return Boolean;

{AI12-0004-1} {AI12-0263-1} {AI12-0439-1} {AI12-0450-1} Returns True if the Wide_Character designated by Item can be present in a string normalized to Normalization Form KC (as defined by Clause 22 of ISO/IEC 10646:2020), otherwise returns False.

Reason: Wide_Characters for which this function returns False are not allowed in identifiers (see 2.3) even if they are categorized as letters or digits.

Implementation Note: This function returns False if the Unicode property NFKC Quick Check (NFKC_QC in the files) has the value No. See the Implementation Notes in 2.3 for the source of this property.

Discussion: A string for which Is_NFKC is true for every character may still not be in Normalization Form KC, as Is_NFKC returns true for characters that are dependent on characters around them as to whether they are removed by normalization. Ada does not provide a full normalization operation (it is complex and expensive).

function Is_Graphic (Item : Wide_Character) return Boolean;

{AI05-0185-1} Returns True if the Wide_Character designated by Item is categorized as graphic_character; otherwise returns False.

function To_Lower (Item : Wide_Character) return Wide_Character;

{AI05-0185-1} {AI05-0266-1} {AI05-0299-1} {AI12-0263-1} {AI12-0450-1} Returns the Simple Lowercase Mapping as defined by documents referenced in the note in Clause 24 of ISO/IEC 10646:2020 of the Wide_Character designated by Item. If the Simple Lowercase Mapping does not exist for the Wide_Character designated by Item, then the value of Item is returned.

Discussion: {AI12-0263-1} {AI12-0450-1} The “documents referenced” means Unicode, Chapter 4 (specifically, section 4.2 — Case). The case mappings come from Unicode as ISO/IEC 10646:2020 does not include complete case mappings. See the Implementation Notes in subclause 1.1.4 for machine-readable versions of both Uppercase and Lowercase mappings (but rather references the Unicode ones as above).

function To_Lower (Item : Wide_String) return Wide_String;

{AI05-0185-1} Returns the result of applying the To_Lower conversion to each Wide_Character element of the Wide_String designated by Item. The result is the null Wide_String if the value of the formal parameter is the null Wide_String. The lower bound of the result Wide_String is 1.

function To_Upper (Item : Wide_Character) return Wide_Character;

{AI05-0185-1} {AI05-0266-1} {AI05-0299-1} {AI12-0263-1} {AI12-0450-1} Returns the Simple Uppercase Mapping as defined by documents referenced in the note in Clause 24 of ISO/IEC 10646:2020 of the Wide_Character designated by Item. If the Simple Uppercase Mapping does not exist for the Wide_Character designated by Item, then the value of Item is returned.

function To_Upper (Item : Wide_String) return Wide_String;

{AI05-0185-1} Returns the result of applying the To_Upper conversion to each Wide_Character element of the Wide_String designated by Item. The result is the null Wide_String if the value of the formal parameter is the null Wide_String. The lower bound of the result Wide_String is 1.

function To_Basic (Item : Wide_Character) return Wide_Character;

{AI12-0260-1} {AI12-0450-1} Returns the Wide_Character whose code_point is given by the first value of its Decomposition Mapping in the code charts of ISO/IEC 10646:2020 if any; returns Item otherwise.
function To_Basic (Item : Wide_String) return Wide_String;

{AI12-0260-1} Returns the result of applying the To_Basic conversion to each Wide_Character element of the Wide_String designated by Item. The result is the null Wide_String if the value of the formal parameter is the null Wide_String. The lower bound of the result Wide_String is 1.

Implementation Advice

{AI05-0266-1} The_string Returned by Character Set Version should include either “10646:” or “Unicode”.

Implementation Advice: The string returned by Wide_Characters.Handling.Character_Set_Version should include either “10646:” or “Unicode”.

Discussion: {AI12-0263-1} {AI12-0450-1} The intent is that the returned string include the year for 10646 (as in “10646:2002:04:14”), and the version number for Unicode (as in “Unicode 13.06.0”). We don't try to specify that further so we don't need to decide how to represent Corrigenda for 10646, nor which of these is preferred. (Giving a Unicode version is more accurate, as the case folding and mapping rules always come from a Unicode version [10646 just tells one to look at Unicode to get those], and the character classifications ought to be the same for equivalent versions, but we don't want to talk about non-ISO standards in an ISO standard.)

NOTE 1 {AI05-0266-1} {AI12-0440-1} {AI12-0450-1} The results returned by these functions can depend on which particular version of ISO/IEC the 10646 standard is supported by the implementation (see 2.1).

NOTE 2 {AI05-0286-1} {AI12-0449-1} The case insensitive equality comparison routines provided in A.4.10 “String Comparison” are also available for wide strings (see A.4.7).

Extensions to Ada 2005

{AI05-0185-1} {AI05-0266-1} The package Wide_Characters.Handling is new.

Incompatibilities With Ada 2012

{AI12-0004-1} {AI12-0260-1} Added additional classification routines Is_Basic and Is_NFKC, and additional conversion routine To_Basic. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

A.3.6 The Package Wide_Wide_Characters.Handling

{AI05-0185-1} The package Wide_Wide_Characters.Handling has the same contents as Wide_Characters.Handling except that each occurrence of Wide_Character is replaced by Wide_Wide_Character, and each occurrence of Wide_String is replaced by Wide_Wide_String.

Extensions to Ada 2005

{AI05-0185-1} The package Wide_Wide_Characters.Handling is new.

A.4 String Handling

{AI95-00285-01} {AI05-0299-1} This subclause presents the specifications of the package Strings and several child packages, which provide facilities for dealing with string data. Fixed-length, bounded-length, and unbounded-length strings are supported, for both String and Wide_String and Wide_Wide_String. The string-handling subprograms include searches for pattern strings and for characters in program-specified sets, translation (via a character-to-character mapping), and transformation (replacing, inserting, overwriting, and deleting of substrings).

Extensions to Ada 83

{AI05-0299-1} This subclause is new to Ada 95.
A.4.1 The Package Strings

The package Strings provides declarations common to the string handling packages.

Static Semantics

The library package Strings has the following declaration:

```ada
package Ada.Strings is
  with pragma Pure is (Strings);

  Space      : constant Character       := ' ';
  Wide_Space : constant Wide_Character := ' ';
  Wide_Wide_Space : constant Wide_Wide_Character := ' ';
  Length_Error, Pattern_Error, Index_Error, Translation_Error : exception;

  type Alignment    is (Left, Right, Center);
  type Truncation   is (Left, Right, Error);
  type Membership   is (Inside, Outside);
  type Direction    is (Forward, Backward);
  type Trim_End     is (Left, Right, Both);
end Ada.Strings;
```

Incompatibilities With Ada 95

Constant Wide_Wide_Space is newly added to Ada.Strings. If Ada.Strings is referenced in a use_clause, and an entity E with a defining identifier of Wide_Wide_Space is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

A.4.2 The Package Strings.Maps

The package Strings.Maps defines the types, operations, and other entities necessary for character sets and character-to-character mappings.

Static Semantics

The library package Strings.Maps has the following declaration:

```ada
package Ada.Strings.Maps is
  with pragma Pure Preelaborate is (Maps);

  Null_Set : constant Character_Set;

  type Character_Range is record
    Low  : Character;
    High : Character;
  end record;

  type Character_Set is private;
  with pragma Preelaborable Initialization(Character_Set);

  type Character_Ranges is array (Positive range <>) of Character_Range;

  function To_Set    (Ranges : in Character_Ranges) return Character_Set;
  function To_Set    (Span   : in Character_Range) return Character_Set;
  function To_Ranges (Set    : in Character_Set) return Character_Ranges;
  function "="   (Left, Right : in Character_Set) return Boolean;
```

Wording Changes from Ada 95

{AI95-00285-01} Included Wide Wide String in this description; the individual changes are documented as extensions as needed.
function "not"  (Right : in Character_Set) return Character_Set;
function "and" (Left, Right : in Character_Set) return Character_Set;
function "or"  (Left, Right : in Character_Set) return Character_Set;
function "xor" (Left, Right : in Character_Set) return Character_Set;
function "-"   (Left, Right : in Character_Set) return Character_Set;

function Is_In (Element : in Character; Set     : in Character_Set) return Boolean;
function Is_Subset (Elements : in Character_Set; Set      : in Character_Set) return Boolean;
function "<=" (Left  : in Character_Set; Right : in Character_Set) return Boolean renames Is_Subset;

-- Alternative representation for a set of character values:
subtype Character_Sequence is String;
function To_Set (Sequence  : in Character_Sequence) return Character_Set;
function To_Set (Singleton : in Character) return Character_Set;
function To_Sequence (Set  : in Character_Set) return Character_Sequence;

{AI95-00161-01} {AI12-0399-1} -- Representation for a character to character mapping:
type Character_Mapping is private;
withpragma Preelaborable_Initialization(Character_Mapping);
function Value (Map     : in Character_Mapping; Element : in Character) return Character;
Identity : constant Character_Mapping;
function To_Mapping (From, To : in Character_Sequence) return Character_Mapping;
function To_Domain (Map : in Character_Mapping) return Character_Sequence;
function To_Range  (Map : in Character_Mapping) return Character_Sequence;
type Character_Mapping_Function is access function (From : in Character) return Character;

private
... -- not specified by the language
end Ada.Strings.Maps;

An object of type Character_Set represents a set of characters.
Null_Set represents the set containing no characters.
An object Obj of type Character_Range represents the set of characters in the range Obj.Low .. Obj.High.
An object Obj of type Character_Ranges represents the union of the sets corresponding to Obj(I) for I in Obj'Range.

function To_Set (Ranges : in Character_Ranges) return Character_Set;

{AI05-0264-1} If Ranges'Length=0 then Null_Set is returned; otherwise, the returned value
represents the set corresponding to Ranges.

function To_Set (Span : in Character_Range) return Character_Set;

The returned value represents the set containing each character in Span.
function To_Ranges (Set : in Character_Set) return Character_Ranges;

{AI05-0264-1} If Set = Null_Set, then an empty Character_Ranges array is returned; otherwise, the shortest array of contiguous ranges of Character values in Set, in increasing order of Low, is returned.

function "=" (Left, Right : in Character_Set) return Boolean;

The function "=" returns True if Left and Right represent identical sets, and False otherwise.

Each of the logical operators "not", "and", "or", and "xor" returns a Character_Set value that represents the set obtained by applying the corresponding operation to the set(s) represented by the parameter(s) of the operator. "-"(Left, Right) is equivalent to "and"("not"(Right)).

Reason: The set minus operator is provided for efficiency.

function Is_In (Element : in Character; Set : in Character_Set) return Boolean;

Is_In returns True if Element is in Set, and False otherwise.

function Is_Subset (Elements : in Character_Set; Set : in Character_Set) return Boolean;

Is_Subset returns True if Elements is a subset of Set, and False otherwise.

subtype Character_Sequence is String;

The Character_Sequence subtype is used to portray a set of character values and also to identify the domain and range of a character mapping.

Reason: Although a named subtype is redundant — the predefined type String could have been used for the parameter to To_Set and To_Mapping below — the use of a differently named subtype identifies the intended purpose of the parameter.

function To_Set (Sequence : in Character_Sequence) return Character_Set;

function To_Set (Singleton : in Character) return Character_Set;

Sequence portrays the set of character values that it explicitly contains (ignoring duplicates). Singleton portrays the set comprising a single Character. Each of the To_Set functions returns a Character_Set value that represents the set portrayed by Sequence or Singleton.

function To_Sequence (Set : in Character_Set) return Character_Sequence;

The function To_Sequence returns a Character_Sequence value containing each of the characters in the set represented by Set, in ascending order with no duplicates.

type Character_Mapping is private;

An object of type Character_Mapping represents a Character-to-Character mapping.

function Value (Map : in Character_Mapping; Element : in Character) return Character;

The function Value returns the Character value to which Element maps with respect to the mapping represented by Map.

A character C matches a pattern character P with respect to a given Character_Mapping value Map if Value(Map, C) = P. A string S matches a pattern string P with respect to a given Character_Mapping if their lengths are the same and if each character in S matches its corresponding character in the pattern string P.
**Discussion:** In an earlier version of the string handling packages, the definition of matching was symmetrical, namely $C$ matches $P$ if $\text{Value(Map,C)} = \text{Value(Map,P)}$. However, applying the mapping to the pattern was confusing according to some reviewers. Furthermore, if the symmetrical version is needed, it can be achieved by applying the mapping to the pattern (via translation) prior to passing it as a parameter.

String handling subprograms that deal with character mappings have parameters whose type is `Character_Mapping`.

```ada
Identity : constant Character_Mapping;
```

Identity maps each Character to itself.

```ada
function To_Mapping (From, To : in Character_Sequence)
return Character_Mapping;
```

To_Mapping produces a Character_Mapping such that each element of From maps to the corresponding element of To, and each other character maps to itself. If From'Length /= To'Length, or if some character is repeated in From, then Translation_Error is propagated.

```ada
function To_Domain (Map : in Character_Mapping)
return Character_Sequence;
```

To_Domain returns the shortest Character_Sequence value $D$ such that each character not in $D$ maps to itself, and such that the characters in $D$ are in ascending order. The lower bound of $D$ is 1.

```ada
function To_Range  (Map : in Character_Mapping)
return Character_Sequence;
```

{8652/0048} {AI95-00151-01} To_Range returns the Character_Sequence value $R$, with lower bound 1 and upper bound $\text{Map'}Length$, such that if $D = \text{To_Domain(Map)}$, then $R$ has the same bounds as $D$, and then $D(I)$ maps to $R(I)$ for each $I$ in $D'$Range.

An object $F$ of type `Character_Mapping_Function` maps a Character value $C$ to the Character value $F.all(C)$, which is said to match $C$ with respect to mapping function $F$.

**NOTE 1** Character_Mapping and Character_Mapping_Function are used both for character equivalence mappings in the search subprograms (such as for case insensitivity) and as transformational mappings in the Translate subprograms.

**NOTE 2** To_Domain(Identity) and To_Range(Identity) each returns the null string.

**Reason:** Package Strings.Maps is not pure, since it declares an access-to-subprogram type.

**Examples**

{AI12-0429-1} **Example of use of Strings.Maps.To_Mapping:**

To_Mapping("ABCD", "ZZAB") returns a Character_Mapping that maps 'A' and 'B' to 'Z', 'C' to 'A', 'D' to 'B', and each other Character to itself.

**Extensions to Ada 95**

{AI95-00161-01} **Amendment Correction:** Added `pragma Preelaborable_Initialization` to types `Character_Set` and `Character_Mapping`, so that they can be used to declare default-initialized objects in preelaborated units.

{AI95-00362-01} **Strings.Maps is now Pure, so it can be used in pure units.**

**Wording Changes from Ada 95**

{8652/0048} {AI95-00151-01} **Corrigendum:** Corrected the definition of the range of the result of To_Range, since the Ada 95 definition makes no sense.

**A.4.3 Fixed-Length String Handling**

The language-defined package Strings.Fixed provides string-handling subprograms for fixed-length strings; that is, for values of type `Standard.String`. Several of these subprograms are procedures that
modify the contents of a String that is passed as an **out** or an **in out** parameter; each has additional parameters to control the effect when the logical length of the result differs from the parameter's length.

For each function that returns a String, the lower bound of the returned value is 1.

**Discussion:** (AI95-00114-01) Most operations that yield a String are provided both as a function and as a procedure. The functional form is possibly a more aesthetic style but may introduce overhead due to extra copying or dynamic memory usage in some implementations. Thus a procedural form, with an **in out** parameter so that all copying is done `in place`, is also supplied.

The basic model embodied in the package is that a fixed-length string comprises significant characters and possibly padding (with space characters) on either or both ends. When a shorter string is copied to a longer string, padding is inserted, and when a longer string is copied to a shorter one, padding is stripped. The Move procedure in Strings.Fixed, which takes a String as an **out** parameter, allows the programmer to control these effects. Similar control is provided by the string transformation procedures.

**Static Semantics**

The library package Strings.Fixed has the following declaration:

```ada
package Ada.Strings.Fixed is
  with Ada.Strings.Maps;
  pragma Preelaborate, Nonblocking, Global => in out synchronized is(Fixed);

  -- "Copy" procedure for strings of possibly different lengths
  procedure Move (Source  : in String;
                   Target  : out String;
                   Drop    : in Truncation := Error;
                   Justify : in Alignment := Left;
                   Pad     : in Character  := Space);

  -- Search subprograms

  function Index (Source  : in String;
                  Pattern : in String;
                  From    : in Positive;
                  Going   : in Direction := Forward;
  return Natural;

  function Index (Source  : in String;
                  Pattern : in String;
                  From    : in Positive;
                  Going   : in Direction := Forward;
                  Mapping : in Maps.Character_Mapping_Function)
  return Natural;

  function Index (Source   : in String;
                  Pattern  : in String;
                  Going    : in Direction := Forward;
                  Mapping  : in Maps.Character_Mapping)
  return Natural;

  function Index (Source   : in String;
                  Pattern  : in String;
                  Going    : in Direction := Forward;
                  Mapping  : in Maps.Character_Mapping_Function)
  return Natural;

  function Index (Source  : in String;
                  Set      : in Maps.Character_Set;
                  From     : in Positive;
                  Test     : in Membership := Inside;
                  Going    : in Direction := Forward)
  return Natural;
```

A.4.3 Fixed-Length String Handling
function Index (Source : in String;
    Set : in Maps.Character_Set;
    Test : in Membership := Inside;
    Going : in Direction := Forward)
return Natural;

{AI95-00301-01} function Index_Non_Blank (Source : in String;
    From : in Positive;
    Going : in Direction := Forward)
return Natural;

function Count (Source : in String;
    Pattern : in String;
return Natural;

function Count (Source : in String;
    Pattern : in String;
    Mapping : in Maps.Character_Mapping_Function)
return Natural;

function Count (Source : in String;
    Set : in Maps.Character_Set)
return Natural;

{AI05-0031-1} procedure Find_Token (Source : in String;
    Set : in Maps.Character_Set;
    From : in Positive;
    Test : in Membership;
    First : out Positive;
    Last : out Natural);

procedure Find_Token (Source : in String;
    Set : in Maps.Character_Set;
    Test : in Membership;
    First : out Positive;
    Last : out Natural);

-- String translation subprograms

function Translate (Source : in String;
    Mapping : in Maps.Character_Mapping)
return String;

procedure Translate (Source : in out String;
    Mapping : in Maps.Character_Mapping);

function Translate (Source : in String;
    Mapping : in Maps.Character_Mapping_Function)
return String;

procedure Translate (Source : in out String;
    Mapping : in Maps.Character_Mapping_Function);

-- String transformation subprograms

function Replace_Slice (Source : in String;
    Low : in Positive;
    High : in Natural;
    By : in String)
return String;

procedure Replace_Slice (Source : in out String;
    Low : in Positive;
    High : in Natural;
    By : in String;
    Drop : in Truncation := Error;
    Justify : in Alignment := Left;
    Pad : in Character := Space);
function Insert (Source   : in String;
    Before   : in Positive;
    New_Item : in String)
return String;
procedure Insert (Source   : in out String;
    Before   : in Positive;
    New_Item : in String;
    Drop     : in Truncation := Error);

function Overwrite (Source   : in String;
    Position : in Positive;
    New_Item : in String)
return String;
procedure Overwrite (Source   : in out String;
    Position : in Positive;
    New_Item : in String;
    Drop     : in Truncation := Right);

function Delete (Source  : in String;
    From    : in Positive;
    Through : in Natural)
return String;
procedure Delete (Source  : in out String;
    From    : in Positive;
    Through : in Natural;
    Justify : in Alignment := Left;
    Pad     : in Character := Space);

-- String selector subprograms
function Trim (Source : in String;
    Side   : in Trim_End)
return String;
procedure Trim (Source : in out String;
    Side   : in Trim_End;
    Justify : in Alignment := Left;
    Pad     : in Character := Space);
function Trim (Source : in String;
    Left   : in Maps.Character_Set;
    Right  : in Maps.Character_Set)
return String;
procedure Trim (Source : in out String;
    Left   : in Maps.Character_Set;
    Right  : in Maps.Character_Set;
    Justify : in Alignment := Strings.Left;
    Pad     : in Character := Space);

function Head (Source : in String;
    Count  : in Natural;
    Pad    : in Character := Space)
return String;
procedure Head (Source : in out String;
    Count  : in Natural;
    Justify : in Alignment := Left;
    Pad     : in Character := Space);

function Tail (Source : in String;
    Count  : in Natural;
    Pad    : in Character := Space)
return String;
procedure Tail (Source : in out String;
    Count  : in Natural;
    Justify : in Alignment := Left;
    Pad     : in Character := Space);
-- String constructor functions

function "*" (Left : in Natural; Right : in Character) return String;
function "*" (Left : in Natural; Right : in String) return String;
end Ada.Strings.Fixed;

The effects of the above subprograms are as follows.

procedure Move (Source : in String; Target : out String;
                  Drop : in Truncation := Error;
                  Justify : in Alignment := Left;
                  Pad : in Character := Space);

{AI05-0264-1} The Move procedure copies characters from Source to Target. If Source has the same length as Target, then the effect is to assign Source to Target. If Source is shorter than Target, then:

- If Justify=Left, then Source is copied into the first Source'Length characters of Target.
- If Justify=Right, then Source is copied into the last Source'Length characters of Target.
- If Justify=Center, then Source is copied into the middle Source'Length characters of Target. In this case, if the difference in length between Target and Source is odd, then the extra Pad character is on the right.
- Pad is copied to each Target character not otherwise assigned.

If Source is longer than Target, then the effect is based on Drop.

- If Drop=Left, then the rightmost Target'Length characters of Source are copied into Target.
- If Drop=Right, then the leftmost Target'Length characters of Source are copied into Target.
- If Drop=Error, then the effect depends on the value of the Justify parameter and also on whether any characters in Source other than Pad would fail to be copied:
  - If Justify=Left, and if each of the rightmost Source'Length-Target'Length characters in Source is Pad, then the leftmost Target'Length characters of Source are copied to Target.
  - If Justify=Right, and if each of the leftmost Source'Length-Target'Length characters in Source is Pad, then the rightmost Target'Length characters of Source are copied to Target.
- Otherwise, Length_Error is propagated.

Ramification: The Move procedure will work even if Source and Target overlap.

Reason: The order of parameters (Source before Target) corresponds to the order in COBOL’s MOVE verb.

function Index (Source : in String; Pattern : in String;
                From : in Positive;
                Going : in Direction := Forward;
  return Natural;

function Index (Source : in String; Pattern : in String;
                From : in Positive;
                Going : in Direction := Forward;
                Mapping : in Maps.Character_Mapping_Function)
  return Natural;
Each Index function searches, starting from From, for a slice of Source, with length Pattern'Length, that matches Pattern with respect to Mapping; the parameter Going indicates the direction of the lookup. If Source is the null string, Index returns 0; otherwise, if From is not in Source'Range, then Index_Error is propagated. If Going = Forward, then Index returns the smallest index I which is greater than or equal to From such that the slice of Source starting at I matches Pattern. If Going = Backward, then Index returns the largest index I such that the slice of Source starting at I matches Pattern and has an upper bound less than or equal to From. If there is no such slice, then 0 is returned. If Pattern is the null string, then Pattern_Error is propagated.

Discussion:
There is no default parameter for From; the default value would need to depend on other parameters (the bounds of Source and the direction Going). It is better to use overloaded functions rather than a special value to represent the default.

There is no default value for the Mapping parameter that is a Character_Mapping_Function; if there were, a call would be ambiguous since there is also a default for the Mapping parameter that is a Character_Mapping.

The language does not define when the Pattern_Error check is made. (That's because many common searching implementations require a nonempty pattern) That means that the result for a call like Index ("", "") could be 0 or could raise Pattern_Error. Similarly, in the call Index ("", "", From => 2), the language does not define whether Pattern_Error or Index_Error is raised.

function Index (Source   : in String;  
Pattern  : in String;  
Going    : in Direction := Forward;  
Mapping  : in Maps.Character_Mapping  
            := Maps.Identity)  
return Natural;

function Index (Source   : in String;  
Pattern  : in String;  
Going    : in Direction := Forward;  
Mapping  : in Maps.Character_Mapping_Function)  
return Natural;

function Index (Source  : in String;  
Set     : in Maps.Character_Set;  
From    : in Positive;  
Test    : in Membership := Inside;  
Going   : in Direction := Forward)  
return Natural;

This paragraph was deleted. Discussion: There is no default value for the Mapping parameter that is a Character_Mapping_Function; if there were, a call would be ambiguous since there is also a default for the Mapping parameter that is a Character_Mapping.

Index searches for the first or last occurrence of any of a set of characters (when Test=Inside), or any of the complement of a set of characters (when Test=Outside). If Source is the null string, Index returns 0; otherwise, if From is not in Source'Range, then Index_Error is propagated. Otherwise, it returns the smallest index I >= From.
(if Going=Forward) or the largest index I <= From (if Going=Backward) such that Source(I) satisfies the Test condition with respect to Set; it returns 0 if there is no such Character in Source.

function Index (Source : in String;  
    Set    : in Maps.Character_Set;  
    Test   : in Membership := Inside;  
    Going  : in Direction := Forward)
return Natural;

{AI95-00301-01} If Going = Forward, returns Index searches for the first or last occurrence of any of a set of characters (when Test=Inside), or any of the complement of a set of characters (when Test=Outside). It returns the smallest index I (if Going=Forward) or the largest index I (if Going=Backward) such that Source(I) satisfies the Test condition with respect to Set; it returns 0 if there is no such Character in Source.

Index (Source, Set, Source'First, Test, Forward);

{AI95-00301-01} Otherwise, returns Index (Source, Set, Source'Last, Test, Backward);

function Index_Non_Blank (Source : in String;  
    From   : in Positive;  
    Going  : in Direction := Forward)
return Natural;

{AI95-00301-01} Returns Index (Source, Maps.To_Set(Space), From, Outside, Going);

function Index_Non_Blank (Source : in String;  
    From   : in Positive;  
    Going  : in Direction := Forward)
return Natural;

Returns Index(Source, Maps.To_Set(Space), Outside, Going)

function Count (Source   : in String;  
    Pattern  : in String;  
return Natural;

function Count (Source   : in String;  
    Pattern  : in String;  
    Mapping  : in Maps.Character_Mapping_Function)
return Natural;

Returns the maximum number of nonoverlapping slices of Source that match Pattern with respect to Mapping. If Pattern is the null string then Pattern_Error is propagated.

Reason: We say `maximum number' because it is possible to slice a source string in different ways yielding different numbers of matches. For example if Source is "ABABABA" and Pattern is "ABA", then Count yields 2, although there is a partitioning of Source that yields just 1 match, for the middle slice. Saying 'maximum number' is equivalent to saying that the pattern match starts either at the low index or the high index position.

function Count (Source   : in String;  
    Set      : in Maps.Character_Set)
return Natural;

Returns the number of occurrences in Source of characters that are in Set.

procedure Find_Token (Source : in String;  
    Set    : in Maps.Character_Set;  
    From   : in Positive;  
    Test   : in Membership;  
    First  : out Positive;  
    Last   : out Natural);
procedure Find_Token (Source : in String;
  Set    : in Maps.Character_Set;
  Test   : in Membership;
  First  : out Positive;
  Last   : out Natural);

function Translate (Source  : in String;
  Mapping : in Maps.Character_Mapping)
return String;

function Translate (Source  : in String;
  Mapping : in Maps.Character_Mapping)
return String;

function Replace_Slice (Source   : in String;
  Low      : in Positive;
  High     : in Natural;
  By       : in String)
return String;

**procedure** Replace_Slice (Source : in out String;
Low : in Positive;
High : in Natural;
By : in String;
Drop : in Truncation := Error;
Justify : in Alignment := Left;
Pad : in Character := Space);

Equivalent to Move(Replace_Slice(Source, Low, High, By), Source, Drop, Justify, Pad).

**function** Insert (Source : in String;
Before : in Positive;
New_Item : in String)
return String;

{AI05-0264-1} Propagates Index_Error if Before is not in Source'First .. Source'Last+1;
otherwise, returns Source(Source'First..Before–1) & New_Item & Source(Before..Source'Last),
but with lower bound 1.

**procedure** Insert (Source : in out String;
Before : in Positive;
New_Item : in String;
Drop : in Truncation := Error);

Equivalent to Move(Insert(Source, Before, New_Item), Source, Drop).

**function** Overwrite (Source : in String;
Position : in Positive;
New_Item : in String)
return String;

{AI05-0264-1} Propagates Index_Error if Position is not in Source'First .. Source'Last+1;
otherwise, returns the string obtained from Source by successively replacing characters starting
at Position with corresponding characters from New_Item. If the end of Source is reached before
the characters in New_Item are exhausted, the remaining characters from New_Item are appended
to the string.

**procedure** Overwrite (Source : in out String;
Position : in Positive;
New_Item : in String;
Drop : in Truncation := Right);

Equivalent to Move(Overwrite(Source, Position, New_Item), Source, Drop).

**function** Delete (Source : in String;
From : in Positive;
Through : in Natural)
return String;

{8652/0049} {AI95-00128-01} {AI05-0264-1} If From <= Through, the returned string is
Replace_Slice(Source, From, Through, "")]; otherwise, it is Source with lower bound 1.

**procedure** Delete (Source : in out String;
From : in Positive;
Through : in Natural;
Justify : in Alignment := Left;
Pad : in Character := Space);

Equivalent to Move(Delete(Source, From, Through), Source, Justify => Justify, Pad => Pad).
function Trim (Source : in String; 
   Side  : in Trim_End) 
   return String; 

Returns the string obtained by removing from Source all leading Space characters (if Side = Left), 
all trailing Space characters (if Side = Right), or all leading and trailing Space characters (if Side 
= Both).

procedure Trim (Source  : in out String; 
   Side  : in Trim_End; 
   Justify : in Alignment := Left; 
   Pad     : in Character := Space); 

Equivalent to Move(Trim(Source, Side), Source, Justify=>Justify, Pad=>Pad).

function Trim (Source : in String; 
   Left   : in Maps.Character_Set; 
   Right  : in Maps.Character_Set) 
   return String; 

Returns the string obtained by removing from Source all leading characters in Left and all trailing 
characters in Right.

procedure Trim (Source  : in out String; 
   Left    : in Maps.Character_Set; 
   Right   : in Maps.Character_Set; 
   Justify : in Alignment := Strings.Left; 
   Pad     : in Character := Space); 

Equivalent to Move(Trim(Source, Left, Right), Source, Justify => Justify, Pad=>Pad).

function Head (Source : in String; 
   Count  : in Natural; 
   Pad    : in Character := Space) 
   return String; 

{AI05-0264-1} Returns a string of length Count. If Count <= Source'Length, the string comprises 
the first Count characters of Source. Otherwise, its contents are Source concatenated with Count– 
Source'Length Pad characters.

procedure Head (Source  : in out String; 
   Count   : in Natural; 
   Justify : in Alignment := Left; 
   Pad     : in Character := Space); 

Equivalent to Move(Head(Source, Count, Pad), Source, Drop=>Error, Justify=>Justify, 
Pad=>Pad).

function Tail (Source : in String; 
   Count  : in Natural; 
   Pad    : in Character := Space) 
   return String; 

{AI05-0264-1} Returns a string of length Count. If Count <= Source'Length, the string comprises 
the last Count characters of Source. Otherwise, its contents are Count-Source'Length Pad 
characters concatenated with Source.

procedure Tail (Source  : in out String; 
   Count   : in Natural; 
   Justify : in Alignment := Left; 
   Pad     : in Character := Space); 

Equivalent to Move(Tail(Source, Count, Pad), Source, Drop=>Error, Justify=>Justify, 
Pad=>Pad).
function "*" (Left : in Natural;  
Right : in Character) return String;

function "*" (Left : in Natural;  
Right : in String) return String;

{8652/0049} {AI95-00128-01} These functions replicate a character or string a specified number of times. The first function returns a string whose length is Left and each of whose elements is Right. The second function returns a string whose length is Left*Right'Length and whose value is the null string if Left = 0 and otherwise is (Left–1)*Right & Right with lower bound 1.

NOTE 1 {AI05-0264-1} {AI12-0442-1} In the Index and Count functions taking Pattern and Mapping parameters, for there to be a match, the actual String parameter passed to Pattern can contain only characters occurring as target characters of the mapping. Otherwise, the pattern will not match.

NOTE 2 In the Insert subprograms, inserting at the end of a string is obtained by passing Source'Last+1 as the Before parameter.

NOTE 3 If a null Character_Mapping_Function is passed to any of the string handling subprograms, Constraint_Error is propagated.

Incompatibilities With Ada 95

{AI95-00301-01} {AI05-0005-1} Overloaded versions of Index and Index_Non_Blank are newly added to Strings.Fixed. If Strings.Fixed is referenced in a use_clause, and an entity E with a defining_identifier of Index or Index_Non_Blank is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Wording Changes from Ada 95

{8652/0049} {AI95-00128-01} Corrigendum: Clarified that Find_Token may raise Constraint_Error if Source'First is not in Positive (which is only possible for a null string).

{8652/0049} {AI95-00128-01} Corrigendum: Clarified that Replace_Slice, Delete, and "*" always return a string with lower bound 1.

Incompatibilities With Ada 2005

{AI05-0031-1} An overloaded version of Find_Token is added to Strings.Fixed. If Strings.Fixed is referenced in a use_clause, and an entity E with a defining_identifier of Find_Token is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Wording Changes from Ada 2005

{AI05-0056-1} Correction: Clarified that Index never raises Index_Error if the source string is null.

A.4.4 Bounded-Length String Handling

{AI12-0445-1} The language-defined package Strings.Bounded provides a generic package each of whose instances yields a private type Bounded_String and a set of operations. An object of a particular Bounded_String type represents a String whose low bound is 1 and whose length can vary conceptually between 0 and a maximum size established at the generic instantiation. The subprograms for fixed-length string handling are either overloaded directly for Bounded_String, or are modified as necessary to reflect the variability in length. Additionally, since the Bounded_String type is private, appropriate constructor and selector operations are provided.

Reason: Strings.Bounded declares an inner generic package, versus itself being directly a generic child of Strings, in order to retain compatibility with a version of the string-handling packages that is generic with respect to the character and string types.

Reason: The bound of a bounded-length string is specified as a parameter to a generic, versus as the value for a discriminant, because of the inappropriateness of assignment and equality of discriminated types for the copying and comparison of bounded strings.
The library package Strings.Bounded has the following declaration:

```ada
package Ada.Strings.Bounded is

with Ada.Strings.Maps;

generic
Max   : Positive;  -- Maximum length of a Bounded_String

package Generic_Bounded_Length is

Max_Length : constant Positive := Max;

type Bounded_String is private;
Null_Bounded_String : constant Bounded_String;

subtype Length_Range is Natural range 0 .. Max_Length;

function Length (Source : in Bounded_String) return Length_Range;

function To_Bounded_String (Source : in String; Drop : in Truncation := Error) return Bounded_String;

function To_String (Source : in Bounded_String) return String;

procedure Set_Bounded_String (Target : out Bounded_String; Source : in String; Drop : in Truncation := Error);

function Append (Left, Right : in Bounded_String; Drop : in Truncation := Error) return Bounded_String;

function Append (Left : in Bounded_String; Right : in String; Drop : in Truncation := Error) return Bounded_String;

function Append (Left : in String; Right : in Bounded_String; Drop : in Truncation := Error) return Bounded_String;

function Append (Left : in Bounded_String; Right : in Character; Drop : in Truncation := Error) return Bounded_String;

function Append (Left : in Character; Right : in Bounded_String; Drop : in Truncation := Error) return Bounded_String;

procedure Append (Source : in out Bounded_String; New_Item : in Bounded_String; Drop : in Truncation := Error);

procedure Append (Source : in out Bounded_String; New_Item : in String; Drop : in Truncation := Error);

procedure Append (Source : in out Bounded_String; New_Item : in Character; Drop : in Truncation := Error);

function "&" (Left, Right : in Bounded_String) return Bounded_String;

function "&" (Left : in Bounded_String; Right : in String) return Bounded_String;
```

---

**Static Semantics**

2

The library package Strings.Bounded has the following declaration:

```ada
{AI12-0241-1} {AI12-0302-1} with Ada.Strings.Maps;

package Ada.Strings.Bounded is

with pragma Preelaborate, Nonblocking, Global => in out synchronized is (Bounded);

generic
Max   : Positive;  -- Maximum length of a Bounded_String

package Generic_Bounded_Length is

Max_Length : constant Positive := Max;

type Bounded_String is private;
Null_Bounded_String : constant Bounded_String;

subtype Length_Range is Natural range 0 .. Max_Length;

function Length (Source : in Bounded_String) return Length_Range;

function To_Bounded_String (Source : in String; Drop : in Truncation := Error) return Bounded_String;

function To_String (Source : in Bounded_String) return String;

{AI95-00301-01} procedure Set_Bounded_String (Target : out Bounded_String; Source : in String; Drop : in Truncation := Error);

function Append (Left, Right : in Bounded_String; Drop : in Truncation := Error) return Bounded_String;

function Append (Left : in Bounded_String; Right : in String; Drop : in Truncation := Error) return Bounded_String;

function Append (Left : in String; Right : in Bounded_String; Drop : in Truncation := Error) return Bounded_String;

function Append (Left : in Bounded_String; Right : in Character; Drop : in Truncation := Error) return Bounded_String;

function Append (Left : in Character; Right : in Bounded_String; Drop : in Truncation := Error) return Bounded_String;

procedure Append (Source : in out Bounded_String; New_Item : in Bounded_String; Drop : in Truncation := Error);

procedure Append (Source : in out Bounded_String; New_Item : in String; Drop : in Truncation := Error);

procedure Append (Source : in out Bounded_String; New_Item : in Character; Drop : in Truncation := Error);

function "&" (Left, Right : in Bounded_String) return Bounded_String;

function "&" (Left : in Bounded_String; Right : in String) return Bounded_String;
```
function "&" (Left : in String; Right : in Bounded_String) return Bounded_String;
function "&" (Left : in Bounded_String; Right : in Character) return Bounded_String;
function "&" (Left : in Character; Right : in Bounded_String) return Bounded_String;
function Element (Source : in Bounded_String; Index : in Positive) return Character;

procedure Replace_Element (Source : in out Bounded_String; Index : in Positive; By : in Character);

function Slice (Source : in Bounded_String; Low : in Positive; High : in Natural) return String;

{AI95-00301-01} function Bounded_Slice (Source : in Bounded_String; Low : in Positive; High : in Natural) return Bounded_String;

{AI95-00301-01} procedure Bounded_Slice (Source : in Bounded_String; Target : out Bounded_String; Low : in Positive; High : in Natural);

function "=" (Left, Right : in Bounded_String) return Boolean;
function "=" (Left : in String; Right : in Bounded_String) return Boolean;
function "=" (Left : in String; Right : in String) return Boolean;
function "<" (Left, Right : in Bounded_String) return Boolean;
function "<" (Left : in Bounded_String; Right : in String) return Boolean;
function "<" (Left : in String; Right : in Bounded_String) return Boolean;
function "<" (Left : in String; Right : in String) return Boolean;
function "<=" (Left, Right : in Bounded_String) return Boolean;
function "<=" (Left : in Bounded_String; Right : in String) return Boolean;
function "<=" (Left : in String; Right : in Bounded_String) return Boolean;
function "<=" (Left : in String; Right : in String) return Boolean;
function ">" (Left, Right : in Bounded_String) return Boolean;
function ">" (Left : in Bounded_String; Right : in String) return Boolean;
function ">" (Left : in String; Right : in Bounded_String) return Boolean;
function ">" (Left : in String; Right : in String) return Boolean;

{AI95-00301-01} -- Search subprograms functions
function Index (Source : in Bounded_String;
Pattern : in String;
From : in Positive;
Going : in Direction := Forward;
return Natural;

function Index (Source : in Bounded_String;
Pattern : in String;
From : in Positive;
Going : in Direction := Forward;
Mapping : in Maps.Character_Mapping_Function)
return Natural;

function Index (Source : in Bounded_String;
Pattern : in String;
Going : in Direction := Forward;
return Natural;

function Index (Source : in Bounded_String;
Pattern : in String;
Going : in Direction := Forward;
Mapping : in Maps.Character_Mapping_Function)
return Natural;

function Index (Source : in Bounded_String;
Pattern : in String;
From : in Positive;
Test : in Membership := Inside;
Going : in Direction := Forward)
return Natural;

function Index (Source : in Bounded_String;
Pattern : in String;
Test : in Membership := Inside;
Going : in Direction := Forward)
return Natural;

function Index_Non_Blank (Source : in Bounded_String;
From : in Positive;
Going : in Direction := Forward)
return Natural;

function Index_Non_Blank (Source : in Bounded_String;
Going : in Direction := Forward)
return Natural;

function Count (Source : in Bounded_String;
Pattern : in String;
return Natural;

function Count (Source : in Bounded_String;
Pattern : in String;
Mapping : in Maps.Character_Mapping_Function)
return Natural;

function Count (Source : in Bounded_String;
Set : in Maps.Character_Set)
return Natural;

procedure Find_Token (Source : in Bounded_String;
Set : in Maps.Character_Set;
From : in Positive;
Test : in Membership;
First : out Positive;
Last : out Natural);
-- String translation subprograms

function Translate (Source : in Bounded_String;
Mapping : in Maps.Character_Mapping)
return Bounded_String;

procedure Translate (Source : in out Bounded_String;
Mapping : in Maps.Character_Mapping);

function Translate (Source : in Bounded_String;
Mapping : in Maps.Character_Mapping_Function)
return Bounded_String;

procedure Translate (Source : in out Bounded_String;
Mapping : in Maps.Character_Mapping_Function);

-- String transformation subprograms

function Replace_Slice (Source   : in Bounded_String;
Low      : in Positive;
High     : in Natural;
By       : in String;
Drop     : in Truncation := Error)
return Bounded_String;

procedure Replace_Slice (Source   : in out Bounded_String;
Low      : in Positive;
High     : in Natural;
By       : in String;
Drop     : in Truncation := Error);

function Insert (Source   : in Bounded_String;
Before   : in Positive;
New_Item : in String;
Drop     : in Truncation := Error)
return Bounded_String;

procedure Insert (Source   : in out Bounded_String;
Before   : in Positive;
New_Item : in String;
Drop     : in Truncation := Error);

function Overwrite (Source    : in Bounded_String;
Position  : in Positive;
New_Item  : in String;
Drop      : in Truncation := Error)
return Bounded_String;

procedure Overwrite (Source    : in out Bounded_String;
Position  : in Positive;
New_Item  : in String;
Drop      : in Truncation := Error);

function Delete (Source  : in Bounded_String;
From    : in Positive;
Through : in Natural)
return Bounded_String;

procedure Delete (Source  : in out Bounded_String;
From    : in Positive;
Through : in Natural);

-- String selector subprograms

function Trim (Source : in Bounded_String;
Side   : in Trim_End)
return Bounded_String;

procedure Trim (Source : in out Bounded_String;
Side   : in Trim_End);
function Trim (Source : in Bounded_String;
Left   : in Maps.Character_Set;
Right  : in Maps.Character_Set)
return Bounded_String;

procedure Trim (Source : in out Bounded_String;
Left   : in Maps.Character_Set;
Right  : in Maps.Character_Set);

function Head (Source : in Bounded_String;
Count  : in Natural;
Pad    : in Character := Space;
Drop   : in Truncation := Error)
return Bounded_String;

procedure Head (Source : in out Bounded_String;
Count  : in Natural;
Pad    : in Character := Space;
Drop   : in Truncation := Error);

function Tail (Source : in Bounded_String;
Count  : in Natural;
Pad    : in Character := Space;
Drop   : in Truncation := Error)
return Bounded_String;

procedure Tail (Source : in out Bounded_String;
Count  : in Natural;
Pad    : in Character := Space;
Drop   : in Truncation := Error);

-- String constructor subprograms

function "*" (Left  : in Natural;
Right : in Character)
return Bounded_String;

function "*" (Left  : in Natural;
Right : in String)
return Bounded_String;

function "*" (Left  : in Natural;
Right : in Bounded_String)
return Bounded_String;

function Replicate (Count : in Natural;
Item  : in Character;
Drop  : in Truncation := Error)
return Bounded_String;

function Replicate (Count : in Natural;
Item  : in String;
Drop  : in Truncation := Error)
return Bounded_String;

function Replicate (Count : in Natural;
Item  : in Bounded_String;
Drop  : in Truncation := Error)
return Bounded_String;

private
... -- not specified by the language
end Generic_Bounded_Length;
end Ada.Strings.Bounded;

This paragraph was deleted.

Implementation Notes: {8652/0097} {AI95-00115-01} {AI95-00344-01} Bounded_String cannot be implemented as a (directly) controlled type, as Ada.Strings.Bounded.Generic_Bounded_Length can be instantiated at any nesting depth. Bounded_String could have a component of a controlled type, as long as that type is declared in some other (nongeneric) package (including directly in Ada.Strings.Bounded).

Null_Bounded_String represents the null string. If an object of type Bounded_String is not otherwise initialized, it will be initialized to the same value as Null_Bounded_String.
The Length function returns the length of the string represented by Source.

If Source'Length <= Max_Length, then this function returns a Bounded_String that represents Source. Otherwise, the effect depends on the value of Drop:

- If Drop=Left, then the result is a Bounded_String that represents the string comprising the rightmost Max_Length characters of Source.
- If Drop=Right, then the result is a Bounded_String that represents the string comprising the leftmost Max_Length characters of Source.
- If Drop=Error, then Strings.Length_Error is propagated.

To_String returns the String value with lower bound 1 represented by Source. If B is a Bounded_String, then B = To_Bounded_String(To_String(B)).

Each of the Append functions returns a Bounded_String obtained by concatenating the string or character given or represented by one of the parameters, with the string or character given or represented by the other parameter, and applying To_Bounded_String to the concatenation result string, with Drop as provided to the Append function.

Each of the procedures Append(Source, New_Item, Drop) has the same effect as the corresponding assignment Source := Append(Source, New_Item, Drop).

Each of the "&" functions has the same effect as the corresponding Append function, with Error as the Drop parameter.

Returns the character at position Index in the string represented by Source; propagates Index_Error if Index > Length(Source).

Updates Source such that the character at position Index in the string represented by Source is By; propagates Index_Error if Index > Length(Source).

1. Returns the slice at positions Low through High in the string represented by Source; propagates Index_Error if Low > Length(Source)+1 or High > Length(Source). The bounds of the returned string are Low and High.
function Bounded_Slice
(Source : in Bounded_String;
Low    : in Positive;
High   : in Natural)
return Bounded_String;

{AI95-00301-01} Returns the slice at positions Low through High in the string represented by Source as a bounded string; propagates Index Error if Low > Length(Source)+1 or High > Length(Source).

procedure Bounded_Slice
(Source : in Bounded_String;
Target : out Bounded_String;
Low    : in Positive;
High   : in Natural);

{AI95-00301-01} Equivalent to Target := Bounded_Slice(Source, Low, High);

Each of the functions "=", "<", ">", "<=", and "=>" returns the same result as the corresponding String operation applied to the String values given or represented by the two parameters.

Each of the search subprograms (Index, Index_Non_Blank, Count, Find_Token) has the same effect as the corresponding subprogram in Strings.Fixed applied to the string represented by the Bounded_String parameter.

Each of the Translate subprograms, when applied to a Bounded_String, has an analogous effect to the corresponding subprogram in Strings.Fixed. For the Translate function, the translation is applied to the string represented by the Bounded_String parameter, and the result is converted (via To_Bounded_String) to a Bounded_String. For the Translate procedure, the string represented by the Bounded_String parameter after the translation is given by the Translate function for fixed-length strings applied to the string represented by the original value of the parameter.

{8652/0049} {AI95-00128-01} Each of the transformation subprograms (Replace_Slice, Insert, Overwrite, Delete), selector subprograms (Trim, Head, Tail), and constructor functions ("*".) has an effect based on its corresponding subprogram in Strings.Fixed, and Replicate is based on Fixed."*". In the case of a function, for each of these subprograms, the corresponding fixed-length string subprogram is applied to the string represented by the Bounded_String parameter. To_Bounded_String is applied to the result string, with Drop (or Error in the case of Generic_Bounded_Length."*") determining the effect when the string length exceeds Max_Length. In the case of a procedure, the corresponding function in Strings.Bounded.Generic_Bounded_Length is applied, with the result assigned into the Source parameter.

Ramification: {AI95-00114-01} The "/=" operations between Bounded_String and String, and between String and Bounded_String, are automatically defined based on the corresponding "=" operations.

Implementation Advice
Bounded string objects should not be implemented by implicit pointers and dynamic allocation.

Implementation Advice: Bounded string objects should not be implemented by implicit pointers and dynamic allocation.

Implementation Note: The following is a possible implementation of the private part of the package:

type Bounded_String_Internals (Length : Length_Range := 0) is
record
  Data : String(1..Length);
end record;
type Bounded_String is
record
  Data : Bounded_String_Internals;  -- Unconstrained
end record;
Null_Bounded_String : constant Bounded_String :=
(Data => (Length => 0,
     Data => (1..0 => ' ')));

Inconsistencies With Ada 95

{AI95-00238-01} Amendment Correction: The bounds of the string returned from Slice are now defined. This is technically an inconsistency; if a program depended on some other lower bound for the string returned from Slice, it could fail when compiled with Ada 2005. Such code is not portable even between Ada 95 implementations, so it should be very rare.

Incompatibilities With Ada 95

{AI95-00301-01} {AI05-0005-1} Procedure Set_Bounded_String, two Bounded_Slice subprograms, and overloaded versions of Index and Index_Non_Blank are needed added to Strings.Bounded_Generic_Bounded_Len. If an instance of Generic_Bounded_Len is referenced in a use_clause, and an entity E with the defining identifier as a new entity in Generic_Bounded_Len is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Wording Changes from Ada 95

{8652/0049} {AI95-00128-01} Corrigendum: Corrected the conditions for which Slice raises Index_Error.

{8652/0049} {AI95-00128-01} Corrigendum: Clarified the meaning of transformation, selector, and constructor subprograms by describing the effects of procedures and functions separately.

Incompatibilities With Ada 2005

{AI05-0031-1} An overloaded version of Find_Token is added to Strings.Bounded_Generic_Bounded_Len. If an instance of Generic_Bounded_Len is referenced in a use_clause, and an entity E with a defining identifier of Find_Token is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

A.4.5 Unbounded-Length String Handling

{AI12-0445-1} The language-defined package Strings.Unbounded provides a private type Unbounded_String and a set of operations. An object of type Unbounded_String represents a String whose low bound is 1 and whose length can vary conceptually between 0 and Natural’Last. The subprograms for fixed-length string handling are either overloaded directly for Unbounded_String, or are modified as necessary needed to reflect the flexibility in length. Since the Unbounded_String type is private, relevant constructor and selector operations are provided.

Reason: The transformation operations for fixed- and bounded-length strings that are not necessarily length preserving are supplied for Unbounded_String as procedures as well as functions. This allows an implementation to do an initial allocation for an unbounded string and to avoid further allocations as long as the length does not exceed the allocated length.

Static Semantics

The library package Strings.Unbounded has the following declaration:

{AI12-0241-1} {AI12-0302-1} with Ada.Strings.Maps;
package Ada.Strings.Unbounded is
   withpragma Preelaborate, Nonblocking, Global => in out synchronized
   is (Unbounded);
{AI95-00161-01} {AI12-0399-1} type Unbounded_String is private;
   withpragma Preelaborable Initialization(Unbounded_String);
   Null_Unbounded_String : constant Unbounded_String;
   function Length (Source : in Unbounded_String) return Natural;
   type String_Access is access all String;
   procedure Free (X : in out String_Access);
   -- Conversion, Concatenation, and Selection functions
function To_Unbounded_String (Source : in String) return Unbounded_String;
function To_Unbounded_String (Length : in Natural) return Unbounded_String;
function To_String (Source : in Unbounded_String) return String;

procedure Set_Unbounded_String (Target : out Unbounded_String; Source : in String);
procedure Append (Source   : in out Unbounded_String; New_Item : in Unbounded_String);
procedure Append (Source   : in out Unbounded_String; New_Item : in String);
procedure Append (Source   : in out Unbounded_String; New_Item : in Character);
function "&" (Left, Right : in Unbounded_String) return Unbounded_String;
function "&" (Left : in Unbounded_String; Right : in String) return Unbounded_String;
function "&" (Left : in String; Right : in Unbounded_String) return Unbounded_String;
function "&" (Left : in Unbounded_String; Right : in Character) return Unbounded_String;
function "&" (Left : in Character; Right : in Unbounded_String) return Unbounded_String;
function Element (Source : in Unbounded_String; Index  : in Positive) return Character;
procedure Replace_Element (Source : in out Unbounded_String; Index  : in Positive; By     : in Character);
function Slice (Source : in Unbounded_String; Low    : in Positive; High   : in Natural) return String;

function Unbounded_Slice (Source : in Unbounded_String; Low    : in Positive; High   : in Natural) return Unbounded_String;

procedure Unbounded_Slice (Source : in Unbounded_String; Target : out Unbounded_String; Low    : in Positive; High   : in Natural);

function "="  (Left, Right : in Unbounded_String) return Boolean;
function "="  (Left : in Unbounded_String; Right : in String) return Boolean;
function "="  (Left : in String; Right : in Unbounded_String) return Boolean;
function "<"  (Left, Right : in Unbounded_String) return Boolean;
function "<"  (Left : in Unbounded_String; Right : in String) return Boolean;
function "<"  (Left : in String; Right : in Unbounded_String) return Boolean;
function "<=" (Left, Right : in Unbounded_String) return Boolean;
function "<="  (Left : in Unbounded_String; Right : in String)  return Boolean;
function "<="  (Left : in String; Right : in Unbounded_String)  return Boolean;
function ">"  (Left, Right : in Unbounded_String) return Boolean;
function ">"  (Left : in Unbounded_String; Right : in String)  return Boolean;
function ">"  (Left : in String; Right : in Unbounded_String)  return Boolean;
function ">="  (Left, Right : in Unbounded_String) return Boolean;
function ">="  (Left : in Unbounded_String; Right : in String)  return Boolean;
function ">="  (Left : in String; Right : in Unbounded_String)  return Boolean;

-- Search subprograms
function Index (Source  : in Unbounded_String;
                Pattern : in String;
                From    : in Positive;
                Going   : in Direction := Forward;
return Natural;

function Index (Source  : in Unbounded_String;
                Pattern : in String;
                From    : in Positive;
                Going   : in Direction := Forward;
                Mapping : in Maps.Character_Mapping_Function)
return Natural;

function Index (Source   : in Unbounded_String;
                Pattern  : in String;
                Going    : in Direction := Forward;
return Natural;

function Index (Source   : in Unbounded_String;
                Pattern  : in String;
                Going    : in Direction := Forward;
                Mapping  : in Maps.Character_Mapping_Function)
return Natural;

function Index (Source  : in Unbounded_String;
                Set     : in Maps.Character_Set;
                From    : in Positive;
                Test    : in Membership := Inside;
                Going   : in Direction := Forward)
return Natural;

function Index (Source : in Unbounded_String;
                Set    : in Maps.Character_Set;
                Test   : in Membership := Inside;
                Going  : in Direction := Forward) return Natural;

function Index_Non_Blank (Source : in Unbounded_String;
                           From     : in Positive;
                           Going    : in Direction := Forward)
return Natural;

function Index_Non_Blank (Source : in Unbounded_String;
                           Going    : in Direction := Forward)
return Natural;
function Count (Source   : in Unbounded_String;
Pattern : in String;
Mapping : in Maps.Character_Mapping
   := Maps.Identity)
return Natural;
function Count (Source   : in Unbounded_String;
Pattern : in String;
Mapping : in Maps.Character_Mapping_Function)
return Natural;
function Count (Source   : in Unbounded_String;
Set      : in Maps.Character_Set)
return Natural;
{AI05-0031-1}
procedure Find_Token (Source :
in Unbounded_String;
   Set    :
in Maps.Character_Set;
   From   :
in Positive;
   Test   :
in Membership;
   First  : out Positive;
   Last   : out Natural);
procedure Find_Token (Source :
in Unbounded_String;
   Set    :
in Maps.Character_Set;
   Test   :
in Membership;
   First  : out Positive;
   Last   : out Natural);
-- String translation subprograms
function Translate (Source  :
in Unbounded_String;
   Mapping :
in Maps.Character_Mapping)
return Unbounded_String;
procedure Translate (Source  :
in out Unbounded_String;
   Mapping :
in Maps.Character_Mapping);
function Translate (Source  :
in Unbounded_String;
   Mapping :
in Maps.Character_Mapping_Function)
return Unbounded_String;
procedure Translate (Source  :
in out Unbounded_String;
   Mapping :
in Maps.Character_Mapping_Function);
-- String transformation subprograms
function Replace_Slice (Source   :
in Unbounded_String;
   Low      :
in Positive;
   High     :
in Natural;
   By       :
in String)
return Unbounded_String;
procedure Replace_Slice (Source   :
in out Unbounded_String;
   Low      :
in Positive;
   High     :
in Natural;
   By       :
in String);
function Insert (Source   :
in Unbounded_String;
   Before   :
in Positive;
   New_Item :
in String)
return Unbounded_String;
procedure Insert (Source   :
in out Unbounded_String;
   Before   :
in Positive;
   New_Item :
in String);
function Overwrite (Source   :
in Unbounded_String;
   Position :
in Positive;
   New_Item :
in String)
return Unbounded_String;
procedure Overwrite (Source   :
in out Unbounded_String;
   Position :
in Positive;
   New_Item :
in String);
function Delete (Source : in Unbounded_String;  
    From : in Positive;  
    Through : in Natural)  
return Unbounded_String;

procedure Delete (Source : in out Unbounded_String;  
    From : in Positive;  
    Through : in Natural);

function Trim (Source : in Unbounded_String;  
    Side : in Trim_End)  
return Unbounded_String;

procedure Trim (Source : in out Unbounded_String;  
    Side : in Trim_End);

function Trim (Source : in Unbounded_String;  
    Left : in Maps.Character_Set;  
    Right : in Maps.Character_Set)  
return Unbounded_String;

procedure Trim (Source : in out Unbounded_String;  
    Left : in Maps.Character_Set;  
    Right : in Maps.Character_Set);

function Head (Source : in Unbounded_String;  
    Count : in Natural;  
    Pad : in Character := Space)  
return Unbounded_String;

procedure Head (Source : in out Unbounded_String;  
    Count : in Natural;  
    Pad : in Character := Space);

function Tail (Source : in Unbounded_String;  
    Count : in Natural;  
    Pad : in Character := Space)  
return Unbounded_String;

procedure Tail (Source : in out Unbounded_String;  
    Count : in Natural;  
    Pad : in Character := Space);

function ** (Left : in Natural;  
    Right : in Character)  
return Unbounded_String;

function ** (Left : in Natural;  
    Right : in String)  
return Unbounded_String;

function ** (Left : in Natural;  
    Right : in Unbounded_String)  
return Unbounded_String;

private  
    ... -- not specified by the language
end Ada.Strings.Unbounded;

{AI95-00360-01} The type Unbounded_String needs finalization (see 7.6).

Null_Unbounded_String represents the null String. If an object of type Unbounded_String is not 
otherwise initialized, it will be initialized to the same value as Null_Unbounded_String.

The function Length returns the length of the String represented by Source.

The type String_Access provides a (nonprivate) access type for explicit processing of unbounded-length 
strings. The procedure Free performs an unchecked deallocation of an object of type String_Access.

The function To_Unbounded_String(Source : in String) returns an Unbounded_String that represents 
Source. The function To_Unbounded_String(Length : in Natural) returns an Unbounded_String that 
represents an uninitialized String whose length is Length.
The function To_String returns the String with lower bound 1 represented by Source. To_String and To_Unbounded_String are related as follows:

- If S is a String, then To_String(To_Unbounded_String(S)) = S.
- If U is an Unbounded_String, then To_Unbounded_String(To_String(U)) = U.

The procedure Set_Unbounded_String sets Target to an Unbounded_String that represents Source.

For each of the Append procedures, the resulting string represented by the Source parameter is given by the concatenation of the original value of Source and the value of New_Item.

Each of the "&" functions returns an Unbounded_String obtained by concatenating the string or character given or represented by one of the parameters, with the string or character given or represented by the other parameter, and applying To_Unbounded_String to the concatenation result string.

Ramification: If the resulting string is longer than Natural'Last, Constraint_Error is raised because the upper bound of the underlying String concatenation is outside of the range of the index subtype of Natural (see 4.5.3). Note that the same is true for other operations that attempt to create an overlong string; either they are defined in terms of this concatenation operation (as with Append) or they are defined in terms of Ada.Strings.Fixed operations (as with Insert and Replace_Slice), which themselves are defined in terms of String concatenation (which raises Constraint_Error for overlong strings as described above). Therefore, it is never possible to create an Unbounded_String with a length greater than Natural'Last.

The Element, Replace_Element, and Slice subprograms have the same effect as the corresponding bounded-length string subprograms.

The function Unbounded_Slice returns the slice at positions Low through High in the string represented by Source as an Unbounded_String. The procedure Unbounded_Slice sets Target to the Unbounded_String representing the slice at positions Low through High in the string represented by Source. Both subprograms propagate Index_Error if Low > Length(Source)+1 or High > Length(Source).

Each of the functions ",", ",", ",", ",", and "," returns the same result as the corresponding String operation applied to the String values given or represented by Left and Right.

Each of the search subprograms (Index, Index_Non_Blank, Count, Find_Token) has the same effect as the corresponding subprogram in Strings.Fixed applied to the string represented by the Unbounded_String parameter.

The Translate function has an analogous effect to the corresponding subprogram in Strings.Fixed. The translation is applied to the string represented by the Unbounded_String parameter, and the result is converted (via To_Unbounded_String) to an Unbounded_String.

Each of the transformation functions (Replace_Slice, Insert, Overwrite, Delete), selector functions (Trim, Head, Tail), and constructor functions ("*") is likewise analogous to its corresponding subprogram in Strings.Fixed. For each of the subprograms, the corresponding fixed-length string subprogram is applied to the string represented by the Unbounded_String parameter, and To_Unbounded_String is applied to the resulting string.

For each of the procedures Translate, Replace_Slice, Insert, Overwrite, Delete, Trim, Head, and Tail, the resulting string represented by the Source parameter is given by the corresponding function for fixed-length strings applied to the string represented by Source's original value.

Implementation Requirements

No storage associated with an Unbounded_String object shall be lost upon assignment or scope exit.
Implementation Note: \{AI95-00301-01\} A sample implementation of the private part of the package and several of the subprograms appears in the Ada 95 Rationale.

Incompatibilities With Ada 95

\{AI95-00360-01\} Amendment Correction: Type Unbounded String is defined to need finalization. If the restriction No Nested Finalization (see D.7) applies to the partition, and Unbounded String does not have a controlled part, it will not be allowed in local objects in Ada 2005 whereas it would be allowed in original Ada 95. Such code is not portable, as most Ada compilers have a controlled part in Unbounded String, and thus would be illegal.

\{AI95-00301-01\} \{AI05-0005-1\} Procedure Set Unbounded String, two Unbounded Slice subprograms, and overloaded versions of Index and Index Non Blank are newly added to Strings.Unbounded. If Strings.Unbounded is referenced in a use_clause, and an entity \(E\) with the same defining_identifier as a new entity in Strings.Unbounded is defined in a package that is also referenced in a use_clause, the entity \(E\) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 95

\{AI95-00161-01\} Amendment Correction: Added a pragma Preelaborable_Initialization to type Unbounded String, so that it can be used to declare default-initialized objects in preelaborated units.

Incompatibilities With Ada 2005

\{AI05-0031-1\} An overloaded version of Find_Token is added to Strings.Unbounded. If Strings.Unbounded is referenced in a use_clause, and an entity \(E\) with a defining_identifier of Find_Token is defined in a package that is also referenced in a use_clause, the entity \(E\) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

A.4.6 String-Handling Sets and Mappings


Discussion: The Constants package is a child of Strings.Maps since it needs visibility of the private part of Strings.Maps in order to initialize the constants in a preelaborable way (i.e. via aggregates versus function calls).

Static Semantics

The library package Strings.Maps.Constants has the following declaration:

\{AI95-00362-01\} \{AI12-0414-1\} package Ada.Strings.Maps.Constants is

  withpragma PurePreelaborate is (Constants);

  Control_Set : constant Character_Set;
  Graphic_Set : constant Character_Set;
  Letter_Set : constant Character_Set;
  Lower_Set : constant Character_Set;
  Basic_Set : constant Character_Set;
  Decimal_Digit_Set : constant Character_Set;
  Hexadecimal_Digit_Set : constant Character_Set;
  Alphanumeric_Set : constant Character_Set;
  Special_Set : constant Character_Set;
  ISO_646_Set : constant Character_Set;
  Lower_Case_Map : constant Character_Mapping;
    -- Maps to lower case for letters, else identity
  Upper_Case_Map : constant Character_Mapping;
    -- Maps to upper case for letters, else identity
  Basic_Map : constant Character_Mapping;
    -- Maps to basic letter for letters, else identity

private
  ... -- not specified by the language
end Ada.Strings.Maps.Constants;

Each of these constants represents a correspondingly named set of characters or character mapping in Characters.Handling (see A.3.2).
A.4.6 String-Handling Sets and Mappings

NOTE {AI05-0114-1} {AI12-0450-1} There are certain characters which are defined to be lower case letters by ISO/IEC 10646 and are therefore allowed in identifiers, but are not considered lower case letters by Ada.Strings.Maps.Constants. Reason: This is to maintain runtime compatibility with the Ada 95 definitions of these constants; existing correct programs could break if the definitions were changed in a way the programs did not anticipate.

A.4.7 Wide_String Handling


Static Semantics

The package Strings.Wide_Maps has the following declaration.

{AI12-0241-1} {AI12-0302-1} package Ada.Strings.Wide_Maps is
withpragma Preelaborate, Nonblocking, Global => in out synchronized
is (Wide_Maps);

{AI95-00161-01} {AI12-0399-1} -- Representation for a set of Wide_Character values:
type Wide_Character_Set is private;
withpragma Preelaborable_Initialization (Wide_Character_Set);

Null_Set : constant Wide_Character_Set;

type Wide_Character_Range is record
  Low  : Wide_Character;
  High : Wide_Character;
end record;
-- Represents Wide_Character range Low..High

type Wide_Character_Ranges is array (Positive range <>) of Wide_Character_Range;

function To_Set (Ranges : in Wide_Character_Ranges) return Wide_Character_Set;

function To_Set (Span   : in Wide_Character_Range) return Wide_Character_Set;

function To_Ranges (Set    : in Wide_Character_Set) return Wide_Character_Ranges;

function "=" (Left, Right : in Wide_Character_Set) return Boolean;
function "not" (Right : in Wide_Character_Set) return Wide_Character_Set;
function "and" (Left, Right : in Wide_Character_Set) return Wide_Character_Set;
function "or" (Left, Right : in Wide_Character_Set) return Wide_Character_Set;
function "xor" (Left, Right : in Wide_Character_Set) return Wide_Character_Set;
function "-" (Left, Right : in Wide_Character_Set) return Wide_Character_Set;
function Is_In (Element : in Wide_Character; Set : in Wide_Character_Set) return Boolean;
function Is_Subset (Elements : in Wide_Character_Set; Set : in Wide_Character_Set) return Boolean;
function "<=" (Left : in Wide_Character_Set; Right : in Wide_Character_Set) return Boolean renames Is_Subset;
-- Alternative representation for a set of Wide_Character values:
subtype Wide_Character_Sequence is Wide_String;
function To_Set (Sequence : in Wide_Character_Sequence) return Wide_Character_Set;
function To_Set (Singleton : in Wide_Character) return Wide_Character_Set;
function To_Sequence (Set : in Wide_Character_Set) return Wide_Character_Sequence;

{AI95-00161-01} {AI12-0399-1} -- Representation for a Wide_Character to Wide_Character mapping:

{AI95-00161-01} {AI12-0399-1} -- Representation for a Wide_Character to Wide_Character mapping:

type Wide_Character_Mapping is private;
withpragma Preelaborable_Initialization(Wide_Character_Mapping);
function Value (Map : in Wide_Character_Mapping; Element : in Wide_Character) return Wide_Character;
Identity : constant Wide_Character_Mapping;
function To_Mapping (From, To : in Wide_Character_Sequence) return Wide_Character_Mapping;
function To_Domain (Map : in Wide_Character_Mapping) return Wide_Character_Sequence;
function To_Range (Map : in Wide_Character_Mapping) return Wide_Character_Sequence;
type Wide_Character_Mapping_Function is access function (From : in Wide_Character) return Wide_Character;
private
... -- not specified by the language
end Ada.Strings.Wide_Maps;

The context clause for each of the packages Strings.Wide_Fixed, Strings.Wide_Bounded, and Strings.Wide_Unbounded identifies Strings.Wide_Maps instead of Strings.Maps.

{AI95-00223-1} Types Wide_Character_Set and Wide_Character_Mapping need finalization.

Insensitive, Strings.Bounded.Equal_CaseInsensitive, and Strings.Unbounded.Equal_CaseInsensitive, the corresponding wide string package or function has the same contents except that

- Wide_Space replaces Space
- Wide_Character replaces Character
- Wide_String replaces String
- Wide_Character_Set replaces Character_Set
- Wide_Character_Mapping replaces Character_Mapping
- Wide_Character_Mapping_Function replaces Character_Mapping_Function
- Wide_Maps replaces Maps
- Bounded_Wide_String replaces Bounded_String
- Null_Bounded_Wide_String replaces Null_Bounded_String
- To_Bounded_Wide_String replaces To_Bounded_String
- To_Wide_String replaces To_String
- \{AI95-00301-01\} Set_Bounded_Wide_String replaces Set_Bounded_String
- Unbounded_Wide_String replaces Unbounded_String
- Null_Unbounded_Wide_String replaces Null_Unbounded_String
- Wide_String_Access replaces String_Access
- To_Unbounded_Wide_String replaces To_Unbounded_String
- \{AI95-00395-01\} Set_Unbounded_Wide_String replaces Set_Unbounded_String

The following additional declaration is present in Strings.Wide_Maps.Wide_Constants:

\{AI95-00395-01\} \{AI95-00395-01\} Character_Set : constant
Wide_Maps.Wide_Character_Set;
-- Contains each Wide_Character value WC such that
-- Characters.Conversions.Is_Character(WC) is True

\{AI95-00395-01\} Each Wide_Character_Set constant in the package Strings.Wide_Maps.Wide_Constants contains no values outside the Character portion of Wide_Character. Similarly, each Wide_Character_Mapping constant in this package is the identity mapping when applied to any element outside the Character portion of Wide_Character.

\{AI95-00362-01\} \{AI12-0302-1\} \{AI12-0414-1\} AspectPragma Pure is replaced by aspects Preelaborate, Nonblocking, Global => in out synchronizedpragma Preelaborate in Strings.Wide_Maps.Wide_Constants.

NOTE If a null Wide_Character_Mapping_Function is passed to any of the Wide_String handling subprograms, Constraint_Error is propagated.

NOTE \{AI95-00395-01\} Each Wide_Character_Set constant in the package Strings.Wide_Maps.Wide_Constants contains no values outside the Character portion of Wide_Character. Similarly, each Wide_Character_Mapping constant in this package is the identity mapping when applied to any element outside the Character portion of Wide_Character.

Incompatibilities With Ada 95

\{AI95-00301-01\} Various new operations are added to Strings.Wide_Fixed, Strings.Wide_Bounded, and Strings.Wide_Unbounded. If one of these packages is referenced in a use_clause, and an entity \(E\) with the same defining identifier as a new entity is defined in a package that is also referenced in a use_clause, the entity \(E\) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.
A.4.7 Extensions to Ada 95

Amendment Correction: Added pragma Preelaborable Initialization to types Wide_Character_Set and Wide_Character_Mapping, so that they can be used to declare default-initialized objects in preelaborated units.

Wording Changes from Ada 95

Corrected the description of Character_Set.


Added wording so that Strings.Wide_Maps.Wide_Constants does not change to Pure.

The second Note is now normative text, since there is no way to derive it from the other rules. It's a little weird given the use of Unicode character classifications in Ada 2005; but changing it would be inconsistent with Ada 95 and a one-to-one mapping isn't necessarily correct anyway.

A.4.8 Wide_Wide_String Handling


Static Semantics

The library package Strings.Wide_Wide_Maps has the following declaration.

\[
\text{package Ada.Strings.Wide_Wide_Maps is}
\]

withpragma Preelaborate Nonblocking Global => \text{in out synchronized}

\[
\text{is (Wide_Wide_Maps);}\]

-- Representation for a set of Wide_Wide_Character values:

\[
\text{type Wide_Wide_Character_Set is private withpragma Preelaborable Initialization(Wide_Wide_Character_Set)};\]

Null_Set : constant Wide_Wide_Character_Set;

\[
\text{type Wide_Wide_Character_Range is record}

\quad \text{Low : Wide_Wide_Character;}

\quad \text{High : Wide_Wide_Character;}

\quad \text{end record;}

\quad -- Represents Wide_Wide_Character range Low..High\]
type Wide_Wide_Character_Ranges is array (Positive range <>) of Wide_Wide_Character_Range;

function To_Set (Ranges : in Wide_Wide_Character_Ranges) return Wide_Wide_Character_Set;
function To_Set (Span : in Wide_Wide_Character_Range) return Wide_Wide_Character_Set;
function To_Ranges (Set : in Wide_Wide_Character_Set) return Wide_Wide_Character_Ranges;

function 
  (Left, Right : in Wide_Wide_Character_Set) return Boolean;
function 
  (Right : in Wide_Wide_Character_Set) return Wide_Wide_Character_Set;
function 
  (Left, Right : in Wide_Wide_Character_Set) return Wide_Wide_Character_Set;
function 
  (Left, Right : in Wide_Wide_Character_Set) return Wide_Wide_Character_Set;
function 
  (Left, Right : in Wide_Wide_Character_Set) return Wide_Wide_Character_Set;
function 
  (Left, Right : in Wide_Wide_Character_Set) return Wide_Wide_Character_Set;
function 
  (Right : in Wide_Wide_Character_Set) return Wide_Wide_Character_Set;
function 
  (Left : in Wide_Wide_Character_Set; Right : in Wide_Wide_Character_Set) return Boolean renames Is_Subset;

-- Alternative representation for a set of Wide_Wide_Character values:
subtype Wide_Wide_Character_Sequence is Wide_Wide_String;
function To_Set (Sequence : in Wide_Wide_Character_Sequence) return Wide_Wide_Character_Set;
function To_Set (Singleton : in Wide_Wide_Character) return Wide_Wide_Character_Set;
function To_Sequence (Set : in Wide_Wide_Character_Set) return Wide_Wide_Character_Sequence;

{AI12-0399-1} -- Representation for a Wide_Wide_Character to Wide_Wide_Character mapping:
type Wide_Wide_Character_Mapping is private;
withpragma Preelaborable_Initialization (Wide_Wide_Character_Mapping);

function Value (Map : in Wide_Wide_Character_Mapping; Element : in Wide_Wide_Character) return Wide_Wide_Character;

Identity : constant Wide_Wide_Character_Mapping;
function To_Mapping (From, To : in Wide_Wide_Character_Sequence) return Wide_Wide_Character_Mapping;
function To_Domain (Map : in Wide_Wide_Character_Mapping) return Wide_Wide_Character_Sequence;
function To_Range (Map : in Wide_Wide_Character_Mapping) return Wide_Wide_Character_Sequence;

type Wide_Wide_Character_Mapping_Function is
  access function (From : in Wide_Wide_Character) return Wide_Wide_Character;

private
  ... -- not specified by the language
end Ada.Strings.Wide_Wide_Maps;
The context clause for each of the packages Strings.Wide_Wide_Fixed, Strings.Wide_Wide_Bounded, and Strings.Wide_Wide_Unbounded identifies Strings.Wide_Wide_Maps instead of Strings.Maps.

Types Wide_Wide_Character_Set and Wide_Wide_Character_Mapping need finalization.


- Wide_Wide_Space replaces Space
- Wide_Wide_Character replaces Character
- Wide_Wide_String replaces String
- Wide_Wide_Character_Set replaces Character_Set
- Wide_Wide_Character_Mapping replaces Character_Mapping
- Wide_Wide_Character_Mapping_Function replaces Character_Mapping_Function
- Wide_Wide_Maps replaces Maps
- Bounded_Wide_Wide_String replaces Bounded_String
- Null_Bounded_Wide_Wide_String replaces Null_Bounded_String
- To_Bounded_Wide_Wide_String replaces To_Bounded_String
- To_Wide_Wide_String replaces To_String
- Set_Bounded_Wide_Wide_String replaces Set_Bounded_String
- Unbounded_Wide_Wide_String replaces Unbounded_String
- Null_Unbounded_Wide_Wide_String replaces Null_Unbounded_String
- Wide_Wide_String_Access replaces String_Access
- To_Unbounded_Wide_Wide_String replaces To_Unbounded_String
- Set_Unbounded_Wide_Wide_String replaces Set_Unbounded_String

The following additional declarations are present in Strings.Wide_Wide_Maps.Wide_Wide_Constants:

```ada
Character_Set : constant Wide_Wide_Maps.Wide_Wide_Character_Set;
   -- Contains each Wide_Wide_Character value WWC such that
   -- Characters.Conversions.Is_Character(WWC) is True
Wide_Character_Set : constant Wide_Wide_Maps.Wide_Wide_Character_Set;
   -- Contains each Wide_Wide_Character value WWC such that
   -- Characters.Conversions.Is_Wide_Character(WWC) is True
```

Each Wide_Wide_Character_Set constant in the package Strings.Wide_Wide_Maps.Wide_Wide_Constants contains no values outside the Character portion of Wide_Wide_Character. Similarly, each Wide_Wide_Character_Mapping constant in this package is the identity mapping when applied to any element outside the Character portion of Wide_Wide_Character.

AspectPragma Pure is replaced by aspects Preelaborate, Nonblocking, Global => in out synchronizedpragma Preelaborate in Strings.Wide_Wide_Maps.Wide_Wide_Constants.
NOTE {AI95-00285-01} If a null Wide_Wide_Character_Mapping Function is passed to any of the Wide_Wide_String handling subprograms, Constraint_Error is propagated.

Extensions to Ada 95

{AI95-00285-01} {AI95-00395-01} The double-wide string-handling packages (Strings.Wide_Wide_Maps, Strings.Wide_Wide_Fixed, Strings.Wide_Wide_Bounded, Strings.Wide_Wide_Unbounded, and Strings.Wide_Wide_Maps.Wide_Wide_Constants), and functions Strings.Wide_Wide_Hash and Strings.Wide_Wide_Unbounded.Wide_Wide_Hash are new.

Extensions to Ada 2005

{AI05-0286-1} The case insensitive library functions (Strings.Wide_Wide_Equal_CaseInsensitive, Strings.Wide_Wide_Fixed.Wide_Wide_Equal_CaseInsensitive, Strings.Wide_Wide_Bounded.Wide_Wide_Equal_CaseInsensitive, Strings.Wide_Wide_Hash.Wide_Wide_Equal_CaseInsensitive, Strings.Wide_Wide_Bounded.Wide_Wide_Hash.Wide_Wide_Equal_CaseInsensitive, and Strings.Wide_Wide_Unbounded.Wide_Wide_Hash.Wide_Wide_Equal_CaseInsensitive) are new.

Wording Changes from Ada 2005

{AI05-0223-1} Correction: Identified Wide Wide Character Set and Wide Wide Character Mapping as needing finalization. It is likely that they are implemented with a controlled type, so this change is unlikely to make any difference in practice.

A.4.9 String Hashing

Static Semantics

{AI95-00302-03} The library function Strings.Hash has the following declaration:

```ada
with Ada.Containers;
function Ada.Strings.Hash (Key : String) return Containers.Hash_Type;
withpragma Pure(Ada.Strings.Hash Hash);
```

Returns an implementation-defined value which is a function of the value of Key. If A and B are strings such that A equals B, Hash(A) equals Hash(B).

Implementation defined: The values returned by Strings.Hash.

{AI95-00302-03} The library function Strings.Fixed.Hash has the following declaration:

```ada
function Ada.Strings.Fixed.Hash (Key : String) return Containers.Hash_Type
renames Ada.Strings.Hash;
pragma Pure(Hash);
```

{AI95-00302-03} The generic library function Strings.Bounded.Hash has the following declaration:

```ada
with Ada.Containers;
generic
with package Bounded is new Ada.Strings.Bounded.Generic_Bounded_Length (<>);
return Containers.Hash_Type;
withpragma Preelaborate, Nonblocking, Global => in out,
synchronized(Ada.Strings.Bounded.HashHash);
```

{AI05-0001-1} Equivalent toStrings.Bounded.Hash is equivalent to the function call Strings.Hash (Bounded.To_String (Key));

{AI95-00302-03} The library function Strings.Unbounded.Hash has the following declaration:

```ada
with Ada.Containers;
generic
with package Bounded is new Ada.Strings.Bounded.Generic_Bounded_Length (<>);
function Ada.Strings.Unbounded.Hash (Key : Unbounded_String)
return Containers.Hash_Type;
withpragma Preelaborate, Nonblocking, Global => in out,
synchronized(Ada.Strings.Unbounded.HashHash);
```


The Hash functions should be good hash functions, returning a wide spread of values for different string values. It should be unlikely for similar strings to return the same value.

Implementation Advice: Strings.Hash should be a good hash function, returning a wide spread of values for different string values, and similar strings should rarely return the same value.

Ramification: The other functions are defined in terms of Strings.Hash, so they don't need separate advice in the Annex.

Extensions to Ada 95


Extensions to Ada 2005

### A.4.10 String Comparison

#### Static Semantics

The library function `Ada.Strings.Equal_CaseInsensitive` has the following declaration:

```ada
function Ada.Strings.Equal_CaseInsensitive (Left, Right : String) return Boolean with
  pragma Pure(Ada.Strings.Equal_CaseInsensitive);
```

Returns True if the strings consist of the same sequence of characters after applying locale-independent simple case folding, as defined by documents referenced in the note in Clause 21 of ISO/IEC 10646:2020. Otherwise, returns False. This function uses the same method as is used to determine whether two identifiers are the same.

**Discussion:** For `String`, this is equivalent to converting to lower case and comparing. Not so for other string types. For `Wide_Strings` and `Wide_Wide_Strings`, note that this result is a more accurate comparison than converting the strings to lower case and comparing the results; it is possible that the lower case conversions are the same but this routine will report the strings as different. Additionally, Unicode says that the result of this function will never change for strings made up solely of defined code points; there is no such guarantee for case conversion to lower case.

The “documents referenced” means Unicode, Chapter 4 (specifically, section 4.2 — Case). See the Implementation Notes in 2.3 for a source for machine-readable definitions of these properties.

The library function `Ada.Strings.Fixed.Equal_CaseInsensitive` has the following declaration:

```ada
with Ada.Strings.Equal_CaseInsensitive;
function Ada.Strings.Fixed.Equal_CaseInsensitive (Left, Right : String) return Boolean
renames Ada.Strings.Equal_CaseInsensitive;
```

The generic library function `Ada.Strings.Bounded.Equal_CaseInsensitive` has the following declaration:

```ada
generic
with package Bounded is
  new Ada.Strings.Bounded.Generic_Bounded_Length (<>);
withpragma Preelaborate, Nonblocking, Global => in out synchronized(Ada.Strings.Bounded.Equal_CaseInsensitive);
```

Equivalent to `Strings.Equal_CaseInsensitive (Bounded.To_String (Left), Bounded.To_String (Right));`

The library function `Ada.Strings.Unbounded.Equal_CaseInsensitive` has the following declaration:

```ada
withpragma Preelaborate, Nonblocking, Global => in out synchronized(Ada.Strings.Unbounded.Equal_CaseInsensitive);
function Ada.Strings.Unbounded.Equal_CaseInsensitive (Left, Right : Unbounded_String) return Boolean;
```

Equivalent to `Strings.Equal_CaseInsensitive (To_String (Left), To_String (Right));`

The library function `Ada.Strings.Less_CaseInsensitive` has the following declaration:

```ada
function Ada.Strings.Less_CaseInsensitive (Left, Right : String) return Boolean with
  pragma Pure(Ada.Strings.Less_CaseInsensitive);
```
Performs a lexicographic comparison of strings Left and Right, converted to lower case.

The library function `Strings.Fixed.Less_Case_Insensitive` has the following declaration:

```ada
with Ada.Strings.Less_Case_Insensitive;
function Ada.Strings.Fixed.Less_Case_Insensitive
(Left, Right : String) return Boolean
renames Ada.Strings.Less_Case_Insensitive;
```

The generic library function `Strings.Bounded.Less_Case_Insensitive` has the following declaration:

```ada
generic
with package Bounded is
new Ada.Strings.Bounded.Generic_Bounded_Length (<>);
function Ada.Strings.Bounded.Less_Case_Insensitive
(Left, Right : Bounded.Bounded_String) return Boolean;
```

Equivalent to `Strings.Less_Case_Insensitive (Bounded.To_String (Left), Bounded.To_String (Right));`

The library function `Strings.Unbounded.Less_Case_Insensitive` has the following declaration:

```ada
function Ada.Strings.Unbounded.Less_Case_Insensitive
(Left, Right : Unbounded_String) return Boolean;
```

Equivalent to `Strings.Less_Case_Insensitive (To_String (Left), To_String (Right));`

String Encoding

Facilities for encoding, decoding, and converting strings in various character encoding schemes are provided by packages `Strings.UTF_Encoding`, `Strings.UTF_Encoding.Conversions`, `Strings.UTF_Encoding.Strings`, `Strings.UTF_Encoding.Wide_Strings`, and `Strings.UTF_Encoding.Wide_Wide_Strings`.

Static Semantics

The encoding library packages have the following declarations:

```ada
package Ada.Strings.UTF_Encoding is
withpragma Pure is (UTF_Encoding);
-- Declarations common to the string encoding packages
type Encoding_Scheme is (UTF_8, UTF_16BE, UTF_16LE);
subtype UTF_String is String;
subtype UTF_8_String is String;
subtype UTF_16_Wide_String is Wide_String;
Encoding_Error : exception;
```
BOM_8 : constant UTF_8_String :=
Character'Val(16#EF#) &
Character'Val(16#BB#) &
Character'Val(16#BF#);

BOM_16BE : constant UTF_String :=
Character'Val(16#FE#) &
Character'Val(16#FF#);

BOM_16LE : constant UTF_String :=
Character'Val(16#FF#) &
Character'Val(16#FE#);

BOM_16 : constant UTF_16_Wide_String :=
(1 => Wide_Character'Val(16#FEFF#));

function Encoding (Item    : UTF_String;
Default : Encoding_Scheme := UTF_8)
return Encoding_Scheme;
end Ada.Strings.UTF_Encoding;

{AI05-0137-2} {AI12-0414-1} package Ada.Strings.UTF_Encoding.Conversions is
withpragma Pure is (Conversions);

-- Conversions between various encoding schemes
function Convert (Item          : UTF_String;
Input_Scheme  : Encoding_Scheme;
Output_BOM    : Boolean := False)
return UTF_String;

function Convert (Item          : UTF_String;
Input_Scheme  : Encoding_Scheme;
Output_BOM    : Boolean := False)
return UTF_16_Wide_String;

function Convert (Item          : UTF_8_String;
Output_BOM    : Boolean := False)
return UTF_16_Wide_String;

function Convert (Item          : UTF_16_Wide_String;
Output_Scheme : Encoding_Scheme;
Output_BOM    : Boolean := False)
return UTF_String;

function Convert (Item          : UTF_16_Wide_String;
Output_BOM    : Boolean := False)
return UTF_8_String;
end Ada.Strings.UTF_Encoding.Conversions;

{AI05-0137-2} {AI12-0414-1} package Ada.Strings.UTF_Encoding.Strings is
withpragma Pure is (Strings);

-- Encoding / decoding between String and various encoding schemes
function Encode (Item       : String;
Output_Scheme : Encoding_Scheme;
Output_BOM    : Boolean := False)
return UTF_8_String;

function Encode (Item       : String;
Output_BOM    : Boolean := False)
return UTF_16_Wide_String;

function Encode (Item       : String;
Output_BOM    : Boolean := False)
return UTF_16_Wide_String;

function Encode (Item       : UTF_String;
Input_Scheme : Encoding_Scheme) return String;

function Decode (Item : UTF_8_String) return String;

function Decode (Item : UTF_16_Wide_String) return String;
end Ada.Strings.UTF_Encoding.Strings;

{AI05-0137-2} {AI12-0414-1} package Ada.Strings.UTF_Encoding.Wide_Strings is
withpragma Pure is (Wide_Strings);
-- Encoding / decoding between Wide_String and various encoding schemes
function Encode (Item          : Wide_String;
                 Output_Scheme : Encoding_Scheme;
                 Output_BOM    : Boolean  := False) return UTF_String;
function Encode (Item          : Wide_String;
                 Output_BOM    : Boolean  := False) return UTF_8_String;
function Encode (Item          : Wide_String;
                 Output_BOM    : Boolean  := False) return UTF_16_Wide_String;

function Decode (Item         : UTF_String;
                 Input_Scheme : Encoding_Scheme) return Wide_String;
function Decode (Item : UTF_8_String) return Wide_String;
function Decode (Item : UTF_16_Wide_String) return Wide_String;
end Ada.Strings.UTF_Encoding.Wide_Strings;

package Ada.Strings.UTF_Encoding.Wide_Wide_Strings is
  withpragma Pure is (Wide_Wide_Strings);
  -- Encoding / decoding between Wide_Wide_String and various encoding schemes
  function Encode (Item          : Wide_Wide_String;
                   Output_Scheme : Encoding_Scheme;
                   Output_BOM    : Boolean  := False) return UTF_String;
  function Encode (Item          : Wide_Wide_String;
                   Output_BOM    : Boolean  := False) return UTF_8_String;
  function Encode (Item          : Wide_Wide_String;
                   Output_BOM    : Boolean  := False) return UTF_16_Wide_String;
  function Decode (Item         : UTF_String;
                   Input_Scheme : Encoding_Scheme) return Wide_Wide_String;
  function Decode (Item : UTF_8_String) return Wide_Wide_String;
  function Decode (Item : UTF_16_Wide_String) return Wide_Wide_String;
end Ada.Strings.UTF_Encoding.Wide_Wide_Strings;

{AI05-0137-2} {AI92-0414-1} The type Encoding_Scheme defines encoding schemes. UTF_8 corresponds to the UTF-8 encoding scheme defined by Annex D of ISO/IEC 10646. UTF_16BE corresponds to the UTF-16 encoding scheme defined by Annex C of ISO/IEC 10646 in 8 bit, big-endian order; and UTF_16BE corresponds to the UTF-16 encoding scheme in 8 bit, little-endian order.

{AI05-0137-2} The subtype UTF_String is used to represent a String of 8-bit values containing a sequence of values encoded in one of three ways (UTF-8, UTF-16BE, or UTF-16LE). The subtype UTF_8_String is used to represent a String of 8-bit values containing a sequence of values encoded in UTF-8. The subtype UTF_16_Wide_String is used to represent a Wide_String of 16-bit values containing a sequence of values encoded in UTF-16.

{AI05-0137-2} The BOM_8, BOM_16BE, BOM_16LE, and BOM_16 constants correspond to values used at the start of a string to indicate the encoding.

{AI05-0262-1} Each of the Encode functions takes a String, Wide_String, or Wide_Wide_String Item parameter that is assumed to be an array of unencoded characters. Each of the Convert functions takes a UTF_String, UTF_8_String, or UTF_16_String Item parameter that is assumed to contain characters whose position values correspond to a valid encoding sequence according to the encoding scheme required by the function or specified by its Input_Scheme parameter.

{AI05-0137-2} Each of the Convert and Encode functions returns a UTF_String, UTF_8_String, or UTF_16_String value whose characters have position values that correspond to the encoding of the Item parameter according to the encoding scheme required by the function or specified by its Output_Scheme parameter. For UTF_8, no overlong encoding is returned. A
BOM is included at the start of the returned string if the Output_BOM parameter is set to True. The lower bound of the returned string is 1.

{AI05-0137-2} Each of the Decode functions takes a UTF String, UTF 8 String, or UTF 16 String Item parameter which is assumed to contain characters whose position values correspond to a valid encoding sequence according to the encoding scheme required by the function or specified by its Input_Scheme parameter, and returns the corresponding String, Wide String, or Wide Wide String value. The lower bound of the returned string is 1.

{AI05-0137-2} For each of the Convert and Decode functions, an initial BOM in the input that matches the expected encoding scheme is ignored, and a different initial BOM causes Encoding_Error to be propagated.

{AI05-0137-2} The exception Encoding_Error is also propagated in the following situations:

- {AI12-0088-1} By a Convert or Decode function when a UTF encoded string contains an invalid encoding sequence.

To be honest: {AI12-0088-1} An overlong encoding is not invalid for the purposes of this check, and this does not depend on the character set version in use. Some recent character set standards declare overlong encodings to be invalid; it would be unnecessary and unfriendly to users for Convert or Decode to raise an exception for an overlong encoding.

- {AI12-0088-1} By a Convert or Decode function when the expected encoding is UTF-16BE or UTF-16LE and the input string has an odd length.

- {AI05-0262-1} By a Decode function yielding a String when the decoding of a sequence results in a code point whose value exceeds 16#FF#.

- By a Decode function yielding a Wide String when the decoding of a sequence results in a code point whose value exceeds 16#FFFF#.

- {AI05-0262-1} By an Encode function taking a Wide_String as input when an invalid character appears in the input. In particular, the characters whose position is in the range 16#D800# .. 16#DFFF# are invalid because they conflict with UTF-16 surrogate encodings, and the characters whose position is 16#FFE# or 16#FFFF# are also invalid because they conflict with BOM codes.

{AI05-0137-2} function Encoding (Item : UTF_String; Default : Encoding_Scheme := UTF_8) return Encoding_Scheme;

{AI05-0137-2} {AI05-0269-1} Inspects a UTF_String value to determine whether it starts with a BOM for UTF-8, UTF-16BE, or UTF 16LE. If so, returns the scheme corresponding to the BOM; otherwise, returns the value of Default.

{AI05-0137-2} function Convert (Item : UTF_String; Input_Scheme : Encoding_Scheme; Output_BOM : Boolean := False) return UTF_String;

Returns the value of Item (originally encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by Input_Scheme) encoded in one of these three schemes as specified by Output_Scheme.

{AI05-0137-2} function Convert (Item : UTF_String; Input_Scheme : Encoding_Scheme; Output_BOM : Boolean := False) return UTF_16Wide_String;

Returns the value of Item (originally encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by Input_Scheme) encoded in UTF-16.
{{AI05-0137-2}} \textbf{function} \texttt{Convert (Item }\ : \ \texttt{UTF\_8\_String;}
\begin{itemize}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False})
\end{itemize}
\textbf{return} \texttt{UTF\_16\_Wide\_String;}

Returns the value of \texttt{Item} (originally encoded in UTF-8) encoded in UTF-16.

{{AI05-0137-2}} \textbf{function} \texttt{Convert (Item }\ : \ \texttt{UTF\_16\_Wide\_String;}
\begin{itemize}
  \item \texttt{Output\_Scheme} : \texttt{Encoding\_Scheme;}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False}) \textbf{return} \texttt{UTF\_String;}
\end{itemize}

Returns the value of \texttt{Item} (originally encoded in UTF-16) encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by \texttt{Output\_Scheme}.

{{AI05-0137-2}} \textbf{function} \texttt{Convert (Item }\ : \ \texttt{UTF\_16\_Wide\_String;}
\begin{itemize}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False}) \textbf{return} \texttt{UTF\_8\_String;}
\end{itemize}

Returns the value of \texttt{Item} (originally encoded in UTF-16) encoded in UTF-8.

{{AI05-0137-2}} \textbf{function} \texttt{Encode (Item }\ : \ \texttt{String;}
\begin{itemize}
  \item \texttt{Output\_Scheme} : \texttt{Encoding\_Scheme;}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False}) \textbf{return} \texttt{UTF\_String;}
\end{itemize}

\{\texttt{AI05-0262}\texttt{-1}\} Returns the value of \texttt{Item} encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by \texttt{Output\_Scheme}.

{{AI05-0137-2}} \textbf{function} \texttt{Encode (Item }\ : \ \texttt{String;}
\begin{itemize}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False}) \textbf{return} \texttt{UTF\_8\_String;}
\end{itemize}

Returns the value of \texttt{Item} encoded in UTF-8.

{{AI05-0137-2}} \textbf{function} \texttt{Encode (Item }\ : \ \texttt{String;}
\begin{itemize}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False}) \textbf{return} \texttt{UTF\_16\_Wide\_String;}
\end{itemize}

Returns the value of \texttt{Item} encoded in UTF-16.

{{AI05-0137-2}} \textbf{function} \texttt{Decode (Item }\ : \ \texttt{UTF\_String;}
\begin{itemize}
  \item \texttt{Input\_Scheme} : \texttt{Encoding\_Scheme}) \textbf{return} \texttt{String;}
\end{itemize}

Returns the result of decoding \texttt{Item}, which is encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by \texttt{Input\_Scheme}.

{{AI05-0137-2}} \textbf{function} \texttt{Decode (Item} : \texttt{UTF\_8\_String}) \textbf{return} \texttt{String;}

Returns the result of decoding \texttt{Item}, which is encoded in UTF-8.

{{AI05-0137-2}} \textbf{function} \texttt{Decode (Item} : \texttt{UTF\_16\_Wide\_String}) \textbf{return} \texttt{String;}

Returns the result of decoding \texttt{Item}, which is encoded in UTF-16.

{{AI05-0137-2}} \textbf{function} \texttt{Encode (Item} : \texttt{Wide\_String;}
\begin{itemize}
  \item \texttt{Output\_Scheme} : \texttt{Encoding\_Scheme;}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False}) \textbf{return} \texttt{UTF\_String;}
\end{itemize}

\{\texttt{AI05-0262}\texttt{-1}\} Returns the value of \texttt{Item} encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by \texttt{Output\_Scheme}.

{{AI05-0137-2}} \textbf{function} \texttt{Encode (Item} : \texttt{Wide\_String;}
\begin{itemize}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False}) \textbf{return} \texttt{UTF\_8\_String;}
\end{itemize}

Returns the value of \texttt{Item} encoded in UTF-8.

{{AI05-0137-2}} \textbf{function} \texttt{Encode (Item} : \texttt{Wide\_String;}
\begin{itemize}
  \item \texttt{Output\_BOM} : \texttt{Boolean} := \texttt{False}) \textbf{return} \texttt{UTF\_16\_Wide\_String;}
\end{itemize}

Returns the value of \texttt{Item} encoded in UTF-16.
function Decode (Item : UTF_String; Input_Scheme : Encoding_Scheme) return Wide_String;
   Returns the result of decoding Item, which is encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by Input_Scheme.

function Decode (Item : UTF_8_String) return Wide_String;
   Returns the result of decoding Item, which is encoded in UTF-8.

function Decode (Item : UTF_16_Wide_String) return Wide_String;
   Returns the result of decoding Item, which is encoded in UTF-16.

function Encode (Item : Wide_Wide_String; Output_Scheme : Encoding_Scheme; Output_BOM : Boolean := False) return UTF_String;
   Returns the value of Item encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by Output_Scheme.

function Encode (Item : Wide_Wide_String; Output_BOM : Boolean := False) return UTF_8_String;
   Returns the value of Item encoded in UTF-8.

function Encode (Item : Wide_Wide_String; Output_BOM : Boolean := False) return UTF_16_Wide_String;
   Returns the value of Item encoded in UTF-16.

function Decode (Item : UTF_String; Input_Scheme : Encoding_Scheme) return Wide_Wide_String;
   Returns the result of decoding Item, which is encoded in UTF-8, UTF-16LE, or UTF-16BE as specified by Input_Scheme.

function Decode (Item : UTF_8_String) return Wide_Wide_String;
   Returns the result of decoding Item, which is encoded in UTF-8.

function Decode (Item : UTF_16_Wide_String) return Wide_Wide_String;
   Returns the result of decoding Item, which is encoded in UTF-16.

Implementation Advice

If an implementation supports other encoding schemes, another similar child of Ada.Strings should be defined.

Implementation Advice: If an implementation supports other string encoding schemes, a child of Ada.Strings similar to UTF_Encoding should be defined.

NOTE

A BOM (Byte-Order Mark, code position 16#FEFF#) can be included in a file or other entity to indicate the encoding; it is skipped when decoding. Typically, only the first line of a file or other entity contains a BOM. When decoding, the Encoding function can be called on the first line to determine the encoding; this encoding will then be used in subsequent calls to Decode to convert all of the lines to an internal format.

Extensions to Ada 2005

The packages Strings.UTF_Encoding, Strings.UTF_Encoding.Conversions, Strings.UTF_Encoding.Strings, Strings.UTF_Encoding.Wide_Strings, and Strings.UTF_Encoding.Wide_Wide_Strings are new.

Wording Changes from Ada 2012

Corrigendum: Fixed the omission that Convert routines make the same checks on input as Decode routines.
A.4.12 Universal Text Buffers

A universal text buffer can be used to save and retrieve text of any language-defined string type. The types used to save and retrieve the text can be different.

Static Semantics

The text buffer library packages have the following declarations:

```ada
package Ada.Strings.Text_Buffers with Pure is
    type Text_Buffer_Count is range 0 .. implementation-defined;
    New_Line_Count : constant Text_Buffer_Count := implementation-defined;

    type Root_Buffer_Type is abstract tagged private
       with Default_Initial_Condition =>
           Current_Indent (Root_Buffer_Type) = 0;
    procedure Put (Buffer : in out Root_Buffer_Type;
                    Item   : in String) is abstract;
    procedure Wide_Put (Buffer : in out Root_Buffer_Type;
                        Item   : in Wide_String) is abstract;
    procedure Wide_Wide_Put (Buffer : in out Root_Buffer_Type;
                             Item   : in Wide_Wide_String) is abstract;
    procedure Put_UTF_8 (Buffer : in out Root_Buffer_Type;
                         Item   : in UTF_Encoding.UTF_8_String) is abstract;
    procedure Wide_Put_UTF_16 (Buffer : in out Root_Buffer_Type;
                              Item   : in UTF_Encoding.UTF_16_Wide_String) is abstract;
    procedure New_Line (Buffer : in out Root_Buffer_Type) is abstract;
    Standard_Indent : constant Text_Buffer_Count := 3;
    function Current_Indent (Buffer : Root_Buffer_Type) return Text_Buffer_Count;
    procedure Increase_Indent (Buffer : in out Root_Buffer_Type;
                                Amount : in Text_Buffer_Count := Standard_Indent)
       with Post'Class =>
           Current_Indent (Buffer) = Current_Indent (Buffer)'Old + Amount;

    procedure Decrease_Indent (Buffer : in out Root_Buffer_Type;
                               Amount : in Text_Buffer_Count := Standard_Indent)
       with Pre'Class =>
           Current_Indent (Buffer) >= Amount
           or else raise Constraint_Error,
           Post'Class =>
           Current_Indent (Buffer) =
           Current_Indent (Buffer)'Old - Amount;

private
    ... -- not specified by the language
end Ada.Strings.Text_Buffers;
```

package Ada.Strings.Text_Buffers.Unbounded

```ada
with Preelaborate, Nonblocking, Global => null is
    type Buffer_Type is new Root_Buffer_Type with private;
```
function Get (
    Buffer : in out Buffer_Type)
return String
with Post'Class =>
    Get'Result'First = 1 and then Current_Indent (Buffer) = 0;

function Wide_Get (
    Buffer : in out Buffer_Type)
return Wide_String
with Post'Class =>
    Wide_Get'Result'First = 1 and then Current_Indent (Buffer) = 0;

function Wide_Wide_Get (
    Buffer : in out Buffer_Type)
return Wide_Wide_String
with Post'Class =>
    Wide_Wide_Get'Result'First = 1 and then Current_Indent (Buffer) = 0;

function Get_UTF_8 (
    Buffer : in out Buffer_Type)
return UTF_Encoding.UTF_8_String
with Post'Class =>
    Get_UTF_8'Result'First = 1 and then Current_Indent (Buffer) = 0;

function Wide_Get_UTF_16 (
    Buffer : in out Buffer_Type)
return UTF_Encoding.UTF_16_Wide_String
with Post'Class =>
    Wide_Get_UTF_16'Result'First = 1 and then Current_Indent (Buffer) = 0;

private
    ... -- not specified by the language, but will include nonabstract
    -- overridings of all inherited subprograms that require overriding.
end Ada.Strings.Text_Buffers.Unbounded;

with Pure, Nonblocking, Global => null is

    type Buffer_Type (Max_Characters : Text_Buffer_Count)
    is new Root_Buffer_Type with private
        with Default_Initial_Condition => not Text_Truncated (Buffer_Type);

    function Text_Truncated (Buffer : in Buffer_Type)
return Boolean;

private
    ... -- not specified by the language, but will include nonabstract
    -- overridings of all inherited subprograms that require overriding.
end Ada.Strings.Text_Buffers.Bounded;

Character_Count returns the number of characters currently stored in a text buffer.

Ramification: This is lower-case "characters". The representation isn't considered, so it is irrelevant
what type of character (Character, Wide_Character, or Wide_Wide_Character) was stored.

New_Line stores New_Line_Count characters that represent a new line into a text buffer. Current_Indent returns the current indentation associated with the buffer, with zero
meaning there is no indentation in effect; Increase_Indent and Decrease_Indent increase or decrease the
indentation associated with the buffer.

A call to Put, Wide_Put, Wide_Wide_Put, Put_UTF_8, or
Wide_Put_UTF_16 stores a sequence of characters into the text buffer, preceded by
Current_Indent(Buffer) spaces (Wide_Wide_Characters with position 32) if there is at least one character
in Item and it would have been the first character on the current line.
A call to function Get, Wide_Get, Wide_Wide_Get, Get_UTF_8, or Wide_Get_UTF_16 returns the same sequence of characters as was present in the calls that stored the characters into the buffer, if representable. For a call to Get, if any character in the sequence is not defined in Character, the result is implementation defined. Similarly, for a call to Wide_Get, if any character in the sequence is not defined in Wide_Character, the result is implementation defined. As part of a call on any of the Get functions, the buffer is reset to an empty state, with no stored characters.

Implementation defined: The value returned by a call to a Text_Buffer Get procedure if any character in the returned sequence is not defined in Character.

Implementation defined: The value returned by a call to a Text_Buffer Wide_Get procedure if any character in the returned sequence is not defined in Wide_Character.

In the case of a Buf of type Text_Buffers.Bounded.Buffer_Type, Text_Truncated (Buf) returns True if the various Put procedures together have attempted to store more than Buf.Max_Characters into Buf. If this function returns True, then the various Get functions return a representation of only the first Buf.Max_Characters characters that were stored in Buf.

Implementation Advice

Bounded buffer objects should be implemented without dynamic allocation.

Implementation Advice: Bounded buffer objects should be implemented without dynamic allocation.

Extensions to Ada 2012


A.5 The Numerics Packages

The library package Numerics is the parent of several child units that provide facilities for mathematical computation. One child, the generic package Generic_Elementary_Functions, is defined in A.5.1, together with nongeneric equivalents; two others, the package Float_Random and the generic package Discrete_Random, are defined in A.5.2. Additional (optional) children are defined in Annex G, “Numerics”.

Static Semantics

This paragraph was deleted.

The Argument_Error exception is raised by a subprogram in a child unit of Numerics to signal that one or more of the actual subprogram parameters are outside the domain of the corresponding mathematical function.

Implementation Permissions

The implementation may specify the values of Pi and e to a larger number of significant digits.

Reason: 51 digits seem more than adequate for all present computers; converted to binary, the values given above are accurate to more than 160 bits. Nevertheless, the permission allows implementations to accommodate unforeseen hardware advances.
Numerics and its children were not predefined in Ada 83.

Extensions to Ada 95

{AI95-00388-01} The alternative declaration of \( \pi \) is new.

A.5.1 Elementary Functions

Implementation-defined approximations to the mathematical functions known as the “elementary functions” are provided by the subprograms in Numerics.Generic_Elementary_Functions. Nongeneric equivalents of this generic package for each of the predefined floating point types are also provided as children of Numerics.

Implementation defined: The accuracy actually achieved by the elementary functions.

Static Semantics

The generic library package Numerics.Generic_Elementary_Functions has the following declaration:

```ada
{AI12-0241-1} generic
  type Float_Type is digits <>;

package Ada.Numerics.Generic_Elementary_Functions is
  with pragma Pure, Nonblocking is [Generic_Elementary_Functions];

function Sqrt (X : Float_Type'Base) return Float_Type'Base;
function Log (X : Float_Type'Base) return Float_Type'Base;
function Log (X, Base : Float_Type'Base) return Float_Type'Base;
function Exp (X : Float_Type'Base) return Float_Type'Base;
function "**" (Left, Right : Float_Type'Base) return Float_Type'Base;
function Sin (X : Float_Type'Base) return Float_Type'Base;
function Sin (X, Cycle : Float_Type'Base) return Float_Type'Base;
function Cos (X : Float_Type'Base) return Float_Type'Base;
function Cos (X, Cycle : Float_Type'Base) return Float_Type'Base;
function Tan (X : Float_Type'Base) return Float_Type'Base;
function Tan (X, Cycle : Float_Type'Base) return Float_Type'Base;
function Cot (X : Float_Type'Base) return Float_Type'Base;
function Cot (X, Cycle : Float_Type'Base) return Float_Type'Base;
function Arcsin (X : Float_Type'Base) return Float_Type'Base;
function Arcsin (X, Cycle : Float_Type'Base) return Float_Type'Base;
function Arccos (X : Float_Type'Base) return Float_Type'Base;
function Arccos (X, Cycle : Float_Type'Base) return Float_Type'Base;
function Arctan (Y, X : Float_Type'Base := 1.0) return Float_Type'Base;
function Arctan (Y, X : Float_Type'Base := 1.0; Cycle : Float_Type'Base) return Float_Type'Base;
function Arccot (X, Y : Float_Type'Base := 1.0) return Float_Type'Base;
function Arccot (X, Y : Float_Type'Base := 1.0; Cycle : Float_Type'Base) return Float_Type'Base;
function Sinh (X : Float_Type'Base) return Float_Type'Base;
function Cosh (X : Float_Type'Base) return Float_Type'Base;
function Tanh (X : Float_Type'Base) return Float_Type'Base;
function Coth (X : Float_Type'Base) return Float_Type'Base;
function Arccosh (X : Float_Type'Base) return Float_Type'Base;
function Arctanh (X : Float_Type'Base) return Float_Type'Base;
function Arccoth (X : Float_Type'Base) return Float_Type'Base;
end Ada.Numerics.Generic_Elementary_Functions;
```
The library package Numerics.Elementary_Functions is declared pure and defines the same subprograms as Numerics.Generic_Elementary_Functions, except that the predefined type Float is systematically substituted for Float_Type'Base throughout. Nongeneric equivalents of Numerics.Generic_Elementary_Functions for each of the other predefined floating point types are defined similarly, with the names Numerics.Short_Elementary_Functions, Numerics.Long_Elementary_Functions, etc.

Reason: The nongeneric equivalents are provided to allow the programmer to construct simple mathematical applications without being required to understand and use generics.

The functions have their usual mathematical meanings. When the Base parameter is specified, the Log function computes the logarithm to the given base; otherwise, it computes the natural logarithm. When the Cycle parameter is specified, the parameter X of the forward trigonometric functions (Sin, Cos, Tan, and Cot) and the results of the inverse trigonometric functions (Arcsin, Arccos, Arctan, and Arccot) are measured in units such that a full cycle of revolution has the given value; otherwise, they are measured in radians.

The computed results of the mathematically multivalued functions are rendered single-valued by the following conventions, which are meant to imply the principal branch:

- The results of the Sqrt and Arccosh functions and that of the exponentiation operator are nonnegative.
- The result of the Arcsin function is in the quadrant containing the point (1.0, x), where x is the value of the parameter X. This quadrant is I or IV; thus, the range of the Arcsin function is approximately –π/2.0 to π/2.0 (–Cycle/4.0 to Cycle/4.0, if the parameter Cycle is specified).
- The result of the Arccos function is in the quadrant containing the point (x, 1.0), where x is the value of the parameter X. This quadrant is I or II; thus, the Arccos function ranges from 0.0 to approximately π (Cycle/2.0, if the parameter Cycle is specified).
- The results of the Arctan and Arccot functions are in the quadrant containing the point (x, y), where x and y are the values of the parameters X and Y, respectively. This may be any quadrant (I through IV) when the parameter X (resp., Y) of Arctan (resp., Arccot) is specified, but it is restricted to quadrants I and IV (resp., I and II) when that parameter is omitted. Thus, the range when that parameter is specified is approximately –π to π (–Cycle/2.0 to Cycle/2.0, if the parameter Cycle is specified); when omitted, the range of Arctan (resp., Arccot) is that of Arcsin (resp., Arccos), as given above. When the point (x, y) lies on the negative x-axis, the result approximates
  - π (resp., –π) when the sign of the parameter Y is positive (resp., negative), if Float_Type'Signed_Zeros is True;
  - π, if Float_Type'Signed_Zeros is False.

(In the case of the inverse trigonometric functions, in which a result lying on or near one of the axes may not be exactly representable, the approximation inherent in computing the result may place it in an adjacent quadrant, close to but on the wrong side of the axis.)

Dynamic Semantics

The exception Numerics.Argument_Error is raised, signaling a parameter value outside the domain of the corresponding mathematical function, in the following cases:

- by any forward or inverse trigonometric function with specified cycle, when the value of the parameter Cycle is zero or negative;
- by the Log function with specified base, when the value of the parameter Base is zero, one, or negative;
by the Sqrt and Log functions, when the value of the parameter X is negative;

by the exponentiation operator, when the value of the left operand is negative or when both operands have the value zero;

by the Arcsin, Arccos, and Arctanh functions, when the absolute value of the parameter X exceeds one;

by the Arctan and Arccot functions, when the parameters X and Y both have the value zero;

by the Arccosh function, when the value of the parameter X is less than one; and

by the Arccoth function, when the absolute value of the parameter X is less than one.

The exception Constraint_Error is raised, signaling a pole of the mathematical function (analogous to dividing by zero), in the following cases, provided that Float_Type'Machine_Overflows is True:

by the Log, Cot, and Coth functions, when the value of the parameter X is zero;

by the exponentiation operator, when the value of the left operand is zero and the value of the exponent is negative;

by the Tan function with specified cycle, when the value of the parameter X is an odd multiple of the quarter cycle;

by the Cot function with specified cycle, when the value of the parameter X is zero or a multiple of the half cycle; and

by the Arctanh and Arccoth functions, when the absolute value of the parameter X is one.

[Constraint_Error can also be raised when a finite result overflows (see G.2.4); this may occur for parameter values sufficiently near poles, and, in the case of some of the functions, for parameter values with sufficiently large magnitudes.] When Float_Type'Machine_Overflows is False, the result at poles is unspecified.

Reason: The purpose of raising Constraint_Error (rather than Numerics.Argument_Error) at the poles of a function, when Float_Type'Machine_Overflows is True, is to provide continuous behavior as the actual parameters of the function approach the pole and finally reach it.

Discussion: It is anticipated that an Ada binding to IEC 559:1989 will be developed in the future. As part of such a binding, the Machine_Overflows attribute of a conformant floating point type will be specified to yield False, which will permit both the predefined arithmetic operations and implementations of the elementary functions to deliver signed infinities (and set the overflow flag defined by the binding) instead of raising Constraint_Error in overflow situations, when traps are disabled. Similarly, it is appropriate for the elementary functions to deliver signed infinities (and set the zero-divide flag defined by the binding) instead of raising Constraint_Error at poles, when traps are disabled. Finally, such a binding should also specify the behavior of the elementary functions, when sensible, given parameters with infinite values.

Implementation Requirements

In the implementation of Numerics.Generic_Elementary_Functions, the range of intermediate values allowed during the calculation of a final result shall not be affected by any range constraint of the subtype Float_Type.

Implementation Note: Implementations of Numerics.Generic_Elementary_Functions written in Ada should therefore avoid declaring local variables of subtype Float_Type; the subtype Float_Type'Base should be used instead.

In the following cases, evaluation of an elementary function shall yield the prescribed result, provided that the preceding rules do not call for an exception to be raised:
• When the parameter X has the value zero, the Sqrt, Sin, Arcsin, Tan, Sinh, Arcsinh, Tanh, and
Arctanh functions yield a result of zero, and the Exp, Cos, and Cosh functions yield a result of
one.
• When the parameter X has the value one, the Sqrt function yields a result of one, and the Log,
Arccos, and Arccosh functions yield a result of zero.
• When the parameter Y has the value zero and the parameter X has a positive value, the Arctan
and Arccot functions yield a result of zero.
• The results of the Sin, Cos, Tan, and Cot functions with specified cycle are exact when the
mathematical result is zero; those of the first two are also exact when the mathematical result is ±
1.0.
• Exponentiation by a zero exponent yields the value one. Exponentiation by a unit exponent yields
the value of the left operand. Exponentiation of the value one yields the value one. Exponentiation
of the value zero yields the value zero.

Other accuracy requirements for the elementary functions, which apply only in implementations
conforming to the Numerics Annex, and then only in the “strict” mode defined there (see G.2), are given
in G.2.4.

When Float_Type'Signed_Zeros is True, the sign of a zero result shall be as follows:
• A prescribed zero result delivered at the origin by one of the odd functions (Sin, Arcsin, Sinh,
Arcsinh, Tan, Arctan or Arccot as a function of Y when X is fixed and positive, Tanh, and
Arctanh) has the sign of the parameter X (Y, in the case of Arctan or Arccot).
• A prescribed zero result delivered by one of the odd functions away from the origin, or by some
other elementary function, has an implementation-defined sign.

  Implementation defined: The sign of a zero result from some of the operators or functions in
Numerics.Generic_Elementary_Functions, when Float_Type'Signed_Zeros is True.

• \{AI12-0453-1\} [A zero result that is not a prescribed result (that is, one that results from
rounding or underflow) has the correct mathematical sign.]

  Reason: This is a consequence of the rules specified in IEC 559:1989 as they apply to underflow situations with traps
disabled.

Implementation Permissions

\{AI12-0444-1\} The nongeneric equivalent packages may, but need not, be actual instantiations of the
generic package for the appropriate predefined type, though that is not required.

Wording Changes from Ada 83

The semantics of Numerics.Generic_Elementary_Functions differs from Generic_Elementary_Functions as defined in
ISO/IEC DIS 11430 (for Ada 83) in the following ways:
• The generic package is a child unit of the package defining the Argument_Error exception.
• DIS 11430 specified names for the nongeneric equivalents, if provided. Here, those nongeneric equivalents
are required.
• Implementations are not allowed to impose an optional restriction that the generic actual parameter
associated with Float_Type be unconstrained. (In view of the ability to declare variables of subtype
Float_Type'Base in implementations of Numerics.Generic_Elementary_Functions, this flexibility is no
longer needed.)
• The sign of a prescribed zero result at the origin of the odd functions is specified, when
Float_Type'Signed_Zeros is True. This conforms with recommendations of Kahan and other numerical
analysts.
• The dependence of Arctan and Arccot on the sign of a parameter value of zero is tied to the value of
Float_Type'Signed_Zeros.
A.5.1 Elementary Functions

- Sqrt is prescribed to yield a result of one when its parameter has the value one. This guarantee makes it easier to achieve certain prescribed results of the complex elementary functions (see G.1.2, “Complex Elementary Functions”).
- Conformance to accuracy requirements is conditional.

Wording Changes from Ada 95

Corrigendum: Explicitly stated that the nongeneric equivalents of Generic_Elementary_Functions are pure.

A.5.2 Random Number Generation

[Facilities for the generation of pseudo-random floating point numbers are provided in the package Numerics.Float_Random; the generic package Numerics.Discrete_Random provides similar facilities for the generation of pseudo-random integers and pseudo-random values of enumeration types. For brevity, pseudo-random values of any of these types are called random numbers.

Some of the facilities provided are basic to all applications of random numbers. These include a limited private type each of whose objects serves as the generator of a (possibly distinct) sequence of random numbers; a function to obtain the “next” random number from a given sequence of random numbers (that is, from its generator); and subprograms to initialize or reinitialize a given generator to a time-dependent state or a state denoted by a single integer.

Other facilities are provided specifically for advanced applications. These include subprograms to save and restore the state of a given generator; a private type whose objects can be used to hold the saved state of a generator; and subprograms to obtain a string representation of a given generator state, or, given such a string representation, the corresponding state.]

Discussion: These facilities support a variety of requirements ranging from repeatable sequences (for debugging) to unique sequences in each execution of a program.

Static Semantics

The library package Numerics.Float_Random has the following declaration:

```ada
package Ada.Numerics.Float_Random
    with Global => in out synchronized is
    -- Basic facilities
    type Generator is limited private;
    subtype Uniformly_Distributed is Float range 0.0 .. 1.0;
    function Random (Gen : Generator) return Uniformly_Distributed
        with Global => overriding in out Gen;
    procedure Reset (Gen : in Generator;
        Initiator : in Integer)
        with Global => overriding in out Gen;
    procedure Reset (Gen : in Generator)
        with Global => overriding in out Gen;
    Max_Image_Width : constant := implementation-defined integer value;
    function Image (Of_State : State) return String;
    function Value (Coded_State : String) return State;
```

A.5.2 Random Number Generation
private
... -- not specified by the language
end Ada.Numerics.Float_Random;

{AI95-00360-01} The type Generator needs finalization (see 7.6).

The generic library package Numerics.Discrete_Random has the following declaration:

generic
package Ada.Numerics.Discrete_Random with Global => in out synchronized is

-- Basic facilities
type Generator is limited private;

{AI12-0302-1} generic function Random (Gen : Generator) return Result_Subtype
with Global => overriding in out Gen;

{AI12-0144-1} {AI12-0302-1} function Random (Gen : Generator; First : Result_Subtype; Last : Result_Subtype) return Result_Subtype
with Post => Random'Result in First .. Last,
Global => overriding in out Gen;

{AI12-0302-1} procedure Reset (Gen : in Generator; Initiator : in Integer)
with Global => overriding in out Gen;
procedure Reset (Gen : in Generator)
with Global => overriding in out Gen;

-- Advanced facilities
type State is private;

{AI12-0302-1} procedure Save (Gen : in Generator;
To_State : out State);
procedure Reset (Gen : in Generator;
From_State : in State)
with Global => overriding in out Gen;

Max_Image_Width : constant := implementation-defined integer value;

{AI12-0302-1} function Image (Of_State : State) return String;
function Value (Coded_State : String) return State;

private
... -- not specified by the language
end Ada.Numerics.Discrete_Random;


Implementation Note: {8652/0097} {AI95-00115-01} The following is a possible implementation of the private part
of Numerics.Float_Random.each package (assuming the presence of "with Ada.Finalization;" as a context clause):

type State is ...;
type Access_State is access State;
type Generator is new Finalization.Limited_Controlled with
record
S : Access_State := new State'(...);
end record;

procedure Finalize (G : in out Generator);

{8652/0097} {AI95-00115-01} {AI95-00344-01} Unfortunately, Numerics.Discrete_Random.Generator also
cannot be implemented this way, as Numerics.Discrete_Random can be instantiated at any nesting depth. However,
Generator could have a component of a controlled type, as long as that type is declared in some other (nongeneric)
package. One possible solution would be to implement Numerics.Discrete_Random in terms of Numerics.Float_Random

Clearly some level of indirection is required in the implementation of a Generator, since the parameter mode is in
for all operations on a Generator. For this reason, Numerics.Float_Random and Numerics.Discrete_Random cannot be
declared pure.
The type Generator needs finalization (see 7.6) in every instantiation of Numerics.Discrete_Random.

An object of the limited private type Generator is associated with a sequence of random numbers. Each generator has a hidden (internal) state, which the operations on generators use to determine the position in the associated sequence. All generators are implicitly initialized to an unspecified state that does not vary from one program execution to another; they may also be explicitly initialized, or reinitialized, to a time-dependent state, to a previously saved state, or to a state uniquely denoted by an integer value.

Discussion: The repeatability provided by the implicit initialization may be exploited for testing or debugging purposes.

An object of the private type State can be used to hold the internal state of a generator. Such objects are only necessary if the application is designed to save and restore generator states or to examine or manufacture them. The implicit initial value of type State corresponds to the implicit initial value of all generators.

Discussion: All generators are implicitly initialized to the same unchanging value, and using Reset on a default initialized object of type State will produce a generator with that same value.

The operations on generators affect the state and therefore the future values of the associated sequence. The semantics of the operations on generators and states are defined below.

function Random (Gen : Generator) return Uniformly_Distributed;
function Random (Gen : Generator) return Result_Subtype;

Obtains the “next” random number from the given generator, relative to its current state, according to an implementation-defined algorithm. The result of the function in Numerics.Float_Random is delivered as a value of the subtype Uniformly_Distributed, which is a subtype of the predefined type Float having a range of 0.0 .. 1.0. The result of the function in an instantiation of Numerics.Discrete_Random is delivered as a value of the generic formal subtype Result_Subtype.

This paragraph was deleted. Implementation defined: The algorithms for random number generation.

Discussion: The algorithm is the subject of a Documentation Requirement, so we don't separately summarize this implementation-defined item.

Reason: The requirement for a level of indirection in accessing the internal state of a generator arises from the desire to make Random a function, rather than a procedure.

function Random (Gen : Generator; First : Result_Subtype; Last : Result_Subtype) return Result_Subtype
with Post => Random'Result in First .. Last;

Obtains the “next” random number from the given generator, relative to its current state, according to an implementation-defined algorithm. If the range First .. Last is a null range, Constraint_Error is raised.

procedure Reset (Gen : in Generator; Initiator : in Integer);
procedure Reset (Gen : in Generator);

Sets the state of the specified generator to one that is an unspecified function of the value of the parameter Initiator (or to a time-dependent state, if only a generator parameter is specified). The latter form of the procedure is known as the time-dependent Reset procedure.

Implementation Note: The time-dependent Reset procedure can be implemented by mapping the current time and date as determined by the system clock into a state, but other implementations are possible. For example, a white-noise generator or a radioactive source can be used to generate time-dependent states.
procedure Save (Gen : in Generator; To_State : out State);
procedure Reset (Gen : in Generator; From_State : in State);

Save obtains the current state of a generator. Reset gives a generator the specified state. A generator that is reset to a state previously obtained by invoking Save is restored to the state it had when Save was invoked.

function Image (Of_State : State) return String;
function Value (Coded_State : String) return State;

Image provides a representation of a state coded (in an implementation-defined way) as a string whose length is bounded by the value of Max_Image_Width. Value is the inverse of Image: Value(Image(S)) = S for each state S that can be obtained from a generator by invoking Save.

Implementation defined: The string representation of a random number generator's state.

Dynamic Semantics

Instantiation of Numerics.Discrete_Random with a subtype having a null range raises Constraint_Error.

This paragraph was deleted. Invoking Value with a string that is not the image of any generator state raises Constraint_Error.

Bounded (Run-Time) Errors

It is a bounded error to invoke Value with a string that is not the image of any generator state. If the error is detected, Constraint Error or Program Error is raised. Otherwise, a call to Reset with the resulting state will produce a generator such that calls to Random with this generator will produce a sequence of values of the appropriate subtype, but which might not necessarily be random in character. That is, the sequence of values might not necessarily fulfill the implementation requirements of this subclause.

Implementation Requirements

Each call of a Random function has a result range; this is the range First .. Last for the version of Random with First and Last parameters and the range of the result subtype of the function otherwise.

A sufficiently long sequence of random numbers obtained by consecutive calls to Random that have the same generator and result range is approximately uniformly distributed over the result range of the result subtype.

Discussion: In this rule, “consecutive” means at least that there are no intervening explicit calls involving the same generator. This restricts the rule to only applying to cases where just the Random function changes the generator. We don't mean to impose a requirement if there are intervening calls to Reset, to Random with the same generator but a different result range, or any other case that would affect the sequence of values returned. Operations that use the resulting random values (for instance, to store them somewhere) are not considered in determining if calls are consecutive.

The Random function in an instantiation of Numerics.Discrete_Random is guaranteed to yield each value in its result subtype in a finite number of calls, provided that the number of such values does not exceed $2^a$.

Other performance requirements for the random number generator, which apply only in implementations conforming to the Numerics Annex, and then only in the “strict” mode defined there (see G.2), are given in G.2.5.
No one algorithm for random number generation is best for all applications. To enable the user to
determine the suitability of the random number generators for the intended application, the
implementation shall describe the algorithm used and shall give its period, if known exactly, or a lower
bound on the period, if the exact period is unknown. Periods that are so long that the periodicity is
unobservable in practice can be described in such terms, without giving a numerical bound.

**Documentation Requirement:** The algorithm used for random number generation, including a description of its
period.

The implementation also shall document the minimum time interval between calls to the time-dependent
Reset procedure that are guaranteed to initiate different sequences, and it shall document the nature of the
strings that Value will accept without raising Constraint_Error.

**Implementation Advice:**

Any storage associated with an object of type Generator should be reclaimed on exit from the scope of the
object.

**Implementation Advice:** Any storage associated with an object of type Generator of the random number packages
should be reclaimed on exit from the scope of the object.

**Ramification:** A level of indirection is implicit in the semantics of the operations, given that they all take parameters
of mode **in**. This implies that the full type of Generator probably should be a controlled type, with appropriate
finalization to reclaim any heap-allocated storage.

If the generator period is sufficiently long in relation to the number of distinct initiator values, then each
possible value of Initiator passed to Reset should initiate a sequence of random numbers that does not, in
a practical sense, overlap the sequence initiated by any other value. If this is not possible, then the
mapping between initiator values and generator states should be a rapidly varying function of the initiator
value.

**Implementation Advice:** Each value of Initiator passed to Reset for the random number packages should initiate a
distinct sequence of random numbers, or, if that is not possible, be at least a rapidly varying function of the initiator
value.

NOTE 1 If two or more tasks are to share the same generator, then the tasks have to synchronize their access to the
generator as for any shared variable (see 9.10).

NOTE 2 Within a given implementation, a repeatable random number sequence can be obtained by relying on the implicit
initialization of generators or by explicitly initializing a generator with a repeatable initiator value. Different sequences of
random numbers can be obtained from a given generator in different program executions by explicitly initializing the
generator to a time-dependent state.

**Ramification:**

A given implementation of the Random function in Numerics.Float_Random is
not guaranteed to **always** or may **not** be capable of delivering the values 0.0 or 1.0. Applications will be more portable if
theyPortable applications should assume that these values, or values sufficiently close to them to behave indistinguishably
from them, can occur. If a sequence of random integers from some fixed range is necessary, the application should use one of the Random
functions in an appropriate instantiation of Numerics.Discrete_Random, rather than transforming the result of the Random function in Numerics.Float_Random. However, some applications with unusual
requirements, such as for a sequence of random integers each drawn from a different range, will find it more convenient to
transform the result of the floating point Random function. For **M** \( \geq 1 \), the expression

\[
\text{Integer}(\text{Float}(M) \times \text{Random}(G)) \mod M
\]

is not always uniformly distributed. (This usually requires that **M** be a power of two.) In other cases, the \( \mod \) operation maps slightly more random values to some result values than others. It is easy to see
this: consider a 4-bit random integer (with a range of 0 \( \ldots 15 \)). If one \( \text{mod} \) this by 6 to get a value in 0 \( \ldots 5 \) (to which
one would add 1 to get the value of a die roll), 3 values would be mapped to each value 0 .. 3, but only 2 values would be mapped to 4 and 5. Even when the input is uniformly distributed, the output clearly is not. A similar effect occurs regardless of the number of bits in the random integer. Since it takes care to get this right, users should use the provided functions (which presumably do this correctly – AI12-0144-1 contains a correct algorithm) and resist the urge to “roll-their-own”.

{AI12-0442-1} transforms the result of Random(G) to an integer uniformly distributed over the range 0 .. M – 1; it is valid even if Random delivers 0.0 or 1.0. Each value of the result range is possible, provided that M is not too large. Exponentially distributed (floating point) random numbers with mean and standard deviation 1.0 can be obtained by the transformation

\[
\text{-Log(Random(G) + Float'Model_Small)}
\]

where Log comes from Numerics.Elementary_Functions (see A.5.1); in this expression, the addition of Float'Model_Small avoids the exception that would be raised were Log to be given the value zero, without affecting the result (in most implementations) when Random returns a nonzero value.

Examples

Example of a program that plays a simulated dice game:

```ada
with Ada.Numerics.Discrete_Random;
procedure Dice_Game is
    subtype Die is Integer range 1 .. 6;
    subtype Dice is Integer range 2*Die'First .. 2*Die'Last;
    package Random_Die is new Ada.Numerics.Discrete_Random (Die);
    use Random_Die;
    G : Generator;
    D : Dice;
begin
    Reset (G);  -- Start the generator in a unique state in each run
    loop
        -- Roll a pair of dice; sum and process the results
        D := Random(G) + Random(G);
        ...
    end loop;
end Dice_Game;
```

Example of a program that simulates coin tosses:

```ada
with Ada.Numerics.Discrete_Random;
procedure Flip_A_Coin is
    type Coin is (Heads, Tails);
    package Random_Coin is new Ada.Numerics.Discrete_Random (Coin);
    use Random_Coin;
    G : Generator;
begin
    Reset (G);  -- Start the generator in a unique state in each run
    loop
        -- Toss a coin and process the result
        case Random(G) is
            when Heads =>$
                ...
            when Tails =>$
                ...
        end case;
    end loop;
end Flip_A_Coin;
```
Example of a parallel simulation of a physical system, with a separate generator of event probabilities in each task:

```ada
with Ada.Numerics.Float_Random;
procedure Parallel_Simulation is
  use Ada.Numerics.Float_Random;
  task type Worker is
    entry Initialize_Generator (Initiator : in Integer);
    ...
  end Worker;
  W : array (1 .. 10) of Worker;
  task body Worker is
    G : Generator;
    Probability_Of_Event : Uniformly_Distributed;
  begin
    accept Initialize_Generator (Initiator : in Integer) do
      Reset (G, Initiator);
      end Initialize_Generator;
    loop
      Probability_Of_Event := Random(G);
      ...
    end loop;
  end Worker;
begin
  -- Initialize the generators in the Worker tasks to different states
  for I in W'Range loop
    W(I).Initialize_Generator (I);
  end loop;
  ...  -- Wait for the Worker tasks to terminate
end Parallel_Simulation;
```

Although each Worker task initializes its generator to a different state, those states will be the same in every execution of the program. The generator states can be initialized uniquely in each program execution by instantiating Ada.Numerics.Discrete_Random for the type Integer in the main procedure, resetting the generator obtained from that instance to a time-dependent state, and then using random integers obtained from that generator to initialize the generators in each Worker task.

**NOTE 4** Although each Worker task initializes its generator to a different state, those states will be the same in every execution of the program. The generator states can be initialized uniquely in each program execution by instantiating Ada.Numerics.Discrete_Random for the type Integer in the main procedure, resetting the generator obtained from that instance to a time-dependent state, and then using random integers obtained from that generator to initialize the generators in each Worker task.

**Incompatibilities With Ada 95**

- **Amendment Correction:** Type Generator in Numerics.Float_Random and in an instance of Numerics.Discrete_Random is defined to need finalization. If the restriction No_Nested_Finalization (see D.7) applies to the partition, and Generator does not have a controlled part, it will not be allowed in local objects in Ada 2005 whereas it would be allowed in original Ada 95. Such code is not portable, as another Ada compiler may have a controlled part in Generator, and thus would be illegal.

- **Wording Changes from Ada 95**
  - **Corrigendum:** Made the passing of an incorrect Image of a generator a bounded error, as it might not be practical to check for problems (if a generator consists of several related values).

- **Extensions to Ada 2012**
  - The function Random with First and Last parameters is new.
A.5.3 Attributes of Floating Point Types

Static Semantics

The following representation-oriented attributes are defined for every subtype S of a floating point type T.

S'Machine_Radix
Yields the radix of the hardware representation of the type T. The value of this attribute is of the type universal_integer.

The values of other representation-oriented attributes of a floating point subtype, and of the “primitive function” attributes of a floating point subtype described later, are defined in terms of a particular representation of nonzero values called the canonical form. The canonical form (for the type T) is the form

\[ \pm \text{mantissa} \cdot \text{T'Machine_Radix}^{\text{exponent}} \]

where

• mantissa is a fraction in the number base T'Machine_Radix, the first digit of which is nonzero, and

• exponent is an integer.

S'Machine_Mantissa
Yields the largest value of p such that every value expressible in the canonical form (for the type T), having a p-digit mantissa and an exponent between T'Machine_Emin and T'Machine_Emax, is a machine number (see 3.5.7) of the type T. This attribute yields a value of the type universal_integer.

Ramification: Values of a type held in an extended register are, in general, not machine numbers of the type, since they cannot be expressed in the canonical form with a sufficiently short mantissa.

S'Machine_Emin
Yields the smallest (most negative) value of exponent such that every value expressible in the canonical form (for the type T), having a mantissa of T'Machine_Mantissa digits, is a machine number (see 3.5.7) of the type T. This attribute yields a value of the type universal_integer.

S'Machine_Emax
Yields the largest (most positive) value of exponent such that every value expressible in the canonical form (for the type T), having a mantissa of T'Machine_Mantissa digits, is a machine number (see 3.5.7) of the type T. This attribute yields a value of the type universal_integer.

Ramification: Note that the above definitions do not determine unique values for the representation-oriented attributes of floating point types. The implementation may choose any set of values that collectively satisfies the definitions.

S'Denorm
Yields the value True if every value expressible in the form

\[ \pm \text{mantissa} \cdot \text{T'Machine_Radix}^{\text{T'Machine_Emin}} \]

where mantissa is a nonzero T'Machine_Mantissa-digit fraction in the number base T'Machine_Radix, the first digit of which is zero, is a machine number (see 3.5.7) of the type T; yields the value False otherwise. The value of this attribute is of the predefined type Boolean.

The values described by the formula in the definition of S'Denorm are called denormalized numbers. A nonzero machine number that is not a denormalized number is a normalized number. A normalized number x of a given type T is said to be represented in canonical form when it is expressed in the canonical form (for the type T) with a mantissa having T'Machine_Mantissa digits; the resulting form is the canonical-form representation of x.
Discussion: The intent is that S'Denorm be True when such denormalized numbers exist and are generated in the circumstances defined by IEC 559:1989, though the latter requirement is not formalized here.

S'Machine_Rounds
Yields the value True if rounding is performed on inexact results of every predefined operation that yields a result of the type \( T \); yields the value False otherwise. The value of this attribute is of the predefined type Boolean.

Discussion: It is difficult to be more precise about what it means to round the result of a predefined operation. If the implementation does not use extended registers, so that every arithmetic result is necessarily a machine number, then rounding seems to imply two things:

- S'Model_Mantissa = S'Machine_Mantissa, so that operand preperturbation never occurs;
- when the exact mathematical result is not a machine number, the result of a predefined operation must be the nearer of the two adjacent machine numbers.

Technically, this attribute should yield False when extended registers are used, since a few computed results will cross over the half-way point as a result of double rounding, if and when a value held in an extended register has to be reduced in precision to that of the machine numbers. It does not seem desirable to preclude the use of extended registers when S'Machine_Rounds could otherwise be True.

S'Machine_Overflows
Yields the value True if overflow and divide-by-zero are detected and reported by raising Constraint_Error for every predefined operation that yields a result of the type \( T \); yields the value False otherwise. The value of this attribute is of the predefined type Boolean.

S'Signed_Zeros
Yields the value True if the hardware representation for the type \( T \) has the capability of representing both positively and negatively signed zeros, these being generated and used by the predefined operations of the type \( T \) as specified in IEC 559:1989; yields the value False otherwise. The value of this attribute is of the predefined type Boolean.

For every value \( x \) of a floating point type \( T \), the normalized exponent of \( x \) is defined as follows:

- the normalized exponent of zero is (by convention) zero;
- for nonzero \( x \), the normalized exponent of \( x \) is the unique integer \( k \) such that \( T'Machine_Radix^{k-1} \leq |x| < T'Machine_Radix^k \).

Ramification: The normalized exponent of a normalized number \( x \) is the value of exponent in the canonical-form representation of \( x \).

The normalized exponent of a denormalized number is less than the value of \( T'Machine_Emin \).

The following primitive function attributes are defined for any subtype \( S \) of a floating point type \( T \).

S'Exponent
S'Exponent denotes a function with the following specification:

```ada
function S'Exponent (X : T) return universal_integer
```

The function yields the normalized exponent of \( X \).

S'Fraction
S'Fraction denotes a function with the following specification:

```ada
function S'Fraction (X : T) return T
```

The function yields the value \( X \cdot T'Machine_Radix^k \), where \( k \) is the normalized exponent of \( X \). A zero result[, which can only occur when \( X \) is zero,] has the sign of \( X \).

Discussion: Informally, when \( X \) is a normalized number, the result is the value obtained by replacing the exponent by zero in the canonical-form representation of \( X \).

Ramification: Except when \( X \) is zero, the magnitude of the result is greater than or equal to the reciprocal of \( T'Machine_Radix \) and less than one; consequently, the result is always a normalized number, even when \( X \) is a denormalized number.

Implementation Note: When \( X \) is a denormalized number, the result is the value obtained by replacing the exponent by zero in the canonical-form representation of the result of scaling \( X \) up sufficiently to normalize it.
S'Compose S'Compose denotes a function with the following specification:

```ada
function S'Compose (Fraction : T;
    Exponent : universal_integer)
    return T
```

Let v be the value Fraction \(\times T'\text{Machine_Radix}^{\text{Exponent}-k}\), where k is the normalized exponent of Fraction. If v is a machine number of the type T, or if |v| \(\geq T'\text{Model_Small}\), the function yields v; otherwise, it yields either one of the machine numbers of the type T adjacent to v. Constraint_Error is optionally raised if v is outside the base range of S. A zero result has the sign of Fraction when S’Signed_Zeros is True.

**Discussion:** Informally, when Fraction and v are both normalized numbers, the result is the value obtained by replacing the exponent by Exponent in the canonical-form representation of Fraction.

**Ramification:** If Exponent is less than T’Machine_Emin and Fraction is nonzero, the result is either zero, T’Model_Small, or (if T’Denorm is True) a denormalized number.

S'Scaling S'Scaling denotes a function with the following specification:

```ada
function S'Scaling (X : T;
    Adjustment : universal_integer)
    return T
```

Let v be the value X \(\times T'\text{Machine_Radix}^{\text{Adjustment}}\). If v is a machine number of the type T, or if |v| \(\geq T'\text{Model_Small}\), the function yields v; otherwise, it yields either one of the machine numbers of the type T adjacent to v. Constraint_Error is optionally raised if v is outside the base range of S. A zero result has the sign of X when S’Signed_Zeros is True.

**Discussion:** Informally, when X and v are both normalized numbers, the result is the value obtained by increasing the exponent by Adjustment in the canonical-form representation of X.

**Ramification:** \{AI12-0453-1\} If Adjustment is sufficiently small (that is, sufficiently negative), the result is either zero, T’Model_Small, or (if T’Denorm is True) a denormalized number.

S'Floor S'Floor denotes a function with the following specification:

```ada
function S'Floor (X : T)
    return T
```

\{AI12-0453-1\} The function yields the value \(\lfloor X\rfloor\), that is, the largest (most positive) integral value less than or equal to X. When X is zero, the result has the sign of X; a zero result otherwise has a positive sign.

S'Ceiling S'Ceiling denotes a function with the following specification:

```ada
function S'Ceiling (X : T)
    return T
```

\{AI12-0453-1\} The function yields the value \(\lceil X\rceil\), that is, the smallest (most negative) integral value greater than or equal to X. When X is zero, the result has the sign of X; a zero result otherwise has a negative sign when S’Signed_Zeros is True.

S'Rounding S'Rounding denotes a function with the following specification:

```ada
function S'Rounding (X : T)
    return T
```

The function yields the integral value nearest to X, rounding away from zero if X lies exactly halfway between two integers. A zero result has the sign of X when S’Signed_Zeros is True.

S'Unbiased_Rounding S'Unbiased_Rounding denotes a function with the following specification:

```ada
function S'Unbiased_Rounding (X : T)
    return T
```

The function yields the integral value nearest to X, rounding toward the even integer if X lies exactly halfway between two integers. A zero result has the sign of X when S’Signed_Zeros is True.
S'Machine_Rounding

{AI95-00267-01} S'Machine_Rounding denotes a function with the following specification:

```ada
function S'Machine_Rounding (X : T) return T
```

The function yields the integral value nearest to X. If X lies exactly halfway between two integers, one of those integers is returned, but which of them is returned is unspecified. A zero result has the sign of X when S'Signed_Zeros is True. This function provides access to the rounding behavior which is most efficient on the target processor.

**Discussion:** We leave the rounding unspecified, so that users cannot depend on a particular rounding. This attribute is intended for use in cases where the particular rounding chosen is irrelevant. If there is a need to know which way values halfway between two integers are rounded, one of the other rounding attributes should be used.

S'Truncation

S'Truncation denotes a function with the following specification:

```ada
function S'Truncation (X : T) return T
```

The function yields the value \(\lfloor X \rfloor\) when X is negative, and \(\lceil X \rceil\) otherwise. A zero result has the sign of X when S'Signed_Zeros is True.

S'Remainder

S'Remainder denotes a function with the following specification:

```ada
function S'Remainder (X, Y : T) return T
```

For nonzero Y, let v be the value X – n · Y, where n is the integer nearest to the exact value of X/Y; if \(|n - X/Y| = 1/2\), then n is chosen to be even. If v is a machine number of the type T, the function yields v; otherwise, it yields zero. Constraint_Error is raised if Y is zero. A zero result has the sign of X when S'Signed_Zeros is True.

**Ramification:** The magnitude of the result is less than or equal to one-half the magnitude of Y.

**Discussion:** Given machine numbers X and Y of the type T, v is necessarily a machine number of the type T, except when Y is in the neighborhood of zero, X is sufficiently close to a multiple of Y, and T'Denorm is False.

S'Adjacent

S'Adjacent denotes a function with the following specification:

```ada
function S'Adjacent (X, Towards : T) return T
```

If Towards = X, the function yields X; otherwise, it yields the machine number of the type T adjacent to X in the direction of Towards, if that machine number exists. If the result would be outside the base range of S, Constraint_Error is raised. When T'Signed_Zeros is True, a zero result has the sign of X. When Towards is zero, its sign has no bearing on the result.

**Ramification:** The value of S'Adjacent(0.0, 1.0) is the smallest normalized positive number of the type T when T'Denorm is False and the smallest denormalized positive number of the type T when T'Denorm is True.

S'Copy_Sign

S'Copy_Sign denotes a function with the following specification:

```ada
function S'Copy_Sign (Value, Sign : T) return T
```

If the value of Value is nonzero, the function yields a result whose magnitude is that of Value and whose sign is that of Sign; otherwise, it yields the value zero. Constraint_Error is optionally raised if the result is outside the base range of S. A zero result has the sign of Sign when S'Signed_Zeros is True.

**Discussion:** S'Copy_Sign is provided for convenience in restoring the sign to a quantity from which it has been temporarily removed, or to a related quantity. When S'Signed_Zeros is True, it is also instrumental in determining the sign of a zero quantity, when required. (Because negative and positive zeros compare equal in systems conforming to IEC 559:1989, a negative zero does not appear to be negative when compared to zero.) The sign determination is accomplished by transferring the sign of the zero quantity to a nonzero quantity and then testing for a negative result.
S'Leading_Part

S'Leading_Part denotes a function with the following specification:

```ada
function S'Leading_Part (X : T;
    Radix_Digits : universal_integer)
return T
```

Let \( v \) be the value \( T'Machine_Radix^{k-Radix_Digits} \), where \( k \) is the normalized exponent of \( X \). The function yields the value

- \( \lfloor X/v \rfloor \cdot v \), when \( X \) is nonnegative and \( Radix_Digits \) is positive;
- \( \lceil X/v \rceil \cdot v \), when \( X \) is negative and \( Radix_Digits \) is positive.

Constraint_Error is raised when \( Radix_Digits \) is zero or negative. A zero result, which can only occur when \( X \) is zero, has the sign of \( X \).

Discussion: Informally, if \( X \) is nonzero, the result is the value obtained by retaining only the specified number of (leading) significant digits of \( X \) (in the machine radix), setting all other digits to zero.

Implementation Note: The result can be obtained by first scaling \( X \) up, if necessary to normalize it, then masking the mantissa so as to retain only the specified number of leading digits, then scaling the result back down if \( X \) was scaled up.

S'Machine

S'Machine denotes a function with the following specification:

```ada
function S'Machine (X : T)
return T
```

If \( X \) is a machine number of the type \( T \), the function yields \( X \); otherwise, it yields the value obtained by rounding or truncating \( X \) to either one of the adjacent machine numbers of the type \( T \). Constraint_Error is raised if rounding or truncating \( X \) to the precision of the machine numbers results in a value outside the base range of \( S \). A zero result has the sign of \( X \) when \( S'Signed_Zeros \) is True.

Discussion: \{AI05-0005-1\} All of the primitive function attributes except Rounding and Machine correspond to subprograms in the Generic_Primitive_Functions generic package that was proposed as a separate ISO standard (ISO/IEC DIS 11729) for Ada 83. The Scaling, Unbiased_Rounding, and Truncate attributes correspond to the Scale, Round, and Truncate functions, respectively, in Generic_Primitive_Functions. The Rounding attribute rounds away from zero; this functionality was not provided in Generic_Primitive_Functions. The name Round was not available for either of the primitive function attributes that perform rounding, since an attribute of that name is used for a different purpose for decimal fixed point types. Likewise, the name Scale was not available, since an attribute of that name is also used for a different purpose for decimal fixed point types. The functionality of the Machine attribute was also not provided in Generic_Primitive_Functions. The functionality of the Decompose procedure of Generic_Primitive_Functions is only provided in the form of the separate attributes Exponent and Fraction. The functionality of the Successor and Predecessor functions of Generic_Primitive_Functions is provided by the extension of the existing Succ and Pred attributes.

Implementation Note: The primitive function attributes may be implemented either with appropriate floating point arithmetic operations or with integer and logical operations that act on parts of the representation directly. The latter is strongly encouraged when it is more efficient than the former; it is mandatory when the former cannot deliver the required accuracy due to limitations of the implementation's arithmetic operations.

The following model-oriented attributes are defined for any subtype \( S \) of a floating point type \( T \).

S'Model_Mantissa

If the Numerics Annex is not supported, this attribute yields an implementation defined value that is greater than or equal to \( \lceil d \cdot \log(10) / \log(T'Machine_Radix) \rceil + 1 \), where \( d \) is the requested decimal precision of \( T \), and less than or equal to the value of \( T'Machine_Mantissa \). See G.2.2 for further requirements that apply to implementations supporting the Numerics Annex. The value of this attribute is of the type universal_integer.

S'Model_Emin

If the Numerics Annex is not supported, this attribute yields an implementation defined value that is greater than or equal to the value of \( T'Machine_Emin \). See G.2.2 for further
requirements that apply to implementations supporting the Numerics Annex. The value of
this attribute is of the type \textit{universal\_integer}.

\paragraph{S'\texttt{Model\_Epsilon}}

Yields the value \(T\text{\textquoteleft\text{Machine\_Radix}}^{-1} - T\text{\textquoteleft\text{Model\_Mantissa}}\). The value of this attribute is of the type \textit{universal\_real}.

\textbf{Discussion:} In most implementations, this attribute yields the absolute value of the difference between one and the smallest machine number of the type \(T\) above one which, when added to one, yields a machine number different from one. Further discussion can be found in G.2.2.

\paragraph{S'\texttt{Model\_Small}}

Yields the value \(T\text{\textquoteleft\text{Machine\_Radix}}^{T\text{\textquoteleft\text{Model\_Emin}} - 1}\). The value of this attribute is of the type \textit{universal\_real}.

\textbf{Discussion:} [AI12-0453-1] In most implementations, this attribute yields the smallest positive normalized number of the type \(T\), that is, the number corresponding to the positive underflow threshold. In some implementations employing a radix-complement representation for the type \(T\), the positive underflow threshold is closer to zero than is the negative underflow threshold, with the consequence that the smallest positive normalized number does not coincide with the positive underflow threshold (that is, it exceeds the latter). Further discussion can be found in G.2.2.

\paragraph{S'\texttt{Model\_denotes a function with the following specification:}}

\begin{verbatim}
  function S'Model (X : T) return T
end
\end{verbatim}

If the Numerics Annex is not supported, the meaning of this attribute is implementation defined; see G.2.2 for the definition that applies to implementations supporting the Numerics Annex.

\paragraph{S'\texttt{Safe\_First}}

Yields the lower bound of the safe range (see 3.5.7) of the type \(T\). If the Numerics Annex is not supported, the value of this attribute is implementation defined; see G.2.2 for the definition that applies to implementations supporting the Numerics Annex. The value of this attribute is of the type \textit{universal\_real}.

\paragraph{S'\texttt{Safe\_Last}}

Yields the upper bound of the safe range (see 3.5.7) of the type \(T\). If the Numerics Annex is not supported, the value of this attribute is implementation defined; see G.2.2 for the definition that applies to implementations supporting the Numerics Annex. The value of this attribute is of the type \textit{universal\_real}.

\textbf{Discussion:} A predefined floating point arithmetic operation that yields a value in the safe range of its result type is guaranteed not to overflow.

\textbf{To be honest:} An exception is made for exponentiation by a negative exponent in 4.5.6.

\textbf{Implementation defined:} The values of the Model\_Mantissa, Model\_Emin, Model\_Epsilon, Model, Safe\_First, and Safe\_Last attributes, if the Numerics Annex is not supported.

\textit{Incompatibilities With Ada 83}

The Epsilon and Mantissa attributes of floating point types are removed from the language and replaced by Model\_Epsilon and Model\_Mantissa, which may have different values (as a result of changes in the definition of model numbers); the replacement of one set of attributes by another is intended to convert what would be an inconsistent change into an incompatible change.

The Emax, Small, Large, Safe\_Emax, Safe\_Small, and Safe\_Large attributes of floating point types are removed from the language. Small and Safe\_Small are collectively replaced by Model\_Small, which is functionally equivalent to Safe\_Small, though it may have a slightly different value. The others are collectively replaced by Safe\_First and Safe\_Last. Safe\_Last is functionally equivalent to Safe\_Large, though it may have a different value; Safe\_First is comparable to the negation of Safe\_Large but may differ slightly from it as well as from the negation of Safe\_Last. Emax and Safe\_Emax had relatively few uses in Ada 83; T\text{\textquoteleft\text{Safe\_Emax}} can be computed in the revised language as Integer\text{\textquoteleft\text{Min}}(T\text{\textquoteleft\text{Exponent}}(T\text{\textquoteleft\text{Safe\_First}}), T\text{\textquoteleft\text{Exponent}}(T\text{\textquoteleft\text{Safe\_Last})).}

Implementations are encouraged to eliminate the incompatibilities discussed here by retaining the old attributes, during a transition period, in the form of implementation-defined attributes with their former values.
A.5.3 Extensions to Ada 83

The Model_Emin attribute is new. It is conceptually similar to the negation of Safe_Emax attribute of Ada 83, adjusted for the fact that the model numbers now have the hardware radix. It is a fundamental determinant, along with Model_Mantissa, of the set of model numbers of a type (see G.2.1).

The Denorm and Signed_Zeros attributes are new, as are all of the primitive function attributes.

A.5.4 Attributes of Fixed Point Types

Static Semantics

The following representation-oriented attributes are defined for every subtype S of a fixed point type T.

S'Machine_Radix
Yields the radix of the hardware representation of the type T. The value of this attribute is of the type universal_integer.

S'Machine_Rounds
Yields the value True if rounding is performed on inexact results of every predefined operation that yields a result of the type T; yields the value False otherwise. The value of this attribute is of the predefined type Boolean.

S'Machine_Overflows
Yields the value True if overflow and divide-by-zero are detected and reported by raising Constraint_Error for every predefined operation that yields a result of the type T; yields the value False otherwise. The value of this attribute is of the predefined type Boolean.

Incompatibilities With Ada 83

The Mantissa, Large, Safe_Small, and Safe_Large attributes of fixed point types are removed from the language. Implementations are encouraged to eliminate the resulting incompatibility by retaining these attributes, during a transition period, in the form of implementation-defined attributes with their former values.

A.5.5 Big Numbers

Support is provided for integer arithmetic involving values larger than those supported by the target machine, and for arbitrary-precision real numbers.

Static Semantics

The library package Numerics.Big_Numbers has the following declaration:

package Ada.Numerics.Big_Numbers
  with Pure, Nonblocking, Global => null is
  subtype Field is Integer range 0 .. implementation_defined;
  subtype Number_Base is Integer range 2 .. 16;
end Ada.Numerics.Big_Numbers;

Extensions to Ada 2012

The package Numerics.Big_Numbers is new.
A.5.6 **Big Integers**

**Static Semantics**

The library package `Numerics.Big_Numbers.Big_Integers` has the following declaration:

```ada
with Ada.Strings.Text_Buffers;
package Ada.Numerics.Big_Numbers.Big_Integers
with Preelaborate, Nonblocking, Global => in out synchronized is

{AI12-0208-1} {AI12-0366-1} type Big_Integer is private
with Integer_Literal => From_Universal_Image,
    Put_Image => Put_Image;

function Is_Valid (Arg : Big_Integer) return Boolean
with Convention => Intrinsic;

Discussion: {AI12-0005-1} The result of Is_Valid on a default-initialized object of type Big_Integer is unspecified, analogous to the value of a Valid attribute reference applied to a default-initialized object of an integer type (see 13.9.2). The language-provided functions in the Big_Integers package only return values for which Is_Valid is certain to be True.

subtype Valid_Big_Integer is Big_Integer
    with Dynamic_Predicate => Is_Valid (Valid_Big_Integer),
        Predicate_Failure => (raise Program_Error);

function "=" (L, R : Valid_Big_Integer) return Boolean;
function "<" (L, R : Valid_Big_Integer) return Boolean;
function "<=" (L, R : Valid_Big_Integer) return Boolean;
function ">" (L, R : Valid_Big_Integer) return Boolean;
function ">=" (L, R : Valid_Big_Integer) return Boolean;

function To_Big_Integer (Arg : Integer) return Valid_Big_Integer;

subtype Big_Positive is Big_Integer
    with Dynamic_Predicate => (if Is_Valid (Big_Positive)
            then Big_Positive > 0),
        Predicate_Failure => (raise Constraint_Error);

subtype Big_Natural is Big_Integer
    with Dynamic_Predicate => (if Is_Valid (Big_Natural)
            then Big_Natural >= 0),
        Predicate_Failure => (raise Constraint_Error);

function In_Range (Arg, Low, High : Valid_Big_Integer) return Boolean is
    (Low <= Arg and Arg <= High);

function To_Integer (Arg : Valid_Big_Integer) return Integer
    with Pre => In_Range (Arg,
            Low => To_Big_Integer (Integer'First),
            High => To_Big_Integer (Integer'Last))
        or else raise Constraint_Error;

generic type Int is range <>
package Signed_Conversions is
    function To_Big_Integer (Arg : Int) return Valid_Big_Integer;
    function From_Big_Integer (Arg : Valid_Big_Integer) return Int
        with Pre => In_Range (Arg,
            Low => To_Big_Integer (Int'First),
            High => To_Big_Integer (Int'Last))
        or else raise Constraint_Error;
end Signed_Conversions;
```
generic
  type Int is mod <>;
package Unsigned_Conversions is
  function To_Big_Integer (Arg : Int) return Valid_Big_Integer;
  function From_Big_Integer (Arg : Valid_Big_Integer) return Int
    with Pre => In_Range (Arg,
      Low => To_Big_Integer (Int'First),
      High => To_Big_Integer (Int'Last))
    or else raise Constraint_Error;
end Unsigned_Conversions;

function To_String (Arg : Valid_Big_Integer;
  Width : Field := 0;
  Base  : Number_Base := 10) return String
  with Post => To_String'Result'First = 1;
function From_String (Arg : String) return Valid_Big_Integer;

private
  ... -- not specified by the language
end Ada.Numerics.Big_Numbers.Big_Integers;

{AI12-0208-1} {AI12-0366-1} To String and From String behave analogously to the Put and Get
procedures defined in Text_IO.Integer_IO (in particular, with respect to the interpretation of the Width
and Base parameters) except that Constraint_Error, not Data_Error, is propagated in error cases and the
result of a call to To_String with a Width parameter of 0 and a nonnegative Arg parameter does not
include a leading blank. Put_Image calls To_String (passing in the default values for the Width and Base
parameters), prepends a leading blank if the argument is nonnegative, and writes the resulting value to the
buffer using Text_Buffers.Put.

{AI12-0208-1} The other functions have their usual mathematical meanings.

{AI12-0208-1} {AI12-0366-1} The type Big_Integer needs finalization (see 7.6).

Dynamic Semantics

{AI12-0208-1} {AI12-0366-1} For purposes of determining whether predicate checks are performed as
part of default initialization, the type Big_Integer is considered to have a subcomponent that has a
default expression.

Ramification: {AI12-0005-1} {AI12-0208-1} This means that the elaboration of
  Default_INITIALIZED_OBJECT : Valid_Big_Integer;

879 16 October 2023
either produces a value for which \texttt{Is\_Valid} is True, or it propagates \texttt{Program\_Error}.

\textbf{Implementation Requirements}

\begin{itemize}
\item \{\texttt{AI12-0208-1} \} \{\texttt{AI12-0366-1}\} No storage associated with a Big Integer object shall be lost upon assignment or scope exit.
\item \{\texttt{AI12-0208-1}\} \{\texttt{AI12-0366-1}\} The “No storage ... shall be lost” requirement does not preclude implementation techniques such as caching or unique number tables.
\end{itemize}

\textbf{Extensions to Ada 2012}

\begin{itemize}
\item \{\texttt{AI12-0208-1} \} \{\texttt{AI12-0366-1}\} The package \texttt{Numerics.Big\_Numbers.Big\_Integers} is new.
\end{itemize}

\section*{A.5.7 Big Reals}

\textbf{Static Semantics}

\begin{itemize}
\item \{\texttt{AI12-0208-1} \} \{\texttt{AI12-0366-1}\} The library package \texttt{Numerics.Big\_Numbers.Big\_Reals} has the following declaration:
\item \begin{verbatim}
with Ada.Numerics.Big_Numbers.Big_Integers;
use all type Big_Integers.Big_Integer;
with Ada.Strings.Text_Buffers;
package Ada.Numerics.Big_Numbers.Big_Reals
with Prelaborate, Nonblocking, Global => in out synchronized is
\end{verbatim}
\item \begin{verbatim}
type Big_Real is private
with Real_Literal => From_Universal_Image,
Put_Image => Put_Image;
\end{verbatim}
\item \begin{verbatim}
function Is_Valid (Arg : Big_Real) return Boolean
with Convention => intrinsic;
\end{verbatim}
\item \begin{verbatim}
subtype Valid_Big_Real is Big_Real
with Dynamic_Predicate => Is_Valid (Valid_Big_Real),
Predicate_Failure => raise Program_Error;
\end{verbatim}
\item \begin{verbatim}
function "/" (Num, Den : Big_Integers.Valid_Big_Integer)
return Valid_Big_Real
with Pre => Den /= 0
or else raise Constraint_Error;
\end{verbatim}
\item \begin{verbatim}
function Numerator (Arg : Valid_Big_Real) return Big_Integers.Valid_Big_Integer
with Post => (if Arg = 0.0 then Numerator'Result = 0);
\end{verbatim}
\item \begin{verbatim}
function Denominator (Arg : Valid_Big_Real)
return Big_Integers.Big_Positive
with Post =>
(if Arg = 0.0 then Denominator'Result = 1
else Big_Integers.Greatest_Common_Divisor
(Numerator (Arg), Denominator'Result) = 1);
\end{verbatim}
\item \begin{verbatim}
function To_Big_Real (Arg : Big_Integers.Valid_Big_Integer)
return Valid_Big_Real is (Arg / 1);
\end{verbatim}
\item \begin{verbatim}
function To_Real (Arg : Integer) return Valid_Big_Real is
(Big_Integers.To_Big_Integer (Arg) / 1);
\end{verbatim}
\end{itemize}
function "=" (L, R : Valid_Big_Real) return Boolean;
function "<" (L, R : Valid_Big_Real) return Boolean;
function "<=" (L, R : Valid_Big_Real) return Boolean;
function "+" (L, R : Valid_Big_Real) return Valid_Big_Real;
function "+" (L : Valid_Big_Real) return Valid_Big_Real;
function "-" (L, R : Valid_Big_Real) return Valid_Big_Real;
function "+" (L, R : Valid_Big_Real) return Valid_Big_Real;
function "**" (L : Valid_Big_Real; R : Integer) return Valid_Big_Real;
function Min (L, R : Valid_Big_Real) return Valid_Big_Real;
function Max (L, R : Valid_Big_Real) return Valid_Big_Real;

private
... -- not specified by the language
end Ada.Numerics.Big_Numbers.Big_Reals;

{AI12-0208-1} {AI12-0366-1} To String and From String behave analogously to the Put and Get procedures defined in Text_IO.Float_IO (in particular, with respect to the interpretation of the Fore, Aft,
and _Exp parameters), except that Constraint Error (not Data Error) is propagated in error cases. From Quotient String implements the inverse function of To Quotient String; Constraint Error is propagated in error cases. Put Image calls To String, and writes the resulting value to the buffer using Text_Buffers.Put.

24/5 \{AI12-0208-1\} For an instance of Float_Conversions or Fixed_Conversions, To_Big_Real is exact (that is, the result represents exactly the same mathematical value as the argument) and From_Big_Real is subject to the same precision rules as a type conversion of a value of type T to the target type Num, where T is a hypothetical floating point type whose model numbers include all of the model numbers of Num as well as the exact mathematical value of the argument.

25/5 \{AI12-0208-1\} The other functions have their usual mathematical meanings.

26/5 \{AI12-0208-1\} \{AI12-0366-1\} The type Big_Real needs finalization (see 7.6).

Dynamic Semantics

27/5 \{AI12-0208-1\} \{AI12-0366-1\} For purposes of determining whether predicate checks are performed as part of default initialization, the type Big_Real is considered to have a subcomponent that has a default_expression.

27.a/5 \{AI12-0005-1\} \{AI12-0208-1\} This means that the elaboration of Default_Initialized_Object : Valid_Big_Real;

27.b/5 either produces a value for which Is_Valid is True, or it propagates Program_Error.

Implementation Requirements

28/5 \{AI12-0208-1\} \{AI12-0366-1\} No storage associated with a Big_Real object shall be lost upon assignment or scope exit.

28.a/5 \{AI12-0208-1\} The “No storage ... shall be lost” requirement does not preclude implementation techniques such as caching or unique number tables.

28.b/5 \{AI12-0208-1\} \{AI12-0366-1\} The package Numerics.Big_Numbers.Big_Reals is new.

A.6 Input-Output

1/5 \{AI95-00285-01\} \{AI12-0445-1\} [ Input-output is provided through language-defined packages, each of which is a child of the root package Ada. The generic packages Sequential_IO and Direct_IO define input-output operations applicable to files containing elements of a given type. The generic package Storage_IO supports reading from and writing to an in-memory buffer. Additional operations for text input-output are supplied in the packages Text_IO, and Wide_Text_IO, and Wide_Wide_Text_IO. Heterogeneous input-output is provided through the child packages Streams.Stream_IO and Text_IO., and Text_Streams (see also 13.13). The package IO_Exceptions defines the exceptions used needed by the predefined input-output packages.]

Inconsistencies With Ada 83

1.a The introduction of Append_File as a new element of the enumeration type File_Mode in Sequential_IO and Text_IO, and the introduction of several new declarations in Text_IO, may result in name clashes in the presence of use clauses.

1.b Text_IO enhancements (Get_Immediate, Look_Ahead, Standard_Error, Modular_IO, Decimal_IO), Wide_Text_IO, and the stream input-output facilities are new in Ada 95.
Wording Changes from Ada 83

RM83-14.6, “Low Level Input-Output”, is removed. This has no semantic effect, since the package was entirely implementation defined, nobody actually implemented it, and if they did, they can always provide it as a vendor-supplied package.

Wording Changes from Ada 95

\{AI95-00285-01\} Included package Wide_Wide_Text_IO in this description.

A.7 External Files and File Objects

Static Semantics

Values input from the external environment of the program, or output to the external environment, are considered to occupy external files. An external file can be anything external to the program that can produce a value to be read or receive a value to be written. An external file is identified by a string (the name). A second string (the form) gives further system-dependent characteristics that may be associated with the file, such as the physical organization or access rights. The conventions governing the interpretation of such strings shall be documented.

\{AI05-0299-1\} Input and output operations are expressed as operations on objects of some file type, rather than directly in terms of the external files. In the remainder of this clause section, the term file is always used to refer to a file object; the term external file is used otherwise.

Input-output for sequential files of values of a single element type is defined by means of the generic package Sequential_IO. In order to define sequential input-output for a given element type, an instantiation of this generic unit, with the given type as actual parameter, has to be declared. The resulting package contains the declaration of a file type (called File_Type) for files of such elements, as well as the operations applicable to these files, such as the Open, Read, and Write procedures.

\{AI95-00285-01\} Input-output for direct access files is likewise defined by a generic package called Direct_IO. Input-output in human-readable form is defined by the (nongeneric) packages Text_IO for Character and String data, and Wide_Text_IO for Wide_Character and Wide_String data, and Wide_Wide_Text_IO for Wide_Wide_Character and Wide_Wide_String data. Input-output for files containing streams of elements representing values of possibly different types is defined by means of the (nongeneric) package Streams.Stream_IO.

Before input or output operations can be performed on a file, the file first has to be associated with an external file. While such an association is in effect, the file is said to be open, and otherwise the file is said to be closed.

The language does not define what happens to external files after the completion of the main program and all the library tasks (in particular, if corresponding files have not been closed). The effect of input-output for access types is unspecified.

An open file has a current mode, which is a value of one of the following enumeration types:

\[
\text{type File_Mode is (In_File, Inout_File, Out_File); -- for Direct_IO}
\]

These values correspond respectively to the cases where only reading, both reading and writing, or only writing are to be performed.

\{AI95-00285-01\} \text{type File_Mode is (In_File, Out_File, Append_File);}  
\text{-- for Sequential_IO, Text_IO, Wide_Text_IO, Wide_Wide_Text_IO and Stream_IO}

These values correspond respectively to the cases where only reading, only writing, or only appending are to be performed.
The mode of a file can be changed.

Several file management operations are common to Sequential_IO, Direct_IO, Text_IO, and Wide_Text_IO, and Wide_Wide_Text_IO. These operations are described in subclause A.8.2 for sequential and direct files. Any additional effects concerning text input-output are described in subclause A.10.2.

The exceptions that can be propagated by the execution of an input-output subprogram are defined in the package IO_Exceptions; the situations in which they can be propagated are described following the description of the subprogram (and in subclause A.13). The exceptions Storage_Error and Program_Error may be propagated. (Program_Error can only be propagated due to errors made by the caller of the subprogram.) Finally, exceptions can be propagated in certain implementation-defined situations.

This paragraph was deleted.

Implementation_defined: Any implementation-defined characteristics of the input-output packages.

Discussion: The last sentence here is referring to the documentation requirements in A.13, “Exceptions in Input-Output”, and the documentation summary item is provided there.

NOTE 1 Each instantiation of the generic packages Sequential_IO and Direct_IO declares a different type File_Type. In the case of Text_IO, Wide_Text_IO, Wide_Wide_Text_IO, and Streams.Stream_IO, the corresponding type File_Type is unique.

NOTE 2 A bidirectional device can often be modeled as two sequential files associated with the device, one of mode In_File, and one of mode Out_File. An implementation can restrict the number of files that can be associated with a given external file.

Wording Changes from Ada 95

Included package Wide_Wide_Text_IO in this description.

A.8 Sequential and Direct Files

Static Semantics

Two kinds of access to external files are defined in this subclause: sequential access and direct access. The corresponding file types and the associated operations are provided by the generic packages Sequential_IO and Direct_IO. A file object to be used for sequential access is called a sequential file, and one to be used for direct access is called a direct file. Access to stream files is described in A.12.1.

For sequential access, the file is viewed as a sequence of values that are transferred in the order of their appearance (as produced by the program or by the external environment). When the file is opened with mode In_File or Out_File, transfer starts respectively from or to the beginning of the file. When the file is opened with mode Append_File, transfer to the file starts after the last element of the file.

Discussion: Adding stream I/O necessitates a review of the terminology. In Ada 83, 'sequential' implies both the access method (purely sequential — that is, no indexing or positional access) and homogeneity. Direct access includes purely sequential access and indexed access, as well as homogeneity. In Ada 95, streams allow purely sequential access but also positional access to an individual element, and are heterogeneous. We considered generalizing the notion of 'sequential file' to include both Sequential_IO and Stream_IO files, but since streams allow positional access it seems misleading to call them sequential files. Or, looked at differently, if the criterion for calling something a sequential file is whether it permits (versus requires) purely sequential access, then one could just as soon regard a Direct_IO file as a sequential file.

It seems better to regard 'sequential file' as meaning 'only permitting purely sequential access'; hence we have decided to supplement 'sequential access' and 'direct access' with a third category, informally called 'access to streams'. (We decided against the term 'stream access' because of possible confusion with the Stream_Access type declared in one of the stream packages.)
For direct access, the file is viewed as a set of elements occupying consecutive positions in linear order; a value can be transferred to or from an element of the file at any selected position. The position of an element is specified by its index, which is a number, greater than zero, of the implementation-defined integer type Count. The first element, if any, has index one; the index of the last element, if any, is called the current size; the current size is zero if there are no elements. The current size is a property of the external file.

An open direct file has a current index, which is the index that will be used by the next read or write operation. When a direct file is opened, the current index is set to one. The current index of a direct file is a property of a file object, not of an external file.

_Wording Changes from Ada 95_

{AI95-00283-01} Italicized “stream file” to clarify that this is another kind of file.

### A.8.1 The Generic Package Sequential_IO

_Static Semantics_

The generic library package Sequential_IO has the following declaration:

```ada
with Ada.IO_Exceptions;
generic
  type Element_Type(<>) is private;
package Ada.Sequential_IO
  with Global => in out synchronized is
    type File_Type is limited private;
    type File_Mode is (In_File, Out_File, Append_File);
    -- File management
    procedure Create(File : in out File_Type;
                     Mode : in File_Mode := Out_File;
                     Name : in String := "");
    procedure Open  (File : in out File_Type;
                     Mode : in File_Mode;
                     Name : in String;
                     Form : in String := ");
    procedure Close (File : in out File_Type);
    procedure Delete(File : in out File_Type);
    procedure Reset (File : in out File_Type;
                     Mode : in File_Mode);
    function Mode   (File : in File_Type) return File_Mode;
    function Name   (File : in File_Type) return String;
    function Form   (File : in File_Type) return String;
    function Is_Open(File : in File_Type) return Boolean;
  {AI12-0302-1}  {AI12-0302-1}  procedure Flush (File : in File_Type)
                    with Global => overriding in out File;
    -- Input and output operations
  {AI12-0302-1}  procedure Read   (File : in File_Type; Item : out Element_Type)
                    with Global => overriding in out File;
  {AI12-0302-1}  procedure Write  (File : in File_Type; Item : in Element_Type)
                    with Global => overriding in out File;
  function End_Of_File(File : in File_Type) return Boolean;
```


--- Exceptions

Status_Error : exception renames IO_Exceptions.Status_Error;
Mode_Error : exception renames IO_Exceptions.Mode_Error;
Name_Error : exception renames IO_Exceptions.Name_Error;
Use_Error : exception renames IO_Exceptions.Use_Error;
Device_Error : exception renames IO_Exceptions.Device_Error;
End_Error : exception renames IO_Exceptions.End_Error;
Data_Error : exception renames IO_Exceptions.Data_Error;

--- Package Wide_File_Names is

procedure Create(File : in out File_Type;
  Mode : in File_Mode := Out_File;
  Name : in Wide_String := "";
  Form : in Wide_String := "");

procedure Open (File : in out File_Type;
  Mode : in File_Mode;
  Name : in Wide_String;
  Form : in Wide_String := "");

function Name (File : in File_Type) return Wide_String;

function Form (File : in File_Type) return Wide_String;

--- Package Wide_Wide_File_Names is

procedure Create(File : in out File_Type;
  Mode : in File_Mode := Out_File;
  Name : in Wide_Wide_String := "";
  Form : in Wide_Wide_String := "");

procedure Open (File : in out File_Type;
  Mode : in File_Mode;
  Name : in Wide_Wide_String;
  Form : in Wide_Wide_String := "");

function Name (File : in File_Type) return Wide_Wide_String;

function Form (File : in File_Type) return Wide_Wide_String;

--- Private...

end Ada.Sequential_IO;

--- Incompatibilities With Ada 83

The new enumeration element Append_File may introduce upward incompatibilities. It is possible that a
program based on the assumption that File_Mode'Last = Out_File will be illegal (e.g., case statement
choice coverage) or execute with a different effect in Ada 95.

Implementation Note: File_Type cannot be implemented as a (directly) controlled type, as
Ada.Sequential_IO can be instantiated at any nesting depth. File_Type could have a component of a
controlled type, as long as that type is declared in some other (nongeneric)
package.

--- Incompatibilities With Ada 95

Amendment Correction: File_Type in an instance of Sequential_IO is defined to need finalization.
If the restriction No_Nested_Finalization (see D.7) applies to the partition, and File_Type does not
have a controlled part, it will not be allowed in local objects in Ada 2005 whereas it would be allowed in
original Ada 95. Such code is not portable, as another Ada compiler may have a controlled part in File_Type,
and thus would be illegal.
A.8.2 File Management

Static Semantics

{AI12-0449-1} The procedures and functions described in this subclause provide for the control of external files; their declarations are repeated in each of the packages for sequential, direct, text, and stream input-output. For text input-output, the procedures Create, Open, and Reset have additional effects described in subclause A.10.2.

procedure Create(File : in out File_Type;
                  Mode : in File_Mode := default_mode;
                  Name : in String := "";
                  Form : in String := "");

{AI95-00283-01} Establishes a new external file, with the given name and form, and associates this external file with the given file. The given file is left open. The current mode of the given file is set to the given access mode. The default access mode is the mode Out_File for sequential, stream, and text input-output; it is the mode Inout_File for direct input-output. For direct access, the size of the created file is implementation defined.

Ramification: {AI12-0005-1} For a direct file, the initial value of current index is 1 (see A.8).

A null string for Name specifies an external file that is not accessible after the completion of the main program (a temporary file). A null string for Form specifies the use of the default options of the implementation for the external file.

The exception Status_Error is propagated if the given file is already open. The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file. The exception Use_Error is propagated if, for the specified mode, the external environment does not support creation of an external file with the given name (in the absence of Name_Error) and form.

procedure Open(File : in out File_Type;
               Mode : in File_Mode;
               Name : in String;
               Form : in String := "");

Associates the given file with an existing external file having the given name and form, and sets the current mode of the given file to the given mode. The given file is left open.

Ramification: {AI12-0005-1} For a direct file, the initial value of current index is 1 (see A.8).

The exception Status_Error is propagated if the given file is already open. The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file; in particular, this exception is propagated if no external file with the given name exists. The exception Use_Error is propagated if, for the specified mode, the external environment does not support opening for an external file with the given name (in the absence of Name_Error) and form.
procedure Close(File : in out File_Type);

Severs the association between the given file and its associated external file. The given file is left closed. In addition, for sequential files, if the file being closed has mode Out_File or Append_File, then the last element written since the most recent open or reset is the last element that can be read from the file. If no elements have been written and the file mode is Out_File, then the closed file is empty. If no elements have been written and the file mode is Append_File, then the closed file is unchanged.

The exception Status_Error is propagated if the given file is not open.

procedure Delete(File : in out File_Type);

Deletes the external file associated with the given file. The given file is closed, and the external file ceases to exist.

The exception Status_Error is propagated if the given file is not open. The exception Use_Error is propagated if deletion of the external file is not supported by the external environment.

procedure Reset(File : in out File_Type; Mode : in File_Mode);

{AI95-00085-01} Resets the given file so that reading from its elements can be restarted from the beginning of the external file (for modes In_File and Inout_File), and so that writing to its elements can be restarted at the beginning of the external file (for modes Out_File and Inout_File) or after the last element of the external file (for mode Append_File). In particular, for direct access this means that the current index is set to one. If a Mode parameter is supplied, the current mode of the given file is set to the given mode. In addition, for sequential files, if the given file has mode Out_File or Append_File when Reset is called, the last element written since the most recent open or reset is the last element that can be read from the external file. If no elements have been written and the file mode is Out_File, the reset file is empty. If no elements have been written and the file mode is Append_File, then the reset file is unchanged.

The exception Status_Error is propagated if the file is not open. The exception Use_Error is propagated if the external environment does not support resetting for the external file and, also, if the external environment does not support resetting to the specified mode for the external file.

function Mode(File : in File_Type) return File_Mode;

Returns the current mode of the given file.

The exception Status_Error is propagated if the file is not open.

function Name(File : in File_Type) return String;

{AI95-00248-01} Returns a string which uniquely identifies the external file currently associated with the given file (and may thus be used in an Open operation). If an external environment allows alternative specifications of the name (for example, abbreviations), the string returned by the function should correspond to a full specification of the name.

Discussion: {AI95-00248-01} Retrieving the full path can be accomplished by passing the result of Name to Directories.Full_Name (see A.16). It is important to drop the requirement on Name, as the only way to accomplish this requirement given that the current directory can be changed with package Directories is to store the full path when the file is opened. That's expensive, and it's better for users that need the full path to explicitly request it.

The exception Status_Error is propagated if the given file is not open. The exception Use_Error is propagated if the associated external file is a temporary file that cannot be opened by any name.
function Form(File : in File_Type) return String;

Returns the form string for the external file currently associated with the given file. If an external environment allows alternative specifications of the form (for example, abbreviations using default options), the string returned by the function should correspond to a full specification (that is, it should indicate explicitly all options selected, including default options).

The exception Status_Error is propagated if the given file is not open.

function Is_Open(File : in File_Type) return Boolean;

{AI05-0264-1} Returns True if the file is open (that is, if it is associated with an external file); otherwise returns False.

{AI12-0130-1} procedure Flush(File : in File_Type);

The Flush procedure synchronizes the external file with the internal file (by flushing any internal buffers) without closing the file. For a direct file, the current index is unchanged; for a stream file (see A.12.1), the current position is unchanged.

The exception Status_Error is propagated if the file is not open. The exception Mode_Error is propagated if the mode of the file is In_File.

{AI12-0021-1} The nested package Wide_File_Names provides operations equivalent to the operations of the same name of the outer package except that Wide_String is used instead of String for the name and form of the external file.

Implementation Note: {AI12-0021-1} The expectation is that if one opens a file with this subpackage and then requests the name with Name from this subpackage, the result will include the same Wide_Characters that were used to open the file (rather than some encoded form). Since file names are completely implementation-defined, we cannot say this normatively. We have no expectations when retrieving the name of a file opened with this package using the String Name. Similar considerations apply to the nested package Wide_Wide_File_Names (see below).

{AI12-0021-1} The nested package Wide_Wide_File_Names provides operations equivalent to the operations of the same name of the outer package except that Wide_Wide_String is used instead of String for the name and form of the external file.

Implementation Permissions

An implementation may propagate Name_Error or Use_Error if an attempt is made to use an I/O feature that cannot be supported by the implementation due to limitations in the external environment. Any such restriction should be documented.

Wording Changes from Ada 95

{AI95-00085-01} Clarified that Reset affects and depends on the external file.

{AI95-00248-01} Removed the requirement for Name to return a full path; this is now accomplished by Directories.Full_Name(Name(File)) (see A.16). This is not documented as an inconsistency, because there is no requirement for implementations to change — the Ada 95 behavior is still allowed, it just is no longer required.

{AI95-00283-01} Added text to specify the default mode for a stream file.

Wording Changes from Ada 2012

{AI12-0130-1} Procedure Flush is now defined here, so it can be used for all of the I/O packages.

{AI12-0021-1} The nested Wide_File_Names and Wide_Wide_File_Names packages are now described here.
A.8.3 Sequential Input-Output Operations

Static Semantics

The operations available for sequential input and output are described in this subclause. The exception Status_Error is propagated if any of these operations is attempted for a file that is not open.

procedure Read(File : in File_Type; Item : out Element_Type);

Operates on a file of mode In_File. Reads an element from the given file, and returns the value of this element in the Item parameter.

Discussion: We considered basing Sequential_IO.Read on Element_Type'Read from an implicit stream associated with the sequential file. However, Element_Type'Read is a type-related attribute, whereas Sequential_IO should take advantage of the particular constraints of the actual subtype corresponding to Element_Type to minimize the size of the external file. Furthermore, forcing the implementation of Sequential_IO to be based on Element_Type'Read would create an upward incompatibility since existing data files written by an Ada 83 program using Sequential_IO might not be readable by the identical program built with an Ada 95 implementation of Sequential_IO.

An Ada 95 implementation might still use an implementation-defined attribute analogous to 'Read to implement the procedure Read, but that attribute will likely have to be subtype-specific rather than type-related, and it need not be user-specifiable. Such an attribute will presumably be needed to implement the generic package Storage_IO (see A.9).

The exception Mode_Error is propagated if the mode is not In_File. The exception End_Error is propagated if no more elements can be read from the given file. The exception Data_Error can be propagated if the element read cannot be interpreted as a value of the subtype Element_Type (see A.13, “Exceptions in Input-Output”).

Discussion: Data_Error need not be propagated if the check is too complex. See A.13, “Exceptions in Input-Output”.

procedure Write(File : in File_Type; Item : in Element_Type);

Operates on a file of mode Out_File or Append_File. Writes the value of Item to the given file.

The exception Mode_Error is propagated if the mode is not Out_File or Append_File. The exception Use_Error is propagated if the capacity of the external file is exceeded.

function End_Of_File(File : in File_Type) return Boolean;

{AI05-0264-1} Operates on a file of mode In_File. Returns True if no more elements can be read from the given file; otherwise, returns False.

The exception Mode_Error is propagated if the mode is not In_File.

A.8.4 The Generic Package Direct_IO

Static Semantics

The generic library package Direct_IO has the following declaration:

{AI12-0302-1} with Ada.IO_Exceptions;
generic
  type Element_Type is private;
package Ada.Direct_IO
  with Global => in out synchronized is
  type File_Type is limited private;
  type File_Mode is (In_File, Inout_File, Out_File);
  type Count is range 0 .. implementation-defined;
  subtype Positive_Count is Count range 1 .. Count'Last;
  -- File management
procedure Create (File : in out File_Type;
    Mode : in File_Mode := Inout_File;
    Name : in String := "");

procedure Open (File : in out File_Type;
    Mode : in File_Mode;
    Name : in String;
    Form : in String := "");

procedure Close (File : in out File_Type);

procedure Delete (File : in out File_Type);

procedure Reset (File : in out File_Type;
    Mode : in File_Mode);

procedure Reset (File : in out File_Type);

function Mode (File : in File_Type) return File_Mode;

function Name (File : in File_Type) return String;

function Form (File : in File_Type) return String;

function Is_Open (File : in File_Type) return Boolean;

{AI12-0130-1} {AI12-0302-1} procedure Flush (File : in File_Type)
    with Global => overriding in out File;

-- Input and output operations

{AI12-0302-1} procedure Read (File : in File_Type; Item : out Element_Type;
    From : in Positive_Count)
    with Global => overriding in out File;

procedure Read (File : in File_Type; Item : out Element_Type)
    with Global => overriding in out File;

{AI12-0302-1} procedure Write (File : in File_Type; Item : in Element_Type;
    To : in Positive_Count)
    with Global => overriding in out File;

procedure Write (File : in File_Type; Item : in Element_Type)
    with Global => overriding in out File;

{AI12-0302-1} procedure Set_Index (File : in File_Type; To : in Positive_Count)
    with Global => overriding in out File;

function Index (File : in File_Type) return Positive_Count;

function Size (File : in File_Type) return Count;

function End_Of_File (File : in File_Type) return Boolean;

-- Exceptions

Status_Error : exception renames IO_Exceptions.Status_Error;
Mode_Error : exception renames IO_Exceptions.Mode_Error;
Name_Error : exception renames IO_Exceptions.Name_Error;
Use_Error : exception renames IO_Exceptions.Use_Error;
Device_Error : exception renames IO_Exceptions.Device_Error;
End_Error : exception renames IO_Exceptions.End_Error;
Data_Error : exception renames IO_Exceptions.Data_Error;

{AI12-0021-1} package Wide_File_Names is

-- File management

procedure Create (File : in out File_Type;
    Mode : in File_Mode := Inout_File;
    Name : in Wide_String := "");

procedure Open (File : in out File_Type;
    Mode : in File_Mode;
    Name : in Wide_String;
    Form : in Wide_String := "");

function Name (File : in File_Type) return Wide_String;

function Form (File : in File_Type) return Wide_String;

end Wide_File_Names;

{AI12-0021-1} package Wide_Wide_File_Names is
-- File management

procedure Create(File : in out File_Type;
                 Mode : in File_Mode := Inout_File;
                 Name : in Wide_Wide_String := "";
                 Form : in Wide_Wide_String := "");

procedure Open (File : in out File_Type;
                Mode : in File_Mode;
                Name : in Wide_Wide_String;
                Form : in Wide_Wide_String := "");

function Name   (File : in File_Type) return Wide_Wide_String;

function Form   (File : in File_Type) return Wide_Wide_String;

end Wide_Wide_File_Names;

private
...
not specified by the language
end Ada.Direct_IO;

Reason:
The Element_Type formal of Direct_IO does not have an unknown_discriminant_part (unlike Sequential_IO) so that the implementation can make use of the ability to declare uninitialized variables of the type.

---

A.8.5 Direct Input-Output Operations

Static Semantics

The operations available for direct input and output are described in this subclause. The exception
Status_Error is propagated if any of these operations is attempted for a file that is not open.

**procedure Read** (File : in File_Type; Item : out Element_Type;
                   From : in Positive_Count);

**procedure Read** (File : in File_Type; Item : out Element_Type);

Operates on a file of mode In_File or Inout_File. In the case of the first form, sets the current
index of the given file to the index value given by the parameter From. Then (for both forms)
returns, in the parameter Item, the value of the element whose position in the given file is
specified by the current index of the file; finally, increases the current index by one.

The exception Mode_Error is propagated if the mode of the given file is Out_File. The exception
End_Error is propagated if the index to be used exceeds the size of the external file. The
exception Data_Error can be propagated if the element read cannot be interpreted as a value of
the subtype Element_Type (see A.13).

```ada
procedure Write(File : in File_Type; Item : in Element_Type;
                To   : in Positive_Count);
```

Operates on a file of mode Inout_File or Out_File. In the case of the first form, sets the index of
the given file to the index value given by the parameter To. Then (for both forms) gives the value
of the parameter Item to the element whose position in the given file is specified by the current
index of the file; finally, increases the current index by one.

The exception Mode_Error is propagated if the mode of the given file is In_File. The exception
Use_Error is propagated if the capacity of the external file is exceeded.

```ada
procedure Set_Index(File : in File_Type; To : in Positive_Count);
```

Operates on a file of any mode. Sets the current index of the given file to the given index value
(which may exceed the current size of the file).

```ada
function Index(File : in File_Type) return Positive_Count;
```

Operates on a file of any mode. Returns the current index of the given file.

```ada
function Size(File : in File_Type) return Count;
```

Operates on a file of any mode. Returns the current size of the external file that is associated with
the given file.

```ada
function End_Of_File(File : in File_Type) return Boolean;
```

{AI05-0264-1} Operates on a file of mode In_File or Inout_File. Returns True if the current index
exceeds the size of the external file; otherwise, returns False.

The exception Mode_Error is propagated if the mode of the given file is Out_File.

NOTE   Append_File mode is not supported for the generic package Direct_IO.

A.9 The Generic Package Storage_IO

The generic package Storage_IO provides for reading from and writing to an in-memory buffer. This
generic package supports the construction of user-defined input-output packages.

Reason: This package exists to allow the portable construction of user-defined direct-access-oriented input-output
packages. The Write procedure writes a value of type Element_Type into a Storage_Array of size Buffer_Size,
flattening out any implicit levels of indirection used in the representation of the type. The Read procedure reads a value
of type Element_Type from the buffer, reconstructing any implicit levels of indirection used in the representation of
the type. It also properly initializes any type tags that appear within the value, presuming that the buffer was written by
a different program and that tag values for the “same” type might vary from one executable to another.

Static Semantics

The generic library package Storage_IO has the following declaration:

```ada
{AI12-0302-1} with Ada.IO_Exceptions;
with System.Storage_Elements;
generic
  type Element_Type is private;
package Ada.Storage_IO
  with Preelaborate, Global => in out synchronized is
    pragma Preelaborate(Storage_IO);
```
Buffer_Size : constant System.Storage_Elements.Storage_Count :=
  implementation-defined;
subtype Buffer_Type is
  System.Storage_Elements.Storage_Array(1..Buffer_Size);
-- Input and output operations
procedure Read (Buffer : in Buffer_Type; Item : out Element_Type);
procedure Write (Buffer : out Buffer_Type; Item : in Element_Type);
-- Exceptions
Data_Error : exception renames IO_Exceptions.Data_Error;
end Ada.Storage_IO;

In each instance, the constant Buffer_Size has a value that is the size (in storage elements) of the buffer
required to represent the content of an object of subtype Element_Type, including any implicit levels of
indirection used by the implementation. The Read and Write procedures of Storage_IO correspond to the
Read and Write procedures of Direct_IO (see A.8.4), but with the content of the Item parameter being
read from or written into the specified Buffer, rather than an external file.

Reason: As with Direct_IO, the Element_Type formal of Storage_IO does not have an unknown_discriminant_part
so that there is a well-defined upper bound on the size of the buffer needed to hold the content of an object of the formal
subtype (i.e. Buffer_Size). If there are no implicit levels of indirection, Buffer_Size will typically equal:
(Element_Type'Size + System.Storage_Unit - 1) / System.Storage_Unit

Implementation defined: The value of Buffer_Size in Storage_IO.

NOTE A buffer used for Storage_IO holds only one element at a time; an external file used for Direct_IO holds a sequence
of elements.

Extensions to Ada 83

Storage_IO is new in Ada 95.

A.10 Text Input-Output

Static Semantics

This subclause describes the package Text_IO, which provides
facilities for input and output in human-readable form. Each file is read or written sequentially, as a
sequence of characters grouped into lines, and as a sequence of lines grouped into pages. The
specification of the package is given below in subclause A.10.1.

The facilities for file management given above, in subclauses A.8.2 and
A.8.3, are available for text input-output. In place of Read and Write, however, there are procedures Get
and Put that input values of suitable types from text files, and output values to them. These values are
provided to the Put procedures, and returned by the Get procedures, in a parameter Item. Several
overloaded procedures of these names exist, for different types of Item. These Get procedures analyze the
input sequences of characters based on lexical elements (see Clause 2) and return the corresponding
values; the Put procedures output the given values as appropriate lexical elements. Procedures Get and
Put are also available that input and output individual characters treated as character values rather than as
lexical elements. Related to character input are procedures to look ahead at the next character without
reading it, and to read a character “immediately” without waiting for an end-of-line to signal availability.

In addition to the procedures Get and Put for numeric and enumeration types of Item that operate on text
files, analogous procedures are provided that read from and write to a parameter of type String. These
procedures perform the same analysis and composition of character sequences as their counterparts which
have a file parameter.
For all Get and Put procedures that operate on text files, and for many other subprograms, there are forms with and without a file parameter. Each such Get procedure operates on an input file, and each such Put procedure operates on an output file. If no file is specified, a default input file or a default output file is used.

At the beginning of program execution the default input and output files are the so-called standard input file and standard output file. These files are open, have respectively the current modes In_File and Out_File, and are associated with two implementation-defined external files. Procedures are provided to change the current default input file and the current default output file.

**Implementation defined:** The external files associated with the standard input, standard output, and standard error files.

**Implementation Note:** The default input file and default output file are not the names of distinct file objects, but rather the role played by one or more (other) file object(s). Thus, they generally will be implemented as accesses to another file object. An implementation that implements them by copying them is incorrect.

At the beginning of program execution a default file for program-dependent error-related text output is the so-called standard error file. This file is open, has the current mode Out_File, and is associated with an implementation-defined external file. A procedure is provided to change the current default error file.

From a logical point of view, a text file is a sequence of pages, a page is a sequence of lines, and a line is a sequence of characters; the end of a line is marked by a *line terminator*; the end of a page is marked by the combination of a line terminator immediately followed by a *page terminator*; and the end of a file is marked by the combination of a line terminator immediately followed by a page terminator and then a *file terminator*. Terminators are generated during output; either by calls of procedures provided expressly for that purpose; or implicitly as part of other operations, for example, when a bounded line length, a bounded page length, or both, have been specified for a file.

The actual nature of terminators is not defined by the language and hence depends on the implementation. Although terminators are recognized or generated by certain of the procedures that follow, they are not necessarily implemented as characters or as sequences of characters. Whether they are characters (and if so which ones) in any particular implementation is not of concern to a user who neither explicitly outputs nor explicitly inputs control characters. The effect of input (Get) or output (Put) of control characters (other than horizontal tabulation) is not specified by the language.

The characters of a line are numbered, starting from one; the number of a character is called its *column number*. For a line terminator, a column number is also defined: it is one more than the number of characters in the line. The lines of a page, and the pages of a file, are similarly numbered. The current column number is the column number of the next character or line terminator to be transferred. The current line number is the number of the current line. The current page number is the number of the current page. These numbers are values of the subtype Positive_Count of the type Count (by convention, the value zero of the type Count is used to indicate special conditions).

```plaintext
type Count is range 0 .. implementation-defined;
subtype Positive_Count is Count range 1 .. Count'Last;
```

For an output file or an append file, a *maximum line length* can be specified and a *maximum page length* can be specified. If a value to be output cannot fit on the current line, for a specified maximum line length, then a new line is automatically started before the value is output; if, further, this new line cannot fit on the current page, for a specified maximum page length, then a new page is automatically started before the value is output. Functions are provided to determine the maximum line length and the maximum page length. When a file is opened with mode Out_File or Append_File, both values are zero: by convention, this means that the line lengths and page lengths are unbounded. (Consequently, output consists of a single line if the subprograms for explicit control of line and page structure are not used.) The constant Unbounded is provided for this purpose.
Append_File is new in Ada 95.

## A.10.1 The Package Text_IO

### Static Semantics

The library package Text_IO has the following declaration:

```ada
{AI12-0302-1} with Ada.IO_Exceptions;
package Ada.Text_IO
with Global => in out synchronized is

  type File_Type is limited private;
  type File_Mode is (In_File, Out_File, Append_File);
  type Count is range 0 .. implementation-defined;
  subtype Positive_Count is Count range 1 .. Count'Last;
  Unbounded : constant Count := 0; -- line and page length
  subtype Field is Integer range 0 .. implementation-defined;
  subtype Number_Base is Integer range 2 .. 16;
  type Type_Set is (Lower_Case, Upper_Case);

  -- File Management

  procedure Create (File : in out File_Type;
                   Mode : in File_Mode := Out_File;
                   Name : in String    := "");

  procedure Open   (File : in out File_Type;
                   Mode : in File_Mode;
                   Name : in String;
                   Form : in String := "");

  procedure Close  (File : in out File_Type);
  procedure Delete (File : in out File_Type);
  procedure Reset (File : in out File_Type;
                   Mode : in File_Mode);
  procedure Reset (File : in out File_Type);

  function Mode   (File : in File_Type) return File_Mode;
  function Name   (File : in File_Type) return String;
  function Form   (File : in File_Type) return String;

  function Is_Open(File : in File_Type) return Boolean;

  -- Control of default input and output files

  procedure Set_Input (File : in File_Type);
  procedure Set_Output(File : in File_Type);
  procedure Set_Error (File : in File_Type);

  function Standard_Input return File_Type;
  function Standard_Output return File_Type;
  function Standard_Error return File_Type;

  function Current_Input return File_Type;
  function Current_Output return File_Type;
  function Current_Error return File_Type;

  type File_Access is access constant File_Type;

  function Standard_Input return File_Access;
  function Standard_Output return File_Access;
  function Standard_Error return File_Access;

  function Current_Input return File_Access;
  function Current_Output return File_Access;
  function Current_Error return File_Access;
```

---

Append_File is new in Ada 95.
procedure Flush (File : in out File_Type) with Global => overriding in out File;

procedure Flush with Global => in out all;

-- Specification of line and page lengths

procedure Set_Line_Length(File : in File_Type; To : in Count) with Global => overriding in out File;

procedure Set_Line_Length(To   : in Count) with Global => in out all;

procedure Set_Page_Length(File : in File_Type; To : in Count) with Global => overriding in out File;

procedure Set_Page_Length(To   : in Count) with Global => in out all;

function Line_Length(File : in File_Type) return Count with Global => in all;

function Page_Length(File : in File_Type) return Count with Global => in all;

-- Column, Line, and Page Control

procedure New_Line   (File    : in File_Type; Spacing : in Positive_Count := 1) with Global => overriding in out File;

procedure New_Line   (Spacing : in Positive_Count := 1) with Global => in out all;

procedure Skip_Line  (File    : in File_Type; Spacing : in Positive_Count := 1) with Global => overriding in out File;

procedure Skip_Line  (Spacing : in Positive_Count := 1) with Global => in out all;

function End_Of_Line(File : in File_Type) return Boolean with Global => in all;

function New_Page   (File : in File_Type) with Global => overriding in out File;

function New_Page with Global => in out all;

procedure Skip_Page  (File : in File_Type) with Global => overriding in out File;

procedure Skip_Page with Global => in out all;

function End_Of_Page(File : in File_Type) return Boolean with Global => in all;

function End_Of_File(File : in File_Type) return Boolean with Global => in all;

procedure Set_Col (File : in File_Type; To : in Positive_Count) with Global => overriding in out File;

procedure Set_Col (To   : in Positive_Count) with Global => in out all;

procedure Set_Line(File : in File_Type; To : in Positive_Count) with Global => overriding in out File;

procedure Set_Line(To   : in Positive_Count) with Global => in out all;

function Col (File : in File_Type) return Positive_Count with Global => in all;
function Line(File : in File_Type) return Positive_Count;
    function Line return Positive_Count
    with Global => in all;

function Page(File : in File_Type) return Positive_Count;
    function Page return Positive_Count
    with Global => in all;

-- Character Input-Output
procedure Get(File : in File_Type; Item : out Character)
    with Global => overriding in out File;
procedure Get(Item : out Character)
    with Global => in out all;

procedure Look_Ahead (File : in File_Type;
    Item : out Character;
    End_Of_Line : out Boolean)
    with Global => overriding in out File;
procedure Look_Ahead (Item : out Character;
    End_Of_Line : out Boolean)
    with Global => in out all;

procedure Get_Immediate(File : in File_Type;
    Item : out Character)
    with Global => overriding in out File;
procedure Get_Immediate(Item : out Character)
    with Global => in out all;

procedure Get_Immediate(File : in File_Type;
    Item : out Character;
    Available : out Boolean)
    with Global => overriding in out File;
procedure Get_Immediate(Item : out Character;
    Available : out Boolean)
    with Global => in out all;

-- String Input-Output
procedure Get(File : in File_Type; Item : out String)
    with Global => overriding in out File;
procedure Get(Item : out String)
    with Global => in out all;

procedure Put(File : in File_Type; Item : in Character)
    with Global => overriding in out File;
procedure Put(Item : in Character)
    with Global => in out all;

procedure Get_Line(File : in File_Type;
    Item : out String;
    Last : out Natural)
    with Global => overriding in out File;
procedure Get_Line(Item : out String;
    Last : out Natural)
    with Global => in out all;

procedure Get_Line(File : in File_Type)
    return String
    with Global => overriding in out File;
procedure Get_Line return String
    with Global => in out all;

procedure Put_Line(File : in File_Type; Item : in String)
    with Global => overriding in out File;
procedure Put_Line(Item : in String)
    with Global => in out all;

-- Generic packages for Input-Output of Integer Types
generic
type Num is range <>;
package Integer_IO is
  Default_Width : Field := Num'Width;
  Default_Base : Number_Base := 10;
  {AI12-0302-1}  procedure Get(File : in File_Type;
                     Item : out Num;
                     Width : in Field := 0)
                  with Global => overriding in out File;
  procedure Get(Item : out Num;
                 Width : in Field := 0)
       with Global => in out all;
{AI12-0302-1} {AI12-0302-1}  procedure Put(File : in File_Type;
     Item : in Num;
     Width : in Field := Default_Width;
     Base : in Number_Base := Default_Base)
             with Global => overriding in out File;
  procedure Put(Item : in Num;
               Width : in Field := Default_Width;
               Base : in Number_Base := Default_Base)
                 with Global => in out all;
  procedure Get(From : in String;
               Item : out Num;
               Last : out Positive)
            with Nonblocking;
  procedure Put(To   : out String;
             Item : in Num;
             Base : in Number_Base := Default_Base)
            with Nonblocking;
end Integer_IO;

generic
type Num is mod <>;
package Modular_IO is
  Default_Width : Field := Num'Width;
  Default_Base : Number_Base := 10;
  {AI12-0302-1}  procedure Get(File : in File_Type;
                     Item : out Num;
                     Width : in Field := 0)
                  with Global => overriding in out File;
  procedure Get(Item : out Num;
                 Width : in Field := 0)
       with Global => in out all;
{AI12-0241-1} {AI12-0302-1}  procedure Put(File : in File_Type;
     Item : in Num;
     Width : in Field := Default_Width;
     Base : in Number_Base := Default_Base)
             with Global => overriding in out File;
  procedure Put(Item : in Num;
               Width : in Field := Default_Width;
               Base : in Number_Base := Default_Base)
                 with Global => in out all;
  procedure Get(From : in String;
               Item : out Num;
               Last : out Positive)
            with Nonblocking;
  procedure Put(To   : out String;
             Item : in Num;
             Base : in Number_Base := Default_Base)
            with Nonblocking;
end Modular_IO;

-- Generic packages for Input-Output of Real Types
generic
type Num is digits <>;
package Float_IO is
  Default_Fore : Field := 2;
  Default_Aft  : Field := Num'Digits-1;
  Default_Exp  : Field := 3;

{AI12-0302-1}
  procedure Get(File  : in  File_Type;
                Item  : out Num;
                Width : in  Field := 0)
      with Global => overriding in out File;
  procedure Get(Item  : out Num;
                Width : in  Field := 0)
      with Global => in out all;
{AI12-0302-1}
  procedure Put(File : in  File_Type;
                Item : in  Num;
                Fore : in  Field := Default_Fore;
                Aft  : in  Field := Default_Aft;
                Exp  : in  Field := Default_Exp)
      with Global => in out all;
end Float_IO;

generic
type Num is delta <>;
package Fixed_IO is
  Default_Fore : Field := Num'Fore;
  Default_Aft  : Field := Num'Aft;
  Default_Exp  : Field := 0;

{AI12-0302-1}
  procedure Get(File  : in  File_Type;
                Item  : out Num;
                Width : in  Field := 0)
      with Global => overriding in out File;
  procedure Get(Item  : out Num;
                Width : in  Field := 0)
      with Global => in out all;
{AI12-0302-1}
  procedure Put(File : in  File_Type;
                Item : in  Num;
                Fore : in  Field := Default_Fore;
                Aft  : in  Field := Default_Aft;
                Exp  : in  Field := Default_Exp)
      with Global => in out all;
procedure Get(From : in String;  
    Item : out Num;  
    Last : out Positive)  
  with Nonblocking;
procedure Put(To   : out String;  
    Item : in Num;  
    Aft  : in Field := Default_Aft;  
    Exp  : in Field := Default_Exp)  
  with Nonblocking;
end Fixed_IO;
generic
  type Num is delta <> digits <>;
package Decimal_IO is
  Default_Fore : Field := Num'Fore;  
  Default_Aft  : Field := Num'Aft;  
  Default_Exp  : Field := 0;
procedure Get(File  : in File_Type;  
    Item : out Num;  
    Width : in Field := 0)  
  with Global => overriding in out File;
procedure Get(Item  : out Num;  
    Width : in Field := 0)  
  with Global => in out all;
procedure Put(File : in File_Type;  
    Item : in Num;  
    Fore : in Field := Default_Fore;  
    Aft  : in Field := Default_Aft;  
    Exp  : in Field := Default_Exp)  
  with Global => overriding in out File;
procedure Put(Item : in Num;  
    Fore : in Field := Default_Fore;  
    Aft  : in Field := Default_Aft;  
    Exp  : in Field := Default_Exp)  
  with Global => in out all;
procedure Get(From : in String;  
    Item : out Num;  
    Last : out Positive)  
  with Nonblocking;
procedure Put(To   : out String;  
    Item : in Num;  
    Aft  : in Field := Default_Aft;  
    Exp  : in Field := Default_Exp)  
  with Nonblocking;
end Decimal_IO;
-- Generic package for Input-Output of Enumeration Types
generic
  type Enum is (<>);
package Enumeration_IO is
  Default_Width   : Field := 0;  
  Default_Setting : Type_Set := Upper_Case;
procedure Get(File : in File_Type;  
    Item : out Enum)  
  with Global => overriding in out File;
procedure Get(Item : out Enum)  
  with Global => in out all;
procedure Put(File : in File_Type;
   Item : in Enum;
   Width : in Field   := Default_Width;
   Set : in Type_Set := Default_Setting)
with Global => overriding in out File;

procedure Get(From : in String;
   Item : out Enum;
   Last : out Positive)
with Nonblocking;

procedure Put(To   : out String;
   Item : in Enum;
   Set  : in Type_Set := Default_Setting)
with Nonblocking;

end Enumeration_IO;

-- Exceptions

Status_Error : exception renames IO_Exceptions.Status_Error;
Mode_Error   : exception renames IO_Exceptions.Mode_Error;
Name_Error   : exception renames IO_Exceptions.Name_Error;
Use_Error    : exception renames IO_Exceptions.Use_Error;
Device_Error : exception renames IO_Exceptions.Device_Error;
End_Error    : exception renames IO_Exceptions.End_Error;
Data_Error   : exception renames IO_Exceptions.Data_Error;
Layout_Error : exception renames IO_Exceptions.Layout_Error;

package Wide_File_Names is

-- File management

procedure Create (File : in out File_Type;
   Mode : in File_Mode := Out_File;
   Name : in Wide_String ::= "*",
   Form : in Wide_String ::= "*");

procedure Open  (File : in out File_Type;
   Mode : in File_Mode;
   Name : in Wide_String;
   Form : in Wide_String ::= "");

function Name    (File : in File_Type) return Wide_String;

function Form    (File : in File_Type) return Wide_String;

end Wide_File_Names;

package Wide_Wide_File_Names is

-- File management

procedure Create (File : in out File_Type;
   Mode : in File_Mode := Out_File;
   Name : in Wide_Wide_String ::= "*",
   Form : in Wide_Wide_String ::= "*");

procedure Open  (File : in out File_Type;
   Mode : in File_Mode;
   Name : in Wide_Wide_String;
   Form : in Wide_Wide_String ::= "");

function Name    (File : in File_Type) return Wide_Wide_String;

function Form    (File : in File_Type) return Wide_Wide_String;

end Wide_Wide_File_Names;
private
... -- not specified by the language
end Ada.Text_IO;

{AI95-00360-01} The type File_Type needs finalization (see 7.6).

Incompatibilities With Ada 83

Append_File is a new element of enumeration type File_Mode.

Extensions to Ada 83

Get_Immediate, Look_Ahead, the subprograms for dealing with standard error, the type File_Access and its associated subprograms, and the generic packages Modular_IO and Decimal_IO are new in Ada 95.

Incompatibilities With Ada 95

{AI95-00360-01} Amendment Correction: Text_IO.File_Type is defined to need finalization. If the restriction No_Nested_Finalization (see D.7) applies to the partition, and File_Type does not have a controlled part, it will not be allowed in local objects in Ada 2005 whereas it would be allowed in original Ada 95. Such code is not portable, as another Ada compiler may have a controlled part in File_Type, and thus would be illegal.

Wording Changes from Ada 95

{8652/0051} {AI95-00057-01} Corrigendum: Corrected the parameter mode of Flush; otherwise it could not be used on Standard_Output.

{AI95-00301-01} The Text_IO.Get_Line functions are new; they are described in A.10.7, “Input-Output of Characters and Strings”.

Incompatibilities With Ada 2012

{AI12-0021-1} The Wide_File_Names and Wide_Wide_File_Names nested packages are newly added to Ada.Text_IO. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

A.10.2 Text File Management

Static Semantics

{AI12-0449-1} The only allowed file modes for text files are the modes In_File, Out_File, and Append_File. The subprograms given in subclause A.8.2 for the control of external files, and the function End_Of_File given in subclause A.8.3 for sequential input-output, are also available for text files. There is also a version of End_Of_File that refers to the current default input file. For text files, the procedures have the following additional effects:

- For the procedures Create and Open: After a file with mode Out_File or Append_File is opened, the page length and line length are unbounded (both have the conventional value zero). After a file (of any mode) is opened, the current column, current line, and current page numbers are set to one. If the mode is Append_File, it is implementation defined whether a page terminator will separate preexisting text in the file from the new text to be written.

  Reason: For a file with mode Append_File, although it may seem more sensible for Open to set the current column, line, and page number based on the number of pages in the file, the number of lines on the last page, and the number of columns in the last line, we rejected this approach because of implementation costs; it would require the implementation to scan the file before doing the append, or to do processing that would be equivalent in effect.

  For similar reasons, there is no requirement to erase the last page terminator of the file, nor to insert an explicit page terminator in the case when the final page terminator of a file is represented implicitly by the implementation.

- For the procedure Close: If the file has the current mode Out_File or Append_File, has the effect of calling New_Page, unless the current page is already terminated; then outputs a file terminator.

- For the procedure Reset: If the file has the current mode Out_File or Append_File, has the effect of calling New_Page, unless the current page is already terminated; then outputs a file terminator. The current column, line, and page numbers are set to one, and the line and page lengths to
Unbounded. If the new mode is Append_File, it is implementation defined whether a page terminator will separate preexisting text in the file from the new text to be written.

**Reason:** The behavior of Reset should be similar to closing a file and reopening it with the given mode

The exception Mode_Error is propagated by the procedure Reset upon an attempt to change the mode of a file that is the current default input file, the current default output file, or the current default error file.

**NOTE** An implementation can define the Form parameter of Create and Open to control effects including the following:

- the interpretation of line and column numbers for an interactive file, and
- the interpretation of text formats in a file created by a foreign program.

### A.10.3 Default Input, Output, and Error Files

**Static Semantics**

The following subprograms provide for the control of the particular default files that are used when a file parameter is omitted from a Get, Put, or other operation of text input-output described below, or when application-dependent error-related text is to be output.

**procedure** Set_Input (File : in File_Type);

Operates on a file of mode In_File. Sets the current default input file to File.

The exception Status_Error is propagated if the given file is not open. The exception Mode_Error is propagated if the mode of the given file is not In_File.

**procedure** Set_Output (File : in File_Type);
**procedure** Set_Error (File : in File_Type);

Each operates on a file of mode Out_File or Append_File. Set_Output sets the current default output file to File. Set_Error sets the current default error file to File. The exception Status_Error is propagated if the given file is not open. The exception Mode_Error is propagated if the mode of the given file is not Out_File or Append_File.

**function** Standard_Input return File_Type;
**function** Standard_Input return File_Access;

Returns the standard input file (see A.10), or an access value designating the standard input file, respectively.

**function** Standard_Output return File_Type;
**function** Standard_Output return File_Access;

Returns the standard output file (see A.10) or an access value designating the standard output file, respectively.

**function** Standard_Error return File_Type;
**function** Standard_Error return File_Access;

{8652/0052} {AI95-00194-01} Returns the standard error file (see A.10), or an access value designating the standard error file, respectively.

The Form strings implicitly associated with the opening of Standard_Input, Standard_Output, and Standard_Error at the start of program execution are implementation defined.

**function** Current_Input return File_Type;
**function** Current_Input return File_Access;

Returns the current default input file, or an access value designating the current default input file, respectively.
function Current_Output return File_Type;
function Current_Output return File_Access;

Returns the current default output file, or an access value designating the current default output file, respectively.

function Current_Error return File_Type;
function Current_Error return File_Access;

Returns the current default error file, or an access value designating the current default error file, respectively.

procedure Flush (File : in out File_Type);

procedure Flush;

{AI95-00057-01} {8652/0051} 
{AI12-0130-1} [The effect of Flush is the same as the corresponding subprogram in Sequential_IO (see A.8.2) Streams.Stream_IO (see A.12.1).] If File is not explicitly specified, Current_Output is used.

Discussion: {AI12-0052-1} For the purpose of determining whether concurrent calls on text input-output subprograms are required to perform as specified, subprograms that implicitly operate on one of the default input-output files are considered to have a parameter of Current_Input or Current_Output (as appropriate). The result of Current_Output is considered to be overlapping with the file given to the latest call of Set_Output (or Standard_Output if Set_Output hasn't been called); a corresponding consideration applies to the result of Current_Input. See the introduction of Annex A for details.

Erroneous Execution

{AI95-00063-01} {8652/0053} The execution of a program is erroneous if it invokes an operation on a current default input, default output, or default error file, and if the corresponding file object is closed or that no longer exists.

Ramification: {AI95-00063-01} {8652/0053} Closing a default file, then setting the default file to another open file before accessing it is not erroneous.

This paragraph was deleted. {AI95-00063-01} {8652/0053} If the Close operation is applied to a file object that is also serving as the default input, default output, or default error file, then subsequent operations on such a default file are erroneous.

NOTE 1 The standard input, standard output, and standard error files cannot be opened, closed, reset, or deleted, because the parameter File of the corresponding procedures has the mode in out.

NOTE 2 The standard input, standard output, and standard error files are different file objects, but not necessarily different external files.

Wording Changes from Ada 95

{AI95-00057-01} {8652/0051} Corrigendum: Corrected the parameter mode of Flush; otherwise it could not be used on Standard_Output.

{AI95-00063-01} {8652/0052} {8652/00194-01} Corrigendum: Corrected Standard_Error so it refers to the correct file.

{AI95-00063-01} {8652/0053} Corrigendum: Clarified that execution is erroneous only when a closed default file is accessed.

Wording Changes from Ada 2012

{AI12-0130-1} Corrigendum: Moved the definition of Flush to A.8.2, as all input-output packages now have it.

A.10.4 Specification of Line and Page Lengths

Static Semantics

{AI12-0445-1} The subprograms described in this subclause are concerned with the line and page structure of a file of mode Out_File or Append_File. They operate either on the file given as the first
parameter, or, in the absence of such a file parameter, on the current default output file. They provide for output of text with a specified maximum line length or page length. In these cases, line and page terminators are output implicitly and automatically when **necessary**. When line and page lengths are unbounded (that is, when they have the conventional value zero), as in the case of a newly opened file, new lines and new pages are only started when explicitly called for.

In all cases, the exception **Status_Error** is propagated if the file to be used is not open; the exception **Mode_Error** is propagated if the mode of the file is not **Out_File** or **Append_File**.

```
procedure Set_Line_Length(File : in File_Type; To : in Count);

procedure Set_Line_Length(To   : in Count);
```

Sets the maximum line length of the specified output or append file to the number of characters specified by To. The value zero for To specifies an unbounded line length.

**Ramification:** The setting does not affect the lengths of lines in the existing file, rather it only influences subsequent output operations.

The exception **Use_Error** is propagated if the specified line length is inappropriate for the associated external file.

```
procedure Set_Page_Length(File : in File_Type; To : in Count);

procedure Set_Page_Length(To   : in Count);
```

Sets the maximum page length of the specified output or append file to the number of lines specified by To. The value zero for To specifies an unbounded page length.

The exception **Use_Error** is propagated if the specified page length is inappropriate for the associated external file.

```
function Line_Length(File : in File_Type) return Count;

function Line_Length return Count;
```

Returns the maximum line length currently set for the specified output or append file, or zero if the line length is unbounded.

```
function Page_Length(File : in File_Type) return Count;

function Page_Length return Count;
```

Returns the maximum page length currently set for the specified output or append file, or zero if the page length is unbounded.

### A.10.5 Operations on Columns, Lines, and Pages

**Static Semantics**

The subprograms described in this subclause provide for explicit control of line and page structure; they operate either on the file given as the first parameter, or, in the absence of such a file parameter, on the appropriate (input or output) current default file. The exception **Status_Error** is propagated by any of these subprograms if the file to be used is not open.

```
procedure New_Line(File : in File_Type; Spacing : in Positive_Count := 1);

procedure New_Line(Spacing : in Positive_Count := 1);
```

Operates on a file of mode **Out_File** or **Append_File**.

For a Spacing of one: Outputs a line terminator and sets the current column number to one. Then increments the current line number by one, except in the case that the current line number is already greater than or equal to the maximum page length, for a bounded page length; in that case a page terminator is output, the current page number is incremented by one, and the current line number is set to one.
For a Spacing greater than one, the above actions are performed Spacing times.

The exception Mode_Error is propagated if the mode is not Out_File or Append_File.

**procedure** Skip_Line( File : in File_Type; Spacing : in Positive_Count := 1);

Operates on a file of mode In_File.

For a Spacing of one: Reads and discards all characters until a line terminator has been read, and then sets the current column number to one. If the line terminator is not immediately followed by a page terminator, the current line number is incremented by one. Otherwise, if the line terminator is immediately followed by a page terminator, then the page terminator is skipped, the current page number is incremented by one, and the current line number is set to one.

For a Spacing greater than one, the above actions are performed Spacing times.

The exception Mode_Error is propagated if the mode is not In_File. The exception End_Error is propagated if an attempt is made to read a file terminator.

**function** End_Of_Line(File : in File_Type) return Boolean;

**function** End_Of_Line return Boolean;

{AI05-0264-1} Operates on a file of mode In_File. Returns True if a line terminator or a file terminator is next; otherwise, returns False.

The exception Mode_Error is propagated if the mode is not In_File.

**procedure** New_Page(File : in File_Type);

Operates on a file of mode Out_File or Append_File. Outputs a line terminator if the current line is not terminated, or if the current page is empty (that is, if the current column and line numbers are both equal to one). Then outputs a page terminator, which terminates the current page. Adds one to the current page number and sets the current column and line numbers to one.

The exception Mode_Error is propagated if the mode is not Out_File or Append_File.

**procedure** Skip_Page(File : in File_Type);

Operates on a file of mode In_File. Reads and discards all characters and line terminators until a page terminator has been read. Then adds one to the current page number, and sets the current column and line numbers to one.

The exception Mode_Error is propagated if the mode is not In_File. The exception End_Error is propagated if an attempt is made to read a file terminator.

**function** End_Of_Page(File : in File_Type) return Boolean;

**function** End_Of_Page return Boolean;

{AI05-0264-1} Operates on a file of mode In_File. Returns True if the combination of a line terminator and a page terminator is next, or if a file terminator is next; otherwise, returns False.

The exception Mode_Error is propagated if the mode is not In_File.

**function** End_Of_File(File : in File_Type) return Boolean;

**function** End_Of_File return Boolean;

{AI05-0264-1} Operates on a file of mode In_File. Returns True if a file terminator is next, or if the combination of a line, a page, and a file terminator is next; otherwise, returns False.

The exception Mode_Error is propagated if the mode is not In_File.
The following subprograms provide for the control of the current position of reading or writing in a file. In all cases, the default file is the current output file.

```ada
procedure Set_Col(File : in File_Type; To : in Positive_Count);
procedure Set_Col(To   : in Positive_Count);
```

If the file mode is Out_File or Append_File:

- If the value specified by To is greater than the current column number, outputs spaces, adding one to the current column number after each space, until the current column number equals the specified value. If the value specified by To is equal to the current column number, there is no effect. If the value specified by To is less than the current column number, has the effect of calling New_Line (with a spacing of one), then outputs (To – 1) spaces, and sets the current column number to the specified value.

- The exception Layout_Error is propagated if the value specified by To exceeds Line_Length when the line length is bounded (that is, when it does not have the conventional value zero).

If the file mode is In_File:

- Reads (and discards) individual characters, line terminators, and page terminators, until the next character to be read has a column number that equals the value specified by To; there is no effect if the current column number already equals this value. Each transfer of a character or terminator maintains the current column, line, and page numbers in the same way as a Get procedure (see A.10.6). (Short lines will be skipped until a line is reached that has a character at the specified column position.)

- The exception End_Error is propagated if an attempt is made to read a file terminator.

```ada
function Col(File : in File_Type) return Positive_Count;
function Col returns Positive_Count;
```

Returns the current column number.

The exception Layout_Error is propagated if this number exceeds Count'Last.
function Line( File : in File_Type ) return Positive_Count;

function Line return Positive_Count;

Returns the current line number.

The exception Layout_Error is propagated if this number exceeds Count'Last.

function Page ( File : in File_Type ) return Positive_Count;

function Page return Positive_Count;

Returns the current page number.

The exception Layout_Error is propagated if this number exceeds Count'Last.

The column number, line number, or page number are allowed to exceed Count'Last (as a consequence of the input or output of sufficiently many characters, lines, or pages). These events do not cause any exception to be propagated. However, a call of Col, Line, or Page propagates the exception Layout_Error if the corresponding number exceeds Count'Last.

NOTE {AI12-0440-1} A page terminator is always skipped whenever the preceding line terminator is skipped. An implementation can represent the combination of these terminators by a single character, provided that it is properly recognized on input.

Inconsistencies With Ada 2005

{AI05-0038-1} Correction: Fixed a glitch in Set_Line such that we could have called New_Line(0), which would have to raise Constraint_Error. It’s now defined to work. The bug occurred in Ada 95 and Ada 2005. It’s very unlikely that any real programs depend on this exception being raised.

A.10.6 Get and Put Procedures

Static Semantics

The procedures Get and Put for items of the type Character, String, numeric types, and enumeration types are described in subsequent subclauses. Features of these procedures that are common to most of these types are described in this subclause. The Get and Put procedures for items of type Character and String deal with individual character values; the Get and Put procedures for numeric and enumeration types treat the items as lexical elements.

All procedures Get and Put have forms with a file parameter, written first. Where this parameter is omitted, the appropriate (input or output) current default file is understood to be specified. Each procedure Get operates on a file of mode In_File. Each procedure Put operates on a file of mode Out_File or Append_File.

All procedures Get and Put maintain the current column, line, and page numbers of the specified file: the effect of each of these procedures upon these numbers is the result of the effects of individual transfers of characters and of individual output or skipping of terminators. Each transfer of a character adds one to the current column number. Each output of a line terminator sets the current column number to one and adds one to the current line number. Each output of a page terminator sets the current column and line numbers to one and adds one to the current page number. For input, each skipping of a line terminator sets the current column number to one and adds one to the current line number; each skipping of a page terminator sets the current column and line numbers to one and adds one to the current page number. Similar considerations apply to the procedures Get_Line, Put_Line, and Set_Col.

Several Get and Put procedures, for numeric and enumeration types, have format parameters which specify field lengths; these parameters are of the nonnegative subtype Field of the type Integer.

{AI95-00223-01} Input-output of enumeration values uses the syntax of the corresponding lexical elements. Any Get procedure for an enumeration type begins by skipping any leading blanks, or line or
page terminators. A get procedures for numeric or enumeration types start by skipping leading blanks, where a blank is defined as a space or a horizontal tabulation character. Next, characters are input only so long as the sequence input is an initial sequence of an identifier or of a character literal (in particular, input ceases when a line terminator is encountered). The character or line terminator that causes input to cease remains available for subsequent input.

For a numeric type, the Get procedures have a format parameter called Width. If the value given for this parameter is zero, the Get procedure proceeds in the same manner as for enumeration types, but using the syntax of numeric literals instead of that of enumeration literals. If a nonzero value is given, then exactly Width characters are input, or the characters up to a line terminator, whichever comes first; any skipped leading blanks are included in the count. The syntax used for numeric literals is an extended syntax that allows a leading sign (but no intervening blanks, or line or page terminators) and that also allows (for real types) an integer literal as well as forms that have digits only before the point or only after the point.

Any Put procedure, for an item of a numeric or an enumeration type, outputs the value of the item as a numeric literal, identifier, or character literal, as appropriate. This is preceded by leading spaces if required by the format parameters Width or Fore (as described in later subclauses), and then a minus sign for a negative value; for an enumeration type, the spaces follow instead of leading. The format given for a Put procedure is overridden if it is insufficiently wide, by using the minimum needed width.

Two further cases arise for Put procedures for numeric and enumeration types, if the line length of the specified output file is bounded (that is, if it does not have the conventional value zero). If the number of characters to be output does not exceed the maximum line length, but is such that they cannot fit on the current line, starting from the current column, then (in effect) New_Line is called (with a spacing of one) before output of the item. Otherwise, if the number of characters exceeds the maximum line length, then the exception Layout_Error is propagated and nothing is output.

The exception Status_Error is propagated by any of the procedures Get, Get_Line, Put, and Put_Line if the file to be used is not open. The exception Mode_Error is propagated by the procedures Get and Get_Line if the mode of the file to be used is not In_File; and by the procedures Put and Put_Line, if the mode is not Out_File or Append_File.

The exception End_Error is propagated by a Get procedure if an attempt is made to skip a file terminator. The exception Data_Error is propagated by a Get procedure if the sequence finally input is not a lexical element corresponding to the type, in particular if no characters were input; for this test, leading blanks are ignored; for an item of a numeric type, when a sign is input, this rule applies to the succeeding numeric literal. The exception Layout_Error is propagated by a Put procedure that outputs to a parameter of type String, if the length of the actual string is insufficient for the output of the item.

**Examples**

In the examples, here and in subclauses A.10.8 and A.10.9, the string quotes and the lower case letter b are not transferred: they are shown only to reveal the layout and spaces.

```ada
N : Integer;
...
Get (N);
-- Characters at input  Sequence input  Value of N
-- bb–12535b  –12535  –12535
-- bb12_535e1b  12_535e1  125350
-- bb12_535e;  12_535e  (none) Data_Error raised
```

Example of overridden width parameter:

```ada
Put (Item => -23, Width => 2);  -- "-23"
```
A.10.7 Input-Output of Characters and Strings

Static Semantics

For an item of type Character the following procedures are provided:

1. procedure Get(File : in File_Type; Item : out Character);
2. procedure Get(Item : out Character);

   After skipping any line terminators and any page terminators, reads the next character from the specified input file and returns the value of this character in the out parameter Item.

   The exception End_Error is propagated if an attempt is made to skip a file terminator.

3. procedure Put(File : in File_Type; Item : in Character);
4. procedure Put(Item : in Character);

   If the line length of the specified output file is bounded (that is, does not have the conventional value zero), and the current column number exceeds it, has the effect of calling New_Line with a spacing of one. Then, or otherwise, outputs the given character to the file.

5. procedure Look_Ahead (File : in File_Type; Item : out Character; End_Of_Line : out Boolean);
6. procedure Look_Ahead (Item : out Character; End_Of_Line : out Boolean);

   Status_Error is propagated if the file is not open. Mode_Error is propagated if the mode of the file is not In_File. Sets End_Of_Line to True if at end of line, including if at end of page or at end of file; in each of these cases the value of Item is not specified. Otherwise, End_Of_Line is set to False and Item is set to the next character (without consuming it) from the file.

7. procedure Get_Immediate(File : in File_Type; Item : out Character);
8. procedure Get_Immediate(Item : out Character);

   Reads the next character, either control or graphic, from the specified File or the default input file. Status_Error is propagated if the file is not open. Mode_Error is propagated if the mode of the file is not In_File. End_Error is propagated if at the end of the file. The current column, line and page numbers for the file are not affected.

9. procedure Get_Immediate(File : in File_Type; Item : out Character; Available : out Boolean);
10. procedure Get_Immediate(Item : out Character; Available : out Boolean);

   If a character, either control or graphic, is available from the specified File or the default input file, then the character is read; Available is True and Item contains the value of this character. If a character is not available, then Available is False and the value of Item is not specified. Status_Error is propagated if the file is not open. Mode_Error is propagated if the mode of the file is not In_File. End_Error is propagated if at the end of the file. The current column, line and page numbers for the file are not affected.

11. procedure Get_Immediate(File : in File_Type; Item : out Character; Available : out Boolean);
12. procedure Get_Immediate(Item : out Character; Available : out Boolean);

   If a character, either control or graphic, is available from the specified File or the default input file, then the character is read; Available is True and Item contains the value of this character. If a character is not available, then Available is False and the value of Item is not specified. Status_Error is propagated if the file is not open. Mode_Error is propagated if the mode of the file is not In_File. End_Error is propagated if at the end of the file. The current column, line and page numbers for the file are not affected.

13. procedure Get_Immediate(File : in File_Type; Item : out Character; Available : out Boolean);
14. procedure Get_Immediate(Item : out Character; Available : out Boolean);

   If a character, either control or graphic, is available from the specified File or the default input file, then the character is read; Available is True and Item contains the value of this character. If a character is not available, then Available is False and the value of Item is not specified. Status_Error is propagated if the file is not open. Mode_Error is propagated if the mode of the file is not In_File. End_Error is propagated if at the end of the file. The current column, line and page numbers for the file are not affected.

{AI95-0023-01} For an item of type String the following subprograms are provided:
procedure Get(File : in File_Type; Item : out String);
procedure Get(Item : out String);

Determines the length of the given string and attempts that number of Get operations for successive characters of the string (in particular, no operation is performed if the string is null).

procedure Put(File : in File_Type; Item : in String);
procedure Put(Item : in String);

Determines the length of the given string and attempts that number of Put operations for successive characters of the string (in particular, no operation is performed if the string is null).

function Get_Line(File : in File_Type) return String;
function Get_Line return String;

(AI95-00301-01) Returns a result string constructed by reading successive characters from the specified input file, and assigning them to successive characters of the result string. The result string has a lower bound of 1 and an upper bound of the number of characters read. Reading stops when the end of the line is met; Skip_Line is then (in effect) called with a spacing of 1.

(AI95-00301-01) Constraint_Error is raised if the length of the line exceeds Positive'Last; in this case, the line number and page number are unchanged, and the column number is unspecified but no less than it was before the call. The exception End_Error is propagated if an attempt is made to skip a file terminator.

Ramification: (AI95-00301-01) Precisely what is left in the file is unspecified if Constraint_Error is raised because the line doesn't fit in a String; it should be consistent with column number. This allows implementers to use whatever buffering scheme makes sense. But the line terminator is not skipped in this case.

procedure Get_Line(File : in File_Type;
Item : out String;
Last : out Natural);
procedure Get_Line(Item : out String;
Last : out Natural);

Reads successive characters from the specified input file and assigns them to successive characters of the specified string. Reading stops if the end of the string is met. Reading also stops if the end of the line is met before meeting the end of the string; in this case Skip_Line is (in effect) called with a spacing of 1. The values of characters not assigned are not specified.

If characters are read, returns in Last the index value such that Item(Last) is the last character assigned (the index of the first character assigned is Item'First). If no characters are read, returns in Last an index value that is one less than Item'First. The exception End_Error is propagated if an attempt is made to skip a file terminator.

procedure Put_Line(File : in File_Type; Item : in String);
procedure Put_Line(Item : in String);

Calls the procedure Put for the given string, and then the procedure New_Line with a spacing of one.

Implementation Advice

The Get_Immediate procedures should be implemented with unbuffered input. For a device such as a keyboard, input should be “available” if a key has already been typed, whereas for a disk file, input should always be available except at end of file. For a file associated with a keyboard-like device, any line-editing features of the underlying operating system should be disabled during the execution of Get_Immediate.

Implementation Advice: Get_Immediate should be implemented with unbuffered input; input should be available immediately; line-editing should be disabled.
NOTE 1 Get_Immediate can be used to read a single key from the keyboard “immediately”; that is, without waiting for an end of line. In a call of Get_Immediate without the parameter Available, the caller will wait until a character is available.

NOTE 2 In a literal string parameter of Put, the enclosing string bracket characters are not output. Each doubled string bracket character in the enclosed string is output as a single string bracket character, as a consequence of the rule for string literals (see 2.6).

NOTE 3 A string read by Get or written by Put can extend over several lines. An implementation is allowed to assume that certain external files do not contain page terminators, in which case Get_Line and Skip_Line can return as soon as a line terminator is read.

Incompatibilities With Ada 95

{AI95-00301-01} {AI05-0005-1} The Get_Line functions are newly added to Ada.Text_IO. If Ada.Text_IO is referenced in a use_clause, and a function Get_Line is defined in a package that is also referenced in a use_clause, the user-defined Get_Line may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 95

{AI95-00301-01} The Text_IO.Get_Line functions are new.

Wording Changes from Ada 2005

{AI05-0038-1} Correction: Added missing wording about raising Status_Error to Look_Ahead and Get_Immediate.

A.10.8 Input-Output for Integer Types

Static Semantics

The following procedures are defined in the generic packages Integer_IO and Modular_IO, which have to be instantiated for the appropriate signed integer or modular type respectively (indicated by Num in the specifications).

Values are output as decimal or based literals, without low line characters or exponent, and, for Integer_IO, preceded by a minus sign if negative. The format (which includes any leading spaces and minus sign) can be specified by an optional field width parameter. Values of widths of fields in output formats are of the nonnegative integer subtype Field. Values of bases are of the integer subtype Number_Base.

```
subtype Number_Base is Integer range 2 .. 16;
```

The default field width and base to be used by output procedures are defined by the following variables that are declared in the generic packages Integer_IO and Modular_IO:

```
Default_Width : Field := Num'Width;
Default_Base  : Number_Base := 10;
```

The following procedures are provided:

```
procedure Get(File : in File_Type; Item : out Num; Width : in Field := 0);
procedure Get(Item : out Num; Width : in Field := 0);
```

If the value of the parameter Width is zero, skips any leading blanks, line terminators, or page terminators, then reads a plus sign if present or (for a signed type only) a minus sign if present, then reads the longest possible sequence of characters matching the syntax of a numeric literal without a point. If a nonzero value of Width is supplied, then exactly Width characters are input, or the characters (possibly none) up to a line terminator, whichever comes first; any skipped leading blanks are included in the count.

Returns, in the parameter Item, the value of type Num that corresponds to the sequence input.
The exception Data_Error is propagated if the sequence of characters read does not form a legal integer literal or if the value obtained is not of the subtype Num (for Integer_IO) or is not in the base range of Num (for Modular_IO).

```ada
procedure Put(File  : in File_Type;
               Item  : in Num;
               Width : in Field := Default_Width;
               Base  : in Number_Base := Default_Base);
```

Outputs the value of the parameter Item as an integer literal, with no low lines, no exponent, and no leading zeros (but a single zero for the value zero), and a preceding minus sign for a negative value.

If the resulting sequence of characters to be output has fewer than Width characters, then leading spaces are first output to make up the difference.

Uses the syntax for decimal literal if the parameter Base has the value ten (either explicitly or through Default_Base); otherwise, uses the syntax for based literal, with any letters in upper case.

```ada
procedure Get(From : in String; Item : out Num; Last : out Positive);
```

Reads an integer value from the beginning of the given string, following the same rules as the Get procedure that reads an integer value from a file, but treating the end of the string as a file terminator. Returns, in the parameter Item, the value of type Num that corresponds to the sequence input. Returns in Last the index value such that From(Last) is the last character read.

The exception Data_Error is propagated if the sequence input does not have the required syntax or if the value obtained is not of the subtype Num.

```ada
procedure Put(To   : out String;
               Item : in Num;
               Base : in Number_Base := Default_Base);
```

Outputs the value of the parameter Item to the given string, following the same rule as for output to a file, using the length of the given string as the value for Width.

Integer_Text_IO is a library package that is a nongeneric equivalent to Text_IO.Integer_IO for the predefined type Integer:

```ada
with Ada.Text_IO;
package Ada.Integer_Text_IO is new Ada.Text_IO.Integer_IO(Integer);
```

For each predefined signed integer type, a nongeneric equivalent to Text_IO.Integer_IO is provided, with names such as Ada.Long_Integer_Text_IO.

### Implementation Permissions

The nongeneric equivalent packages can, may, but need not, be actual instantiations of the generic package for the appropriate predefined type, though that is not required.

This paragraph was deleted. NOTE— The execution of Get propagates Data_Error if the sequence of characters read forms an integer literal outside the range 0..Num'Last.

Paragraphs 24 and 25 were deleted.

### Examples

Examples of use of an instantiation of Text_IO.Integer_IO.
### A.10.8 Input-Output for Integer Types

#### Static Semantics

The following procedures are defined in the generic packages Float_IO, Fixed_IO, and Decimal_IO, which have to be instantiated for the appropriate floating point, ordinary fixed point, or decimal fixed point type respectively (indicated by Num in the specifications).

Values are output as decimal literals without low line characters. The format of each value output consists of a Fore field, a decimal point, an Aft field, and (if a nonzero Exp parameter is supplied) the letter E and an Exp field. The two possible formats thus correspond to:

- \[ \text{Fore} . \text{Aft} \]
- \[ \text{Fore} . \text{Aft} \ E \text{Exp} \]

without any spaces between these fields. The Fore field may include leading spaces, and a minus sign for negative values. The Aft field includes only decimal digits (possibly with trailing zeros). The Exp field includes the sign (plus or minus) and the exponent (possibly with leading zeros).

For floating point types, the default lengths of these fields are defined by the following variables that are declared in the generic package Float_IO:

- \( \text{Default_Fore} : \text{Field} := 2; \)
- \( \text{Default_Aft} : \text{Field} := \text{Num}'\text{Digits}-1; \)
- \( \text{Default_Exp} : \text{Field} := 3; \)

For ordinary or decimal fixed point types, the default lengths of these fields are defined by the following variables that are declared in the generic packages Fixed_IO and Decimal_IO, respectively:

- \( \text{Default_Fore} : \text{Field} := \text{Num}'\text{Fore}; \)
- \( \text{Default_Aft} : \text{Field} := \text{Num}'\text{Aft}; \)
- \( \text{Default_Exp} : \text{Field} := 0; \)

The following procedures are provided:

- \( \text{procedure Get} \Big( \text{File : in File_Type; Item : out Num; Width : in Field := 0} \Big); \)
- \( \text{procedure Get} \Big( \text{Item : out Num; Width : in Field := 0} \Big); \)

If the value of the parameter Width is zero, skips any leading blanks, line terminators, or page terminators, then reads the longest possible sequence of characters matching the syntax of any of the following (see 2.4):

- \([+–]\text{numeric~literal}\)
- \([+–]\text{numeral.[exponent]}\)
• \([+–].\text{numeral}[\text{exponent}]\)
• \([+–]\text{base}\#\text{based_numeral}.#[\text{exponent}]\)
• \([+–]\text{base}\#.\text{based_numeral}#[\text{exponent}]\)

If a nonzero value of Width is supplied, then exactly Width characters are input, or the characters (possibly none) up to a line terminator, whichever comes first; any skipped leading blanks are included in the count.

Returns in the parameter Item the value of type Num that corresponds to the sequence input, preserving the sign (positive if none has been specified) of a zero value if Num is a floating point type and Num’Signed_Zeros is True.

The exception Data_Error is propagated if the sequence input does not have the required syntax or if the value obtained is not of the subtype Num.

```ada
procedure Put(File : in File_Type;  
    Item : in Num;  
    Fore : in Field := Default_Fore;  
    Aft : in Field := Default_Aft;  
    Exp : in Field := Default_Exp);  
```

Outputs the value of the parameter Item as a decimal literal with the format defined by Fore, Aft and Exp. If the value is negative, or if Num is a floating point type where Num’Signed_Zeros is True and the value is a negatively signed zero, then a minus sign is included in the integer part. If Exp has the value zero, then the integer part to be output has as many digits as are needed to represent the integer part of the value of Item, overriding Fore if necessary, or consists of the digit zero if the value of Item has no integer part.

If Exp has a value greater than zero, then the integer part to be output has a single digit, which is nonzero except for the value 0.0 of Item.

In both cases, however, if the integer part to be output has fewer than Fore characters, including any minus sign, then leading spaces are first output to make up the difference. The number of digits of the fractional part is given by Aft, or is one if Aft equals zero. The value is rounded; a value of exactly one half in the last place is rounded away from zero.

If Exp has the value zero, there is no exponent part. If Exp has a value greater than zero, then the exponent part to be output has as many digits as are needed to represent the exponent part of the value of Item (for which a single digit integer part is used), and includes an initial sign (plus or minus). If the exponent part to be output has fewer than Exp characters, including the sign, then leading zeros precede the digits, to make up the difference. For the value 0.0 of Item, the exponent has the value zero.

```ada
procedure Get(From : in String;  
    Item : out Num;  
    Last : out Positive);  
```

Reads a real value from the beginning of the given string, following the same rule as the Get procedure that reads a real value from a file, but treating the end of the string as a file terminator. Returns, in the parameter Item, the value of type Num that corresponds to the sequence input. Returns in Last the index value such that From(Last) is the last character read.

The exception Data_Error is propagated if the sequence input does not have the required syntax, or if the value obtained is not of the subtype Num.
procedure Put(To : out String;
        Item : in Num;
        Aft : in Field := Default_Aft;
        Exp : in Field := Default_Exp);

Outputs the value of the parameter Item to the given string, following the same rule as for output to a file, using a value for Fore such that the sequence of characters output exactly fills the string, including any leading spaces.

Float_Text_IO is a library package that is a nongeneric equivalent to Text_IO.Float_IO for the predefined type Float:

```ada
with Ada.Text_IO;
package Ada.Float_Text_IO is new Ada.Text_IO.Float_IO(Float);
```

For each predefined floating point type, a nongeneric equivalent to Text_IO.Float_IO is provided, with names such as Ada.Long_Float_Text_IO.

**Implementation Permissions**

An implementation may extend Get [and Put] for floating point types to support special values such as infinities and NaNs.

**Discussion:** [AI05-0005-1] See also the similar permission for the Wide_Wide_Value, Wide_Value, and Value attributes in 3.5.

**AI12-0444-1** The implementation of Put may produce an output value with no greater accuracy than that which is supported for the base subtype. The additional accuracy, if any, of the value produced by Put when the number of requested digits in the integer and fractional parts exceeds the required accuracy is implementation defined.

**Discussion:** The required accuracy is thus Num'Base'Digits digits if Num is a floating point subtype. For a fixed point subtype the required accuracy is a function of the subtype's Fore, Aft, and Delta attributes.

**Implementation defined:** The accuracy of the value produced by Put.

**AI12-0444-1** The nongeneric equivalent packages can, but need not, be actual instantiations of the generic package for the appropriate predefined type, though that is not required.

**NOTE 1** For an item with a positive value, if output to a string exactly fills the string without leading spaces, then output of the corresponding negative value will propagate Layout_Error.

**NOTE 2** The rules for the Value attribute (see 3.5) and the rules for Get are based on the same set of formats.

**Examples**

**AI12-0429-1** *Examples of use of an instantiation of Text_IO.Float_IO:*

```ada
package Real_IO is new Float_IO(Real); use Real_IO;
-- default format used at instantiation, Default_Exp = 3
X : Real := -123.4567; -- digits 8 (see 3.5.7)
Put(X); -- default format
"-1.2345670E+02"
Put(X, Fore => 5, Aft => 3, Exp => 2); -- "bbb-1.235E+2"
Put(X, 5, 3, 0); -- "b-123.457"
```

### A.10.10 Input-Output for Enumeration Types

**Static Semantics**

The following procedures are defined in the generic package Enumeration_IO, which has to be instantiated for the appropriate enumeration type (indicated by Enum in the specification).

Values are output using either upper or lower case letters for identifiers. This is specified by the parameter Set, which is of the enumeration type Type_Set.
type Type_Set is (Lower_Case, Upper_Case);

The format (which includes any trailing spaces) can be specified by an optional field width parameter.
The default field width and letter case are defined by the following variables that are declared in the
generic package Enumeration_IO:

Default_Width   : Field := 0;
Default_Setting : Type_Set := Upper_Case;

The following procedures are provided:

procedure Get(File : in File_Type; Item : out Enum);
procedure Get(Item : out Enum);

After skipping any leading blanks, line terminators, or page terminators, reads an identifier according to the syntax of this lexical element (lower and upper case being considered equivalent), or a character literal according to the syntax of this lexical element (including the apostrophes). Returns, in the parameter Item, the value of type Enum that corresponds to the sequence input.

The exception Data_Error is propagated if the sequence input does not have the required syntax, or if the identifier or character literal does not correspond to a value of the subtype Enum.

procedure Put(File : in File_Type;
Item : in Enum;
Width : in Field := Default_Width;
Set   : in Type_Set := Default_Setting);

procedure Put(Item : in Enum;
Width : in Field := Default_Width;
Set   : in Type_Set := Default_Setting);

Outputs the value of the parameter Item as an enumeration literal (either an identifier or a character literal). The optional parameter Set indicates whether lower case or upper case is used for identifiers; it has no effect for character literals. If the sequence of characters produced has fewer than Width characters, then trailing spaces are finally output to make up the difference. If Enum is a character type, the sequence of characters produced is as for Enum'Image(Item), as modified by the Width and Set parameters.

Discussion: {AI05-0005-1} For a character type, the literal might be a Wide_Wide_Character, Wide_Character, or a control character. Whatever Image does for these things is appropriate here, too.

{AI05-0036-1} The "characters produced" defines the "characters to be output" in the sense of A.10.6, so a result that cannot fit on any bounded line will raise Layout_Error.

procedure Get(From : in String; Item : out Enum; Last : out Positive);

Reads an enumeration value from the beginning of the given string, following the same rule as the Get procedure that reads an enumeration value from a file, but treating the end of the string as a file terminator. Returns, in the parameter Item, the value of type Enum that corresponds to the sequence input. Returns in Last the index value such that From(Last) is the last character read.

The exception Data_Error is propagated if the sequence input does not have the required syntax, or if the identifier or character literal does not correspond to a value of the subtype Enum.

To be honest: {AI05-0005-1} For a character type, it is permissible for the implementation to make Get do the inverse of what Put does, in the case of wide and wide_wide character literals and control characters.

procedure Put(To   : out String;
Item : in Enum;
Set  : in Type_Set := Default_Setting);

Outputs the value of the parameter Item to the given string, following the same rule as for output to a file, using the length of the given string as the value for Width.
Although the specification of the generic package Enumeration_IO would allow instantiation for an integer type, this is not the intended purpose of this generic package, and the effect of such instantiations is not defined by the language.

NOTE 1 There is a difference between Put defined for characters, and for enumeration values. Thus

```
package Char_IO is new Ada.Text_IO Enumeration_IO (Character);
Char_IO.Put ('A');  -- outputs the character 'A', between apostrophes
```

NOTE 2 The type Boolean is an enumeration type, hence Enumeration_IO can be instantiated for this type.

Corrigendum: Corrected the wording to say Enumeration_IO can be instantiated with an integer type, not a float type.

### A.10.11 Input-Output for Bounded Strings

The package Text_IO.Bounded_IO provides input-output in human-readable form for Bounded_Strings.

#### Static Semantics

The generic library package Text_IO.Bounded_IO has the following declaration:

```
with Ada.Strings.Bounded;  
-- with Ada.Strings.Bounded generic  
-- with package Bounded is  
new Ada.Strings.Bounded.Generic_Bounded_Length (<>);
package Ada.Text_IO.Bounded_IO  
-- with Global => in out synchronized is
  procedure Put  
    (File : in File_Type;
     Item : in Bounded.Bounded_String);
  procedure Put  
    (Item : in Bounded.Bounded_String);
  procedure Put_Line  
    (File : in File_Type;
     Item : in Bounded.Bounded_String);
  procedure Put_Line  
    (Item : in Bounded.Bounded_String);
  function Get_Line  
    (File : in File_Type)  
    return Bounded.Bounded_String;
  function Get_Line  
    return Bounded.Bounded_String;
  procedure Get_Line  
    (File : in File_Type; Item : out Bounded.Bounded_String);
  procedure Get_Line  
    (Item : out Bounded.Bounded_String);
end Ada.Text_IO.Bounded_IO;
```

For an item of type Bounded_String, the following subprograms are provided:

```
procedure Put  
  (File : in File_Type;
   Item : in Bounded.Bounded_String);

Equivalent to Text_IO.Put (File, Bounded.To_String(Item));
```
A.10.12 Input-Output for Unbounded Strings

The package Text_IO.Unbounded_IO provides input-output in human-readable form for Unbounded Strings.

Static Semantics

The library package Text_IO.Unbounded_IO has the following declaration:

```ada
with Ada.Strings.Unbounded;
package Ada.Text_IO.Unbounded_IO is
    with Global => in out synchronized is
    procedure Put
        (File : in File_Type;
         Item : in Strings.Unbounded.Unbounded_String);
    procedure Put
        (Item : in Strings.Unbounded.Unbounded_String);
    procedure Put_Line
        (File : in File_Type;
         Item : in Strings.Unbounded.Unbounded_String);
    procedure Put_Line
        (Item : in Strings.Unbounded.Unbounded_String);
    function Get_Line
        (File : in File_Type)
        return Strings.Unbounded.Unbounded_String;
```

Extensions to Ada 95

Package Text_IO.Bounded_IO is new.
function Get_Line
return Strings.Unbounded.Unbounded_String;

procedure Get_Line
(File : in File_Type; Item : out Strings.Unbounded.Unbounded_String);

procedure Get_Line
(Item : out Strings.Unbounded.Unbounded_String);
end Ada.Text_IO.Unbounded_IO;

{AI95-00301-01} For an item of type Unbounded_String, the following subprograms are provided:

procedure Put
(File : in File_Type;
   Item : in Strings.Unbounded.Unbounded_String);

{AI95-00301-01} Equivalent to Text_IO.Put (File, Strings.Unbounded.To_String(Item));

procedure Put
(Item : in Strings.Unbounded.Unbounded_String);

{AI95-00301-01} Equivalent to Text_IO.Put (Strings.Unbounded.To_String(Item));

procedure Put_Line
(File : in File_Type;
   Item : in Strings.Unbounded.Unbounded_String);

{AI95-00301-01} Equivalent to Text_IO.Put_Line (File, Strings.Unbounded.To_String(Item));

procedure Put_Line
(Item : in Strings.Unbounded.Unbounded_String);

{AI95-00301-01} Equivalent to Text_IO.Put_Line (Strings.Unbounded.To_String(Item));

function Get_Line
(File : in File_Type)
return Strings.Unbounded.Unbounded_String;

{AI95-00301-01} Returns Strings.Unbounded.To_Unbounded_String(Text_IO.Get_Line(File));

function Get_Line
return Strings.Unbounded.Unbounded_String;

{AI95-00301-01} Returns Strings.Unbounded.To_Unbounded_String(Text_IO.Get_Line);

procedure Get_Line
(File : in File_Type; Item : out Strings.Unbounded.Unbounded_String);

{AI95-00301-01} Equivalent to Item := Get_Line (File);

procedure Get_Line
(Item : out Strings.Unbounded.Unbounded_String);

{AI95-00301-01} Equivalent to Item := Get_Line;

Extensions to Ada 95

{AI95-00301-01} Package Text_IO.Unbounded_IO is new.

A.11 Wide Text Input-Output and Wide Wide Text Input-Output

{AI95-00285-01} The packages Wide_Text_IO and Wide_Wide_Text_IO provide facilities for input and output in human-readable form. Each file is read or written sequentially, as a sequence of wide characters (or wide wide characters) grouped into lines, and as a sequence of lines grouped into pages.
The specification of package Wide_Text_IO is the same as that for Text_IO, except that in each Get, Look_Ahead, Get_Immediate, Get_Line, Put, and Put_Line subroutine, any occurrence of Character is replaced by Wide_Character, and any occurrence of String is replaced by Wide_String. Nongeneric equivalents of Wide_Text_IO.Integer_IO and Wide_Text_IO.Float_IO are provided (as for Text_IO) for each predefined numeric type, with names such as Ada.Integer_Wide_Text_IO, Ada.Long_Integer_Wide_Text_IO, Ada.Float_Wide_Text_IO, Ada.Long_Float_Wide_Text_IO.

The specification of package Wide_Wide_Text_IO is the same as that for Text_IO, except that in each Get, Look_Ahead, Get_Immediate, Get_Line, Put, and Put_Line subroutine, any occurrence of Character is replaced by Wide_Wide_Character, and any occurrence of String is replaced by Wide_Wide_String. Nongeneric equivalents of Wide_Wide_Text_IO.Integer_IO and Wide_Wide_Text_IO.Float_IO are provided (as for Text_IO) for each predefined numeric type, with names such as Ada.Integer_Wide_Wide_Text_IO, Ada.Long_Integer_Wide_Wide_Text_IO, Ada.Float_Wide_Wide_Text_IO, Ada.Long_Float_Wide_Wide_Text_IO.

The specification of package Wide_Text_IO.Wide_Bounded_IO is the same as that for Text_IO.Bounded_IO, except that any occurrence of Bounded_String is replaced by Bounded_Wide_String, and any occurrence of package Bounded is replaced by Wide_Bounded. The specification of package Wide_Wide_Text_IO.Wide_Wide_Bounded_IO is the same as that for Text_IO.Bounded_IO, except that any occurrence of Bounded_String is replaced by Bounded_Wide_Wide_String, and any occurrence of package Bounded is replaced by Wide_Wide_Bounded.

Support for Wide_Character and Wide_String I/O is new in Ada 95.

Packages Wide_Text_IO.Wide_Unbounded_IO and Wide_Wide_Text_IO.Wide_Wide_Unbounded_IO are also new.
Wording Changes from Ada 2005

\{AI05-0092-1\} **Correction:** Corrected the names of various entities in the above description. Since the previously named entities don’t exist and the intent is obvious, this is just considered a presentation change.

A.12 Stream Input-Output

\{AI95-00285-01\} The packages Streams.Stream_IO, Text_IO.Text_Streams, and Wide_Text_IO.Text_Streams, and Wide_Wide_Text_IO.Text_Streams provide stream-oriented operations on files.

Wording Changes from Ada 95

\{AI95-00285-01\} Included package Wide_Wide_Text_IO.Text_Streams in this description.

A.12.1 The Package Streams.Stream_IO

[The subprograms in the child package Streams.Stream_IO provide control over stream files. Access to a stream file is either sequential, via a call on Read or Write to transfer an array of stream elements, or positional (if supported by the implementation for the given file), by specifying a relative index for an element. Since a stream file can be converted to a Stream_Access value, calling stream-oriented attribute subprograms of different element types with the same Stream_Access value provides heterogeneous input-output.] See 13.13 for a general discussion of streams.

Static Semantics

\{8652/0055\} \{AI95-00026-01\} The elements of a stream file are stream elements. If positioning is supported for the specified external file, a current index and current size are maintained for the file as described in A.8. If positioning is not supported, a current index is not maintained, and the current size is implementation defined.

**Implementation defined:** Current size for a stream file for which positioning is not supported.

The library package Streams.Stream_IO has the following declaration:

\{AI05-0283-1\} \{AI12-0302-1\} with Ada.IO_Exceptions;
package Ada.Streams.Stream_IO
with Preelaborate, Global => in out synchronized is
pragma Preelaborate(Stream_IO);

type Stream_Access is access all Root_Stream_Type'Class;

\{AI12-0102-1\} \{AI12-0399-1\} type File_Type is limited private;
withpragma Preelaborable_Initialization(File_Type);

type File_Mode is (In_File, Out_File, Append_File);

type Count is range 0 .. implementation-defined;
subtype Positive_Count is Count range 1 .. Count'Last;

procedure Create (File : in out File_Type;
    Mode : in File_Mode := Out_File;
    Name : in String := "";
    Form : in String := "");

procedure Open (File : in out File_Type;
    Mode : in File_Mode;
    Name : in String;
    Form : in String := "");

procedure Close (File : in out File_Type);
procedure Delete (File : in out File_Type);
procedure Reset (File : in out File_Type; Mode : in File_Mode);
procedure Reset (File : in out File_Type);
function Mode (File : in File_Type) return File_Mode;
function Name (File : in File_Type) return String;
function Form (File : in File_Type) return String;
function Is_Open (File : in File_Type) return Boolean;
function End_Of_File (File : in File_Type) return Boolean;
function Stream (File : in File_Type) return Stream_Access;

-- Return stream access for use with T'Input and T'Output

procedure Read (File : in File_Type;
Item : out Stream_Element_Array;
Last : out Stream_Element_Offset;
From : in Positive_Count)
with Global => overriding in out File;

procedure Write (File : in File_Type;
Item : in Stream_Element_Array;
To : in Positive_Count)
with Global => overriding in out File;

procedure Set_Index (File : in out File_Type; To : in Positive_Count)
with Global => overriding in out File;

function Index (File : in File_Type) return Positive_Count;
function Size (File : in File_Type) return Count;

procedure Set_Mode (File : in out File_Type;
Mode : in File_Mode);

package Wide_File_Names is
    -- File management
    procedure Create (File : in out File_Type;
Mode : in File_Mode := Out_File;
Name : in Wide_String := "");
    procedure Open (File : in out File_Type;
Mode : in File_Mode;
Name : in Wide_String;  
Form : in Wide_String := ");

function Name (File : in File_Type) return Wide_String;
function Form (File : in File_Type) return Wide_String;

end Wide_File_Names;
package Wide_Wide_File_Names is
  -- File management
  procedure Create (File : in out File_Type;
                   Mode : in File_Mode := Out_File;
                   Name : in Wide_Wide_String := "";
                   Form : in Wide_Wide_String := "");
  procedure Open (File : in out File_Type;
                  Mode : in File_Mode;
                  Name : in Wide_Wide_String;
                  Form : in Wide_Wide_String := "");
  function Name (File : in File_Type) return Wide_Wide_String;
  function Form (File : in File_Type) return Wide_Wide_String;
end Wide_Wide_File_Names;

private
  ... -- not specified by the language
end Ada.Streams.Stream_IO;

The type File_Type needs finalization (see 7.6).

The subprograms given in subclause A.8.2 for the control of external files (Create, Open, Close, Delete, Reset, Mode, Name, Form, and Is_Open, and Flush) are available for stream files, and End_of_File have the same effect as the corresponding subprograms in Sequential_IO (see A.8.2).

The End_of_File function:

- Propagates Mode_Error if the mode of the file is not In_File;
- If positioning is supported for the given external file, the function returns True if the current index exceeds the size of the external file; otherwise, it returns False;
- If positioning is not supported for the given external file, the function returns True if no more elements can be read from the given file; otherwise, it returns False.

The Set_Mode procedure sets changes the mode of the file. If the new mode is Append_File, the file is positioned to its end; otherwise, the position in the file is unchanged.

This paragraph was deleted. The Flush procedure synchronizes the external file with the internal file (by flushing any internal buffers) without closing the file or changing the position. Mode_Error is propagated if the mode of the file is In_File.

The Stream function returns a Stream_Access result from a File_Type object, thus allowing the stream-oriented attributes Read, Write, Input, and Output to be used on the same file for multiple types. Stream propagates Status_Error if File is not open.

The procedures Read and Write are equivalent to the corresponding operations in the package Streams. Read propagates Mode_Error if the mode of File is not In_File. Write propagates Mode_Error if the mode of File is not Out_File or Append_File. The Read procedure with a Positive_Count parameter starts reading at the specified index. The Write procedure with a Positive_Count parameter starts writing at the specified index. For a file that supports positioning, Read without a Positive Count parameter starts reading at the current index, and Write without a Positive Count parameter starts writing at the current index.

The Size function returns the current size of the file.

The Index function returns the current file index, as a count (in stream elements) from the beginning of the file. The position of the first element in the file is 1.
The notion of Index for Stream_IO is analogous to that of Index in Direct_IO, except that the former is measured in Stream_Element units, whereas the latter is in terms of Element_Type values.

The Set_Index procedure sets the current index to the specified value.

- **If positioning is supported for the external file, the current index is maintained as follows:**
  
  - **For Open and Create, if the Mode parameter is Append_File, the current index is set to the current size of the file plus one; otherwise, the current index is set to one.**
  
  - **For Reset, if the Mode parameter is Append_File, or no Mode parameter is given and the current mode is Append_File, the current index is set to the current size of the file plus one; otherwise, the current index is set to one.**
  
  - **For Set_Mode, if the new mode is Append_File, the current index is set to current size plus one; otherwise, the current index is unchanged.**
  
  - **For Read and Write without a Positive_Count parameter, the current index is incremented by the number of stream elements read or written.**
  
  - **For Read and Write with a Positive_Count parameter, the value of the current index is set to the value of the Positive_Count parameter plus the number of stream elements read or written.**

If positioning is not supported for the given file, then a call of Index or Set_Index propagates Use_Error. Similarly, a call of Read or Write with a Positive_Count parameter propagates Use_Error.

**Implementation Note:** It is permissible for an implementation to implement mode Append_File using the Unix append mode (the O_APPEND bit). Such an implementation does not support positioning when the mode is Append_File, and therefore the operations listed above must raise Use_Error. This is acceptable as there is no requirement that any particular file support positioning; therefore it is acceptable that a file support positioning when opened with mode Out_File, and the same file not support positioning when opened with mode Append_File. But it is not acceptable for a file to support positioning (by allowing the above operations), but to do something other than the defined semantics (that is, always write at the end, even when explicitly commanded to write somewhere else).

**Paragraphs 34 through 36 were deleted.**

- **The Size function returns the current size of the file, in stream elements.**

- **The Set_Mode procedure changes the mode of the file. If the new mode is Append_File, the file is positioned to its end; otherwise, the position in the file is unchanged.**

- **The Flush procedure synchronizes the external file with the internal file (by flushing any internal buffers) without closing the file or changing the position. Mode_Error is propagated if the mode of the file is In_File.**

**Erroneous Execution**

- **If the File_Type object passed to the Stream function is later closed or finalized, and the stream-oriented attributes are subsequently called (explicitly or implicitly) on the Stream_Access value returned by Stream, execution is erroneous. This rule applies even if the File_Type object was opened again after it had been closed.**

  **Reason:** These rules are analogous to the rule for the result of the Current_Input, Current_Output, and Current_Error functions. These rules make it possible to represent a value of (some descendant of) Root_Stream_Type which represents a file as an access value, with a null value corresponding to a closed file.

**Inconsistencies With Ada 95**

- **Amendment Correction:** The description of the subprograms for managing files was corrected so that they do not require truncation of the external file — a stream file is not a sequential file. An Ada 95 program that expects truncation of the stream file might not work under Ada 2005. Note that the Ada 95
standard was ambiguous on this point (the normative wording seemed to require truncation, but didn’t explain where; the AARM notes seemed to expect behavior like Direct_IO), and implementations varied widely. Therefore, as a practical matter, code that depends on stream truncation might not work even in Ada 95; deleting the file before opening it provides truncation that works in both Ada 95 and Ada 2005.

Incompatibilities With Ada 95

{AI95-00360-01} Amendment Correction: Stream_IO.File_Type is defined to need finalization. If the restriction No_Nested_Finalization (see D.7) applies to the partition, and File_Type does not have a controlled part, it will not be allowed in local objects in Ada 2005 whereas it would be allowed in original Ada 95. Such code is not portable, as another Ada compiler may have a controlled part in File_Type, and thus would be illegal.

Wording Changes from Ada 95

{8652/0051} {AI95-00057-01} Corrigendum: Corrected the parameter mode of Flush; otherwise it could not be used on Standard_Output.

{8652/0055} {AI95-00026-01} {AI95-00256-01} Corrigendum: Added wording to describe the effects of the various operations on the current index. The Amendment adds an explanation of the use of current index for Read and Write.

{8652/0056} {AI95-00001-01} {AI95-00026-01} Corrigendum: Clarified that Stream can raise Status_Error, and clarified that using a Stream_Access whose file has been closed is erroneous.

{AI95-00085-01} Clarified that Set_Mode can be called with the current mode.

Extensions to Ada 2005

{AI05-0283-1} Package Ada.Streams.Stream_IO is now preelaborated, allowing it to be used in more contexts (including in distributed systems). Note that it is not a remote types package; File_Type objects cannot be passed between partitions.

Incompatibilities With Ada 2012

{AI12-0021-1} The_Wide_File_Names and Wide_Wide_File_Names nested packages are newly added to Ada.Stream_IO. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

Extensions to Ada 2012

{AI12-0102-1} Corrigendum: Type Ada.Streams.Stream_IO.File_Type now has preelaborable initialization. This allows declaring library-level file objects in preelaborable packages (an oversight from the change above).

Wording Changes from Ada 2012

{AI12-0130-1} Corrigendum: The definition of the Flush procedure was moved to A.8.2, so that it could be shared by all of the I/O packages.

A.12.2 The Package Text_IO.Text_Streams

The package Text_IO.Text_Streams provides a function for treating a text file as a stream.

Static Semantics

The library package Text_IO.Text_Streams has the following declaration:

{AI12-0302-1} with Ada.Streams;
package Ada.Text_IO.Text_Streams
  with Global => in out synchronized is
    type Stream_Access is access all Streams.Root_Stream_Type’Class;
    function Stream (File : in File_Type) return Stream_Access;
end Ada.Text_IO.Text_Streams;

The Stream function has the same effect as the corresponding function in Streams.Stream_IO.

NOTE 1 The ability to obtain a stream for a text file allows Current_Input, Current_Output, and Current_Error to be processed with the functionality of streams, including the mixing of text and binary input-output, and the mixing of binary input-output for different types.

NOTE 2 Performing operations on the stream associated with a text file does not affect the column, line, or page counts.
A.12.3 The Package Wide_Text_IO.Text_Streams

The package Wide_Text_IO.Text_Streams provides a function for treating a wide text file as a stream.

Static Semantics

The library package Wide_Text_IO.Text_Streams has the following declaration:

```ada
{AI12-0302-1} with Ada.Streams;
package Ada.Wide_Text_IO.Text_Streams
  with Global => in out synchronized is
  type Stream_Access is access all Streams.Root_Stream_Type'Class;
  function Stream (File : in File_Type) return Stream_Access;
end Ada.Wide_Text_IO.Text_Streams;
```

The Stream function has the same effect as the corresponding function in Streams.Stream_IO.

A.12.4 The Package Wide_Wide_Text_IO.Text_Streams

The package Wide_Wide_Text_IO.Text_Streams provides a function for treating a wide wide text file as a stream.

Static Semantics

The library package Wide_Wide_Text_IO.Text_Streams has the following declaration:

```ada
{AI95-00285-01} with Ada.Streams;
package Ada.Wide_Wide_Text_IO.Text_Streams
  with Global => in out synchronized is
  type Stream_Access is access all Streams.Root_Stream_Type'Class;
  function Stream (File : in File_Type) return Stream_Access;
end Ada.Wide_Wide_Text_IO.Text_Streams;
```

The Stream function has the same effect as the corresponding function in Streams.Stream_IO.

Extensions to Ada 95

{AI95-00285-01} Package Wide_Wide_Text_IO.Text_Streams is new.

A.13 Exceptions in Input-Output

The package IO_Exceptions defines the exceptions used needed by the predefined input-output packages.

Static Semantics

The library package IO_Exceptions has the following declaration:

```ada
{AI12-0445-1} package Ada.IO_Exceptions is
  pragma Pure is(IO_Exceptions);
  Status_Error : exception;
  Mode_Error   : exception;
  Name_Error   : exception;
  Use_Error    : exception;
  Device_Error : exception;
  End_Error    : exception;
  Data_Error   : exception;
  Layout_Error : exception;
end Ada.IO_Exceptions;
```
If more than one error condition exists, the corresponding exception that appears earliest in the following list is the one that is propagated.

The exception **Status_Error** is propagated by an attempt to operate upon a file that is not open, and by an attempt to open a file that is already open.

The exception **Mode_Error** is propagated by an attempt to read from, or test for the end of, a file whose current mode is **Out_File** or **Append_File**, and also by an attempt to write to a file whose current mode is **In_File**. In the case of **Text_IO**, the exception **Mode_Error** is also propagated by specifying a file whose current mode is **Out_File** or **Append_File** in a call of **Set_Input**, **Skip_Line**, **End_Of_Line**, **Skip_Page**, or **End_Of_Page**; and by specifying a file whose current mode is **In_File** in a call of **Set_Output**, **Set_Line_Length**, **Set_Page_Length**, **Line_Length**, **Page_Length**, **New_Line**, or **New_Page**.

The exception **Name_Error** is propagated by a call of Create or Open if the string given for the parameter Name does not allow the identification of an external file. For example, this exception is propagated if the string is improper, or, alternatively, if either none or more than one external file corresponds to the string.

The exception **Use_Error** is propagated if an operation is attempted that is not possible for reasons that depend on characteristics of the external file. For example, this exception is propagated by the procedure Create, among other circumstances, if the given mode is **Out_File** but the form specifies an input only device, if the parameter Form specifies invalid access rights, or if an external file with the given name already exists and overwriting is not allowed.

The exception **Device_Error** is propagated if an input-output operation cannot be completed because of a malfunction of the underlying system.

The exception **End_Error** is propagated by an attempt to skip (read past) the end of a file.

The exception **Data_Error** can be propagated by the procedure **Read** (or by the **Read** attribute) if the element read cannot be interpreted as a value of the required subtype. This exception is also propagated by a procedure **Get** (defined in the package **Text_IO**) if the input character sequence fails to satisfy the required syntax, or if the value input does not belong to the range of the required subtype.

The exception **Layout_Error** is propagated (in text input-output) by **Col**, **Line**, or **Page** if the value returned exceeds Count'Last. The exception **Layout_Error** is also propagated on output by an attempt to set column or line numbers in excess of specified maximum line or page lengths, respectively (excluding the unbounded cases). It is also propagated by an attempt to Put too many characters to a string.

{AI05-0262-1} These exceptions are also propagated by various other language-defined packages and operations, see the definition of those entities for other reasons that these exceptions are propagated.

**Reason:** {AI05-0299-1} This subclause is based in Ada 95. Later versions of Ada (starting with Technical Corrigendum 1) have added a number of additional places and reasons that cause these exceptions. In particular, TC1 says that stream attributes need to raise **End_Error** in some circumstances; Amendment 1 adds **Ada.Directories** and a number of new places and reasons that Name_Error and Use_Error are raised. There are more. We don't want to try to update this text (or even this note!) for every possible reason and place that might raise one of these exceptions, so we add this blanket statement.

**Documentation Requirements**

The implementation shall document the conditions under which **Name_Error**, **Use_Error** and **Device_Error** are propagated.

**Documentation Requirement:** The conditions under which **Io_Exceptions.Name_Error**, **Io_Exceptions.Use_Error**, and **Io_Exceptions.Device_Error** are propagated.
A.13 Exceptions in Input-Output

A.14 File Sharing

Dynamic Semantics

1 It is not specified by the language whether the same external file can be associated with more than one file object. If such sharing is supported by the implementation, the following effects are defined:

2 - Operations on one text file object do not affect the column, line, and page numbers of any other file object.

3 - For direct and stream files, the current index is a property of each file object; an operation on one file object does not affect the current index of any other file object.

5 - For direct and stream files, the current size of the file is a property of the external file.

6 All other effects are identical.

Wording Changes from Ada 95

A.15 The Package Command_Line

The package Command_Line allows a program to obtain the values of its arguments and to set the exit status code to be returned on normal termination.


Static Semantics

The library package Ada.Command_Line has the following declaration:

package Ada.Command_Line is
   withpragma Preelaborate, Nonblocking, Global => in out synchronized
   in Command_Line);
   function Argument_Count return Natural;
   function Argument (Number : in Positive) return String;
function Command_Name return String;

type Exit_Status is implementation-defined integer type;

Success : constant Exit_Status;
Failure : constant Exit_Status;

procedure SetExit_Status (Code : in Exit_Status);

private
  ... -- not specified by the language
end Ada.Command_Line;

function Argument_Count return Natural;
  {AI05-0264-1} If the external execution environment supports passing arguments to a program,
  then Argument_Count returns the number of arguments passed to the program invoking the
  function. Otherwise, it returns 0. The meaning of “number of arguments” is implementation
  defined.

function Argument (Number : in Positive) return String;
  {AI12-0259-1} If the external execution environment supports passing arguments to a program,
  then Argument returns an implementation-defined value with lower bound 1 corresponding to the
  argument at relative position Number. If Number is outside the range 1..Argument_Count, then
  Constraint_Error is propagated.

  Ramification: If the external execution environment does not support passing arguments to a program, then
  Argument(N) for any N will raise Constraint_Error, since Argument_Count is 0.

function Command_Name return String;
  {AI05-0264-1} {AI12-0259-1} If the external execution environment supports passing arguments
  to a program, then Command_Name returns an implementation-defined value with lower bound 1 corresponding to the
  name of the command invoking the program; otherwise, Command_Name
  returns the null string.

type Exit_Status is implementation-defined integer type;

The type Exit_Status represents the range of exit status values supported by the external
execution environment. The constants Success and Failure correspond to success and failure,
respectively.

procedure SetExit_Status (Code : in Exit_Status);

  If the external execution environment supports returning an exit status from a program, then
  Set Exit_Status sets Code as the status. Normal termination of a program returns as the exit status
  the value most recently set by Set Exit_Status, or, if no such value has been set, then the value
  Success. If a program terminates abnormally, the status set by Set Exit_Status is ignored, and an
  implementation-defined exit status value is set.

  If the external execution environment does not support returning an exit value from a program,
  then Set Exit_Status does nothing.

Implementation Permissions

An alternative declaration is allowed for package Command_Line if different functionality is appropriate
for the external execution environment.

NOTE Argument_Count, Argument, and Command_Name correspond to the C language's argc, argv[n] (for n>0) and
argv[0], respectively.

To be honest: The correspondence of Argument_Count to argc is not direct — argc would be one more than
Argument_Count, since the argc count includes the command name, whereas Argument_Count does not.
Extensions to Ada 83

22.b/3

{AI05-0299-1} This subclause is new in Ada 95.

Wording Changes from Ada 2012

22.c/5

{AI12-0259-1} Correction: Defined the lower bound of functions Argument and Command_Name. This could be inconsistent if someone depended on the lower bound of these routines (and it wasn't 1), but such code was never portable (even to later versions of the same implementation). Thus we don't document it as an inconsistency.

A.15.1 The Packages Wide_Command_Line and Wide_Wide_Command_Line

1/5

{AI12-0021-1} The packages Wide_Command_Line and Wide_Wide_Command_Line allow a program to obtain the values of its arguments and to set the exit status code to be returned on normal termination.

Static Semantics

2/5

{AI12-0021-1} The specification of package Wide_Command_Line is the same as for Command_Line, except that each occurrence of String is replaced by Wide_String.

3/5

{AI12-0021-1} The specification of package Wide_Wide_Command_Line is the same as for Command_Line, except that each occurrence of String is replaced by Wide_Wide_String.

Extensions to Ada 2012

3.a/5

{AI12-0021-1} These packages are new.

A.16 The Package Directories

1/2

{AI95-00248-01} The package Directories provides operations for manipulating files and directories, and their names.

Discussion: {AI05-0299-1} The notes for this subclause contain the expected interpretations of some of the operations on various target systems. “Unix” refers to the UNIX® operating system, and in most cases also covers Unix-like systems such as Linux and POSIX. “Windows®” refers to the Microsoft® Windows® 2000 operating system and usually also covers most other versions that use the Win32 API.

Static Semantics

2/2

{AI95-00248-01} The library package Directories has the following declaration:

3/5

{AI12-0302-1} with Ada.IO_Exceptions;
with Ada.Calendar;
package Ada.Directories
with Global => in out synchronized is

4/2

-- Directory and file operations:

5/2

function Current_Directory return String;

6/2

procedure Set_Directory (Directory : in String);

7/2

procedure Create_Directory (New_Directory : in String;
Form          : in String := "");

8/2

procedure Delete_Directory (Directory : in String);

9/2

procedure Create_Path (New_Directory : in String;
Form          : in String := "");

10/2

procedure Delete_Tree (Directory : in String);

11/2

procedure Delete_File (Name : in String);

12/2

procedure Rename (Old_Name, New_Name : in String);
procedure Copy_File (Source_Name, Target_Name : in String; Form : in String := "") with Nonblocking;

function Full_Name (Name : in String) return String with Nonblocking;

function Simple_Name (Name : in String) return String with Nonblocking;

function Containing_Directory (Name : in String) return String with Nonblocking;

function Extension (Name : in String) return String with Nonblocking;

function Base_Name (Name : in String) return String with Nonblocking;


type Name_Case_Kind is (Unknown, Case_Sensitive, Case_Insensitive, Case_Preserving);

function Name_Case_Equivalence (Name : in String) return Name_Case_Kind;

type File_Kind is (Directory, Ordinary_File, Special_File);

type File_Size is range 0 .. implementation-defined;

function Exists (Name : in String) return Boolean;

function Kind (Name : in String) return File_Kind;

function Size (Name : in String) return File_Size;

function Modification_Time (Name : in String) return Ada.Calendar.Time;

procedure Start_Search (Search : in out Search_Type; Directory : in String; Pattern : in String; Filter : in Filter_Type := (others => True));

procedure End_Search (Search : in out Search_Type);

function More_Entries (Search : in Search_Type) return Boolean;

procedure Get_Next_Entry (Search : in out Search_Type; Directory_Entry : out Directory_Entry_Type);

procedure Search (Directory : in String; Pattern : in String; Filter : in Filter_Type := (others => True); Process : not null access procedure (Directory_Entry : in Directory_Entry_Type)) with Allows_Exit;

function Simple_Name (Directory_Entry : in Directory_Entry_Type) return String;

function Full_Name (Directory_Entry : in Directory_Entry_Type) return String;
procedure Kind (Directory_Entry : in Directory_Entry_Type)
    return File_Kind;

procedure Size (Directory_Entry : in Directory_Entry_Type)
    return File_Size;

procedure Modification_Time (Directory_Entry : in Directory_Entry_Type)
    return Ada.Calendar.Time;

Status_Error : exception renames Ada.IO_Exceptions.Status_Error;
Name_Error   : exception renames Ada.IO_Exceptions.Name_Error;
Use_Error    : exception renames Ada.IO_Exceptions.Use_Error;
Device_Error : exception renames Ada.IO_Exceptions.Device_Error;

end Ada.Directories;

External files may be classified as directories, special files, or ordinary files. A directory is an external file that is a container for files on the target system. A special file is an external file that cannot be created or read by a predefined Ada input-output package. External files that are not special files or directories are called ordinary files.

Ramification: A directory is an external file, although it may not have a name on some targets. A directory is not a special file, as it can be created and read by Directories.

Discussion: Devices and soft links are examples of special files on Windows® and Unix. Even if an implementation provides a package to create and read soft links, such links are still special files.

A file name is a string identifying an external file. Similarly, a directory name is a string identifying a directory. The interpretation of file names and directory names is implementation defined.

Implementation defined: The interpretation of file names and directory names.

The full name of an external file is a full specification of the name of the file. If the external environment allows alternative specifications of the name (for example, abbreviations), the full name should not use such alternatives. A full name typically will include the names of all of the directories that contain the item. The simple name of an external file is the name of the item, not including any containing directory names. Unless otherwise specified, a file name or directory name parameter in a call to a predefined Ada input-output subprogram can be a full name, a simple name, or any other form of name supported by the implementation.

Discussion: The full name on Unix is a complete path to the root. For Windows®, the full name includes a complete path, as well as a disk name ("C:"), or network share name. For both systems, the simple name is the part of the name following the last "/" (or \\ for Windows®). For example, in the name "/usr/randy/ada-directories.ads", "ada-directories.ads" is the simple name.

Ramification: It is possible for a file or directory name to be neither a full name nor a simple name. For instance, the Unix name "/parent/myfile" is neither a full name nor a simple name.

A root directory is a directory that has no containing directory.

Implementation Note: For Unix and Unix-like systems, "/" is the root. For Windows®, "C:" and "\Computer\Share" are roots.

The default directory is the directory that is used if a directory or file name is not a full name (that is, when the name does not fully identify all of the containing directories).

Discussion: The default directory is the one maintained by the familiar "cd" command on Unix and Windows®. Note that Windows® maintains separate default directories for each disk drive; implementations should use the natural implementation.

A directory entry is a single item in a directory, identifying a single external file (including directories and special files).

For each function that returns a string, the lower bound of the returned value is 1.
The following file and directory operations are provided:

*function* Current_Directory *return* String;

Returns the full directory name for the current default directory. The name returned shall be suitable for a future call to Set_Directory. The exception Use_Error is propagated if a default directory is not supported by the external environment.

*procedure* Set_Directory (Directory : *in* String);

Sets the current default directory. The exception Name_Error is propagated if the string given as Directory does not identify an existing directory. The exception Use_Error is propagated if the external environment does not support making Directory (in the absence of Name_Error) a default directory.

*procedure* Create_Directory (New_Directory : *in* String;

Form : *in* String := "");

Creates a directory with name New_Directory. The Form parameter can be used to give system-dependent characteristics of the directory; the interpretation of the Form parameter is implementation defined. A null string for Form specifies the use of the default options of the implementation of the new directory. The exception Name_Error is propagated if the string given as New_Directory does not allow the identification of a directory. The exception Use_Error is propagated if the external environment does not support the creation of a directory with the given name (in the absence of Name_Error) and form.

*procedure* Delete_Directory (Directory : *in* String);

{AI05-0231-1} Deletes an existing empty directory with name Directory. The exception Name_Error is propagated if the string given as Directory does not identify an existing directory. The exception Use_Error is propagated if the directory is not empty or the external environment does not support the deletion of the directory (or some portion of its contents) with the given name (in the absence of Name_Error).

*procedure* Create_Path (New_Directory : *in* String;

Form : *in* String := "");

{AI05-0271-1} Creates zero or more directories with name New_Directory. Each nonexistent directory named by New_Directory is created.[ For example, on a typical Unix system, Create_Path("/usr/me/my"); would create directory "me" in directory "usr", then create directory "my" in directory "me".] The Form parameter can be used to give system-dependent characteristics of the directory; the interpretation of the Form parameter is implementation defined. A null string for Form specifies the use of the default options of the implementation of the new directory. The exception Name_Error is propagated if the string given as New_Directory does not allow the identification of any directory. The exception Use_Error is propagated if the external environment does not support the creation of any directories with the given name (in the absence of Name_Error) and form. If Use_Error is propagated, it is unspecified whether a portion of the directory path is created.

*procedure* Delete_Tree (Directory : *in* String);

Deletes an existing directory with name Directory. The directory and all of its contents (possibly including other directories) are deleted. The exception Name_Error is propagated if the string given as Directory does not identify an existing directory. The exception Use_Error is propagated if the external environment does not support the deletion of the directory or some portion of its contents with the given name (in the absence of Name_Error). If Use_Error is propagated, it is unspecified whether a portion of the contents of the directory is deleted.
procedure Delete_File (Name : in String);
  Deletes an existing ordinary or special file with name Name. The exception Name_Error is propagated if the string given as Name does not identify an existing ordinary or special external file. The exception Use_Error is propagated if the external environment does not support the deletion of the file with the given name (in the absence of Name_Error).

procedure Rename (Old_Name, New_Name : in String);
  \{AI05-0231-1\} Renames an existing external file (including directories) with name Old_Name to New_Name. The exception Name_Error is propagated if the string given as Old_Name does not identify an existing external file or if the string given as New_Name does not allow the identification of an external file. The exception Use_Error is propagated if the external environment does not support the renaming of the file with the given name (in the absence of Name_Error). In particular, Use_Error is propagated if a file or directory already exists with name New_Name.

Implementation Note: This operation is expected to work within a single directory, and implementers are encouraged to support it across directories on a single device. Copying files from one device to another is discouraged (that's what Copy_File is for). However, there is no requirement to detect file copying by the target system. If the target system has an API that gives that for “free”, it can be used. For Windows®, for instance, MoveFile can be used to implement Rename.

procedure Copy_File (Source_Name, Target_Name : in String; Form        : in String := "");
  \{AI05-0092-1\} \{AI05-0271-1\} Copies the contents of the existing external file with name Source_Name to an external file with name Target_Name. The resulting external file is a duplicate of the source external file. The Form parameter can be used to give system-dependent characteristics of the resulting external file; the interpretation of the Form parameter is implementation defined. Exception Name_Error is propagated if the string given as Source_Name does not identify an existing external ordinary or special file, or if the string given as Target_Name does not allow the identification of an external file. The exception Use_Error is propagated if the external environment does not support creating the file with the name given by Target_Name and form given by Form, or copying of the file with the name given by Source_Name (in the absence of Name_Error). If Use_Error is propagated, it is unspecified whether a portion of the file is copied.

Ramification: Name_Error is always raised if Source_Name identifies a directory. It is up to the implementation whether special files can be copied, or if Use_Error will be raised.

The following file and directory name operations are provided:

function Full_Name (Name : in String) return String;
  Returns the full name corresponding to the file name specified by Name. The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file (including directories and special files).

Discussion: Full name means that no abbreviations are used in the returned name, and that it is a full specification of the name. Thus, for Unix and Windows®, the result should be a full path that does not contain any "." or ".." directories. Typically, the default directory is used to fill in any missing information.

function Simple_Name (Name : in String) return String;
  \{AI12-0337-1\} \{AI12-0433-1\} Returns the simple name portion of the file name specified by Name. The simple name of a root directory is a name of the root itself. The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file (including directories and special files).
**Discussion**: {AI12-0337-1} The result of Simple_Name corresponds to the result of the “basename” command on Linux and Unix. If the filename ends with a ‘/’, and is not a root, then “basename” returns the part in front of all of the trailing ‘/’s. It returns a root intact. The null string is never returned. Similar rules should be used for Windows filenames.

**function** Containing_Directory (Name : in String) return String;

Returns the name of the containing directory of the external file (including directories) identified by Name. (If more than one directory can contain Name, the directory name returned is implementation defined.) The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file. The exception Use_Error is propagated if the external file does not have a containing directory.

**Discussion**: This is purely a string manipulation function. If Name is not given as a full name, the containing directory probably won’t be one, either. For example, if Containing_Directory ("C:\AARM\RM-A-8") is called on Windows®, the result should be "C:\AARM". If there is no path at all on the name, the result should be ",," (which represents the current directory). Use Full_Name on the result of Containing_Directory if the full name is needed.

**Ramification**: {AI12-0337-1} Containing_Directory raises Use_Error when passed a string representing a root directory.

**function** Extension (Name : in String) return String;

Returns the extension name corresponding to Name. The extension name is a portion of a simple name (not including any separator characters), typically used to identify the file class. If the external environment does not have extension names, then the null string is returned. The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file.

**Discussion**: For Unix and Windows®, the extension is the portion of the simple name following the rightmost period. For example, in the simple name "RM-A-8.html", the extension is "html".

**function** Base_Name (Name : in String) return String;

Returns the base name corresponding to Name. The base name is the remainder of a simple name after removing any extension and extension separators. The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file (including directories and special files).

**Discussion**: For Unix and Windows®, the base name is the portion of the simple name preceding the rightmost period (except for the special directory names ",," and ",," whose Base_Name is ",," and ",,"). For example, in the simple name "RM-A-8.html", the base name is "RM-A-8".

**function** Compose (Containing_Directory : in String := "";

Name : in String;

Extension : in String := "") return String;

{AI05-0264-1} {AI12-0337-1} Returns the name of the external file with the specified Containing_Directory, Name, and Extension. If Extension is the null string, then Name is interpreted as a simple name; otherwise, Name is interpreted as a base name. The exception Name_Error is propagated if the string given as Containing_Directory is not null and does not allow the identification of a directory, or if the string given as Extension is not null and is not a possible extension, or if the string given as Name is not a possible simple name (if Extension is null) or base name (if Extension is nonnull).

- the string given as Containing_Directory is not null and does not allow the identification of a directory;
- the string given as Extension is not null and is not a possible extension;
- the string given as Name is not a possible simple name (if Extension is null) or base name (if Extension is nonnull); or
the string given as Name is a root directory, and Containing Directory or Extension is nonnull.

Ramification: The above definition implies that if the Extension is null, for Unix and Windows® no '.' is added to Name.

Discussion: If Name is null, Name_Error should be raised, as nothing is not a possible simple name or base name.

Generally, Compose(Containing Directory(F), Base_Name(F), Extension(F)) = F. However, this is not true on Unix or Windows® for file names that end with a ':', Compose(Base_Name("Fooey."), Extension("Fooey.")) = "Fooey". This is not a problem for Windows®, as the names have the same meaning with or without the '.'; but these are different names for Unix. Thus, care needs to be taken on Unix; if Extension is null, Base_Name should be avoided. (That's not usually a problem with file names generated by a program.)

function Name_Case_Equivalence (Name : in String) return Name_Case_Kind;

Returns the file name equivalence rule for the directory containing Name. Raises Name_Error if Name is not a full name. Returns Case_Sensitive if file names that differ only in the case of letters are considered different names. If file names that differ only in the case of letters are considered the same name, then Case_Preserving is returned if names have the case of the file name used when a file is created; and Case_Insensitive is returned otherwise. Returns Unknown if the file name equivalence is not known.

Implementation Note: Unix, Linux, and their relatives are Case_Sensitive systems. Microsoft® Windows® is a Case_Preserving system (unless the rarely used POSIX mode is used). Ancient systems like CP/M and early MS-DOS were Case_Insensitive systems (file names were always in UPPER CASE). Unknown is provided in case it is impossible to tell (such as could be the case for network files).

type File_Kind is (Directory, Ordinary_File, Special_File);

The type File_Kind represents the kind of file represented by an external file or directory.

type File_Size is range 0 .. implementation-defined;

The type File_Size represents the size of an external file.

Implementation defined: The maximum value for a file size in Directories.

function Exists (Name : in String) return Boolean;

Returns True if an external file represented by Name exists, and False otherwise. The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file (including directories and special files).

function Kind (Name : in String) return File_Kind;

Returns the kind of external file represented by Name. The exception Name_Error is propagated if the string given as Name does not allow the identification of an existing external file.

function Size (Name : in String) return File_Size;

Returns the size of the external file represented by Name. The size of an external file is the number of stream elements contained in the file. If the external file is not an ordinary file, the result is implementation defined. The exception Name_Error is propagated if the string given as Name does not allow the identification of an existing external file. The exception Constraint_Error is propagated if the file size is not a value of type File_Size.

Implementation defined: The result for Directories.Size for a directory or special file.

Discussion: We allow raising Constraint_Error, so that an implementation for a system with 64-bit file sizes does not need to support full numerics on 64-bit integers just to implement this package. Of course, if 64-bit integers are available on such a system, they should be used when defining type File_Size.
function Modification_Time (Name : in String) return Ada.Calendar.Time;

Returns the time that the external file represented by Name was most recently modified. If the external file is not an ordinary file, the result is implementation defined. The exception Name_Error is propagated if the string given as Name does not allow the identification of an existing external file. The exception Use_Error is propagated if the external environment does not support reading the modification time of the file with the name given by Name (in the absence of Name_Error).

Implementation defined: The result for Directories.Modification_Time for a directory or special file.

{AI95-00248-01} The following directory searching operations and types are provided:

type Directory_Entry_Type is limited private;

The type Directory_Entry_Type represents a single item in a directory. These items can only be created by the Get_Next_Entry procedure in this package. Information about the item can be obtained from the functions declared in this package. A default-initialized object of this type is invalid; objects returned from Get_Next_Entry are valid.

type Filter_Type is array (File_Kind) of Boolean;

The type Filter_Type specifies which directory entries are provided from a search operation. If the Directory component is True, directory entries representing directories are provided. If the Ordinary_File component is True, directory entries representing ordinary files are provided. If the Special_File component is True, directory entries representing special files are provided.

type Search_Type is limited private;

The type Search_Type contains the state of a directory search. A default-initialized Search_Type object has no entries available (function More Entries returns False). Type Search_Type needs finalization (see 7.6).

procedure Start_Search (Search    : in out Search_Type;
                         Directory : in String;
                         Pattern   : in String;
                         Filter    : in Filter_Type := (others => True));

{AI05-0092-1} {AI05-0262-1} Starts a search in the directory named by Directory for entries matching Pattern and Filter. Pattern represents a pattern for matching file names. If Pattern is the null string, all items in the directory are matched; otherwise, the interpretation of Pattern is implementation defined. Only items that match Filter will be returned. After a successful call on Start_Search, the object Search may have entries available, but it may have no entries available if no files or directories match Pattern and Filter. The exception Name_Error is propagated if the string given by Directory does not identify an existing directory, or if Pattern does not allow the identification of any possible external file or directory. The exception Use_Error is propagated if the external environment does not support the searching of the directory with the given name (in the absence of Name_Error). When Start_Search propagates Name_Error or Use_Error, the object Search will have no entries available.

Implementation defined: The interpretation of a nonnull search pattern in Directories.

procedure End_Search (Search : in out Search_Type);

Ends the search represented by Search. After a successful call on End_Search, the object Search will have no entries available.

Ramification: The only way that a call to End_Search could be unsuccessful if Device_Error (see A.13) is raised because of an underlying failure (or bug).
function More_Entries (Search : in Search_Type) return Boolean;

Returns True if more entries are available to be returned by a call to Get_Next_Entry for the specified search object, and False otherwise.

procedure Get_Next_Entry (Search : in out Search_Type; Directory_Entry : out Directory_Entry_Type);

{AI05-0262-1} Returns the next Directory_Entry for the search described by Search that matches the pattern and filter. If no further matches are available, Status_Error is raised. It is implementation defined as to whether the results returned by this subprogram routine are altered if the contents of the directory are altered while the Search object is valid (for example, by another program). The exception Use_Error is propagated if the external environment does not support continued searching of the directory represented by Search.

Implementation defined: The results of a Directories search if the contents of the directory are altered while a search is in progress.

{AI12-0286-1} procedure Search (Directory : in String; Pattern : in String; Filter : in Filter_Type := (others => True); Process : not null access procedure (Directory_Entry : in Directory_Entry_Type) with Allows Exit);

{AI05-0092-1} {AI05-0262-1} Searches in the directory named by Directory for entries matching Pattern and Filter. The subprogram designated by Process is called with each matching entry in turn. Pattern represents a pattern for matching file names. If Pattern is the null string, all items in the directory are matched; otherwise, the interpretation of Pattern is implementation defined. Only items that match Filter will be returned. The exception Name_Error is propagated if the string given by Directory does not identify an existing directory, or if Pattern does not allow the identification of any possible external file or directory. The exception Use_Error is propagated if the external environment does not support the searching of the directory with the given name (in the absence of Name_Error).

Discussion: “In turn” means that the calls to the subprogram designated by Process are not made in parallel; they can be made in any order but must be in sequence.

function Simple_Name (Directory_Entry : in Directory_Entry_Type) return String;

Returns the simple external name of the external file (including directories) represented by Directory_Entry. The format of the name returned is implementation defined. The exception Status_Error is propagated if Directory_Entry is invalid.

function Full_Name (Directory_Entry : in Directory_Entry_Type) return String;

Returns the full external name of the external file (including directories) represented by Directory_Entry. The format of the name returned is implementation defined. The exception Status_Error is propagated if Directory_Entry is invalid.

function Kind (Directory_Entry : in Directory_Entry_Type) return File_Kind;

Returns the kind of external file represented by Directory_Entry. The exception Status_Error is propagated if Directory_Entry is invalid.
function Size (Directory_Entry : in Directory_Entry_Type)
    return File_Size;

Returns the size of the external file represented by Directory_Entry. The size of an external file is
the number of stream elements contained in the file. If the external file represented by
Directory_Entry is not an ordinary file, the result is implementation defined. The exception
Status_Error is propagated if Directory_Entry is invalid. The exception Constraint_Error is
propagated if the file size is not a value of type File_Size.

function Modification_Time (Directory_Entry : in Directory_Entry_Type)
    return Ada.Calendar.Time;

Returns the time that the external file represented by Directory_Entry was most recently
modified. If the external file represented by Directory_Entry is not an ordinary file, the result is
implementation defined. The exception Status_Error is propagated if Directory_Entry is invalid.
The exception Use_Error is propagated if the external environment does not support reading the
modification time of the file represented by Directory_Entry.

Implementation Requirements

For Copy_File, if Source_Name identifies an existing external ordinary file created by a predefined Ada
input-output package, and Target_Name and Form can be used in the Create operation of that input-
output package with mode Out_File without raising an exception, then Copy_File shall not propagate
Use_Error.

Discussion: This means that Copy_File will copy any file that the Ada programmer could copy (by writing some
possibly complicated Ada code).

Implementation Advice

If other information about a file (such as the owner or creation date) is available in a directory entry, the
implementation should provide functions in a child package Directories.Information to retrieve it.

Implementation Advice: Package Directories.Information should be provided to retrieve other information about a
file.

Implementation Note: For Windows®, Directories.Information should contain at least the following routines:

```ada
{AI12-0302-1} package Ada.Directories.Information
    with Global => in out synchronized is
      -- System-specific directory information.
      -- Version for the Microsoft® Windows® operating system.
      function Creation_Time (Name : in String) return Ada.Calendar.Time;
      function Last_Access_Time (Name : in String) return Ada.Calendar.Time;
      function Is_Read_Only (Name : in String) return Boolean;
      function Needs_Archiving (Name : in String) return Boolean;
      -- This generally means that the file needs to be backed up.
      -- The flag is only cleared by backup programs.
      function Is_Compressed (Name : in String) return Boolean;
      function Is_Encrypted (Name : in String) return Boolean;
      function Is_Hidden (Name : in String) return Boolean;
      function Is_System (Name : in String) return Boolean;
      function Is_Offline (Name : in String) return Boolean;
      function Is_Temporary (Name : in String) return Boolean;
      function Is_Sparse (Name : in String) return Boolean;
      function Is_Not_Indexed (Name : in String) return Boolean;
      function Creation_Time (Directory_Entry : in Directory_Entry_Type)
        return Ada.Calendar.Time;
      function Last_Access_Time (Directory_Entry : in Directory_Entry_Type)
        return Ada.Calendar.Time;
```


function Is_Read_Only (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Needs_Archiving (Directory_Entry : in Directory_Entry_Type) return Boolean;
-- This generally means that the file needs to be backed up.
-- The flag is only cleared by backup programs.
function Is_Compressed (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Is_Encrypted (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Is_Hidden (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Is_System (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Is_Offline (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Is_Sparse (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Is_Not_Indexed (Directory_Entry : in Directory_Entry_Type) return Boolean;

end Ada.Directories.Information;

For Unix-like systems (Unix, POSIX, Linux, etc.), Directories.Information should contain at least the following routines:

package Ada.Directories.Information
  with Global => in out synchronized is
  -- System-specific directory information.
  -- Unix and similar systems version.
  function Last_Access_Time (Name : in String) return Ada.Calendar.Time;
  function Last_Status_Change_Time (Name : in String) return Ada.Calendar.Time;
  type Permission is
    Others_Execute, Others_Write, Others_Read,
    Group_Execute, Group_Write, Group_Read,
    Owner_Execute, Owner_Write, Owner_Read,
    Set_Group_ID, Set_User_ID;
  type Permission_Set_Type is array (Permission) of Boolean;
  function Permission_Set (Name : in String) return Permission_Set_Type;
  function Owner (Name : in String) return String;
  -- Returns the image of the User_Id. If a definition of User_Id
  -- is available, an implementation-defined version of Owner
  -- returning User_Id should also be defined.
  function Group (Name : in String) return String;
  -- Returns the image of the Group_Id. If a definition of Group_Id
  -- is available, an implementation-defined version of Group
  -- returning Group_Id should also be defined.
  function Is_Block_Special_File (Name : in String) return Boolean;
  function Is_Character_Special_File (Name : in String) return Boolean;
  function Is_FIFO (Name : in String) return Boolean;
  function Is_Symbolic_Link (Name : in String) return Boolean;
  function Is_Socket (Name : in String) return Boolean;
  function Last_Access_Time (Directory_Entry : in Directory_Entry_Type) return Ada.Calendar.Time;
  function Last_Status_Change_Time (Directory_Entry : in Directory_Entry_Type) return Ada.Calendar.Time;
  function Permission_Set (Directory_Entry : in Directory_Entry_Type) return Permission_Set_Type;
  function Owner (Directory_Entry : in Directory_Entry_Type) return String;
  -- See Owner above.
  function Group (Directory_Entry : in Directory_Entry_Type) return String;
  -- See Group above.
  function Is_Block_Special_File (Directory_Entry : in Directory_Entry_Type) return Boolean;
  function Is_Character_Special_File (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Is_Symbolic_Link (Directory_Entry : in Directory_Entry_Type) return Boolean;
function Is_Socket (Directory_Entry : in Directory_Entry_Type) return Boolean;
-- Additional implementation-defined subprograms allowed here.
end Ada.Directories.Information;

We give these definitions to give guidance so that every implementation for a given target is not unnecessarily different. Implementers are encouraged to make packages for other targets as similar to these as possible.

{AI05-0231-1} {AI12-0439-1} Start Search and Search should raise Name_Error Use_Error if Pattern is malformed, but not if it can could represent a file in the directory but does not actually do so.

Implementation Advice: Directories.Start Search and Directories.Search should raise Name_Error Use_Error for malformed patterns.

Rename should be supported at least when both New_Name and Old_Name are simple names and New_Name does not identify an existing external file.

Implementation Advice: Directories.Rename should be supported at least when both New_Name and Old_Name are simple names and New_Name does not identify an existing external file.

Discussion: “Supported” includes raising an exception if either name is malformed, the file to rename doesn’t exist, insufficient permission for the operation exists, or similar problems. But this advice requires implementations to document what they do, and tells implementers that simply raising Use_Error isn't acceptable.

NOTE 1 {AI12-0442-1} The operations Containing Directory, Full_Name, Simple_Name, Base_Name, Extension, and Compose operate on file names, not external files. The files identified by these operations do not necessarily need to exist. Name_Error is raised only if the file name is malformed and cannot possibly identify a file. Of these operations, only the result of Full_Name depends on the current default directory; the result of the others depends only on their parameters.

NOTE 2 Using access types, values of Search_Type and Directory_Entry_Type can be saved and queried later. However, another task or application can modify or delete the file represented by a Directory_Entry_Type value or the directory represented by a Search_Type value; such a value can only give the information valid at the time it is created. Therefore, long-term storage of these values is not recommended.

NOTE 3 If the target system does not support directories inside of directories, then Kind will never return Directory and Containing.Directory will always raise Use_Error.

NOTE 4 If the target system does not support creation or deletion of directories, then Create_Directory, Create_Path, Delete_Directory, and Delete_Tree will always propagate Use_Error.

NOTE 5 {AI12-0442-1} {AI12-0447-1} To move a file or directory to a different location, use Rename. Most target systems will allow renaming of files from one directory to another. If the target file or directory can might already exist, it should be deleted first.

Discussion: While Rename is only guaranteed to work for name changes within a single directory, it's unlikely that implementers would purposely prevent functionality present in the underlying system from working. To move a file totally portably, it's necessary to handle failure of the Rename and fall back to Copy_File and Delete:

begin
____ Rename (Source, Target);
exception
____ when Use_Error =>
_____ Copy_File (Source, Target);
_____ Delete (Source);
end;

Extensions to Ada 95

{AI95-00248-01} Package Ada.Directories is new.

Inconsistencies With Ada 2005

{AI05-0231-1} Correction: Clarified when and which exceptions are raised for Start Search, Search, Delete_Directory, and Rename. If an implementation followed the original incorrect wording, it might raise Use_Error instead of Name_Error for Start Search and Search, Name_Error instead of Use_Error for Rename, and might have deleted a nonempty directory instead of raising Use_Error for Delete_Directory. The first two cases are very unlikely to matter in practice, and it’s unlikely that an implementation would have followed the latter implementation strategy, as it would be more work and would make Delete_Directory identical to Delete_Tree (which is obvious nonsense).
Incompatibilities With Ada 2005

{AI05-0049-1} A new enumeration type Name_Case_KIND and a new function Name_Case_Equivalence is added to Directories. If Directories is referenced in a use_clause, and an entity E with a defining identifier of one of the new entities is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Wording Changes from Ada 2005

{AI05-0271-1} Correction: We now explicitly say that the behavior of Create_Path and Copy_File is unspecified when Use_Error is raised. Nothing has changed here, as the behavior was (implicitly) unspecified in the 2007 Amendment.

Wording Changes from Ada 2012

{AI12-0337-1} {AI12-0433-1} Correction: Clarified the meaning of Simple_Name in the case that the parameter is a root directory. This was not previously described.

A.16.1 The Package Directories.Hierarchical_File_Names

{AI05-0049-1} The library package Directories.Hierarchical_File_Names is an optional package providing operations for file name construction and decomposition for targets with hierarchical file naming.

Static Semantics

{AI05-0049-1} If provided, the library package Directories.Hierarchical_File_Names has the following declaration:

```
{AI12-0241-1} {AI12-0302-1} package Ada.Directories.Hierarchical_File_Names
with Nonblocking, Global => in out synchronized is

function Is_Simple_Name (Name : in String) return Boolean;

function Is_Root_Directory_Name (Name : in String) return Boolean;

function Is_Parent_Directory_Name (Name : in String) return Boolean;

function Is_Current_Directory_Name (Name : in String) return Boolean;

function Is_Full_Name (Name : in String) return Boolean;

function Is_Relative_Name (Name : in String) return Boolean;

function Simple_Name (Name : in String) return String
renames Ada.Directories.Simple_Name;

function Containing_Directory (Name : in String) return String
renames Ada.Directories.Containing_Directory;

function Initial_Directory (Name : in String) return String;

function Relative_Name (Name : in String) return String;

function Compose (Directory      : in String := "");
Relative_Name : in String;
Extension      : in String := ")" return String;

end Ada.Directories.Hierarchical_File_Names;
```

{AI05-0049-1} {AI05-0269-1} In addition to the operations provided in package Directories.Hierarchical_File_Names, the operations in package Directories can be used with hierarchical file names. In particular, functions Full_Name, Base_Name, and Extension provide additional capabilities for hierarchical file names.

Function Is_Simple_Name (Name : in String) return Boolean;

Returns True if Name is a simple name, and returns False otherwise.

Ramification: {AI12-0337-1} Root directories are considered simple names, so this function will return True if Name represents a root. Use Is_Root_Directory if it is necessary to distinguish roots and other simple names.
function Is_Root_Directory_Name (Name : in String) return Boolean;
Returns True if Name is syntactically a root (a directory that cannot be decomposed further), and returns False otherwise.

Implementation Note: {AI12-0337-1} For Unix and Unix-like systems, "/" is the root. For Windows®, "C:" and "\Computer\Share" are roots.

function Is_Parent_Directory_Name (Name : in String) return Boolean;
Returns True if Name can be used to indicate symbolically the parent directory of any directory, and returns False otherwise.

Implementation Note: Is Parent Directory Name returns True if and only if Name is ". .." for both Unix and Windows®.

function Is_Current_Directory_Name (Name : in String) return Boolean;
Returns True if Name can be used to indicate symbolically the directory itself for any directory, and returns False otherwise.

Implementation Note: Is Current Directory Name returns True if and only if Name is ". ." for both Unix and Windows®.

function Is_Full_Name (Name : in String) return Boolean;
Returns True if the leftmost directory part of Name is a root, and returns False otherwise.

function Is_Relative_Name (Name : in String) return Boolean;
{AI05-0049-1} {AI105-0269-1} Returns True if Name allows the identification of an external file (including directories and special files) but is not a full name, and returns False otherwise.

Ramification: {AI05-0049-1} Relative names include simple names other than root directories as a special case. This function returns False if the syntax of the name is incorrect.

function Initial_Directory (Name : in String) return String;
{AI05-0049-1} {AI05-0248-1} Returns the leftmost directory part in Name. [That is, it returns a root directory name (for a full name), or one of a parent directory name, a current directory name, or a simple name (for a relative name).] The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file (including directories and special files).

function Relative_Name (Name : in String) return String;
Returns the entire file name except the Initial_Directory portion. The exception Name_Error is propagated if the string given as Name does not allow the identification of an external file (including directories and special files), or if Name has a single part (this includes if any of Is_Simple_Name, Is_Root_Directory_Name, Is_Parent_Directory_Name, or Is_Current_Directory_Name are True).

Ramification: The result might be a simple name.

function Compose (Directory      : in String := "");
Relative_Name  : in String;
Extension      : in String := ") return String;
Returns the name of the external file with the specified Directory, Relative_Name, and Extension. The exception Name_Error is propagated if the string given as Directory is not the null string and does not allow the identification of a directory, or if Is_Relative_Name (Relative_Name) is False, or if the string given as Extension is not the null string and is not a possible extension, or if Extension is not the null string and Simple_Name (Relative_Name) is not a base name.

The result of Compose is a full name if Is_Full_Name (Directory) is True; result is a relative name otherwise.
Ramification: Name_Error is raised by Compose if Directory is not the null string, and both Is_Full_Name and Is_Relative_Name return False.

Discussion: A common security problem is to include a parent directory name in the middle of a file name; this is often used to navigate outside of an intended root directory. We considered attempting to prevent that case by having Compose detect it and raise an exception. But the extra rules necessary were more confusing than helpful.

{AI12-0337-1} We can say more about the details of these operations by adopting the notation of a subscript to specify how many path fragments a particular result has. Then, we can abbreviate "Full Name" as "Full" and "Relative Name" as "Rel". In this notation, Unix file name "a/b" is a Rel(2), ".//c/d" is a Rel(3), and "/a/b" is a Full(2). Rel(1) is equivalent to a simple name that is not a root; thus we don't have to describe that separately.

In this notation,

For N>1,

\[ \text{Containing Directory}(\text{Rel}(N)) = \text{Leftmost } \text{Rel}(N-1), \]
\[ \text{Containing Directory}(\text{Full}(N)) = \text{Leftmost } \text{Full}(N-1), \]
Else if N = 1, raise Use_Error Name_Error.

Similarly,

For N>1,

\[ \text{Relative Name}(\text{Rel}(N)) = \text{Rightmost } \text{Rel}(N-1), \]
\[ \text{Relative Name}(\text{Full}(N)) = \text{Rightmost } \text{Full}(N-1), \]
Else if N = 1, raise Name_Error.

Finally, for Compose (ignoring the extension here):

For N>1,

\[ \text{Compose }((\text{Directory} \Rightarrow \text{Full}(N), \text{Relative Name} \Rightarrow \text{Rel}(M)) \Rightarrow \text{Full}(N+M) \]
\[ \text{Compose }((\text{Directory} \Rightarrow \text{Rel}(N), \text{Relative Name} \Rightarrow \text{Rel}(M)) \Rightarrow \text{Rel}(N+M) \]
Name_Error if Relative_Name is a Full(M).

We didn't try to write wording to reflect these details of these functions.

Implementation Advice

Directories.Hierarchical_File_Names should be provided for systems with hierarchical file naming, and should not be provided on other systems.

Implementation Advice: Directories.Hierarchical_File_Names should be provided for systems with hierarchical file naming, and should not be provided on other systems.

Implementation Note: This package should be provided when targeting Microsoft® Windows®, Unix, Linux, and most Unix-like systems.

NOTE 1 {AI05-0049-1} {AI12-0442-1} These operations operate on file names, not external files. The files identified by these operations do not necessarily need to exist. Name_Error is raised only as specified or if the file name is malformed and cannot possibly identify a file. The result of these operations depends only on their parameters.

NOTE 2 {AI05-0049-1} Containing_Directory raises Use_Error if Name does not have a containing directory, including when any of Is_Simple_Name, Is_Root_Directory_Name, Is_Parent_Directory_Name, or Is_Current_Directory_Name are True.

Ramification: In particular, the default directory is not used to find the containing directory either when Is_Parent_Directory_Name or Is_Current_Directory_Name is True. As noted above, these functions operate purely on the syntax of the file names and do not attempt to interpret them. If interpretation is needed, Directories.Full_Name can be to expand any shorthands used before calling Containing_Directory.

Extensions to Ada 2005

A.16.2 The Packages Wide_Directories and Wide_Wide_Directories

The packages Wide_Directories and Wide_Wide_Directories provide operations for manipulating files and directories, and their names.
Static Semantics

\{AI12-0021-1\} The specification of package \texttt{Wide_Directories} is the same as for \texttt{Directories} (including its optional child packages \texttt{Information} and \texttt{Hierarchical_File_Names}), except that each occurrence of \texttt{String} is replaced by \texttt{Wide_String}.

\{AI12-0021-1\} The specification of package \texttt{Wide_Wide_Directories} is the same as for \texttt{Directories} (including its optional child packages \texttt{Information} and \texttt{Hierarchical_File_Names}), except that each occurrence of \texttt{String} is replaced by \texttt{Wide_Wide_String}.

Extensions to Ada 2012

\{AI12-0021-1\} These six packages are new.

A.17 \textbf{The Package Environment Variables}

\{AI95-00370-01\} The package Environment Variables allows a program to read or modify environment variables. Environment variables are name-value pairs, where both the name and value are strings. The definition of what constitutes an environment variable, and the meaning of the name and value, are implementation defined.

\textbf{Implementation defined:} The definition and meaning of an environment variable.

Static Semantics

\{AI95-00370-01\} The library package Environment Variables has the following declaration:

\{AI12-0241-1\} \{AI12-0302-1\} \texttt{package Ada.Environment_Variables is}
\begin{verbatim}
  withpragma Prelaborate, Nonblocking, Global => in out synchronized
  is [Environment_Variables];
  function Value (Name : in String) return String;
  function Value (Name : in String; Default : in String) return String;
  function Exists (Name : in String) return Boolean;
  procedure Set (Name : in String; Value : in String);
  procedure Clear (Name : in String);
  procedure Clear;
  procedure Iterate (Process : not null access procedure
                     (Name, Value : in String)) with Allows_Exit;
end Ada.Environment_Variables;
\end{verbatim}

\texttt{function Value (Name : in String) return String;}

\{AI95-00370-01\} If the external execution environment supports environment variables, then Value returns the value of the environment variable with the given name. If no environment variable with the given name exists, then Constraint_Error is propagated. If the execution environment does not support environment variables, then Program_Error is propagated.

\texttt{function Value (Name : in String; Default : in String) return String;}

\{AI05-0285-1\} If the external execution environment supports environment variables and an environment variable with the given name currently exists, then Value returns its value; otherwise, it returns Default.
function Exists (Name : in String) return Boolean;

{A195-00370-01} {AI05-0264-1} If the external execution environment supports environment variables and an environment variable with the given name currently exists, then Exists returns True; otherwise, it returns False.

procedure Set (Name : in String; Value : in String);

{A195-00370-01} {AI05-0264-1} If the external execution environment supports environment variables, then Set first clears any existing environment variable with the given name, and then defines a single new environment variable with the given name and value. Otherwise, Program_Error is propagated.

If implementation-defined circumstances prohibit the definition of an environment variable with the given name and value, then Constraint_Error is propagated.

Implementation defined: The circumstances where an environment variable cannot be defined.

It is implementation defined whether there exist values for which the call Set(Name, Value) has the same effect as Clear (Name).

Implementation defined: Environment names for which Set has the effect of Clear.

procedure Clear (Name : in String);

{A195-00370-01} {AI05-0264-1} {AI05-0269-1} If the external execution environment supports environment variables, then Clear deletes all existing environment variables with the given name. Otherwise, Program_Error is propagated.

procedure Clear;

{A195-00370-01} {AI05-0264-1} If the external execution environment supports environment variables, then Clear deletes all existing environment variables. Otherwise, Program_Error is propagated.

{AI05-0248-1} {AI12-0286-1} procedure Iterate with Allows Exit;

{A195-00370-01} {AI05-0264-1} If the external execution environment supports environment variables, then Iterate calls the subprogram designated by Process for each existing environment variable, passing the name and value of that environment variable. Otherwise, Program_Error is propagated.

If several environment variables exist that have the same name, Process is called once for each such variable.

Bounded (Run-Time) Errors

{A195-00370-01} It is a bounded error to call Value if more than one environment variable exists with the given name; the possible outcomes are that:

• one of the values is returned, and that same value is returned in subsequent calls in the absence of changes to the environment; or

• Program_Error is propagated.

Erroneous Execution

{A195-00370-01} Making calls to the procedures Set or Clear concurrently with calls to any subprogram of package Environment_Variables, or to any instantiation of Iterate, results in erroneous execution.
Making calls to the procedures Set or Clear in the actual subprogram corresponding to the Process parameter of Iterate results in erroneous execution.

Documentation Requirements

\{AI95-00370-01\} An implementation shall document how the operations of this package behave if environment variables are changed by external mechanisms (for instance, calling operating system services).

**Documentation Requirement:** The behavior of package Environment Variables when environment variables are changed by external mechanisms.

Implementation Permissions

\{AI95-00370-01\} An implementation running on a system that does not support environment variables is permitted to define the operations of package Environment Variables with the semantics corresponding to the case where the external execution environment does support environment variables. In this case, it shall provide a mechanism to initialize a nonempty set of environment variables prior to the execution of a partition.

Implementation Advice

\{AI95-00370-01\} If the execution environment supports subprocesses, the currently defined environment variables should be used to initialize the environment variables of a subprocess.

**Implementation Advice:** If the execution environment supports subprocesses, the current environment variables should be used to initialize the environment variables of a subprocess.

Changes to the environment variables made outside the control of this package should be reflected immediately in the effect of the operations of this package. Changes to the environment variables made using this package should be reflected immediately in the external execution environment. This package should not perform any buffering of the environment variables.

**Implementation Advice:** Changes to the environment variables made outside the control of Environment Variables should be reflected immediately.

Extensions to Ada 95

\{AI95-00370-01\} Package Environment Variables is new.

Incompatibilities With Ada 2005

\{AI05-0285-1\} A new overloaded function Value is added to Environment Variables. If Environment Variables is referenced in a use clause, and an entity E with the name Value is defined in a package that is also referenced in a use clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

**A.17.1 The Packages Wide Environment Variables and Wide Wide Environment Variables**

\{AI12-0021-1\} The packages Wide Environment Variables and Wide Wide Environment Variables allow a program to read or modify environment variables.

Static Semantics

\{AI12-0021-1\} The specification of package Wide Environment Variables is the same as for Environment Variables, except that each occurrence of String is replaced by Wide String.

\{AI12-0021-1\} The specification of package Wide Wide Environment Variables is the same as for Environment Variables, except that each occurrence of String is replaced by Wide Wide String.
A.17 Containers

These packages are new.

A.18 Containers

This clause presents the specifications of the package Containers and several child packages, which provide facilities for storing collections of elements.

Term entry: container — structured object that represents a collection of elements all of the same (potentially class-wide) type, such as a vector or a tree

Note: Several predefined container types are provided by the children of package Ada.Containers (see A.18.1).

A variety of sequence and associative containers are provided. Each container package defines includes a cursor type as well as a container type. A cursor is a reference to an element within a container. Many operations on cursors are common to all of the containers. A cursor referencing an element in a container is considered to be overlapping only with the element container object itself.

Reason: The last sentence is intended to clarify that operations that just use a cursor do not interfere if the cursor objects designated different elements of the containers on the same footing as operations that use a container in terms of the concurrent callreentrancy rules of Annex A.

Ramification: A cursor is not considered to overlap with other elements of the associated container, thus parallel operations involving a set of cursors each operating on mutually exclusive sets of elements from the same container are expected to work.

Discussion: We use the term "container" alone when it is clear from context what kind of entity (package, type, or object) that we are talking about. Otherwise, we use "container package", "container type", or "container object". Note that "container type" is defined in 4.3.5 for a different usage; in all of A.18 we mean "container type" to be one of the primary types declared in the child packages of package Containers, such as Vector, List, or Map.

Some operations of the language-defined child units of Ada.Containers have access-to-subprogram parameters. To ensure such operations are well-defined, they guard against certain actions by the designated subprogram. An action on a container that can add or remove an element is considered to tamper with cursors, and these are prohibited during all such operations. An action on a container that can replace an element with one of a different size is considered to tamper with elements, and these are prohibited during certain of such operations. The details of the specific actions that are considered to tamper with cursors or elements are defined for each child unit of Ada.Containers.

Several of the language-defined child units of Ada.Containers include a nested package named Stable, which provides a view of a container that prohibits any operations that would tamper with elements. By using a Stable view for manipulating a container, the number of tampering checks performed while performing the operations can be reduced. The details of the Stable subpackage are defined separately for each child unit of Ada.Containers that includes such a nested package.

Within this clause we provide Implementation Advice for the desired average or worst case time complexity of certain operations on a container. This advice is expressed using the Landau symbol $O(X)$. Presuming $f$ is some function of a length parameter $N$ and $t(N)$ is the time the operation takes (on average or worst case, as specified) for the length $N$, a complexity of $O(f(N))$ means that there exists a finite $A$ such that for any $N$, $t(N)/f(N) < A$.

Discussion: Of course, an implementation can do better than a specified $O(f(N))$: for example, $O(1)$ meets the requirements for $O(\log N)$.

This concept seems to have as many names as there are authors. We used “Landau symbol” because that’s what our reference does. But we’d also seen this referred as big-O notation (sometimes written as big-oh), and as Bachmann notation. Whatever the name, it always has the above definition.
If the advice suggests that the complexity should be less than $O(f(N))$, then for any arbitrarily small positive real $D$, there should exist a positive integer $M$ such that for all $N > M$, $t(N)/f(N) < D$.

{AI05-0001-1} {AI05-0044-1} {AI12-0416-1} When a formal function is used to provide an ordering for a container, it is generally required to define a strict weak ordering. A function "$<" defines a strict weak ordering if it is irreflexive, asymmetric, transitive, and in addition, if $x < y$ for any values $x$ and $y$, then for all other values $z$, $(x < z)$ or $(z < y)$. Elements are in a smallest first order using such an operator if, for every element $y$ with a predecessor $x$ in the order, $(y < x)$ is false.

**Reason:** {AI12-0416-1} A given "$<" operator that provides a strict weak ordering, knowing that $(y < x)$ is false is enough to know that $(x <= y)$ is true. For a strict weak ordering, $(x = y)$ when both $(x < y)$ and $(y < x)$ are false. Therefore, it is not necessary to use the "$<=" operator or test $(x < y)$. We only need to discuss adjacent elements since a strict weak ordering is transitive.

Language Design Principles

{AI95-00302-03} {AI05-0299-1} This subclause provides a number of useful containers for Ada. Only the most useful containers are provided. Ones that are relatively easy to code, redundant, or rarely used are omitted from this set, even if they are generally included in containers libraries.

The containers packages are modeled on the Standard Template Library (STL), an algorithms and data structure library popularized by Alexander Stepanov, and included in the C++ standard library. The structure and terminology differ from the STL where that better maps to common Ada usage. For instance, what the STL calls "iterators" are called "cursors" here.

The following major nonlimited containers are provided:

- (Expandable) Vectors of any nonlimited type;
- Doubly-linked Lists of any nonlimited type;
- Hashed Maps keyed by any nonlimited hashable type, and containing any nonlimited type;
- Ordered Maps keyed by any nonlimited ordered type, and containing any nonlimited type;
- {AI05-0136-1} Hashed Sets of any nonlimited hashable type;
- {AI05-0136-1} Ordered Sets of any nonlimited ordered type;
- {AI05-0136-1} Multiway Trees of any nonlimited type;
- {AI05-0069-1} Holders of any (indefinite) nonlimited type;
- {AI05-0159-1} Synchronized queues of any definite nonlimited type; and
- {AI05-0159-1} Priority queues of any definite nonlimited type.

{AI05-0001-1} Separate versions for definite and indefinite element types are provided, as those for definite types can be implemented more efficiently. Similarly, a separate bounded version is provided in order to give more predictable memory usage.

Each container includes a cursor, which is a reference to an element within a container. Cursors generally remain valid as long as the container exists and the element referenced is not deleted. Many operations on cursors are common to all of the containers. This makes it possible to write generic algorithms that work on any kind of container.

The containers packages are structured so that additional packages can be added in the future. Indeed, we hope that these packages provide the basis for a more extensive secondary standard for containers.

If containers with similar functionality (but different performance characteristics) are provided (by the implementation or by a secondary standard), we suggest that a prefix be used to identify the class of the functionality: "Ada.Containers.Bounded Sets" (for a set with a maximum number of elements); "Ada.Containers.Protected Maps" (for a map which can be accessed by multiple tasks at one time); "Ada.Containers.Persistent Vectors" (for a persistent vector which continues to exist between executions of a program) and so on.

Note that the language already includes several requirements that are important to the use of containers. These include:

- {AI2-0196-1} Library packages must allow concurrent calls by concurrent – multiple tasks can use the packages as long as they operate on separate containers. Thus, it is only necessary for a user to protect a container if a single container needs to be used by multiple tasks and concurrent calls to operations of the container have overlapping parameters.
- Language-defined types must stream "properly". That means that the stream attributes can be used to implement persistence of containers when necessary, and containers can be passed between partitions of a program.
• Equality of language-defined types must compose “properly”. This means that the version of "=" directly used by users is the same one that will be used in generics and in predefined equality operators of types with components of the containers and/or cursors. This prevents the abstraction from breaking unexpectedly.

• [AI05-0048-1] Redispatching is not allowed (unless it is required). That means that overriding a container operation will not change the behavior of any other predefined container operation. This provides a stable base for extensions.

{AI12-0258-1} If a container’s element type is controlled, the point at which the element is finalized will depend on the implementation of the container. For certain kinds of containers, we require finalization behavior based on the canonical implementation of the container (see the Implementation Requirements below). For the “normal” containers, we do not specify precisely where this will happen (it will happen no later than the finalization of the container, of course) in order to give implementations flexibility to cache, block, or split, or reuse the nodes of the container. In particular, Delete does not necessarily finalize the element; the implementation may (or may not) hold the space for reuse.

This paragraph was deleted {AI12-0258-1} This is not likely to be a hardship, as the element type has to be nonlimited. Types used to manage scarce resources generally need to be limited. Otherwise, the amount of resources needed is hard to control, as the language allows a lot of variation in the number or order of adjusts/finalizations. For common uses of nonlimited controlled types such as managing storage, the types already have to manage arbitrary copies.

The use of controlled types also brings up the possibility of failure of finalization (and thus deallocation) of an element. This is a “serious bug”, as AI95-179 puts it, so we don't try to specify what happens in that case. The implementation should propagate the exception.

Implementation Note: It is expected that exceptions propagated from these operations do not damage containers. That is, if Storage_Error is propagated because of an allocation failure, or Constraint_Error is propagated by the assignment of elements, the container can continue to be used without further exceptions. The intent is that it should be possible to recover from errors without losing data. We don't try to state this formally in most cases, because it is hard to define precisely what is and is not allowed behavior.

Implementation Note: [AI12-0005-1] When this clause says that the behavior of something is unspecified, we really mean that any result of executing Ada code short of erroneous execution is allowed. We do not mean that memory not belonging to the parameters of the operation can be trashed. When we mean to allow erroneous behavior, we specifically say that execution is erroneous. All this means that, if the containers are written in Ada, is that checks should not be suppressed or removed assuming some behavior of other code, and that the implementation should take care to avoid creating internal dangling accesses by assuming behavior from generic formals that can't be guaranteed. We don't try to say this normatively because it would be fairly complex, and implementers are unlikely to increase their support costs by fielding implementations that are unstable if given buggy hash functions, et al.

Static Semantics

{AI12-0035-1} {AI12-0449-1} Certain subprograms declared within instances of some of the generic packages presented in this clause are said to perform indefinite insertion. These subprograms are those corresponding (in the sense of the copying described in subclause 12.3) to subprograms that have formal parameters of a generic formal indefinite type and that are identified as performing indefinite insertion in the subclause defining the generic package.

{AI12-0035-1} {AI12-0449-1} If a subprogram performs indefinite insertion, then certain run-time checks are performed as part of a call to the subprogram; if any of these checks fail, then the resulting exception is propagated to the caller and the container is not modified by the call. These checks are performed for each parameter corresponding (in the sense of the copying described in 12.3) to a parameter in the corresponding generic whose type is a generic formal indefinite type. The checks performed for a given parameter are those checks explicitly specified in subclause 4.8 that would be performed as part of the evaluation of an initialized allocator whose access type is declared immediately within the instance, where:

• the value of the qualified_expression is that of the parameter; and

• the designated subtype of the access type is the subtype of the parameter; and

• finalization of the collection of the access type has started if and only if the finalization of the instance has started.

Discussion: [AI12-0449-1] The phrase "explicitly specified" means those checks for which subclause 4.8 includes the phrase "<some exception> is raised if ...". It does not refer, for example, to any checks performed as part of any
subtype conversion. In particular, this wording includes the checks described in subclause 4.8 to be performed in the case of a class-wide designated type, and of a designated subtype that has access discriminant parts. These checks are needed to prevent containers from outliving their contained (Element_Type or Key_Type) values.

**Implementation Note:** These rules have a dual purpose. Mainly, we are requiring checks needed to prevent dangling references. As a side effect, we are also allowing checks needed to permit an implementation of a container generic to make use of access types in a straightforward way. As an example of the second purpose, suppose that an implementation does declare such an access type and suppose further that the finalization of the collection of the access type has started. These rules allow Program_Error to be propagated in this case (as specified in 4.8); this is necessary to allow an all-Ada implementation of these packages.

**Implementation Requirements**

\{AI12-0258-1\} For an indefinite container (one whose type is defined in an instance of a child package of Containers whose defining_identifier contains "Indefinite"), each element of the container shall be created when it is inserted into the container and finalized when it is deleted from the container (or when the container object is finalized if the element has not been deleted). For a bounded container (one whose type is defined in an instance of a child package of Containers whose defining_identifier starts with "Bounded") that is not an indefinite container, all of the elements of the capacity of the container shall be created and default initialized when the container object is created; the elements shall be finalized when the container object is finalized. [For other kinds of containers, when elements are created and finalized is unspecified.]

**Ramification:** This allows a user to be able to reason about the behavior of elements that have controlled parts. In most cases, such elements need to be stored in an indefinite container.

**Implementation Note:** If the containers are implemented in Ada, this implies that elements for an indefinite container are allocated individually, and that a bounded container contains an array of elements or other data structure that is initialized for the entire capacity of the container when it is created. There is no such restriction on the implementation of the “normal” containers; these can be handled in any way convenient to the implementation — in particular, node reuse is allowed.

\{AI12-0112-1\} For an instance \(I\) of a container package with a container type, the specific type \(T\) of the object returned from a function that returns an object of an iterator interface, as well as the primitive operations of \(T\), shall be nonblocking. The Global aspect specified for \(T\) and the primitive operations of \(T\) shall be \((in\ all,\ out\ synchronized)\) or a specification that allows access to fewer global objects.

**Implementation Note:** This requires that the traversal and iteration operations of a container do not create, destroy, or assign any objects of a formal type of \(I\), nor call any formal subprograms of \(I\). Those objects and subprograms might be blocking (depending on the actual parameters). We put similar requirements on the individual traversal operations in the container package definitions.

**Reason:** These requirements allows users to use container iterators inside of parallel constructs, regardless of the actual parameters to the instantiation. If such an iterator allowed blocking, it would be illegal inside of a parallel construct (see 9.5). If such an iterator allowed writing of unsynchronized global objects, it would be illegal when the default conflict checking policy is in effect (see 9.10.1). These requirements include sequential iterators; the iterator does not need to appear in a parallel loop to trigger these requirements.

**Discussion:** We have to give these requirements as a text rule, as there is no place to declare suitable aspects. The specific type of a container iterator is declared by the implementation and is not part of the visible specification (iterator functions just return a value of a class-wide type). The iterator interface itself cannot impose such a requirement since it needs to be able to work with user-defined types that do need to allow blocking. We give this as a global requirement to avoid duplication.

**Extensions to Ada 95**

\{AI95-00302-03\} \{AI05-0299-1\} This subclause is new. It just provides an introduction to the following subclauses.

**Wording Changes from Ada 2005**

\{AI05-0044-1\} **Correction:** Added a definition of strict weak ordering.
Extensions to Ada 2012

Correction: We now say that a cursor only overlaps with the element it designates, rather than with the whole container. This allows some reading operations to operate on the container in parallel without separate synchronization.

Wording Changes from Ada 2012

Corrigendum: Added a definition of “performs indefinite insertion”. This is used in other subclauses and any resulting inconsistencies are documented there.

Moved the basic description of tampering checks here, to cut duplication in description of the individual containers. Added a description of stable views of containers.

Added a global requirement that iterators returned from containers are nonblocking if the instance is nonblocking.

Correction: Defined when objects are created and finalized for Bounded and Indefinite containers, so that these can be used reliably with controlled element types. This is not incompatible as this behavior was previously unspecified; code depending on specific behavior was wrong.

Corrigendum: Added a definition of “smallest first” ordering, so that the behavior of the Sort procedures when elements are equal is well-defined.

A.18.1 The Package Containers

The package Containers is the root of the containers subsystem.

Static Semantics

The library package Containers has the following declaration:

```ada
package Ada.Containers is
  withpragma Pure is (Containers);
  type Hash_Type is mod implementation-defined;
  type Count_Type is range 0 .. implementation-defined;
  exception Capacity_Error;
end Ada.Containers;
```

Hash_Type represents the range of the result of a hash function. Count_Type represents the (potential or actual) number of elements of a container.

Implementation defined: The value of Containers.Hash_Type'Modulus. The value of Containers.Count_Type'Last.

Capacity_Error is raised when the capacity of a container is exceeded.

Implementation Advice

Hash_Type'Modulus should be at least 2**32. Count_Type'Last should be at least 2**31–1.

Containers.Hash_Type'Modulus should be at least 2**32. Containers.Count_Type'Last should be at least 2**31–1.

Discussion: This is not a requirement so that these types can be declared properly on machines with native sizes that are not 32 bits. For instance, a 24-bit target could use 2**24 for Hash_Type'Modulus.

Extensions to Ada 95

The package Containers is new.

Incompatibilities With Ada 2005

Exception Capacity_Error is added to Containers. If Containers is referenced in a use_clause, and an entity with the name Capacity_Error is defined in a package that is also referenced in a use_clause, the entity Capacity_Error may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.
A.18.2 The Generic Package Containers.Vectors

The language-defined generic package Containers.Vectors provides private types Vector and Cursor, and a set of operations for each type. A vector container allows insertion and deletion at any position, but it is specifically optimized for insertion and deletion at the high end (the end with the higher index) of the container. A vector container also provides random access to its elements.

A vector container behaves conceptually as an array that expands as necessary as items are inserted. The length of a vector is the number of elements that the vector contains. The capacity of a vector is the maximum number of elements that can be inserted into the vector prior to it being automatically expanded.

Elements in a vector container can be referred to by an index value of a generic formal type. The first element of a vector always has its index value equal to the lower bound of the formal type.

A vector container may contain empty elements. Empty elements do not have a specified value.

**Implementation Note:** Vectors are not intended to be sparse (that is, there are elements at all defined positions). Users are expected to use other containers (like a Map) when they need sparse structures (there is a Note to this effect at the end of this subclause).

The internal array is a conceptual model of a vector. There is no requirement for an implementation to be a single contiguous array.

Static Semantics

{AI95-00302-03} The generic library package Containers.Vectors has the following declaration:

```
{AI05-0084-1} {AI05-0212-1} {AI12-0112-1} with Ada.Iterator_Interfaces;

generic
  type Index_Type is range <>;
  type Element_Type is private;
  with function "=" (Left, Right : Element_Type)
      return Boolean is <>;
package Ada.Containers.Vectors is
  with Preelaborate, Remote_Types, Nonblocking, Global => in out synchronized is
  pragma Preelaborate(Vectors);
  pragma Remote_Types(Vectors);

Discussion: {AI12-0112-1} For the Global aspect, any side-effects of the actual parameters of an instance are ignored. So Global => in out synchronized means that the only global side-effects allowed are associated with the actual generic parameters of the instance or with any synchronized state. Unsynchronized package state is not allowed for any container package, and pure packages do not allow any package state at all (they typically have Global => null).

{AI12-0112-1} Similarly, when Nonblocking is set to True for a generic unit, it still includes the blocking effects of the actual parameters to the instance. Thus, the only blocking allowed is that associated with the actual generic parameters. If none of the actual parameters allow blocking, then no operation of the generic instance may block.

subtype Extended_Index is
  Index_Type'Base range Index_Type'First-1 ..
  Index_Type'Min (Index_Type'Base'Last - 1, Index_Type'Last) + 1;
  No_Index : constant Extended_Index := Extended_Index'First;

Ramification: {AI12-0112-1} The base type of a scalar type is always nonblocking and has Global => null. Therefore, so long as this type is used in the implementation, whether or not the actual type for Index_Type allows blocking or side-effects does not matter. Therefore, we require that operations that only operate on the container implementation be nonblocking and have Global => null regardless of the actual parameters.
type Vector is tagged private
  with Constant_Indexing => Constant_Reference,
  Variable_Indexing => Reference,
  Default Iterator => Iterate,
  Iterator Element => Element_Type,
  Iterator View => Stable.Vector,
  Aggregate => (Empty => Empty,
                 AddUnnamed => Append,
                 New Indexed => New Vector,
                 Assign Indexed => Replace Element),
  Stable Properties => (Length, Capacity,
                         Tampering With Cursors Prohibited,
                         Tampering With Elements Prohibited),
  Default Initial Condition =>
    Length (Vector) = 0 and then
    (not Tampering With Cursors Prohibited (Vector)) and then
    (not Tampering With Elements Prohibited (Vector)),
pragma Preelaborable_Initialization (Vector);

   type Cursor is private
withpragma Preelaborable_Initialization (Cursor);

Empty_Vector : constant Vector;
No_Element : constant Cursor;

function Has_Element (Position : Cursor) return Boolean
with Nonblocking, Global => in all, Use Formal => null;

function Has_Element (Container : Vector; Position : Cursor) return Boolean
with Nonblocking, Global => null, Use Formal => null;

package Vector_Iterator_Interfaces is new
Ada.Iterator_Interfaces (Cursor, Has_Element);

function "=" (Left, Right : Vector) return Boolean;

function Tampering With Cursors Prohibited
  (Container : Vector) return Boolean
with Nonblocking, Global => null, Use Formal => null;

function Tampering With Elements Prohibited
  (Container : Vector) return Boolean
with Nonblocking, Global => null, Use Formal => null;

function Maximum Length return Count_Type
with Nonblocking, Global => null, Use Formal => null;

function Empty (Capacity : Count_Type := implementation-defined)
  return Vector
with Pre => Capacity <= Maximum Length
  or else raise Constraint_Error,
Post =>
  Capacity (Empty' Result) >= Capacity and then
  not Tampering With Elements Prohibited (Empty' Result) and then
  not Tampering With Cursors Prohibited (Empty' Result) and then
  Length (Empty' Result) = 0;
function To_Vector (Length : Count_Type) return Vector with Pre => Length <= Maximum_Length or else raise Constraint_Error,
Post =>
To_Vector'Result.Length = Length and then
not Tampering_With_Elements_Prohibited (To_Vector'Result) and then
not Tampering_With_Cursors_Prohibited (To_Vector'Result) and then
To_Vector'Result.Capacity >= Length;

function To_Vector
(Left, Right : Vector; Length : Count_Type) return Vector
is
To Vector (Count Type (Last - First + 1));

function "&" (Left, Right : Vector) return Vector with Pre => Length (Left) <= 2 or else raise Constraint_Error,
Post =>
Length (Vectors."&"Result) =
Length (Left) + Length (Right) and then
not Tampering_With_Elements_Prohibited
(Vectors."&"Result) and then
not Tampering_With_Cursors_Prohibited
(Vectors."&"Result) and then
Vectors."&"Result.Capacity >= Length (Left) + Length (Right);

function "&" (Left : Element_Type; Right : Vector) return Vector with Pre => Length (Right) <= 2 or else raise Constraint_Error,
Post =>
Length (Vectors."&"Result) = Length (Right) + 1 and then
not Tampering_With_Elements_Prohibited
(Vectors."&"Result) and then
not Tampering_With_Cursors_Prohibited
(Vectors."&"Result) and then
Vectors."&"Result.Capacity >= Length (Right) + 1;

function "&" (Left : Element_Type; Right : Vector) return Vector with Pre => Length (Right) <= 2 or else raise Constraint_Error,
Post =>
Length (Vectors."&"Result) = Length (Right) + 1 and then
not Tampering_With_Elements_Prohibited
(Vectors."&"Result) and then
not Tampering_With_Cursors_Prohibited
(Vectors."&"Result) and then
Vectors."&"Result.Capacity >= Length (Right) + 1;

function "&" (Left, Right : Element_Type) return Vector with Pre => Maximum Length >= 2 or else raise Constraint_Error,
Post =>
Length ("&"Result) = 2 and then
not Tampering_With_Elements_Prohibited
(Vectors."&"Result) and then
not Tampering_With_Cursors_Prohibited
(Vectors."&"Result) and then
Vectors."&"Result.Capacity >= 2;

function Capacity (Container : Vector) return Count_Type with Nonblocking, Global => null, Use Formal => null;
procedure Reserve_Capacity (Container : in out Vector;
Capacity : in Count_Type);
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Container.Capacity >= Capacity;

function Length (Container : Vector) return Count_Type
with Nonblocking, Global => null, Use_Formal => null;

procedure Set_Length (Container : in out Vector;
Length : in Count_Type)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Length <= Maximum_Length
or else raise Constraint_Error),
Post => Container.Length = Length and then
Capacity (Container) >= Length;

function Is_Empty (Container : Vector) return Boolean
with Nonblocking, Global => null, Use_Formal => null,
Post => Is_Empty'Result = (Length (Container) = 0);

procedure Clear (Container : in out Vector)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Length (Container) = 0;

function To_Cursor (Container : Vector;
Index     : Extended_Index) return Cursor
with Post => (if Index in
First_Index (Container) .. Last_Index (Container)
then Has_Element (Container, To_Cursor'Result)
else to_Cursor'Result = No_Element),
Nonblocking, Global => null, Use_Formal => null;

function To_Index (Position  : Cursor)
return Extended_Index
with Pre => Position /= No_Element
or else raise Constraint_Error,
Nonblocking, Global => in all,
Post => Position = No_Element
or else raise Program_Error;

function To_Index (Container : Vector;
Position  : Cursor) return Extended_Index
with Pre => Position /= No_Element
or else raise Program_Error,
Post => (if Position = No_Element then To_Index'Result = No_Index
else To_Index'Result in First_Index (Container) ..
Last_Index (Container)),
Nonblocking, Global => null, Use_Formal => null;

function Element (Container : Vector;
Index     : Index_Type) return Element_Type
with Pre in First_Index (Container) .. Last_Index (Container)
or else raise Constraint_Error,
Nonblocking, Global => null, Use_Formal => Element_Type;

function Element (Position : Cursor) return Element_Type
with Pre => Position /= No_Element
or else raise Constraint_Error,
Nonblocking, Global => in all, Use_Formal => Element_Type;

function Element (Container : Vector;
Position  : Cursor) return Element_Type
with Pre => (Position /= No_Element
or else raise Constraint_Error) and then
Has_Element (Container, Position)
or else raise Program_Error,
Nonblocking, Global => null, Use_Formal => Element_Type;

Discussion: Here the Nonblocking and Global contracts are saying that Element depends on the properties of the actual for Element_Type, but not on the properties of the actuals for Index_Type or "=". This is necessary as copying the element may require calling Adjust and Finalize for the actual Element_Type, and those may have side-effects or block.
procedure Replace_Element (Container : in out Vector;
  Index     : in    Index_Type;
  New_Item  : in    Element_Type)
with Pre => (not Tampering_With_Elements_Prohibited (Container)
  or else raise Program_Error) and then
  (Index in First_Index (Container) .. Last_Index (Container)
  or else raise Constraint_Error);

procedure Replace_Element (Container : in out Vector;
  Position  : in    Cursor;
  New_item  : in    Element_Type)
with Pre => (not Tampering_With_Elements_Prohibited (Container)
  or else raise Program_Error) and then
  (Position /= No_Element
  or else raise Constraint_Error) and then
  (Has_Element (Container, Position)
  or else raise Program_Error);

procedure Query_Element
(Container : in Vector;
  Index     : in    Index_Type;
  Process   : not null access procedure (Element : in Element_Type))
with Pre => Index in First_Index (Container) .. Last_Index (Container)
  or else raise Constraint_Error;

procedure Query_Element
(Position : in Cursor;
  Process  : not null access procedure (Element : in Element_Type))
with Pre => Position /= No_Element or else raise Constraint_Error.
  Global => in all;

procedure Query_Element
(Container : in Vector;
  Position  : in    Cursor;
  Process   : not null access procedure (Element : in Element_Type))
with Pre => (Position /= No_Element
  or else raise Constraint_Error) and then
  (Has_Element (Container, Position)
  or else raise Program_Error);

procedure Update_Element
(Container : in out Vector;
  Index     : in    Index_Type;
  Process   : not null access procedure (Element : in out Element_Type))
with Pre => Index in First_Index (Container) .. Last_Index (Container)
  or else raise Constraint_Error;

procedure Update_Element
(Container : in out Vector;
  Position  : in    Cursor;
  Process   : not null access procedure (Element : in out Element_Type))
with Pre => (Position /= No_Element
  or else raise Constraint_Error) and then
  (Has_Element (Container, Position)
  or else raise Program_Error);

type Constant_Reference_Type
(Element : not null access constant Element_Type)
  is private
  with Implicit_Dereference => Element,
  Nonblocking, Global => in out synchronized,
  Default_Initial_Condition => (raise Program_Error);

Discussion: Finalization of this type will update the tampering counter of an associated container. We know this has to be an object of type Vector, but we don't have a way to specify that. We need this separate Global in case an object of this type is declared to exist separately from the short-lived object associated with a call of the Constant_Reference function.
**type** Reference_Type (Element : not null access Element_Type) is private
  with Implicit Dereference => Element,
  Nonblocking, Global => in out synchronized,
  Default Initial Condition => (raise Program_Error);

**function** Constant_Reference (Container : aliased in Vector;
  Index : in Index_Type)
  return Constant_Reference_Type
  with Pre => Index in
  First_Index (Container) .. Last_Index (Container)
  or else raise Constraint_Error,
  Post => Tampering_With_Cursors_Prohibited (Container),
  Nonblocking, Global => null, Use Formal => null;

**function** Reference (Container : aliased in out Vector;
  Index : in Index_Type)
  return Reference_Type
  with Pre => Index in
  First_Index (Container) .. Last_Index (Container)
  or else raise Constraint_Error,
  Post => Tampering_With_Cursors_Prohibited (Container),
  Nonblocking, Global => null, Use Formal => null;

**function** Constant_Reference (Container : aliased in Vector;
  Position : in Cursor)
  return Constant_Reference_Type
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
  (Has_Element (Container, Position) or else raise Program_Error),
  Post => Tampering_With_Cursors_Prohibited (Container),
  Nonblocking, Global => null, Use Formal => null;

**function** Reference (Container : aliased in out Vector;
  Position : in Cursor)
  return Reference_Type
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
  (Has_Element (Container, Position) or else raise Program_Error),
  Post => Tampering_With_Cursors_Prohibited (Container),
  Nonblocking, Global => null, Use Formal => null;

**procedure** Assign (Target : in out Vector; Source : in Vector)
  with Pre => not Tampering_With_Cursors_Prohibited (Target)
  or else raise Program_Error,
  Post => Length (Source) = Length (Target) and then
  Capacity (Target) >= Length (Target);

**function** Copy (Source : Vector; Capacity : Count_Type := 0)
  return Vector
  with Pre => Capacity = 0 or else Capacity >= Length (Source)
  or else raise Capacity_Error,
  Post => Length (Copy'Result) = Length (Source) and then
  not Tampering_With_Elements_Prohibited (Copy'Result) and then
  not Tampering_With_Cursors_Prohibited (Copy'Result) and then
  Copy'Result.Capacity >= (if Capacity = 0 then Length (Source) else Capacity);
procedure Move (Target : in out Vector; 
    Source : in out Vector)
with Pre => (not Tampering_With.Cursors_Prohibited (Target) 
  or else raise Program_Error) and then 
  (not Tampering_With.Cursors_Prohibited (Source) 
  or else raise Program_Error), 
Post => (if not Target'Has_Same_Storage (Source) then 
  Length (Target) = Length (Source)'Old and then 
  Length (Source) = 0 and then 
  Capacity (Target) >= Length (Source)'Old) ;

procedure Insert_VectorInsert (Container : in out Vector; 
    Before    : in Extended_Index; 
    New_Item  : in Vector)
with Pre => (not Tampering_With.Cursors_Prohibited (Container) 
  or else raise Program_Error) and then 
  (Before in 
    First_Index (Container) .. Last_Index (Container) + 1 
  or else raise Constraint_Error) and then 
  (Length (Container) <= Maximum_Length - Length (New_Item) 
  or else raise Constraint_Error), 
Post => Length (Container)'Old + Length (New_Item) = 
  Length (Container) and then 
  Capacity (Container) >= Length (Container) ;

procedure Insert_VectorInsert (Container : in out Vector; 
    Before    : in Cursor; 
    New_Item  : in Vector)
with Pre => (not Tampering_With.Cursors_Prohibited (Container) 
  or else raise Program_Error) and then 
  (Before = No_Element or else 
    Has_Element (Container, Before) 
  or else raise Program_Error) and then 
  (Length (Container) <= Maximum_Length - Length (New_Item) 
  or else raise Constraint_Error), 
Post => Length (Container)'Old + Length (New_Item) = 
  Length (Container) and then 
  Capacity (Container) >= Length (Container) ;

procedure Insert_VectorInsert (Container : in out Vector; 
    Before    : in Cursor; 
    New_Item  : in Vector; 
    Position  : out Cursor)
with Pre => (not Tampering_With.Cursors_Prohibited (Container) 
  or else raise Program_Error) and then 
  (Before = No_Element or else 
    Has_Element (Container, Before) 
  or else raise Program_Error) and then 
  (Length (Container) <= Maximum_Length - Length (New_Item) 
  or else raise Constraint_Error), 
Post => Length (Container)'Old + Length (New_Item) = 
  Length (Container) and then 
  Has_Element (Container, Position) and then 
  Capacity (Container) >= Length (Container) ;
procedure Insert (Container : in out Vector;
Before : in   Extended_Index;
New Item : in   Element_Type;
Count : in   Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Before in First_Index (Container) .. Last_Index (Container) + 1
or else raise Constraint_Error)
Post => Length (Container)'Old + Count =
Capacity (Container) >= Length (Container);
procedure Insert (Container : in out Vector;
    Before    : in   Cursor;
    Position  : out  Cursor;
    Count     : in   Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
    (Before = No_Element or else
     Has_Element (Container, Before)
or else raise Program_Error) and then
    (Length (Container) <= Maximum_Length - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count = Length (Container)
and then Has_Element (Container, Position) and then
    Capacity (Container) >= Length (Container);

procedure Prepend_VectorPrepend (Container : in out Vector;
    New_Item  : in   Vector)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
    (Length (Container) <= Maximum_Length - Length (New_Item)
or else raise Constraint_Error),
Post => Length (Container)'Old + Length (New_Item) =
    Length (Container) and then
    Capacity (Container) >= Length (Container);

procedure Prepend (Container : in out Vector;
    New_Item  : in   Element_Type;
    Count     : in   Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
    (Length (Container) <= Maximum_Length - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count =
    Length (Container) and then
    Capacity (Container) >= Length (Container);

procedure Append_VectorAppend (Container : in out Vector;
    New_Item  : in   Vector)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
    (Length (Container) <= Maximum_Length - Length (New_Item)
or else raise Constraint_Error),
Post => Length (Container)'Old + Length (New_Item) =
    Length (Container) and then
    Capacity (Container) >= Length (Container);

procedure Append (Container : in out Vector;
    New_Item  : in   Element_Type)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
    (Length (Container) <= Maximum_Length - 1
or else raise Constraint_Error),
Post => Length (Container)'Old + 1 = Length (Container) and then
    Capacity (Container) >= Length (Container);
procedure Insert_Space (Container : in out Vector;
Before    : in Extended_Index;
Count     : in Count_Type := 1)
with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Before in First Index (Container) .. Last Index (Container) + 1
or else raise Constraint_Error) and then
(Length (Container) <= Maximum Length - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count =
Length (Container) and then
Capacity (Container) >= Length (Container);

procedure Insert_Space (Container : in out Vector;
Before    : in Cursor;
Position  : out Cursor;
Count     : in Count_Type := 1)
with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Before = No_Element or else
Has Element (Container, Before)
or else raise Program_Error) and then
(Length (Container) <= Maximum Length - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count =
Length (Container) and then
Has Element (Container, Position) and then
Capacity (Container) >= Length (Container);

procedure Delete (Container : in out Vector;
Index     : in Extended_Index;
Count     : in Count_Type := 1)
with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Index in First Index (Container) .. Last Index (Container) + 1
or else raise Constraint_Error),
Post => Length (Container)'Old - Count <=
Length (Container);

procedure Delete (Container : in out Vector;
Position  : in out Cursor;
Count     : in Count_Type := 1)
with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Position /= No_Element
or else raise Constraint_Error) and then
(Has Element (Container, Position)
or else raise Program_Error),
Post => Length (Container)'Old - Count <=
Length (Container) and then
Position = No_Element;

procedure Delete First (Container : in out Vector;
Count     : in Count_Type := 1)
with Pre => not Tampering With Cursors Prohibited (Container)
or else raise Program_Error,
Post => Length (Container)'Old - Count <= Length (Container);

procedure Delete Last (Container : in out Vector;
Count     : in Count_Type := 1)
with Pre => not Tampering With Cursors Prohibited (Container)
or else raise Program Error,
Post => Length (Container)'Old - Count <= Length (Container);

procedure Reverse_Elements (Container : in out Vector)
with Pre => not Tampering With Cursors Prohibited (Container)
or else raise Program Error;
procedure Swap (Container : in out Vector;  
I, J : in Index_Type) 
with Pre => (not Tampering_With_Elements_Prohibited (Container) 
or else raise Program_Error) and then 
(I in First_Index (Container) .. Last_Index (Container) 
or else raise Constraint_Error) and then 
(J in First_Index (Container) .. Last_Index (Container) 
or else raise Constraint_Error);

procedure Swap (Container : in out Vector;  
I, J : in Cursor) 
with Pre => (not Tampering_With_Elements_Prohibited (Container) 
or else raise Program_Error) and then 
(I /= No_Element or else Constraint_Error) and then 
(J /= No_Element or else Constraint_Error) and then 
(Has_Element (Container, I) 
or else raise Program_Error) and then 
(Has_Element (Container, J) 
or else raise Program_Error);

function First_Index (Container : Vector) return Index_Type 
with Nonblocking, Global => null, Use Formal => null, 
Post => First_Index'Result = Index_Type'First;

function First (Container : Vector) return Cursor 
with Nonblocking, Global => null, Use Formal => null, 
Post => (if not Is_Empty (Container) 
then Has_Element (Container, First'Result) 
else First'Result = No_Element);

function First_Element (Container : Vector) return Element_Type 
with Pre => (not Is_Empty (Container) 
or else raise Constraint_Error);

function Last_Index (Container : Vector) return Extended_Index 
with Nonblocking, Global => null, Use Formal => null, 
Post => (if Length (Container) = 0 
then Last_Index'Result = No_Index 
else Count_Type(Last_Index'Result - Index_Type'First) = 
Length (Container) - 1);

function Last (Container : Vector) return Cursor 
with Nonblocking, Global => null, Use Formal => null, 
Post => (if not Is_Empty (Container) 
then Has_Element (Container, Last'Result) 
else Last'Result = No_Element);

function Last_Element (Container : Vector) return Element_Type 
with Pre => (not Is_Empty (Container) 
or else raise Constraint_Error);

function Next (Position : Cursor) return Cursor 
with Nonblocking, Global => in all, Use Formal => null, 
Post => (if Position = No_Element then Next'Result = No_Element);

function Next (Container : Vector; Position : Cursor) return Cursor 
with Nonblocking, Global => null, Use Formal => null, 
Pre => Position = No_Element or else 
Has_Element (Container, Position) 
or else raise Program_Error, 
Post => (if Position = No_Element then Next'Result = No_Element 
elif Has_Element (Container, Next'Result) then 
To_Index (Container, Next'Result) = 
To_Index (Container, Position) + 1 
elif Next'Result = No_Element then 
Position = Last (Container) 
else False);

procedure Next (Position : in out Cursor) 
with Nonblocking, Global => in all, Use Formal => null;
procedure Next (Container : in Vector;  
Position : in out Cursor)  
with Nonblocking, Global => null, Use Formal => null,  
Pre => Position = No Element or else  
Has_Element (Container, Position)  
or else raise Program_Error,  
Post => (if Position /= No Element  
then Has_Element (Container, Position)));  

function Previous (Position : Cursor) return Cursor  
with Nonblocking, Global => in all, Use Formal => null,  
Post => (if Position = No Element  
then Previous'Result = No_Element);  

function Previous (Container : Vector;  
Position : Cursor) return Cursor  
with Nonblocking, Global => null, Use Formal => null,  
Pre => Position = No Element or else  
Has_Element (Container, Position)  
or else raise Program_Error,  
Post => (if Position = No Element  
then Previous'Result = No_Element  
elsif Has_Element (Container, Previous'Result) then  
To_Index (Container, Previous'Result) =  
To_Index (Container, Position) - 1  
elsif Previous'Result = No_Element then  
Position = First (Container)  
else False);  

function Find_Index (Container : Vector;  
Item : Element_Type;  
Index : Index_Type := Index_Type'First)  
return Extended_Index;  

function Find (Container : Vector;  
Item : Element_Type;  
Position : Cursor := No_Element)  
return Cursor  
with Pre => Position = No Element or else  
Has_Element (Container, Position)  
or else raise Program_Error,  
Post => (if Find'Result /= No Element  
then Has_Element (Container, Find'Result));  

function Reverse_Find_Index (Container : Vector;  
Item : Element_Type;  
Index : Index_Type := Index_Type'Last)  
return Extended_Index;  

function Reverse_Find (Container : Vector;  
Item : Element_Type;  
Position : Cursor := No_Element)  
return Cursor  
with Pre => Position = No Element or else  
Has_Element (Container, Position)  
or else raise Program_Error,  
Post => (if Reverse_Find'Result /= No Element  
then Has_Element (Container, Reverse_Find'Result));
function Contains (Container : Vector; Item : Element_Type) return Boolean;

This paragraph was deleted.

function Has_Element (Position : Cursor) return Boolean;

procedure Iterate
(Container : in Vector;
 Process : not null access procedure (Position : in Cursor))
with Allows_Exit;

procedure Reverse_Iterate
(Container : in Vector;
 Process : not null access procedure (Position : in Cursor))
with Allows_Exit;

function Iterate (Container : in Vector) return
Vector_Iterator_Interfaces.Parallel_Reversible_Iterator'Class
with Post => Tampering_With_Cursors_Prohibited (Container);

function Iterate (Container : in Vector; Start : in Cursor)
return Vector_Iterator_Interfaces.Reversible_Iterator'Class
with Pre => (Start /= No_Element
or else raise Constraint_Error) and then
(Has_Element (Container, Start)
or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container);

with generic function "<" (Left, Right : Element_Type) is <; package Generic_Sorting
with Nonblocking, Global => null is
function Is_Sorted (Container : Vector) return Boolean;

procedure Sort (Container : in out Vector)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error;

procedure Merge (Target : in out Vector;
 Source : in out Vector)
with Pre => (not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error) and then
(not Tampering_With_Cursors_Prohibited (Source)
or else raise Program_Error) and then
((Length (Target) <= Maximum_Length - Length (Source)
or else raise Constraint_Error) and then
((Length (Source) = 0 or else
not Target'Has_Same_Storage (Source))
or else raise Program_Error),
Post => (declare
Result_Length : constant Count_Type :=
Length (Source)'Old + Length (Target)'Old;
begin
Length (Source) = 0 and then
Length (Target) = Result_Length and then
Capacity (Target) >= Result_Length));

end Generic_Sorting;

package Stable is
type Vector (Base : not null access Vectors.Vector) is
tagged limited private
with Constant_Indexing => Constant_Reference,
Variable_Indexing => Reference,
Default_Iterator => Iterate,
Iterator_Element => Element_Type,
Stable_Properties => (Length, Capacity),
Global => null,
Default_Initial_Condition => Length (Vector) = 0,
Preelaborable_Initialization;

Discussion: The Global of null assumes that the user of a stable object is including effects associated
with the access discriminant. For operations with in parameters (after any overridi
ging), the object designated by the access discriminant is assumed to be read, and for other operations (including initialization and finalization) the object
designated by the access discriminant is assumed to be read and updated.

type Cursor is private
with Preelaborable_Initialization;

Empty_Vector : constant Vector;
No_Element : constant Cursor;

function Has_Element (Position : Cursor) return Boolean
with Nonblocking, Global => in all, Use_Formal => null;

package Vector_Iterator_Interfaces is new
Ada.Iterator_Interfaces (Cursor, Has_Element);

procedure Assign (Target : in out Vectors.Vector;
Source : in Vector)
with Post => Length (Source) = Length (Target) and then
Capacity (Target) => Length (Target);

function Copy (Source : Vectors.Vector) return Vector
with Post => Length (Copy'Result) = Length (Source);

type Constant_Reference_Type
(Element : not null access constant Element_Type) is private
with Implicit_Dereference => Element,
Nonblocking, Global => null, Use Formal => null,
Default_Initial_Condition => raise Program_Error;

type Reference_Type
(Element : not null access Element_Type) is private
with Implicit_Dereference => Element,
Nonblocking, Global => null, Use Formal => null,
Default_Initial_Condition => raise Program_Error;

-- Additional subprograms as described in the text
-- are declared here.

private
... -- not specified by the language

end Stable;

private
... -- not specified by the language

end Ada.Containers.Vectors;

The actual function for the generic formal function "=" on Element_Type values is
expected to define a reflexive and symmetric relationship and return the same result value each time it is
called with a particular pair of values. If it behaves in some other manner, the functions defined to use it
return an unspecified value. The exact arguments and number of calls of this generic formal function by
the functions defined to use it are unspecified.

Ramification: The “functions defined to use it” are Find, Find_Index, Reverse_Find, Reverse_Find_Index, and "=" for
Vectors. This list is a bit too long to give explicitly.
If the actual function for "=" is not symmetric and consistent, the result returned by any of the functions defined to use "=" cannot be predicted. The implementation is not required to protect against "=" raising an exception, or returning random results, or any other "bad" behavior. And it can call "=" in whatever manner makes sense. But note that only the results of the functions defined to use "=" are unspecified; other subprograms are not allowed to break if "=" is bad.

{AI95-00302-03} The type Vector is used to represent vectors. The type Vector needs finalization (see 7.6).

{AI95-00302-03} Empty_Vector represents the empty vector object. It has a length of 0. If an object of type Vector is not otherwise initialized, it is initialized to the same value as Empty_Vector.

{AI95-00302-03} No_Element represents a cursor that designates no element. If an object of type Cursor is not otherwise initialized, it is initialized to the same value as No_Element.

{AI95-00302-03} [AI12-0434-1] The predefined "=" operator for type Cursor returns True if both cursors are No_Element, or designate the same element in the same container.

To be honest: [AI12-0434-1] "The primitive "=" operator" is the one with two parameters of type Cursor which returns Boolean. We're not talking about some other (hidden) primitive function named "=".

{AI95-00302-03} Execution of the default implementation of the Input, Output, Read, or Write attribute of type Cursor raises Program_Error.

Reason: A cursor will probably be implemented in terms of one or more access values, and the effects of streaming access values is unspecified. Rather than letting the user stream junk by accident, we mandate that streaming of cursors raise Program_Error by default. The attributes can always be specified if there is a need to support streaming.

{AI05-0001-1} {AI05-0262-1} {AI12-0437-1} Vector'Write for a Vector object V writes Length(V) elements of the vector to the stream. It may also may write additional information about the vector.

{AI05-0001-1} {AI05-0262-1} Vector'Read reads the representation of a vector from the stream, and assigns to Item a vector with the same length and elements as was written by Vector'Write.

Implementation Note: The Reference Manual requires streaming of all language-defined nonlimited types (including containers) to "work" (see 13.13.2). In addition, we do not want all of the elements that make up the capacity of the vector streamed, as those beyond the length of the container have undefined contents (and might cause bad things when read back in). This will require a custom stream attribute implementation; the language-defined default implementation will not work (even for a bounded form, as that would most likely stream the entire capacity of the vector). There is a separate requirement that the unbounded and Bounded form use the same streaming representation for the same element type, see A.18.19.

{AI95-00302-03} No_Index represents a position that does not correspond to any element. The subtype Extended_Index includes the indices covered by Index_Type plus the value No_Index and, if it exists, the successor to the Index_Type'Last.

Discussion: We require the existence of Index_Type'First – 1, so that No_Index and Last_Index of an empty vector is well-defined. We don't require the existence of Index_Type'Last + 1, as it is only used as the position of insertions (and needs to be allowed only when inserting an empty vector).

{AI05-0001-1} {AI12-0112-1} If an operation attempts to modify the vector such that the position of the last element would be greater than Index_Type'Last, then the operation propagates Constraint_Error.

Reason: We don't want to require an implementation to go to heroic efforts to handle index values larger than the base type of the index subtype.

{AI95-00302-03} [AI12-0111-1] {AI12-0112-1} [Some operations of this generic package have access to subprogram parameters. To ensure such operations are well defined, they guard against certain actions by the designated subprogram. In particular, some operations check for "tampering with cursors" of a container because they depend on the set of elements of the container remaining constant, and others check for "tampering with elements" of a container because they depend on elements of the container not being replaced.] When tampering with cursors is prohibited for a particular vector object V, Program_Error is propagated by the finalization of V, as well as by a call that passes V to certain of the operations of this package, as indicated by the precondition of such an operation. Similarly, when
tampering with elements is prohibited for \( V \). Program_Error is propagated by a call that passes \( V \) to certain of the other operations of this package, as indicated by the precondition of such an operation.

Paragraphs 91 through 97 are removed as preconditions now describe these rules.

A subprogram is said to tamper with cursors of a vector object \( V \) if:

- it inserts or deletes elements of \( V \), that is, it calls the Insert, Insert_Space, Clear, Delete, or Set_Length procedures with \( V \) as a parameter; or

  To be honest: Operations which are defined to be equivalent to a call on one of these operations also are included. Similarly, operations which call one of these as part of their definition are included.

- it finalizes \( V \); or

- it calls the Assign procedure with \( V \) as the Target parameter; or

  Ramification: We don’t need to explicitly mention assignment_statement, because that finalizes the target object as part of the operation, and finalization of an object is already defined as tampering with cursors.

- it calls the Move procedure with \( V \) as a parameter.

Discussion: Swap, Sort, and Merge copy elements rather than reordering them, so they don’t tamper with cursors.

A subprogram is said to tamper with elements of a vector object \( V \) if:

- it tampers with cursors of \( V \); or

- it replaces one or more elements of \( V \), that is, it calls the Replace_Element, Reverse_Elements, or Swap procedures or the Sort or Merge procedures of an instance of Generic_Sorting with \( V \) as a parameter.

Reason: Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can’t be allowed. However, a simple modification of (part of) an element is not a problem, so Update_Element does not cause a problem.

When tampering with cursors is prohibited for a particular vector object \( V \), Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the cursors of \( V \), leaving \( V \) unmodified. Similarly, when tampering with elements is prohibited for a particular vector object \( V \), Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the elements of \( V \) (or tamper with the cursors of \( V \)), leaving \( V \) unmodified. These checks are made before any other defined behavior of the body of the language-defined subprogram.

Proof: Tampering with elements includes tampering with cursors, so we mention it only from completeness in the second sentence.

function Has_Element (Position : Cursor) return Boolean
with Nonblocking, Global => in all, Use Formal => null;

Returns True if Position designates an element, and returns False otherwise.

To be honest: This function might not detect cursors that designate deleted elements; such cursors are invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

function Has_Element (Container : Vector; Position : Cursor)
return Boolean
with Nonblocking, Global => null, Use Formal => null;

Returns True if Position designates an element in Container, and returns False otherwise.

Ramification: If Position is No_Element, Has_Element returns False.
function 
"=" (Left, Right : Vector) return Boolean;

{AI95-00302-03} {AI05-0264-1} If Left and Right denote the same vector object, then the
function returns True. If Left and Right have different lengths, then the function returns False. Otherwise, it compares each element in Left to the corresponding element in Right using the
generic formal equality operator. If any such comparison returns False, the function returns False; otherwise it returns True. Any exception raised during evaluation of element equality is
propagated.

Implementation Note: This wording describes the canonical semantics. However, the order and number of calls on the
formal equality function is unspecified for all of the operations that use it in this package, so an implementation can
call it as many or as few times as it needs to get the correct answer. Specifically, there is no requirement to call the
formal equality additional times once the answer has been determined.

function Tampering_With_Cursors_Prohibited
(Container : Vector) return Boolean
with Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} Returns True if tampering with cursors or tampering with elements is currently
prohibited for Container, and returns False otherwise.

Reason: {AI12-0112-1} Prohibiting tampering with elements also needs to prohibit tampering with cursors, as deleting
an element is similar to replacing it.

Implementation Note: {AI12-0112-1} Various contracts elsewhere in this specification require that this function be
implemented with synchronized data. Moreover, it is possible for tampering to be prohibited by multiple operations
(sequentially or in parallel). Therefore, tampering needs to be implemented with an atomic or protected counter. The
counter is initialized to zero, and is incremented when tampering is prohibited, and decremented when leaving an area
that prohibited tampering. Function Tampering_With_Cursors_Prohibited returns True if the counter is nonzero. (Note
that any case where the result is not well-defined for one task is incorrect use of shared variables and would be
erroneous by the rules of 9.10, so no special protection is needed to read the counter.)

function Tampering_With_Elements_Prohibited
(Container : Vector) return Boolean
with Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} Always returns False, regardless of whether tampering with elements is
prohibited.

Reason: {AI12-0111-1} A definite element cannot change size, so we allow operations that tamper with elements even
when tampering with elements is prohibited. That's not true for the indefinite containers, which is why this kind of
tampering exists.

function Maximum_Length return Count_Type
with Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} Returns the maximum Length of a Vector, based on the index type.

Implementation Note: This is just:

\[ \text{Count Type (Index Type'Last - Index Type'First + 1)} \]

but since the inner calculation can overflow or the type conversion can fail, this can't be evaluated in general with an
expression function. Note that if this expression raises Constraint_Error, then the result is Count_Type'Last, since the
Capacity of a Vector cannot exceed Count_Type'Last.

function Empty (Capacity : Count_Type := implementation-defined)
return Vector
with Pre => Capacity <= Maximum_Length
or else raise Constraint_Error,
Post =>
Capacity (Empty'Result) => Capacity and then
not Tampering_With_Elements_Prohibited (Empty'Result) and then
not Tampering_With_Cursors_Prohibited (Empty'Result) and then
Length (Empty'Result) = 0;

{AI12-0339-1} Returns an empty vector.
function To_Vector (Length : Count_Type) return Vector
  with Pre => Length <= Maximum_Length or else raise Constraint_Error,
  Post =>
    To_Vector'Result.Length = Length and then
    not Tampering_With_Elements_Prohibited (To_Vector'Result)
    and then
    not Tampering_With_Cursors_Prohibited (To_Vector'Result)
    and then
    To_Vector'Result.Capacity >= Length;

{AI95-00302-03} Returns a vector with a length of Length, filled with empty elements.

function To_Vector (New_Item : Element_Type;
   Length   : Count_Type) return Vector
  with Pre => Length <= Maximum_Length or else raise Constraint_Error,
  Post =>
    To_Vector'Result.Length = Length and then
    not Tampering_With_Elements_Prohibited (To_Vector'Result)
    and then
    not Tampering_With_Cursors_Prohibited (To_Vector'Result)
    and then
    To_Vector'Result.Capacity >= Length;

{AI95-00302-03} Returns a vector with a length of Length, filled with elements initialized to the value New_Item.

function "&" (Left, Right : Vector) return Vector
  with Pre => Length (Left) <= Maximum_Length - Length (Right)
  or else raise Constraint_Error,
  Post =>
    Length (Vectors."&"Result) =
    Length (Left) + Length (Right) and then
    not Tampering_With_Elements_Prohibited (Vectors."&"Result)
    and then
    not Tampering_With_Cursors_Prohibited (Vectors."&"Result)
    and then
    Vectors."&"Result.Capacity >=
    Length (Left) + Length (Right);

{AI95-00302-03} Returns a vector comprising the elements of Left followed by the elements of Right.

function "&" (Left  : Vector;
     Right : Element_Type) return Vector
  with Pre => Length (Left) <= Maximum_Length - 1
  or else raise Constraint_Error,
  Post =>
    Length (Vectors."&"Result) = Length (Left) + 1 and then
    not Tampering_with_Elements_Prohibited (Vectors."&"Result)
    and then
    not Tampering_With_Cursors_Prohibited (Vectors."&"Result)
    and then
    Vectors."&"Result.Capacity >= Length (Left) + 1;

{AI95-00302-03} Returns a vector comprising the elements of Left followed by the element Right.
function "&" (Left : Element_Type; Right : Vector) return Vector
  with Pre => Length (Right) <= Maximum_Length - 1
  or else raise Constraint_Error,
  Post => Length (Vectors."&"Result) = Length (Right) + 1 and then
      not Tampering_With_Elements_Prohibited (Vectors."&"Result)
      and then
      not Tampering_With_Cursors_Prohibited (Vectors."&"Result)
      and then
      Vectors."&"Result.Capacity >= Length (Right) + 1;

  {AI95-00302-03} Returns a vector comprising the element Left followed by the elements of Right.

function "&" (Left, Right : Element_Type) return Vector
  with Pre => Maximum_Length >= 2 or else raise Constraint_Error,
  Post => Length ("&"Result) = 2 and then
      not Tampering_With_Elements_Prohibited (Vectors."&"Result)
      and then
      not Tampering_With_Cursors_Prohibited (Vectors."&"Result)
      and then
      Vectors."&"Result.Capacity >= 2;

  {AI95-00302-03} Returns a vector comprising the element Left followed by the element Right.

{AI12-0112-1} function Capacity (Container : Vector) return Count_Type
  with Nonblocking, Global => null, Use_Formal => null;

{AI95-00302-03} Returns the capacity of Container.

{AI12-0112-1} procedure Reserve_Capacity (Container : in out Vector;
                                      Capacity : in Count_Type)
  with Pre => not Tampering_With_Cursors_Prohibited (Container)
  or else raise Program_Error,
  Post => Container.Capacity >= Capacity;

  {AI95-00302-03} {AI05-0001-1} {AI05-0264-1} If the capacity of Container is already greater
  than or equal to Capacity, then Reserve Capacity has no effect. Otherwise, Reserve Capacity
  allocates additional storage as necessary to ensure new internal data structures such that the length
  of the resulting vector can become at least the value Capacity without requiring an additional call
  to Reserve Capacity, and is large enough to hold the current length of Container.
  Reserve Capacity then, as necessary, moves copies the elements into the new storagedata
  structures and deallocates any storage no longer neededthe old data structures. Any exception
  raised during allocation is propagated and Container is not modified.

Discussion: Expanding the internal array can be done by allocating a new, longer array, copying the elements, and
deeallocating the original array. This may raise Storage_Error, or cause an exception from a controlled subprogram. We
require that a failed Reserve Capacity does not lose any elements if an exception occurs, but we do not require a
specific order of evaluations or copying.

This routine is used to preallocate the internal array to the specified capacity such that future Inserts do not require
memory allocation overhead. Therefore, the implementation should allocate the needed memory to make that true at
this point, even though the visible semantics could be preserved by waiting until the memory is needed. This doesn't
apply to the indefinite element container, because elements will have to be allocated individually.

The implementation does not have to contract the internal array if the capacity is reduced, as any capacity greater than
or equal to the specified capacity is allowed.

function Length (Container : Vector) return Count_Type
  with Nonblocking, Global => null, Use_Formal => null;

  {AI95-00302-03} Returns the number of elements in Container.
procedure Set_Length (Container : in out Vector;  
   Length    : in  Count_Type)  
   with Pre  => (not Tampering_With_Cursors_Prohibited (Container)  
      or else raise Program_Error) and then  
      (Length <= Maximum_Length or else raise Constraint_Error),  
   Post => Container.Length = Length and then  
      Capacity (Container) >= Length; 

{AI95-00302-03} {AI05-0264-1} If Length is larger than the capacity of Container, Set_Length  
calls Reserve_Capacity (Container, Length), then sets the length of the Container to Length. If  
Length is greater than the original length of Container, empty elements are added to Container;  
otherwise, elements are removed from Container.

Ramification: No elements are moved by this operation; any new empty elements are added at the end. This follows  
from the rules that a cursor continues to designate the same element unless the routine is defined to make the cursor  
ambiguous or invalid; this operation does not do that.

function Is_Empty (Container : Vector) return Boolean  
   with Nonblocking, Global => null, Use Formal => null,  
       Post => Is.Empty'Result = (Length (Container) = 0); 

{AI95-00302-03} {AI12-0112-1} Returns True if Container is empty Equivalent to Length  
(Container) = 0.

procedure Clear (Container : in out Vector)  
   with Pre  => not Tampering_With_Cursors_Prohibited (Container)  
      or else raise Program_Error,  
   Post => Length (Container) = 0; 

{AI95-00302-03} Removes all the elements from Container. The capacity of Container does not  
change.

function To_Cursor (Container : Vector;  
   Index     : Extended_Index) return Cursor  
   with Post => (if Index in  
      First_Index (Container) .. Last_Index (Container)  
      then Has_Element (Container, To_Cursor'Result)  
      else To_Cursor'Result = No_Element),  
      Nonblocking, Global => null, Use Formal => null; 

{AI95-00302-03} {AI12-0112-1} {AI12-0196-1} Returns If Index is not in the range First_Index  
(Container) .. Last_Index (Container), then No_Element is returned. Otherwise, a cursor  
designating the element at position Index in Container; returns No_Element if Index does not  
designate an element is returned. For the purposes of determining whether the parameters overlap  
in a call to To_Cursor, the Container parameter is not considered to overlap with any object  
[including itself].

Reason: {AI12-0196-1} Without the preceding rule, concurrent calls to To_Cursor on the same container would  
interfere by the concurrent call rules in Annex A, since the container object of the concurrent calls would overlap with  
itself. We want these to not interfere, for example to allow the Vector elements to be split into separate “chunks” for  
parallel processing.

function To_Index (Position : Cursor) return Extended_Index  
   with Nonblocking, Global => in all, Use Formal => null; 

{AI95-00302-03} If Position is No_Element, No_Index is returned. Otherwise, the index (within  
its containing vector) of the element designated by Position is returned.

Ramification: This implies that the index is determinable from a bare cursor alone. The basic model is that a vector  
cursor is implemented as a record containing an access to the vector container and an index value. This does constrain  
implementations, but it also allows all of the cursor operations to be defined in terms of the corresponding index  
operation (which should be primary for a vector).
function To_Index (Container : Vector;  
     Position  : Cursor) return Extended_Index  
     with Pre => Position = No_Element  
     or else  
     Has_Element (Container, Position)  
     or else  
     raise Program_Error,  
     Post => 'if Position = No_Element then To_Index'Result = No_Index  
     else To_Index'Result in First_Index (Container) ..  
     Last_Index (Container),  
     Nonblocking, Global => null, Use_Formal => null;  

{AI12-0112-1} Returns the index (within Container) of the element designated by Position;  
returns No_Index if Position does not designate an element. For the purposes of determining  
whether the parameters overlap in a call to To_Index, the Container parameter is not considered  
to overlap with any object [(including itself)].

function Element (Container : Vector;  
     Index     : Index_Type) return Element_Type  
     with Pre => Index in First_Index (Container) .. Last_Index (Container)  
     or else raise Constraint_Error,  
     Nonblocking, Global => null, Use_Formal => Element_Type;  

{AI95-00302-03} {AI12-0112-1} If Index is not in the range First_Index (Container) ..  
Last_Index (Container), then Constraint_Error is propagated. Otherwise, Element returns the  
element at position Index.

function Element (Position  : Cursor) return Element_Type  
     with Pre => Position /= No_Element  
     or else raise Constraint_Error,  
     Nonblocking, Global => in all, Use_Formal => Element_Type;  

{AI95-00302-03} {AI12-0112-1} If If Position equals No_Element, then Constraint_Error is  
propagated. Otherwise, Element returns the element designated by Position.

function Element (Container : Vector;  
     Position  : Cursor) return Element_Type  
     with Pre => (Position /= No_Element  
     or else raise Constraint_Error) and then  
     (Has_Element (Container, Position)  
     or else raise Program_Error),  
     Nonblocking, Global => null, Use_Formal => Element_Type;  

{AI12-0112-1} Element returns the element designated by Position in Container.

procedure Replace_Element (Container : in out Vector;  
     Index     : in Index_Type;  
     New_Item  : in Element_Type)  
     with Pre => (not Tampering_With_Elements_Prohibited (Container)  
     or else raise Program_Error) and then  
     (Index in First_Index (Container) .. Last_Index (Container)  
     or else raise Constraint_Error);  

{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} {AI12-0196-1} If Index is not in the range  
First_Index (Container) .. Last_Index (Container), then Constraint_Error is propagated.  
Otherwise, Replace_Element assigns the value New_Item to the element at position Index. Any  
exception raised during the assignment is propagated. The element at position Index is not an  
empty element after successful call to Replace_Element. For the purposes of determining whether  
the parameters overlap in a call to Replace_Element, the Container parameter is not considered to  
overlap with any object [(including itself)], and the Index parameter is considered to overlap with  
the element at position Index.
procedure Replace_Element (Container : in out Vector;
Position : in Cursor;
New_Item : in Element_Type)
with Pre => (not Tampering_With_Elements_Prohibited(Container)
or else raise Program_Error) and then
(Position /= No_Element
or else raise Constraint_Error) and then
(Has_Element(Container, Position)
or else raise Program_Error);

{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} {AI12-0196-1}
If Position equals No_Element,
then Constraint_Error is propagated; if Position does not designate an element in Container,
then Program_Error is propagated. Otherwise, Replace_Element assigns New_Item to the element
designated by Position. Any exception raised during the assignment is propagated. The element at
Position is not an empty element after successful call to Replace_Element. For the purposes of
determining whether the parameters overlap in a call to Replace_Element, the Container
parameter is not considered to overlap with any object [(including itself)].

Ramification: {AI05-0212-1} Replace_Element, and Update_Element, and Reference are the only ways that an
element can change from empty to nonempty. Also see the note following Update_Element.

procedure Query_Element
(Container : in Vector;
Index : in Index_Type;
Process : not null access procedure (Element : in Element_Type))
with Pre => Index in First_Index(Container) .. Last_Index(Container)
or else raise Constraint_Error;

{AI95-00302-03} {AI05-0265-1} {AI12-0112-1}
If Index is not in the range First_Index(Container) .. Last_Index(Container), then Constraint_Error is propagated. Otherwise,
Query_Element calls Process.all with the element at position Index as the argument.
Tampering_Program_Error is propagated if Process.all tampers with the elements of Container is
prohibited during the execution of the call on Process.all. Any exception raised by Process.all is
propagated.

Reason: {AI05-0005-1} The “tamper with the elements” check is intended to prevent the Element parameter of
Process from being replaced or deleted outside of Process. The check prevents data loss (if Element_Type is
passed by copy) or erroneous execution (if Element_Type is an unconstrained type in an indefinite container).

procedure Query_Element
(Position : in Cursor;
Process : not null access procedure (Element : in Element_Type))
with Pre => Position /= No_Element or else raise Constraint_Error
Global => in all;

{AI95-00302-03} {AI05-0021-1} {AI05-0265-1} {AI12-0112-1}
If Position equals No_Element,
then Constraint_Error is propagated. Otherwise, Query_Element calls Process.all with the element
designated by Position as the argument. Tampering_Program_Error is propagated if Process.all tampers with the elements of the vector that contains the element designated by
Position is prohibited during the execution of the call on Process.all. Container. Any exception
raised by Process.all is propagated.

procedure Query_Element
(Container : in Vector;
Position : in Cursor;
Process : not null access procedure (Element : in Element_Type))
with Pre => (Has_Element(Container, Position)
or else raise Constraint_Error) and then
(has Empty (Container, Position)
or else raise Program_Error);
Query Element calls Process.all with the element designated by Position as the argument. Tampering with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

```
procedure Update_Element
(Container : in out Vector;
Index     : in     Index_Type;
Process   : not null access procedure
           (Element : in out Element_Type));
with Pre  => (Index in First_Index(Container) .. Last_Index(Container)
or else raise Constraint_Error);
```

If Index is not in the range First_Index(Container) .. Last_Index(Container), then Constraint_Error is propagated. Otherwise, Update Element calls Process.all with the element at position Index as the argument. Tampering Program_Error is propagated if Process.all tampers with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

If Element_Type is unconstrained and definite, then the actual Element parameter of Process.all shall be unconstrained.

Ramification: This means that the elements cannot be directly allocated from the heap; it must be possible to change the discriminants of the element in place.

The element at position Index is not an empty element after successful completion of this operation.

Ramification: Since reading an empty element is a bounded error, attempting to use this procedure to replace empty elements may fail. Use Replace Element to do that reliably.

```
procedure Update_Element
(Container : in out Vector;
Position  : in     Cursor;
Process   : not null access procedure
           (Element : in out Element_Type));
with Pre  => (Position /= No_Element
           or else raise Constraint_Error) and then
           (Has_Element(Container, Position)
or else raise Program_Error);
```

If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Update Element calls Process.all with the element designated by Position as the argument. Tampering Program_Error is propagated if Process.all tampers with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

If Element_Type is unconstrained and definite, then the actual Element parameter of Process.all shall be unconstrained.

The element designated by Position is not an empty element after successful completion of this operation.

```
type Constant_Reference_Type
  (Element : not null access constant Element_Type)
is private
with Implicit_Dereference => Element,
Nonblocking, Global => in out synchronized,
Default_Initial_Condition => (raise Program_Error);
```
type Reference_Type (Element : not null access Element_Type) is
private
with Implicit_Dereference => Element,
Nonblocking, Global => in out synchronized,
Default_Initial_Condition => (raise Program_Error);

The types Constant_Reference_Type and Reference_Type need finalization.

This paragraph was deleted.

The default initialization of an object of type Constant_Reference_Type or Reference_Type propagates Program_Error.

Reason: It is expected that Reference_Type (and Constant_Reference_Type) will be a controlled type, for which
finalization will have some action to terminate the tampering check for the associated container. If the object is created
by default, however, there is no associated container. Since this is useless, and supporting this case would take extra
work, we define it to raise an exception.

function Constant_Reference (Container : aliased in Vector; Index : in Index_Type)
return Constant_Reference_Type
with Pre => Index in First_Index (Container) .. Last_Index (Container)
or else raise Constraint_Error,
Post => Tampering_With_Cursors_Prohibited (Container),
Nonblocking, Global => null, Use_Formal => null;

This function (combined with the Constant_Indexing and Implicit_Dereference aspects) provides a convenient way to gain read access to an individual
element of a vector given an index value.

If Index is not in the range First_Index (Container) .. Last_Index (Container), then Constraint_Error is propagated. Otherwise,
Constant_Reference returns an object whose discriminant is an access value that designates the element at position Index. Tampering with the elements of Container is prohibited while the
object returned by Constant_Reference exists and has not been finalized.

function Reference (Container : aliased in out Vector; Index : in Index_Type)
return Reference_Type
with Pre => Index in First_Index (Container) .. Last_Index (Container)
or else raise Constraint_Error,
Post => Tampering_With_Cursors_Prohibited (Container),
Nonblocking, Global => null, Use_Formal => null;

This function (combined with the Variable_Indexing and Implicit_Dereference aspects) provides a convenient way to gain read and write access to an
individual element of a vector given an index value.

If Index is not in the range First_Index (Container) .. Last_Index (Container), then Constraint_Error is propagated. Otherwise,
Reference returns an object whose discriminant is an access value that designates the element at position Index. Tampering with the elements of Container is prohibited while the object returned by Reference exists and has not been finalized.

The element at position Index is not an empty element after successful completion of this operation.
function Constant_Reference (Container : aliased in Vector; Position : in Cursor)
return Constant_Reference_Type
with Pre  => (Position /= No_Element
or else raise Constraint_Error) and then
(Has_Element (Container, Position)
or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container),
Nonblocking, Global => null, Use_Formal => null;

This function (combined with the Constant Indexing and Implicit Dereference aspects) provides a convenient way to gain read access to an individual element of a vector given a cursor.

If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Constant_Reference returns an object whose discriminant is an access value that designates the element designated by Position. Tampering with the elements of Container is prohibited while the object returned by Constant_Reference exists and has not been finalized.

function Reference (Container : aliased in out Vector; Position : in Cursor)
return Reference_Type
with Pre  => (Position /= No_Element
or else raise Constraint_Error) and then
(Has_Element (Container, Position)
or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container),
Nonblocking, Global => null, Use_Formal => null;

This function (combined with the Variable Indexing and Implicit Dereference aspects) provides a convenient way to gain read and write access to an individual element of a vector given a cursor.

If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Reference returns an object whose discriminant is an access value that designates the element designated by Position. Tampering with the elements of Container is prohibited while the object returned by Reference exists and has not been finalized.

The element designated by Position is not an empty element after successful completion of this operation.

procedure Assign (Target : in out Vector; Source : in Vector)
with Pre  => not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error,
Post => Length (Source) = Length (Target) and then
Capacity (Target) >= Length (Target);

If Target denotes the same object as Source, the operation has no effect. If the length of Source is greater than the capacity of Target, Reserve_Capacity (Target, Length (Source)) is called. The elements of Source are then copied to Target as for an assignment_statement assigning Source to Target (this includes setting the length of Target to be that of Source).

Discussion: This routine exists for compatibility with the bounded vector container. For an unbounded vector, Assign (A, B) and A := B behave identically. For a bounded vector, := will raise an exception if the container capacities are different, while Assign will not raise an exception if there is enough room in the target.
function Copy (Source : Vector; Capacity : Count_Type := 0)
   return Vector
with Pre => Capacity = 0 or else Capacity >= Length(Source)
   or else raise Capacity_Error,
   Post => Length(Copy'Result) = Length(Source) and then
      not Tampering_With_Elements_Prohibited(Copy'Result)
      and then
      not Tampering_With_Cursors_Prohibited(Copy'Result)
      and then
      Copy'Result.Capacity >= (if Capacity = 0 then
                                Length(Source) else Capacity)
      {AI05-0001-1} {AI12-0112-1} Returns a vector whose elements are initialized from the
corresponding elements of Source. If Capacity is 0, then the vector capacity is the length
of Source; if Capacity is equal to or greater than the length of Source, the vector capacity is at least
the specified value. Otherwise, the operation propagates Capacity_Error.

procedure Move (Target : in out Vector; Source : in out Vector)
with Pre => (not Tampering_With_Cursors_Prohibited(Target)
            or else raise Program_Error)
            and then
            (not Tampering_With_Cursors_Prohibited(Source)
            or else raise Program_Error),
            Post => (if not Target'Has_Same_Storage(Source) then
                       Length(Target) = Length(Source)'Old and then
                       Length(Source) = 0 and then
                       Capacity(Target) >= Length(Source)'Old)
            {AI95-00302-03} {AI05-0001-1} {AI05-0248-1} {AI12-0112-1} If Target denotes the same
object as Source, then the operation Move has no effect. Otherwise, Move first calls
Reserve_Capacity(Target, Length(Source)) and then Clear(Target); then, each element from
Source is removed from Source and inserted into Target in the original order. The length of
Source is 0 after a successful call to Move.

Discussion: The idea is that the internal array is removed from Source and moved to Target. (See the Implementation
Advice for Move). If Capacity(Target) /= 0, the previous internal array may need to be deallocated. We don't mention
this explicitly, because it is covered by the "no memory loss" Implementation Requirement.

procedure Insert_VectorInsert (Container : in out Vector;
                              Before    : in Extended_Index;
                              New_Item  : in Vector)
with Pre => (not Tampering_With_Cursors_Prohibited(Container)
            or else raise Program_Error)
            and then
            (Before in First_Index(Container) .. Last_Index(Container) + 1
            or else raise Constraint_Error) and then
            (Length(Container) <= Maximum_Length - Length(New_Item)
            or else raise Constraint_Error),
            Post => Length(Container)'Old + Length(New_Item) =
                    Length(Container) and then
                    Capacity(Container) >= Length(Container)
            {AI95-00302-03} {AI05-0264-1} {AI12-0112-1} {AI12-0400-1} If Before is not in the range
First_Index(Container) .. Last_Index(Container) + 1, then Constraint_Error is propagated. If
Length(New Item) is 0, then Insert_VectorInsert does nothing. Otherwise, it computes the new
length NL as the sum of the current length and Length(New Item); if the value of Last
appropriate for length NL would be greater than Index_Type'Last, then Constraint Error is
propagated.

{AI12-0400-1} If the current vector capacity is less than NL, Reserve_Capacity(Container, NL) is
called to increase the vector capacity. Then Insert_VectorInsert slides the elements in the range
Before .. Last Index(Container) up by Length(New Item) positions, and then copies the
elements of New_Item to the positions starting at Before. Any exception raised during the copying is propagated.

**Ramification:** Moving the elements does not necessarily involve copying. Similarly, since Reserve Capacity does not require the copying of elements, it does not need to be explicitly called (the implementation can combine the operations if it wishes to).

```ada
procedure Insert_VectorInsert (Container : in out Vector;
                             Before    : in     Cursor;
                             New_Item  : in     Vector)
with Pre => (not Tampering With Cursors Prohibited (Container)
          or else raise Program Error) and then
          (Before = No_Element or else
           Has Element (Container, Before)
          or else raise Program Error) and then
          (Length (Container) <= Maximum Length - Length (New_Item)
          or else raise Constraint Error),
        Post => Length (Container)'Old + Length (New_Item) =
               Length (Container) and then
               Capacity (Container) >= Length (Container);
```

**Discussion:** The messy wording is needed because Before is invalidated by Insert VectorInsert, and we don't want Position to be invalid after this call. An implementation probably only needs to copy Before to Position.
{AI12-0112-1} procedure Insert (Container : in out Vector;
    Before    : in   Extended_Index;
    New_Item  : in   Element_Type;
    Count     : in   Count_Type := 1)
    with Pre => (not Tampering_With_Cursors_Prohibited (Container)
                 or else raise Program_Error) and then
                (Before in First_Index (Container) .. Last_Index (Container) + 1
                 or else raise Constraint_Error),
                 Post => Length (Container)'Old + Count = Length (Container)
                and then
                Capacity (Container) >= Length (Container);
{AI95-00302-03} Equivalent to Insert (Container, Before, To_Vector (New_Item, Count));

{AI12-0112-1} procedure Insert (Container : in out Vector;
    Before    : in   Cursor;
    New_Item  : in   Element_Type;
    Count     : in   Count_Type := 1)
    with Pre => (not Tampering_With_Cursors_Prohibited (Container)
                 or else raise Program_Error) and then
                (Before = No_Element or else
                Has_Element (Container, Before)
                or else raise Program_Error) and then
                (Length (Container) <= Maximum_Length - Count
                or else raise Constraint_Error),
                Post => Length (Container)'Old + Count = Length (Container)
                and then
                Capacity (Container) >= Length (Container);
{AI95-00302-03} Equivalent to Insert (Container, Before, To_Vector (New_Item, Count));

{AI12-0112-1} procedure Insert (Container : in out Vector;
    Before    : in   Cursor;
    New_Item  : in   Element_Type;
    Position  : out  Cursor;
    Count     : in   Count_Type := 1)
    with Pre => (not Tampering_With_Cursors_Prohibited (Container)
                 or else raise Program_Error) and then
                (Before = No_Element or else
                Has_Element (Container, Before)
                or else raise Program_Error) and then
                (Length (Container) <= Maximum_Length - Count
                or else raise Constraint_Error),
                Post => Length (Container)'Old + Count = Length (Container)
                and then
                Has_Element (Container, Position) and then
                Capacity (Container) => Length (Container);
{AI95-00302-03} Equivalent to Insert (Container, Before, To Vector (New Item, Count),
    Position);

Ramification: {AI05-0257-1} If Count equals 0, Position will designate the element designated by Before, rather than
a newly inserted element. Otherwise, Position will designate the first newly inserted element.
procedure Insert (Container : in out Vector;
Before    : in   Extended_Index;
Count     : in   Count_Type := 1)
with Pre => (not Tampering_With.Cursors.Prohibited (Container)
or else raise Program_Error) and then
(Before in First_Index (Container) .. Last_Index (Container) + 1 or else raise Constraint_Error)
and then (Length (Container) <= Maximum_Length - Count or else raise Constraint_Error)
and then (Length (Container)'Old + Count = Length (Container) and then Capacity (Container) >= Length (Container));

{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} If Before is not in the range First_Index (Container) .. Last_Index (Container) + 1, then Constraint_Error is propagated. If Count is 0, then Insert does nothing. Otherwise, it computes the new length $NL$ as the sum of the current length and Count; if the value of Last appropriate for length $NL$ would be greater than Index_Type'Last, then Constraint_Error is propagated.

If the current vector capacity is less than $NL$, Reserve_Capacity (Container, $NL$) is called to increase the vector capacity. Then Insert slides the elements in the range Before .. Last_Index (Container) up by Count positions, and then inserts elements that are initialized by default (see 3.3.1) in the positions starting at Before.

procedure Insert (Container : in out Vector;
Before    : in   Cursor;
Position  : out Cursor;
Count     : in   Count_Type := 1)
with Pre => (not Tampering_With.Cursors.Prohibited (Container)
or else raise Program_Error) and then (Before = No_Element or else Has_Element (Container, Before) or else raise Program_Error)
and then (Length (Container) <= Maximum_Length - Count or else raise Constraint_Error)
and then (Length (Container)'Old + Count = Length (Container) and then Has_Element (Container, Position) and then Capacity (Container) >= Length (Container));

{AI95-00302-03} {AI12-0112-1} If Before is not No_Element, and does not designate an element in Container, then Program_Error is propagated. If Before equals No_Element, then let $T$ be Last_Index (Container) + 1; otherwise, let $T$ be To_Index (Before). Insert (Container, $T$, Count) is called, and then Position is set to To_Cursor (Container, $T$).

Reason: This routine exists mainly to ease conversion between Vector and List containers. Unlike Insert_Space, this routine default initializes the elements it inserts, which can be more expensive for some element types.

procedure Prepend_VectorPrepend (Container : in out Vector;
New_Item  : in   Vector;
Count     : in   Count_Type := 1)
with Pre => (not Tampering_With.Cursors.Prohibited (Container)
or else raise Program_Error) and then (Length (Container) <= Maximum_Length - Length (New_Item) or else raise Constraint_Error),
Post => Length (Container)'Old + Length (New_Item) = Length (Container) and then Capacity (Container) >= Length (Container);

{AI95-00302-03} Equivalent to Insert (Container, First_Index (Container), New_Item).
procedure Prepend (Container: in out Vector;
New_Item: in Element_Type;
Count: in Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Maximum Length - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count = Length (Container) and then
Capacity (Container) >= Length (Container);

{AI95-00302-03} Equivalent to Insert (Container, First Index (Container), New Item, Count).

procedure Append_VectorAppend (Container: in out Vector;
New_Item: in Vector)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error)
and then
(Length (Container) <= Maximum Length - Length (New_Item)
or else raise Constraint_Error),
Capacity (Container) >= Length (Container);

{AI95-00302-03} Equivalent to Insert (Container, Last Index (Container) + 1, New Item).

procedure Append (Container: in out Vector;
New_Item: in Element_Type;
Count: in Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Maximum Length - 1
or else raise Constraint_Error),
Capacity (Container) >= Length (Container);

{AI95-00302-03} Equivalent to Insert (Container, Last Index (Container) + 1, New Item, Count).

procedure Append (Container: in out Vector;
New_Item: in Element_Type)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error)
and then
(Length (Container) <= Maximum Length - 1
or else raise Constraint_Error),
Capacity (Container) >= Length (Container);

{AI12-0112-1} {AI12-0121-2} {AI12-0400-1} Equivalent to Insert (Container, Last Index (Container) + 1, New Item, 1).

procedure Insert_Space (Container: in out Vector;
Before: in Extended_Index;
Count: in Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error)
and then
(Before in First Index (Container) .. Last Index (Container) + 1
or else raise Constraint_Error)
and then
(Length (Container) <= Maximum Length - Count
or else raise Constraint_Error),
Capacity (Container) >= Length (Container);

{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} If Before is not in the range First Index (Container) .. Last Index (Container) + 1, then Constraint_Error is propagated. If Count is 0, then Insert Space does nothing. Otherwise, it computes the new length NL as the sum of the current
length and Count; if the value of Last appropriate for length \( NL \) would be greater than \( \text{Index Type'Last} \), then Constraint_Error is propagated.

If the current vector capacity is less than \( NL \), Reserve Capacity \((\text{Container, NL})\) is called to increase the vector capacity. Then Insert Space slides the elements in the range Before .. Last Index \((\text{Container})\) up by Count positions, and then inserts empty elements in the positions starting at Before.

```ada
procedure Insert_Space (Container : in out Vector;
                        Before    : in    Cursor;
                        Position  : out   Cursor;
                        Count     : in    Count_Type := 1)
    with Pre => (not Tampering With Cursors_Prohibited (Container)
                    or else raise Program_Error) and then
                (Before = No Element or else
                    Has Element (Container, Before).
                    or else raise Program_Error) and then
                (Length (Container) <= Maximum Length - Count
                    or else raise Constraint_Error),
        Post => Length (Container)'Old + Count = Length (Container) and then
                Has Element (Container, Position) and then
                Capacity (Container) >= Length (Container);
{AI95-00302-03} {AI12-0112-1} If Before is not No_Element, and does not designate an element in Container, then Program_Error is propagated. If Before equals No_Element, then let \( T \) be Last Index \((\text{Container})\) + 1; otherwise, let \( T \) be To_Index \((\text{Before})\). Insert Space \((\text{Container, T, Count})\) is called, and then Position is set to To_Cursor \((\text{Container, T})\).
```

```ada
procedure Delete (Container : in out Vector;
                 Index     : in    Extended_Index;
                 Count     : in    Count_Type := 1)
    with Pre => (not Tampering With Cursors_Prohibited (Container)
                    or else raise Program_Error) and then
                (Index in First_Index (Container) .. Last_Index (Container) + 1
                    or else raise Constraint_Error),
        Post => Length (Container)'Old - Count <= Length (Container);
{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} If Index is not in the range First_Index \((\text{Container})\) .. Last_Index \((\text{Container})\) + 1, then Constraint_Error is propagated. If Count is 0, Delete has no effect. Otherwise, Delete slides the elements (if any) starting at position Index + Count down to Index. Any exception raised during element assignment is propagated.
```

Ramification: If Index + Count >= Last_Index\((\text{Container})\), this effectively truncates the vector (setting Last_Index to \( \text{Index} - \text{Index Type'First} \) and consequently sets Length to Index – 1).

```ada
procedure Delete (Container : in out Vector;
                 Position  : in out Cursor;
                 Count     : in    Count_Type := 1)
    with Pre => (not Tampering With Cursors_Prohibited (Container)
                    or else raise Program_Error) and then
                (Position /= No Element
                    or else raise Constraint_Error) and then
                (Has Element (Container, Position)
                    or else raise Program_Error),
        Post => Length (Container)'Old - Count <= Length (Container)
                and then Position = No_Element;
{AI95-00302-03} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated. If Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Delete \((\text{Container, To_Index (Position), Count})\) is called, and then Position is set to No_Element.
```
procedure Delete_First (Container : in out Vector; Count : in Count_Type := 1)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Length (Container)'Old - Count <= Length (Container);

{AI95-00302-03} Equivalent to Delete (Container, First_Index (Container), Count).

procedure Delete_Last (Container : in out Vector; Count : in Count_Type := 1)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Length (Container)'Old - Count <= Length (Container);

{AI95-00302-03} {AI05-0264-1} If Length (Container) <= Count, then Delete_Last is equivalent to Clear (Container). Otherwise, it is equivalent to Delete (Container, Index_Type'Val(Index_Type'Pos(Last_Index (Container)) – Count + 1), Count).

procedure Reverse_Elements (Container : in out VectorList)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error;

{AI95-00302-03} Reorders the elements of Container in reverse order.

Discussion: This can copy the elements of the vector — all cursors referencing the vector are ambiguous afterwards and may designate different elements afterwards.

procedure Swap (Container : in out Vector; I, J : in Index_Type)
with Pre => (not Tampering_With_Elements_Prohibited (Container)
or else raise Program_Error) and then
(I in First_Index (Container) .. Last_Index (Container)
or else raise Constraint_Error) and then
(J in First_Index (Container) .. Last_Index (Container)
or else raise Constraint_Error);

{AI95-00302-03} {AI12-0112-1} If either I or J is not in the range First_Index (Container) .. Last_Index (Container), then Constraint_Error is propagated. Otherwise, Swap exchanges the values of the elements at positions I and J.

To be honest: The implementation is not required to actually copy the elements if it can do the swap some other way. But it is allowed to copy the elements if needed.

procedure Swap (Container : in out Vector; I, J : in Cursor)
with Pre => (not Tampering_With_Elements_Prohibited (Container)
or else raise Program_Error) and then
(I /= No_Element or else Constraint_Error) and then
(J /= No_Element or else Constraint_Error) and then
(Has_Element (Container, I)
or else raise Program_Error) and then
(Has_Element (Container, J)
or else raise Program_Error);

{AI95-00302-03} {AI12-0112-1} If either I or J is No_Element, then Constraint_Error is propagated. If either I or J do not designate an element in Container, then Program_Error is propagated. Otherwise, Swap exchanges the values of the elements designated by I and J.

Ramification: After a call to Swap, I designates the element value previously designated by J, and J designates the element value previously designated by I. The cursors do not become ambiguous from this operation.

To be honest: The implementation is not required to actually copy the elements if it can do the swap some other way. But it is allowed to copy the elements if needed.
function First_Index (Container : Vector) return Index_Type
with Nonblocking, Global => null, Use Formal => null,
Post => First_Index'Result = Index_Type'First;

Returns the value Index_Type'First.

Discussion: We'd rather call this “First”, but then calling most routines in here with First (Some_Vect) would be ambiguous.

function First (Container : Vector) return Cursor
with Nonblocking, Global => null, Use Formal => null,
Post => (if not Is_Empty (Container)
then Has_Element (Container, First'Result)
else First'Result = No_Element);

If Container is empty, First returns No_Element. Otherwise, it returns a cursor that designates the first element in Container.

function First_Element (Container : Vector) return Element_Type
with Pre => (not Is_Empty (Container)
or else raise Constraint_Error);

Equivalent to Element (Container, First_Index (Container)).

function Last_Index (Container : Vector) return Extended_Index
with Nonblocking, Global => null, Use Formal => null,
Post => (if Length (Container) = 0 then Last_Index'Result = No_Index
else Count_Type(Last_Index'Result - Index_Type'First) =
Length (Container) - 1);

If Container is empty, Last_Index returns No_Index. Otherwise, it returns the position of the last element in Container.

function Last (Container : Vector) return Cursor
with Nonblocking, Global => null, Use Formal => null,
Post => (if not Is_Empty (Container)
then Has_Element (Container, Last'Result)
else Last'Result = No_Element);

If Container is empty, Last returns No_Element. Otherwise, it returns a cursor that designates the last element in Container.

function Last_Element (Container : Vector) return Element_Type
with Pre => (not Is_Empty (Container)
or else raise Constraint_Error);

Equivalent to Element (Container, Last_Index (Container)).

function Next (Position : Cursor) return Cursor
with Nonblocking, Global => in all, Use Formal => null,
Post => (if Position = No_Element then Next'Result = No_Element);

If Position equals No_Element or designates the last element of the container, then Next returns the value No_Element. Otherwise, it returns a cursor that designates the element with index To_Index (Position) + 1 in the same vector as Position.
function Next (Container : Vector;  
  Position : Cursor) return Cursor 
with Nonblocking, Global => null, Use Formal => null,  
  Pre => Position = No Element or else  
    Has Element (Container, Position)  
  or else raise Program_Error,  
  Post => (if Position = No Element then Next'Result = No Element  
    elsif Has_Element (Container, Next'Result) then  
      To_Index (Container, Next'Result) =  
      To_Index (Container, Position) + 1  
    elsif Next'Result = No Element then  
      Position = Last (Container)  
    else False);  
  
{AI12-0112-1} Returns a cursor designating the next element in Container, if any.

procedure Next (Position : in out Cursor) 
with Nonblocking, Global => in all, Use Formal => null;  
{AI95-00302-03} Equivalent to Position := Next (Position).

procedure Next (Container : in Vector;  
  Position : in out Cursor)  
with Nonblocking, Global => null, Use Formal => null,  
  Pre => Position = No Element or else  
    Has Element (Container, Position)  
  or else raise Program_Error,  
  Post => (if Position /= No_Element  
    then Has_Element (Container, Position));  
{AI12-0112-1} Equivalent to Position := Next (Container, Position).

function Previous (Position : Cursor) return Cursor 
with Nonblocking, Global => in all, Use Formal => null,  
  Post => (if Position = No_Element then Previous'Result = No_Element  
    then Previous'Result = No_Element  
    elsif Has_Element (Container, Previous'Result) then  
      To_Index (Container, Previous'Result) =  
      To_Index (Container, Position) - 1  
    elsif Previous'Result = No_Element then  
      Position = First (Container)  
    else False);  
  
{AI95-00302-03} If Position equals No_Element or designates the first element of the container, 
then Previous returns the value No_Element. Otherwise, it returns a cursor that designates the 
element with index To_Index (Position) – 1 in the same vector as Position.

function Previous (Container : Vector;  
  Position : Cursor) return Cursor  
with Nonblocking, Global => null, Use Formal => null,  
  Pre => Position = No Element or else  
    Has Element (Container, Position)  
  or else raise Program_Error,  
  Post => (if Position = No_Element then Previous'Result = No_Element  
    elsif Has_Element (Container, Previous'Result) then  
      To_Index (Container, Previous'Result) =  
      To_Index (Container, Position) - 1  
    elsif Previous'Result = No_Element then  
      Position = First (Container)  
    else False);  
  
{AI12-0112-1} Returns a cursor designating the previous element in Container, if any.

procedure Previous (Position : in out Cursor) 
with Nonblocking, Global => in all, Use Formal => null;  
{AI95-00302-03} Equivalent to Position := Previous (Position).
procedure Previous (Container : in Vector;
  Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
  Pre => Position = No_Element or else
    Has_Element (Container, Position)
  or else raise Program_Error,
  Post => (if Position /= No_Element
    then Has_Element (Container, Position));

{AI12-0112-1} Equivalent to Position := Previous (Container, Position).

function Find_Index (Container : Vector;
  Item      : Element_Type;
  Index     : Index_Type := Index_Type'First)
return Extended_Index;

{AI95-00302-03} Searches the elements of Container for an element equal to Item (using the
generic formal equality operator). The search starts at position Index and proceeds towards
Last_Index (Container). If no equal element is found, then Find_Index returns No_Index.
Otherwise, it returns the index of the first equal element encountered.

function Find (Container : Vector;
  Item      : Element_Type;
  Position  : Cursor := No_Element)
return Cursor
with Pre => Position = No_Element or else
  Has_Element (Container, Position)
  or else raise Program_Error,
  Post => (if Find'Result /= No_Element
    then Has_Element (Container, Find'Result));

{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} If Position is not No_Element, and does not
designate an element in Container, then Program_Error is propagated. Otherwise, Find searches
the elements of Container for an element equal to Item (using the generic formal equality
operator). The search starts at the first element if Position equals No_Element, and at the element
designated by Position otherwise. It proceeds towards the last element of Container. If no equal
element is found, then Find returns No_Element. Otherwise, it returns a cursor designating the
first equal element encountered.

function Reverse Find_Index (Container : Vector;
  Item      : Element_Type;
  Index     : Index_Type := Index_Type'Last)
return Extended_Index;

{AI95-00302-03} Searches the elements of Container for an element equal to Item (using the
generic formal equality operator). The search starts at position Index or, if Index is greater than
Last_Index (Container), at position Last_Index (Container). It proceeds towards First_Index
(Container). If no equal element is found, then Reverse Find Index returns No_Index.
Otherwise, it returns the index of the first equal element encountered.

function Reverse Find (Container : Vector;
  Item      : Element_Type;
  Position  : Cursor := No_Element)
return Cursor
with Pre => Position = No_Element or else
  Has_Element (Container, Position)
  or else raise Program_Error,
  Post => (if Reverse_Find'Result /= No_Element
    then Has_Element (Container, Reverse_Find'Result));

{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} If Position is not No_Element, and does not
designate an element in Container, then Program_Error is propagated. Otherwise, Reverse Find
searches the elements of Container for an element equal to Item (using the generic formal equality
operator). The search starts at the last element if Position equals No_Element, and at the element
designated by Position otherwise. It proceeds towards the first element of Container. If no equal
element is found, then Reverse_Find returns No_Element. Otherwise, it returns a cursor
designating the first equal element encountered.

function Contains (Container : Vector;  
    Item      : Element_Type) return Boolean;

{AI95-00302-03} Equivalent to Has_Element (Find (Container, Item)).

function Has_Element (Position : Cursor) return Boolean;

{AI95-00302-03} {AI05-0212-1} Returns True if Position designates an element, and returns
False otherwise.

To be honest: {AI05-0212-1} This function may not detect cursors that designate deleted elements; such cursors are
invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

Paragraphs 225 and 226 were moved above.

{AI12-0112-1} procedure Iterate  
    (Container : in Vector;  
    Process   : not null access procedure (Position : in Cursor))

{AI95-00302-03} {AI05-0265-1} Invokes Process.all with a cursor that designates each element
in Container, in index order. TamperingProgram_Error is propagated if Process.all tampers with
the cursors of Container is prohibited during the execution of a call on Process.all. Any exception
raised by Process.all is propagated.

Discussion: The purpose of the “tamper with the cursors” check is to prevent erroneous execution from the Position
parameter of Process.all becoming invalid. This check takes place when the operations that tamper with the cursors of
the container are called. The check cannot be made later (say in the body of Iterate), because that could cause the
Position cursor to be invalid and potentially cause execution to become erroneous -- defeating the purpose of the
check.

There is no check needed if an attempt is made to insert or delete nothing (that is, Count = 0 or Length(Item) = 0).

{AI12-0112-1} procedure Reverse_Iterate  
    (Container : in Vector;  
    Process   : not null access procedure (Position : in Cursor))

{AI95-00302-03} {AI05-0212-1} Iterates over the elements in Container as per procedure Iterate,
except that elements are traversed in reverse index order.

{AI05-0212-1} {AI05-0265-1} {AI05-0269-1} {AI12-0266-1} Iterate returns a reversible
iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating
each node in Container, starting with the first node and moving the cursor as per the Next
function when used as a forward iterator, and starting with the last node and moving the cursor
as per the Previous function when used as a reverse iterator, and processing all nodes concurrently
when used as a parallel iterator. Tampering with the cursors of Container is prohibited while the
iterator object exists (in particular, in the sequence of statements of the loop statement
whose iterator_specification denotes this object). The iterator object needs finalization.
```ada
function Iterate (Container : in Vector; Start : in Cursor)
return Vector_Iterator_Interfaces.Reversible_Iterator'Class
with Pre    => (Start /= No_Element
or else raise Constraint_Error) and then
               (Has_Element (Container, Start)
or else raise Program_Error),
               Post   => Tampering_With_Cursors_Prohibited (Container);
{AI05-0212-1} {AI05-0262-1} {AI05-0265-1} {AI05-0269-1} {AI12-0212-1} If Start is not
No_Element and does not designate an item in Container, then Program_Error is propagated. If
Start is No_Element, then Constraint_Error is propagated. Otherwise, Iterate returns a reversible
iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating
each node in Container, starting with the node designated by Start and moving the cursor as per
the Next function when used as a forward iterator, or moving the cursor as per the Previous
function when used as a reverse iterator. Tampering with the cursors of Container is prohibited
while the iterator object exists (in particular, in the sequence of statements of the
loop_statement whose iterator_specification denotes this object). The iterator object needs
finalization.

Discussion: Exits are allowed from the loops created using the iterator objects. In particular, to stop the iteration at a
particular cursor, just add
   exit when Cur = Stop;
in the body of the loop (assuming that Cur is the loop parameter and Stop is the cursor that you want to stop at).

{AI05-0044-1} {AI05-0262-1} The actual function for the generic formal function "<" of
Generic_Sorting is expected to return the same value each time it is called with a particular pair of
element values. It should define a strict weak ordering relationship (see A.18), that is, be irreflexive,
asymmetric, and transitive; it should not modify Container. If the actual for "<" behaves in some other
manner, the behavior of the subprograms of Generic_Sorting are unspecified. The number ofHow many
times the subprograms of Generic_Sorting call "<" is unspecified.

function Is_Sorted (Container : Vector) return Boolean;
{AI95-00302-03} Returns True if the elements are sorted smallest first as determined by the
generic formal "<" operator; otherwise, Is_Sorted returns False. Any exception raised during
evaluation of "<" is propagated.

{AI12-0112-1} procedure Sort (Container : in out Vector)
with Pre  => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error;
{AI95-00302-03} Reorders the elements of Container such that the elements are sorted smallest
first as determined by the generic formal "<" operator provided. Any exception raised during
evaluation of "<" is propagated.

Ramification: This implies swapping the elements, usually including an intermediate copy. This means that the
elements will usually be copied. (As with Swap, if the implementation can do this some other way, it is allowed to.)
Since the elements are nonlimited, this usually will not be a problem. Note that there is Implementation Advice below
that the implementation should use a sort that minimizes copying of elements.

The sort is not required to be stable (and the fast algorithm required will not be stable). If a stable sort is needed, the
user can include the original location of the element as an extra "sort key". We considered requiring the
implementation to do that, but it is mostly extra overhead -- usually there is something already in the element that
provides the needed stability.
```
procedure Merge (Target : in out Vector;
Source : in out Vector)
with Pre => (not Tampering_With_Cursors_Prohibited (Target)
  or else raise Program_Error) and then
  (not Tampering_With_Cursors_Prohibited (Source)
  or else raise Program_Error) and then
  (Length (Target) <= Maximum Length - Length (Source)
  or else raise Constraint_Error) and then
  ((Length (Source) = 0 or else
    not Target'Has_Same_Storage (Source))
  or else raise Program_Error),
  Post => (declare
    Result_Length : constant Count_Type :=
    Length (Source)'Old + Length (Target)'Old;
    begin
      Length (Source) = 0 and then
      Length (Target) = Result_Length and then
      Capacity (Target) >= Result_Length));

{AI95-00302-03} {AI05-0021-1} {AI12-0112-1} If Source is empty, then Merge does nothing. If Source and Target are the same nonempty container object, then Program_Error is propagated. Otherwise, Merge removes elements from Source and inserts them into Target; afterwards, Target contains the union of the elements that were initially in Source and Target; Source is left empty. If Target and Source are initially sorted smallest first, then Target is ordered smallest first as determined by the generic formal "<" operator; otherwise, the order of elements in Target is unspecified. Any exception raised during evaluation of "<" is propagated.

Discussion: It is a bounded error if either of the vectors is unsorted, see below. The bounded error can be recovered by sorting Target after the merge call, or the vectors can be pretested with Is_Sorted.

Implementation Note: The Merge operation will usually require copying almost all of the elements. One implementation strategy would be to extend Target to the appropriate length, then copying elements from the back of the vectors working towards the front. An alternative approach would be to allocate a new internal data array of the appropriate length, copy the elements into it in an appropriate order, and then replacing the data array in Target with the temporary.

{AI12-0111-1} The nested package Vectors.Stable provides a type Stable.Vector that represents a stable vector, which is one that cannot grow and shrink. Such a vector can be created by calling the To_Vector or Copy functions, or by establishing a stabilized view of an ordinary vector.

{AI12-0111-1} The subprograms of package Containers.Vectors that have a parameter or result of type Vector are included in the nested package Stable with the same specification, except that the following are omitted:

{AI12-0111-1} {AI12-0400-1} Tampering_With_Cursors_Prohibited, Tampering_With_Elements_Prohibited, Reserve_Capacity, Assign, Move, Insert, Insert_Space, Insert_Vector, Append, Append_Vector, Prepend, Prepend_Vector, Clear, Delete, Delete_First, Delete_Last, and Set_Length

The generic package Generic_Sorting is also included with the same specification, except that Merge is omitted.

Ramification: The names Vector and Cursor mean the types declared in the nested package in these subprogram specifications.

Reason: The omitted routines are those that tamper with cursors or elements (or test that state). The model is that it is impossible to tamper with cursors or elements of a stable view since no such operations are included. Thus tampering checks are not needed for a stable view, and we omit the operations associated with those checks.

{AI12-0111-1} The operations of this package are equivalent to those for ordinary vectors, except that the calls to Tampering_With_Cursors_Prohibited and Tampering_With_Elements_Prohibited that occur in preconditions are replaced by False, and any that occur in postconditions are replaced by True.
If a stable vector is declared with the Base discriminant designating a pre-existing ordinary vector, the stable vector represents a stabilized view of the underlying ordinary vector, and any operation on the stable vector is reflected on the underlying ordinary vector. While a stabilized view exists, any operation that tampers with elements performed on the underlying vector is prohibited. The finalization of a stable vector that provides such a view removes this restriction on the underlying ordinary vector [(though some other restriction can exist due to other concurrent iterations or stabilized views)].

If a stable vector is declared without specifying Base, the object is necessarily initialized. The initializing expression of the stable vector, [typically a call on To_Vector or Copy], determines the Length of the vector. The Length of a stable vector never changes after initialization.

Proof: Initialization is required as the type is indefinite, see 3.3.1.

## Bounded (Run-Time) Errors

Reading the value of an empty element by calling Element, Query_Element, Update_Element, Constant_Reference, Reference, Swap, Is_Sorted, Sort, Merge, "=". Find, or Reverse_Find is a bounded error. The implementation may treat the element as having any normal value (see 13.9.1) of the element type, or raise Constraint_Error or Program_Error before modifying the vector.

Ramification: For instance, a default initialized element could be returned. Or some previous value of an element. But returning random junk is not allowed if the type has default initial value(s).

Assignment and streaming of empty elements are not bounded errors. This is consistent with regular composite types, for which assignment and streaming of uninitialized components do not cause a bounded error, but reading the uninitialized component does cause a bounded error.

There are other operations which are defined in terms of the operations listed above.

Calling Merge in an instance of Generic_Sorting with either Source or Target not ordered smallest first using the provided generic formal "<" operator is a bounded error. Either Program_Error is raised after Target is updated as described for Merge, or the operation works as defined.

It is a bounded error for the actual function associated with a generic formal subprogram, when called as part of an operation of this package, to tamper with elements of any Vector parameter of the operation. Either Program_Error is raised, or the operation works as defined on the value of the Vector either prior to, or subsequent to, some or all of the modifications to the Vector.

It is a bounded error to call any subprogram declared in the visible part of Containers.Vectors when the associated container has been finalized. If the operation takes Container as an in out parameter, then it raises Constraint_Error or Program_Error. Otherwise, the operation either proceeds as it would for an empty container, or it raises Constraint_Error or Program_Error.

A Cursor value is ambiguous if any of the following have occurred since it was created:

- Insert, Insert_Space, Insert_Vector, or Delete has been called on the vector that contains the element the cursor designates with an index value (or a cursor designating an element at such an index value) less than or equal to the index value of the element designated by the cursor; or

- The vector that contains the element it designates has been passed to the Sort or Merge procedures of an instance of Generic_Sorting, or to the Reverse_Elements procedure.

It is a bounded error to call any subprogram other than "=" or Has_Element declared in Containers.Vectors with an ambiguous (but not invalid, see below) cursor parameter. Possible results are:

- The cursor may be treated as if it were No_Element;
• The cursor may designate some element in the vector (but not necessarily the element that it originally designated);
• Constraint Error may be raised; or
• Program Error may be raised.

**Reason:** Cursors are made ambiguous if an Insert or Delete occurs that moves the elements in the internal array including the designated ones. After such an operation, the cursor probably still designates an element (although it might not after a deletion), but it is a different element. That violates the definition of cursor — it designates a particular element.

For "=" or Has Element, the cursor works normally (it would not be No Element). We don't want to trigger an exception simply for comparing a bad cursor.

While it is possible to check for these cases or ensure that cursors survive such operations, in many cases the overhead necessary to make the check (or ensure cursors continue to designate the same element) is substantial in time or space.

**Erroneous Execution**

**AI95-00302-03** A Cursor value is invalid if any of the following have occurred since it was created:

- The vector that contains the element it designates has been finalized;
- **AI05-0160-1** The vector that contains the element it designates has been used as the Target of a call to Assign, or as the target of an assignment statement;
- **AI05-0262-1** The element it designates has been deleted or removed from the vector that previously contained the element.

**Proof:** Move has been reworded in terms of Assign and Clear, which are covered by other bullets, so this text is redundant.

**AI05-0160-1** The element it designates has been deleted or removed from the vector that previously contained the element.

**Ramification:** **AI05-0160-1** An element can be removed via calls to Set Length, Clear, and Merge; and indirectly via calls to Assign and Move.

**AI95-00302-03** The result of "=" or Has Element is unspecified if it is called with an invalid cursor parameter. Execution is erroneous if any other subprogram declared in Containers.Vectors is called with an invalid cursor parameter.

**Discussion:** The list above (combined with the bounded error cases) is intended to be exhaustive. In other cases, a cursor value continues to designate its original element. For instance, cursor values survive the appending of new elements.

**AI05-0212-1** Execution is erroneous if the vector associated with the result of a call to Reference or Constant Reference is finalized before the result object returned by the call to Reference or Constant Reference is finalized.

**Reason:** Each object of Reference Type and Constant Reference Type probably contains some reference to the originating container. If that container is prematurely finalized (which is only possible via Unchecked Deallocation, as accessibility checks prevent passing a container to Reference that will not live as long as the result), the finalization of the object of Reference Type will try to access a nonexistent object. This is a normal case of a dangling pointer created by Unchecked Deallocation; we have to explicitly mention it here as the pointer in question is not visible in the specification of the type. (This is the same reason we have to say this for invalid cursors.)

**Implementation Requirements**

**AI95-00302-03** No storage associated with a vector object shall be lost upon assignment or scope exit.

**AI95-00302-03** **AI05-0262-1** The execution of an assignment statement for a vector shall have the effect of copying the elements from the source vector object to the target vector object and changing the length of the target object to that of the source object.

**Implementation Note:** **AI05-0298-1** **AI12-0005-1** An assignment of a Vector is a “deep” copy; that is the elements are copied as well as the data structures. We say “effect of” in order to allow the implementation to avoid
copying elements immediately if it wishes. For instance, an implementation that avoided copying until one of the containers is modified would be allowed. (Note that such an implementation would require care, as Query Element and Constant Reference both could be used to access an element which later needs to be reallocated while the parameter or reference still exists, potentially leaving the parameter or reference pointing at the wrong element.)

**Implementation Advice**

{AI95-00302-03} Containers.Vectors should be implemented similarly to an array. In particular, if the length of a vector is \( N \), then

- **the worst-case time complexity of Element should be** \( O(\log N) \);
  
  **Implementation Advice**: The worst-case time complexity of Element for Containers.Vector should be \( O(\log N) \).

- **the worst-case time complexity of Append with Count=1 when \( N \) is less than the capacity of the vector should be** \( O(\log N) \); and
  
  **Implementation Advice**: The worst-case time complexity of Append with Count = 1 when \( N \) is less than the capacity for Containers.Vector should be \( O(\log N) \).

- **the worst-case time complexity of Prepend with Count=1 and Delete First with Count=1 should be** \( O(N \log N) \).
  
  **Implementation Advice**: The worst-case time complexity of Prepend with Count = 1 and Delete First with Count=1 for Containers.Vectors should be \( O(N \log N) \).

  **Reason**: We do not mean to overly constrain implementation strategies here. However, it is important for portability that the performance of large containers has roughly the same factors on different implementations. If a program is moved to an implementation that takes \( O(N) \) time to access elements, that program could be unusable when the vectors are large. We allow \( O(\log N) \) access because the proportionality constant and caching effects are likely to be larger than the log factor, and we don't want to discourage innovative implementations.

{AI95-00302-03} The worst-case time complexity of a call on procedure Sort of an instance of Containers.Vectors.Generic_Sorting should be \( O(N^2) \), and the average time complexity should be better than \( O(N^2) \).

**Implementation Advice**: The worst-case time complexity of a call on procedure Sort of an instance of Containers.Vectors.Generic_Sorting should be \( O(N^2) \), and the average time complexity should be better than \( O(N^2) \).

**Ramification**: In other words, we're requiring the use of a better than \( O(N^2) \) sorting algorithm, such as Quicksort. No bubble sorts allowed!


**To be honest**: We do not mean “absolutely minimize” here; we're not intending to require a single copy for each element. Rather, we want to suggest that the sorting algorithm chosen is one that does not copy items unnecessarily. Bubble sort would not meet this advice, for instance.

{AI95-00302-03} Move should not copy elements, and should minimize copying of internal data structures.

**Implementation Advice**: Containers.Vectors.Move should not copy elements, and should minimize copying of internal data structures.

**Implementation Note**: Usually that can be accomplished simply by moving the pointer(s) to the internal data structures from the Source vector to the Target vector.

{AI95-00302-03} If an exception is propagated from a vector operation, no storage should be lost, nor any elements removed from a vector unless specified by the operation.

**Implementation Advice**: If an exception is propagated from a vector operation, no storage should be lost, nor any elements removed from a vector unless specified by the operation.

**Reason**: This is important so that programs can recover from errors. But we don't want to require heroic efforts, so we just require documentation of cases where this can't be accomplished.
NOTE 1 {AI12-0440-1} All elements of a vector occupy locations in the internal array. If a sparse container is required, a Hashed Map can be used rather than a vector.

NOTE 2 If Index_Type'Base'First = Index_Type'First an instance of Ada.Containers.Vectors will raise Constraint_Error. A value below Index_Type'First is required so that an empty vector has a meaningful value of Last_Index.

Discussion: This property is the main reason why only integer types (as opposed to any discrete type) are allowed as the index type of a vector. An enumeration or modular type would require a subtype in order to meet this requirement.

Extensions to Ada 95

{AI95-00302-03} The package Containers.Vectors is new.

Incompatibilities With Ada 2005

{AI05-0001-1} Subprograms Assign and Copy are added to Containers.Vectors. If an instance of Containers.Vectors is referenced in a use_clause, and an entity E with the same defining_identifier as a new entity in Containers.Vectors is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 2005

{AI05-0212-1} Added iterator, reference, and indexing support to make vector containers more convenient to use.

Wording Changes from Ada 2005

{AI05-0001-1} Generalized the definition of Reserve_Capacity and Move. Specified which elements are read/written by stream attributes.

{AI05-0022-1} Correction: Added a Bounded (Run-Time) Error to cover tampering by generic actual subprograms.

{AI05-0027-1} Correction: Added a Bounded (Run-Time) Error to cover access to finalized vector containers.

{AI05-0044-1} Correction: Redefined "e" actuals to require a strict weak ordering; the old definition allowed indeterminant comparisons that would not have worked in a container.

{AI05-0084-1} Correction: Added a pragma Remote_Types so that containers can be used in distributed programs.

{AI05-0160-1} Correction: Revisited the definition of invalid cursors to cover missing (and new) cases.

{AI05-0265-1} Correction: Defined when a container prohibits tampering in order to more clearly define where the check is made and the exception raised.

Inconsistencies With Ada 2012

{AI12-0005-1} {AI12-0212-1} {AI12-0400-1} Vector objects now support aggregates. This introduces a potential incompatibility for overloaded routines, including the "&" operations defined in this package. If the Element_Type of the vector is a type that allows aggregates (such as a record type), then calls to the "&" operations with an aggregate element will become ambiguous in Ada 2022, while they would have been legal in Ada 2012. This can be fixed by qualifying the aggregate with the element type.

{AI12-0400-1} Correction: The Insert, Append, and Prepend operations that operate on two vectors have been renamed Insert_Vector, Append_Vector, and Prepend_Vector, respectively. This was done in order to eliminate the aggregate ambiguity for the commonly used single element Append and Insert routines. The renamed routines are rarely used in Ada 2012 code, so the impact should be minimal.
Extensions to Ada 2012

{AI12-0196-1} **Correction:** To Cursor and Replace Element are now defined such that they can be used concurrently so long as they operate on different elements. This allows some container operations to be used in parallel without separate synchronization.

{AI12-0212-1} Vectors now support indexed container aggregates, so aggregate syntax can be used to create Vectors.

{AI12-0266-1} The iterator for the entire container now can return a parallel iterator which can be used to process the container in parallel.

Wording Changes from Ada 2012

{AI12-0110-1} **Corrigendum:** Clarified that tampering checks precede all other checks made by a subprogram (but come after those associated with the call).

{AI12-0112-1} Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).

{AI12-0400-1} **Correction:** Split the Append routine into two routines rather than having a single routine with a default parameter, in order that a routine with the appropriate profile for the Aggregate aspect exists. This change should not change the behavior of any existing code.

A.18.3 The Generic Package Containers.Doubly_Linked_Lists

{AI95-00302-03} The language-defined generic package Containers.Doubly_Linked_Lists provides private types List and Cursor, and a set of operations for each type. A list container is optimized for insertion and deletion at any position.

{AI95-00302-03} A doubly-linked list container object manages a linked list of internal nodes, each of which contains an element and pointers to the next (successor) and previous (predecessor) internal nodes. A cursor designates a particular node within a list (and by extension the element contained in that node). A cursor keeps designating the same node (and element) as long as the node is part of the container, even if the node is moved in the container.

{AI95-00302-03} The length of a list is the number of elements it contains.

Static Semantics

{AI95-00302-03} The generic library package Containers.Doubly_Linked_Lists has the following declaration:

```ada
generic
    type Element_Type is private;
    with function "=" (Left, Right : Element_Type) return Boolean is <>;
package Ada.Containers.Doubly_Linked_Lists is
    with Preelaborate, Remote_Types, Nonblocking, Global => in out synchronized is
    pragma Preelaborate(Doubly_Linked_Lists);
    pragma Remote_Types(Doubly_Linked_Lists);
Discussion: {AI12-0112-1} For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).
```
type List is tagged private
  with Constant_Indexing => Constant_Reference,
  Variable_Indexing => Reference,
  Default_Iterator => Iterate,
  Iterator_Element => Element_Type,
  Iterator_View => Stable.List,
  Aggregate => (Empty => Empty,
                 AddUnnamed => Append),
  Stable_Properties => (Length,
                        Tampering_With_Cursors_Prohibited,
                        Tampering_With_Elements_Prohibited),
  Default_Initial_Condition =>
    Length (List) = 0 and then
    (not Tampering_With_Cursors_Prohibited (List)) and then
    (not Tampering_With_Elements_Prohibited (List)),
    pragma Preelaborable_Initialization (List);

  type Cursor is private
  with pragma Preelaborable_Initialization (Cursor);

  Empty_List : constant List;
  No_Element : constant Cursor;

function Has_Element (Position : Cursor) return Boolean
  with Nonblocking, Global => in all, Use Formal => null;
function Has_Element (Container : List; Position : Cursor) return Boolean
  with Nonblocking, Global => null, Use Formal => null;
package List_Iterator_Interfaces is new Ada.Iterator_Interfaces (Cursor, Has_Element);

function "=" (Left, Right : List) return Boolean;
function Tampering_With_Cursors_Prohibited (Container : List) return Boolean
  with Nonblocking, Global => null, Use Formal => null;
function Tampering_With_Elements_Prohibited (Container : List) return Boolean
  with Nonblocking, Global => null, Use Formal => null;

function Empty return List is (Empty_List)
  with Post =>
    not Tampering_With_Elements_Prohibited (Empty'Result) and then
    not Tampering_With_Cursors_Prohibited (Empty'Result) and then
    Length (Empty'Result) = 0;

function Length (Container : List) return Count_Type
  with Nonblocking, Global => null, Use Formal => null;
function Is_Empty (Container : List) return Boolean
  with Nonblocking, Global => null, Use Formal => null,
  Post => Is_Empty'Result = (Length (Container) = 0);

procedure Clear (Container : in out List)
  with Pre => not Tampering_With_Cursors_Prohibited (Container)
             or else raise Program_Error,
  Post => Length (Container) = 0;

function Element (Position : Cursor) return Element_Type
  with Pre => Position /= No_Element or else raise Constraint_Error,
  Nonblocking, Global => in all, Use Formal => Element_Type;
function Element (Container : List; Position : Cursor) return Element_Type
with Pre => (Position /= No_Element or else raise Constraint_Error) and then
(Has_Element (Container, Position) or else raise Program_Error),
Nonblocking, Global => null, Use Formal => Element_Type;

procedure Replace_Element (Container : in out List; Position : in Cursor; New_item : in Element_Type)
with Pre => (not Tampering_With_Elements_Prohibited (Container) or else raise Program_Error)
and then (Position /= No_Element or else raise Constraint_Error) and then
(Has_Element (Container, Position) or else raise Program_Error);

procedure Query_Element (Position : in Cursor; Process : not null access procedure (Element : in Element_Type))
with Pre => (Position /= No_Element or else raise Constraint_Error, Global => in all);

procedure Update_Element (Container : in out List; Position : in Cursor; Process : not null access procedure (Element : in out Element_Type))
with Pre => (Position /= No_Element or else raise Constraint_Error) and then
(Has_Element (Container, Position) or else raise Program_Error);

type Constant_Reference_Type
(Element : not null access constant Element_Type)
is private
with Implicit_Dereference => Element,
Nonblocking, Global => in out synchronized,
Default Initial Condition => (raise Program_Error);

type Reference_Type (Element : not null access Element_Type)
is private
with Implicit_Dereference => Element,
Nonblocking, Global => in out synchronized,
Default Initial Condition => (raise Program_Error);

function Constant_Reference (Container : aliased in List; Position : in Cursor)
return Constant_Reference_Type
with Pre => (Position /= No_Element or else raise Constraint_Error) and then
(Has_Element (Container, Position) or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container),
Nonblocking, Global => null, Use Formal => null;
function Reference (Container : aliased in out List;
  Position : in Cursor)
  return Reference_Type
  with Pre => (Position /= No_Element or else
    raise Constraint_Error) and then
    (Has_Element (Container, Position) or else
      raise Program_Error),
  Post => Tampering_With_Cursors_Prohibited (Container),
  Nonblocking, Global => null, Use_Formal => null;

procedure Assign (Target : in out List; Source : in List)
  with Pre => not Tampering_With_Cursors_Prohibited (Target)
    or else raise Program_Error,
  Post => Length (Source) = Length (Target);

function Copy (Source : List)
  return List
  with Post =>
    Length (Copy'Result) = Length (Source) and then
    not Tampering_With_Elements_Prohibited (Copy'Result) and then
    not Tampering_With_Cursors_Prohibited (Copy'Result);

procedure Move (Target : in out List;
  Source : in out List)
  with Pre => (not Tampering_With_Cursors_Prohibited (Target)
    or else raise Program_Error),
  Post => (if not Target'Has_Same_Storage (Source) then
    Length (Target) = Length (Source'Old) and then
    Length (Source) = 0);

procedure Insert (Container : in out List;
  Before    : in Cursor;
  New_Item  : in Element_Type;
  Count     : in Count_Type := 1)
  with Pre => (not Tampering_With_Cursors_Prohibited (Container)
    or else raise Program_Error) and then
    (Before = No_Element or else
      Has_Element (Container, Before)
        or else raise Program_Error) and then
    (Length (Container) <= Count_Type'Last - Count
      or else raise Constraint_Error),
  Post => Length (Container)'Old + Count = Length (Container);
procedure Insert (Container : in out List;
Before    : in  Cursor;
Position  : out Cursor;
Count     : in  Count_Type := 1)
  with Pre => (not Tampering With Cursors_Prohibited (Container)
or else raise Program_Error) and then
   (Before /= No_Element or else
    Has_Element (Container, Before)
or else raise Program_Error),
   Length (Container) <= Count_Type'Last - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count = Length (Container)
and then Has_Element (Container, Position);

procedure Prepend (Container : in out List;
New_Item  : in  Element_Type;
Count     : in  Count_Type := 1)
  with Pre => (not Tampering With Cursors_Prohibited (Container)
or else raise Program_Error) and then
   Length (Container) <= Count_Type'Last - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count = Length (Container);

procedure Append (Container : in out List;
New_Item  : in  Element_Type)
  with Pre => (not Tampering With Cursors_Prohibited (Container)
or else raise Program_Error) and then
   Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => Length (Container)'Old + 1 = Length (Container);

procedure Delete (Container : in out List;
Position  : in out Cursor;
Count     : in  Count_Type := 1)
  with Pre => (not Tampering With Cursors_Prohibited (Container)
or else raise Program_Error) and then
   (Position /= No_Element or else
    Has_Element (Container, Position)
or else raise Program_Error),
Post => Length (Container)'Old - Count <= Length (Container)
and then Position = No_Element;

procedure Delete First (Container : in out List;
Count     : in  Count_Type := 1)
  with Pre => not Tampering With Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Length (Container)'Old - Count <= Length (Container);

procedure Delete_Last (Container : in out List;
Count     : in  Count_Type := 1)
  with Pre => not Tampering With Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Length (Container)'Old - Count <= Length (Container);

procedure Reverse Elements (Container : in out List)
  with Pre => not Tampering With Cursors_Prohibited (Container)
or else raise Program_Error;
procedure Swap (Container : in out List; I, J : in Cursor)
  with Pre => (not Tampering With Elements Prohibited (Container)
    or else raise Program Error) and then
    (I /= No_Element or else Constraint_Error) and then
    (J /= No_Element or else Constraint_Error) and then
    (Has_Element (Container, I)
    or else raise Program Error) and then
    (Has_Element (Container, J)
    or else raise Program Error);

procedure Swap_Links (Container : in out List; I, J : in Cursor)
  with Pre => (not Tampering With Elements Prohibited (Container)
    or else raise Program Error) and then
    (I /= No_Element or else Constraint_Error) and then
    (J /= No_Element or else Constraint_Error) and then
    (Has_Element (Container, I)
    or else raise Program Error) and then
    (Has_Element (Container, J)
    or else raise Program Error);

procedure Splice (Target : in out List; Before : in Cursor;
  Source : in out List)
  with Pre => (not Tampering With Cursors Prohibited (Target)
    or else raise Program Error) and then
    (not Tampering With Cursors Prohibited (Source)
    or else raise Program Error) and then
    (Before = No_Element or else
    Has_Element (Target, Before)
    or else raise Program Error) and then
    (Target'Has_Same_Storage (Source) or else
    Length (Target) <= Count_Type'Last - Length (Source)
    or else raise Constraint_Error),
  Post => (if not Target'Has_Same_Storage (Source) then
    declare
      Result_Length : constant Count_Type :=
      Length (Source)'Old + Length (Target)'Old;
    begin
      Length (Source) = 0 and then Length (Target) = Result_Length);
procedure Splice (Target : in out List;
Before   : in   Cursor;
Source   : in out List;
Position : in out Cursor)

with Pre => (not Tampering With Cursors Prohibited (Target)
or else raise Program_Error) and then
(not Tampering With Cursors Prohibited (Source)
or else raise Program_Error) and then
(Position /= No_Element
or else raise Constraint_Error) and then
(Has_element (Source, Position)
or else raise Program_Error) and then
(Before = No_Element or else
Has_element (Target, Before)
or else raise Program_Error) and then
(Target.Has_Same_Storage (Source) or else
Length (Target) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Org_Target_Length : constant Count_Type :=
Length (Target)'Old;
Org_Source_Length : constant Count_Type :=
Length (Source)'Old;
begin
(if Target.Has_Same_Storage (Source) then
Position = Position'Old
else
Length (Source) = Org_Source_Length - 1 and then
Length (Target) = Org_Target_Length + 1 and then
Has_element (Target, Position));

procedure Splice (Container: in out List;
Before   : in   Cursor;
Position : in   Cursor)

with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Position /= No_Element
or else raise Constraint_Error) and then
(Has_element (Container, Position)
or else raise Program_Error) and then
(Before = No_Element or else
Has_element (Container, Before)
or else raise Program_Error),
Post => Length (Container) = Length (Container)'Old;

function First (Container : List) return Cursor
with Nonblocking, Global => null, Use Formal => null,
Post => (if not Is_empty (Container)
then Has_element (Container, First'Result)
else First'Result = No_Element);

function First_Element (Container : List) return Element_Type
with Pre => (not Is_Empty (Container)
or else raise Constraint_Error);

function Last (Container : List) return Cursor
with Nonblocking, Global => null, Use Formal => null,
Post => (if not Is_empty (Container)
then Has_element (Container, Last'Result)
else Last'Result = No_Element);

function Last_Element (Container : List) return Element_Type
with Pre => (not Is_Empty (Container)
or else raise Constraint_Error);

function Next (Position : Cursor) return Cursor
with Nonblocking, Global => in all, Use Formal => null,
Post => (if Position = No_Element then Next'Result = No_Element);
function Next (Container : List;
    Position : Cursor) return Cursor
with Nonblocking, Global => null, Use Formal => null,
    Pre => Position = No Element or else
        Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Position = No Element then
            Next'Result = No Element
        elsif Next'Result = No Element
            then Position = Last (Container)
        else Has Element (Container, Next'Result));

function Previous (Position : Cursor) return Cursor
with Nonblocking, Global => in all, Use Formal => null,
    Post => (if Position = No Element
            then Previous'Result = No Element)

function Previous (Container : List;
    Position : Cursor) return Cursor
with Nonblocking, Global => null, Use Formal => null,
    Pre => Position = No Element or else
        Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Position = No Element
            then Previous'Result = No Element
        elsif Previous'Result = No Element
            then Position = First (Container)
        else Has Element (Container, Previous'Result));

procedure Next (Position : in out Cursor)
with Nonblocking, Global => in all, Use Formal => null;

procedure Next (Container : in List;
    Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
    Pre => Position = No Element or else
        Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Position /= No Element
            then Has Element (Container, Position));

procedure Previous (Position : in out Cursor)
with Nonblocking, Global => in all, Use Formal => null;

procedure Previous (Container : in List;
    Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
    Pre => Position = No Element or else
        Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Position /= No Element
            then Has Element (Container, Position));

function Find (Container : List;
    Item : Element_Type;
    Position : Cursor := No_Element)
return Cursor
with Pre => Position = No Element or else
        Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Find'Result /= No Element
            then Has Element (Container, Find'Result));

function Reverse Find (Container : List;
    Item : Element_Type;
    Position : Cursor := No_Element)
return Cursor
with Pre => Position = No Element or else
        Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Reverse Find'Result /= No Element
            then Has Element (Container, Reverse Find'Result));
function Contains (Container : List; Item : Element_Type) return Boolean;

This paragraph was deleted.

function Has_Element (Position : Cursor) return Boolean;

procedure Iterate (Container : in List; Process : not null access procedure (Position : in Cursor)) with Allows Exit;

procedure Reverse_Iterate (Container : in List; Process : not null access procedure (Position : in Cursor)) with Allows Exit;

function Iterate (Container : in List) return List_Iterator_Interfaces.Parallel_Reversible_Iterator'Class with Post => Tampering_With_Cursors_Prohibited (Container);

function Iterate (Container : in List; Start : in Cursor) return List_Iterator_Interfaces.Reversible_Iterator'Class with Pre => (Start /= No_Element or else raise Constraint_Error) and then (Has_Element (Container, Start) or else raise Program_Error), Post => Tampering_With_Cursors_Prohibited (Container);

generic with function "<" (Left, Right : Element_Type) return Boolean is <>;

package Generic_Sorting with Nonblocking, Global => null is

function Is_Sorted (Container : List) return Boolean;

procedure Sort (Container : in out List) with Pre => not Tampering_With_Cursors_Prohibited (Container) or else raise Program_Error;

procedure Merge (Target : in out List; Source : in out List) with Pre => (not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error) and then (not Tampering_With_Elements_Prohibited (Source) or else raise Program_Error) and then (Length (Target) <= Count_Type'Last - Length (Source) or else raise Constraint_Error) and then ((Length (Source) = 0 or else not Target'Has_Same_Storage (Source)) or else raise Constraint_Error), Post => (declare Result_Length : constant Count_Type := Length (Source)'Old + Length (Target)'Old;

begin

(Length (Source) = 0 and then Length (Target) = Result_Length));

end Generic_Sorting;

package Stable is
A.18.3 The Generic Package Containers.Doubly_Linked_Lists

The actual function for the generic formal function "=" on Element_Type values is expected to define a reflexive and symmetric relationship and return the same result value each time it is called with a particular pair of values. If it behaves in some other manner, the functions Find, Reverse Find, and "=" on list values return an unspecified value. The exact arguments and number of calls of this generic formal function by the functions Find, Reverse Find, and List "=" are unspecified. Other subprograms are not allowed to break if "=" is bad (they aren't expected to use "=").

Ramification: If the actual function for "=" is not symmetric and consistent, the result returned by the listed functions cannot be predicted. The implementation is not required to protect against "=" raising an exception, or returning random results, or any other "bad" behavior. And it can call "=" in whatever manner makes sense. But note that only the results of Find, Reverse Find, and List "=" are unspecified; other subprograms are not allowed to break if "=" is bad (they aren't expected to use "=").

The type List is used to represent lists. The type List needs finalization (see 7.6).
Empty_List represents the empty List object. It has a length of 0. If an object of type List is not otherwise initialized, it is initialized to the same value as Empty_List.

No_Element represents a cursor that designates no element. If an object of type Cursor is not otherwise initialized, it is initialized to the same value as No_Element.

The predefined "=" operator for type Cursor returns True if both cursors are No_Element, or designate the same element in the same container.

To be honest: The primitive "=" operator is the one with two parameters of type Cursor which returns Boolean. We're not talking about some other (hidden) primitive function named "=".

Execution of the default implementation of the Input, Output, Read, or Write attribute of type Cursor raises Program_Error.

Reason: A cursor will probably be implemented in terms of one or more access values, and the effects of streaming access values is unspecified. Rather than letting the user stream junk by accident, we mandate that streaming of cursors raise Program_Error by default. The attributes can always be specified if there is a need to support streaming.

List'Write for a List object L writes Length(L) elements of the list to the stream. It may also write additional information about the list.

List'Read reads the representation of a list from the stream, and assigns to Item a list with the same length and elements as was written by List'Write.

Ramification: Streaming more elements than the container length is wrong. For implementation implications of this rule, see the Implementation Note in A.18.2.

Some operations of this generic package have access to subprogram parameters. To ensure such operations are well defined, they guard against certain actions by the designated subprogram. In particular, some operations check for "tampering with cursors" of a container because they depend on the set of elements of the container remaining constant, and others check for "tampering with elements" of a container because they depend on elements of the container not being replaced. When tampering with cursors is prohibited for a particular list object L, Program_Error is propagated by the finalization of L, as well as by a call that passes L to certain of the operations of this package, as indicated by the precondition of such an operation. Similarly, when tampering with elements is prohibited for L, Program_Error is propagated by a call that passes L to certain of the other operations of this package, as indicated by the precondition of such an operation.

Paragraphs 62 through 69 are removed as preconditions now describe these rules.

A subprogram is said to tamper with cursors of a list object L if:

- it inserts or deletes elements of L, that is, it calls the Insert, Clear, Delete, or Delete_Last procedures with L as a parameter; or

  To be honest: Operations which are defined to be equivalent to a call on one of these operations also are included. Similarly, operations which call one of these as part of their definition are included.

- it reorders the elements of L, that is, it calls the Splice, Swap_Links, or Reverse_Elements procedures or the Sort or Merge procedures of an instance of Generic_Sorting with L as a parameter; or

- it finalizes L; or

- it calls the Assign procedure with L as the Target parameter; or

  Ramification: We don't need to explicitly mention assignment_statement, because that finalizes the target object as part of the operation, and finalization of an object is already defined as tampering with cursors.

- it calls the Move procedure with L as a parameter.

  Reason: Swap copies elements rather than reordering them, so it doesn't tamper with cursors.
A subprogram is said to tamper with elements of a list object \( L \) if:

- it tampers with cursors of \( L \); or
- it replaces one or more elements of \( L \), that is, it calls the Replace_Element or Swap procedures with \( L \) as a parameter.

**Reason:** Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can't be allowed. However, a simple modification of (part of) an element is not a problem, so Update_Element does not cause a problem.

When tampering with cursors is prohibited for a particular list object \( L \), Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the cursors of \( L \), leaving \( L \) unmodified. Similarly, when tampering with elements is prohibited for a particular list object \( L \), Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the elements of \( L \) (or tamper with the cursors of \( L \)), leaving \( L \) unmodified. These checks are made before any other defined behavior of the body of the language-defined subprogram.

**Proof:** Tampering with elements includes tampering with cursors, so we mention it only from completeness in the second sentence.

```ada
function Has_Element (Position : Cursor) return Boolean
with Nonblocking, Global => in all, Use_Formal => null;

{AI05-0212-1} Returns True if Position designates an element, and returns False otherwise.
```

**To be honest:** \{AI05-0005-1\} \{AI05-0212-1\} This function might not detect cursors that designate deleted elements; such cursors are invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

```ada
function Has_Element (Container : List; Position : Cursor)
return Boolean
with Nonblocking, Global => null, Use_Formal => null;

{AI12-0112-1} Returns True if Position designates an element in Container, and returns False otherwise.
```

**Ramification:** If Position is No_Element, Has_Element returns False.

```ada
function "=" (Left, Right : List) return Boolean;

{AI95-00302-03} {AI05-0264-1} If Left and Right denote the same list object, then the function returns True. If Left and Right have different lengths, then the function returns False. Otherwise, it compares each element in Left to the corresponding element in Right using the generic formal equality operator. If any such comparison returns False, the function returns False; otherwise, it returns True. Any exception raised during evaluation of element equality is propagated.
```

**Implementation Note:** This wording describes the canonical semantics. However, the order and number of calls on the formal equality function is unspecified for all of the operations that use it in this package, so an implementation can call it as many or as few times as it needs to get the correct answer. Specifically, there is no requirement to call the formal equality additional times once the answer has been determined.

```ada
function Tampering_With_Cursors_Prohibited
(Container : List) return Boolean
with Nonblocking, Global => null, Use_Formal => null;

{AI12-0112-1} Returns True if tampering with cursors or tampering with elements is currently prohibited for Container, and returns False otherwise.
```

**Reason:** \{AI12-0112-1\} Prohibiting tampering with elements also needs to prohibit tampering with cursors, as deleting an element is similar to replacing it.

**Implementation Note:** \{AI12-0112-1\} Various contracts elsewhere in this specification require that this function be implemented with synchronized data. Moreover, it is possible for tampering to be prohibited by multiple operations...
(sequentially or in parallel). Therefore, tampering needs to be implemented with an atomic or protected counter. The counter is initialized to zero, and is incremented when tampering is prohibited, and decremented when leaving an area that prohibited tampering. Function Tampering_With_Cursors_Prohibited returns True if the counter is nonzero. (Note that any case where the result is not well-defined for one task is incorrect use of shared variables and would be erroneous by the rules of 9.10, so no special protection is needed to read the counter.)

```ada
function Tampering_With_Elements_Prohibited
(Container : List) return Boolean
with Nonblocking, Global => null, Use_Formal => null;

{AI12-0112-1} Always returns False, regardless of whether tampering with elements is prohibited.

Reason: {AI12-0111-1} A definite element cannot change size, so we allow operations that tamper with elements even when tampering with elements is prohibited. That's not true for the indefinite containers, which is why this kind of tampering exists.

function Length (Container : List) return Count_Type
with Nonblocking, Global => null, Use_Formal => null;

{AI95-00302-03} Returns the number of elements in Container.

function Is_Empty (Container : List) return Boolean
with Nonblocking, Global => null, Use_Formal => null,
Post => Is_Empty'Result = (Length (Container) = 0);

{AI95-00302-03} {AI12-0112-1} Returns True if Container is empty. Equivalent to Length (Container) = 0.

procedure Clear (Container : in out List)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
| or else raise Program_Error,
Post => Length (Container) = 0;

{AI95-00302-03} Removes all the elements from Container.

function Element (Position : Cursor) return Element_Type
with Pre => Position /= No_Element
| or else raise Constraint_Error,
Nonblocking, Global => in all, Use_Formal => Element_Type;

{AI95-00302-03} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated. Otherwise, Element returns the element designated by Position.

function Element (Container : List; Position : Cursor) return Element_Type
with Pre => (Position /= No_Element
| or else raise Constraint_Error) and then
| (Has_Element (Container, Position)
| or else raise Program_Error),
Nonblocking, Global => null, Use_Formal => Element_Type;

{AI12-0112-1} Element returns the element designated by Position in Container.

procedure Replace_Element (Container : in out List;
Position : in Cursor;
New_Item : in Element_Type)
with Pre => (not Tampering_With_Elements_Prohibited (Container)
| or else raise Program_Error) and then
| (Position /= No_Element
| or else raise Constraint_Error) and then
| (Has_Element (Container, Position)
| or else raise Program_Error);

{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} {AI12-0196-1} If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Replace Element assigns the value New_Item to the element designated by Position. For the purposes of determining whether the parameters overlap
in a call to Replace_Element, the Container parameter is not considered to overlap with any object [(including itself)].

```ada
procedure Query_Element
(Position : in Cursor;
Process   : not null access procedure (Element : in Element_Type))
with Pre => Position /= No_Element or else raise Constraint_Error,
          Global => in all;
```

{82/5} {83/5} {A195-00302-03} {A105-0021-1} {A105-0265-1} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated. Otherwise, Query_Element calls Process.all with the element designated by Position as the argument. Tampering with the elements of the list that contains the element designated by Position is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

```ada
procedure Query_Element
(Container : in List;
Position   : in Cursor;
Process    : not null access procedure (Element : in Element_Type))
with Pre => (Position /= No_Element
               or else raise Constraint_Error)
          and then
               (Has_Element (Container, Position)
               or else raise Program_Error);
```

{83.1/5} {AI12-0112-1} Query_Element calls Process.all with the element designated by Position as the argument. Tampering with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

```ada
procedure Update_Element
(Container : in out List;
Position   : in Cursor;
Process    : not null access procedure (Element : in out Element_Type))
with Pre => (Position /= No_Element
               or else raise Constraint_Error)
          and then
               (Has_Element (Container, Position)
               or else raise Program_Error);
```

{85/5} {A195-00302-03} {A105-0264-1} {A105-0265-1} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Update_Element calls Process.all with the element designated by Position as the argument. Tampering with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

If Element_Type is unconstrained and definite, then the actual Element parameter of Process.all shall be unconstrained.

**Ramification:** This means that the elements cannot be directly allocated from the heap; it must be possible to change the discriminants of the element in place.

```ada
type Constant_Reference_Type
(Element : not null access constant Element_Type) is private
with Implicit_Dereference => Element,
          Nonblocking, Global => in out synchronized,
          Default_Initial_Condition => (raise Program_Error);
```

{86.1/5} {AI12-0112-1}
type Reference_Type (Element : not null access Element_Type) is
private
   with Implicit_Dereference => Element,
   Nonblocking, Global => in out synchronized,
   Default_Initial.Condition => (raise Program_Error);

The types Constant_Reference_Type and Reference_Type need finalization.

This paragraph was deleted.
The default initialization of an object of type Constant_Reference_Type or Reference_Type propagates Program_Error.

Reason: It is expected that Reference_Type (and Constant_Reference_Type) will be a controlled type, for which finalization will have some action to terminate the tampering check for the associated container. If the object is created by default, however, there is no associated container. Since this is useless, and supporting this case would take extra work, we define it to raise an exception.

function Constant_Reference (Container : aliased in List; Position : in Cursor) return Constant_Reference_Type with Pre => (Position /= No_Element or else raise Constraint_Error) and then (Has_Element (Container, Position) or else raise Program_Error), Nonblocking, Global => null, Use_Formal => null;

This function (combined with the Constant_Indexing and Implicit_Dereference aspects) provides a convenient way to gain read access to an individual element of a list given a cursor.

function Reference (Container : aliased in out List; Position : in Cursor) return Reference_Type with Pre => (Position /= No_Element or else raise Constraint_Error) and then (Has_Element (Container, Position) or else raise Program_Error), Nonblocking, Global => null, Use_Formal => null;

This function (combined with the Variable_Indexing and Implicit_Dereference aspects) provides a convenient way to gain read and write access to an individual element of a list given a cursor.
procedure Assign (Target : in out List; Source : in List)
with Pre => not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error,
Post => Length (Source) = Length (Target);

If Target denotes the same object as Source, the operation has no effect. Otherwise, the elements of Source are copied to Target as for an assignment statement assigning Source to Target.

Discussion: This routine exists for compatibility with the bounded list container. For an unbounded list, Assign(A, B) and A := B behave identically. For a bounded list, := will raise an exception if the container capacities are different, while Assign will not raise an exception if there is enough room in the target.

function Copy (Source : List) return List
with Post =>
Length (Copy'Result) = Length (Source) and then
not Tampering_With_Elements_Prohibited (Copy'Result) and then
not Tampering_With_Cursors_Prohibited (Copy'Result);

Returns a list whose elements match the elements of Source.

procedure Move (Target : in out List; Source : in out List)
with Pre =>
not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error,
not Tampering_With_Cursors_Prohibited (Source)
or else raise Program_Error,
Post =>
if not Target'Has_Same_Storage (Source) then
Length (Target) = Length (Source'Old) and then
Length (Source) = 0;

If Target denotes the same object as Source, then the operation Move has no effect. Otherwise, the operation is equivalent to Assign (Target, Source) followed by Clear (Source). Move first calls Clear (Target). Then, the nodes in Source are moved to Target (in the original order). The length of Target is set to the length of Source, and the length of Source is set to 0.

procedure Insert (Container : in out List; Before : in Cursor; New_Item : in Element_Type; Count : in Count_Type := 1)
with Pre =>
not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error)
and then
(Count <= Count_Type'Last - Count)
or else raise Constraint_Error,
Post => Length (Container)'Old + Count = Length (Container);

If Before is not No_Element, and does not designate an element in Container, then Program_Error is propagated. Otherwise, Insert inserts Count copies of New Item prior to the element designated by Before. If Before equals No_Element, the new elements are inserted after the last node (if any). Any exception raised during allocation of internal storage is propagated, and Container is not modified.

Ramification: The check on Before checks that the cursor does not belong to some other Container. This check implies that a reference to the container is included in the cursor value. This wording is not meant to require detection of dangling cursors; such cursors are defined to be invalid, which means that execution is erroneous, and any result is allowed (including not raising an exception).
procedure Insert (Container : in out List;
Before : in Cursor;
New_Item : in Element_Type;
Position : out Cursor;
Count : in Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Before = No_Element or else Has_Element (Container, Before)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count = Length (Container)
and then Has_Element (Container, Position);

{AI95-00302-03} {AI05-0257-1} {AI12-0112-1} If Before is not No_Element, and does not designate an element in Container, then Program_Error is propagated. Otherwise, Insert allocates Count copies of New_Item, and inserts them prior to the element designated by Before. If Before equals No_Element, the new elements are inserted after the last element (if any). Position designates the first newly-inserted element, or if Count equals 0, then Position is assigned the value of Before. Any exception raised during allocation of internal storage is propagated, and Container is not modified.

procedure Insert (Container : in out List;
Before : in Cursor;
Position : out Cursor;
Count : in Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Before = No_Element or else Has_Element (Container, Before)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count = Length (Container)
and then Has_Element (Container, Position);

{AI95-00302-03} {AI05-0257-1} {AI12-0112-1} If Before is not No_Element, and does not designate an element in Container, then Program_Error is propagated. Otherwise, Insert inserts Count new elements prior to the element designated by Before. If Before equals No_Element, the new elements are inserted after the last node (if any). The new elements are initialized by default (see 3.3.1). Position designates the first newly-inserted element, or if Count equals 0, then Position is assigned the value of Before. Any exception raised during allocation of internal storage is propagated, and Container is not modified.

procedure Prepend (Container : in out List;
New_Item : in Element_Type;
Count : in Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - Count
or else raise Constraint_Error),
Post => Length (Container)'Old + Count = Length (Container);

{AI95-00302-03} Equivalent to Insert (Container, First (Container), New_Item, Count).
procedure Append (Container : in out List;
            New_Item : in Element_Type;
            Count : in Count_Type := 1)
   with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
               (Length (Container) <= Count_Type'Last - Count
               or else raise Constraint_Error),
   Post => Length (Container)'Old + Count = Length (Container);

   {AI95-00302-03} Equivalent to Insert (Container, No_Element, New_Item, Count).

procedure Append (Container : in out List;
            New_Item : in Element_Type)
   with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
               (Length (Container) <= Count_Type'Last - 1
               or else raise Constraint_Error),
   Post => Length (Container)'Old + 1 = Length (Container);

   {AI12-0391-1} Equivalent to Insert (Container, No_Element, New_Item, 1).

procedure Delete (Container : in out List;
            Position  : in out Cursor;
            Count     : in Count_Type := 1)
   with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
               (Position /= No_Element
               or else raise Constraint_Error) and then
               (Has_Element (Container, Position)
               or else raise Program_Error),
   Post => Length (Container)'Old - Count <= Length (Container)
               and then Position = No_Element;

   {AI95-00302-03} {AI05-0264-1} {AI12-0112-1} If Position equals No_Element, then
Constraint_Error is propagated. If Position does not designate an element in Container, then
Program_Error is propagated. Otherwise, Delete removes (from Container) Count elements
starting at the element designated by Position (or all of the elements starting at Position if there
are fewer than Count elements starting at Position). Finally, Position is set to No_Element.

procedure Delete_First (Container : in out List;
            Count     : in Count_Type := 1)
   with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error),
   Post => Length (Container)'Old - Count <= Length (Container);

   {AI95-00302-03} {AI05-0264-1} If Length (Container) <= Count, then Delete_First is equivalent
to Clear (Container). Otherwise, it removes the first Count nodes from Container Equivalent to
Delete (Container, First (Container), Count).

procedure Delete_Last (Container : in out List;
            Count     : in Count_Type := 1)
   with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error),
   Post => Length (Container)'Old - Count <= Length (Container);

   {AI95-00302-03} {AI05-0264-1} If Length (Container) <= Count, then Delete_Last is equivalent
to Clear (Container). Otherwise, it removes the last Count nodes from Container.

procedure Reverse_Elements (Container : in out List)
   with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error),
   Post => Length (Container)'Old - Count <= Length (Container);

   {AI95-00302-03} Reorders the elements of Container in reverse order.

Discussion: Unlike the similar routine for a vector, elements should not be copied; rather, the nodes should be
exchanged. Cursors are expected to reference the same elements afterwards.
procedure Swap (Container : in out List;  
I, J      : in Cursor) 
  with Pre => (not Tampering With Elements Prohibited (Container) 
              or else raise Program_Error) and then 
              (I /= No Element or else Constraint_Error) and then 
              (J /= No Element or else Constraint_Error) and then 
              (Has Element (Container, I) 
              or else raise Program_Error) and then 
              (Has Element (Container, J) 
              or else raise Program_Error); 

{AI95-00302-03} {AI12-0112-1} If either I or J is No_Element, then Constraint_Error is 
propagated. If either I or J do not designate an element in Container, then Program_Error is 
propagated. Otherwise, Swap exchanges the values of the elements designated by I and J.

Ramification: After a call to Swap, I designates the element value previously designated by J, and J designates the 
element value previously designated by I. The cursors do not become ambiguous from this operation.

To be honest: The implementation is not required to actually copy the elements if it can do the swap some other way. 
But it is allowed to copy the elements if needed.

procedure Swap_Links (Container : in out List;  
I, J      : in Cursor) 
  with Pre => (not Tampering With Elements Prohibited (Container) 
              or else raise Program_Error) and then 
              (I /= No Element or else Constraint_Error) and then 
              (J /= No Element or else Constraint_Error) and then 
              (Has Element (Container, I) 
              or else raise Program_Error) and then 
              (Has Element (Container, J) 
              or else raise Program_Error); 

{AI95-00302-03} {AI12-0112-1} If either I or J is No_Element, then Constraint_Error is 
propagated. If either I or J do not designate an element in Container, then Program_Error is 
propagated. Otherwise, Swap_Links exchanges the nodes designated by I and J.

Ramification: Unlike Swap, this exchanges the nodes, not the elements. No copying is performed. I and J designate the 
same elements after this call as they did before it. This operation can provide better performance than Swap if the 
element size is large.

procedure Splice (Target   : in out List;  
Before   : in Cursor;  
Source   : in out List) 
  with Pre => (not Tampering With Cursors_Prohibited (Target) 
              or else raise Program_Error) and then 
              (not Tampering With Cursors_Prohibited (Source) 
              or else raise Program_Error) and then 
              (Before = No_Element or else 
              Has Element (Target, Before) 
              or else raise Program_Error) and then 
              (Target'Has_Same_Storage (Source) or else 
              Length (Target) <= Count_Type'Last - Length (Source) 
              or else raise Constraint_Error), 
  Post => (if not Target'Has_Same_Storage (Source) then 
  declare 
      Result_Length : constant Count_Type := 
      Length (Source)'Old + Length (Target)'Old; 
  begin 
      Length (Source) = 0 and then 
      Length (Target) = Result_Length)); 

{AI95-00302-03} {AI12-0112-1} If Before is not No_Element, and does not designate an element 
in Target, then Program_Error is propagated. Otherwise, if Source denotes the same object as 
Target, the operation has no effect. Otherwise, Splice records elements such that they are 
removed from Source and moved to Target, immediately prior to Before. If Before equals
No_Element, the nodes of Source are spliced after the last node of Target. The length of Target is incremented by the number of nodes in Source, and the length of Source is set to 0.

```ada
procedure Splice (Target : in out List;
                 Before   : in   Cursor;
                 Source   : in out List;
                 Position : in out Cursor)
with Pre => (not Tampering_With.Cursors.Prohibited (Target)
            or else raise Program_Error) and then
            (not Tampering_With.Cursors.Prohibited (Source)
            or else raise Program_Error) and then
            (Position /= No_Element
            or else raise Constraint_Error) and then
            (Has Element (Source, Position)
            or else raise Program_Error) and then
            (Before = No_Element or else
            Has Element (Target, Before)
            or else raise Program_Error) and then
            (Target'Has_Same_Storage (Source) or else
            Length (Target) <= Count_Type'Last - 1
            or else raise Constraint_Error),
           Post => (declare
            Org_Target_Length : constant Count_Type :=
            Length (Target)'Old;
            Org_Source_Length : constant Count_Type :=
            Length (Source)'Old;
            begin
            if Target'Has_Same_Storage (Source) then
                Position = Position'Old
            else
                Length (Source) = Org_Source_Length - 1 and then
                Length (Target) = Org_Target_Length + 1 and then
                Has Element (Target, Position));
            end if;
            Constraint_Error is propagated. If Before does not equal No_Element, and does not designate an element in Target, then Program_Error is propagated. If Position does not equal No_Element, and does not designate a node in Source, then Program_Error is propagated. If Source denotes the same object as Target, then there is no effect if Position equals Before, else the element designated by Position is moved immediately prior to Before, or, if Before equals No_Element, after the last element. In both cases, Position and the length of Target are unchanged. Otherwise, the element designated by Position is removed from Source and moved to Target, immediately prior to Before, or, if Before equals No_Element, after the last element of Target. The length of Target is incremented, the length of Source is decremented, and Position is updated to represent an element in Target.
```

Ramification: If Source is the same as Target, and Position = Before, or Next(Position) = Before, Splice has no effect, as the element does not have to move to meet the postcondition.

```ada
procedure Splice (Container: in out List;
                 Before   : in   Cursor;
                 Position : in   Cursor)
with Pre => (not Tampering_With.Cursors.Prohibited (Container)
            or else raise Program_Error) and then
            (Position /= No_Element
            or else raise Constraint_Error) and then
            (Has Element (Container, Position)
            or else raise Program_Error) and then
            (Before = No_Element or else
            Has Element (Container, Before)
            or else raise Program_Error),
           Post => Length (Container) = Length (Container)'Old;
```

If Position is No_Element, then Constraint_Error is propagated. If Before does not equal No_Element, and does not designate an element in Container, then Program_Error is propagated. If Position does not equal No_Element, and does not designate a node in Container, then Program_Error is propagated. If Container denotes the same object as Target, then there is no effect if Position equals Before, else the element designated by Position is moved immediately prior to Before, or, if Before equals No_Element, after the last element. In both cases, Position and the length of Target are unchanged. Otherwise, the element designated by Position is removed from Source and moved to Target, immediately prior to Before, or, if Before equals No_Element, after the last element of Target. The length of Target is incremented, the length of Source is decremented, and Position is updated to represent an element in Target.
element in Container, then Program_Error is propagated. If Position does not equal No_Element, and does not designate a node in Container, then Program_Error is propagated. If Position equals No_Element before there is no effect. Otherwise, the element designated by Position is moved immediately prior to Before, or, if Before equals No_Element, after the last element. The length of Container is unchanged.

```ada
function First (Container : List) return Cursor
   with Nonblocking, Global => null, Use Formal => null,
   Post => if not Is Empty (Container)
      then Has Element (Container, First'Result)
      else First'Result = No_Element);

{AI95-00302-03} If Container is empty, First returns No_Element. Otherwise, it returns a cursor that designates the first node in Container.

function First_Element (Container : List) return Element_Type
   with Pre => (not Is Empty (Container)
      or else raise Constraint_Error);

{AI95-00302-03} Equivalent to Element (Container, First_INDEX (Container)).

function Last (Container : List) return Cursor
   with Nonblocking, Global => null, Use Formal => null,
   Post => if not Is Empty (Container)
      then Has Element (Container, Last'Result)
      else Last'Result = No_Element);

{AI95-00302-03} If Container is empty, Last returns No_Element. Otherwise, it returns a cursor that designates the last node in Container.

function Last_Element (Container : List) return Element_Type
   with Pre => (not Is Empty (Container)
      or else raise Constraint_Error);

{AI95-00302-03} Equivalent to Element (Last (Container)).

function Next (Position : Cursor) return Cursor
   with Nonblocking, Global => in all, Use Formal => null,
   Post => if Position = No_Element then Next'Result = No_Element
      elsif Next'Result = No_Element then
         Position = Last (Container)
      else Has Element (Container, Next'Result));

function Next (Container : List;
   Position : Cursor) return Cursor
   with Nonblocking, Global => null, Use Formal => null,
   Pre => Position = No_Element or else Has Element (Container, Position)
      or else raise Program Error,
   Post => if Position = No_Element then Next'Result = No_Element
      elsif Next'Result = No_Element then
         Position = Last (Container)
      else Has Element (Container, Next'Result));

{AI12-0112-1} Returns a cursor designating the successor of the element designated by Position in Container.
```
function Previous (Position : Cursor) return Cursor
  with Nonblocking, Global => in all, Use Formal => null,
  Post => (if Position = No_Element then
            Previous'Result = No_Element);

{AI95-00302-03} If Position equals No_Element or designates the first element of the container, then Previous returns the value No_Element. Otherwise, it returns a cursor that designates the predecessor of the element designated by Position.

function Previous (Container : List; Position : Cursor) return Cursor
  with Nonblocking, Global => null, Use Formal => null;
  Pre => Position = No_Element or else
         Has Element (Container, Position)
  or else raise Program_Error,
  Post => (if Position = No_Element then
            Previous'Result = No_Element
            elsif Previous'Result = No_Element then
            Position = First (Container)
            else Has Element (Container, Previous'Result));

{AI12-0112-1} Returns a cursor designating the predecessor of the element designated by Position in Container, if any.

procedure Next (Position : in out Cursor)
  with Nonblocking, Global => in all, Use Formal => null;
  {AI95-00302-03} Equivalent to Position := Next (Position).

procedure Next (Container : in List; Position : in out Cursor)
  with Nonblocking, Global => null, Use Formal => null;
  Pre => Position = No_Element or else
         Has Element (Container, Position)
  or else raise Program_Error,
  Post => (if Position /= No_Element then
            Has Element (Container, Position));
{AI12-0112-1} Equivalent to Position := Next (Container, Position).

procedure Previous (Position : in out Cursor)
  with Nonblocking, Global => null, Use Formal => null;
  {AI95-00302-03} Equivalent to Position := Previous (Position).

procedure Previous (Container : in List; Position : in out Cursor)
  with Nonblocking, Global => null, Use Formal => null;
  Pre => Position = No_Element or else
         Has Element (Container, Position)
  or else raise Program_Error,
  Post => (if Position /= No_Element then
            Has Element (Container, Position));
{AI12-0112-1} Equivalent to Position := Previous (Container, Position).
function Find (Container : List;
             Item      : Element_Type;
             Position  : Cursor := No_Element)
    return Cursor
with Pre => Position = No_Element or else
           Has_Element (Container, Position)
    or else raise Program_Error,
Post => (if Find'Result /= No_Element
           then Has_Element (Container, Find'Result));

{AI95-00302-03} {AI12-0112-1} If Position is not No_Element, and does not designate an
element in Container, then Program_Error is propagated. Find searches the elements of Container
for an element equal to Item (using the generic formal equality operator). The search starts at the
element designated by Position, or at the first element if Position equals No_Element. It proceeds
towards Last (Container). If no equal element is found, then Find returns No_Element. Otherwise,
it returns a cursor designating the first equal element encountered.

function Reverse_Find (Container : List;
                       Item      : Element_Type;
                       Position  : Cursor := No_Element)
    return Cursor
with Pre => Position = No_Element or else
           Has_Element (Container, Position)
    or else raise Program_Error,
Post => (if Reverse_Find'Result /= No_Element
           then Has_Element (Container, Reverse_Find'Result));

{AI95-00302-03} {AI12-0112-1} If Position is not No_Element, and does not designate an
element in Container, then Program_Error is propagated. Find searches the elements of Container
for an element equal to Item (using the generic formal equality operator). The search starts at the
element designated by Position, or at the last element if Position equals No_Element. It proceeds
Towards First (Container). If no equal element is found, then Reverse_Find returns No_Element.
Otherwise, it returns a cursor designating the first equal element encountered.

function Contains (Container : List;
                  Item      : Element_Type)
    return Boolean;

{AI95-00302-03} Equivalent to Find (Container, Item) /= No_Element.

function Has_Element (Position : Cursor)
    return Boolean;

{AI95-00302-03} {AI05-0212-1} Returns True if Position designates an element, and returns
false otherwise.

To be honest: {AI05-0212-1} This function may not detect cursors that designate deleted elements; such cursors are
invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

Paragraphs 139 and 140 were moved above.

{AI12-0112-1} procedure Iterate
(Container : in List;
Process   : not null access procedure (Position : in Cursor))
with Allows Exit;

{AI95-00302-03} {AI05-0265-1} Iterate calls Process.all with a cursor that designates each node
in Container, starting with the first node and moving the cursor as per the Next function.
TamperingProgram_Error is propagated if Process.all tampers with the cursors of Container is
prohibited during the execution of a call on Process.all. Any exception raised by Process.all is
propagated.

Implementation Note: The purpose of the tamper with cursors check is to prevent erroneous execution from the
Position parameter of Process.all becoming invalid. This check takes place when the operations that tamper with the
cursors of the container are called. The check cannot be made later (say in the body of Iterate), because that could
cause the Position cursor to be invalid and potentially cause execution to become erroneous -- defeating the purpose of the check.

See Iterate for vectors (A.18.2) for a suggested implementation of the check.

{AI12-0112-1} procedure Reverse_Iterate
(Container : in List;
Process   : not null access procedure (Position : in Cursor))
with Allows Exit;

{AI95-00302-03} {AI05-0212-1} Iterates over the nodes in Container as per procedure Iterate, except that elements are traversed in reverse order, starting with the last node and moving the cursor as per the Previous function.

{AI12-0112-1} {AI12-0266-1} function Iterate (Container : in List)
return
List_Iterator_Interfaces.Parallel_Reversible_Iterator'Reversible_Iterator'Class
with Post   => Tampering_With_Cursors_Prohibited (Container);

{AI05-0212-1} {AI05-0265-1} {AI05-0269-1} {AI12-0266-1} Iterate returns a reversible iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each node in Container, starting with the first node and moving the cursor as per the Next function when used as a forward iterator, and starting with the last node and moving the cursor as per the Previous function when used as a reverse iterator, and processing all nodes concurrently when used as a parallel iterator. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop_statement whose iterator_specification denotes this object). The iterator object needs finalization.

function Iterate (Container : in List; Start : in Cursor)
return List_Iterator_Interfaces.Reversible_Iterator'Class
with Pre    => (Start /= No_Element
or else raise Constraint_Error) and then
(Has_Element (Container, Start)
or else raise Program_Error),
Post   => Tampering_With_Cursors_Prohibited (Container);

{AI05-0212-1} {AI05-0262-1} {AI05-0265-1} {AI05-0269-1} {AI12-0266-1} If Start is not No_Element and does not designate an item in Container, then Program_Error is propagated. If Start is No_Element, then Constraint_Error is propagated. Otherwise, Iterate returns a reversible iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each node in Container, starting with the node designated by Start and moving the cursor as per the Next function when used as a forward iterator, or moving the cursor as per the Previous function when used as a reverse iterator. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop_statement whose iterator_specification denotes this object). The iterator object needs finalization.

Discussion: Exits are allowed from the loops created using the iterator objects. In particular, to stop the iteration at a particular cursor, just add

exit when Cur = Stop;

in the body of the loop (assuming that Cur is the loop parameter and Stop is the cursor that you want to stop at).

{AI05-0044-1} {AI05-0262-1} The actual function for the generic formal function "<" of Generic_Sorting is expected to return the same value each time it is called with a particular pair of element values. It should define a strict weak ordering relationship (see A.18), that is, be irreflexive, asymmetric, and transitive; it should not modify Container. If the actual for "<" behaves in some other manner, the behavior of the subprograms of Generic_Sorting are unspecified. The number of how many times the subprograms of Generic_Sorting call "<" is unspecified.
function Is_Sorted (Container : List) return Boolean;

{AI95-00302-03} Returns True if the elements are sorted smallest first as determined by the generic formal "<" operator; otherwise, Is_Sorted returns False. Any exception raised during evaluation of "<" is propagated.

procedure Sort (Container : in out List);

{AI12-0112-1} Reorders the nodes of Container such that the elements are sorted smallest first as determined by the generic formal "<" operator provided. The sort is stable. Any exception raised during evaluation of "<" is propagated.

Ramification: Unlike array sorts, we do require stable sorts here. That's because algorithms in the merge sort family (as described by Knuth) can be both fast and stable. Such sorts use the extra memory as offered by the links to provide better performance.

Note that list sorts never copy elements; it is the nodes, not the elements, that are reordered.

procedure Merge (Target : in out List;
    Source : in out List);

with Pre => not Tampering With Cursors Prohibited (Target)
or else raise Program_Error;

or else raise Program_Error) and then

(not Tampering With Elements Prohibited (Source)
or else raise Program_Error) and then

(Length (Target) <= Count_Type'Last - Length (Source)
or else raise Constraint_Error) and then

((Length (Source) = 0 or else not Target'Has_Same_Storage (Source))
or else raise Constraint_Error),
Post => (declare

Result Length : constant Count_Type :=
    Length (Source)'Old + Length (Target)'Old;

begin
    (Length (Source) = 0 and then
        Length (Target) = Result Length));

{AI95-00302-03} {AI05-0021-1} {AI12-0112-1} If Source is empty, then Merge does nothing. If Source and Target are the same nonempty container object, then Program_Error is propagated. Otherwise, Merge removes elements from Source and inserts them into Target; afterwards, Target contains the union of the elements that were initially in Source and Target; Source is left empty. If Target and Source are initially sorted smallest first, then Target is ordered smallest first as determined by the generic formal "<" operator; otherwise, the order of elements in Target is unspecified. Any exception raised during evaluation of "<" is propagated.

Ramification: It is a bounded error if either of the lists is unsor ted, see below. The bounded error can be recovered by sorting Target after the merge call, or the lists can be pretested with Is_Sorted.

The nested package Doubly Linked Lists.Stable provides a type Stable.List that represents a stable list, which is one that cannot grow and shrink. Such a list can be created by calling the Copy function, or by establishing a stabilized view of an ordinary list.

The subprograms of package Containers.Doubly Linked Lists that have a parameter or result of type List are included in the nested package Stable with the same specification, except that the following are omitted:

Tampering With Cursors Prohibited, Tampering With Elements Prohibited, Assign, Move, Insert, Append, Prepend, Clear, Delete, Delete First, Delete Last, Splice, Swap Links, and Reverse Elements

Ramification: The names List and Cursor mean the types declared in the nested package in these subprogram specifications.
Reason: The omitted routines are those that tamper with cursors or elements (or test that state). The model is that it is impossible to tamper with cursors or elements of a stable view since no such operations are included. Thus tampering checks are not needed for a stable view, and we omit the operations associated with those checks.

The Generic_Sorting generic is omitted entirely, as only function Is_Sorting does not tamper with cursors. It isn't useful enough by itself to include.

{AI12-0111-1} The operations of this package are equivalent to those for ordinary lists, except that the calls to Tampering With Cursors Prohibited and Tampering With Elements Prohibited that occur in preconditions are replaced by False, and any that occur in postconditions are replaced by True.

{AI12-0439-1} If a stable list is declared with the Base discriminant designating a pre-existing ordinary list, the stable list represents a stabilized view of the underlying ordinary list, and any operation on the stable list is reflected on the underlying ordinary list. While a stabilized view exists, any operation that tampers with elements performed on the underlying list is prohibited. The finalization of a stable list that provides such a view removes this restriction on the underlying ordinary list [(though some other restriction can exist due to other concurrent iterations or stabilized views)].

{AI12-0111-1} If a stable list is declared without specifying Base, the object is necessarily initialized. The initializing expression of the stable list, [typically a call on Copy], determines the Length of the list. The Length of a stable list never changes after initialization.

Proof: {AI12-0438-1} Initialization is required as the type is indefinite, see 3.3.1.

Bounded (Run-Time) Errors

{AI95-00302-03} Calling Merge in an instance of Generic_Sorting with either Source or Target not ordered smallest first using the provided generic formal "<" operator is a bounded error. Either Program_Error is raised after Target is updated as described for Merge, or the operation works as defined.

{AI05-0022-1} {AI05-0248-1} It is a bounded error for the actual function associated with a generic formal subprogram, when called as part of an operation of this package, to tamper with elements of any List parameter of the operation. Either Program_Error is raised, or the operation works as defined on the value of the List either prior to, or subsequent to, some or all of the modifications to the List.

{AI05-0027-1} It is a bounded error to call any subprogram declared in the visible part of Containers.Doubly_Linked_Lists when the associated container has been finalized. If the operation takes Container as an in out parameter, then it raises Constraint_Error or Program_Error. Otherwise, the operation either proceeds as it would for an empty container, or it raises Constraint_Error or Program_Error.

Erroneous Execution

{AI95-00302-03} A Cursor value is invalid if any of the following have occurred since it was created:

- The list that contains the element it designates has been finalized;
- The list that contains the element it designates has been used as the Target of a call to Assign, or as the target of an assignment statement;
- [The list that contains the element it designates has been used as the Source or Target of a call to Move;] or

Proof: {AI05-0001-1} Move has been reworded in terms of Assign and Clear, which are covered by other bullets, so this text is redundant.

- The element it designates has been removed from the list that previously contained the element deleted.

To be honest: {AI05-0160-1} The cursor modified by the four parameter Splice is not invalid, even though the element it designates has been removed from the source list, because that cursor has been modified to designate that element in the target list – the cursor no longer designates an element in the source list.
Ramification: \{AI05-0160-1\} This can happen directly via calls to Delete, DeleteLast, Clear, Splice with a Source parameter, and Merge; and indirectly via calls to DeleteFirst, Assign, and Move.

\{AI95-00302-03\} The result of "=" or Has Element is unspecified if it is called with an invalid cursor parameter. Execution is erroneous if any other subprogram declared in Containers.Doubly_Linked_Lists is called with an invalid cursor parameter.

Discussion: The list above is intended to be exhaustive. In other cases, a cursor value continues to designate its original element. For instance, cursor values survive the insertion and deletion of other nodes.

While it is possible to check for these cases, in many cases the overhead necessary to make the check is substantial in time or space. Implementations are encouraged to check for as many of these cases as possible and raise Program_Error if detected.

\{AI05-0212-1\} Execution is erroneous if the list associated with the result of a call to Reference or Constant_Reference is finalized before the result object returned by the call to Reference or Constant_Reference is finalized.

Reason: Each object of Reference_Type and Constant_Reference_Type probably contains some reference to the originating container. If that container is prematurely finalized (which is only possible via Unchecked_Deallocation, as accessibility checks prevent passing a container to Reference that will not live as long as the result), the finalization of the object of Reference_Type will try to access a nonexistent object. This is a normal case of a dangling pointer created by Unchecked_Deallocation; we have to explicitly mention it here as the pointer in question is not visible in the specification of the type. (This is the same reason we have to say this for invalid cursors.)

Implementation Requirements

\{AI95-00302-03\} \{AI12-0437-1\} No storage associated with a doubly-linked list object shall be lost upon assignment or scope exit.

\{AI95-00302-03\} \{AI05-0262-1\} The execution of an assignment statement for a list shall have the effect of copying the elements from the source list object to the target list object and changing the length of the target object to that of the source object.

Implementation Note: \{AI05-0298-1\} An assignment of a List is a “deep” copy; that is the elements are copied as well as the data structures. We say “effect of” in order to allow the implementation to avoid copying elements immediately if it wishes. For instance, an implementation that avoided copying until one of the containers is modified would be allowed. (Note that this implementation would require care, see A.18.2 for more.)

Implementation Advice

\{AI95-00302-03\} Containers.Doubly_Linked_Lists should be implemented similarly to a linked list. In particular, if \(N\) is the length of a list, then the worst-case time complexity of Element, Insert with Count=1, and Delete with Count=1 should be \(O(\log N)\).

Implementation Advice: The worst-case time complexity of Element, Insert with Count=1, and Delete with Count=1 for Containers.Doubly_Linked_Lists should be \(O(\log N)\).

Reason: We do not mean to overly constrain implementation strategies here. However, it is important for portability that the performance of large containers has roughly the same factors on different implementations. If a program is moved to an implementation that takes \(O(N)\) time to access elements, that program could be unusable when the lists are large. We allow \(O(\log N)\) access because the proportionality constant and caching effects are likely to be larger than the log factor, and we don't want to discourage innovative implementations.

\{AI95-00302-03\} The worst-case time complexity of a call on procedure Sort of an instance of Containers.Doubly_Linked_Lists.Generic_Sorting should be \(O(N^{**2})\), and the average time complexity should be better than \(O(N^{**2})\).

Implementation Advice: A call on procedure Sort of an instance of Containers.Doubly_Linked_Lists.Generic_Sorting should have an average time complexity better than \(O(N^{**2})\) and worst case no worse than \(O(N^{**2})\).

Ramification: In other words, we're requiring the use of a better than \(O(N^{**2})\) sorting algorithm, such as Quicksort. No bubble sorts allowed!

\{AI95-00302-03\} Move should not copy elements, and should minimize copying of internal data structures.
Implementation Advice: Containers.Doubly_Linked_Lists.Move should not copy elements, and should minimize copying of internal data structures.

Implementation Note: Usually that can be accomplished simply by moving the pointer(s) to the internal data structures from the Source container to the Target container.

\{AI95-00302-03\} If an exception is propagated from a list operation, no storage should be lost, nor any elements removed from a list unless specified by the operation.

Implementation Advice: If an exception is propagated from a list operation, no storage should be lost, nor any elements removed from a list unless specified by the operation.

Reason: This is important so that programs can recover from errors. But we don't want to require heroic efforts, so we just require documentation of cases where this can't be accomplished.

NOTE \{AI95-00302-03\} \{AI12-0442-1\} Sorting a list never copies elements, and is a stable sort (equal elements remain in the original order). This is different than sorting an array or vector, which will often need to copy elements, and hence is probably not a stable sort.

Extensions to Ada 95

\{AI95-00302-03\} The generic package Containers.Doubly_Linked_Lists is new.

Inconsistencies With Ada 2005

\{AI05-0248-1\} \{AI05-0257-1\} Correction: The Insert versions that return a Position parameter are now defined to return Position = Before if Count = 0. This was unspecified for Ada 2005; so this will only be inconsistent if an implementation did something else and a program depended on that something else — this should be very rare.

Incompatibilities With Ada 2005

\{AI05-0001-1\} Subprograms Assign and Copy are added to Containers.Doubly_Linked_Lists. If an instance of Containers.Doubly_Linked_Lists is referenced in a use clause, and an entity \(E\) with the same defining_identifier as a new entity in Containers.Doubly_Linked_Lists is defined in a package that is also referenced in a use clause, the entity \(E\) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 2005

\{AI05-0212-1\} Added iterator, reference, and indexing support to make list containers more convenient to use.

Wording Changes from Ada 2005

\{AI05-0001-1\} Generalized the definition of Move. Specified which elements are read/written by stream attributes.

\{AI05-0022-1\} Correction: Added a Bounded (Run-Time) Error to cover tampering by generic actual subprograms.

\{AI05-0027-1\} Correction: Added a Bounded (Run-Time) Error to cover access to finalized list containers.

\{AI05-0044-1\} Correction: Redefined \(=\) actuals to require a strict weak ordering; the old definition allowed indeterminant comparisons that would not have worked in a container.

\{AI05-0084-1\} Correction: Added a pragma Remote_Types so that containers can be used in distributed programs.

\{AI05-0160-1\} Correction: Revised the definition of invalid cursors to cover missing (and new) cases.

\{AI05-0257-1\} Correction: Added missing wording to describe the Position after Inserting 0 elements.

\{AI05-0265-1\} Correction: Defined when a container prohibits tampering in order to more clearly define where the check is made and the exception raised.

Inconsistencies With Ada 2012

\{AI12-0111-1\} Correction: Tampering with elements is now defined to be equivalent to tampering with cursors for ordinary containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

Incompatibilities With Ada 2012

\{AI12-0111-1\} \{AI12-0112-1\} \{AI12-0339-1\} \{AI12-0391-1\} A number of new subprograms, types, and even a nested package were added to Containers.Doubly_Linked_Lists to better support contracts and stable views. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.
Extensions to Ada 2012

{AI12-0196-1} Replace Element is now defined such that it can be used concurrently so long as it operates on different elements. This allows some container operations to be used in parallel without separate synchronization.

{AI12-0212-1} {AI12-0391-1} Lists now support positional container aggregates, so aggregate syntax can be used to create Lists.

{AI12-0266-1} The iterator for the entire container now can return a parallel iterator which can be used to process the container in parallel.

Wording Changes from Ada 2012

{AI12-0110-1} Corrigendum: Clarified that tampering checks precede all other checks made by a subprogram (but come after those associated with the call).

{AI12-0112-1} Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).

{AI12-0400-1} Correction: Split the Append routine into two routines rather than having a single routine with a default parameter, in order that a routine with the appropriate profile for the Aggregate aspect exists. This change should not change the behavior of any existing code.

A.18.4 Maps

{AI95-00302-03} The language-defined generic packages Containers.Hashed_Maps and Containers.Ordered_Maps provide private types Map and Cursor, and a set of operations for each type. A map container allows an arbitrary type to be used as a key to find the element associated with that key. A hashed map uses a hash function to organize the keys, while an ordered map orders the keys per a specified relation.

{AI95-00302-03} {AI05-0299-1} This subclause section describes the declarations that are common to both kinds of maps. See A.18.5 for a description of the semantics specific to Containers.Hashed_Maps and A.18.6 for a description of the semantics specific to Containers.Ordered_Maps.

Static Semantics

{AI95-00302-03} The actual function for the generic formal function "=" on Element_Type values is expected to define a reflexive and symmetric relationship and return the same result value each time it is called with a particular pair of values. If it behaves in some other manner, the function "=" on map values returns an unspecified value. The exact arguments and number of calls of this generic formal function by the function "=" on map values are unspecified.

Ramification: If the actual function for "=" is not symmetric and consistent, the result returned by "=" for Map objects cannot be predicted. The implementation is not required to protect against "=" raising an exception, or returning random results, or any other “bad” behavior. And it can call "=" in whatever manner makes sense. But note that only the result of "=" for Map objects is unspecified; other subprograms are not allowed to break if "=" is bad (they aren't expected to use "=").

{AI95-00302-03} The type Map is used to represent maps. The type Map needs finalization (see 7.6).

{AI95-00302-03} A map contains pairs of keys and elements, called nodes. Map cursors designate nodes, but also can be thought of as designating an element (the element contained in the node) for consistency with the other containers. There exists an equivalence relation on keys, whose definition is different for hashed maps and ordered maps. A map never contains two or more nodes with equivalent keys. The length of a map is the number of nodes it contains.

{AI95-00302-03} Each nonempty map has two particular nodes called the first node and the last node (which may be the same). Each node except for the last node has a successor node. If there are no other intervening operations, starting with the first node and repeatedly going to the successor node will visit each node in the map exactly once until the last node is reached. The exact definition of these terms is different for hashed maps and ordered maps.
[Some operations of these generic packages have access to subprogram parameters. To ensure such operations are well-defined, they guard against certain actions by the designated subprogram. In particular, some operations check for “tampering with cursors” of a container because they depend on the set of elements of the container remaining constant, and others check for “tampering with elements” of a container because they depend on elements of the container not being replaced.] When tampering with cursors is prohibited for a particular map object $M$, Program_Error is propagated by the finalization of $M$, as well as by a call that passes $M$ to certain of the operations of this package, as indicated by the precondition of such an operation. Similarly, when tampering with elements is prohibited for $M$, Program_Error is propagated by a call that passes $M$ to certain of the other operations of this package, as indicated by the precondition of such an operation.

Paragraphs 8 through 15 are removed as preconditions now describe these rules.

A subprogram is said to tamper with cursors of a map object $M$ if:

- it inserts or deletes elements of $M$, that is, it calls the Insert, Include, Clear, Delete, or Exclude procedures with $M$ as a parameter; or

  To be honest: Operations which are defined to be equivalent to a call on one of these operations also are included. Similarly, operations which call one of these as part of their definition are included.

- it finalizes $M$; or

- it calls the Assign procedure with $M$ as the Target parameter; or

  Ramification: We don't need to explicitly mention assignment statement, because that finalizes the target object as part of the operation, and finalization of an object is already defined as tampering with cursors.

- it calls the Move procedure with $M$ as a parameter; or

- it calls one of the operations defined to tamper with the cursors of $M$.

  Ramification: Replace only modifies a key and element rather than rehashing, so it does not tamper with cursors.

A subprogram is said to tamper with elements of a map object $M$ if:

- it tampers with cursors of $M$; or

- it replaces one or more elements of $M$, that is, it calls the Replace or Replace_Element procedures with $M$ as a parameter;

  Reason: Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can't be allowed. However, a simple modification of (part of) an element is not a problem, so Update_Element does not cause a problem.

When tampering with cursors is prohibited for a particular map object $M$, Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the cursors of $M$, leaving $M$ unmodified. Similarly, when tampering with elements is prohibited for $M$, Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the elements of $M$, leaving $M$ unmodified. These checks are made before any other defined behavior of the body of the language-defined subprogram.

Proof: Tampering with elements includes tampering with cursors, so we mention it only from completeness in the second sentence.

Empty_Map represents the empty Map object. It has a length of 0. If an object of type Map is not otherwise initialized, it is initialized to the same value as Empty_Map.

No_Element represents a cursor that designates no node. If an object of type Cursor is not otherwise initialized, it is initialized to the same value as No_Element.
The primitive predefined "=" operator for type Cursor returns True if both cursors are No_Element, or designate the same element in the same container.

To be honest: “The primitive "=" operator” is the one with two parameters of type Cursor which returns Boolean. We’re not talking about some other (hidden) primitive function named "=".

Execution of the default implementation of the Input, Output, Read, or Write attribute of type Cursor raises Program_Error.

Reason: A cursor will probably be implemented in terms of one or more access values, and the effects of streaming access values is unspecified. Rather than letting the user stream junk by accident, we mandate that streaming of cursors raise Program_Error by default. The attributes can always be specified if there is a need to support streaming.

Map'Write for a Map object M writes Length(M) elements of the map to the stream. It may also may write additional information about the map.

Map'Read reads the representation of a map from the stream, and assigns to Item a map with the same length and elements as was written by Map'Write.

Ramification: Streaming more elements than the container length is wrong. For implementation implications of this rule, see the Implementation Note in A.18.2.

function Has_Element (Position : Cursor) return Boolean
with Nonblocking, Global => in all, Use Formal => null;

Returns True if Position designates an element, and returns False otherwise.

To be honest: This function might not detect cursors that designate deleted elements; such cursors are invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

function Has_Element (Container : Map; Position : Cursor) return Boolean
with Nonblocking, Global => null, Use Formal => null;

Returns True if Position designates an element in Container, and returns False otherwise.

Ramification: If Position is No_element, Has_Element returns False.

function "=" (Left, Right : Map) return Boolean;

If Left and Right denote the same map object, then the function returns True. If Left and Right have different lengths, then the function returns False. Otherwise, for each key K in Left, the function returns False if:

- a key equivalent to K is not present in Right; or
- the element associated with K in Left is not equal to the element associated with K in Right (using the generic formal equality operator for elements).

If the function has not returned a result after checking all of the keys, it returns True. Any exception raised during evaluation of key equivalence or element equality is propagated.

Implementation Note: This wording describes the canonical semantics. However, the order and number of calls on the formal equality function is unspecified for all of the operations that use it in this package, so an implementation can call it as many or as few times as it needs to get the correct answer. Specifically, there is no requirement to call the formal equality additional times once the answer has been determined.

function Tampering_With_Cursors_Prohibited (Container : Map) return Boolean
with Nonblocking, Global => null, Use Formal => null;

Returns True if tampering with cursors or tampering with elements is currently prohibited for Container, and returns False otherwise.
Reason: {AI12-0112-1} Prohibiting tampering with elements also needs to prohibit tampering with cursors, as deleting an element is similar to replacing it.

Implementation Note: {AI12-0112-1} Various contracts elsewhere in this specification require that this function be implemented with synchronized data. Moreover, it is possible for tampering to be prohibited by multiple operations (sequentially or in parallel). Therefore, tampering needs to be implemented with an atomic or protected counter. The counter is initialized to zero, and is incremented when tampering is prohibited, and decremented when leaving an area that prohibited tampering. Function Tampering_With_Cursors_Prohibited returns True if the counter is nonzero. (Note that any case where the result is not well-defined for one task is incorrect use of shared variables and would be erroneous by the rules of 9.10, so no special protection is needed to read the counter.)

function Tampering_With_Elements_Prohibited (Container : Map) return Boolean
with Nonblocking, Global => null, Use Formal => null;

Reason: {AI12-0112-1} Always returns False, regardless of whether tampering with elements is prohibited.

Reason: {AI12-0111-1} A definite element cannot change size, so we allow operations that tamper with elements even when tampering with elements is prohibited. That's not true for the indefinite containers, which is why this kind of tampering exists.

function Length (Container : Map) return Count_Type
with Nonblocking, Global => null, Use Formal => null;

{AI95-00302-03} Returns the number of nodes in Container.

function Is_Empty (Container : Map) return Boolean
with Nonblocking, Global => null, Use Formal => null,
    Post => 'Is Empty'.Result = (Length (Container) = 0);

{AI95-00302-03} {AI12-0112-1} Returns True if Container is empty. Equivalent to Length (Container) = 0.

procedure Clear (Container : in out Map)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
    or else raise Program_Error,
    Post => Length (Container) = 0;

{AI95-00302-03} Removes all the nodes from Container.

function Key (Position : Cursor) return Key_Type
with Pre => Position /= No_Element
    or else raise Constraint_Error,
    Nonblocking, Global => in all, Use Formal => Key_Type;

{AI95-00302-03} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated. Otherwise, Key returns the key component of the node designated by Position.

function Key (Container : Map; Position : Cursor) return Key_Type
with Pre => (Position /= No_Element
    or else raise Constraint_Error) and then
    Has_Element (Container, Position)
    or else raise Program_Error),
    Nonblocking, Global => null, Use Formal => Key_Type;

{AI12-0112-1} Key returns the key component of the node designated by Position.

function Element (Position : Cursor) return Element_Type
with Pre => Position /= No_Element
    or else raise Constraint_Error,
    Nonblocking, Global => in all, Use Formal => Element_Type;

{AI95-00302-03} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated. Otherwise, Element returns the element component of the node designated by Position.
function Element (Container : Map;  
   Position  : Cursor) return Element_Type 
   with Pre => (Position /= No_Element  
       or else raise Constraint_Error) and then  
       (Has Element (Container, Position)  
       or else raise Program_Error),  
       Nonblocking, Global => null, Use Formal => Element_Type;  

{AI12-0112-1} Element returns the element component of the node designated by Position.

procedure Replace_Element (Container : in out Map;  
   Position  : in Cursor;  
   New_item  : in Element_Type) 
   with Pre => (not Tampering_With_Elements_Prohibited (Container)  
       or else raise Program_Error) and then  
       (Position /= No_Element  
       or else raise Constraint_Error) and then  
       (Has Element (Container, Position)  
       or else raise Program_Error);  

{AI95-00302-03} {AI05-0264-1} {AI12-0112-1} {AI12-0196-1} If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Replace_Element assigns New Item to the element of the node designated by Position. For the purposes of determining whether the parameters overlap in a call to Replace_Element, the Container parameter is not considered to overlap with any object [(including itself)].

procedure Query_Element  
   (Position : in Cursor;  
   Process  : not null access procedure (Key     : in Key_Type;  
                                             Element : in Element_Type)) 
   with Pre => Position /= No_Element  
       or else raise Constraint_Error,  
       Global => in all;  

{AI95-00302-03} {AI05-0021-1} {AI05-0265-1} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated. Otherwise, Query_Element calls Process.all with the key and element from the node designated by Position as the arguments. Tampering with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

procedure Query_Element  
   (Container : in Map;  
   Position  : in Cursor;  
   Process   : not null access procedure (Key     : in Key_Type;  
                                             Element : in Element_Type)) 
   with Pre => (Position /= No_Element  
       or else raise Constraint_Error) and then  
       (Has Element (Container, Position)  
       or else raise Program_Error);  

{AI12-0112-1} Query_Element calls Process.all with the key and element from the node designated by Position as the arguments. Tampering with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.
procedure Update_Element
  (Container : in out Map;
   Position : in Cursor;
   Process  : not null access procedure (Key : in Key_Type;
                                 Element : in out Element_Type))
with Pre => (Position /= No_Element
            or else raise Constraint_Error)
         and then
         (Has_Element (Container, Position)
          or else raise Program_Error);
  {AI95-00302-03} {AI05-0264-1} {AI12-0112-1} If Position equals No_Element,
  then Constraint_Error is propagated; if Position does not designate an element in Container, then
  Program_Error is propagated. Otherwise, Update_Element calls Process.all with the key and
  element from the node designated by Position as the arguments. Tampering
  Program_Error is propagated if Process.all tampers with the elements of Container
  is prohibited during the execution of the call on Process.all. Any exception raised by Process.all
  shall be unconstrained.

Ramification: This means that the elements cannot be directly allocated from the heap; it must be possible to change
the discriminants of the element in place.

{AI12-0112-1} type Constant_Reference_Type
  (Element : not null access constant Element_Type) is private
with Implicit Dereference => Element;
  Nonblocking, Global => in out synchronized,
  Default_Initial_Condition => (raise Program_Error);
  {AI12-0112-1} type Reference_Type (Element : not null access Element_Type) is
  private
with Implicit Dereference => Element,
  Nonblocking, Global => in out synchronized,
  Default_Initial_Condition => (raise Program_Error);
  {AI05-0212-1} The types Constant_Reference_Type and Reference_Type need finalization.

This paragraph was deleted.{AI12-0112-1} The default initialization of an object of type
Constant_Reference_Type or Reference_Type propagates Program_Error.

Reason: It is expected that Reference_Type (and Constant Reference_Type) will be a controlled type, for which
finalization will have some action to terminate the tampering check for the associated container. If the object is created
by default, however, there is no associated container. Since this is useless, and supporting this case would take extra
work, we define it to raise an exception.

{AI12-0112-1} function Constant_Reference
  (Container : aliased in Map;
   Position : in Cursor)
  return Constant_Reference_Type
with Pre => (Position /= No_Element
            or else raise Constraint_Error)
         and then
         (Has_Element (Container, Position)
          or else raise Program_Error),
         Post => Tampering_With_Cursors_Prohibited (Container),
   Nonblocking, Global => null, Use Formal => null;
  {AI05-0212-1} {AI05-0269-1} This function (combined with the Constant Indexing and
  Implicit Dereference aspects) provides a convenient way to gain read access to an individual
element of a Map given a cursor.

{AI05-0212-1} {AI05-0265-1} {AI12-0112-1} If Position equals No_Element, then
  Constraint_Error is propagated; if Position does not designate an element in Container, then
  Program_Error is propagated. Otherwise, Constant_Reference returns an object whose
discriminant is an access value that designates the element designated by Position. Tampering
with the elements of Container is prohibited while the object returned by Constant_Reference exists and has not been finalized.

{AI12-0112-1} function Reference (Container : aliased in out Map; Position : in Cursor) return Reference_Type
             with Pre => (Position /= No_Element or else raise Constraint_Error) and then
             (Has Element (Container, Position) or else raise Program_Error),
             Post => Tampering_With_Cursors_Prohibited (Container),
             Nonblocking, Global => null, Use_Formal => null;

{AI105-0212-1} {AI105-0269-1} This function (combined with the Variable_Indexing and Implicit_Dereference aspects) provides a convenient way to gain read and write access to an individual element of a Map given a cursor.

{AI105-0212-1} {AI105-0265-1} {AI112-0112-1} If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Reference returns an object whose discriminant is an access value that designates the element designated by Position. Tampering with the elements of Container is prohibited while the object returned by Reference exists and has not been finalized.

{AI112-0112-1} function Constant_Reference (Container : aliased in Map; Key : in Key_Type) return Constant_Reference_Type
             with Pre => Find (Container, Key) /= No_Element or else raise Constraint_Error,
             Post => Tampering_With_Cursors_Prohibited (Container),
             Nonblocking, Global => null, Use_Formal => null;

{AI105-0212-1} {AI105-0269-1} This function (combined with the Constant_Indexing and Implicit_Dereference aspects) provides a convenient way to gain read access to an individual element of a map given a key value.

Equivalent to Constant_Reference (Container, Find (Container, Key)).

{AI112-0112-1} function Reference (Container : aliased in out Map; Key : in Key_Type) return Reference_Type
             with Pre => Find (Container, Key) /= No_Element or else raise Constraint_Error,
             Post => Tampering_With_Cursors_Prohibited (Container),
             Nonblocking, Global => null, Use_Formal => null;

{AI105-0212-1} {AI105-0269-1} This function (combined with the Variable_Indexing and Implicit_Dereference aspects) provides a convenient way to gain read and write access to an individual element of a map given a key value.

Equivalent to Reference (Container, Find (Container, Key)).

{AI112-0112-1} procedure Assign (Target : in out Map; Source : in Map)
             with Pre => not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error,
             Post => Length (Source) = Length (Target);

{AI105-0001-1} {AI105-0248-1} If Target denotes the same object as Source, the operation has no effect. Otherwise, the key/element pairs of Source are copied to Target as for an assignment_statement assigning Source to Target.

Discussion: {AI105-0005-1} This routine exists for compatibility with the bounded map containers. For an unbounded map, Assign(A, B) and A := B behave identically. For a bounded map, := will raise an exception if the container capacities are different, while Assign will not raise an exception if there is enough room in the target.
procedure Move (Target : in out Map;
  Source : in out Map)
with Pre => (not Tampering With Cursors Prohibited (Target)
  or else raise Program Error) and then
  (not Tampering With Cursors Prohibited (Source)
  or else raise Program Error),
Post => (if not Target'Has Same Storage (Source) then
  Length (Target) = Length (Source'Old) and then
  Length (Source) = 0);

If Target denotes the same object as Source, then the operation Move has no effect. Otherwise, the operation is equivalent to Assign (Target, Source) followed by Clear (Source). Move first calls Clear (Target). Then, each node from Source is removed from Source and inserted into Target. The length of Source is 0 after a successful call to Move.

procedure Insert (Container : in out Map;
  Key       : in Key_Type;
  New_Item  : in Element_Type;
  Position  : out Cursor;
  Inserted  : out Boolean)
with Pre => (not Tampering With Cursors Prohibited (Container)
  or else raise Program Error) and then
  (Length (Container) <= Count_Type'Last - 1
  or else raise Constraint_Error),
Post => (declare
  Original_Length : constant Count_Type :=
  Length (Container)'Old;
begin
  Has_Element (Container, Position) and then
  if Inserted then
    Length (Container) = Original_Length + 1
  else
    Length (Container) = Original_Length);

Insert checks if a node with a key equivalent to Key is already present in Container. If a match is found, Inserted is set to False and Position designates the element with the matching key. Otherwise, Insert allocates a new node, initializes it to Key and New_Item, and adds it to Container; Inserted is set to True and Position designates the newly-inserted node. Any exception raised during allocation is propagated and Container is not modified.

procedure Insert (Container : in out Map;
  Key       : in Key_Type;
  Position  : out Cursor;
  Inserted  : out Boolean)
with Pre => (not Tampering With Cursors Prohibited (Container)
  or else raise Program Error) and then
  (Length (Container) <= Count_Type'Last - 1
  or else raise Constraint_Error),
Post => (declare
  Original_Length : constant Count_Type :=
  Length (Container)'Old;
begin
  Has_Element (Container, Position) and then
  if Inserted then
    Length (Container) = Original_Length + 1
  else
    Length (Container) = Original_Length);

Insert inserts Key into Container as per the five-parameter Insert, with the difference that an element initialized by default (see 3.3.1) is inserted.
procedure Insert (Container : in out Map;
  Key : in Key_Type;
  New_Item : in Element_Type)
with Pre => not Tampering_With.Cursors.Prohibited (Container)
or else raise Program_Error)
and then
  (Length (Container) <= Count_Type'Last - 1
  or else raise Constraint_Error),
Post => Length (Container) = Length (Container)'Old + 1;

Insert inserts Key and New_Item into Container as per the five-parameter Insert, with the difference that if a node with a key equivalent to Key is already in the map, then Constraint_Error is propagated.

Ramification: This is equivalent to:

declare
  Inserted : Boolean; C : Cursor;
begin
  Insert (Container, Key, New_Item, C, Inserted);
  if not Inserted then
    raise Constraint_Error;
  end if;
end;

but doesn't require the hassle of out parameters.

procedure Include (Container : in out Map;
  Key : in Key_Type;
  New_Item : in Element_Type)
with Pre => not Tampering_With.Cursors.Prohibited (Container)
or else raise Program_Error)
and then
  (Length (Container) <= Count_Type'Last - 1
  or else raise Constraint_Error),
Post => Length (Container) = Length (Container)'Old + 1;

Include inserts Key and New_Item into Container as per the five-parameter Insert, with the difference that if a node with a key equivalent to Key is already in the map, then this operation assigns Key and New_Item to the matching node. Any exception raised during assignment is propagated.

Ramification: This is equivalent to:

declare
  C : Cursor := Find (Container, Key);
begin
  if C = No_Element then
    Insert (Container, Key, New_Item);
  else
    Replace (Container, Key, New_Item);
  end if;
end;

but this avoids doing the search twice.

procedure Replace (Container : in out Map;
  Key : in Key_Type;
  New_Item : in Element_Type)
with Pre => not Tampering_With.Cursors.Prohibited (Container)
or else raise Program_Error)
Post => Length (Container) = Length (Container)'Old;

Replace checks if a node with a key equivalent to Key is present in Container. If a match is found, Replace assigns Key and New_Item to the matching node; otherwise, Constraint_Error is propagated.
Discussion: We update the key as well as the element, as the key might include additional information that does not participate in equivalence. If only the element needs to be updated, use Replace_Element (Find (Container, Key), New_Element).

procedure Exclude (Container : in out Map; Key : in Key_Type)

with Pre => not Tampering With Cursors Prohibited (Container)
    or else raise Program_Error,
    Post => (declare
        Original Length : constant Count_Type :=
            Length (Container)'Old;
        begin
            Length (Container)
            in Original Length - 1 | Original Length);

{AI12-0112-1} Exclude checks if a node with a key equivalent to Key is present in Container. If a match is found, Exclude removes the node from the map.

Ramification: Exclude should work on an empty map; nothing happens in that case.

procedure Delete (Container : in out Map; Key : in Key_Type)

with Pre => not Tampering With Cursors Prohibited (Container)
    or else raise Program_Error,
    Post => Length (Container) = Length (Container)'Old - 1;

{AI195-00302-03} Delete checks if a node with a key equivalent to Key is present in Container. If a match is found, Delete removes the node from the map; otherwise, Constraint_Error is propagated.

procedure Delete (Container : in out Map; Position : in out Cursor)

with Pre => (not Tampering With Cursors Prohibited (Container)
    or else raise Program_Error) and then
    (Position /= No_Element
    or else raise Constraint_Error) and then
    (Has_Element (Container, Position)
    or else raise Program_Error),
    Post => Length (Container) = Length (Container)'Old - 1 and then
    Position = No_Element;

{AI195-00302-03} If Position equals No_Element, then Constraint_Error is propagated. If Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Delete removes the node designated by Position from the map. Position is set to No_Element on return.

Ramification: The check on Position checks that the cursor does not belong to some other map. This check implies that a reference to the map is included in the cursor value. This wording is not meant to require detection of dangling cursors; such cursors are defined to be invalid, which means that execution is erroneous, and any result is allowed (including not raising an exception).

function First (Container : Map) return Cursor

with Nonblocking, Global => null, Use Formal => null,
    Post => (if not Is Empty (Container)
        then Has_Element (Container, First'Result)
        else First'Result = No_Element);

{AI195-00302-03} If Length (Container) = 0, then First returns No_Element. Otherwise, First returns a cursor that designates the first node in Container.
function Next (Position : Cursor) return Cursor
   with Nonblocking, Global => in all, Use Formal => null,
   Post => (if Position = No Element then Next'Result = No Element);

{AI95-00302-03} Returns a cursor that designates the successor of the node designated by Position. If Position designates the last node, then No_Element is returned. If Position equals No_Element, then No_Element is returned.

function Next (Container : Map;
   Position  : Cursor)
   return Cursor
   with Nonblocking, Global => null, Use Formal => null,
   Pre => Position = No Element or else
      Has Element (Container, Position)
   or else raise Program_Error,
   Post => (if Position = No Element then Next'Result = No_Element
           elsif Next'Result = No Element then
              Position = Last (Container)
           else Has Element (Container, Next'Result));

{AI12-0112-1} Returns a cursor designating the successor of the node designated by Position in Container.

{AI12-0112-1} procedure Next (Position : in out Cursor)
   with Nonblocking, Global => in all, Use Formal => null;

{AI95-00302-03} Equivalent to Position := Next (Position).

procedure Next (Container : in Map;
   Position  : in out Cursor)
   with Nonblocking, Global => null, Use Formal => null,
   Pre => Position = No Element or else
      Has Element (Container, Position)
   or else raise Program_Error,
   Post => (if Position /= No_Element
           then Has Element (Container, Position));

{AI12-0112-1} Equivalent to Position := Next (Container, Position).

function Find (Container : Map;
   Key       : Key_Type)
   return Cursor
   with Post => (if Find'Result = No Element
                  then Has Element (Container, Find'Result));

{AI95-00302-03} If Length (Container) equals 0, then Find returns No_Element. Otherwise, Find checks if a node with a key equivalent to Key is present in Container. If a match is found, a cursor designating the matching node is returned; otherwise, No_Element is returned.

function Element (Container : Map;
   Key       : Key_Type)
   return Element_Type;

{AI95-00302-03} Equivalent to Element (Find (Container, Key)).

function Contains (Container : Map;
   Key       : Key_Type)
   return Boolean;

{AI95-00302-03} Equivalent to Find (Container, Key) /= No_Element.

function Has_Element (Position : Cursor) return Boolean;

{AI95-00302-03} {AI05-0212-1} Returns True if Position designates an element, and returns False otherwise.

To be honest: {AI05-0212-1} This function may not detect cursors that designate deleted elements; such cursors are invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

Paragraphs 72 and 73 were moved above.
procedure Iterate
(Container : in Map;
Process : not null access procedure (Position : in Cursor))
with Allows Exit;

Iterate calls Process.all with a cursor that designates each node in Container, starting with the first node and moving the cursor according to the successor relation. TamperingProgram_Error is propagated if Process.all tampers with the cursors of Container is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.

Implementation Note: The “tamper with cursors” check takes place when the operations that insert or delete elements, and so on, are called.

See Iterate for vectors (A.18.2) for a suggested implementation of the check.

The nested package Stable provides a type Stable.Map that represents a stable map, which is one that cannot grow and shrink. Such a map can be created by calling the Copy function, or by establishing a stabilized view of an ordinary map.

The subprograms of the map package that have a parameter or result of type Map are included in the nested package Stable with the same specification, except that the following are omitted:

Tampering With Cursors Prohibited, Tampering With Elements Prohibited, Assign, Move, Insert, Include, Clear, Delete, Exclude, (for Ordered Maps) Delete First and Delete Last, and (for Hashed Maps) Reserve Capacity

Ramification: The names Map and Cursor mean the types declared in the nested package in these subprogram specifications.

Reason: The omitted routines are those that tamper with cursors or elements (or test that state). The model is that it is impossible to tamper with cursors or elements of a stable view since no such operations are included. Thus tampering checks are not needed for a stable view, and we omit the operations associated with those checks.

The operations of this package are equivalent to those for ordinary maps, except that the calls to Tampering With Cursors Prohibited and Tampering With Elements Prohibited that occur in preconditions are replaced by False, and any that occur in postconditions are replaced by True.

If a stable map is declared with the Base discriminant designating a pre-existing ordinary map, the stable map represents a stabilized view of the underlying ordinary map, and any operation on the stable map is reflected on the underlying ordinary map. While a stabilized view exists, any operation that tampers with elements performed on the underlying map is prohibited. The finalization of a stable map that provides such a view removes this restriction on the underlying ordinary map [(though some other restriction can exist due to other concurrent iterations or stabilized views)].

If a stable map is declared without specifying Base, the object is necessarily initialized. The initializing expression of the stable map, [typically a call on Copy], determines the Length of the map. The Length of a stable map never changes after initialization.

Proof: Initialiation is required as the type is indefinite, see 3.3.1.

Bounded (Run-Time) Errors

It is a bounded error for the actual function associated with a generic formal subprogram, when called as part of an operation of a map package, to tamper with elements of any map parameter of the operation. Either Program_Error is raised, or the operation works as defined on the value of the map either prior to, or subsequent to, some or all of the modifications to the map.

It is a bounded error to call any subprogram declared in the visible part of a map package when the associated container has been finalized. If the operation takes Container as an in out parameter,
then it raises Constraint_Error or Program_Error. Otherwise, the operation either proceeds as it would for an empty container, or it raises Constraint_Error or Program_Error.

Erroneous Execution

{AI95-00302-03} A Cursor value is invalid if any of the following have occurred since it was created:

- The map that contains the node it designates has been finalized;
- {AI05-0160-1} The map that contains the node it designates has been used as the Target of a call to Assign, or as the target of an assignment_statement;
- The map that contains the node it designates has been used as the Source or Target of a call to Move; or
- {AI05-0160-1} {AI05-0262-1} The node it designates has been removed from the map that previously contained the node.

Ramification: {AI05-0160-1} This can happen directly via calls to Clear, Exclude, and Delete.

The result of "=" or Has Element is unspecified if these functions are called with an invalid cursor parameter. Execution is erroneous if any other subprogram declared in Containers.Hashed_Maps or Containers.Ordered_Maps is called with an invalid cursor parameter.

Discussion: The list above is intended to be exhaustive. In other cases, a cursor value continues to designate its original element. For instance, cursor values survive the insertion and deletion of other nodes.

While it is possible to check for these cases, in many cases the overhead necessary to make the check is substantial in time or space. Implementations are encouraged to check as many of these cases as possible and raise Program_Error if detected.

{AI05-0212-1} Execution is erroneous if the map associated with the result of a call to Reference or Constant_Reference is finalized before the result object returned by the call to Reference or Constant_Reference is finalized.

Reason: Each object of Reference_Type and Constant_Reference_Type probably contains some reference to the originating container. If that container is prematurely finalized (which is only possible via Unchecked_Deallocation, as accessibility checks prevent passing a container to Reference that will not live as long as the result), the finalization of the object of Reference_Type will try to access a nonexistent object. This is a normal case of a dangling pointer created by Unchecked_Deallocation; we have to explicitly mention it here as the pointer in question is not visible in the specification of the type. (This is the same reason we have to say this for invalid cursors.)

Implementation Requirements

{AI95-00302-03} {AI12-0437-1} No storage associated with a map object shall be lost upon assignment or scope exit.

{AI95-00302-03} {AI05-0262-1} The execution of an assignment_statement for a map shall have the effect of copying the elements from the source map object to the target map object and changing the length of the target object to that of the source object.

Implementation Note: {AI05-0298-1} An assignment of a Map is a “deep” copy; that is the elements are copied as well as the data structures. We say “effect of” in order to allow the implementation to avoid copying elements immediately if it wishes. For instance, an implementation that avoided copying until one of the containers is modified would be allowed. (Note that this implementation would require care, see A.18.2 for more.)

Implementation Advice

{AI95-00302-03} Move should not copy elements, and should minimize copying of internal data structures.

Implementation Advice: Move for a map should not copy elements, and should minimize copying of internal data structures.

Implementation Note: Usually that can be accomplished simply by moving the pointer(s) to the internal data structures from the Source container to the Target container.
If an exception is propagated from a map operation, no storage should be lost, nor any elements removed from a map unless specified by the operation.

Implementation Advice: If an exception is propagated from a map operation, no storage should be lost, nor any elements removed from a map unless specified by the operation.

Reason: This is important so that programs can recover from errors. But we don't want to require heroic efforts, so we just require documentation of cases where this can't be accomplished.

Wording Changes from Ada 95

This description of maps is new; the extensions are documented with the specific packages.

Extensions to Ada 2005

Added reference support to make map containers more convenient to use.

Wording Changes from Ada 2005

Added procedure Assign; the extension and incompatibility is documented with the specific packages.

Generalized the definition of Move. Specified which elements are read/written by stream attributes.

Correction: Added a Bounded (Run-Time) Error to cover tampering by generic actual subprograms.

Correction: Added a Bounded (Run-Time) Error to cover access to finalized map containers.

Correction: Revised the definition of invalid cursors to cover missing (and new) cases.

Correction: Defined when a container prohibits tampering in order to more clearly define where the check is made and the exception raised.

Inconsistencies With Ada 2012

Tampering with elements is now defined to be equivalent to tampering with cursors for ordinary containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

Extensions to Ada 2012

Correction: Replace Element is now defined such that it can be used concurrently so long as it operates on different elements. This allows some container operations to be used in parallel without separate synchronization.

Wording Changes from Ada 2012

Clarified that tampering checks precede all other checks made by a subprogram (but come after those associated with the call).

Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).
A.18.5 The Generic Package Containers.Hashed_Maps

Static Semantics

{AI95-00302-03} The generic library package Containers.Hashed_Maps has the following declaration:

{AI05-0084-1} {AI05-0212-1} {AI12-0112-1} with Ada.Iterator_Interfaces;

generic

  type Key_Type is private;
  type Element_Type is private;
  with function Hash (Key : Key_Type) return Hash_Type;
  with function Equivalent_Keys (Left, Right : Key_Type) return Boolean;
  with function "=" (Left, Right : Element_Type) return Boolean is <>;

package Ada.Containers.Hashed_Maps is

  with Preelaborate, Remote_Types, Nonblocking, Global => in out synchronized is

  pragma Preelaborate(Hashed_Maps);

  pragma Remote_Types(Hashed_Maps);

  Discussion: {AI12-0112-1} For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).

{AI05-0212-1} {AI12-0112-1} {AI12-0212-1} {AI12-0339-1} {AI12-0339-1}

  type Map is tagged private
    with Constant_Indexing => Constant_Reference,
    Variable_Indexing => Reference,
    Default_Iterator => Iterate,
    Iterator_Element => Element_Type,
    Iterator_View => Stable.Map,
    Aggregate => (Empty => Empty, Add Named => Insert),
    Stable_Properties => (Length, Tampering_With_Cursors_Prohibited, Tampering_With_Elements_Prohibited),
    Default_Initial_Condition =>
      Length (Map) = 0 and then
      (not Tampering_With_Cursors_Prohibited (Map)) and then
      (not Tampering_With_Elements_Prohibited (Map)),
    pragma Preelaborable_Initialization(Map);

  Discussion: {AI12-0112-1} Unlike a Vector, the Stable_Properties of a Hashed_Map do not include the Capacity. If we had included it, some of the otherwise shared definitions would need different postconditions for Hashed_Maps and Ordered_Maps. If we were starting these containers from scratch, we probably would have approached the sharing of definitions differently so that we could avoid issues like this, but a major reorganization of this existing material would be too much change.

{AI12-0399-1} type Cursor is private
  with Preelaborable_Initialization(Cursor);

  Empty_Map : constant Map;
  No_Element : constant Cursor;

{AI05-0212-1} {AI12-0112-1} function Has_Element (Position : Cursor) return Boolean
  with Nonblocking, Global => in all, Use Formal => null;

{AI12-0112-1} function Has_Element (Container : Map; Position : Cursor)
  return Boolean
  with Nonblocking, Global => null, Use Formal => null;

{AI05-0212-1} package Map_Iterator_Interfaces is new Ada.Iterator_Interfaces (Cursor, Has_Element);

  function "=" (Left, Right : Map) return Boolean;
function Tampering_With_Cursors_Prohibited
(Container : Map) return Boolean
    with Nonblocking, Global => null, Use Formal => null;

function Tampering_With_Elements_Prohibited
(Container : Map) return Boolean
    with Nonblocking, Global => null, Use Formal => null;

function Empty (Capacity : Count_Type := implementation-defined)
    return Map
    with Post =>
                Capacity (Empty'Result) => Capacity and then
                not Tampering_With_Elements_Prohibited (Empty'Result) and then
                not Tampering_With_Cursors_Prohibited (Empty'Result) and then
                Length (Empty'Result) = 0;

function Capacity (Container : Map) return Count_Type
    with Nonblocking, Global => null, Use Formal => null;

procedure Reserve_Capacity (Container : in out Map;
Capacity : in Count_Type)
    with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Capacity (Container) = Capacity (Container)'Old
and then
Length (Container) = 0;

function Length (Container : Map) return Count_Type
    with Nonblocking, Global => null, Use Formal => null;

function Is_Empty (Container : Map) return Boolean
    with Nonblocking, Global => null, Use Formal => null,
Post => Is Empty'Result = (Length (Container) = 0);

procedure Clear (Container : in out Map)
    with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Capacity (Container) = Capacity (Container)'Old
and then
Length (Container) = 0;

function Key (Position : Cursor) return Key_Type
    with Pre => Position /= No_Element
or else raise Constraint_Error,
Nonblocking, Global => in all, Use Formal => Key_Type;

function Key (Container : Map; Position : Cursor) return Key_Type
    with Pre => (Position /= No_Element
or else raise Constraint_Error) and then
      (Has Element (Container, Position)
or else raise Program_Error),
Nonblocking, Global => null, Use Formal => Key_Type;

function Element (Position : Cursor) return Element_Type
    with Pre => Position /= No_Element
or else raise Constraint_Error,
Nonblocking, Global => in all, Use Formal => Element_Type;

function Element (Container : Map; Position : Cursor) return Element_Type
    with Pre => (Position /= No_Element
or else raise Constraint_Error) and then
      (Has Element (Container, Position)
or else raise Program_Error),
Nonblocking, Global => null, Use Formal => Element_Type;

procedure Replace_Element (Container : in out Map;
Position : in Cursor;
New Item : in Element_Type)
    with Pre => (not Tampering_With_Elements_Prohibited (Container)
or else raise Program_Error) and then
      (Position /= No_Element
or else raise Constraint_Error) and then
      (Has Element (Container, Position)
or else raise Program_Error);
procedure Query_Element
(Position : in Cursor;
Process  : not null access procedure (Key     : in Key_Type;
Element : in Element_Type))
with Pre => Position /= No_Element
         or else raise Constraint_Error,
Global => in all;
procedure Query_Element
(Container : in Map;
Position  : in Cursor;
Process   : not null access procedure (Key     : in Key_Type;
Element : in Element_Type))
with Pre => (Position /= No_Element
         or else raise Constraint_Error) and then
         (Has_Element (Container, Position)
         or else raise Program_Error);
procedure Update_Element
(Container : in out Map;
Position  : in Cursor;
Process   : not null access procedure (Key     : in Key_Type;
Element : in out Element_Type))
with Pre => (Position /= No_Element
         or else raise Constraint_Error) and then
         (Has_Element (Container, Position)
         or else raise Program_Error);

function Constant_Reference (Container : aliased in
Map;
Position  : in Cursor)
return Constant_Reference_Type
with Pre => (Position /= No_Element
         or else raise Constraint_Error) and then
         (Has_Element (Container, Position)
         or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container),
Nonblocking, Global => null, Use_Formal => null;
function Reference (Container : aliased in out Map;
Position  : in Cursor)
return Reference_Type
with Pre => (Position /= No_Element
         or else raise Constraint_Error) and then
         (Has_Element (Container, Position)
         or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container),
Nonblocking, Global => null, Use_Formal => null;
function Constant_Reference (Container : aliased in
Map;
Key       : in Key_Type)
return Constant_Reference_Type
with Pre => Find (Container, Key) /= No_Element
         or else raise Constraint_Error,
Post => Tampering_With_Cursors_Prohibited (Container),
Nonblocking, Global => null, Use_Formal => null;
function Reference (Container : aliased in out Map;
  Key       : in Key_Type)
  return Reference_Type
  with Pre => Find (Container, Key) /= No_Element
  or else raise Constraint_Error,
  Post => Tampering With Cursors Prohibited (Container),
  Nonblocking, Global => null, Use Formal => null;

procedure Assign (Target : in out Map; Source : in Map)
  with Pre => not Tampering With Cursors Prohibited (Target)
  or else raise Program_Error,
  Post => Length (Source) = Length (Target) and then
  Capacity (Target) => Length (Source),
  Length (Source) = Length (Source);

function Copy (Source : Map; Capacity : Count_Type
  := 0)
  return Map
  with Pre => Capacity = 0 or else Capacity >= Length (Source)
  or else raise Capacity_Error,
  Post =>
    Length (Copy'Result) = Length (Source) and then
    not Tampering With Elements Prohibited (Copy'Result) and then
    not Tampering With Cursors Prohibited (Copy'Result) and then
    Copy'Result.Capacity = (if Capacity = 0 then
    Length (Source) else Capacity);

procedure Move (Target : in out Map;
  Source : in out Map)
  with Pre => (not Tampering With Cursors Prohibited (Target)
  or else raise Program_Error) and then
  (not Tampering With Cursors Prohibited (Source)
  or else raise Program_Error),
  Post => (if not Target'Has_Same_Storage (Source) then
  Length (Target) = Length (Source)'Old and then
  Length (Source) = 0);

procedure Insert (Container : in out Map;
  Key       : in Key_Type;
  New_Item  : in Element_Type;
  Position  : out Cursor;
  Inserted  : out Boolean)
  with Pre => (not Tampering With Cursors Prohibited (Container)
  or else raise Program_Error) and then
  (Length (Container) <= Count_Type'Last - 1
  or else raise Constraint_Error),
  Post => (declare
  Original Length : constant Count_Type :=
  Length (Container)'Old;
  begin
  Has_Element (Container, Position) and then
  (if Inserted then
  Length (Container) = Original Length + 1
  else
  Capacity (Container) => Length (Container));
procedure Insert (Container : in out Map;
    Key       : in     Key_Type;
    Position  : out    Cursor;
    Inserted  : out    Boolean)
with Pre  => (not Tampering With Cursors Prohibited (Container)
    or else raise Program Error) and then
    (Length (Container) <= Count_Type'Last - 1
    or else raise Constraint_Error),
Post => (declare
    Original Length : constant Count_Type :=
    Length (Container)'Old;
begin
    Has_Element (Container, Position) and then
    (if Inserted then
      Length (Container) = Original Length + 1
    else
      Length (Container) = Original Length) and then
    Capacity (Container) >= Length (Container);

procedure Insert (Container : in out Map;
    Key       : in     Key_Type;
    New_Item  : in     Element_Type)
with Pre  => (not Tampering With Cursors Prohibited (Container)
    or else raise Program Error) and then
    (Length (Container) <= Count_Type'Last - 1
    or else raise Constraint_Error),
Post => Length (Container) = Length (Container)'Old + 1 and then
    Capacity (Container) >= Length (Container);

procedure Include (Container : in out Map;
    Key       : in     Key_Type;
    New_Item  : in     Element_Type)
with Pre  => (not Tampering With Cursors Prohibited (Container)
    or else raise Program Error) and then
    (Length (Container) <= Count_Type'Last - 1
    or else raise Constraint_Error),
Post => (declare
    Original Length : constant Count_Type :=
    Length (Container)'Old;
begin
    Length (Container)
    in Original Length | Original Length + 1) and then
    Capacity (Container) >= Length (Container);

procedure Replace (Container : in out Map;
    Key       : in     Key_Type;
    New_Item  : in     Element_Type)
with Pre  => not Tampering With Cursors Prohibited (Container)
    or else raise Program Error,
Post => Length (Container) = Length (Container)'Old;

procedure Exclude (Container : in out Map;
    Key       : in     Key_Type)
with Pre  => not Tampering With Cursors Prohibited (Container)
    or else raise Program Error,
Post => (declare
    Original Length : constant Count_Type :=
    Length (Container)'Old;
begin
    Length (Container)
    in Original Length - 1 | Original Length);

procedure Delete (Container : in out Map;
    Key       : in     Key_Type)
with Pre  => not Tampering With Cursors Prohibited (Container)
    or else raise Program Error,
Post => Length (Container) = Length (Container)'Old - 1;
procedure Delete (Container : in out Map; Position : in out Cursor)
  with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
  (Position /= No_Element
  or else raise Constraint_Error) and then
  (Has_Element (Container, Position)
or else raise Program_Error),
  Post => Length (Container) = Length (Container)'Old - 1 and then
  Position = No_Element;

function First (Container : Map) return Cursor
  with Nonblocking, Global => null, Use Formal => null,
  Post => (if not Is_Empty (Container)
  then Has_Element (Container, First'Result)
  else First'Result = No_Element);

function Next (Position : Cursor) return Cursor
  with Nonblocking, Global => in all, Use Formal => null,
  Post => (if Position = No_Element then Next'Result = No_Element);

function Next (Container : Map; Position : in out Cursor)
  with Nonblocking, Global => null, Use Formal => null,
  Pre => Position = No_Element or else
  Has_Element (Container, Position)
or else raise Program_Error,
  Post => (if Position = No_Element then Next'Result = No_Element
  elsif Next'Result = No_Element then
  Position = Last (Container)
  else Has_Element (Container, Next'Result));

procedure Next (Position : in out Cursor)
  with Nonblocking, Global => in all, Use Formal => null;

procedure Next (Container : in Map; Position : in out Cursor)
  with Nonblocking, Global => null, Use Formal => null,
  Pre => Position = No_Element or else
  Has_Element (Container, Position)
or else raise Program_Error,
  Post => (if Position /= No_Element
  then Has_Element (Container, Position)));

procedure Next (Container : in Map; Position : in out Cursor)
  with Nonblocking, Global => null, Use Formal => null,
  Pre => Position = No_Element or else
  Has_Element (Container, Position)
or else raise Program_Error,
  Post => (if Position /= No_Element
  then Has_Element (Container, Position)));

function Find (Container : Map; Key : Key_Type)
  return Cursor
  with Post => (if Find'Result /= No_Element
  then Has_Element (Container, Find'Result));

function Element (Container : Map; Key : Key_Type)
  return Element_Type;

function Contains (Container : Map; Key : Key_Type) return Boolean;

This paragraph was deleted.

function Has_Element (Position : Cursor) return Boolean;

function Equivalent_Keys (Left, Right : Cursor) return Boolean
  with Pre => (Left /= No_Element and then Right /= No_Element)
or else raise Constraint_Error,
  Global => in all;

function Equivalent_Keys (Left : Cursor; Right : Key_Type) return Boolean
  with Pre => Left /= No_Element or else raise Constraint_Error,
  Global => in all;
function Equivalent_Keys (Left : Key_Type; Right : Cursor)
return Boolean
with Pre => Right /= No_Element or else raise Constraint_Error,
Global => in all;

procedure Iterate
(Container : in Map;
Process   : not null access procedure (Position : in Cursor))
with Allows_Exit;

function Iterate (Container : in Map)
return Map_Iterator_Interfaces.Parallel_IteratorForward_Iterator'Class
with Post => Tampering_With_Cursors_Prohibited (Container);

package Stable is
tagged limited private
with Constant_Indexing => Constant_Reference,
Variable_Indexing => Reference,
Default_Iterator => Iterate,
Iterator_Element => Element_Type,
Stable_Properties => (Length),
Global => null,
Default_Initial_Condition => Length (Map) = 0,
Preelaborable_Initialization;

package Map_Iterator_Interfaces is new Ada.Iterator_Interfaces (Cursor, Has_Element);

procedure Assign (Target : in out Hashed_Maps.Map;
Source : in Map)
with Post => Length (Source) = Length (Target);

function Copy (Source : Hashed_Maps.Map)
return Map
with Post => Length (Copy'Result) = Length (Source);

type Constant_Reference_Type
(Element : not null access constant Element_Type)

with Implicit_Dereference => Element,
Nonblocking, Global => null, Use_Formal => null,
Default_Initial.Condition => (raise Program_Error);

type Reference_Type
(Element : not null access Element_Type)

with Implicit_Dereference => Element,
Nonblocking, Global => null, Use_Formal => null,
Default_Initial.Condition => (raise Program_Error);

-- Additional subprograms as described in the text
-- are declared here.

private
... -- not specified by the language

end Ada.Containers.Hashed_Maps;
An object of type `Map` contains an expandable hash table, which is used to provide direct access to nodes. The *capacity* of an object of type `Map` is the maximum number of nodes that can be inserted into the hash table prior to it being automatically expanded.

**Implementation Note:** The expected implementation for a `Map` uses a hash table which is grown when it is too small, with linked lists hanging off of each bucket. Note that in that implementation a cursor needs a back pointer to the `Map` object to implement iteration; that could either be in the nodes, or in the cursor object. To provide an average $O(1)$ access time, capacity would typically equal the number of buckets in such an implementation, so that the average bucket linked list length would be no more than 1.0.

There is no defined relationship between elements in a hashed map. Typically, iteration will return elements in the order that they are hashed in.

Two keys $K_1$ and $K_2$ are defined to be *equivalent* if `Equivalent_Keys(K_1, K_2)` returns `True`.

The actual function for the generic formal function `Hash` is expected to return the same value each time it is called with a particular key value. For any two equivalent key values, the actual for `Hash` is expected to return the same value. If the actual for `Hash` behaves in some other manner, the behavior of this package is unspecified. Which subprograms of this package call `Hash`, and how many times they call it, is unspecified.

**Implementation Note:** The implementation is not required to protect against `Hash` raising an exception, or returning random numbers, or any other “bad” behavior. It's not practical to do so, and a broken `Hash` function makes the container unusable.

The implementation can call `Hash` whenever it is needed; we don't want to specify how often that happens. The result must remain the same (this is a logically pure function), or the behavior is unspecified.

The actual function for the generic formal function `Equivalent_Keys` on `Key_Type` values is expected to return the same value each time it is called with a particular pair of key values. It should define an equivalence relationship, that is, be reflexive, symmetric, and transitive. If the actual for `Equivalent_Keys` behaves in some other manner, the behavior of this package is unspecified. Which subprograms of this package call `Equivalent_Keys`, and how many times they call it, is unspecified.

**Implementation Note:** As with `Hash`, the implementation is not required to protect against `Equivalent_Keys` raising an exception or returning random results. Similarly, the implementation can call this operation whenever it is needed. The result must remain the same (this is a logically pure function), or the behavior is unspecified.

If the value of a key stored in a node of a map is changed other than by an operation in this package such that at least one of `Hash` or `Equivalent_Keys` give different results, the behavior of this package is unspecified.

**Implementation Note:** The implementation is not required to protect against changes to key values other than via the operations declared in the `Hashed_Maps` package.

To see how this could happen, imagine an instance of `Hashed_Maps` where the key type is an access-to-variable type and `Hash` returns a value derived from the components of the designated object. Then, any operation that has a key value could modify those components and change the hash value:

```
Key(Map).Some_Component := New_Value;
```

This is really a design error on the part of the user of the map; it shouldn't be possible to modify keys stored in a map. But we can't prevent this error anymore than we can prevent someone passing as `Hash` a random number generator.

Which nodes are the first node and the last node of a map, and which node is the successor of a given node, are unspecified, other than the general semantics described in A.18.4.

**Implementation Note:** Typically the first node will be the first node in the first bucket, the last node will be the last node in the last bucket, and the successor will be obtained by following the collision list, and going to the next bucket at the end of each bucket.
function Empty (Capacity : Count_Type := implementation-defined)
  return Map
  with Post =>
  Capacity (Empty'Result) >= Capacity and then
  not Tampering With Elements Prohibited (Empty'Result) and then
  not Tampering With Cursors Prohibited (Empty'Result) and then
  Length (Empty'Result) = 0;

{AI12-0339-1} Returns an empty map.

{AI12-0112-1} function Capacity (Container : Map) return Count_Type
  with Nonblocking, Global => null, Use_Formal => null;

{AI95-00302-03} Returns the capacity of Container.

{AI12-0112-1} procedure Reserve_Capacity (Container : in out Map;
  Capacity : in Count_Type)
  with Pre  => not Tampering With Cursors Prohibited (Container)
       or else raise Program_Error,
       Post => Container.Capacity >= Capacity;

{AI95-00302-03} Reserve_Capacity allocates a new hash table such that the length of the
resulting map can become at least the value Capacity without requiring an additional call to
Reserve_Capacity, and is large enough to hold the current length of Container. Reserve_Capacity
then rehashes the nodes in Container onto the new hash table. It replaces the old hash table with
the new hash table, and then deallocates the old hash table. Any exception raised during
allocation is propagated and Container is not modified.

This paragraph was deleted.{AI12-0112-1} Reserve_Capacity tampers with the cursors of
Container.

Implementation Note: This routine is used to preallocate the internal hash table to the specified capacity such that
future inserts do not require expansion of the hash table. Therefore, the implementation should allocate the needed
memory to make that true at this point, even though the visible semantics could be preserved by waiting until enough
elements are inserted.

{AI95-0005-1} While Reserve_Capacity can be used to reduce the capacity of a map, we do not specify whether an
implementation actually supports reduction of the capacity. Since the actual capacity can be anything greater than or
equal to Capacity, an implementation never has to reduce the capacity.

Reserve_Capacity tampers with the cursors, as rehashing probably will change the order that elements are stored in the
map.

{AI12-0112-1} procedure Clear (Container : in out Map)
  with Pre  => not Tampering With Cursors Prohibited (Container)
       or else raise Program_Error,
       Post => Capacity (Container) = Capacity (Container)'Old and then
       Length (Container) = 0;

{AI95-00302-03} In addition to the semantics described in A.18.4, Clear does not affect the
capacity of Container.

{AI12-0112-1} procedure Assign (Target : in out Map; Source : in Map)
  with Pre => not Tampering With Cursors Prohibited (Target)
       or else raise Program_Error,
       Post => Length (Source) = Length (Target) and then
       Capacity (Target) >= Length (Source);

{AI05-0001-1} {AI05-0248-1} In addition to the semantics described in A.18.4, if the length of
Source is greater than the capacity of Target, Reserve_Capacity (Target, Length (Source)) is
called before assigning any elements.
function Copy (Source : Map; Capacity : Count_Type := 0) return Map
with Pre => Capacity = 0 or else Capacity >= Length (Source)
or else raise Capacity_Error,
Post =>
Length (Copy'Result) = Length (Source) and then
not Tampering_With_Elements_Prohibited (Copy'Result) and then
not Tampering_With_Cursors_Prohibited (Copy'Result) and then
Copy'Result.Capacity = (if Capacity = 0 then
Length (Source) else Capacity);}

{AI05-0001-1} {AI12-0112-1} Returns a map whose keys and elements are initialized from the keys and elements of Source. If Capacity is 0, then the map capacity is the length of Source; if Capacity is equal to or greater than the length of Source, the map capacity is at least the specified value. Otherwise, the operation propagates Capacity_Error.

Implementation Note: In:
procedure Move (Target : in out Map;
Source : in out Map);
The intended implementation is that the internal hash table of Target is first deallocated; then the internal hash table is removed from Source and moved to Target.

{AI12-0112-1} procedure Insert (Container : in out Map;
Key : in Key_Type;
New_Item : in Element_Type;
Position : out Cursor;
Inserted : out Boolean)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Original_Length : constant Count_Type :=
Length (Container)'Old;
beg
Has_Element (Container, Position) and then
(if Inserted then
Length (Container) = Original_Length + 1
else
Length (Container) = Original_Length)) and then
Capacity (Container) >= Length (Container);

{AI95-00302-03} In addition to the semantics described in A.18.4, if Length (Container) equals Capacity (Container), then Insert first calls Reserve_Capacity to increase the capacity of Container to some larger value.

Implementation Note: Insert should only compare keys that hash to the same bucket in the hash table.

We specify when Reserve_Capacity is called to bound the overhead of capacity expansion operations (which are potentially expensive). Moreover, expansion can be predicted by comparing Capacity(Map) to Length(Map). Since we don't specify by how much the hash table is expanded, this only can be used to predict the next expansion, not later ones.

Implementation Note: In:
procedure Exclude (Container : in out Map;
Key : in Key_Type);
Exclude should only compare keys that hash to the same bucket in the hash table.

Implementation Note: In:
procedure Delete (Container : in out Map;
Key : in Key_Type);
Delete should only compare keys that hash to the same bucket in the hash table. The node containing the element may be deallocated now, or it may be saved and reused later.
Implementation Note: In:

function First (Container : Map) return Cursor;

In a typical implementation, this will be the first node in the lowest numbered hash bucket that contains a node.

Implementation Note: In:

function Next (Position : Cursor) return Cursor;

In a typical implementation, this will return the next node in a bucket; if Position is the last node in a bucket, this will return the first node in the next nonempty bucket.

A typical implementation will need to keep a pointer at the map container in the cursor in order to implement this function.

Implementation Note: In:

function Find (Container : Map; Key : Key_Type) return Cursor;

Find should only compare keys that hash to the same bucket in the hash table.

{AI12-0112-1} function Equivalent_Keys (Left, Right : Cursor) return Boolean

with Pre => (Left /= No_Element and then Right /= No_Element) or else raise Constraint_Error,

Global => in all;

{AI95-00302-03} Equivalent to Equivalent_Keys (Key (Left), Key (Right)).

{AI12-0112-1} function Equivalent_Keys (Left : Cursor; Right : Key_Type) return Boolean

with Pre => Left /= No_Element or else raise Constraint_Error,

Global => in all;

{AI95-00302-03} Equivalent to Equivalent_Keys (Key (Left), Right).

{AI12-0112-1} function Equivalent_Keys (Left : Key_Type; Right : Cursor) return Boolean

with Pre => Right /= No_Element or else raise Constraint_Error,

Global => in all;

{AI95-00302-03} Equivalent to Equivalent_Keys (Left, Key (Right)).

{AI12-0112-1} {AI05-0265-1} {AI05-0269-1} {AI12-0266-1} function Iterate (Container : in Map) return Map_Iterator_Interfaces.Parallel_IteratorForward_Iterator'Class

with Post => Tampering_With_Cursors_Prohibited (Container);

{AI05-0212-1} {AI05-0265-1} {AI05-0269-1} {AI12-0266-1} Iterate returns an iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each node in Container, starting with the first node and moving the cursor according to the successor relation when used as a forward iterator, and processing all nodes concurrently when used as a parallel iterator. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence_of_statements of the loop_statement whose iterator_specification denotes this object). The iterator object needs finalization.

Implementation Advice

{AI95-00302-03} If \( N \) is the length of a map, the average time complexity of the subprograms Element, Insert, Include, Replace, Delete, Exclude, and Find that take a key parameter should be \( O(\log N) \). The average time complexity of the subprograms that take a cursor parameter should be \( O(1) \). The average time complexity of Reserve_Capacity should be \( O(N) \).

Implementation Advice: The average time complexity of Element, Insert, Include, Replace, Delete, Exclude, and Find operations that take a key parameter for Containers.Hashed_Maps should be \( O(\log N) \). The average time complexity of the subprograms of Containers.Hashed_Maps that take a cursor parameter should be \( O(1) \). The average time complexity of Reserve_Capacity should be \( O(N) \).

Reason: We do not mean to overly constrain implementation strategies here. However, it is important for portability that the performance of large containers has roughly the same factors on different implementations. If a program is
moved to an implementation for which Find is \(O(N)\), that program could be unusable when the maps are large. We allow \(O(\log N)\) access because the proportionality constant and caching effects are likely to be larger than the log factor, and we don't want to discourage innovative implementations.

**Extensions to Ada 95**

\{AII2-0112-1\} Added iterator and indexing support to make hashed map containers more convenient to use.

**Wording Changes from Ada 2005**

\{AI05-0212-1\} Correction: Added a pragma Remote_Types so that containers can be used in distributed programs.

**Incompatibilities With Ada 2005**

\{AI05-0001-1\} Subprograms Assign and Copy are added to Containers.Hashed_Maps. If an instance of Containers.Hashed_Maps is referenced in a use clause, and an entity \(E\) with the same defining identifier as a new entity in Containers.Hashed_Maps is defined in a package that is also referenced in a use clause, the entity \(E\) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

**Incompatibilities With Ada 2012**

\{AI12-0112-1\} \{AI12-0111-1\} \{AI12-0339-1\} A number of new subprograms, types, and even a nested package were added to Containers.Hashed_Maps to better support contracts and stable views. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

**Extensions to Ada 2012**

\{AI12-0212-1\} Maps now support named container aggregates, so aggregate syntax can be used to create Maps.

\{AI12-0266-1\} The iterator for the container now can return a parallel iterator which can be used to process the container in parallel.

**Wording Changes from Ada 2012**

\{AI12-0112-1\} Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).

### A.18.6 The Generic Package Containers.Ordered_Maps

**Static Semantics**

\{AI95-00302-03\} The generic library package Containers.Ordered_Maps has the following declaration:

```ada
generic
  type Key_Type is private;
  type Element_Type is private;
with function "<" (Left, Right : Key_Type) return Boolean is <=;
with function ":=" (Left, Right : Element_Type) return Boolean is <=;
package Ada.Containers.Ordered_Maps is
  with Preelaborate, Remote_Types,
  Nonblocking, Global => in out synchronized is
  pragma Preelaborate(Ordered_Maps);
  pragma Remote_Types(Ordered_Maps);
```

**Discussion:** \{AI12-0112-1\} For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).

```ada
function Equivalent_Keys (Left, Right : Key_Type) return Boolean is (not ((Left < Right) or (Right < Left)));
```
type Map is tagged private
  with Constant_Indexing => Constant_Reference,
  Variable_Indexing => Reference,
  Default_Iterator => Iterate,
  Iterator_Element => Element_Type,
  Iterator_View => Stable.Map,
  Aggregate => (Empty => Empty,
                 Add_Named => Insert),
  Stable_Properties => (Length,
                        Tampering_With_Cursors_Prohibited,
                        Tampering_With_Elements_Prohibited),
  Default_Initial_Condition =>
    Length (Map) = 0
    and then
    (not Tampering_With_Cursors_Prohibited (Map))
    and then
    (not Tampering_With_Elements_Prohibited (Map)),
pragma Preelaborable_Initialization(Map);

{AI05-0212-1} {AI12-0011-1} type Cursor is private
  withpragma Preelaborable_Initialization(Cursor);
{AI05-0212-1} Empty_Map : constant Map;
{AI05-0212-1} No_Element : constant Cursor;

{AI05-0212-1} {AI12-0011-1} function Has_Element (Position : Cursor) return Boolean
  with Nonblocking, Global => in all, Use Formal => null;
{AI12-0011-1} function Has_Element (Container : Map; Position : Cursor)
  return Boolean
  with Nonblocking, Global => null, Use Formal => null;
{AI05-0212-1} package Map_Iterator_Interfaces is new
  Ada.Iterator_Interfaces (Cursor, Has_Element);
function "=" (Left, Right : Map) return Boolean;
{AI12-0011-1} function Tampering_With_Cursors_Prohibited
  (Container : Map) return Boolean
  with Nonblocking, Global => null, Use Formal => null;
{AI12-0011-1} function Tampering_With_Elements_Prohibited
  (Container : Map) return Boolean
  with Nonblocking, Global => null, Use Formal => null;
{AI12-0339-1} function Empty return Map
  is (Empty_Map)
  with Post =>
    not Tampering_With_Elements_Prohibited (Empty'Result)
    and then
    not Tampering_With_Cursors_Prohibited (Empty'Result)
    and then
    Length (Empty'Result) = 0;
{AI12-0011-1} function Length (Container : Map) return Count_Type
  with Nonblocking, Global => null, Use Formal => null;
{AI12-0011-1} function Is_Empty (Container : Map) return Boolean
  with Nonblocking, Global => null, Use Formal => null,
  Post => Is_Empty'Result = (Length (Container) = 0);
{AI12-0011-1} procedure Clear (Container : in out Map)
  with Pre => not Tampering_With_Cursors_Prohibited (Container)
  or else raise Program_Error,
  Post => Length (Container) = 0;
{AI12-0011-1} function Key (Position : Cursor) return Key_Type
  with Pre => Position /= No_Element or else raise Constraint_Error,
  Nonblocking, Global => in all, Use Formal => Key_Type;
function Key (Container : Map; Position : Cursor) return Key_Type
with Pre => (Position /= No_Element or else raise Constraint_Error) and then
          (Has Element (Container, Position) or else raise Program_Error),
          Nonblocking, Global => null, Use Formal => Key_Type;

function Element (Position : Cursor) return Element_Type
with Pre => Position /= No_Element or else raise Constraint_Error,
          Nonblocking, Global => null, Use Formal => Element_Type;

function Element (Container : Map; Position : Cursor) return Element_Type
with Pre => (Position /= No_Element or else raise Constraint_Error) and then
          (Has Element (Container, Position) or else raise Program_Error),
          Nonblocking, Global => null, Use Formal => Element_Type;

procedure Replace_Element (Container : in out Map; Position : in Cursor;
                           New_item : in Element_Type)
with Pre => (not Tampering_With_Elements_Prohibited (Container) or else raise Program_Error) and then
          (Position /= No_Element or else raise Constraint_Error) and then
          (Has Element (Container, Position) or else raise Program_Error);

procedure Query_Element (Position : in Cursor;
                         Process : not null access procedure (Key : in Key_Type;
                                                         Element : in Element_Type))
with Pre => Position /= No_Element or else raise Constraint_Error,
          Global => in all;

procedure Query_Element (Container : in Map;
                         Position : in Cursor;
                         Process : not null access procedure (Key : in Key_Type;
                                                        Element : in Element_Type))
with Pre => (Position /= No_Element or else raise Constraint_Error) and then
          (Has Element (Container, Position) or else raise Program_Error);

procedure Update_Element (Container : in out Map;
                         Position : in Cursor;
                         Process : not null access procedure (Key : in Key_Type;
                                                           Element : in out Element_Type))
with Pre => (Position /= No_Element or else raise Constraint_Error) and then
          (Has Element (Container, Position) or else raise Program_Error);

type Constant_Reference_Type (Element : not null access constant Element_Type) is private
with Implicit Dereference => Element,
    Nonblocking, Global => in out synchronized,
    Default Initial Condition => (raise Program_Error);

type Reference_Type (Element : not null access Element_Type) is private
with Implicit Dereference => Element,
    Nonblocking, Global => in out synchronized,
    Default Initial Condition => (raise Program_Error);
function Constant_Reference (Container : aliased in Map; Position : in Cursor) return Constant_Reference_Type
with Pre => (Position /= No_Element or else raise Constraint_Error) and then (Has_Element (Container, Position) or else raise Program_Error), Post => Tampering_With_Cursors_Prohibited (Container), Nonblocking, Global => null, Use_Formal => null;

function Reference (Container : aliased in out Map; Position : in Cursor) return Reference_Type
with Pre => (Position /= No_Element or else raise Constraint_Error) and then (Has_Element (Container, Position) or else raise Program_Error), Post => Tampering_With_Cursors_Prohibited (Container), Nonblocking, Global => null, Use_Formal => null;

function Constant_Reference (Container : aliased in Map; Key : in Key_Type) return Constant_Reference_Type
with Pre => Find (Container, Key) /= No_Element or else raise Constraint_Error, Post => Tampering_With_Cursors_Prohibited (Container), Nonblocking, Global => null, Use_Formal => null;

function Reference (Container : aliased in out Map; Key : in Key_Type) return Reference_Type
with Pre => Find (Container, Key) /= No_Element or else raise Constraint_Error, Post => Tampering_With_Cursors_Prohibited (Container), Nonblocking, Global => null, Use_Formal => null;

procedure Assign (Target : in out Map; Source : in Map)
with Pre => not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error, Post => Length (Source) = Length (Target);

function Copy (Source : Map) return Map
with Post => Length (Copy'Result) = Length (Source) and then not Tampering_With_Elements_Prohibited (Copy'Result) and then not Tampering_With_Cursors_Prohibited (Copy'Result);

procedure Move (Target : in out Map; Source : in out Map)
with Pre => (not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error) and then (not Tampering_With_Cursors_Prohibited (Source) or else raise Program_Error), Post => (if not Target'Has_Same_Storage (Source) then Length (Target) = Length (Source'Old) and then Length (Source) = 0).
procedure Insert (Container : in out Map;
Key       : in  Key_Type;
New_Item  : in  Element_Type;
Position  : out Cursor;
Inserted  : out Boolean)

with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Original Length : constant Count_Type :=
Length (Container)'Old;
begin
Has Element (Container, Position) and then
(if Inserted then
Length (Container) = Original Length + 1
else
Length (Container) = Original Length));

procedure Insert (Container : in out Map;
Key       : in  Key_Type;
Position  : out Cursor;
Inserted  : out Boolean)

with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Original Length : constant Count_Type :=
Length (Container)'Old;
begin
Has Element (Container, Position) and then
(if Inserted then
Length (Container) = Original Length + 1
else
Length (Container) = Original Length));

procedure Insert (Container : in out Map;
Key       : in  Key_Type;
New_Item  : in  Element_Type)

with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Original Length : constant Count_Type :=
Length (Container)'Old;
begin
Length (Container)
in Original Length | Original Length + 1);

procedure Replace (Container : in out Map;
Key        : in  Key_Type;
New_Item   : in  Element_Type)

with Pre => not Tampering With Cursors Prohibited (Container)
or else raise Program_Error,
Post => Length (Container) = Length (Container)'Old;}
procedure Exclude (Container : in out Map;
   Key       : in   Key_Type)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
   or else raise Program_Error,
Post => (declare
   Original_Length : constant Count_Type :=
       Length (Container)'Old;
   begin
       Length (Container)
       in Original_Length - 1 | Original_Length);
procedure Delete (Container : in out Map;
   Key       : in   Key_Type)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
   or else raise Program_Error,
Post => Length (Container) = Length (Container)'Old - 1;
procedure Delete (Container : in out Map;
   Position  : in out Cursor)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
   or else raise Program_Error) and then
   (Position /= No_Element
   or else raise Constraint_Error) and then
   (Has_Element (Container, Position)
   or else raise Program_Error),
Post => Length (Container) = Length (Container)'Old - 1 and then
   Position = No_Element;
procedure Delete First (Container : in out Map)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
   or else raise Program_Error,
Post => (declare
   Original_Length : constant Count_Type :=
       Length (Container)'Old;
   begin
       (if Original_Length = 0 then Length (Container) = 0
       else Length (Container) = Original_Length - 1));
procedure Delete Last (Container : in out Map)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
   or else raise Program_Error,
Post => (declare
   Original_Length : constant Count_Type :=
       Length (Container)'Old;
   begin
       (if Original_Length = 0 then Length (Container) = 0
       else Length (Container) = Original_Length - 1));
function First (Container : Map) return Cursor 
with Nonblocking, Global => null, Use Formal => null,
   Post => (if not Is_Empty (Container)
       then Has_Element (Container, First'Result)
       else First'Result = No_Element);
function First Element (Container : Map) return Element_Type
with Pre => (not Is_Empty (Container)
   or else raise Constraint_Error);
function First Key (Container : Map) return Key_Type
with Pre => (not Is_Empty (Container)
   or else raise Constraint_Error);
function Last (Container : Map) return Cursor 
with Nonblocking, Global => null, Use Formal => null,
   Post => (if not Is_Empty (Container)
       then Has_Element (Container, Last'Result)
       else Last'Result = No_Element);
function Last Element (Container : Map) return Element_Type
with Pre => (not Is_Empty (Container)
   or else raise Constraint_Error);
function Last_Key (Container : Map) return Key_Type with Pre => (not Is_Empty (Container) or else raise Constraint_Error);

function Next (Position : Cursor) return Cursor with Nonblocking, Global => in all, Use Formal => null, Post => (if Position = No_Element then Next'Result = No_Element);

function Next (Container : Map; Position : Cursor) return Cursor with Nonblocking, Global => null, Use Formal => null, Pre => Position = No_Element or else Has_Element (Container, Position) or else raise Program_Error, Post => (if Position = No_Element then Next'Result = No_Element else Has_Element (Container, Next'Result));

procedure Next (Position : in out Cursor) with Nonblocking, Global => in all, Use Formal => null;

procedure Next (Container : in Map; Position : in out Cursor) with Nonblocking, Global => null, Use Formal => null, Pre => Position = No_Element or else Has_Element (Container, Position) or else raise Program_Error, Post => (if Position /= No_Element then Has_Element (Container, Position));

function Previous (Position : Cursor) return Cursor with Nonblocking, Global => in all, Use Formal => null, Post => (if Position = No_Element then Previous'Result = No_Element);

function Previous (Container : Map; Position : Cursor) return Cursor with Nonblocking, Global => null, Use Formal => null, Pre => Position = No_Element or else Has_Element (Container, Position) or else raise Program_Error, Post => (if Position /= No_Element then Previous'Result = No_Element else Has_Element (Container, Previous'Result));

procedure Previous (Position : in out Cursor) with Nonblocking, Global => in all, Use Formal => null;

procedure Previous (Container : in Map; Position : in out Cursor) with Nonblocking, Global => null, Use Formal => null, Pre => Position = No_Element or else Has_Element (Container, Position) or else raise Program_Error, Post => (if Position /= No_Element then Has_Element (Container, Position));

function Find (Container : Map; Key : Key_Type) return Cursor with Post => (if Find'Result /= No_Element then Has_Element (Container, Find'Result));

function Element (Container : Map; Key : Key_Type) return Element_Type;

function Floor (Container : Map; Key : Key_Type) return Cursor with Post => (if Floor'Result /= No_Element then Has_Element (Container, Floor'Result));
function Ceiling (Container : Map; 
Key       : Key_Type) return Cursor 
with Post => (if Ceiling'Result /= No_Element 
then Has_Element (Container, Ceiling'Result)); 

function Contains (Container : Map; 
Key       : Key_Type) return Boolean;

This paragraph was deleted.

function Has_Element (Position : Cursor) return Boolean;

function "<" (Left, Right : Cursor) return Boolean 
with Pre => (Left /= No_Element and then Right /= No_Element) 
or else raise Constraint_Error, 
Global => in all;

function ">" (Left, Right : Cursor) return Boolean 
with Pre => (Left /= No_Element and then Right /= No_Element) 
or else raise Constraint_Error, 
Global => in all;

function "<" (Left : Cursor; Right : Key_Type) return Boolean 
with Pre => Left /= No_Element or else raise Constraint_Error, 
Global => in all;

function ">" (Left : Cursor; Right : Key_Type) return Boolean 
with Pre => Left /= No_Element or else raise Constraint_Error, 
Global => in all;

function "<" (Left : Key_Type; Right : Cursor) return Boolean 
with Pre => Right /= No_Element or else raise Constraint_Error, 
Global => in all;

function ">" (Left : Key_Type; Right : Cursor) return Boolean 
with Pre => Right /= No_Element or else raise Constraint_Error, 
Global => in all;

procedure Iterate 
(Container : in Map; 
Process   : not null access procedure (Position : in Cursor)) 
with Allows_Exit;

procedure Reverse_Iterate 
(Container : in Map; 
Process   : not null access procedure (Position : in Cursor)) 
with Allows_Exit;

function Iterate (Container : in Map; Start : in Cursor) 
return Map_Iterator_Interfaces.Reversible_Iterator'Class 
with Post => Tampering_With_Cursors_Prohibited (Container);

package Stable is 

type Map (Base : not null access Ordered_Maps.Map) is 
tagged limited private 
with Constant_Indexing => Constant_Reference, 
Variable_Indexing => Reference, 
Default_Initializer => Iterate, 
Iterator_Element => Element_Type, 
Stable_Properties => (Length), 
Global => null, 
Default_Initial_Condition => Length (Map) = 0, 
Preelaborable_Initialization;
type Cursor is private 
with Preelaborable Initialization;

Empty_Map : constant Map;
No_Element : constant Cursor;

function Has_Element (Position : Cursor) return Boolean 
with Nonblocking, Global => in all, Use Formal => null;

package Map_Interfaces is new 
Ada.Iterator_Interfaces (Cursor, Has_Element);

procedure Assign (Target : in out Ordered_Maps.Map; 
Source : in Map) 
with Post => Length (Source) = Length (Target);

function Copy (Source : Ordered_Maps.Map) return Map 
with Post => Length (Copy'Result) = Length (Source);

type Constant_Reference_Type 
(Element : not null access constant Element_Type) is private 
with Implicit Dereference => Element, 
Nonblocking, Global => null, Use Formal => null, 
Default Initial Condition => (raise Program Error);

type Reference_Type 
(Element : not null access Element_Type) is private 
with Implicit Dereference => Element, 
Nonblocking, Global => null, Use Formal => null, 
Default Initial Condition => (raise Program Error);

-- Additional subprograms as described in the text
-- are declared here.

-- Additional subprograms as described in the text
-- are declared here.

private 
... -- not specified by the language

end Stable;

Two keys K1 and K2 are equivalent if both K1 < K2 and K2 < K1 return False, using 
the generic formal "<" operator for keys. Function Equivalent Keys returns True if Left and Right are 
equivalent, and False otherwise.

The actual function for the generic formal function "<" on Key_Type 
values is expected to return the same value each time it is called with a particular pair of key values. It 
should define a strict weak ordering relationship (see A.18), that is, be irreflexive, asymmetric, and 
transitive. If the actual for "<" behaves in some other manner, the behavior of this package is unspecified. 
Which subprograms of this package call "<" and how many times they call it, is unspecified.

Implementation Note: The implementation is not required to protect against "<" raising an exception, or returning 
random results, or any other "bad" behavior. It's not practical to do so, and a broken "<" function makes the container 
unusable.

The implementation can call "<" whenever it is needed; we don't want to specify how often that happens. The result 
must remain the same (this is a logically pure function), or the behavior is unspecified.

If the value of a key stored in a map is changed other than by an operation in this 
package such that at least one of "<" or "=" give different results, the behavior of this package is 
unspecified.

Implementation Note: The implementation is not required to protect against changes to key values other than via the 
operations declared in the Ordered Maps package.

To see how this could happen, imagine an instance of Ordered_Maps package where the key type is an access-to- 
variable type and "<" returns a value derived from comparing the components of the designated objects. Then, any
operation that has a key value (even if the key value is constant) could modify those components and change the result of "<":

\[
\text{Key (Map).Some Component} := \text{New Value;}
\]

This is really a design error on the part of the user of the map; it shouldn't be possible to modify keys stored in a map such that "<" changes. But we can't prevent this error anymore than we can prevent someone passing as "<" a routine that produces random answers.

\{AI95-00302-03\} \{AI05-0262-1\} The first node of a nonempty map is the one whose key is less than the key of all the other nodes in the map. The last node of a nonempty map is the one whose key is greater than the key of all the other elements in the map. The successor of a node is the node with the smallest key that is larger than the key of the given node. The predecessor of a node is the node with the largest key that is smaller than the key of the given node. All comparisons are done using the generic formal "<" operator for keys.

\{AI12-0112-1\} \textbf{function} \texttt{Copy} (Source : Map) \textbf{return} Map \textbf{with} Post => 
\begin{align*}
&\text{Length (Copy'Result) = Length (Source) and then} \\
&\text{not Tampering With Elements Prohibited (Copy'Result) and then} \\
&\text{not Tampering With Cursors Prohibited (Copy'Result);} \\
\end{align*} 
\{AI05-0001-1\} Returns a map whose keys and elements are initialized from the corresponding keys and elements of Source.

\{AI12-0112-1\} \textbf{procedure} \texttt{Delete First} (Container : in out Map) \textbf{with} Pre => not Tampering With Cursors Prohibited (Container) \textbf{or else raise} Program_Error, 
\textbf{Post => (declare} 
\begin{align*}
&\text{Original Length : constant Count_Type :=} \\
&\text{Length (Container)'Old;} \\
&\text{begin} \\
&\quad(\text{if Original Length} = 0 \text{ then} \text{Length (Container)} = 0 \\
&\quad\text{else} \text{Length (Container)} = \text{Original Length} - 1); \\
\end{align*} 
\{AI95-00302-03\} \{AI05-0264-1\} If Container is empty, Delete First has no effect. Otherwise, the node designated by First (Container) is removed from Container. Delete First tampers with the cursors of Container.

\{AI12-0112-1\} \textbf{procedure} \texttt{Delete Last} (Container : in out Map) \textbf{with} Pre => not Tampering With Cursors Prohibited (Container) \textbf{or else raise} Program_Error, 
\textbf{Post => (declare} 
\begin{align*}
&\text{Original Length : constant Count_Type :=} \\
&\text{Length (Container)'Old;} \\
&\text{begin} \\
&\quad(\text{if Original Length} = 0 \text{ then} \text{Length (Container)} = 0 \\
&\quad\text{else} \text{Length (Container)} = \text{Original Length} - 1); \\
\end{align*} 
\{AI95-00302-03\} \{AI05-0264-1\} If Container is empty, Delete Last has no effect. Otherwise, the node designated by Last (Container) is removed from Container. Delete Last tampers with the cursors of Container.

\{AI12-0112-1\} \textbf{function} \texttt{First Element} (Container : Map) \textbf{return} Element_Type \textbf{with} Pre => (not Is Empty (Container) \\
\textbf{or else raise} Constraint_Error); 
\{AI95-00302-03\} Equivalent to Element (First (Container)).

\{AI12-0112-1\} \textbf{function} \texttt{First Key} (Container : Map) \textbf{return} Key_Type \textbf{with} Pre => (not Is Empty (Container) \\
\textbf{or else raise} Constraint_Error); 
\{AI95-00302-03\} Equivalent to Key (First (Container)).
function Last (Container : Map) return Cursor
with Nonblocking, Global => null, Use Formal => null,
Post => (if not Is_Empty (Container)
then Has_Element (Container, Last'Result)
else Last'Result = No_Element);

{AI95-00302-03} Returns a cursor that designates the last node in Container. If Container is empty, returns No_Element.

function Last_Element (Container : Map) return Element_Type
with Pre => (not Is_Empty (Container)
or else raise Constraint_Error);

{AI95-00302-03} Equivalent to Element (Last (Container)).

function Last_Key (Container : Map) return Key_Type
with Pre => (not Is_Empty (Container)
or else raise Constraint_Error);

{AI95-00302-03} Equivalent to Key (Last (Container)).

function Previous (Position : Cursor) return Cursor
with Nonblocking, Global => in all, Use Formal => null,
Post => (if Position = No_Element then
Previous'Result = No_Element);

{AI95-00302-03} {AI05-0262-1} If Position equals No_Element, then Previous returns No_Element. Otherwise, Previous returns a cursor designating the predecessor node of that precedes the one designated by Position. If Position designates the first element, then Previous returns No_Element.

function Previous (Container : Map; Position : Cursor) return Cursor
with Nonblocking, Global => null, Use Formal => null,
Pre => Position = No_Element or else Has_Element (Container, Position)
or else raise Program_Error,
Post => (if Position = No_Element then
Previous'Result = No_Element
elsif Previous'Result = No_Element then
Position = First (Container)
else Has_Element (Container, Previous'Result));

{AI12-0112-1} Returns a cursor designating the predecessor of the node designated by Position in Container, if any.

procedure Previous (Position : in out Cursor)
with Nonblocking, Global => in all, Use Formal => null;

{AI95-00302-03} Equivalent to Position := Previous (Position).

procedure Previous (Container : in Map; Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
Pre => Position = No_Element or else Has_Element (Container, Position)
or else raise Program_Error,
Post => (if Position /= No_Element
then Has_Element (Container, Position));

{AI12-0112-1} Equivalent to Position := Previous (Container, Position).
function Floor (Container : Map;
          Key       : Key_Type) return Cursor
with Post => (if Floor'Result /= No_Element
             then Has_Element (Container, Floor'Result));

Floor searches for the last node whose key is not greater than
Key, using the generic formal "<" operator for keys. If such a node is found, a cursor that
designates it is returned. Otherwise, No_Element is returned.

function Ceiling (Container : Map;
                 Key       : Key_Type) return Cursor
with Post => (if Ceiling'Result /= No_Element
               then Has_Element (Container, Ceiling'Result));

Ceiling searches for the first node whose key is not less than
Key, using the generic formal "<" operator for keys. If such a node is found, a cursor that
designates it is returned. Otherwise, No_Element is returned.

function "<" (Left, Right : Cursor) return Boolean
with Pre => (Left /= No_Element and then Right /= No_Element)
         or else raise Constraint_Error,
         Global => in all;

Equivalent to Key (Left) < Key (Right).

function ">" (Left, Right : Cursor) return Boolean
with Pre => (Left /= No_Element and then Right /= No_Element)
         or else raise Constraint_Error,
         Global => in all;

Equivalent to Key (Right) < Key (Left).

function "<" (Left : Cursor; Right : Key_Type) return Boolean
with Pre => Left /= No_Element or else raise Constraint_Error,
         Global => in all;

Equivalent to Key (Left) < Right.

function ">" (Left : Cursor; Right : Key_Type) return Boolean
with Pre => Left /= No_Element or else raise Constraint_Error,
         Global => in all;

Equivalent to Right < Key (Left).

function "<" (Left : Key_Type; Right : Cursor) return Boolean
with Pre => Right /= No_Element or else raise Constraint_Error,
         Global => in all;

Equivalent to Left < Key (Right).

function ">" (Left : Key_Type; Right : Cursor) return Boolean
with Pre => Right /= No_Element or else raise Constraint_Error,
         Global => in all;

Equivalent to Key (Right) < Left.

procedure Reverse_Iterate
(Container : in Map;
    Process   : not null access procedure (Position : in Cursor))
with Allows Exit;

Iterates over the nodes in Container as per procedure Iterate,
with the difference that the nodes are traversed in predecessor order, starting with the last node.
function Iterate (Container : in Map) return Map_Iterator_Interfaces.Parallel_Reversible_Iterator'Class
    with Post => Tampering_With.Cursors_Prohibited (Container),
{105-0212-1} {105-0265-1} {105-0269-1} {112-0266-1}
{105-0262-1} {105-0265-1} {105-0269-1} {112-0266-1}

Iterate returns an reversible iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each node in Container, starting with the first node and moving the cursor according to the successor relation when used as a forward iterator, and starting with the last node and moving the cursor according to the predecessor relation when used as a reverse iterator, and processing all nodes concurrently when used as a parallel iterator. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop statement whose iterator specification denotes this object). The iterator object needs finalization.

function Iterate (Container : in Map; Start : in Cursor) return Map_Iterator_Interfaces.Reversible_Iterator'Class
    with Pre => (Start /= No_Element
               or else raise Constraint_Error) and then
               (Has_Element (Container, Start)
               or else raise Program_Error),
    Post => Tampering_With.Cursors_Prohibited (Container),

If Start is not No_Element and does not designate an item in Container, then Program_Error is propagated. If Start is No_Element, then Constraint_Error is propagated. Otherwise, Iterate returns a reversible iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each node in Container, starting with the node designated by Start and moving the cursor according to the successor relation when used as a forward iterator, or moving the cursor according to the predecessor relation when used as a reverse iterator. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop statement whose iterator specification denotes this object). The iterator object needs finalization.

Discussion: Exits are allowed from the loops created using the iterator objects. In particular, to stop the iteration at a particular cursor, just add

```
exit when Cur = Stop;
```

in the body of the loop (assuming that Cur is the loop parameter and Stop is the cursor that you want to stop at).

Implementation Advice

If \( N \) is the length of a map, then the worst-case time complexity of the Element, Insert, Include, Replace, Delete, Exclude, and Find operations that take a key parameter should be \( O((\log N)^2) \) or better. The worst-case time complexity of the subprograms that take a cursor parameter should be \( O(1) \).

Implementation Advice: The worst-case time complexity of Element, Insert, Include, Replace, Delete, Exclude, and Find operations that take a key parameter for Containers.Ordered_Maps should be \( O((\log N)^2) \) or better. The worst-case time complexity of the subprograms of Containers.Ordered_Maps that take a cursor parameter should be \( O(1) \).

Implementation Note: A balanced (red-black) tree for keys has \( O(\log N) \) worst-case performance. Note that a \( O(N) \) worst-case implementation (like a list) would be wrong.

Reason: We do not mean to overly constrain implementation strategies here. However, it is important for portability that the performance of large containers has roughly the same factors on different implementations. If a program is moved to an implementation that takes \( O(N) \) to find elements, that program could be unusable when the maps are large. We allow the extra \( \log N \) factors because the proportionality constant and caching effects are likely to be larger than the \( \log \) factor, and we don't want to discourage innovative implementations.

Extensions to Ada 95

The generic package Containers.Ordered_Maps is new.
Incompatibilities With Ada 2005

{AI05-0001-1} Subprograms Assign and Copy are added to Containers.Ordered Maps. If an instance of Containers.Ordered Maps is referenced in a use_clause, and an entity E with the same defining_identifier as a new entity in Containers.Ordered Maps is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 2005

{AI05-0212-1} Added iterator and indexing support to make ordered map containers more convenient to use.

Wording Changes from Ada 2005

{AI05-0044-1} Correction: Redefined "<" actuals to require a strict weak ordering; the old definition allowed indeterminant comparisons that would not have worked in a container.

{AI05-0084-1} Correction: Added a pragma Remote_Types so that containers can be used in distributed programs.

Incompatibilities With Ada 2012

{AI12-0111-1} {AI12-0112-1} {AI12-0339-1} A number of new subprograms, types, and even a nested package were added to Containers.Ordered Maps to better support contracts and stable views. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

Extensions to Ada 2012

{AI12-0212-1} Maps now support named container aggregates, so aggregate syntax can be used to create Maps.

{AI12-0266-1} The iterator for the entire container now can return a parallel iterator which can be used to process the container in parallel.

Wording Changes from Ada 2012

{AI12-0112-1} Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).

A.18.7 Sets

{AI95-00302-03} The language-defined generic packages Containers.Hashed_Sets and Containers.Ordered_Sets provide private types Set and Cursor, and a set of operations for each type. A set container allows elements of an arbitrary type to be stored without duplication. A hashed set uses a hash function to organize elements, while an ordered set orders its element per a specified relation.

{AI95-00302-03} {AI05-0299-1} This subclause describes the declarations that are common to both kinds of sets. See A.18.8 for a description of the semantics specific to Containers.Hashed_Sets and A.18.9 for a description of the semantics specific to Containers.Ordered_Sets.

Static Semantics

{AI95-00302-03} The actual function for the generic formal function "+=" on Element_Type values is expected to define a reflexive and symmetric relationship and return the same result value each time it is called with a particular pair of values. If it behaves in some other manner, the function "+=" on set values returns an unspecified value. The exact arguments and number of calls of this generic formal function by the function "+=" on set values are unspecified.

Ramification: If the actual function for "+=" is not symmetric and consistent, the result returned by the "+=" for Set objects cannot be predicted. The implementation is not required to protect against "+=" raising an exception, or returning random results, or any other “bad” behavior. And it can call "+=" in whatever manner makes sense. But note that only the result of "+=" for Set objects is unspecified; other subprograms are not allowed to break if "+=" is bad (they aren’t expected to use "+=").

{AI95-00302-03} The type Set is used to represent sets. The type Set needs finalization (see 7.6).
A set contains elements. Set cursors designate elements. There exists an equivalence relation on elements, whose definition is different for hashed sets and ordered sets. A set never contains two or more equivalent elements. The length of a set is the number of elements it contains.

Each nonempty set has two particular elements called the first element and the last element (which may be the same). Each element except for the last element has a successor element. If there are no other intervening operations, starting with the first element and repeatedly going to the successor element will visit each element in the set exactly once until the last element is reached. The exact definition of these terms is different for hashed sets and ordered sets.

Some operations of these generic packages have access to subprogram parameters. To ensure such operations are well-defined, they guard against certain actions by the designated subprogram. In particular, some operations check for “tampering with cursors” of a container because they depend on the set of elements of the container remaining constant and, and others check for “tampering with elements” of a container because they depend on elements of the container not being replaced. When tampering with cursors is prohibited for a particular set object \( S \), Program_Error is propagated by the finalization of \( S \), as well as by a call that passes \( S \) to certain of the operations of this package, as indicated by the precondition of such an operation.

Discussion: Note that Replace_Element tampers with cursors because it might delete and reinsert the element if it moves in the set. That could change the order of iteration, which is what this check is designed to prevent. Replace also tampers with cursors, as it is defined in terms of Replace_Element.

These inclusions mean that there are no operations that would tamper with elements that do not tamper with cursors. As such, we do not define tampering with elements at all for set containers. Earlier versions of Ada did so just so the description of subprograms are the same between containers, but since we've changed those to pre- and postconditions which are necessarily specific to each container, there no longer seems to be any reason to define tampering with elements for sets.

Paragraphs 8 through 14 are removed as preconditions now describe these rules.

A subprogram is said to tamper with cursors of a set object \( S \) if:

- it inserts or deletes elements of \( S \), that is, it calls the Insert, Include, Clear, Delete, Exclude, or Replace_Element procedures with \( S \) as a parameter; or
- it finalizes \( S \); or
- it calls the Assign procedure with \( S \) as the Target parameter; or
- it calls the Move procedure with \( S \) as a parameter; or
- it calls one of the operations defined to tamper with the cursors of \( S \).

Reason: Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can't be allowed. However, a simple modification of (part of) an element is not a problem, so Update_Element_Preserving_Key does not cause a problem.
We don't need to list Replace and Replace_Element here because they are covered by "tamper with cursors". For Set, "tamper with cursors," and "tamper with elements" are the same. We leave both terms so that the rules for routines like Iterate and Query_Element are consistent across all containers.

When tampering with cursors is prohibited for a particular set object $S$, Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the cursors of $S$, leaving $S$ unmodified. Similarly, when tampering with elements is prohibited for a particular set object $S$, Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the elements of $S$ (or tamper with the cursors of $S$), leaving $S$ unmodified. These checks are made before any other defined behavior of the body of the language-defined subprogram.

Proof: Tampering with elements includes tampering with cursors, so we mention it only from completeness in the second sentence.

Empty_Set represents the empty Set object. It has a length of 0. If an object of type Set is not otherwise initialized, it is initialized to the same value as Empty_Set.

No_Element represents a cursor that designates no element. If an object of type Cursor is not otherwise initialized, it is initialized to the same value as No_Element.

The predefined "=" operator for type Cursor returns True if both cursors are No_Element, or designate the same element in the same container.

The primitive "=" operator is the one with two parameters of type Cursor which returns Boolean. We're not talking about some other (hidden) primitive function named ".=".

Execution of the default implementation of the Input, Output, Read, or Write attribute of type Cursor raises Program_Error.

Reason: A cursor will probably be implemented in terms of one or more access values, and the effects of streaming access values is unspecified. Rather than letting the user stream junk by accident, we mandate that streaming of cursors raise Program_Error by default. The attributes can always be specified if there is a need to support streaming.

Set'Write for a Set object $S$ writes Length($S$) elements of the set to the stream. It may also write additional information about the set.

Set'Read reads the representation of a set from the stream, and assigns to Item a set with the same length and elements as was written by Set'Write.

Ramification: Streaming more elements than the container length is wrong. For implementation implications of this rule, see the Implementation Note in A.18.2.

Returns True if Position designates an element, and returns False otherwise.

This function might not detect cursors that designate deleted elements; such cursors are invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

Returns True if Position designates an element in Container, and returns False otherwise.

Ramification: If Position is No_Element, Has_Element returns False.

If Left and Right denote the same set object, then the function returns True. If Left and Right have different lengths, then the function returns False. Otherwise, for each element
E in Left, the function returns False if an element equal to E (using the generic formal equality operator) is not present in Right. If the function has not returned a result after checking all of the elements, it returns True. Any exception raised during evaluation of element equality is propagated.

Implementation Note: This wording describes the canonical semantics. However, the order and number of calls on the formal equality function is unspecified for all of the operations that use it in this package, so an implementation can call it as many or as few times as it needs to get the correct answer. Specifically, there is no requirement to call the formal equality additional times once the answer has been determined.

function Equivalent_Sets (Left, Right : Set) return Boolean;  
{AI95-00302-03} If Left and Right denote the same set object, then the function returns True. If Left and Right have different lengths, then the function returns False. Otherwise, for each element E in Left, the function returns False if an element equivalent to E is not present in Right. If the function has not returned a result after checking all of the elements, it returns True. Any exception raised during evaluation of element equivalence is propagated.

function Tampering_With_Cursors_Prohibited (Container : Set) return Boolean with Nonblocking, Global => null, Use Formal => null;  
{AI12-0112-1} Returns True if tampering with cursors is currently prohibited for Container, and returns False otherwise.

Implementation Note: {AI12-0112-1} Various contracts elsewhere in this specification require that this function be implemented with synchronized data. Moreover, it is possible for tampering to be prohibited by multiple operations (sequentially or in parallel). Therefore, tampering needs to be implemented with an atomic or protected counter. The counter is initialized to zero, and is incremented when tampering is prohibited, and decremented when leaving an area that prohibited tampering. Function Tampering_With_Cursors_Prohibited returns True if the counter is nonzero. (Note that any case where the result is not well-defined for one task is incorrect use of shared variables and would be erroneous by the rules of 9.10, so no special protection is needed to read the counter.)

function To_Set (New_Item : Element_Type) return Set with Post => Length (To_Set'Result) = 1 and then not Tampering_with_Cursors_Prohibited (To_Set'Result);  
{AI95-00302-03} Returns a set containing the single element New_Item.

function Length (Container : Set) return Count_Type with Nonblocking, Global => null, Use Formal => null;  
{AI95-00302-03} Returns the number of elements in Container.

function Is_Empty (Container : Set) return Boolean with Nonblocking, Global => null, Use Formal => null, Post => Is_Empty'Result = (Length (Container) = 0);  
{AI95-00302-03} {AI12-0112-1} Returns True if Container is empty Equivalent to Length (Container) = 0.

procedure Clear (Container : in out Set) with Pre => not Tampering_with_Cursors_Prohibited (Container) or else raise Program_Error, Post => Length (Container) = 0;  
{AI95-00302-03} Removes all the elements from Container.

function Element (Position : Cursor) return Element_Type with Pre => Position /= No_Element or else raise Constraint_Error, Nonblocking, Global => in all, Use Formal => Element_Type;  
{AI95-00302-03} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated. Otherwise, Element returns the element designated by Position.
function Element (Container : Set;  
               Position  : Cursor) return Element_Type
with Pre => (Position /= No_Element
                   or else raise Constraint_Error)
               and then
               (Has Element (Container, Position)
                   or else raise Program_Error),
               Nonblocking, Global => null, Use Formal => Element_Type;

{AI12-0112-1} Element returns the element designated by Position.

procedure Replace_Element (Container : in out Set;
                           Position  : in Cursor;
                           New_item  : in Element_Type)
with Pre => (not Tampering_With_Elements_Prohibited (Container)
                   or else raise Program_Error)
               and then
               (Position /= No_Element
                   or else raise Constraint_Error)
               and then
               (Has Element (Container, Position)
                   or else raise Program_Error);

{AI95-00302-03} {AI12-0112-1} {AI12-0196-1} If Position equals No_Element, then
Constraint_Error is propagated; if Position does not designate an element in Container, then
Program_Error is propagated. If an element equivalent to New_Item is already present in
Container at a position other than Position, Program_Error is propagated. Otherwise,
Replace_Element assigns New_Item to the element designated by Position. Any exception raised
by the assignment is propagated. For the purposes of determining whether the parameters overlap
in a call to Replace_Element, the Container parameter is not considered to overlap with any
object (including itself).

Implementation Note: The final assignment may require that the node of the element be moved in the Set's data
structures. That could mean that implementing this operation exactly as worded above could require the overhead
of searching twice. Implementations are encouraged to avoid this extra overhead when possible, by prechecking if the old
element is equivalent to the new one, by inserting a placeholder node while checking for an equivalent element, and
similar optimizations.

The cursor still designates the same element after this operation; only the value of that element has changed. Cursors
cannot include information about the relative position of an element in a Set (as they must survive insertions and
deletions of other elements), so this should not pose an implementation hardship.

procedure Query_Element
(Position : in Cursor;
 Process : not null access procedure (Element : in Element_Type))
with Pre => Position /= No_Element
                  or else raise Constraint_Error,
             Global => in all;

{AI95-00302-03} {AI05-0021-1} {AI05-0265-1} {AI12-0112-1} If Position equals No_Element,
then Constraint_Error is propagated. Otherwise, Query_Element calls Process.all with the
element designated by Position as the argument. TamperingProgram_Error is propagated if
Process.all tampers with the elements of the set that contains the element designated by Position
is prohibited during the execution of the call on Process.allContainer. Any exception raised by
Process.all is propagated.

procedure Query_Element
(Container : in Set;
 Process : not null access procedure (Element : in Element_Type))
with Pre => (Position /= No_Element
                 or else raise Constraint_Error)
          and then
          (Has Element (Container, Position)
             or else raise Program_Error);
Query_Element calls Process.all with the key and element from the node designated by Position as the arguments. Tampering with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

The type Constant_Reference_Type needs finalization.

This paragraph was deleted.

Reason: It is expected that Constant_Reference_Type will be a controlled type, for which finalization will have some action to terminate the tampering check for the associated container. If the object is created by default, however, there is no associated container. Since this is useless, and supporting this case would take extra work, we define it to raise an exception.

This function (combined with the Constant Indexing and Implicit Dereference aspects) provides a convenient way to gain read access to an individual element of a set given a cursor.

If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Constant_Reference returns an object whose discriminant is an access value that designates the element designated by Position. Tampering with the cursor elements of Container is prohibited while the object returned by Constant_Reference exists and has not been finalized.

If Target denotes the same object as Source, the operation has no effect. Otherwise, the elements of Source are copied to Target as for an assignment statement assigning Source to Target.

Discussion: This routine exists for compatibility with the bounded set containers. For an unbounded set, Assign(A, B) and A := B behave identically. For a bounded set, := will raise an exception if the container capacities are different, while Assign will not raise an exception if there is enough room in the target.
procedure Move (Target : in out Set;
Source : in out Set)
with Pre => (not Tampering With Cursors Prohibited (Target)
or else raise Program_Error) and then
(not Tampering With Cursors Prohibited (Source)
or else raise Program_Error),
Post => (if not Target'Has Same Storage (Source) then
Length (Target) = Length (Source'Old) and then
Length (Source) = 0);

If Target denotes the same object as Source, then the operation Move has no effect. Otherwise, the operation is equivalent to Assign (Target, Source) followed by Clear (Source). Move first clears Target. Then, each element from Source is removed from Source and inserted into Target. The length of Source is 0 after a successful call to Move.

procedure Insert (Container : in out Set;
New_Item : in Element_Type;
Position : out Cursor;
Inserted : out Boolean)
with Pre => (not Tampering With Elements Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Original_Length : constant Count_Type :=
Length (Container)'Old;
beginn
Has_Element (Container, Position) and then
(if Inserted then
Length (Container) = Original_Length + 1
else
Length (Container) = Original Length));

Insert checks if an element equivalent to New_Item is already present in Container. If a match is found, Inserted is set to False and Position designates the matching element. Otherwise, Insert adds New_Item to Container; Inserted is set to True and Position designates the newly-inserted element. Any exception raised during allocation is propagated and Container is not modified.

procedure Insert (Container : in out Set;
New_Item : in Element_Type)
with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => Length (Container) = Length (Container)'Old + 1;

Insert inserts New_Item into Container as per the four-parameter Insert, with the difference that if an element equivalent to New_Item is already in the set, then Constraint_Error is propagated.

Discussion: This is equivalent to:

declare
Inserted : Boolean; C : Cursor;
beginn
Insert (Container, New_Item, C, Inserted);
if not Inserted then
raise Constraint_Error;
end if;
end;

but doesn't require the hassle of out parameters.
procedure Include (Container : in out Set;  
New_Item : in Element_Type) 
with Pre => (not Tampering_With.Cursors_Prohibited (Container) 
or else raise Program_Error) and then 
(Length (Container) <= Count_Type'Last - 1 
or else raise Constraint_Error), 
Post => (declare 
Original_Length : constant Count_Type := 
Length (Container)'Old; 
begin 
Length (Container) in 
Original_Length | Original_Length + 1); 

Include inserts New_Item into Container as per the four-parameter Insert, with 
the difference that if an element equivalent to New_Item is already in the set, then it is replaced. 
Any exception raised during assignment is propagated.

procedure Replace (Container : in out Set;  
New_Item : in Element_Type) 
with Pre => not Tampering_With.Cursors_Prohibited (Container) 
or else raise Program_Error, 
Post => Length (Container) = Length (Container)'Old; 

Replace checks if an element equivalent to New_Item is already in the set. If a 
match is found, that element is replaced with New_Item; otherwise, Constraint_Error is 
propagated.

procedure Exclude (Container : in out Set;  
Item : in Element_Type) 
with Pre => not Tampering_With.Cursors_Prohibited (Container) 
or else raise Program_Error, 
Post => (declare 
Original_Length : constant Count_Type := 
Length (Container)'Old; 
begin 
Length (Container) in 
Original_Length - 1 | Original_Length); 

Exclude checks if an element equivalent to Item is present in Container. If a 
match is found, Exclude removes the element from the set.

procedure Delete (Container : in out Set;  
Item : in Element_Type) 
with Pre => not Tampering_With.Cursors_Prohibited (Container) 
or else raise Program_Error, 
Post => Length (Container) = Length (Container)'Old - 1; 

Delete checks if an element equivalent to Item is present in Container. If a 
match is found, Delete removes the element from the set; otherwise, Constraint_Error is 
propagated.

procedure Delete (Container : in out Set;  
Position : in out Cursor) 
with Pre => (not Tampering_With.Cursors_Prohibited (Container) 
or else raise Program_Error) and then 
(Position /= No_Element 
or else raise Constraint_Error) and then 
(Has_Element (Container, Position) 
or else raise Program_Error), 
Post => Length (Container) = Length (Container)'Old - 1 and then 
Position = No_Element; 

If Position equals No_Element, then Constraint_Error is 
propagated. If Position does not designate an element in Container, then Program_Error is
Delete removes the element designated by Position from the set. Position is set to No-Element on return.

Ramification: The check on Position checks that the cursor does not belong to some other set. This check implies that a reference to the set is included in the cursor value. This wording is not meant to require detection of dangling cursors; such cursors are defined to be invalid, which means that execution is erroneous, and any result is allowed (including not raising an exception).

```
procedure Union (Target : in out Set;
                   Source : in  Set)
with Pre  => not Tampering_With_Cursors_Prohibited (Target)
          or else raise Program_Error,
    Post => Length (Target) <= Length (Target)'Old + Length (Source);
```

\{AI95-00302-03\} Union inserts into Target the elements of Source that are not equivalent to some element already in Target.

Implementation Note: If the objects are the same, the result is the same as the original object. The implementation needs to take care so that aliasing effects do not make the result trash; Union (S, S); must work.

```
function Union (Left, Right : Set)
return Set
with Post => Length (Union'Result) <= Length (Left) + Length (Right) and then
      not Tampering_With_Cursors_Prohibited (Union'Result);
```

\{AI95-00302-03\} Returns a set comprising all of the elements of Left, and the elements of Right that are not equivalent to some element of Left.

```
procedure Intersection (Target : in out Set;
                       Source : in  Set)
with Pre  => not Tampering_With_Cursors_Prohibited (Target)
       or else raise Program_Error,
    Post => Length (Target) <= Length (Target)'Old + Length (Source);
```

\{AI95-00302-03\} \{AI05-0004-1\} IntersectionUnion deletes from Target the elements of Target that are not equivalent to some element of Source.

Implementation Note: If the objects are the same, the result is the same as the original object. The implementation needs to take care so that aliasing effects do not make the result trash; Intersection (S, S); must work.

```
function Intersection (Left, Right : Set)
return Set
with Post => Length (Intersection'Result) <=
          Length (Left) + Length (Right) and then
      not Tampering_With_Cursors_Prohibited (Intersection'Result);
```

\{AI95-00302-03\} Returns a set comprising all the elements of Left that are equivalent to the some element of Right.

```
procedure Difference (Target : in out Set;
                     Source : in  Set)
with Pre  => not Tampering_With_Cursors_Prohibited (Target)
       or else raise Program_Error,
    Post => Length (Target) <= Length (Target)'Old + Length (Source);
```

\{AI95-00302-03\} If Target denotes the same object as Source, then Difference clears Target. Otherwise, it deletes from Target the elements that are equivalent to some element of Source.

```
function Difference (Left, Right : Set)
return Set
with Post => Length (Difference'Result) <= Length (Left) +
        Length (Right) and then
      not Tampering_With_Cursors_Prohibited (Difference'Result);
```

\{AI95-00302-03\} Returns a set comprising the elements of Left that are not equivalent to some element of Right.
procedure Symmetric_Difference (Target : in out Set; 
Source : in Set) 
with Pre => not Tampering_With.Cursors_Prohibited (Target) 
or else raise Program_Error, 
Post => Length (Target) <= Length (Target)'Old + Length (Source); 

function Symmetric_Difference (Left, Right : Set) return Set 
with Post => Length (Symmetric_Difference'Result) <= 
Length (Left) + Length (Right) and then 
not Tampering_With.Cursors_Prohibited (Symmetric_Difference'Result); 

function Overlap (Left, Right : Set) return Boolean; 
function Is_Subset (Subset : Set; 
Of_Set : Set) return Boolean; 

function First (Container : Set) return Cursor 
with Nonblocking, Global => null, Use Formal => null, 
Post => (if not Is_Empty (Container) 
then Has_Element (Container, First'Result) 
else First'Result = No_Element); 

function Next (Position : Cursor) return Cursor 
with Nonblocking, Global => in all, Use Formal => null, 
Post => (if Position = No_Element then Next'Result = No_Element); 

function Next (Container : Set; 
Position : Cursor) return Cursor 
with Nonblocking, Global => null, Use Formal => null, 
Pre => Position = No_Element or else 
Has_Element (Container, Position) 
or else raise Program_Error, 
Post => (if Position = No_Element then Next'Result = No_Element 
elsif Next'Result = No_Element then 
Position = Last (Container) 
else Has_Element (Container, Next'Result)); 

Returns a cursor designating the successor of the node designated by Position in Container.
procedure Next (Position : in out Cursor)
  with Nonblocking, Global => in all, Use Formal => null;

{AI95-00302-03} Equivalent to Position := Next (Position).

procedure Next (Container : in Set;
  Position : in out Cursor)
  with Nonblocking, Global => null, Use Formal => null,
  Pre => Position = No_Element or else
  Has_Element (Container, Position)
  or else raise Program_Error,
  Post => (if Position /= No_Element
    then Has_Element (Container, Position));

{AI12-0112-1} Equivalent to Position := Next (Container, Position).

This paragraph was deleted.

{AI95-00302-03} {AI05-0004-1} Equivalent to Find (Container, Item) /= No_Element.

function Find (Container : Set;
  Item : Element_Type) return Cursor
  with Post => (if Find'Result /= No_Element
    then Has_Element (Container, Find'Result));

{AI95-00302-03} If Length (Container) equals 0, then Find returns No_Ele ment. Otherwise, Find checks if an element equivalent to Item is present in Container. If a match is found, a cursor designating the matching element is returned; otherwise, No_Element is returned.

function Contains (Container : Set;
  Item : Element_Type) return Boolean;

{AI05-0004-1} Equivalent to Find (Container, Item) /= No_Element.

function Has_Element (Position : Cursor) return Boolean;

{AI95-00302-03} {AI05-0212-1} Returns True if Position designates an element, and returns False otherwise.

To be honest: {AI05-0212-1} This function may not detect cursors that designate deleted elements: such cursors are invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

Paragraphs 83 and 84 were moved above.

procedure Iterate
  (Container : in Set;
  Process : not null access procedure (Position : in Cursor))
  with Allows Exit;

{AI95-00302-03} {AI05-0265-1} Iterate calls Process.all with a cursor that designates each element in Container, starting with the first element and moving the cursor according to the successor relation. Tampering Program_Error is propagated if Process.all tampers with the cursors of Container is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.

Implementation Note: The “tamper with cursors” check takes place when the operations that insert or delete elements, and so on are called.

See Iterate for vectors (A.18.2) for a suggested implementation of the check.

{AI95-00302-03} Both Containers.Hashed_Set and Containers.Ordered_Set declare a nested generic package Generic_Keys, which provides operations that allow set manipulation in terms of a key (typically, a portion of an element) instead of a complete element. The formal function Key of Generic_Keys extracts a key value from an element. It is expected to return the same value each time it is called with a particular element. The behavior of Generic_Keys is unspecified if Key behaves in some other manner.
A key is expected to unambiguously determine a single equivalence class for elements. The behavior of Generic Keys is unspecified if the formal parameters of this package behave in some other manner.

```ada
function Key (Position : Cursor) return Key_Type
  with Pre => Position /= No_Element or else raise Constraint_Error,
  Global => in all;

function Key (Container : Set; Position : Cursor) return Key_Type
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
             (Has_Element (Container, Position) or else raise Program_Error);
```

Equivalent to Key (Element (Position)).

Equivalent to Key (Element (Container, Position)).

The subprograms in package Generic Keys named Contains, Find, Element, Delete, and Exclude, are equivalent to the corresponding subprograms in the parent package, with the difference that the Key parameter is used to locate an element in the set.

```ada
procedure Replace (Container : in out Set; Key : in Key_Type;
                   New_Item : in Element_Type)
  with Pre => not Tampering_With_Cursors_Prohibited (Container)
            or else raise Program_Error,
  Post => Length (Container) = Length (Container)'Old;
```

Equivalent to Replace_Element (Container, Find (Container, Key), New_Item).

```ada
procedure Update_Element_Preserving_Key
  (Container : in out Set; Position : in Cursor; Process : not null access procedure
    (Element : in out Element_Type))
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
             (Has_Element (Container, Position) or else raise Program_Error);
```

Equivalent to Replace_Element (Container, Find (Container, Key), New_Item).

If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Update_Element_Preserving_Key uses Key to save the key value K of the element designated by Position. Update_Element_Preserving_Key then calls Process.all with that element as the argument. Tampering_Program_Error is propagated if Process.all tampers with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated. After Process.all returns, Update_Element_Preserving_Key checks if K determines the same equivalence class as that for the new element; if not, the element is removed from the set and Program_Error is propagated.

Reason: The key check ensures that the invariants of the set are preserved by the modification. The “tampers with the elements” check prevents data loss (if Element_Type is by-copy) or erroneous execution (if element type is unconstrained and indefinite).

If Element_Type is unconstrained and definite, then the actual Element parameter of Process.all shall be unconstrained.

Ramification: This means that the elements cannot be directly allocated from the heap; it must be possible to change the discriminants of the element in place.
type Reference_Type (Element : not null access Element_Type) is
private
  with Implicit_Dereference => Element,
     Nonblocking, Global => in out synchronized,
     Default Initial Condition => (raise Program_Error);

The type Reference_Type needs finalization.

This paragraph was deleted.

The default initialization of an object of type Reference_Type propagates Program_Error.

function Reference_Preserving_Key (Container : aliased in out Set;
  Position : in Cursor)
  return Reference_Type
  with Pre => (Position /= No_Element
               or else raise Constraint_Error) and then
               (Has_Element (Container, Position)
               or else raise Program_Error),
     Post => Tampering_With_Cursors_Prohibited (Container);

This function (combined with the Implicit_Dereference aspect)
provides a convenient way to gain read and write access to an individual element of a set given a
cursor.

If Position equals No_Element, then
Constraint_Error is propagated; if Position does not designate an element in Container, then
Program_Error is propagated. Otherwise, Reference_Preserving_Key uses Key to save the key
value K; then returns an object whose discriminant is an access value that designates the element
designated by Position. Tampering with the cursorelements of Container is prohibited while the
object returned by Reference_Preserving_Key exists and has not been finalized. When the object
returned by Reference_Preserving_Key is finalized, a check is made if K determines the same
equivalence class as that for the new element; if not, the element is removed from the set and
Program_Error is propagated.

function Constant_Reference (Container : aliased in Set;
  Key       : in Key_Type)
  return Constant_Reference_Type
  with Pre => Find (Container, Key) /= No_Element
          or else raise Constraint_Error,
     Post => Tampering_With_Cursors_Prohibited (Container);

This function (combined with the Implicit_Dereference aspect)
provides a convenient way to gain read access to an individual element of a set given a key value.
Equivalent to Constant_Reference (Container, Find (Container, Key)).

function Reference_Preserving_Key (Container : aliased in out Set;
  Key       : in Key_Type)
  return Reference_Type
  with Pre => Find (Container, Key) /= No_Element
          or else raise Constraint_Error,
     Post => Tampering_With_Cursors_Prohibited (Container);

This function (combined with the Implicit_Dereference aspect)
provides a convenient way to gain read and write access to an individual element of a set given a
key value.
Equivalent to Reference_Preserving_Key (Container, Find (Container, Key)).

The nested package Stable provides a type Stable.Set that represents a stable set, which is
one that cannot grow and shrink. Such a set can be created by calling the Copy function, or by
establishing a stabilized view of an ordinary set.
The subprograms of the set package that have a parameter or result of type Set are included in the nested package Stable with the same specification, except that the following are omitted:

- Tampering With Cursors Prohibited, Assign, Move, Insert, Include, Clear, Delete, Exclude, Replace, Replace Element, procedures Union, Intersection, Difference, and Symmetric Difference, (for Ordered sets) Delete First and Delete Last, and (for Hashed sets) Reserve Capacity.

**Discussion:** The Generic Keys package is not included in the Stable package. The functions Union, Intersection, Difference, and Symmetric Difference are included in the Stable package.

**Ramification:** The names Set and Cursor mean the types declared in the nested package in these subprogram specifications.

**Reason:** The omitted routines are those that tamper with cursors (or test that state). The model is that it is impossible to tamper with cursors of a stable view since no such operations are included. Thus tampering checks are not needed for a stable view, and we omit the operations associated with those checks.

The operations of this package are equivalent to those for ordinary sets, except that the calls to Tampering With Cursors Prohibited that occur in preconditions are replaced by False, and any that occur in postconditions are replaced by True.

If a stable set is declared with the Base discriminant designating a pre-existing ordinary set, the stable set represents a stabilized view of the underlying ordinary set, and any operation on the stable set is reflected on the underlying ordinary set. While a stabilized view exists, any operation that tampers with cursors performed on the underlying set is prohibited. The finalization of a stable set that provides such a view removes this restriction on the underlying ordinary set [(though some other restriction can exist due to other concurrent iterations or stabilized views)].

If a stable set is declared without specifying Base, the object is necessarily initialized. The initializing expression of the stable set, [typically a call on Copy], determines the Length of the set. The Length of a stable set never changes after initialization.

**Proof:** Initialiation is required as the type is indefinite, see 3.3.1.

**Bounded (Run-Time) Errors**

It is a bounded error for the actual function associated with a generic formal subprogram, when called as part of an operation of a set package, to tamper with elements of any set parameter of the operation. Either Program_Error is raised, or the operation works as defined on the value of the set either prior to, or subsequent to, some or all of the modifications to the set.

It is a bounded error to call any subprogram declared in the visible part of a set package when the associated container has been finalized. If the operation takes Container as an in out parameter, then it raises Constraint_Error or Program_Error. Otherwise, the operation either proceeds as it would for an empty container, or it raises Constraint_Error or Program_Error.

**Erroneous Execution**

A Cursor value is invalid if any of the following have occurred since it was created:

- The set that contains the element it designates has been finalized;
- The set that contains the element it designates has been used as the Target of a call to Assign, or as the target of an assignment statement;
- The set that contains the element it designates has been used as the Source or Target of a call to Move;
- The element it designates has been removed/deleted from the set that previously contained the element.
Ramification:  

\{AI05-0160-1\}  This can happen directly via calls to Clear, Exclude, Delete, and Update Element Preserving Key, and indirectly via calls to procedures Intersection, Difference, and Symmetric Difference.

\{AI95-00302-03\}  The result of "=" or Has Element is unspecified if these functions are called with an invalid cursor parameter. Execution is erroneous if any other subprogram declared in Containers.Hashed_Sets or Containers.Ordered_Sets is called with an invalid cursor parameter.

Discussion:  

The list above is intended to be exhaustive. In other cases, a cursor value continues to designate its original element. For instance, cursor values survive the insertion and deletion of other elements.

While it is possible to check for these cases, in many cases the overhead necessary to make the check is substantial in time or space. Implementations are encouraged to check for as many of these cases as possible and raise Program_Error if detected.

\{AI05-0212-1\}  Execution is erroneous if the set associated with the result of a call to Reference or Constant Reference is finalized before the result object returned by the call to Reference or Constant Reference is finalized.

Reason:  

Each object of Reference_Type and Constant_Reference_Type probably contains some reference to the originating container. If that container is prematurely finalized (which is only possible via Unchecked_Deallocation, as accessibility checks prevent passing a container to Reference that will not live as long as the result), the finalization of the object of Reference_Type will try to access a nonexistent object. This is a normal case of a dangling pointer created by Unchecked_Deallocation; we have to explicitly mention it here as the pointer in question is not visible in the specification of the type. (This is the same reason we have to say this for invalid cursors.)

Implementation Requirements

\{AI95-00302-03\} \{AI12-0437-1\}  No storage associated with a set object shall be lost upon assignment or scope exit.

\{AI95-00302-03\} \{AI05-0262-1\}  The execution of an assignment_statement for a set shall have the effect of copying the elements from the source set object to the target set object and changing the length of the target object to that of the source object.

Implemnetation Note:  

\{AI05-0298-1\}  An assignment of a Set is a “deep” copy; that is the elements are copied as well as the data structures. We say “effect of” in order to allow the implementation to avoid copying elements immediately if it wishes. For instance, an implementation that avoided copying until one of the containers is modified would be allowed. (Note that this implementation would require care, see A.18.2 for more.)

Implementation Advice

\{AI95-00302-03\}  Move should not copy elements, and should minimize copying of internal data structures.

Implementation Advice:  Move for sets should not copy elements, and should minimize copying of internal data structures.

Implementation Note:  Usually that can be accomplished simply by moving the pointer(s) to the internal data structures from the Source container to the Target container.

\{AI95-00302-03\}  If an exception is propagated from a set operation, no storage should be lost, nor any elements removed from a set unless specified by the operation.

Implementation Advice:  If an exception is propagated from a set operation, no storage should be lost, nor any elements removed from a set unless specified by the operation.

Reason:  This is important so that programs can recover from errors. But we don't want to require heroic efforts, so we just require documentation of cases where this can't be accomplished.

Wording Changes from Ada 95

\{AI95-00302-03\}  This description of sets is new; the extensions are documented with the specific packages.

Extensions to Ada 2005

\{AI05-0212-1\}  Added reference support to make set containers more convenient to use.
Wording Changes from Ada 2005

- {AI05-0001-1} Added procedure Assign; the extension and incompatibility is documented with the specific packages.
- {AI05-0001-1} Generalized the definition of Move. Specified which elements are read/written by stream attributes.
- {AI05-0022-1} Correction: Added a Bounded (Run-Time) Error to cover tampering by generic actual subprograms.
- {AI05-0027-1} Correction: Added a Bounded (Run-Time) Error to cover access to finalized set containers.
- {AI05-0160-1} Correction: Revised the definition of invalid cursors to cover missing (and new) cases.
- {AI05-0265-1} Correction: Defined when a container prohibits tampering in order to more clearly define where the check is made and the exception raised.

Inconsistencies With Ada 2012

- {AI12-0111-1} Procedures Union, Intersection, Difference, and Symmetric Difference are now defined to tamper with the cursors of the Target parameter. A program which attempts to use one of these operations while tampering is prohibited will raise Program_Error. However, since the operations do modify the container, the effects would have been unpredictable, so this change will likely fix bugs.

Extensions to Ada 2012

- {AI12-0196-1} Correction: Replace Element is now defined such that it can be used concurrently so long as it operates on different elements. This allows some container operations to be used in parallel without separate synchronization.

Wording Changes from Ada 2012

- {AI12-0110-1} Corrigendum: Clarified that tampering checks precede all other checks made by a subprogram (but come after those associated with the call).
- {AI12-0112-1} Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).

A.18.8 The Generic Package Containers.Hashed_Sets

Static Semantics

- {AI95-00302-03} The generic library package Containers.Hashed_Sets has the following declaration:

  ```
  generic
  type Element_Type is private;
  with function Hash (Element : Element_Type) return Hash_Type;
  with function Equivalent_Elements (Left, Right : Element_Type)
    return Boolean;
  with function "=" (Left, Right : Element_Type) return Boolean is <>;
  package Ada.Containers.Hashed_Sets is
    with Preelaborate, Remote_Types, Nonblocking, Global => in out synchronized is
    pragma Preelaborate(Hashed_Sets);
    pragma Remote_Types(Hashed_Sets);
  end Ada.Containers.Hashed_Sets;
  ```

Discussion: {AI12-0112-1} For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).
type Set is tagged private
with Constant_Indexing => Constant_Reference,
  Default_Iterator => Iterate,
  Iterator_Element => Element_Type,
  Iterator_View => Stable.Set,
  Aggregate => (Empty => Empty, AddUnnamed => Include),
  Stable_Properties => (Length,
            Tampering_With_Cursors_Prohibited),
  Default_Initial_Condition =>
    Length (Set) = 0 and then
    not Tampering_With_Cursors_Prohibited (Set)),
pragma Preelaborable_Initialization(Set);

Discussion: Unlike a Vector, the Stable_Properties of a Hashed_Set do not include the Capacity. If we had included it, some of the otherwise shared definitions would need different postconditions for Hashed_Sets and Ordered_Sets. If we were starting these containers from scratch, we probably would have approached the sharing of definitions differently so that we could avoid issues like this, but a major reorganization of this existing material would be too much change.

type Cursor is private
withpragma Preelaborable_Initialization(Cursor);

Empty_Set : constant Set;
No_Element : constant Cursor;
function Has_Element (Position : Cursor) return Boolean
  with Nonblocking, Global => in all, Use Formal => null;
function Has_Element (Container : Set; Position : Cursor)
  return Boolean
  with Nonblocking, Global => null, Use Formal => null;
package Set_Iterator_Interfaces is new
  Ada.Iterator_Interfaces (Cursor, Has_Element);
function "=" (Left, Right : Set) return Boolean;
function Equivalent_Sets (Left, Right : Set) return Boolean;
function Tampering_With_Cursors_Prohibited
  (Container : Set)
  return Boolean
  with Nonblocking, Global => null, Use Formal => null;
function Empty (Capacity : Count_Type := implementation-defined)
  return Set
  with Post =>
    Capacity (Empty'Result) >= Capacity and then
    not Tampering_With_Cursors_Prohibited (Empty'Result) and then
    Length (Empty'Result) = 0;
function To_Set (New_Item : Element_Type)
  return Set
  with Post =>
    Length (To_Set'Result) = 1 and then
    not Tampering_with_Cursors_Prohibited (To_Set'Result);
function Capacity (Container : Set)
  return Count_Type
  with Nonblocking, Global => null, Use Formal => null;
procedure Reserve_Capacity (Container : in out Set;
  Capacity : in Count_Type)
  with Pre => not Tampering_With_Cursors_Prohibited (Container)
  or else raise Program_Error,
  Post => Container.Capacity >= Capacity;
function Length (Container : Set)
  return Count_Type
  with Nonblocking, Global => null, Use Formal => null;
function Is.Empty (Container : Set)
  return Boolean
  with Nonblocking, Global => null, Use Formal => null,
  Post => Is.Empty'Result = (Length (Container) = 0);
```ada
procedure Clear (Container : in out Set)
   with Pre => not Tampering_With_Cursors_Prohibited (Container)
   Post => Capacity (Container) = Capacity (Container)'Old and then
           Length (Container) = 0;

function Element (Position : Cursor) return Element_Type
   with Pre => (Position /= No_Element or else raise Constraint_Error)
   Nonblocking, Global => in all, Use_Formal => Element_Type;

procedure Replace_Element (Container : in out Set;
                           Position : in Cursor;
                           New_item : in Element_Type)
   with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
               (Position /= No_Element
               or else raise Constraint_Error) and then
               (Has_Element (Container, Position)
               or else raise Program_Error),
               Nonblocking, Global => null, Use_Formal => Element_Type;

procedure Query_Element (Position : in Cursor;
                         Process : not null access procedure (Element : in Element_Type))
   with Pre => (Position /= No_Element
               or else raise Constraint_Error) and then
               (Has_Element (Container, Position)
               or else raise Program_Error);

procedure Query_Element (Container : in Set;
                         Position : in Cursor;
                         Process : not null access procedure (Element : in Element_Type))
   with Pre => (Position /= No_Element
               or else raise Constraint_Error) and then
               (Has_Element (Container, Position)
               or else raise Program_Error);

type Constant_Reference_Type (Element : not null access constant Element_Type)
   is private
   with Implicit_Dereference => Element,
   Nonblocking, Global => in all synchronized,
   Default_Initial_Condition => (raise Program_Error);

function Constant_Reference (Container : aliased in Set;
                            Position : in Cursor)
   return Constant_Reference_Type
   with Pre => (Position /= No_Element
               or else raise Constraint_Error) and then
               (Has_Element (Container, Position)
               or else raise Program_Error),
               Post => Tampering_With_Cursors_Prohibited (Container),
               Nonblocking, Global => null, Use_Formal => null;

procedure Assign (Target : in out Set; Source : in Set)
   with Pre => not Tampering_With_Cursors_Prohibited (Target)
   or else raise Program_Error,
   Post => Length (Source) = Length (Target) and then
           Capacity (Target) => Length (Source);
function Copy (Source : Set; Capacity : Count_Type := 0)
return Set
with Pre => Capacity = 0 or else Capacity >= Length (Source)
or else raise Capacity_Error,
Post =>
Length (Copy'Result) = Length (Source) and then
not Tampering_With_Cursors_Prohibited (Copy'Result) and then
Copy'Result.Capacity = (if Capacity = 0 then
Length (Source) else Capacity);
procedure Move (Target : in out Set;
Source : in out Set)
with Pre => (not Tampering_With_Cursors_Prohibited (Target)
 or else raise Program_Error) and then
(not Tampering_With_Cursors_Prohibited (Source)
 or else raise Program_Error),
Post => (if not Target'Has_Same_Storage (Source) then
Length (Target) = Length (Source'Old) and then
Length (Source) = 0);
procedure Insert (Container : in out Set;
New_Item  : in Element_Type;
Position  : out Cursor;
Inserted  : out Boolean)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
 or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
 or else raise Constraint_Error),
Post =>
begin
Original_Length := Length (Container)'Old;
Has_Element (Container, Position)
and then
(if Inserted then
Length (Container) = Original_Length + 1
else
Length (Container) = Original_Length)) and then
Capacity (Container) >= Length (Container);
procedure Insert (Container : in out Set;
New_Item  : in Element_Type)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
 or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
 or else raise Constraint_Error),
Post => Length (Container) = Length (Container)'Old + 1 and then
Capacity (Container) >= Length (Container);
procedure Include (Container : in out Set;
New_Item  : in Element_Type)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
 or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
 or else raise Constraint_Error),
Post =>
begin
Original_Length := Length (Container)'Old;
Length (Container)
in Original Length | Original Length + 1) and then
Capacity (Container) >= Length (Container);
procedure Replace (Container : in out Set;
New_Item  : in Element_Type)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Length (Container) = Length (Container)'Old;
procedure Exclude (Container : in out Set; Item : in Element_Type) with Pre => not Tampering_With_Cursors_Prohibited (Container) or else raise Program_Error, Post => (declare Original Length : constant Count_Type := Length (Container)'Old; begin Length (Container) in Original Length - 1 | Original Length);

procedure Delete (Container : in out Set; Item : in Element_Type) with Pre => not Tampering_With_Cursors_Prohibited (Container) or else raise Program_Error, Post => Length (Container) = Length (Container)'Old - 1;

procedure Delete (Container : in out Set; Position : in out Cursor) with Pre => (not Tampering_With_Cursors_Prohibited (Container) or else raise Program_Error) and then (Position /= No_Element or else raise Constraint_Error) and then (Has_Element (Container, Position) or else raise Program_Error), Post => Length (Container) = Length (Container)'Old - 1 and then Position = No_Element;

procedure Union (Target : in out Set; Source : in Set) with Pre => not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error, Post => Length (Target) <= Length (Target)'Old + Length (Source);

function Union (Left, Right : Set) return Set with Post => Length (Union'Result) <= Length (Left) + Length (Right) and then not Tampering_With_Cursors_Prohibited (Union'Result);

function "or" (Left, Right : Set) return Set renames Union;

procedure Intersection (Target : in out Set; Source : in Set) with Pre => not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error, Post => Length (Target) <= Length (Target)'Old + Length (Source);

function Intersection (Left, Right : Set) return Set with Post => Length (Intersection'Result) <= Length (Left) + Length (Right) and then not Tampering_With_Cursors_Prohibited (Intersection'Result);

function "and" (Left, Right : Set) return Set renames Intersection;

procedure Difference (Target : in out Set; Source : in Set) with Pre => not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error, Post => Length (Target) <= Length (Target)'Old + Length (Source);

function Difference (Left, Right : Set) return Set with Post => Length (Difference'Result) <= Length (Left) + Length (Right) and then not Tampering_With_Cursors_Prohibited (Difference'Result);

function "-" (Left, Right : Set) return Set renames Difference;

procedure Symmetric_Difference (Target : in out Set; Source : in Set) with Pre => not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error, Post => Length (Target) <= Length (Target)'Old + Length (Source);
**Symmetric_Difference** (Left, Right : Set) return Set

with Post =>

Length (Symmetric_Difference'Result) <=
Length (Left) + Length (Right) and then
not Tampering_With_Cursors_Prohibited (Symmetric_Difference'Result);

**xor** (Left, Right : Set) return Set

renames Symmetric_Difference;

**Overlap** (Left, Right : Set) return Boolean;

**Is_Subset** (Subset : Set; Of_Set : Set) return Boolean;

**First** (Container : Set) return Cursor

with Nonblocking, Global => null, Use Formal => null,
Post => (if not Is_Empty (Container)
then Has_Element (Container, First'Result)
else First'Result = No_Element);

**Next** (Position : Cursor) return Cursor

with Nonblocking, Global => in all, Use Formal => null,
Post => (if Position = No_Element then Next'Result = No_Element);

**Next** (Container : Set; Position : Cursor) return Cursor

with Nonblocking, Global => null, Use Formal => null,
Pre => Position = No_Element or else
Has_Element (Container, Position)
or else raise Program_Error,
Post => (if Position = No_Element then Next'Result = No_Element
elseif Next'Result = No_Element then
Position = Last (Container)
else Has_Element (Container, Next'Result));

**Next** (Position : in out Cursor)

with Nonblocking, Global => in all, Use Formal => null;

**Next** (Container : in Set; Position : in out Cursor)

with Nonblocking, Global => null, Use Formal => null,
Pre => Position = No_Element or else
Has_Element (Container, Position)
or else raise Program_Error,
Post => (if Position /= No_Element
then Has_Element (Container, Position));

**Find** (Container : Set; Item : Element_Type)

return Cursor

with Post => (if Find'Result /= No_Element
then Has_Element (Container, Find'Result));

**Contains** (Container : Set; Item : Element_Type) return Boolean;

This paragraph was deleted.

**Equivalent_Elements** (Left, Right : Cursor)

return Boolean

with Pre => (Left /= No_Element and then Right /= No_Element)
or else raise Constraint_Error,
Global => in all;

**Equivalent_Elements** (Left : Cursor; Right : Element_Type)

return Boolean

with Pre => Left /= No_Element or else raise Constraint_Error,
Global => in all;
**A.18.8** The Generic Package Containers.Hashed_Sets

```ada
{AI12-0112-1} function Equivalent_Elements (Left : Element_Type;
                                           Right : Cursor)
    return Boolean
    with Pre => Right /= No_Element or else raise Constraint_Error,
        Global => in all;
{AI12-0112-1} procedure Iterate
                (Container : in Set;
                 Process   : not null access procedure (Position : in Cursor))
    with Allows Exit;
{AI05-0212-1} {AI12-0112-1} {AI12-0266-1} function Iterate (Container : in Set)
    return Set_Iterator.Interfaces.Parallel_IteratorForward_Iterator'Class
    with Post => Tampering_With_Cursors_Prohibited (Container);
{AI12-0112-1} generic
    type Key_Type (<>) is private
    with function Key (Element : Element_Type)
              return Key_Type;
    with function Hash (Key : Key_Type)
           return Hash_Type;
    with function Equivalent_Keys (Left, Right : Key_Type)
          return Boolean;
package Generic_Keys
    with Nonblocking, Global => null is
{AI12-0112-1} function Key (Position : Cursor)
     return Key_Type
     with Pre => Position /= No_Element or else raise Constraint_Error,
         Global => in all;
{AI12-0112-1} function Key (Container : Set;
                               Position : Cursor)
     return Key_Type
     with Pre => (Position = No_Element
                               or else raise Constraint_Error) and then
                               (Has_Element (Container, Position)
                               or else raise Program_Error);
function Element (Container : Set;
                  Key       : Key_Type)
     return Element_Type;
procedure Replace (Container : in out Set;
                  Key       : in   Key_Type;
                  New_Item  : in   Element_Type)
     with Pre => not Tampering_With_Cursors_Prohibited (Container)
                 or else raise Program_Error,
                 Post => Length (Container) = Length (Container)'Old;
procedure Exclude (Container : in out Set;
                  Key       : in   Key_Type)
     with Pre => not Tampering_With_Cursors_Prohibited (Container)
                 or else raise Program_Error,
     Post => (declare
              Original_Length : constant Count_Type :=
                              Length (Container)'Old;
              begin
                 Length (Container)
                              in Original Length - 1 | Original Length);
procedure Delete (Container : in out Set;
                  Key       : in   Key_Type)
     with Pre => not Tampering_With_Cursors_Prohibited (Container)
                 or else raise Program_Error,
     Post => Length (Container) = Length (Container)'Old - 1;
function Find (Container : Set;
               Key       : Key_Type)
     return Cursor
     with Post => (if Find'Result = No_Element
                    then Has_Element (Container, Find'Result));
function Contains (Container : Set;
                   Key       : Key_Type)
     return Boolean;
```
procedure Update_Element_Preserving_Key
(Container : in out Set;
Position : in Cursor;
Process   : not null access procedure
(Element : in out Element_Type))
with Pre => (Position /= No_Element or else
raise Constraint_Error) and then
(Has_Element (Container, Position) or else
raise Program_Error);

type Reference_Type
(Element : not null access Element_Type)
is private
with Implicit_Dereference => Element,
Nonblocking, Global => in out synchronized,
Default_Initial_Condition => (raise Program_Error);

function Reference_Preserving_Key (Container :
aliased in out Set;
Position : in Cursor)
return Reference_Type
with Pre => (Position /= No_Element
or else raise Constraint_Error) and then
(Has_Element (Container, Position)
or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container);

function Constant_Reference (Container : aliased in Set;
Key       : in Key_Type)
return Constant_Reference_Type
with Pre => Find (Container, Key) /= No_Element
or else raise Constraint_Error,
Post => Tampering_With_Cursors_Prohibited (Container);

function Reference_Preserving_Key (Container :
aliased in out Set;
Key       : in Key_Type)
return Reference_Type
with Pre => Find (Container, Key) /= No_Element
or else raise Constraint_Error,
Post => Tampering_With_Cursors_Prohibited (Container);

end Generic_Keys;

package Stable is

type Set (Base : not null access Hashed_Sets.Set) is
tagged limited private
with Constant_Indexing => Constant_Reference,
Default_Iterator => Iterate,
Iterator_Element => Element_Type,
Stable_Properties => (Length),
Global => null,
Default_Initial.Condition => Length (Set) = 0,
Preelaborable_Initialization;

type Cursor is private
with Preelaborable_Initialization;

Empty_Set : constant Set;
No_Element : constant Cursor;
function Has_Element (Position : Cursor) return Boolean
with Nonblocking, Global => in all, Use Formal => null;

package Set_Iterator_Interfaces is new
Ada.Iterator_Interfaces (Cursor, Has_Element);

procedure Assign (Target :
in out Hashed_Sets.Set;
Source : in Set)
with Post => Length (Source) = Length (Target);
function Copy (Source : Hashed_Sets.Set) return Set
with Post => Length (Copy'Result) = Length (Source);

type Constant_Reference_Type
(Element : not null access constant Element_Type) is private
with Implicit_Dereference => Element,
Nonblocking, Global => null, Use_Formal => null,
Default_Initial_Condition => raise Program_Error;

-- Additional subprograms as described in the text
are declared here.

private
... -- not specified by the language
end Stable;

end Ada.Containers.Hashed_Sets;

An object of type Set contains an expandable hash table, which is used to provide direct access to elements. The capacity of an object of type Set is the maximum number of elements that can be inserted into the hash table prior to it being automatically expanded.

Two elements E1 and E2 are defined to be equivalent if Equivalent_Elements (E1, E2) returns True.

The actual function for the generic formal function Hash is expected to return the same value each time it is called with a particular element value. For any two equivalent elements, the actual for Hash is expected to return the same value. If the actual for Hash behaves in some other manner, the behavior of this package is unspecified. Which subprograms of this package call Hash, and how many times they call it, is unspecified.

The actual function for the generic formal function Equivalent_Elements is expected to return the same value each time it is called with a particular pair of Element values. It should define an equivalence relationship, that is, be reflexive, symmetric, and transitive. If the actual for Equivalent_Elements behaves in some other manner, the behavior of this package is unspecified. Which subprograms of this package call Equivalent_Elements, and how many times they call it, is unspecified.

If the actual function for the generic formal function "=\" returns True for any pair of nonequivalent elements, then the behavior of the container function "=\" is unspecified.

If the value of an element stored in a set is changed other than by an operation in this package such that at least one of Hash or Equivalent_Elements give different results, the behavior of this package is unspecified.

Discussion: See A.18.5, “The Generic Package Containers.Hashed_Maps” for a suggested implementation, and for justification of the restrictions regarding Hash and Equivalent_Elements. Note that sets only need to store elements, not key/element pairs.

Which elements are the first element and the last element of a set, and which element is the successor of a given element, are unspecified, other than the general semantics described in A.18.7.

Returns an empty set.
function Capacity (Container : Set) return Count_Type
with Nonblocking, Global => null, Use Formal => null;

Returns the capacity of Container.

procedure Reserve Capacity (Container : in out Set;
   Capacity  : in Count_Type)
with Pre  => not Tampering With Cursors Prohibited (Container)
or else raise Program Error,
   Post => Container.Capacity >= Capacity;

Reserve Capacity allocates a new hash table such that the length of the
resulting set can become at least the value Capacity without requiring an additional call to
Reserve Capacity, and is large enough to hold the current length of Container. Reserve Capacity
then rehashes the elements in Container onto the new hash table. It replaces the old hash table
with the new hash table, and then deallocates the old hash table. Any exception raised during
allocation is propagated and Container is not modified.

This paragraph was deleted. Reserve Capacity tampers with the cursors of
Container.

Reason: Reserve Capacity tampers with the cursors, as rehashing probably will change the relationships of the
elements in Container.

procedure Clear (Container : in out Set)
with Pre  => not Tampering With Cursors Prohibited (Container)
or else raise Program Error,
   Post => Capacity (Container) = Capacity (Container)'Old and then
          Length (Container) = 0;

In addition to the semantics described in A.18.7, Clear does not affect the
capacity of Container.

procedure Assign (Target : in out Set; Source : in Set)
with Pre  => not Tampering With Cursors Prohibited (Target)
or else raise Program Error,
   Post => Length (Source) = Length (Target) and then
          Capacity (Target) >= Length (Source);

In addition to the semantics described in A.18.7, if the length of
Source is greater than the capacity of Target, Reserve Capacity (Target, Length (Source)) is
called before assigning any elements.

function Copy (Source : Set; Capacity : Count_Type := 0)
return Set
with Pre  => Capacity = 0 or else Capacity >= Length (Source)
or else raise Capacity_Error,
   Post =>
          Length (Copy'Result) = Length (Source) and then
          not Tampering With Cursors Prohibited (Copy'Result) and then
          Copy'Result.Capacity = (if Capacity = 0 then
             Length (Source) else Capacity);

Returns a set whose elements are initialized from the elements of
Source. If Capacity is 0, then the set capacity is the length of Source; if Capacity is equal to or
greater than the length of Source, the set capacity is at least the specified value. Otherwise, the
operation propagates Capacity_Error.
procedure Insert (Container : in out Set; New_Item : in Element_Type; Position : out Cursor; Inserted : out Boolean)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Original_Length : constant Count_Type :=
Length (Container)'Old;
begin
Has_Element (Container, Position) and then
(if Inserted then
Length (Container) = Original_Length + 1
else
Length (Container) = Original_Length)) and then
Capacity (Container) >= Length (Container);
{AI95-00302-03} In addition to the semantics described in A.18.7, if Length (Container) equals
Capacity (Container), then Insert first calls Reserve Capacity to increase the capacity of
Container to some larger value.

function First (Container : Set) return Cursor;
{AI95-00302-03} If Length (Container) = 0, then First returns No_Element. Otherwise, First
returns a cursor that designates the first hashed element in Container.

function Equivalent_Elements (Left, Right : Cursor) return Boolean
with Pre => (Left /= No_Element and then Right /= No_Element)
or else raise Constraint_Error,
Global => in all;
{AI95-00302-03} Equivalent to Equivalent_Elements (Element (Left), Element (Right)).

function Equivalent_Elements (Left  : Cursor; Right : Element_Type) return Boolean
with Pre => Left /= No_Element or else raise Constraint_Error,
Global => in all;
{AI95-00302-03} Equivalent to Equivalent_Elements (Element (Left), Right).

function Equivalent_Elements (Left  : Element_Type; Right : Cursor) return Boolean
with Pre => Right /= No_Element or else raise Constraint_Error,
Global => in all;
{AI95-00302-03} Equivalent to Equivalent_Elements (Left, Element (Right)).

function Iterate (Container : in Set) return Set_Iterator_Interfaces.Parallel_IteratorForward_Iterator'Class
with Post => Tampering_With_Cursors_Prohibited (Container);
{AI05-0212-1} {AI05-0265-1} {AI12-0266-1} Iterate returns an iterator object
(see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each element in
Container, starting with the first element and moving the cursor according to the successor
relation when used as a forward iterator, and processing all nodes concurrently when used as a
parallel iterator. Tampering with the cursors of Container is prohibited while the iterator object
exists (in particular, in the sequence of statements of the loop statement whose
iterator_specification denotes this object). The iterator object needs finalization.

{AI95-00302-03} For any element E, the actual function for the generic formal function
Generic_Keys.Hash is expected to be such that Hash (E) = Generic_Keys.Hash (Key (E)). If the actuals
for Key or Generic_Keys.Hash behave in some other manner, the behavior of Generic_Keys is unspecified. Which subprograms of Generic_Keys call Generic_Keys.Hash, and how many times they call it, is unspecified.

{AI95-00302-03} For any two elements \( E_1 \) and \( E_2 \), the boolean values Equivalent_Elements \((E_1, E_2)\) and Equivalent_Keys \((\text{Key} (E_1), \text{Key} (E_2))\) are expected to be equal. If the actuals for Key or Equivalent_Keys behave in some other manner, the behavior of Generic_Keys is unspecified. Which subprograms of Generic_Keys call Equivalent_Keys, and how many times they call it, is unspecified.

**Implementation Advice**

{AI95-00302-03} If \( N \) is the length of a set, the average time complexity of the subprograms Insert, Include, Replace, Delete, Exclude, and Find that take an element parameter should be \( O(\log N) \). The average time complexity of the subprograms that take a cursor parameter should be \( O(1) \). The average time complexity of Reserve_Capacity should be \( O(N) \).

**Implementation Note:** {AI95-00302-03} See A.18.5, “The Generic Package Containers.Hashed_Maps” for implementation notes regarding some of the operations of this package.

**Extensions to Ada 95**

{AI95-00302-03} The generic package Containers.Hashed_Sets is new.

**Incompatibilities With Ada 2005**

{AI05-0001-1} Subprograms Assign and Copy are added to Containers.Hashed_Sets. If an instance of Containers.Hashed_Sets is referenced in a use_clause, and an entity \( E \) with the same defining_identifier as a new entity in Containers.Hashed_Sets is defined in a package that is also referenced in a use_clause, the entity \( E \) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

**Extensions to Ada 2005**

{AI05-0212-1} Added iterator and indexing support to make hashed set containers more convenient to use.

**Wording Changes from Ada 2005**

{AI05-0044-1} Correction: Added wording to require the formal function be such that equal elements are also equivalent.

{AI05-0084-1} Correction: Added a pragma Remote_Types so that containers can be used in distributed programs.

**Incompatibilities With Ada 2012**

\{AI12-0111-1\} \{AI12-0112-1\} \{AI12-0339-1\} A number of new subprograms, types, and even a nested package were added to Containers.Hashed_Sets to better support contracts and stable views. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

**Extensions to Ada 2012**

{AI12-0212-1} Sets now support positional container aggregates, so aggregate syntax can be used to create Sets.

{AI12-0266-1} The iterator for the container now can return a parallel iterator which can be used to process the container in parallel.

**Wording Changes from Ada 2012**

{AI12-0112-1} Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).
A.18.9 The Generic Package Containers.Ordered_Sets

Static Semantics

The generic library package Containers.Ordered_Sets has the following declaration:

```ada
generic
  type Element_Type is private;
  with function "<" (Left, Right : Element_Type) return Boolean is <>;
  with function "=" (Left, Right : Element_Type) return Boolean is <>;

package Ada.Containers.Ordered_Sets is
  with Preelaborate, Remote_Types, Nonblocking, Global => in out synchronized is
    pragma Preelaborate(Ordered_Sets);
    pragma Remote_Types(Ordered_Sets);
  pragma Preelaborable_Initialization(Ordered_Sets);

    function Equivalent_Elements (Left, Right : Element_Type) return Boolean;

    type Set is tagged private
      with Constant_Indexing => Constant_Reference,
      Default_Initial_Condition =>
        Length (Set) = 0 and then
        not Tampering_With_Cursors_Prohibited (Set),
      pragma Preelaborable_Initialization(Set);

    type Cursor is private
      with pragma Preelaborable_Initialization(Cursor);

    Empty_Set : constant Set;
    No_Element : constant Cursor;

    function Has_Element (Position : Cursor) return Boolean
      with Nonblocking, Global => in all, Use_Formal => null;

    function Has_Element (Container : Set; Position : Cursor) return Boolean
      with Nonblocking, Global => null, Use_Formal => null;

    function "=" (Left, Right : Set) return Boolean;
    function Equivalent_Sets (Left, Right : Set) return Boolean;

    function Tampering_With_Cursors_Prohibited
      (Container : Set) return Boolean
      with Nonblocking, Global => null, Use_Formal => null;

    function To_Set (New_Item : Element_Type) return Set
      is (Empty_Set)
      with Post =>
        not Tampering_With_Cursors_Prohibited (Empty'Result) and then
        Length (Empty'Result) = 0;

    function To_Set (New_Item : Element_Type) return Set
      with Post => Length (To_Set'Result) = 1 and then
        not Tampering_With_Cursors_Prohibited (To_Set'Result);
```

Discussion: For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).
function Length (Container : Set) return Count_Type
  with Nonblocking, Global => null, Use Formal => null;

function Is_Empty (Container : Set) return Boolean
  with Nonblocking, Global => null, Use Formal => null,
      Post => Is_Empty'Result = (Length (Container) = 0);

procedure Clear (Container : in out Set)
  with Pre => not Tampering With Cursors Prohibited (Container)
      or else raise Program_Error,
      Post => Length (Container) = 0;

function Element (Position : Cursor) return Element_Type
  with Pre => Position /= No_Element or else raise Constraint_Error,
      Nonblocking, Global => in all, Use Formal => Element_Type;

function Element (Container : Set; Position : Cursor) return Element_Type
  with Pre => (Position /= No_Element or else raise Constraint_Error)
      and then (Has_Element (Container, Position)
          or else raise Program_Error),
      Nonblocking, Global => null, Use Formal => Element_Type;

procedure Replace_Element (Container : in out Set; Position : in Cursor;
    New_item : in Element_Type)
  with Pre => (not Tampering With Cursors Prohibited (Container)
      or else raise Program_Error)
      and then (Position /= No_Element
          or else raise Constraint_Error) and then
      (Has_Element (Container, Position)
          or else raise Program_Error);

procedure Query_Element (Position : in Cursor;
    Process : not null access procedure (Element : in Element_Type))
  with Pre => Position /= No_Element
      or else raise Constraint_Error,
      Global => in all;

procedure Query_Element (Container : in Set; Position : in Cursor;
    Process : not null access procedure (Element : in Element_Type))
  with Pre => (Position /= No_Element or else raise Constraint_Error)
      and then (Has_Element (Container, Position)
          or else raise Program_Error);

type Constant_Reference_Type
  is private
  with Implicit Dereference => Element,
      Nonblocking, Global => in out synchronized,
      Default Initial Condition => (raise Program_Error);

function Constant_Reference (Container : aliased in Set;
    Position : in Cursor)
  return Constant_Reference_Type
  with Pre => (Position /= No_Element or else raise Constraint_Error)
      and then (Has_Element (Container, Position)
          or else raise Program_Error),
      Post => Tampering With Cursors Prohibited (Container),
      Nonblocking, Global => null, Use Formal => null;

procedure Assign (Target : in out Set; Source : in Set)
  with Pre => not Tampering With Cursors Prohibited (Target)
      or else raise Program_Error,
      Post => Length (Source) = Length (Target);
function Copy (Source : Set) return Set
with Post => Length (Copy'Result) = Length (Source) and then
not Tampering With Cursors Prohibited (Copy'Result);

procedure Move (Target : in out Set;
Source : in out Set)
with Pre => (not Tampering With Cursors Prohibited (Target)
or else raise Program Error) and then
(not Tampering With Cursors Prohibited (Source)
or else raise Program Error),
Post => (if not Target'Has_Same_Storage (Source) then
Length (Target) = Length (Source'Old) and then
Length (Source) = 0);

procedure Insert (Container : in out Set;
New_Item  : in Element_Type;
Position  : out Cursor;
Inserted  : out Boolean)
with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Original_Length : constant Count_Type :=
Length (Container)'Old;
begin
Has_Element (Container, Position) and then
(if Inserted then
Length (Container) = Original_Length + 1
else
Length (Container) = Original_Length));

procedure Insert (Container : in out Set;
New_Item  : in Element_Type)
with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => Length (Container) = Length (Container)'Old + 1;

procedure Include (Container : in out Set;
New_Item  : in Element_Type)
with Pre => (not Tampering With Cursors Prohibited (Container)
or else raise Program Error) and then
(Length (Container) <= Count_Type'Last - 1
or else raise Constraint_Error),
Post => (declare
Original_Length : constant Count_Type :=
Length (Container)'Old;
begin
Length (Container) in Original_Length | Original_Length + 1);

procedure Replace (Container : in out Set;
New_Item  : in Element_Type)
with Pre => not Tampering With Cursors Prohibited (Container)
or else raise Program Error,
Post => Length (Container) = Length (Container)'Old;

procedure Exclude (Container : in out Set;
Item      : in Element_Type)
with Pre => not Tampering With Cursors Prohibited (Container)
or else raise Program Error,
Post => (declare
Original_Length : constant Count_Type :=
Length (Container)'Old;
begin
Length (Container) in Original_Length - 1 | Original_Length);
procedure Delete (Container : in out Set; Item : in Element_Type)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => Length (Container) = Length (Container)'Old - 1;

procedure Delete (Container : in out Set; Position : in out Cursor)
with Pre => (Position /= No_Element
or else raise Constraint_Error) and then
(Has_Element (Container, Position)
or else raise Program_Error),
Post => Length (Container) = Length (Container)'Old - 1 and then
Position = No_Element;

procedure Delete_First (Container : in out Set)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => (declare
Original_Length : constant Count_Type :=
Length (Container)'Old;
begind (if Original_Length = 0 then Length (Container) = 0
else Length (Container) = Original_Length - 1));

procedure Delete_Last (Container : in out Set)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error,
Post => (declare
Original_Length : constant Count_Type :=
Length (Container)'Old;
begind (if Original_Length = 0 then Length (Container) = 0
else Length (Container) = Original_Length - 1));

procedure Union (Target : in out Set; Source : in Set)
with Pre => not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error,
Post => Length (Target) <= Length (Target)'Old + Length (Source);
function Union (Left, Right : Set) return Set
with Post => Length (Union'Result) <=
Length (Left) + Length (Right) and then
not Tampering_With_Cursors_Prohibited (Union'Result);
function "or" (Left, Right : Set) return Set renames Union;

procedure Intersection (Target : in out Set; Source : in Set)
with Pre => not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error,
Post => Length (Target) <= Length (Target)'Old + Length (Source);
function Intersection (Left, Right : Set) return Set
with Post =>
(declare
Length (Intersection'Result) <=
Length (Left) + Length (Right) and then
not Tampering_With_Cursors_Prohibited (Intersection'Result);
function "and" (Left, Right : Set) return Set renames Intersection;

procedure Difference (Target : in out Set; Source : in Set)
with Pre => not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error,
Post => Length (Target) <= Length (Target)'Old + Length (Source);
function Difference (Left, Right : Set) return Set
with Post =>
    Length (Difference'Result) <=
    Length (Left) + Length (Right) and then
    not Tampering_With_Cursors_Prohibited (Difference'Result);

function "-" (Left, Right : Set) return Set renames Difference;

procedure Symmetric Difference (Target : in out Set; Source : in Set)
with Pre =>
    not Tampering_With_Cursors_Prohibited (Target)
    or else raise Program_Error,
    Post =>
        Length (Target) <= Length (Target)'Old + Length (Source);

function Symmetric Difference (Left, Right : Set) return Set
with Post =>
    Length (Symmetric Difference'Result) <=
    Length (Left) + Length (Right) and then
    not Tampering_With_Cursors_Prohibited (Symmetric Difference'Result);

function "xor" (Left, Right : Set) return Set renames Symmetric Difference;

function Overlap (Left, Right : Set) return Boolean;

function Is_Subset (Subset : Set; Of_Set : Set) return Boolean;

function First (Container : Set) return Cursor
with Nonblocking, Global => null, Use Formal => null,
    Post => (if not Is_Empty (Container)
        then Has_Element (Container, First'Result)
        else First'Result = No_Element);

function First_Element (Container : Set) return Element_Type
with Pre => (not Is_Empty (Container)
    or else raise Constraint_Error);

function Last (Container : Set) return Cursor
with Nonblocking, Global => null, Use Formal => null,
    Post => (if not Is_Empty (Container)
        then Has_Element (Container, Last'Result)
        else Last'Result = No_Element);

function Last_Element (Container : Set) return Element_Type
with Pre => (not Is_Empty (Container)
    or else raise Constraint_Error);

function Next (Position : Cursor) return Cursor
with Nonblocking, Global => in all, Use Formal => null,
    Post => (if Position = No_Element then Next'Result = No_Element);

function Next (Container : Set; Position : Cursor) return Cursor
with Nonblocking, Global => null, Use Formal => null,
    Pre => Position = No_Element or else
        Has_Element (Container, Position)
    or else raise Program_Error,
    Post =>
        (if Position = No_Element then Next'Result = No_Element
            elsif Next'Result = No_Element then
                Position = Last (Container)
            else Has_Element (Container, Next'Result));

procedure Next (Position : in out Cursor)
with Nonblocking, Global => in all, Use Formal => null;
procedure Next (Container : in Set;
    Position : in out Cursor);
    with Nonblocking, Global => null,
    Pre => Position = No Element or else Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Position /= No Element
    then Has Element (Container, Position));

function Previous (Position : Cursor) return Cursor
    with Nonblocking, Global => in all,
    Post => (if Position = No_Element then
    Previous'Result = No_Element);

function Previous (Container : Set;
    Position  : Cursor) return Cursor
    with Nonblocking, Global => null,
    Pre => Position = No Element or else Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Position /= No Element
    then Has Element (Container, Previous'Result));

procedure Previous (Position :
    in out Cursor)
    with Nonblocking, Global => in all,
    Use Formal => null;

procedure Previous (Container :
    in Set;
    Position  : in out Cursor)
    with Nonblocking, Global => null,
    Pre => Position = No Element or else Has Element (Container, Position)
    or else raise Program_Error,
    Post => (if Position /= No Element
    then Has Element (Container, Position));

function Find (Container : Set;
    Item      : Element_Type) return Cursor
    with Post => (if Find'Result /= No_Element
    then Has Element (Container, Find'Result));

function Floor (Container : Set;
    Item      : Element_Type) return Cursor
    with Post => (if Floor'Result /= No_Element
    then Has Element (Container, Floor'Result));

function Ceiling (Container : Set;
    Item      : Element_Type) return Cursor
    with Post => (if Ceiling'Result /= No_Element
    then Has Element (Container, Ceiling'Result));

function Contains (Container : Set;
    Item      : Element_Type) return Boolean;

This paragraph was deleted.

function "<" (Left, Right : Cursor) return Boolean
    with Pre => (Left /= No Element and then Right /= No Element)
    or else raise Constraint_Error,
    Global => in all;

function ">" (Left, Right : Cursor) return Boolean
    with Pre => (Left /= No Element and then Right /= No_Element)
    or else raise Constraint_Error,
    Global => in all;

function "<" (Left : Cursor; Right : Element_Type) return Boolean
    with Pre => Left /= No_Element or else raise Constraint_Error,
    Global => in all;
function ">" (Left : Cursor; Right : Element_Type) return Boolean
with Pre => Left /= No_Element or else raise Constraint_Error,
          Global => in all;

function "<" (Left : Element_Type; Right : Cursor) return Boolean
with Pre => Right /= No_Element or else raise Constraint_Error,
          Global => in all;

function ">" (Left : Element_Type; Right : Cursor) return Boolean
with Pre => Right /= No_Element or else raise Constraint_Error,
          Global => in all;

procedure Iterate
(Container : in Set;
Process   : not null access procedure (Position : in Cursor))
with Allows Exit;

procedure Reverse_Iterate
(Container : in Set;
Process   : not null access procedure (Position : in Cursor))
with Allows Exit;

function Iterate (Container : in Set) return Set_Iterator_Interfaces.Parallel_Reversible_Iterator'Reversible_Iterator'Class
with Post => Tampering_With_Cursors_Prohibited (Container);

function Iterate (Container : in Set; Start : in Cursor)
return Set_Iterator_Interfaces.Reversible_Iterator'Class
with Pre  => (Start /= No_Element or else raise Constraint_Error) and then
       (Has_Element (Container, Start) or else raise Program_Error),
       Post => Tampering_With_Cursors_Prohibited (Container);

generic
   type Key_Type (<>) is private;
   with function Key (Element : Element_Type) return Key_Type;
   with function ">" (Left, Right : Key_Type) return Boolean is <>;
package Generic_Keys
   with Nonblocking, Global => null is
       function Equivalent_Keys (Left, Right : Key_Type)
        return Boolean;

function Key (Position : Cursor) return Key_Type
with Pre => Position /= No_Element or else raise Constraint_Error,
       Global => in all;

function Key (Container : Set; Position : Cursor) return Key_Type
with Pre => (Position /= No_Element or else raise Constraint_Error) and then
       (Has_Element (Container, Position) or else raise Program_Error);

function Element (Container : Set; Key : Key_Type)
return Element_Type;

procedure Replace (Container : in out Set;
                   Key       : in Key_Type;
                   New_Item  : in Element_Type)
with Pre => not Tampering_With_Cursors_Prohibited (Container)
       or else raise Program_Error,
       Post => Length (Container) = Length (Container)'Old;
procedure Exclude (Container : in out Set; 
                  Key : in Key_Type); 
with Pre => not Tampering_With_Cursors_Prohibited (Container) 
    or else raise Program_Error, 
Post => (declare 
______________
begin 
______________
Length (Container) in 
______________
Original Length - 1 | Original Length); 
procedure Delete (Container : in out Set; 
                 Key : in Key_Type); 
with Pre => not Tampering_With_Cursors_Prohibited (Container) 
    or else raise Program_Error, 
Post => Length (Container) = Length (Container)'Old - 1; 
function Find (Container : Set; 
              Key : Key_Type) return Cursor; 
with Post => (if Find'Result /= No_Element 
______________
then Has_Element (Container, Find'Result)); 
function Floor (Container : Set; 
               Key : Key_Type) return Cursor; 
with Post => (if Floor'Result /= No_Element 
______________
then Has_Element (Container, Floor'Result)); 
function Ceiling (Container : Set; 
                 Key : Key_Type) return Cursor; 
with Post => (if Ceiling'Result /= No_Element 
______________
then Has_Element (Container, Ceiling'Result)); 
function Contains (Container : Set; 
                   Key : Key_Type) return Boolean; 
procedure Update_Element_Preserving_Key 
    (Container : in out Set; 
     Position : in Cursor; 
     Process : not null access procedure 
______________
(Element : in out Element_Type)); 
with Pre => (Position /= No_Element 
______________
or else raise Constraint_Error) and then 
______________
(Has Element (Container, Position) 
______________
or else raise Program_Error); 
function Reference_Preserving_Key (Container : aliased in out Set; 
                                    Position : in Cursor) return Reference_Type; 
with Pre => (Position /= No_Element 
______________
or else raise Constraint_Error) and then 
______________
(Has Element (Container, Position) 
______________
or else raise Program_Error), 
Post => Tampering_With_Cursors_Prohibited (Container); 
function Constant_Reference (Container : aliased in Set; 
                             Key : in Key_Type) return Constant_Reference_Type; 
with Pre => Find (Container, Key) /= No_Element 
______________
or else raise Constraint_Error, 
Post => Tampering_With_Cursors_Prohibited (Container);
function Reference_Preserving_Key (Container : aliased in out Set; Key : in Key_Type)
return Reference_Type
with Pre => Find (Container, Key) /= No_Element
or else raise Constraint_Error,
Post => Tampering_With_Cursors_Prohibited (Container);
end Generic_Keys;

package Stable is

type Set (Base : not null access Ordered_Sets.Set) is
tagged limited private
with Constant_Indexing => Constant_Reference,
Default_Iterator => Iterate,
Iterator_Element => Element_Type,
Stable_Properties => (Length),
Global => null,
Default_Initial_Condition => Length (Set) = 0,
Preelaborable_Initialization;

type Cursor is private
with Preelaborable_Initialization;

Empty_Set : constant Set;
No_Element : constant Cursor;

function Has_Element (Position : Cursor) return Boolean
with Nonblocking, Global => in all, Use_Formal => null;

package Set_Iterator_Interfaces is new Ada.Iterator_Interfaces (Cursor, Has_Element);

procedure Assign (Target : in out Ordered_Sets.Set; Source : in Set)
with Post => Length (Source) = Length (Target);

function Copy (Source : Ordered_Sets.Set) return Set
with Post => Length (Copy'Result) = Length (Source);

type Constant_Reference_Type (Element : not null access constant Element_Type) is private
with Implicit_Dereference => Element,
Nonblocking, Global => null, Use_Formal => null,
Default_Initial Condition => raise Program_Error;

-- Additional subprograms as described in the text
-- are declared here.

private
... -- not specified by the language

end Stable;
private
... -- not specified by the language
end Ada.Containers.Ordered_Sets;

Two elements E1 and E2 are equivalent if both E1 < E2 and E2 < E1 return False, using the generic formal "<" operator for elements. Function Equivalent_Elements returns True if Left and Right are equivalent, and False otherwise.

The actual function for the generic formal function "<" on Element_Type values is expected to return the same value each time it is called with a particular pair of key values. It should define a strict weak ordering relationship (see A.18), that is, be irreflexive, asymmetric, and transitive. If the actual for "<" behaves in some other manner, the behavior of this
package is unspecified. Which subprograms of this package call "<" and how many times they call it, is unspecified.

{AI05-0044-1} If the actual function for the generic formal function "=" returns True for any pair of nonequivalent elements, then the behavior of the container function "=" is unspecified.

{AI95-00302-03} If the value of an element stored in a set is changed other than by an operation in this package such that at least one of "<" or "=" give different results, the behavior of this package is unspecified.

Discussion: See A.18.6, “The Generic Package Containers.Ordered_Maps” for a suggested implementation, and for justification of the restrictions regarding "<" and "=". Note that sets only need to store elements, not key/element pairs.

{AI95-00302-03} {AI05-0262-1} The first element_of a nonempty set is the one which is less than all the other elements in the set. The last element_of a nonempty set is the one which is greater than all the other elements in the set. The successor_of an element is the smallest element that is larger than the given element. The predecessor_of an element is the largest element that is smaller than the given element. All comparisons are done using the generic formal ",<" operator for elements.

{AI12-0112-1} function Copy (Source : Set) return Set
with Post = Length (Copy'Result) = Length (Source) and then not Tampering With Cursors Prohibited (Copy'Result);

{AI05-0001-1} Returns a set whose elements are initialized from the corresponding elements of Source.

{AI12-0112-1} procedure Delete First (Container : in out Set)
with Pre = not Tampering With Cursors Prohibited (Container)
or else raise Program_Error,
Post => (declare
Original Length : constant Count_Type := Length (Container)'Old;
beginn
(if Original Length = 0 then Length (Container) = 0
else Length (Container) = Original Length - 1));

{AI95-00302-03} {AI05-0264-1} If Container is empty, Delete First has no effect. Otherwise, the element designated by First (Container) is removed from Container. Delete First tampers with the cursors of Container.

{AI12-0112-1} procedure Delete Last (Container : in out Set)
with Pre = not Tampering With Cursors Prohibited (Container)
or else raise Program_Error,
Post => (declare
Original Length : constant Count_Type := Length (Container)'Old;
beginn
(if Original Length = 0 then Length (Container) = 0
else Length (Container) = Original Length - 1));

{AI95-00302-03} {AI05-0264-1} If Container is empty, Delete Last has no effect. Otherwise, the element designated by Last (Container) is removed from Container. Delete Last tampers with the cursors of Container.

{AI12-0112-1} function First Element (Container : Set) return Element_Type
with Pre = (not Is Empty (Container)
or else raise Constraint_Error);

{AI95-00302-03} Equivalent to Element (First (Container)).
function Last (Container : Set) return Cursor
    with Nonblocking, Global => null, Use Formal => null,
    Post => (if not Is_Empty (Container) then
                Has_Element (Container, Last'Result)
              else Last'Result = No_Element);

Returns a cursor that designates the last element in Container. If Container is empty, returns No_Element.

function Last_Element (Container : Set) return Element_Type
    with Pre => (not Is_Empty (Container)
              or else raise Constraint_Error);

Equivalent to Element (Last (Container)).

function Previous (Position : Cursor) return Cursor
    with Nonblocking, Global => in all, Use Formal => null,
    Post => (if Position = No_Element then
               Previous'Result = No_Element
             elsif Previous'Result = No_Element then
               Position = First (Container)
             else Has_Element (Container, Previous'Result));

If Position equals No_Element, then Previous returns No_Element. Otherwise, Previous returns a cursor designating the predecessor element of that precedes the one designated by Position. If Position designates the first element, then Previous returns No_Element.

function Previous (Container : Set; Position : Cursor) return Cursor
    with Nonblocking, Global => null, Use Formal => null,
    Pre  => Position = No_Element or else Has_Element (Container, Position)
          or else raise Program_Error,
    Post => (if Position /= No_Element
              then Has_Element (Container, Position)
              elsif Previous'Result = No_Element then
               Position = First (Container)
              else Has_Element (Container, Previous'Result));

Returns a cursor designating the predecessor of the node designated by Position in Container, if any.

procedure Previous (Position : in out Cursor)
    with Nonblocking, Global => in all, Use Formal => null;

Equivalent to Position := Previous (Position).

procedure Previous (Container : in Set; Position : in out Cursor)
    with Nonblocking, Global => null, Use Formal => null,
    Pre  => Position = No_Element or else Has_Element (Container, Position)
          or else raise Program_Error,
    Post => (if Position /= No_Element
              then Has_Element (Container, Position)));

Equivalent to Position := Previous (Container, Position).

function Floor (Container : Set; Item : Element_Type) return Cursor
    with Post => (if Floor'Result /= No_Element
              then Has_Element (Container, Floor'Result));

Floor searches for the last element which is not greater than Item. If such an element is found, a cursor that designates it is returned. Otherwise, No_Element is returned.
function Ceiling (Container : Set; Item : Element_Type) return Cursor
    with Post => (if Ceiling'Result /= No_Element
                    then Has_Element (Container, Ceiling'Result));

function "<" (Left, Right : Cursor) return Boolean
    with Pre    => (Left /= No_Element and then Right /= No_Element)
                or else raise Constraint_Error,
    Global => in all;

function ">" (Left, Right : Cursor) return Boolean
    with Pre    => (Left /= No_Element and then Right /= No_Element)
                or else raise Constraint_Error,
    Global => in all;

function "<" (Left : Cursor; Right : Element_Type) return Boolean
    with Pre    => Left /= No_Element or else raise Constraint_Error,
    Global => in all;

function ">" (Left : Cursor; Right : Element_Type) return Boolean
    with Pre    => Left /= No_Element or else raise Constraint_Error,
    Global => in all;

function ">" (Left : Element_Type; Right : Cursor) return Boolean
    with Pre    => Right /= No_Element or else raise Constraint_Error,
    Global => in all;

function ">" (Left : Element_Type; Right : Cursor) return Boolean
    with Pre    => Right /= No_Element or else raise Constraint_Error,
    Global => in all;

procedure Reverse_Iterate (Container : in Set;
                           Process   : not null access procedure (Position : in Cursor))
    with Allows Exit;

function Iterate (Container : in Set)
    return Set_Iterator_Interfaces.Parallel_Reversible_Iterator
            Reversible_Iterator'Class
    with Post => Tampering_With_Cursors_Prohibited (Container);

Iterate returns an reversible iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each element in Container, starting with the first element and moving the cursor according to the successor relation when used as a forward iterator, and starting with the last element and moving the cursor according to the predecessor relation when used as a reverse iterator, and processing all
nodes concurrently when used as a parallel iterator. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop statement whose iterator specification denotes this object). The iterator object needs finalization.

```ada
function Iterate (Container : in Set; Start : in Cursor)
return Set_Iterator_Interfaces.Reversible_Iterator'Class
with Pre => (Start /= No_Element
or else raise Constraint_Error) and then
(Has_Element (Container, Start)
or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container);
```

{AI05-0262-1} {AI05-0265-1} {AI05-0269-1} {AI12-0112-1} If Start is not No_Element and does not designate an item in Container, then Program_Error is propagated. If Start is No_Element, then Constraint_Error is propagated. Otherwise, Iterate returns a reversible iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each element in Container, starting with the element designated by Start and moving the cursor according to the successor relation when used as a forward iterator, or moving the cursor according to the predecessor relation when used as a reverse iterator. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop statement whose iterator specification denotes this object). The iterator object needs finalization.

Discussion: Exits are allowed from the loops created using the iterator objects. In particular, to stop the iteration at a particular cursor, just add

```ada
exit when Cur = Stop;
```

in the body of the loop (assuming that Cur is the loop parameter and Stop is the cursor that you want to stop at).

{AI95-00302-03} For any two elements $E1$ and $E2$, the boolean values ($E1 < E2$) and (Key($E1$) < Key($E2$)) are expected to be equal. If the actuals for Key or Generic_Keys."<" behave in some other manner, the behavior of this package is unspecified. Which subprograms of this package call Key and Generic_Keys."<", and how many times the functions are called, is unspecified.

{AI95-00302-03} In addition to the semantics described in A.18.7, the subprograms in package Generic_Keys named Floor and Ceiling, are equivalent to the corresponding subprograms in the parent package, with the difference that the Key subprogram parameter is compared to elements in the container using the Key and "<" generic formal functions. The function named Equivalent_Keys in package Generic_Keys returns True if both Left < Right and Right < Left return False using the generic formal "<" operator, and returns True otherwise.

Implementation Advice

{AI95-00302-03} If $N$ is the length of a set, then the worst-case time complexity of the Insert, Include, Replace, Delete, Exclude, and Find operations that take an element parameter should be $O((\log N)^2)$ or better. The worst-case time complexity of the subprograms that take a cursor parameter should be $O(1)$.

Implementation Advice: The worst-case time complexity of the Insert, Include, Replace, Delete, Exclude, and Find operations of Containers.Ordered_Sets that take an element parameter should be $O((\log N)^2)$. The worst-case time complexity of the subprograms of Containers.Ordered_Sets that take a cursor parameter should be $O(1)$.

Implementation Note: {AI95-00302-03} See A.18.6, “The Generic Package Containers.Ordered_Maps” for implementation notes regarding some of the operations of this package.

Extensions to Ada 95

{AI95-00302-03} The generic package Containers.Ordered_Sets is new.
Incompatibilities With Ada 2005

{AI05-0001-1} Subprograms Assign and Copy are added to Containers.Ordered_Sets. If an instance of Containers.Ordered_Sets is referenced in a use_clause, and an entity \( E \) with the same defining_identifier as a new entity in Containers.Ordered_Sets is defined in a package that is also referenced in a use_clause, the entity \( E \) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 2005

{AI05-0212-1} Added iterator and indexing support to make ordered set containers more convenient to use.

Wording Changes from Ada 2005

{AI05-0044-1} Correction: Added wording to require the formal function be such that equal elements are also equivalent.

{AI05-0044-1} Correction: Redefined "<" actuals to require a strict weak ordering; the old definition allowed indeterminant comparisons that would not have worked in a container.

{AI05-0084-1} Correction: Added a pragma Remote_Types so that containers can be used in distributed programs.

Incompatibilities With Ada 2012

{AI12-0111-1} {AI12-0112-1} A number of new subprograms, types, and even a nested package were added to Containers.Ordered_Sets to better support contracts and stable views. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

Extensions to Ada 2012

{AI12-0212-1} Sets now support positional container aggregates, so aggregate syntax can be used to create Sets.

{AI12-0266-1} The iterator for the entire container now can return a parallel iterator which can be used to process the container in parallel.

Wording Changes from Ada 2012

{AI12-0112-1} Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).

A.18.10 The Generic Package Containers.Multiway_Trees

{AI05-0136-1} The language-defined generic package Containers.Multiway_Trees provides private types Tree and Cursor, and a set of operations for each type. A multiway tree container is well-suited to represent nested structures.

Discussion: {AI05-0136-1} This tree just provides a basic structure, and make no promises about balancing or other automatic organization. In this sense, it is different than the indexed (Map, Set) forms. Rather, it provides a building block on which to construct more complex and more specialized tree containers.

{AI05-0136-1} A multiway tree container object manages a tree of internal nodes, consisting of a root node and a set of internal nodes; each internal node of which contains an element and pointers to the parent, first child, last child, next (successor) sibling, and previous (predecessor) sibling internal nodes. A cursor designates a particular node within a tree (and by extension the element contained in that node, if any). A cursor keeps designating the same node (and element) as long as the node is part of the container, even if the node is moved within the container.

{AI05-0136-1} A subtree is a particular node (which roots the subtree) and all of its child nodes (including all of the children of the child nodes, recursively). The root node. There is a special node, the root, which is always present and has neither an associated element value nor any parent node; it has pointers to its first child and its last child, if any. The root node provides a place to add nodes to an otherwise empty tree and represents the base of the tree.

{AI05-0136-1} A node that has no children is called a leaf node. The ancestors of a node are the node itself, its parent node, the parent of the parent node, and so on until a node with no parent is
reached. Similarly, the descendants of a node are the node itself, its child nodes, the children of each child node, and so on.

The nodes of a subtree can be visited in several different orders. For a depth-first order, after visiting a node, the nodes of its child list are each visited in depth-first order, with each child node visited in natural order (first child to last child).

Ramification: For the depth-first order, when each child node is visited, the child list of the child node is visited before the next sibling of the child node is visited.

Static Semantics

The generic library package Containers.Multiway_Trees has the following declaration:

```ada
package Ada.Containers.Multiway_Trees is
  --body
end Containers.Multiway_Trees;
```

Discussion: For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).

```ada
package Tree_Iterator_Interfaces is new Ada.Iterator_Interfaces (Cursor, Has_Element);
```

```ada
function Equal_Subtree (Left_Position : Cursor; Right_Position : Cursor) return Boolean;
function "=" (Left, Right : Tree) return Boolean;
function Tampering_With_Cursors_Prohibited (Container : Tree) return Boolean;
```

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
Empty_Tree : constant Tree;
No_Element : constant Cursor;
```

```ada
function Equal_Element (Left, Right : Element_Type) return Boolean
renames "=";
function Has_Element (Position : Cursor) return Boolean;
function Has_Element (Container : Tree; Position : Cursor) return Boolean;
```

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
function Tampering_With_Cursors_Prohibited (Container : Tree) return Boolean;
```

```ada
with Ada.Iterator_Interfaces;
generic
  type Element_Type is private;
  with function "=" (Left, Right : Element_Type) return Boolean is <>;
package Ada.Containers.Multiway_Trees is
  --body
end Containers.Multiway_Trees;
```

```ada
package Ada.Iterator_Interfaces;
```

```ada
pragma Preelaborate (Multiway_Trees);
pragma Remote_Types (Multiway_Trees);
```

```ada
static Semantics
```

```ada
pragma Preelaborate (Multiway_Trees);
pragma Remote_Types (Multiway_Trees);
```

```ada
pragma Preelaborate(Multiway_Trees);
pragma Remote_Types(Multiway_Trees);
```

Discussion: For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).

```ada
pragma Preelaborable_Initialization (Tree);
```

```ada
pragma Preelaborable_Initialization (Cursor);
```

```ada
Empty_Tree : constant Tree;
No_Element : constant Cursor;
```

```ada
function Equal_Element (Left, Right : Element_Type) return Boolean
renames "=";
function Has_Element (Position : Cursor) return Boolean;
function Has_Element (Container : Tree; Position : Cursor) return Boolean;
```

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
function Tampering_With_Cursors_Prohibited (Container : Tree) return Boolean;
```

```ada
with Ada.Iterator_Interfaces;
generic
  type Element_Type is private;
  with function "=" (Left, Right : Element_Type) return Boolean is <>;
package Ada.Containers.Multiway_Trees is
  --body
end Containers.Multiway_Trees;
```

```ada
package Ada.Iterator_Interfaces;
```

```ada
pragma Preelaborate (Multiway_Trees);
pragma Remote_Types (Multiway_Trees);
```

Discussion: For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
Empty_Tree : constant Tree;
No_Element : constant Cursor;
```

```ada
function Equal_Element (Left, Right : Element_Type) return Boolean
renames "=";
function Has_Element (Position : Cursor) return Boolean;
function Has_Element (Container : Tree; Position : Cursor) return Boolean;
```

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
function Tampering_With_Cursors_Prohibited (Container : Tree) return Boolean;
```

```ada
with Ada.Iterator_Interfaces;
generic
  type Element_Type is private;
  with function "=" (Left, Right : Element_Type) return Boolean is <>;
package Ada.Containers.Multiway_Trees is
  --body
end Containers.Multiway_Trees;
```

```ada
package Ada.Iterator_Interfaces;
```

```ada
pragma Preelaborate (Multiway_Trees);
pragma Remote_Types (Multiway_Trees);
```

Discussion: For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
Empty_Tree : constant Tree;
No_Element : constant Cursor;
```

```ada
function Equal_Element (Left, Right : Element_Type) return Boolean
renames "=";
function Has_Element (Position : Cursor) return Boolean;
function Has_Element (Container : Tree; Position : Cursor) return Boolean;
```

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
function Tampering_With_Cursors_Prohibited (Container : Tree) return Boolean;
```

```ada
with Ada.Iterator_Interfaces;
generic
  type Element_Type is private;
  with function "=" (Left, Right : Element_Type) return Boolean is <>;
package Ada.Containers.Multiway_Trees is
  --body
end Containers.Multiway_Trees;
```

```ada
package Ada.Iterator_Interfaces;
```

```ada
pragma Preelaborate (Multiway_Trees);
pragma Remote_Types (Multiway_Trees);
```

Discussion: For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
Empty_Tree : constant Tree;
No_Element : constant Cursor;
```

```ada
function Equal_Element (Left, Right : Element_Type) return Boolean
renames "=";
function Has_Element (Position : Cursor) return Boolean;
function Has_Element (Container : Tree; Position : Cursor) return Boolean;
```

```ada
pragma Preelaborable_Initialization (Tree);
pragma Preelaborable_Initialization (Cursor);
```

```ada
function Tampering_With_Cursors_Prohibited (Container : Tree) return Boolean;
```
{AI12-0112-1} function Tampering_With_Elements_Prohibited
(Container : Tree) return Boolean
with Nonblocking, Global => null, Use Formal => null;

{AI12-0339-1} function Empty return Tree
is (Empty_Tree)
with Post =>
not Tampering_With_Elements_Prohibited (Empty'Result) and then
not Tampering_With_Cursors_Prohibited (Empty'Result) and then
Node_Count (Empty'Result) = 1;

{AI12-0112-1} function Is_Empty (Container : Tree)
return Boolean
with Nonblocking, Global => null, Use Formal => null,
Post => Is_Empty'Result = (Node_Count (Container) = 1);

{AI12-0112-1} function Node_Count (Container : Tree)
return Count_Type
with Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} function Subtree_Node_Count (Position : Cursor)
return Count_Type
with Nonblocking, Global => in all, Use Formal => null;

{AI12-0112-1} function Subtree_Node_Count (Container : Tree; Position : Cursor)
return Count_Type
with Pre => Meaningful_For (Container, Position)
or else raise Program_Error,
Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} function Depth (Position : Cursor)
return Count_Type
with Nonblocking, Global => in all, Use Formal => null;

{AI12-0112-1} function Depth (Container : Tree; Position : Cursor)
return Count_Type
with Pre => Meaningful_For (Container, Position)
or else raise Program_Error,
Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} function Is_Root (Position : Cursor)
return Boolean
with Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} function Is_Root (Container : Tree; Position : Cursor)
return Boolean
with Nonblocking, Global => in all, Use Formal => null;

{AI12-0112-1} function Is_Leaf (Position : Cursor)
return Boolean
with Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} function Is_Leaf (Container : Tree; Position : Cursor)
return Boolean
with Pre => Meaningful_For (Container, Position)
or else raise Program_Error,
Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} function Is_Ancestor_Of (Container : Tree;
Parent : Cursor;
Position : Cursor) return Boolean
with Pre => (Meaningful_For (Container, Position)
or else raise Program_Error) and then
(Meaningful_For (Container, Parent)
or else raise Program_Error),
Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} function Root (Container : Tree)
return Cursor
with Nonblocking, Global => null, Use Formal => null,
Post => Root'Result /= No_Element and then
not Has_Element (Container, Root'Result);

{AI12-0112-1} function Meaningful_For (Container : Tree; Position : Cursor)
return Boolean
with (Position = No_Element or else
Is_Root (Container, Position) or else
Has_Element (Container, Position))
or else raise Program_Error,
Nonblocking, Global => null, Use Formal => null;

Reason: {AI12-0112-1} When this function is true, the Position can be meaningfully used with operations for
the Container. We define this because many operations allow the root (which does not have an element, so Has Element

1105 16 October 2023 The Generic Package Containers.Multiway_Trees A.18.10
returns False), so many preconditions get unwieldy. We allow No_Element as it is allowed by many queries, and for existing routines, it raises a different exception (Constraint_Error rather than Program_Error) than a cursor for the wrong container does.

```ada
{AI12-0112-1} procedure Clear (Container : in out Tree)
  with Pre => not Tampering_With_Cursors_Prohibited (Container)
         or else raise Program_Error,
  Post => Node_Count (Container) = 1;

{AI12-0112-1} function Element (Position : Cursor) return Element_Type
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
         (Has_Element (Position) or else raise Program_Error),
  Nonblocking, Global => in all, Use Formal => Element_Type;

{AI12-0112-1} function Element (Container : Tree; Position : Cursor) return Element_Type
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
         (Has_Element (Container, Position) or else raise Program_Error),
  Nonblocking, Global => null, Use Formal => Element_Type;

{AI12-0112-1} procedure Replace_Element (Container : in out Tree; Position : in Cursor;
  New_item : in Element_Type)
  with Pre => (not Tampering_With_Elements_Prohibited (Container)
          or else raise Program_Error) and then
         (Position /= No_Element or else raise Constraint_Error) and then
         (Has_Element (Container, Position) or else raise Program_Error);

{AI12-0112-1} procedure Query_Element (Position : in Cursor;
  Process : not null access procedure (Element : in Element_Type))
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
         (Has_Element (Position) or else raise Program_Error),
  Global => in all;

{AI12-0112-1} procedure Query_Element (Container : in Tree; Position : in Cursor;
  Process : not null access procedure (Element : in Element_Type))
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
         (Has_Element (Container, Position) or else raise Program_Error);

{AI12-0112-1} procedure Update_Element (Container : in out Tree; Position : in Cursor;
  Process : not null access procedure (Element : in out Element_Type))
  with Pre => (Position /= No_Element or else raise Constraint_Error) and then
         (Has_Element (Container, Position) or else raise Program_Error);

{AI05-0212-1} {AI12-0112-1} type Constant_Reference_Type
  (Element : not null access constant Element_Type) is private
  with Implicit_Dereference => Element,
  Nonblocking, Global => in out synchronized,
  Default Initial Condition => (raise Program_Error);

{AI05-0212-1} {AI12-0112-1} type Reference_Type (Element : not null access Element_Type) is private
  with Implicit_Dereference => Element,
  Nonblocking, Global => in out synchronized,
  Default Initial Condition => (raise Program_Error);
```
function Constant_Reference (Container : aliased in Tree;
                  Position  : in Cursor)
return Constant_Reference_Type
with Pre => (Position /= No_Element
                 or else raise Constraint_Error) and then
                    (Has_Element (Container, Position)
                 or else raise Program_Error),
    Post  => Tampering_With_Cursors_Prohibited (Container),
            Nonblocking, Global => null, Use Formal => null;

function Reference (Container : aliased in out Tree;
                   Position  : in Cursor)
return Reference_Type
with Pre => (Position /= No_Element
                 or else raise Constraint_Error) and then
                    (Has_Element (Container, Position)
                 or else raise Program_Error),
    Post  => Tampering_With_Cursors_Prohibited (Container),
            Nonblocking, Global => null, Use Formal => null;

procedure Assign (Target : in out Tree; Source : in Tree)
with Pre  => not Tampering_With_Cursors_Prohibited (Target)
                  or else raise Program_Error,
    Post => Node_Count (Source) = Node_Count (Target);

function Copy (Source : Tree)
return Tree
with Post =>
            Node_Count (Copy'Result) = Node_Count (Source) and then
                  not Tampering_With_Elements_Prohibited (Copy'Result)
                  and then
                  not Tampering_With_Cursors_Prohibited (Copy'Result);

procedure Move (Target : in out Tree; Source : in out Tree)
with Pre  => (not Tampering_With_Cursors_Prohibited (Target)
                  or else raise Program_Error) and then
                  (not Tampering_With_Cursors_Prohibited (Source)
                  or else raise Program_Error),
    Post => (if not Target'Has_Same_Storage (Source) then
                  Node_Count (Target) = Node_Count (Source'Old) and then
                  Node_Count (Source) = 1);}

procedure Delete_Leaf (Container : in out Tree;
                        Position  : in out Cursor)
with Pre  => (not Tampering_With_Cursors_Prohibited (Container)
                  or else raise Program_Error) and then
                  (Position /= No_Element
                  or else raise Constraint_Error) and then
                  (Has_Element (Container, Position)
                  or else raise Program_Error) and then
                  (Is_Leaf (Container, Position)
                  or else raise Constraint_Error),
    Post  =>
            Node_Count (Container)'Old = Node_Count (Container)+1 and then
            Position = No_Element;

procedure Delete_Subtree (Container : in out Tree;
                          Position  : in out Cursor)
with Pre  => (not Tampering_With_Cursors_Prohibited (Container)
                  or else raise Program_Error) and then
                  (Position /= No_Element
                  or else raise Constraint_Error) and then
                  (Has_Element (Container, Position)
                  or else raise Program_Error),
    Post  => Node_Count (Container)'Old = Node_Count (Container) +
                  Subtree_Node_Count (Container, Position)'Old and then
            Position = No_Element;
procedure Swap (Container : in out Tree;
I, J : in Cursor);

with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error)
and then
(I /= No_Element or else Constraint_Error)
and then
(J /= No_Element or else Constraint_Error)
and then
(Has_Element (Container, I)
or else raise Program_Error)
and then
(Has_Element (Container, J)
or else raise Program_Error);

function Find (Container : Tree;
Item : Element_Type)
return Cursor
with Post => (if Find'Result /= No_Element
then Has_Element (Container, Find'Result));

function Find_In_Subtree (Position :
Cursor;
Item : Element_Type)
return Cursor
with Pre => Position /= No_Element
or else raise Constraint_Error,
Post => (if Find_In_Subtree'Result /= No_Element
then Has_Element (Find_In_Subtree'Result)),
Global => in all;

function Find_In_Subtree (Container : Tree;
Position : Cursor;
Item : Element_Type)
return Cursor
with Pre => (Position /= No_Element
or else raise Constraint_Error)
and then
(Meaningful_For (Container, Position)
or else raise Program_Error),
Post => (if Find_In_Subtree'Result /= No_Element
then Has_Element (Container, Find_In_Subtree'Result));

function Ancestor_Find (Position :
Cursor;
Item : Element_Type)
return Cursor
with Pre => Position /= No_Element
or else raise Constraint_Error,
Post => (if Ancestor_Find'Result /= No_Element
then Has_Element (Ancestor_Find'Result)),
Global => in all;

function Ancestor_Find (Container : Tree;
Position : Cursor;
Item : Element_Type)
return Cursor
with Pre => (Position /= No_Element
or else raise Constraint_Error)
and then
(Meaningful_For (Container, Position)
or else raise Program_Error),
Post => (if Ancestor_Find'Result /= No_Element
then Has_Element (Container, Ancestor_Find'Result));

function Contains (Container : Tree;
Item : Element_Type) return Boolean;

procedure Iterate
(Container : in Tree;
Process : not null access procedure (Position : in Cursor))
with Allows Exit;

procedure Iterate_Subtree
(Position : in Cursor;
Process : not null access procedure (Position : in Cursor))
with Allows Exit,
Pre => Position /= No_Element
or else raise Constraint_Error,
Global => in all;
procedure Iterate_Subtree
  (Container : in Tree;
   Position  : in Cursor;
   Process   : not null access procedure (Position : in Cursor))
with Allows Exit,
  Pre => (Position /= No_Element
   or else raise Constraint_Error) and then
  (Meaningful_For (Container, Position)
   or else raise Program_Error);

function Iterate (Container : in Tree)
return Tree_Iterator_Interfaces.Parallel_IteratorForward_Iterator'Class
with Post => Tampering_With_Cursors_Prohibited (Container);

function Iterate_Subtree (Position : in Cursor)
return Tree_Iterator_Interfaces.Parallel_IteratorForward_Iterator'Class
with Pre    => Position /= No_Element or else raise Constraint_Error,
   Global => in all;

function Iterate_Subtree (Container : Tree; Position : in Cursor)
return Tree_Iterator_Interfaces.Parallel_Iterator'Class
with Pre => (Position /= No_Element
   or else raise Constraint_Error) and then
  (Meaningful_For (Container, Position)
   or else raise Program_Error),
  Post => Tampering_With_Cursors_Prohibited (Container);

function Child_Count (Parent : Cursor) return Count_Type
with Post => (if Parent = No_Element then Child_Count'Result = 0),
   Nonblocking, Global => in all, Use Formal => null;

function Child_Count (Container : Tree; Parent : Cursor)
return Count_Type
with Pre => Meaningful_For (Container, Parent)
   or else raise Program_Error,
  Post => (if Parent = No_Element then Child_Count'Result = 0),
   Nonblocking, Global => null, Use Formal => null;

function Child_Depth (Parent, Child : Cursor) return Count_Type
with Pre => (Parent = No_Element and then Child = No_Element)
   or else raise Constraint_Error,
   Post => (if Parent = No_Element then Child_Depth'Result = 0),
   Nonblocking, Global => in all, Use Formal => null;

function Child_Depth (Container : Tree; Parent, Child : Cursor)
return Count_Type
with Pre => ((Parent = No_Element and then Child = No_Element)
   or else raise Constraint_Error) and then
  (Meaningful_For (Container, Parent)
   or else raise Program_Error) and then
  (Meaningful_For (Container, Child)
   or else raise Program_Error),
  Nonblocking, Global => null, Use Formal => null;
{AI12-0112-1} procedure Insert_Child (Container : in out Tree;
    Parent    : in   Cursor;
    Before    : in   Cursor;
    New_Item  : in   Element_Type;
    Count     : in   Count_Type := 1)
    with Pre => (not Tampering With Cursors Prohibited (Container)
      or else raise Program_Error) and then
      (Parent /= No_Element
      or else raise Constraint_Error) and then
      (Meaningful For (Container, Parent)
      or else raise Program_Error) and then
      (Meaningful For (Container, Before)
      or else raise Program_Error) and then
      (Before = No_Element or else
      Container.Parent (Before) = Parent
      or else raise Constraint_Error),
    Post => Node_Count (Container) =
            Node_Count (Container)'Old + Count;

{AI12-0112-1} procedure Insert_Child (Container : in out Tree;
    Parent    : in   Cursor;
    Before    : in   Cursor;
    New_Item  : in   Element_Type;
    Position  : out  Cursor;
    Count     : in   Count_Type := 1)
    with Pre => (not Tampering With Cursors Prohibited (Container)
      or else raise Program_Error) and then
      (Parent /= No_Element
      or else raise Constraint_Error) and then
      (Meaningful For (Container, Parent)
      or else raise Program_Error) and then
      (Meaningful For (Container, Before)
      or else raise Program_Error) and then
      (Before = No_Element or else
      Container.Parent (Before) = Parent
      or else raise Constraint_Error),
    Post => (Node_Count (Container) =
              Node_Count (Container)'Old + Count) and then
            Has_Element (Container, Position);

{AI12-0112-1} procedure Insert_Child (Container : in out Tree;
    Parent    : in   Cursor;
    Before    : in   Cursor;
    Position  : out  Cursor;
    Count     : in   Count_Type := 1)
    with Pre => (not Tampering With Cursors Prohibited (Container)
      or else raise Program_Error) and then
      (Parent /= No_Element
      or else raise Constraint_Error) and then
      (Meaningful For (Container, Parent)
      or else raise Program_Error) and then
      (Meaningful For (Container, Before)
      or else raise Program_Error) and then
      (Before = No_Element or else
      Container.Parent (Before) = Parent
      or else raise Constraint_Error),
    Post => (Node_Count (Container) =
              Node_Count (Container)'Old + Count) and then
            Has_Element (Container, Position);
procedure Prepend_Child (Container : in out Tree;
   Parent    : in   Cursor;
   New_Item  : in   Element_Type;
   Count     : in   Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
   (Parent /= No_Element
or else raise Constraint_Error) and then
   (Meaningful_For (Container, Parent)
or else raise Program_Error),
Post => Node_Count (Container) =
   Node_Count (Container)'Old + Count;

procedure Append_Child (Container : in out Tree;
   Parent    : in   Cursor;
   New_Item  : in   Element_Type;
   Count     : in   Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
   (Parent /= No_Element
or else raise Constraint_Error) and then
   (Meaningful_For (Container, Parent)
or else raise Program_Error),
Post => Node_Count (Container) =
   Node_Count (Container)'Old + Count;

procedure Delete_Children (Container : in out Tree;
   Parent    : in   Cursor)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
   (Parent /= No_Element
or else raise Constraint_Error) and then
   (Meaningful_For (Container, Parent)
or else raise Program_Error),
Post => (Child_Count (Container, Parent) =
   Child_Count (Container, Parent)'Old) and then
   Child_Count (Container, Parent) = 0;

procedure Copy_Subtree (Target   : in out Tree;
   Parent   : in   Cursor;
   Before   : in   Cursor;
   Source   : in   Cursor)
with Pre => (not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error) and then
   (Parent /= No_Element
or else raise Constraint_Error) and then
   (Meaningful_For (Target, Parent)
or else raise Program_Error) and then
   (Meaningful_For (Target, Before)
or else raise Program_Error) and then
   (Before = No_Element or else
   Target.Parent (Before) = Parent
or else raise Constraint_Error) and then
   (not Is_Root (Source)
or else raise Constraint_Error),
Post => Node_Count (Target) =
   Node_Count (Target)'Old + Subtree_Node_Count (Source),
Global => in all;
procedure Copy_Local_Subtree (Target: in out Tree;
Parent: in Cursor;
Before: in Cursor;
Source: in Cursor)
  with Pre => (not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error) and then
  (Parent /= No_Element
  or else raise Constraint_Error) and then
  (Meaningful_For (Target, Parent)
or else raise Program_Error) and then
  (Meaningful_For (Target, Before)
or else raise Program_Error) and then
  (Before = No_Element or else
  Target.Parent (Before) = Parent
  or else raise Constraint_Error)
  and then
  (Meaningful_For (Source, Subtree)
or else raise Program_Error) and then
  (not Is_Root (Source)
or else raise Constraint_Error),
Post => Node_Count (Target) = Node_Count (Target)'Old +
Subtree_Node_Count (Target, Source);

procedure Copy_Subtree (Target: in out Tree;
Parent: in Cursor;
Before: in Cursor;
Source: in Tree;
Subtree: in Cursor)
  with Pre => (not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error) and then
  (Parent /= No_Element
  or else raise Constraint_Error) and then
  (Meaningful_For (Target, Parent)
or else raise Program_Error) and then
  (Meaningful_For (Target, Before)
or else raise Program_Error) and then
  (Before = No_Element or else
  Target.Parent (Before) = Parent
  or else raise Constraint_Error)
  and then
  (Meaningful_For (Source, Subtree)
or else raise Program_Error) and then
  (not Is_Root (Source, Subtree)
or else raise Constraint_Error),
Post => Node_Count (Target) = Node_Count (Target)'Old +
Subtree_Node_Count (Source, Subtree);
procedure Splice_Subtree (Target : in out Tree;
    Parent : in   Cursor;
    Before : in   Cursor;
    Source : in out Tree;
    Position : in out Cursor)
  with Pre => (not Tampering_With_Cursors_Prohibited (Target)
    or else raise Program_Error) and then
    (not Tampering_With_Cursors_Prohibited (Source)
    or else raise Program_Error) and then
    (Parent /= No_Element
    or else raise Constraint_Error) and then
    (Meaningful_For (Target, Parent)
    or else raise Program_Error) and then
    (Meaningful_For (Target, Before)
    or else raise Program_Error) and then
    (Before = No_Element or else 
    Target.Parent (Before) /= Parent
    or else raise Constraint_Error) and then
    (Position /= No_Element
    or else raise Constraint_Error) and then
    (Has_Element (Target, Position)
    or else raise Program_Error) and then
    (Target.Has_Same_Storage (Source) or else 
    Position = Before or else 
    Is_Ancestor_Of (Target, Position, Parent)
    or else raise Constraint_Error),
  Post => (declare 
    Org_Sub_Count renames 
    Subtree_Node_Count (Source, Position)'Old;
    Org_Target_Count renames 
    Node_Count (Target)'Old;
    begin
    (if not Target.Has_Same_Storage (Source) then
      Node_Count (Target) = Org_Target_Count + 
      Org_Sub_Count and then
      Node_Count (Source) = Node_Count (Source)'Old - 
      Org_Sub_Count and then
      Has_Element (Target, Position)
    else
      Target.Parent (Position) = Parent and then
      Node_Count (Target) = Org_Target_Count));

procedure Splice_Subtree (Container: in out Tree;
    Parent : in   Cursor;
    Before : in   Cursor;
    Position : in   Cursor)
  with Pre => (not Tampering_With_Cursors_Prohibited (Container)
    or else raise Program_Error) and then
    (Parent /= No_Element
    or else raise Constraint_Error) and then
    (Meaningful_For (Container, Parent)
    or else raise Program_Error) and then
    (Meaningful_For (Container, Before)
    or else raise Program_Error) and then
    (Before = No_Element or else 
    Container.Parent (Before) /= Parent
    or else raise Constraint_Error) and then
    (Position /= No_Element
    or else raise Constraint_Error) and then
    (Has_Element (Container, Position)
    or else raise Program_Error) and then
    (Position = Before or else 
    Is_Ancestor_Of (Container, Position, Parent)
    or else raise Constraint_Error),
  Post => (Node_Count (Container) = 
    Node_Count (Container)'Old and then
    Container.Parent (Position) = Parent);
procedure Splice_Children( Target          : in out Tree;  
Target_Parent   : in   Cursor;  
Before          : in   Cursor;  
Source          : in out Tree;  
Source_Parent   : in   Cursor)

with Pre => (not Tampering_With_Cursors_Prohibited (Target)  
or else raise Program_Error) and then  
(not Tampering_With_Cursors_Prohibited (Source)  
or else raise Program_Error) and then  
(Target_Parent /= No_Element  
or else raise Constraint_Error) and then  
(Meaningful_For (Target, Target_Parent)  
or else raise Program_Error) and then  
(Meaningful_For (Target, Before)  
or else raise Program_Error) and then  
(Source_Parent /= No_Element  
or else raise Constraint_Error) and then  
(Meaningful_For (Source, Source_Parent)  
or else raise Program_Error) and then  
(Before = No_Element or else  
Parent (Target, Before) /= Target_Parent  
or else raise Constraint_Error) and then  
(Target'Has_Same_Storage (Source) or else  
Target Parent = Source Parent or else  
Is_Ancestor_Of (Target, Source_Parent, Target_Parent)  
or else raise Constraint_Error),

Post => (declare
  Org_Child_Count renames
  Child_Count (Source, Source_Parent)'Old;
  Org_Target_Count renames Node_Count (Target)'Old;
begin
  if not Target'Has_Same_Storage (Source) then
    Node_Count (Target) = Org_Target_Count +  
      Org_Child_Count and then
    Node_Count (Source) = Node_Count (Source)'Old -  
      Org_Child_Count
  else
    Node_Count (Target) = Org_Target_Count);
end procedure Splice_Children;

procedure Splice_Children( Container       : in out Tree;  
Target_Parent   : in   Cursor;  
Before          : in   Cursor;  
Source_Parent   : in   Cursor)

with Pre => (not Tampering_With_Cursors_Prohibited (Container)  
or else raise Program_Error) and then  
(Target_Parent /= No_Element  
or else raise Constraint_Error) and then  
(Meaningful_For (Container, Target_Parent)  
or else raise Program_Error) and then  
(Meaningful_For (Container, Before)  
or else raise Program_Error) and then  
(Source_Parent /= No_Element  
or else raise Constraint_Error) and then  
(Meaningful_For (Container, Source_Parent)  
or else raise Program_Error) and then  
(Before = No_Element or else  
Parent (Container, Before) /= Target_Parent  
or else raise Constraint_Error) and then  
(Target_Parent = Source Parent or else  
Is_Ancestor_Of (Container, Source_Parent, Target_Parent)  
or else raise Constraint_Error),

Post => (declare
  Org_Child_Count renames
  Child_Count (Source, Source_Parent)'Old;
  Org_Target_Count renames Node_Count (Target)'Old;
begin
  if not Target'Has_Same_Storage (Source) then
    Node_Count (Target) = Org_Target_Count +  
      Org_Child_Count and then
    Node_Count (Source) = Node_Count (Source)'Old -  
      Org_Child_Count
  else
    Node_Count (Target) = Org_Target_Count);
end procedure Splice_Children;

function Parent (Position : Cursor) return Cursor
with NonBlocking, Global => in all, Use Formal => null,
Post => (if Position = No_Element or else is Root (Position) then Parent'Result = No_Element);
function Parent (Container : Tree; Position : Cursor) return Cursor
  with Nonblocking, Global => null, Use Formal => null,
  Pre => Meaningful_For (Container, Position)
  or else raise Program_Error,
  Post => (if Position = No_Element or else Is_Root (Container, Position)
    then Parent'Result = No_Element
    else Has_Element (Container, Parent'Result));

function First_Child (Parent : Cursor) return Cursor
  with Nonblocking, Global => in all, Use Formal => null,
  Pre => Parent /= No_Element or else raise Constraint_Error;

function First_Child (Container : Tree; Parent : Cursor) return Cursor
  with Nonblocking, Global => null, Use Formal => null,
  Pre => (Parent /= No_Element
    or else raise Constraint_Error) and then
    Meaningful_For (Container, Parent)
  or else raise Program_Error),
  Post => First_Child'Result = No_Element or else Has_Element (Container, First_Child'Result);

function First_Child_Element (Parent : Cursor) return Element_Type
  with Nonblocking, Global => in all, Use Formal => Element_Type,
  Pre => (Parent /= No_Element and then
    Last_Child (Parent) /= No_Element)
  or else raise Constraint_Error;

function First_Child_Element (Container : Tree; Parent : Cursor) return Element_Type
  with Nonblocking, Global => null, Use Formal => Element_Type,
  Pre => (Parent /= No_Element
    or else raise Constraint_Error) and then
    Meaningful_For (Container, Parent)
  or else raise Program_Error) and then
    (First_Child (Container, Parent) /= No_Element
    or else raise Constraint_Error);

function Last_Child (Parent : Cursor) return Cursor
  with Nonblocking, Global => in all, Use Formal => null,
  Pre => Parent /= No_Element or else raise Constraint_Error;

function Last_Child (Container : Tree; Parent : Cursor) return Cursor
  with Nonblocking, Global => null, Use Formal => null,
  Pre => (Parent /= No_Element
    or else raise Constraint_Error) and then
    Meaningful_For (Container, Parent)
  or else raise Program_Error),
  Post => Last_Child'Result = No_Element or else Has_Element (Container, Last_Child'Result);

function Last_Child_Element (Parent : Cursor) return Element_Type
  with Nonblocking, Global => in all, Use Formal => Element_Type,
  Pre => (Parent /= No_Element and then
    Last_Child (Parent) /= No_Element)
  or else raise Constraint_Error;

function Last_Child_Element (Container : Tree; Parent : Cursor) return Element_Type
  with Nonblocking, Global => null, Use Formal => Element_Type,
  Pre => (Parent /= No_Element
    or else raise Constraint_Error) and then
    Meaningful_For (Container, Parent)
  or else raise Program_Error) and then
    (Last_Child (Container, Parent) /= No_Element
    or else raise Constraint_Error);
function Next_Sibling (Position : Cursor) return Cursor
with Nonblocking, Global => in all, Use Formal => null,
Post => (if Position = No_Element
    then Next_Sibling'Result = No_Element);}

function Next_Sibling (Container : Tree;
  Position : Cursor) return Cursor
with Nonblocking, Global => null, Use Formal => null,
Pre => Meaningful For (Container, Position),
or else raise Program_Error,
Post => (if Next_Sibling'Result = No_Element then
    Position = No_Element or else
    Is_Root (Container, Position) or else
    Last_Child (Container, Parent (Container, Position))
    = Position
  else Has_Element (Container, Next_Sibling'Result));

procedure Next_Sibling (Position : in out Cursor)
with Nonblocking, Global => in all, Use Formal => null;

procedure Next_Sibling (Container : in Tree;
  Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
Pre => Meaningful For (Container, Position),
or else raise Program_Error,
Post => (if Position /= No_Element
    then Has_Element (Container, Position));

function Previous_Sibling (Position : Cursor) return Cursor
with Nonblocking, Global => in all, Use Formal => null,
Post => (if Position = No_Element
    then Previous_Sibling'Result = No_Element);}

function Previous_Sibling (Container : Tree;
  Position : Cursor) return Cursor
with Nonblocking, Global => null, Use Formal => null,
Pre => Meaningful For (Container, Position),
or else raise Program_Error,
Post => (if Previous_Sibling'Result = No_Element then
    Position = No_Element or else
    Is_Root (Container, Position) or else
    First_Child (Container, Parent (Container, Position))
    = Position
  else Has_Element (Container, Previous_Sibling'Result));

procedure Previous_Sibling (Position : in out Cursor)
with Nonblocking, Global => in all, Use Formal => null;

procedure Previous_Sibling (Container : in Tree;
  Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
Pre => Meaningful For (Container, Position),
or else raise Program_Error,
Post => (if Position /= No_Element
    then Has_Element (Container, Position));

procedure Iterate_Children (Parent  : in Cursor;
  Process : not null access procedure (Position : in Cursor))
with Allows Exit,
Pre => Parent /= No_Element or else raise Constraint_Error,
Global => in all, Use Formal => null;

procedure Iterate_Children (Container : in Tree;
  Parent : in Cursor;
  Process : not null access procedure (Position : in Cursor))
with Allows Exit,
Pre => (Parent /= No_Element
  or else raise Constraint_Error) and then
  (Meaningful For (Container, Parent)
or else raise Program_Error);
procedure Reverse_Iterate_Children
(Parent  : in Cursor;
Process : not null access procedure (Position : in Cursor))
with Allows Exit,
Pre => Parent /= No_Element or else raise Constraint_Error,
Global => in all, Use Formal => null;

procedure Reverse_Iterate_Children
(Container   : in Tree;
Parent    : in Cursor;
Process   : not null access procedure (Position : in Cursor))
with Allows Exit,
Pre => (Parent /= No_Element
    or else raise Constraint_Error) and then
    (Meaningful For (Container, Parent)
    or else raise Program_Error);

function Iterate_Children (Container   : in Tree; Parent : in Cursor)
return Tree_Iterator_Interfaces.Parallel_Reversible_Iterator;
with Pre => (Parent /= No_Element
    or else raise Constraint_Error) and then
    (Meaningful For (Container, Parent)
    or else raise Program_Error),
    Post => Tampering_With_Cursors_Prohibited (Container);

package Stable is
    type Tree (Base : not null access Multiway_Trees.Tree) is
        tagged limited private
        with Constant_Indexing => Constant_Reference,
        Variable_Indexing => Reference,
        Default_Initializer => Iterate,
        Iterator_Element => Element_Type,
        Stable_Properties => (Node_Count),
        Global => null,
        Default_Initial_Condition => Node_Count (Tree) = 1,
        Preelaborable_Initialization;

    type Cursor is private
    with Preelaborable_Initialization;

    Empty_Tree : constant Tree;
    No_Element : constant Cursor;

    function Has_Element (Position : Cursor) return Boolean
    with Nonblocking, Global => in all, Use Formal => null;

    package Tree_Iterator_Interfaces is new
        Ada.Iterator_Interfaces (Cursor, Has_Element);

    procedure Assign (Target : in out Multiway_Trees.Tree;
        Source : in Tree)
    with Post => Node_Count (Source) = Node_Count (Target);

    function Copy (Source : Multiway_Trees.Tree) return Tree
    with Post => Node_Count (Copy'Result) = Node_Count (Source);

    type Constant_Reference_Type
        (Element : not null access constant Element_Type) is private
        with Implicit_Dereference => Element,
        Nonblocking, Global => null,
        Default_Initial_Condition => (raise Program_Error);

    type Reference_Type
        (Element : not null access Element_Type) is private
        with Implicit_Dereference => Element,
        Nonblocking, Global => null,
        Default_Initial_Condition => (raise Program_Error);

    -- Additional subprograms as described in the text
    -- are declared here.
A.18.10 The Generic Package Containers.Multiway_Trees

{AI12-0111-1} __private
{AI12-0111-1} ... -- not specified by the language
{AI12-0111-1} __end Stable;

private
... -- not specified by the language
end Ada.Containers.Multiway_Trees;

{AI05-0136-1} The actual function for the generic formal function "=" on Element_Type values is expected to define a reflexive and symmetric relationship and return the same result value each time it is called with a particular pair of values. If it behaves in some other manner, the functions Find, Reverse_Find, Equal_Subtree, and "=" on tree values return an unspecified value. The exact arguments and number of calls of this generic formal function by the functions Find, Reverse_Find, Equal_Subtree, and "=" on tree values are unspecified.

{AI05-0136-1} The type Tree is used to represent trees. The type Tree needs finalization (see 7.6).

{AI05-0136-1} {AI05-0248-1} Empty_Tree represents the empty Tree object. It contains only the root node (Node_Count (Empty_Tree) returns 1). If an object of type Tree is not otherwise initialized, it is initialized to the same value as Empty_Tree.

{AI05-0136-1} No_Element represents a cursor that designates no element. If an object of type Cursor is not otherwise initialized, it is initialized to the same value as No_Element.

{AI05-0136-1} {AI12-0434-1} The primitive predefined "=" operator for type Cursor returns True if both cursors are No_Element, or designate the same element in the same container.

To be honest: {AI12-0434-1} “The primitive "=" operator” is the one with two parameters of type Cursor which returns Boolean. We’re not talking about some other (hidden) primitive function named "=".

{AI05-0136-1} Execution of the default implementation of the Input, Output, Read, or Write attribute of type Cursor raises Program_Error.

{AI05-0136-1} {AI05-0248-1} {AI12-0437-1} Tree’Write for a Tree object T writes Node_Count(T) - 1 elements of the tree to the stream. It may also write additional information about the tree.

{AI05-0136-1} {AI05-0248-1} {AI10-0526-1} Tree’Read reads the representation of a tree from the stream, and assigns to Item a tree with the same elements and structure as was written by Tree’Write.

Ramification: Streaming more elements than the container holds is wrong. For implementation implications of this rule, see the Implementation Note in A.18.2.

{AI05-0136-1} {AI12-0111-1} {AI12-0112-1} [Some operations of this generic package have access to subprogram parameters. To ensure such operations are well-defined, they guard against certain actions by the designated subprogram. In particular, some operations check for “tampering with cursors” of a container because they depend on the set of elements of the container remaining constant, and others check for “tampering with elements” of a container because they depend on elements of the container not being replaced.] When tampering with cursors is prohibited for a particular tree object T, Program_Error is propagated by the finalization of T, as well as by a call that passes T to certain of the operations of this package, as indicated by the precondition of such an operation. Similarly, when tampering with elements is prohibited for T, Program_Error is propagated by a call that passes T to certain of the other operations of this package, as indicated by the precondition of such an operation.

Paragraphs 81 through 90 are removed as preconditions now describe these rules.

{AI05-0136-1} {AI12-0111-1} {AI12-0112-1} A subprogram is said to tamper with cursors of a tree object T if:

A.18.10 The Generic Package Containers.Multiway_Trees

16 October 2023  1118
• it inserts or deletes elements of \( T \), that is, it calls the Clear, Delete_Leaf, Insert_Child, Delete_Children, Delete_Subtree, or Copy_Subtree procedures with \( T \) as a parameter; or

To be honest: Operations which are defined to be equivalent to a call on one of these operations also are included. Similarly, operations which call one of these as part of their definition are included.

• \{AI05-0136-1\} \{AI05-0248-1\} it reorders the elements of \( T \), that is, it calls the Splice_Subtree or Splice_Children procedures with \( T \) as a parameter; or

• it finalizes \( T \); or

• it calls Assign with \( T \) as the Target parameter; or

Ramification: We don't need to explicitly mention assignment_statement, because that finalizes the target object as part of the operation, and finalization of an object is already defined as tampering with cursors.

• it calls the Move procedure with \( T \) as a parameter.

Reason: Swap copies elements rather than reordering them, so it doesn't tamper with cursors.

\{AI05-0136-1\} \{AI12-0111-1\} \{AI12-0112-1\} A subprogram is said to tamper with elements of a tree object \( T \) if:

• it tampers with cursors of \( T \); or

• it replaces one or more elements of \( T \), that is, it calls the Replace_Element or Swap procedures with \( T \) as a parameter.

Reason: Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can't be allowed. However, a simple modification of (part of) an element is not a problem, so Update_Element does not cause a problem.

Ramification: Assign is defined in terms of Clear and Replace_Element, so we don't need to mention it explicitly. Similarly, we don't need to explicitly mention assignment_statement, because that finalizes the target object as part of the operation, and finalization of an object is already defined as tampering with the element.

\{AI05-0265-1\} \{AI12-0110-1\} \{AI12-0111-1\} \{AI12-0112-1\} When tampering with cursors is prohibited for a particular tree object \( T \), Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the cursors of \( T \), leaving \( T \) unmodified. Similarly, when tampering with elements is prohibited for a particular tree object \( T \), Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the elements of \( T \) (or tamper with the cursors of \( T \)), leaving \( T \) unmodified. These checks are made before any other defined behavior of the body of the language-defined subprogram.

Proof: Tampering with elements includes tampering with cursors, so we mention it only from completeness in the second sentence.

\{AI12-0112-1\} function Has_Element (Position : Cursor) return Boolean with Nonblocking, Global => in all, Use Formal => null;

Returns True if Position designates an element, and returns False otherwise. [In particular, Has_Element returns False if the cursor designates a root node or equals No_Element.]

To be honest: \{AI05-0005-1\} \{AI05-0136-1\} This function might not detect cursors that designate deleted elements; such cursors are invalid (see below) and the result of calling Has_Element with an invalid cursor is unspecified (but not erroneous).

function Has_Element (Container : Tree; Position : Cursor) return Boolean with Nonblocking, Global => null, Use Formal => null;

\{AI12-0112-1\} Returns True if Position designates an element in Container, and returns False otherwise. [In particular, Has_Element returns False if the cursor designates a root node or equals No_Element.]
function Equal_Subtree (Left_Position: Cursor; Right_Position: Cursor) return Boolean;

{AI05-0136-I} {AI05-0248-I} {AI05-0262-I} {AI05-0264-I} If Left_Position or Right_Position equals No_Element, propagates Constraint_Error. If the number of child nodes of the element designated by Left_Position is different from the number of child nodes of the element designated by Right_Position, the function returns False. If Left_Position designates a root node and Right_Position does not, the function returns False. If Right_Position designates a root node and Left_Position does not, the function returns False. Unless both cursors designate a root node, the elements are compared using the generic formal equality operator. If the result of the element comparison is False, the function returns False. Otherwise, it calls Equal_Subtree on a cursor designating each child element of the element designated by Left_Position and a cursor designating the corresponding child element of the element designated by Right_Position. If any such call returns False, the function returns False; otherwise, it returns True. Any exception raised during the evaluation of element equality is propagated.

Ramification: Left_Position and Right_Position do not need to be from the same tree.

Implementation Note: This wording describes the canonical semantics. However, the order and number of calls on the formal equality function is unspecified for all of the operations that use it in this package, so an implementation can call it as many or as few times as it needs to get the correct answer. Similarly, a global rule (see the introduction of Annex A) says that language-defined routines are not affected by overriding of other language-defined routines. This means that no reasonable program can tell how many times Equal_Subtree is called, and thus an implementation can call it as many or as few times as it needs to get the correct answer. Specifically, there is no requirement to call the formal equality or Equal_Subtree additional times once the answer has been determined.

function “=” (Left, Right : Tree) return Boolean;

{AI05-0136-I} {AI05-0262-I} If Left and Right denote the same tree object, then the function returns True. Otherwise, it calls Equal_Subtree with cursors designating the root nodes of Left and Right; the result is returned. Any exception raised during the evaluation of Equal_Subtree is propagated.

Implementation Note: Similar considerations apply here as apply to Equal_Subtree. The actual number of calls performed is unspecified.

function Tampering_With_Cursors_Prohibited (Container: Tree) return Boolean with Nonblocking, Global => null, Use_Formal => null;

{AI12-0112-I} Returns True if tampering with cursors or tampering with elements is currently prohibited for Container, and returns False otherwise.

Reason: {AI12-0112-I} Prohibiting tampering with elements also needs to prohibit tampering with cursors, as deleting an element is similar to replacing it.

Implementation Note: {AI12-0112-I} Various contracts elsewhere in this specification require that this function be implemented with synchronized data. Moreover, it is possible for tampering to be prohibited by multiple operations (sequentially or in parallel). Therefore, tampering needs to be implemented with an atomic or protected counter. The counter is initialized to zero, and is incremented when tampering is prohibited, and decremented when leaving an area that prohibited tampering. Function Tampering_With_Cursors_Prohibited returns True if the counter is nonzero. (Note that any case where the result is not well-defined for one task is incorrect use of shared variables and would be erroneous by the rules of 9.10, so no special protection is needed to read the counter.)

function Tampering_With_Elements_Prohibited (Container: Tree) return Boolean with Nonblocking, Global => null, Use_Formal => null;

{AI12-0112-I} Always returns False, regardless of whether tampering with elements is prohibited.

Reason: {AI12-0111-I} A definite element cannot change size, so we allow operations that tamper with elements even when tampering with elements is prohibited. That's not true for the indefinite containers, which is why this kind of tampering exists.
function Is_Empty (Container : Tree) return Boolean
   with Nonblocking, Global => null, Use Formal => null,
   Post => Is_Empty'Result = (Node_Count (Container) = 1);

{AI05-0136-1} {AI12-0112-1} Returns True if Container is empty.

Ramification: An empty tree contains just the root node.

function Node_Count (Container : Tree) return Count_Type
   with Nonblocking, Global => null, Use Formal => null;

{AI05-0136-1} Node_Count returns the number of nodes in Container.

Ramification: Since all tree objects have a root node, this can never return a value of 0. Node_Count (Some_Tree) should always equal Subtree_Node_Count (Root (Some_Tree)).

function Subtree_Node_Count (Position : Cursor) return Count_Type
   with Nonblocking, Global => in all, Use Formal => null);

{AI05-0136-1} {AI05-0248-1} If Position is No_Element, Subtree_Node_Count returns 0; otherwise, Subtree_Node_Count returns the number of nodes in the subtree that is rooted by Position.

function Subtree_Node_CountIs_Empty (Container : Tree; Position : Cursor)
   return Count_Type
   with Pre => Meaningful_For (Container, Position)
   or else raise Program_Error,
   Nonblocking, Global => null, Use Formal => nullBoolean;

{AI05-0136-1} {AI12-0112-1} If Position is No_Element, Subtree_Node_Count returns 0; otherwise, Subtree_Node_Count returns the number of nodes in the subtree of Container that is rooted by Position Equivalent to Node_Count (Container) = 1.

This paragraph was deleted. Ramification: {AI12-0112-1} An empty tree contains just the root node.

Reason: {AI12-0112-1} We raise Program Error if Position belongs to some other container because we have promised to read only the container passed to this function. Determining the answer requires reading the container that Position belongs to, which we've promised not to do if it is not Container. We don't make this check for functions like Has_Element and Is_Root which do not require reading another container to determine the answer, but we do make it for most functions.

function Depth (Position : Cursor) return Count_Type
   with Nonblocking, Global => in all, Use Formal => null;

{AI05-0136-1} {AI05-0248-1} If Position equals No_Element, Depth returns 0; otherwise, Depth returns the number of ancestor nodes of the node designated by Position (including the node itself).

Ramification: Depth (Root (Some_Tree)) = 1.

function Depth (Container : Tree; Position : Cursor)
   return Count_Type
   with Pre => Meaningful_For (Container, Position)
   or else raise Program_Error,
   Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} If Position equals No_Element, Depth returns 0; otherwise, Depth returns the number of ancestor nodes of the node of Container designated by Position (including the node itself).

function Is_Root (Position : Cursor) return Boolean
   with Nonblocking, Global => in all, Use Formal => null;

{AI05-0136-1} {AI05-0248-1} Is_Root returns True if the Position designates the root node of some tree; and returns False otherwise.
function Is_Root (Container : Tree; Position : Cursor)  
return Boolean  
with Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} Is_Root returns True if the Position designates the root node of Container; and returns False otherwise.

**Ramification:** The two parameter Is_Root returns False even if Position is the root of some other tree than Container.

function Is_Leaf (Position : Cursor)  
return Boolean  
with Nonblocking, Global => in all, Use Formal => null;

{AI05-0136-1} Is_Leaf returns True if Position designates a node that does not have any child nodes; and returns False otherwise.

**Ramification:** Is_Leaf returns False if passed No_Element, since No_Element does not designate a node. Is_Leaf can be passed a cursor that designates the root node; Is_Leaf will return True if passed the root node of an empty tree.

function Is_Leaf (Container : Tree; Position : Cursor)  
return Boolean  
with Pre => Meaningful For (Container, Position)  
    or else raise Program_Error,  
Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} Is_Leaf returns True if Position designates a node in Container that does not have any child nodes; and returns False otherwise.

function Is_Ancestor_Of (Container : Tree;  
Parent   : Cursor;  
Position : Cursor)  
return Boolean  
with Pre => (Meaningful For (Container, Position)  
    or else raise Program_Error) and then  
    (Meaningful For (Container, Parent)  
    or else raise Program_Error),  
Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} Is_Ancestor_Of returns True if Parent designates an ancestor node of Position (including Position itself), and returns False otherwise.

function Root (Container : Tree)  
return Cursor  
with Nonblocking, Global => null, Use Formal => null;  
Post => Root'Result /= No_Element and then  
    not Has_Element (Container, Root'Result);

{AI05-0136-1} Root returns a cursor that designates the root node of Container.

**Ramification:** There is always a root node, even in an empty container, so this function never returns No_Element.

procedure Clear (Container : in out Tree)  
with Pre => not Tampering With Cursors Prohibited (Container)  
    or else raise Program_Error,  
Post => Node_Count (Container) = 1;

{AI05-0136-1} Removes all the elements from Container.

**Ramification:** The root node is not removed; all trees have a root node.

function Element (Position : Cursor)  
return Element_Type  
with Pre => (Position /= No_Element or else  
    raise Constraint_Error) and then  
    (Has Element (Position) or else raise Program_Error),  
Nonblocking, Global => in all, Use Formal => Element_Type;

{AI05-0136-1} If Position equals No_Element, then Constraint_Error is propagated; if Position designates the root node of a tree, then Program_Error is propagated. Otherwise, Element returns the element designated by Position.

**Ramification:** The root node does not contain an element, so that value cannot be read or written.
function Element (Container : Tree;   
    Position : Cursor) return Element_Type  
with Pre => (Position /= No_Element  
    or else raise Constraint_Error) and then  
    (Has_Element (Container, Position)  
    or else raise Program_Error),  
    Nonblocking, Global => null, Use Formal => Element_Type;  

{AI12-0112-1} Element returns the element designated by Position in Container.

procedure Replace_Element (Container : in out Tree;   
    Position : in Cursor;   
    New_item : in Element_Type)  
with Pre  => (not Tampering_With_Elements_Prohibited (Container)  
    or else raise Program_Error) and then  
    (Position /= No_Element  
    or else raise Constraint_Error) and then  
    (Has_Element (Container, Position)  
    or else raise Program_Error);  

{AI05-0136-1} {AI05-0264-1} {AI12-0112-1} {AI12-0196-1} If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container (including if it designates the root node), then Program_Error is propagated. Otherwise, Replace Element assigns the value New_Item to the element designated by Position. For the purposes of determining whether the parameters overlap in a call to Replace Element, the Container parameter is not considered to overlap with any object [(including itself)].

procedure Query_Element  
    (Position : in Cursor;   
    Process : not null access procedure (Element : in Element_Type))  
with Pre => (Position /= No_Element  
    or else raise Constraint_Error) and then  
    (Has_Element (Position)  
    or else raise Program_Error),  
    Global => in all;  

{AI05-0136-1} {AI05-0265-1} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated; if Position designates the root node of a tree, then Program_Error is propagated. Otherwise, Query Element calls Process.all with the element designated by Position as the argument. Tampering with the elements of the tree that contains the element designated by Position is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

procedure Query_Element  
    (Container : in Tree;   
    Position : in Cursor;   
    Process : not null access procedure (Element : in Element_Type))  
with Pre => (Position /= No_Element  
    or else raise Constraint_Error) and then  
    (Has_Element (Container, Position)  
    or else raise Program_Error);  

{AI12-0112-1} Query Element calls Process.all with the element designated by Position as the argument. Tampering with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.
procedure Update_Element
  (Container : in out Tree;
   Position : in Cursor;
   Process   : not null access procedure
              (Element : in out Element_Type))
with Pre => (Position /= No_Element
            or else raise Constraint_Error) and then
             (Has_Element (Container, Position)
            or else raise Program_Error);

If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container (including if it designates the root node), then Program_Error is propagated. Otherwise, Update_Element calls Process.all with the element designated by Position as the argument. Tampering with the elements of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

If Element_Type is unconstrained and definite, then the actual Element parameter of Process.all shall be unconstrained.

Ramification: This means that the elements cannot be directly allocated from the heap; it must be possible to change the discriminants of the element in place.

type Constant_Reference_Type (Element : not null access constant Element_Type) is private
  with Implicit_Dereference => Element,
       Nonblocking, Global => in out synchronized,
       Default_Initial_Condition => (raise Program_Error);

The types Constant_Reference_Type and Reference_Type need finalization.

This paragraph was deleted. The default initialization of an object of type Constant_Reference_Type or Reference_Type propagates Program_Error.

Reason: It is expected that Reference_Type (and Constant_Reference_Type) will be a controlled type, for which finalization will have some action to terminate the tampering check for the associated container. If the object is created by default, however, there is no associated container. Since this is useless, and supporting this case would take extra work, we define it to raise an exception.

function Constant_Reference (Container : aliased in Tree;
                             Position : in Cursor)
return Constant_Reference_Type
with Pre => (Position /= No_Element
            or else raise Constraint_Error) and then
             (Has_Element (Container, Position)
            or else raise Program_Error),
       Post => Tampering_With_Cursors_Prohibited (Container),
       Nonblocking, Global => null, Use_Explicit => null;

This function (combined with the Constant Indexing and Implicit_Dereference aspects) provides a convenient way to gain read access to an individual element of a tree given a cursor.
with the elements of Container is prohibited while the object returned by Constant_Reference exists and has not been finalized.

{AI12-0112-1} function Reference (Container : aliased in out Tree;  
    Position : in Cursor) return Reference_Type  
    with Pre => (Position /= No_Element  
      or else raise Constraint_Error) and then  
      (Has Element (Container, Position)  
      or else raise Program_Error),  
      Post => Tampering_With_Cursors_Prohibited (Container),  
      Nonblocking, Global => null, Use_Formal => null;  

{AI05-0212-1} {AI05-0269-1} This function (combined with the Variable Indexing and Implicit Dereference aspects) provides a convenient way to gain read and write access to an individual element of a tree given a cursor.

{AI05-0212-1} {AI05-0265-1} {AI12-0112-1} If Position equals No_Element, then Constraint_Error is propagated; if Position does not designate an element in Container, then Program_Error is propagated. Otherwise, Reference returns an object whose discriminant is an access value that designates the element designated by Position. Tampering with the elements of Container is prohibited while the object returned by Reference exists and has not been finalized.

{AI12-0112-1} procedure Assign (Target : in out Tree; Source : in Tree)  
    with Pre => not Tampering_With_Cursors_Prohibited (Target),  
      Post => Node_Count (Source) = Node_Count (Target);  

{AI05-0136-1} {AI05-0248-1} If Target denotes the same object as Source, the operation has no effect. Otherwise, the elements of Source are copied to Target as for an assignment_statement assigning Source to Target.

Ramification: Each element in Target has a parent element that corresponds to the parent element of the Source element, and has child elements that correspond to the child elements of the Source element.

Discussion: {AI05-0005-1} This routine exists for compatibility with the bounded tree container. For an unbounded tree, Assign(A, B) and A := B behave identically. For a bounded tree, := will raise an exception if the container capacities are different, while Assign will not raise an exception if there is enough room in the target.

{AI12-0112-1} function Copy (Source : Tree) return Tree  
    with Post =>  
      Node_Count (Copy'Result) = Node_Count (Source) and then  
      not Tampering_With_Elements_Prohibited (Copy'Result) and then  
      not Tampering_With_Cursors_Prohibited (Copy'Result);  

{AI05-0136-1} Returns a tree with the same structure as Source and whose elements are initialized from the corresponding elements of Source.

{AI12-0112-1} procedure Move (Target : in out Tree;  
    Source : in out Tree)  
    with Pre => (not Tampering_With_Cursors_Prohibited (Target)  
      or else raise Program_Error) and then  
      (not Tampering_With_Cursors_Prohibited (Source)  
      or else raise Program_Error),  
    Post => (if not Target'Has_Same_Storage (Source) then  
      Node_Count (Target) = Node_Count (Source'Old) and then  
      Node_Count (Source) = 1) ;  

{AI05-0136-1} {AI05-0248-1} If Target denotes the same object as Source, then the operation has no effect. Otherwise, Move first calls Clear (Target). Then, the nodes other than the root node in Source are moved to Target (in the same positions). After Move completes, Node_Count (Target) is the number of nodes originally in Source, and Node_Count (Source) is 1.
procedure Delete_Leaf (Container : in out Tree;
  Position  : in out Cursor)
  with Pre  => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
            (Position /= No_Element
               or else raise Constraint_Error) and then
            (Has_Element (Container, Position)
               or else raise Program_Error) and then
            (Is_Leaf (Container, Position)
               or else raise Constraint_Error),
  Post  =>
         Node_Count (Container)'Old = Node_Count (Container) + 1
            and then
         Position = No_Element;

{AI05-0136-1} {AI05-0248-1} {AI12-0112-1} If Position equals No_Element, then
Constraint_Error is propagated; if Position does not designate an element in Container (including
if it designates the root node), then Program_Error is propagated. If the element designated by
position has any child elements, then Constraint_Error is propagated. Otherwise, Delete Leaf
removes (from Container) the element designated by Position, and finally, Position is set to
No_Element.

Ramification: The check on Position checks that the cursor does not belong to some other Container. This check
implies that a reference to the container is included in the cursor value. This wording is not meant to require detection
of dangling cursors; such cursors are defined to be invalid, which means that execution is erroneous, and any result is
allowed (including not raising an exception).

The root node cannot be deleted.

procedure Delete_Subtree (Container : in out Tree;
  Position  : in out Cursor)
  with Pre  => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
            (Position /= No_Element
               or else raise Constraint_Error) and then
            (Has_Element (Container, Position)
               or else raise Program_Error),
  Post  =>
         Node_Count (Container)'Old = Node_Count (Container) +
            Subtree_Node_Count (Container, Position)'Old
            and then
         Position = No_Element;

{AI05-0136-1} {AI05-0264-1} {AI05-0269-1} {AI12-0112-1} If Position equals No_Element,
then Constraint_Error is propagated. If Position does not designate an element in Container
(including if it designates the root node), then Program_Error is propagated. Otherwise,
Delete Subtree removes (from Container) the subtree designated by Position (that is, all
descendants of the node designated by Position including the node itself), and Position is set to
No_Element.

Ramification: The root node cannot be deleted. To delete the entire contents of the tree, call Clear(Container).

procedure Swap (Container : in out Tree;
  I, J      : in Cursor)
  with Pre  => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
            (I /= No_Element or else Constraint_Error) and then
            (J /= No_Element or else Constraint_Error) and then
            (Has_Element (Container, I)
               or else raise Program_Error) and then
            (Has_Element (Container, J)
               or else raise Program_Error),
  Post  =>
         {AI05-0136-1} {AI12-0112-1} If either I or J equals No_Element, then Constraint_Error
is propagated. If either I or J do not designate an element in Container (including if either designates
the root node), then Program_Error is propagated. Otherwise, Swap exchanges the values of the
elements designated by I and J.

Ramification: After a call to Swap, I designates the element value previously designated by J, and J designates the
element value previously designated by I. The position of the elements do not change; for instance, the parent node and
the first child node of I are unchanged by the operation.

The root nodes do not contain element values, so they cannot be swapped.

To be honest: The implementation is not required to actually copy the elements if it can do the swap some other way.
But it is allowed to copy the elements if needed.

{AI12-0112-1} function Find (Container : Tree;
                   Item        : Element_Type)
  return Cursor
with Post => (if Find'Result /= No_Element
             then Has_Element (Container, Find'Result));

{AI05-0136-1} {AI05-0262-1} Find searches the elements of Container for an element equal to
Item (using the generic formal equality operator). The search starts at the root node. The search
traverses the tree in a depth-first order. If no equal element is found, then Find returns
No_Element. Otherwise, it returns a cursor designating the first equal element encountered.

function Find_In_Subtree (Position : Cursor;
                          Item     : Element_Type)
  return Cursor
with Pre  => Position /= No_Element or else raise
          Constraint_Error,
          Post => (if Find_In_Subtree'Result = No_Element
                   then Has_Element (Find_In_Subtree'Result)),
          Global => in all;

{AI05-0136-1} {AI05-0248-1} Find_In_Subtree searches the subtree rooted by Position for an
element equal to Item (using the generic formal equality operator). The search starts at the
element designated by Position. The search traverses the subtree in a depth-first order. If no equal
element is found, then Find_In_Subtree returns No_Element. Otherwise, it returns a cursor designating
the first equal element encountered.

Ramification: Find_In_Subtree does not check any siblings of the element designated by Position. The root node does
not contain an element, and therefore it can never be returned, but it can be explicitly passed to Position.

function Find_In_Subtree (Container : Tree;
                          Position  : Cursor;
                          Item      : Element_Type)
  return Cursor
with Pre  => (Position /= No_Element or else raise
              Constraint_Error) and then
              (Meaningful_For (Container, Position)
               or else raise Program_Error),
              Post => (if Find_In_Subtree'Result = No_Element
                      then Has_Element (Container, Find_In_Subtree'Result));

{AI12-0112-1} Find_In_Subtree searches the subtree of Container rooted by Position for an
element equal to Item (using the generic formal equality operator). The search starts at the
element designated by Position. The search traverses the subtree in a depth-first order. If no equal
element is found, then Find_In_Subtree returns No_Element. Otherwise, it returns a cursor designating the
first equal element encountered.

function Ancestor_Find (Position : Cursor;
                        Item     : Element_Type)
  return Cursor
with Pre  => Position /= No_Element or else raise
          Constraint_Error,
          Post => (if Ancestor_Find'Result = No_Element
                   then Has_Element (Container, Ancestor_Find'Result)),
          Global => in all;

{AI05-0136-1} {AI05-0248-1} Ancestor_Find searches for an element equal to Item
(using the generic formal equality operator). The search starts at the node designated by Position, and checks each ancestor proceeding toward the root of the subtree. If no equal element is found, then Ancestor_Find returns No_Element. Otherwise, it returns a cursor designating the first equal element encountered.

**Ramification:** 
No_Element is returned if Position is the root node.

```ada
function Ancestor_Find (Container : Tree;
     Position  : Cursor;
     Item      : Element_Type)
return Cursor
with Pre => (Position /= No_Element
     or else raise Constraint_Error) and then
     (Meaningful_For (Container, Position)
     or else raise Program_Error),
     Post => (if Ancestor_Find'Result = No_Element
     then Has_Element (Container, Ancestor_Find'Result));
```

Ancestor_Find searches for an element equal to Item (using the generic formal equality operator). The search starts at the node designated by Position in Container, and checks each ancestor proceeding toward the root of the subtree. If no equal element is found, then Ancestor_Find returns No_Element. Otherwise, it returns a cursor designating the first equal element encountered.

```ada
function Contains (Container : Tree;
     Item      : Element_Type)
return Boolean;
```

Equivalent to Find (Container, Item) /= No_Element.

```ada
procedure Iterate
(Container : in Tree;
     Process   : not null access procedure (Position : in Cursor))
with Allows.Exit;
```

Iterate calls Process.all with a cursor that designates each element in Container, starting from the root node and proceeding in a depth-first order. Tampering with the cursors of Container is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.

**Ramification:** Process is not called with the root node, which does not have an associated element.

**Implementation Note:** The purpose of the tamper with cursors check is to prevent erroneous execution from the Position parameter of Process.all becoming invalid. This check takes place when the operations that tamper with the cursors of the container are called. The check cannot be made later (say in the body of Iterate), because that could cause the Position cursor to be invalid and potentially cause execution to become erroneous — defeating the purpose of the check.

See Iterate for vectors (A.18.2) for a suggested implementation of the check.

```ada
procedure Iterate_Subtree
(Position  : in Cursor;
     Process   : not null access procedure (Position : in Cursor))
with Allows.Exit,
     Pre => Position /= No_Element or else raise Constraint_Error,
     Global => in all;
```

If Position equals No_Element, then Constraint_Error is propagated. Otherwise, Iterate_Subtree calls Process.all with a cursor that designates each element in the subtree rooted by the node designated by Position, starting from the node designated by Position and proceeding in a depth-first order. Tampering with the cursors of the tree that contains the element designated by Position is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.
Ramification: Position can be passed a cursor designating the root node; in that case, Process is not called with the root node, which does not have an associated element.

procedure Iterate_Subtree
(Container : in Tree;
Position : in Cursor;
Process : not null access procedure (Position : in Cursor))
with Allows Exit,
Pre => (Position /= No_Element
            or else raise Constraint_Error) and then
            (Meaningful_For (Container, Position)
            or else raise Program_Error);

{AI12-0112-1} Iterate_Subtree calls Process.all with a cursor that designates each element in the subtree rooted by the node designated by Position in Container, starting from the node designated by Position and proceeding in a depth-first order. Tampering with the cursors of the tree that contains the element designated by Position is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.

{AI12-0112-1} function Iterate (Container : in Tree)
return Tree_Iterator_Interfaces.Parallel_IteratorForward_Iterator'Class
with Post => Tampering_With_Cursors_Prohibited (Container);

{AI05-0212-1} {AI05-0265-1} {AI05-0269-1} {AI12-0069-1} {AI12-0266-1} Iterate returns an iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each element in Container, starting from the root node and proceeding in a depth-first order when used as a forward iterator, and processing all nodes concurrently when used as a parallel iterator. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop_statement whose iterator_specification denotes this object). The iterator object needs finalization.

Discussion: Exits are allowed from the loops created using the iterator objects. In particular, to stop the iteration at a particular cursor, just add
exit when Cur = Stop;

in the body of the loop (assuming that Cur is the loop parameter and Stop is the cursor that you want to stop at).

function Iterate_Subtree (Position : in Cursor)
return Tree_Iterator_Interfaces.Parallel_IteratorForward_Iterator'Class
with Pre => Position /= No_Element or else raise Constraint_Error,
Global => in all;

{AI05-0212-1} {AI05-0265-1} {AI05-0269-1} {AI12-0069-1} {AI12-0112-1} {AI12-0266-1} If Position equals No_Element, then Constraint_Error is propagated. Otherwise, Iterate_Subtree returns an iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each element in the subtree rooted by the node designated by Position, starting from the node designated by Position and proceeding in a depth-first order when used as a forward iterator, and processing all nodes in the subtree concurrently when used as a parallel iterator. If Position equals No_Element, then Constraint_Error is propagated. Tampering with the cursors of the container that contains the node designated by Position is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop_statement whose iterator_specification denotes this object). The iterator object needs finalization.
function Iterate_Subtree (Container : in Tree; Position : in Cursor) return Tree_Iterator_Interfaces.Parallel_Iterator'Class
with Pre => (Position /= No_Element
or else raise Constraint_Error) and then
(Meaningful_For (Container, Position)
or else raise Program_Error),
Post => Tampering_With_Cursors_Prohibited (Container);

{AI12-0112-1} Iterate_Subtree returns an iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each element in the subtree rooted by the node designated by Position in Container, starting from the node designated by Position and proceeding in a depth-first order when used as a forward iterator, and processing all nodes in the subtree concurrently when used as a parallel iterator. Tampering with the cursors of the container that contains the node designated by Position is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop statement whose iterator specification denotes this object). The iterator object needs finalization.

function Child_Count (Parent : Cursor) return Count_Type
with Post => (if Parent = No_Element then Child_Count'Result = 0),
Nonblocking, Global => in all, Use Formal => null;

function Child_Count (Container : Tree; Parent : Cursor) return Count_Type
with Pre => Meaningful_For (Container, Parent)
or else raise Program_Error,
Post => (if Parent = No_Element then Child_Count'Result = 0),
Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} Child_Count returns the number of child nodes of the node designated by Parent in Container.

function Child_Depth (Parent, Child : Cursor) return Count_Type
with Pre => (Parent /= No_Element and then Child /= No_Element
or else raise Constraint_Error,
Nonblocking, Global => in all, Use Formal => null;

{AI05-0136-1} {AI05-0262-1} {AI12-0112-1} If Child or Parent is equal to No_Element, then Constraint_Error is propagated. Otherwise, Child_Depth returns the number of ancestor nodes of Child (including Child itself), up to but not including Parent; Program_Error is propagated if Parent is not an ancestor of Child.

Ramification: Program_Error is propagated if Parent and Child are nodes in different containers.
Child_Depth (Root (Some_Tree), Child) + 1 = Depth (Child) as the root is not counted.

function Child_Depth (Container : Tree; Parent, Child : Cursor) return Count_Type
with Pre => ((Parent /= No_Element and then Child /= No_Element)
or else raise Constraint_Error) and then
(Meaningful_For (Container, Parent)
or else raise Program_Error) and then
(Meaningful_For (Container, Child)
or else raise Program_Error),
Nonblocking, Global => null, Use Formal => null;

{AI12-0112-1} Child_Depth returns the number of ancestor nodes of Child within Container (including Child itself), up to but not including Parent; Program_Error is propagated if Parent is not an ancestor of Child.
procedure Insert_Child (Container : in out Tree;
Parent    : in    Cursor;
Before    : in    Cursor;
New_Item  : in    Element_Type;
Count     : in    Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
  (Parent /= No_Element
or else raise Constraint_Error) and then
  (Meaningful_For (Container, Parent)
or else raise Program_Error) and then
  (Meaningful_For (Container, Before)
or else raise Program_Error) and then
  (Before = No_Element or else
   Container.Parent (Before) = Parent
or else raise Constraint_Error),
Post => Node_Count (Container) =
  Node_Count (Container)'Old + Count;

{AI05-0136-1} {AI05-0248-1} {AI05-0262-1} {AI12-0112-1} If Parent equals No_Element, then
Constraint_Error is propagated. If Parent does not designate a node in Container, then
Program_Error is propagated. If Before is not equal to No_Element, and does not designate a
node in Container, then Program_Error is propagated. If Before is not equal to No_Element, and
Parent does not designate the parent node of the node designated by Before, then
Constraint_Error is propagated. Otherwise, Insert_Child allocates Count nodes containing copies
of New_Item and inserts them as children of Parent. If Parent already has child nodes, then the
new nodes are inserted after the last existing child node of Parent. Any exception raised
during allocation of internal storage is propagated, and Container is not modified.

procedure Insert_Child (Container : in out Tree;
Parent    : in    Cursor;
Before    : in    Cursor;
New_Item  : in    Element_Type;
Position  : out    Cursor;
Count     : in    Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
  (Parent /= No_Element
or else raise Constraint_Error) and then
  (Meaningful_For (Container, Parent)
or else raise Program_Error) and then
  (Meaningful_For (Container, Before)
or else raise Program_Error) and then
  (Before = No_Element or else
   Container.Parent (Before) = Parent
or else raise Constraint_Error),
Post => (Node_Count (Container) =
  Node_Count (Container)'Old + Count)
and then
  Has_Element (Container, Position);

{AI05-0136-1} {AI05-0248-1} {AI05-0257-1} {AI05-0262-1} {AI12-0112-1} If Parent equals No_Element, then
Constraint_Error is propagated. If Parent does not designate a node in Container, then
Program_Error is propagated. If Before is not equal to No_Element, and does not designate a
node in Container, then Program_Error is propagated. If Before is not equal to No_Element, and
Parent does not designate the parent node of the node designated by Before, then
Constraint_Error is propagated. Otherwise, Insert_Child allocates Count nodes containing copies
of New_Item and inserts them as children of Parent. If Parent already has child nodes, then the
new nodes are inserted after the last existing child node of Parent. Any exception raised
during allocation of internal storage is propagated, and Container is not modified.
of Before. Any exception raised during allocation of internal storage is propagated, and Container is not modified.

```ada
procedure Insert_Child (Container : in out Tree;
                      Parent    : in   Cursor;
                      Before    : in   Cursor;
                      Position  : out  Cursor;
                      Count     : in   Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
                or else raise Program_Error)
                and then
                (Parent /= No_Element
                 or else raise Constraint_Error)
                and then
                (Meaningful_For (Container, Parent)
                 or else raise Program_Error)
                and then
                (Meaningful_For (Container, Before)
                 or else raise Program_Error)
                and then
                (Before = No_Element or else
                 Container.Parent (Before) = Parent
                 or else raise Constraint_Error)
                ,
                Post => (Node_Count (Container) =
                       Node_Count (Container)'Old + Count)
                       and then
                       Has_Element (Container, Position);
```

If Parent equals No_Element, then Constraint_Error is propagated. If Parent does not designate a node in Container, then Program_Error is propagated. If Before is not equal to No_Element, and does not designate a node in Container, then Program_Error is propagated. If Before is not equal to No_Element, and Parent does not designate the parent node of the node designated by Before, then Constraint_Error is propagated. Otherwise, Insert_Child allocates Count nodes, the elements contained in the new nodes are initialized by default (see 3.3.1), and the new nodes are inserted as children of Parent. If Parent already has child nodes, then the new nodes are inserted prior to the node designated by Before, or, if Before equals No_Element, the new nodes are inserted after the last existing child node of Parent. Position designates the first newly-inserted node, or if Count equals 0, then Position is assigned the value of Before. Any exception raised during allocation of internal storage is propagated, and Container is not modified.

```ada
procedure Prepend_Child (Container : in out Tree;
                        Parent    : in   Cursor;
                        New_Item  : in   Element_Type;
                        Count     : in   Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
              or else raise Program_Error)
              and then
              (Parent /= No_Element
               or else raise Constraint_Error)
              and then
              (Meaningful_For (Container, Parent)
               or else raise Program_Error)
              and then
              (New_Item /= No_Element
               or else raise Constraint_Error)
              and then
              (New_Item.Payment_Type ( newItem) /= 1
               or else raise Constraint_Error)
              ,
              Post => Node_Count (Container) =
                     Node_Count (Container)'Old + Count;
```

Equivalent to Insert_Child (Container, Parent, First_Child (Container, Parent),
New_Item, Count).
procedure Append_Child (Container : in out Tree;
         Parent     : in   Cursor;
         New_Item   : in   Element_Type;
         Count      : in   Count_Type := 1)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
               (Parent /= No_Element
               or else raise Constraint_Error) and then
               (Meaningful_For (Container, Parent)
               or else raise Program_Error),
Post => Node_Count (Container) = Node_Count (Container)'Old + Count;

{AI12-0112-1} {AI105-0269-1} Equivalent to Insert_Child (Container, Parent, No_Element,
New_Item, Count).

procedure Delete_Children (Container : in out Tree;
       Parent     : in   Cursor)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
               or else raise Program_Error) and then
               (Parent /= No_Element
               or else raise Constraint_Error) and then
               (Meaningful_For (Container, Parent)
               or else raise Program_Error),
Post => (Node_Count (Container) = Node_Count (Container)'Old -
Child_Count (Container, Parent)'Old + Count;
Child_Count (Container, Parent) = 0;

{AI105-0136-1} {AI12-0112-1} If Parent equals No_Element, then Constraint_Error is
propagated. If Parent does not designate a node in Container, Program_Error is propagated.
Otherwise, Delete_Children removes (from Container) all of the descendants of Parent other than
Parent itself.

Discussion: This routine deletes all of the child subtrees of Parent at once. Use Delete_Subtree to delete an individual
subtree.

procedure Copy_Subtree (Target   : in out Tree;
       Parent   : in   Cursor;
       Before   : in   Cursor;
       Source   : in   Cursor)
with Pre => (not Tampering_With_Cursors_Prohibited (Target)
               or else raise Program_Error) and then
               (Parent /= No_Element
               or else raise Constraint_Error) and then
               (Meaningful_For (Target, Parent)
               or else raise Program_Error) and then
               (Meaningful_For (Target, Before)
               or else raise Program_Error) and then
               (Before = No_Element or else
               Target.Parent (Before) = Parent
               or else raise Constraint_Error) and then
               (not Is_Root (Source)
               or else raise Constraint_Error),
Post => Node_Count (Target) = Node_Count (Target)'Old + Subtree_Node_Count (Source),
Global => in all;

{AI105-0136-1} {AI105-0248-1} {AI105-0262-1} {AI12-0112-1} If Parent equals No_Element, then
Constraint_Error is propagated. If Parent does not designate a node in Target, then
Program_Error is propagated. If Before is not equal to No_Element, and does not designate a
node in Target, then Program_Error is propagated. If Before is not equal to No_Element, and
Parent does not designate the parent node of the node designated by Before, then
Constraint_Error is propagated. If Source designates a root node, then Constraint_Error is
propagated. If Source is equal to No_Element, then the operation has no effect. Otherwise, the
subtree rooted by Source (which can be from any tree; it does not have to be a subtree of Target)
is copied (new nodes are allocated to create a new subtree with the same structure as the Source subtree, with each element initialized from the corresponding element of the Source subtree) and inserted into Target as a child of Parent. If Parent already has child nodes, then the new nodes are inserted prior to the node designated by Before, or, if Before equals No_Element, the new nodes are inserted after the last existing child node of Parent. The parent of the newly created subtree is set to Parent, and the overall count of Target is incremented by Subtree_Node_Count (Source). Any exception raised during allocation of internal storage is propagated, and Container is not modified.

Discussion: {AI12-0112-1} We only need one routine here, as the source object is not modified, so we can use the same routine for both copying within and between containers. However, that requires a contract that allows reading of any container of the correct type, so we provide two other routines with more restrictive contracts.

Ramification: We do not allow copying a subtree that includes a root node, as that would require inserting a node with no value in the middle of the target tree. To copy an entire tree to another tree object, use Copy.

```ada
procedure Copy_Local_Subtree (Target   : in out Tree;
                             Parent   : in  Cursor;
                             Before   : in  Cursor;
                             Source   : in  Cursor)

with Pre => (not Tampering_With_Cursors_Prohibited (Target)
        or else raise Program_Error) and then
    (Parent /= No_Element
        or else raise Constraint_Error) and then
    (Meaningful_For (Target, Parent)
        or else raise Program_Error) and then
    (Meaningful_For (Target, Before)
        or else raise Program_Error) and then
    (Before = No_Element or else
        Target.Parent (Before) = Parent
        or else raise Constraint_Error) and then
    (Meaningful_For (Target, Source)
        or else raise Program_Error) and then
    (not Is_Root (Source)
        or else raise Constraint_Error),
    Post => Node_Count (Target) = Node_Count (Target)'Old +
            Subtree_Node_Count (Target, Source);
```

{AI12-0112-1} If Source is equal to No_Element, then the operation has no effect. Otherwise, the subtree rooted by Source in Target is copied (new nodes are allocated to create a new subtree with the same structure as the Source subtree, with each element initialized from the corresponding element of the Source subtree) and inserted into Target as a child of Parent. If Parent already has child nodes, then the new nodes are inserted prior to the node designated by Before, or, if Before equals No_Element, the new nodes are inserted after the last existing child node of Parent. The parent of the newly created subtree is set to Parent. Any exception raised during allocation of internal storage is propagated, and Container is not modified.
procedure Copy_Subtree (Target : in out Tree;
Parent : in Cursor;
Before : in Cursor;
Source : in Tree;
Subtree : in Cursor)
with Pre => (not Tampering_With_Cursors_Prohibited (Target)
or else raise Program_Error) and then
(Parent /= No_Element
or else raise Constraint_Error) and then
(Meaningful_For (Target, Parent)
or else raise Program_Error) and then
(Meaningful_For (Target, Before)
or else raise Program_Error) and then
(Before = No_Element or else
Target.Parent (Before) = Parent
or else raise Constraint_Error) and then
(Meaningful_For (Source, Subtree)
or else raise Program_Error) and then
(not Is_Root (Source, Subtree).
or else raise Constraint_Error),
Post => Node_Count (Target) = Node_Count (Target)'Old +
Subtree_Node_Count (Source, Subtree);

{AI12-0112-1} If Subtree is equal to No_Element, then the operation has no effect. Otherwise, the subtree rooted by Subtree in Source is copied (new nodes are allocated to create a new subtree with the same structure as the Subtree, with each element initialized from the corresponding element of the Subtree) and inserted into Target as a child of Parent. If Parent already has child nodes, then the new nodes are inserted prior to the node designated by Before, or, if Before equals No_Element, the new nodes are inserted after the last existing child node of Parent. The parent of the newly created subtree is set to Parent. Any exception raised during allocation of internal storage is propagated, and Container is not modified.
procedure Splice_Subtree (Target : in out Tree;
    Parent   : in   Cursor;
    Before   : in   Cursor;
    Source   : in out Tree;
    Position : in out Cursor)
with Pre => (not Tampering_With.Cursors.Prohibited (Target)
            or else raise Program_Error) and then
            (not Tampering_With.Cursors.Prohibited (Source)
            or else raise Program_Error) and then
            (Parent /= No_Element
            or else raise Constraint_Error) and then
            (Meaningful_For (Target, Parent)
            or else raise Program_Error) and then
            (Meaningful_For (Target, Before)
            or else raise Program_Error) and then
            (Before = No_Element or else
            Target.Parent (Before) /= Parent
            or else raise Constraint_Error) and then
            (Position /= No_Element
            or else raise Constraint_Error) and then
            (Has_Element (Source, Position)
            or else raise Program_Error) and then
            (Target.'Has_Same_Storage (Source) or else
            Position = Before or else
            Is_Ancestor_Of (Target, Position, Parent)
            or else raise Constraint_Error),
Post => (declare
    Org_Sub_Count renames
    Subtree_Node_Count (Source, Position)'Old;
    Org_Target_Count renames Node_Count (Target)'Old;
begin
    if not Target.'Has_Same_Storage (Source) then
        Node_Count (Target) = Org_Target_Count +
        Org_Sub_Count and then
        Node_Count (Source) = Node_Count (Source)'Old -
        Org_Sub_Count and then
        Has_Element (Target, Position)
        else
        Target.Parent (Position) = Parent and then
        Node_Count (Target) = Org_Target_Count);

{AI05-0136-1} {AI05-0248-1} {AI05-0262-1} {AI05-0269-1} {AI12-0112-1} If Parent equals
No_Element, then Constraint_Error is propagated. If Parent does not designate a node in Target,
then Program_Error is propagated. If Before is not equal to No_Element, and does not designate a
node in Target, then Program_Error is propagated. If Before is not equal to No_Element, and
Parent does not designate the parent node of the node designated by Before, then
Constraint_Error is propagated. If Position equals No_Element, Constraint_Error is propagated. If
Position does not designate a node in Source or designates a root node, then Program_Error is
propagated. If Source denotes the same object as Target, then: if Position equals Before there is
no effect; if Position designates an ancestor of Parent (including Parent itself), Constraint_Error is
propagated; otherwise, the subtree rooted by the element designated by Position is moved to be a
child of Parent. If Parent already has child nodes, then the moved nodes are inserted prior to the
node designated by Before, or, if Before equals No_Element, the moved nodes are inserted after
the last existing child node of Parent. In each of these cases, Position and the count of Target are
unchanged, and the parent of the element designated by Position is set to Parent.

Reason: We can’t allow moving the subtree of Position to a proper descendant node of the subtree, as the descendant
node will be part of the subtree being moved. The result would be a circularly linked tree, or one with inaccessible
nodes. Thus we have to check Position against Parent, even though such a check is O(Depth(Source)).

{AI05-0136-1} {AI05-0248-1} Otherwise (if Source does not denote the same object as Target),
the subtree designated by Position is removed from Source and moved to Target. The subtree is
inserted as a child of Parent. If Parent already has child nodes, then the moved nodes are inserted prior to the node designated by Before, or, if Before equals No_Element, the moved nodes are inserted after the last existing child node of Parent. In each of these cases, the count of Target is incremented by Subtree Node Count (Position), and the count of Source is decremented by Subtree Node Count (Position), Position is updated to represent an element in Target.

**Ramification:** If Source is the same as Target, and Position = Before, or Next Sibling(Position) = Before, Splice Subtree has no effect, as the subtree does not have to move to meet the postcondition.

We do not allow splicing a subtree that includes a root node, as that would require inserting a node with no value in the middle of the target tree. Splice the children of the root node instead.

For this reason there is no operation to splice an entire tree, as that would necessarily involve splicing a root node.

```ada
procedure Splice_Subtree (Container: in out Tree;
Parent   : in Cursor;
Before   : in Cursor;
Position : in Cursor)
with Pre => (
not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Parent /= No_Element
or else raise Constraint_Error) and then
(Meaningful For (Container, Parent)
or else raise Program_Error) and then
(Meaningful For (Container, Before)
or else raise Program_Error) and then
(Before = No Element or else
Container.Parent (Before) /= Parent
or else raise Constraint_Error) and then
(Position /= No Element
or else raise Constraint_Error) and then
(Has Element (Container, Position)
or else raise Program_Error) and then
(Position = Before or else
Is_Ancestor_Of (Container, Position, Parent)
or else raise Constraint_Error),
Post => (Node_Count (Container) =
Node_Count (Container)'Old and then
Container.Parent (Position) = Parent);
```

If Parent equals No_Element, then Program_Error is propagated. If Parent does not designate a node in Container, then Program_Error is propagated. If Before is not equal to No_Element, and does not designate a node in Container, then Program_Error is propagated. If Before is not equal to No_Element, and Parent does not designate the parent node of the node designated by Before, then Constraint_Error is propagated. If Position equals No_Element, Constraint_Error is propagated. If Position does not designate a node in Container or designates a root node, then Program_Error is propagated. If Position equals Before, there is no effect. If Position designates an ancestor of Parent (including Parent itself), Constraint_Error is propagated. Otherwise, the subtree rooted by the element designated by Position is moved to be a child of Parent. If Parent already has child nodes, then the moved nodes are inserted prior to the node designated by Before, or, if Before equals No_Element, the moved nodes are inserted after the last existing child node of Parent. The parent of the element designated by Position is set to Parent.

**Reason:** We can't allow moving the subtree of Position to a proper descendant node of the subtree, as the descendant node will be part of the subtree being moved.
procedure Splice_Children (Target   : in out Tree;
  Target_Parent   : in   Cursor;
  Before          : in   Cursor;
  Source          : in out Tree;
  Source_Parent   : in   Cursor)
with Pre => (not Tampering With Cursors Prohibited (Target)
  or else raise Program_Error) and then
  (Target_Parent /= No_Element
  or else raise Constraint_Error) and then
  (Meaningful For (Target, Target_Parent)
  or else raise Program_Error) and then
  (Source_Parent /= No_Element
  or else raise Constraint_Error) and then
  (Meaningful For (Source, Source_Parent)
  or else raise Program_Error) and then
  (Before = No_Element or else Parent (Target, Before) /= Target_Parent
  or else raise Constraint_Error) and then
  (Target'Has Same Storage (Source) or else
  Target Parent = Source Parent or else
  Is Ancestor Of (Target, Source Parent, Target Parent)
  or else raise Constraint_Error),
Post => (declare
  Org_Child_Count renames Child Count (Source, Source Parent)'Old;
  Org_Target_Count renames Node Count (Target)'Old;
begin
  if not Target'Has Same Storage (Source) then
    Node Count (Target) = Org_Target_Count +
    Org_Child_Count and then
    Node Count (Source) = Node Count (Source)'Old -
    Org_Child_Count
  else
    Node Count (Target) = Org_Target_Count
This paragraph was deleted. ([A105-0136-1] [A105-0262-1] [A112-0112-1]) If Target Parent equals No Element, then Constraint_Error is propagated. If Target Parent does not designate a node in Target, then Program_Error is propagated. If Before is not equal to No Element, and does not designate an element in Target, then Program_Error is propagated. If Source Parent equals No Element, then Constraint_Error is propagated. If Source Parent does not designate a node in Source, then Program_Error is propagated. If Before is not equal to No Element, and Target Parent does not designate the parent node of the node designated by Before, then Constraint_Error is propagated.

If Source denotes the same object as Target, then:

• if Target Parent equals Source Parent there is no effect; else

• This paragraph was deleted. ([A105-0136-1] [A105-0269-1] [A112-0112-1]) if Source Parent is an ancestor of Target Parent other than Target Parent itself, then Constraint_Error is propagated; else

• the child elements (and the further descendants) of Source Parent are moved to be child elements of Target Parent. If Target Parent already has child elements, then the moved elements are inserted prior to the node designated by Before, or, if Before equals No Element, the moved elements are inserted after the last existing child node of Target Parent. The parent of each moved child element is set to Target Parent.
Reason: We can't allow moving the children of Source_Parent to a proper descendant node, as the descendant node
will be part of one of the subtrees being moved.

{AI05-0136-1} {AI05-0248-1} {AI05-0269-1} Otherwise (if Source does not denote the same
object as Target), the child elements (and the further descendants) of Source_Parent are removed
from Source and moved to Target. The child elements are inserted as children of Target_Parent. If
Target_Parent already has child elements, then the moved elements are inserted prior to the node
designated by Before, or, if Before equals No_Element, the moved elements are inserted after the
last existing child node of Target_Parent. In each of these cases, the overall count of Target is
incremented by Subtree_Node_Count(Source_Parent)-1, and the overall count of Source is
decremented by Subtree_Node_Count(Source_Parent)-1.

Ramification: The node designated by Source_Parent is not moved, thus we never need to update Source_Parent.

Move (Target, Source) could be written Splice_Children (Target, Target.Root, No_Element, Source, Source.Root);

procedure Splice_Children (Container : in out Tree;
Target_Parent : in out Cursor;
Before : in out Cursor;
Source_Parent : in out Cursor)
with Pre => (not Tampering_With_Cursors_Prohibited (Container)
or else raise Program_Error) and then
(Target_Parent /= No_Element
or else raise Constraint_Error) and then
(Meaningful_For (Container, Target_Parent)
or else raise Program_Error) and then
(Meaningful_For (Container, Before)
or else raise Program_Error) and then
(Source_Parent /= No_Element
or else raise Constraint_Error) and then
(Meaningful_For (Container, Source_Parent)
or else raise Program_Error) and then
(Before = No_Element or else
Parent (Container, Before) /= Target_Parent
or else raise Constraint_Error) and then
(Target_Parent = Source_Parent or else
Is_Ancestor_Of (Container, Source_Parent, Target_Parent)
or else raise Constraint_Error),
Post => Node_Count (Container) = Node_Count (Container)'Old;

{AI05-0136-1} {AI05-0248-1} {AI05-0262-1} {AI05-0264-1} {AI05-0269-1} {AI12-0112-1} If
Target_Parent equals No_Element, then Constraint_Error is propagated. If Target_Parent does
not designate a node in Container, then Program_Error is propagated. If Before is not equal to
No_Element, and does not designate an element in Container, then Program_Error is propagated.
If Source_Parent equals No_Element, then Constraint_Error is propagated. If Source_Parent does
not designate a node in Container, then Program_Error is propagated. If Before is not equal to
No_Element, and Target_Parent does not designate the parent node of the node
designated by
Before, then Constraint_Error is propagated. If Target_Parent equals Source_Parent there is no
effect. If Source_Parent is an ancestor of Target_Parent other than Target_Parent itself, then
Constraint_Error is propagated. Otherwise, the child elements (and the further descendants) of
Source_Parent are moved to be child elements of Target_Parent. If Target_Parent already has
child elements, then the moved elements are inserted prior to the node designated by Before, or, if
Before equals No_Element, the moved elements are inserted after the last existing child node of
Target_Parent. The parent of each moved child element is set to Target_Parent.
function Parent (Position : Cursor) return Cursor
  with Nonblocking, Global => in all, Use Formal => null,
  Post => (if Position = No_Element or else Is_Root (Position) then Parent'Result = No_Element);

{AI05-0136-1} {AI12-0112-1} Returns if Position is equal to No_Element or designates a root
node, No_Element is returned. Otherwise, a cursor designating the parent node of the node
designated by Position is returned.

function Parent (Container : Tree; Position : Cursor) return Cursor
  with Nonblocking, Global => null, Use Formal => null,
  Pre => Meaningful_For (Container, Position)
        or else raise Program_Error,
  Post => (if Position = No_Element or else Is_Root (Container, Position)
          then Parent'Result = No_Element
          else Has_Element (Container, Parent'Result));

{AI12-0112-1} Returns a cursor designating the parent node of the node designated by Position
in Container.

function First_Child (Parent : Cursor) return Cursor
  with Nonblocking, Global => in all, Use Formal => null,
  Post => (if Parent = No_Element or else is_Root (Parent) then Parent'Result = No_Element or else
          Has_Element (Container, Parent'Result));

{AI12-0112-1} {AI12-0112-1} If Parent is equal to No_Element, then Constraint_Error is
propagated. Otherwise, First_Child returns a cursor designating the first child node of the node
designated by Parent; if there is no such node, No_Element is returned.

function First_Child (Container : Tree; Parent : Cursor) return Cursor
  with Nonblocking, Global => null, Use Formal => null,
  Pre => (Parent /= No_Element or else raise Constraint_Error)
        and then (Meaningful_For (Container, Parent) or else raise Program_Error),
  Post => First_Child'Result = No_Element or else Has_Element (Container, First_Child'Result);

{AI12-0112-1} First_Child returns a cursor designating the first child node of the node
designated by Parent in Container; if there is no such node, No_Element is returned.

function First_Child_Element (Parent : Cursor) return Element_Type
  with Nonblocking, Global => in all, Use Formal => Element_Type,
  Pre => (Parent /= No_Element and then Last_Child (Parent) /= No_Element)
        or else raise Constraint_Error;

{AI05-0136-1} Equivalent to Element (First_Child (Parent)).

function First_Child_Element (Container : Tree; Parent : Cursor) return Element_Type
  with Nonblocking, Global => null, Use Formal => Element_Type,
  Pre => (Parent /= No_Element and then (Meaningful_For (Container, Parent) or else raise Program_Error) and then
          (First_Child (Container, Parent) /= No_Element)
        or else raise Constraint_Error);

{AI12-0112-1} Equivalent to Element (Container, First_Child (Container, Parent)).
function Last_Child (Parent : Cursor) return Cursor
    with Nonblocking, Global => in all, Use Formal => null,
    Pre => Parent /= No_Element or else raise Constraint_Error;
{AI05-0136-1} {AI12-0112-1} If Parent is equal to No_Element, then Constraint_Error is propagated. Otherwise, Last_Child returns a cursor designating the last child node of the node designated by Parent; if there is no such node, No_Element is returned.

function Last_Child (Container : Tree;
    Parent    : Cursor) return Cursor
    with Nonblocking, Global => null, Use Formal => null,
    Pre => (Parent /= No_Element
        or else raise Constraint_Error) and then
        (Meaningful_For (Container, Parent)
        or else raise Program_Error),
    Post => Last_Child'Result = No_Element or else
        Has_Element (Container, Last_Child'Result);
{AI12-0112-1} Last_Child returns a cursor designating the last child node of the node designated by Parent in Container; if there is no such node, No_Element is returned.

function Last_Child_Element (Parent : Cursor) return Element_Type
    with Nonblocking, Global => in all, Use Formal => Element_Type,
    Pre => (Parent /= No_Element and then
        Last_Child (Parent) /= No_Element)
        or else raise Constraint_Error;
{AI05-0136-1} Equivalent to Element (Last_Child (Parent)).

function Last_Child_Element (Container : Tree;
    Parent    : Cursor) return Element_Type
    with Nonblocking, Global => null, Use Formal => Element_Type,
    Pre => (Parent /= No_Element
        or else raise Constraint_Error) and then
        (Meaningful_For (Container, Parent)
        or else raise Program_Error) and then
        (Last_Child (Container, Parent) /= No_Element
        or else raise Constraint_Error);
{AI12-0112-1} Equivalent to Element (Container, Last_Child (Container, Parent)).

function Next_Sibling (Position : Cursor) return Cursor
    with Nonblocking, Global => in all, Use Formal => null,
    Post => (if Position = No_Element
        then Next_Sibling'Result = No_Element);
{AI05-0136-1} If Position equals No_Element or designates the last child node of its parent, then Next_Sibling returns the value No_Element. Otherwise, it returns a cursor that designates the successor (with the same parent) of the node designated by Position.

function Next_Sibling (Container : Tree;
    Position  : Cursor) return Cursor
    with Nonblocking, Global => null, Use Formal => null,
    Pre => Meaningful_For (Container, Position)
        or else raise Program_Error,
    Post => (if Next_Sibling'Result = No_Element then
        Position = No_Element or else
        Is_Root (Container, Position) or else
        Last_Child (Container, Parent (Container, Position))
        = Position
        else Has_Element (Container, Next_Sibling'Result)));
{AI12-0112-1} Next_Sibling returns a cursor that designates the successor (with the same parent) of the node designated by Position in Container.
function Previous_Sibling (Position : in out Cursor)
with Nonblocking, Global => in all, Use Formal => null,
    Post => (if Position = No_Element
        then Previous_Sibling'Result = No_Element);

If Position equals No_Element or designates the first child node of its parent, then
Previous_Sibling returns the value No_Element. Otherwise, it returns a cursor that designates the
predecessor (with the same parent) of the node designated by Position.

function Previous_Sibling (Container : Tree;
    Position : Cursor) return Cursor
with Nonblocking, Global => null, Use Formal => null,
    or else raise Program_Error,
    Post => (if Previous_Sibling'Result = No_Element then
        Position = No_Element or else
        is Root (Container, Position) or else
        First_Child (Container, Parent (Container, Position))
        = Position
        else Has_Element (Container, Previous_Sibling'Result));

Previous_Sibling returns a cursor that designates the predecessor (with the same
parent) of the node designated by Position in Container.

procedure Next_Sibling (Position : in out Cursor)
with Nonblocking, Global => in all, Use Formal => null;

Equivalent to Position := Next_Sibling (Position);

procedure Next_Sibling (Container : in Tree;
    Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
    or else raise Program_Error,
    Post => (if Position /= No_Element
        then Has_Element (Container, Position));

Equivalent to Position := Next_Sibling (Container, Position);

procedure Previous_Sibling (Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
    or else raise Program_Error,
    Post => (if Position /= No_Element
        then Has_Element (Container, Position));

Equivalent to Position := Previous_Sibling (Position);

procedure Previous_Sibling (Container : in Tree;
    Position : in out Cursor)
with Nonblocking, Global => null, Use Formal => null,
    or else raise Program_Error,
    Post => (if Position /= No_Element
        then Has_Element (Container, Position));

Equivalent to Position := Previous_Sibling (Container, Position);

procedure Iterate_Children
(Parent : in Cursor;
    Process : not null access procedure (Position : in Cursor))
with Allows Exit,
    Pre => Parent /= No_Element or else raise Constraint_Error,
        Global => in all, Use Formal => null;

This paragraph was deleted.

If Parent equals No_Element, then Constraint_Error is propagated.

Iterate_Children calls Process.all with a cursor that designates each child node of Parent, starting
with the first child node and moving the cursor as per the Next_Sibling function.
{AI05-0265-1} Tampering with the cursors of the tree containing Parent is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.

{AI12-0112-1} procedure Iterate_Children
    (Container : in Tree;
     Parent    : in Cursor;
     Process   : not null access procedure (Position : in Cursor))
with Allows Exit,
     Pre => (Parent /= No_Element
     or else raise Constraint_Error) and then
     (Meaningful_For (Container, Parent)
     or else raise Program_Error);

{AI12-0112-1} Iterate_Children calls Process.all with a cursor that designates each child node of Container and Parent, starting with the first child node and moving the cursor as per the Next_Sibling function.

{AI12-0112-1} Tampering with the cursors of the tree containing Parent is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.

{AI12-0112-1} procedure Reverse_Iterate_Children
    (Parent  : in Cursor;
     Process : not null access procedure (Position : in Cursor))
with Allows Exit,
     Pre => Parent /= No_Element or else raise Constraint_Error,
     Global => in all, Use_Formal => null;
This paragraph was deleted. {AI05-0136-1} {AI05-0248-1} {AI12-0112-1} If Parent equals No_Element, then Constraint_Error is propagated.

Reverse_Iterate_Children calls Process.all with a cursor that designates each child node of Parent, starting with the last child node and moving the cursor as per the Previous_Sibling function.

{AI05-0265-1} Tampering with the cursors of the tree containing Parent is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.

{AI12-0112-1} procedure Reverse_Iterate_Children
    (Container : in Tree;
     Parent    : in Cursor;
     Process   : not null access procedure (Position : in Cursor))
with Allows Exit,
     Pre => (Parent /= No_Element
     or else raise Constraint_Error) and then
     (Meaningful_For (Container, Parent)
     or else raise Program_Error);

{AI12-0112-1} Reverse_Iterate_Children calls Process.all with a cursor that designates each child node of Container and Parent, starting with the last child node and moving the cursor as per the Previous_Sibling function.

{AI12-0112-1} Tampering with the cursors of the tree containing Parent is prohibited during the execution of a call on Process.all. Any exception raised by Process.all is propagated.

function Iterate_Children (Container : in Tree; Parent : in Cursor)
return
Tree_Iterator_Interfaces.Parallel_Reversible_Iterator'Reversible_Iterator'Class
with Pre => (Parent /= No_Element
or else raise Constraint_Error) and then
(Meaningful_For (Container, Parent)
or else raise Program_Error);
Post => Tampering_With_Cursors_Prohibited (Container);

{AI05-0212-1} {AI05-0265-1} {AI12-0112-1} Iterate_Children returns an reversible iterator object (see 5.5.1) that will generate a value for a loop parameter (see 5.5.2) designating each child node of Parent. When If Parent equals No_Element, then Constraint_Error
is propagated. If Parent does not designate a node in Container, then Program_Error is propagated. Otherwise, when used as a forward iterator, the nodes are designated starting with the first child node and moving the cursor as per the function Next_Sibling; when used as a reverse iterator, the nodes are designated starting with the last child node and moving the cursor as per the function Previous_Sibling; when used as a parallel iterator, processing all child nodes concurrently. Tampering with the cursors of Container is prohibited while the iterator object exists (in particular, in the sequence of statements of the loop statement whose iterator_specification denotes this object). The iterator object needs finalization.

{AI12-0111-1} The nested package Multiway_Trees.Stable provides a type Stable.Tree that represents a stable tree, which is one that cannot grow and shrink. Such a tree can be created by calling the Copy function, or by establishing a stabilized view of an ordinary tree.

{AI12-0111-1} The subprograms of package Containers.Multiway_Trees that have a parameter or result of type tree are included in the nested package Stable with the same specification, except that the following are omitted:

- Tampering_With_Cursors_Prohibited
- Tampering_With_Elements_Prohibited
- Assign
- Move
- Clear
- Delete_Leaf
- Insert_Child
- Delete_Children
- Delete_Subtree
- Copy_Subtree
- Copy_Local_Subtree
- Splice_Subtree
- Splice_Children

Ramification: The names Tree and Cursor mean the types declared in the nested package in these subprogram specifications.

Reason: The omitted routines are those that tamper with cursors or elements (or test that state). The model is that it is impossible to tamper with cursors or elements of a stable view since no such operations are included. Thus tampering checks are not needed for a stable view, and we omit the operations associated with those checks.

{AI12-0111-1} The operations of this package are equivalent to those for ordinary trees, except that the calls to Tampering_With_Cursors_Prohibited and Tampering_With_Elements_Prohibited that occur in preconditions are replaced by False, and any that occur in postconditions are replaced by True.

{AI12-0111-1} If a stable tree is declared with the Base discriminant designating a pre-existing ordinary tree, the stable tree represents a stabilized view of the underlying ordinary tree, and any operation on the stable tree is reflected on the underlying ordinary tree. While a stabilized view exists, any operation that tampers with elements performed on the underlying tree is prohibited. The finalization of a stable tree that provides such a view removes this restriction on the underlying ordinary tree (though some other restriction can exist due to other concurrent iterations or stabilized views).

{AI12-0111-1} If a stable tree is declared without specifying Base, the object is necessarily initialized. The initializing expression of the stable tree, [typically a call on Copy], determines the Node_Count of the tree. The Node_Count of a stable tree never changes after initialization.

Proof: Initialization is required as the type is indefinite, see 3.3.1.

Bounded (Run-Time) Errors

{AI05-0136-1} It is a bounded error for the actual function associated with a generic formal subprogram, when called as part of an operation of this package, to tamper with elements of any Tree parameter of the operation. Either Program_Error is raised, or the operation works as defined on the value of the Tree either prior to, or subsequent to, some or all of the modifications to the Tree.

{AI05-0136-1} It is a bounded error to call any subprogram declared in the visible part of Containers.Multiway_Trees when the associated container has been finalized. If the operation takes Container as an in out parameter, then it raises Constraint_Error or Program_Error. Otherwise, the operation either proceeds as it would for an empty container, or it raises Constraint_Error or Program_Error.
Erroneous Execution

\{AI05-0136-1\} A Cursor value is invalid if any of the following have occurred since it was created:

- The tree that contains the element it designates has been finalized;
- The tree that contains the element it designates has been used as the Source or Target of a call to Move;
- The tree that contains the element it designates has been used as the Target of a call to Assign or the target of an assignment_statement;
- The element it designates has been removed from the tree that previously contained the element.

**Reason:** We talk about which tree the element was removed from in order to handle splicing nodes from one tree to another. The node still exists, but any cursors that designate it in the original tree are now invalid. This bullet covers removals caused by calls to Clear, Delete_Leaf, Delete_Subtree, Delete_Children, Splice_Children, and Splice_Subtree.

The result of "=" or `Has_Element` is unspecified if it is called with an invalid cursor parameter. Execution is erroneous if any other subprogram declared in `Containers.Multiway_Trees` is called with an invalid cursor parameter.

**Discussion:** The list above is intended to be exhaustive. In other cases, a cursor value continues to designate its original element (or the root node). For instance, cursor values survive the insertion and deletion of other nodes.

While it is possible to check for these cases, in many cases the overhead necessary to make the check is substantial in time or space. Implementations are encouraged to check for as many of these cases as possible and raise `Program_Error` if detected.

\{AI05-0212-1\} Execution is erroneous if the tree associated with the result of a call to Reference or Constant_Reference is finalized before the result object returned by the call to Reference or Constant_Reference is finalized.

**Reason:** Each object of Reference_Type and Constant_Reference_Type probably contains some reference to the originating container. If that container is prematurely finalized (which is only possible via Unchecked_Deallocation, as accessibility checks prevent passing a container to Reference that will not live as long as the result), the finalization of the object of Reference_Type will try to access a nonexistent object. This is a normal case of a dangling pointer created by Unchecked_Deallocation; we have to explicitly mention it here as the pointer in question is not visible in the specification of the type. (This is the same reason we have to say this for invalid cursors.)

Implementation Requirements

\{AI05-0136-1\} No storage associated with a multiway tree object shall be lost upon assignment or scope exit.

\{AI05-0136-1\} \{AI05-0262-1\} The execution of an assignment_statement for a tree shall have the effect of copying the elements from the source tree object to the target tree object and changing the node count of the target object to that of the source object.

**Implementation Note:** \{AI05-0298-1\} An assignment of a Tree is a "deep" copy; that is the elements are copied as well as the data structures. We say "effect of" in order to allow the implementation to avoid copying elements immediately if it wishes. For instance, an implementation that avoided copying until one of the containers is modified would be allowed. (Note that this implementation would require care, see A.18.2 for more.)

Implementation Advice

\{AI05-0136-1\} Containers.Multiway_Trees should be implemented similarly to a multiway tree. In particular, if \( N \) is the overall number of nodes for a particular tree, then the worst-case time complexity of Element, Parent, First_Child, Last_Child, Next_Sibling, Previous_Sibling, Insert_Child with Count=1, and Delete should be \( O(\log N) \).

**Implementation Advice:** The worst-case time complexity of the Element, Parent, First_Child, Last_Child, Next_Sibling, Previous_Sibling, Insert_Child with Count=1, and Delete operations of Containers.Multiway_Trees should be \( O(\log N) \).
Reason: We do not mean to overly constrain implementation strategies here. However, it is important for portability that the performance of large containers has roughly the same factors on different implementations. If a program is moved to an implementation that takes $O(N)$ time to access elements, that program could be unusable when the trees are large. We allow $O(\log N)$ access because the proportionality constant and caching effects are likely to be larger than the log factor, and we don't want to discourage innovative implementations.

AI05-0136-1 Move should not copy elements, and should minimize copying of internal data structures.

Implementation Advice: Containers.Multiway_Trees.Move should not copy elements, and should minimize copying of internal data structures.

Implementation Note: Usually that can be accomplished simply by moving the pointer(s) to the internal data structures from the Source container to the Target container.

AI05-0136-1 If an exception is propagated from a tree operation, no storage should be lost, nor any elements removed from a tree unless specified by the operation.

Implementation Advice: If an exception is propagated from a tree operation, no storage should be lost, nor any elements removed from a tree unless specified by the operation.

Reason: This is important so that programs can recover from errors. But we don't want to require heroic efforts, so we just require documentation of cases where this can't be accomplished.

Extensions to Ada 2005

AI05-0136-1 AI05-0257-1 AI05-0265-1 AI05-0269-1 The generic package Containers.Multiway_Trees is new.

Inconsistencies With Ada 2012

AI12-0111-1 Correction: Tampering with elements is now defined to be equivalent to tampering with cursors for ordinary containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

Incompatibilities With Ada 2012

AI12-0111-1 AI12-0112-1 A number of new subprograms, types, and even a nested package were added to Containers.Multiway_Trees to better support contracts and stable views. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.

Extensions to Ada 2012

AI12-0196-1 Correction: Replace Element is now defined such that it can be used concurrently so long as it operates on different elements. This allows some container operations to be used in parallel without separate synchronization.

AI12-0266-1 Most iterators can now return parallel iterators, to be used in parallel constructs.

Wording Changes from Ada 2012

AI12-0069-1 Corrigendum: Fixed the function Iterate so it is clear that the root node is never visited.

AI12-0078-1 Corrigendum: The definition of node is clarified so that it it doesn't appear to say all nodes have an element.

AI12-0110-1 Corrigendum: Clarified that tampering checks precede all other checks made by a subprogram (but come after those associated with the call).

AI12-0112-1 Corrigendum: Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).

A.18.11 The Generic Package Containers.Indefinite_Vectors

AI95-00302-03 The language-defined generic package Containers.Indefinite_Vectors provides a private type Vector and a set of operations. It provides the same operations as the package Containers.Vectors (see A.18.2), with the difference that the generic formal Element_Type is indefinite.
The declaration of the generic library package Containers.Indefinite_Vectors has the same contents and semantics as Containers.Vectors except:

- The generic formal Element_Type is indefinite.
- The procedures with the profiles:
  
    ```
    procedure Insert (Container : in out Vector;
                    Before    : in Extended_Index;
                    Count     : in Count_Type := 1);
    procedure Insert (Container : in out Vector;
                    Before    : in Cursor;
                    Position  : out Cursor;
                    Count     : in Count_Type := 1);
    ```
  
  are omitted.

  **Discussion:** These procedures are omitted because there is no way to create a default-initialized object of an indefinite type. Note that Insert_Space can be used instead of this routine in most cases. Omitting the routine completely allows any problems to be diagnosed by the compiler when converting from a definite to indefinite vector.

- The actual Element parameter of access subprogram Process of Update_Element may be constrained even if Element_Type is unconstrained.
- The operations "$\&\$", Append, Insert, Prepend, Replace_Element, and To_Vector that have a formal parameter of type Element_Type perform indefinite insertion (see A.18).
- The description of Tampering With Elements_Prohibited is replaced by:
  
  Returns True if tampering with elements is prohibited for Container, and False otherwise.

  **Reason:** Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can't be allowed. However, a simple modification of (part of) an element is not a problem, so Update_Element does not cause a problem.

- Tampering With Cursors_Prohibited is replaced by Tampering With Elements_Prohibited in the postcondition for the operations Reference and Constant_Reference.
- The operations Replace_Element, Reverse_Elements, and Swap, and the nested generic unit Generic_Sorting are omitted from the nested package Stable.

**Extensions to Ada 95**

The generic package Containers.Indefinite_Vectors is new.

**Inconsistencies With Ada 2012**

- **Corrigendum:** Defined some routines to “perform indefinite insertion”. This could mean that some calls to those routines would now raise Program_Error where they previously worked. However, this is extremely unlikely, as it would require that the package was not implemented in Ada (an Ada allocator would raise Program_Error in these circumstances), and that a program inserted a more nested tagged type (or access discriminant) into a container, and then used that object before its type or discriminant went out of scope. All known implementations are implemented in Ada, so we believe there is no practical incompatibility. As such, we mention this only for completeness.

- Defined the Iterator_View aspect, so that the stable view is used for container element iterators. This means that tampering with elements is prohibited during the entire loop, rather than tampering with cursors being prohibited during the loop, and tampering with elements being prohibited only during the lifetimes of references to the loop parameter. Thus, if a container element iterator does an operation that tampers with elements on the iterated container, that operation will fail a tampering check in Ada 2022 (and thus raise Program_Error), while it would have worked in Ada 2012 so long as the loop parameter is not involved. We believe this to be a dubious loop structure that should be rare. Note that this issue only occurs for the indefinite container form, the ordinary and bounded containers allow such operations at any time in Ada 2022.
A.18.12 The Generic Package Containers.Indefinite_Doubly_Linked_Lists

The language-defined generic package Containers.Indefinite_Doubly_Linked_Lists provides private types List and Cursor, and a set of operations for each type. It provides the same operations as the package Containers.Doubly_Linked_Lists (see A.18.3), with the difference that the generic formal Element_Type is indefinite.

Static Semantics

The declaration of the generic library package Containers.Indefinite_Doubly_Linked_Lists has the same contents and semantics as Containers.Doubly_Linked_Lists except:

- The generic formal Element_Type is indefinite.
- The procedure with the profile:
  
  ```
  procedure Insert (Container : in out List;
  Before    : in     Cursor;
  Position  : out   Cursor;
  Count     : in     Count_Type := 1);
  ```

  is omitted.

Discussion: This procedure is omitted because there is no way to create a default-initialized object of an indefinite type. We considered having this routine insert an empty element similar to the empty elements of a vector, but rejected this possibility because the semantics are fairly complex and very different from the existing definite container. That would make it more error-prone to convert a container from a definite type to an indefinite type; by omitting the routine completely, any problems will be diagnosed by the compiler.

- The actual Element parameter of access subprogram Process of Update_Element may be constrained even if Element_Type is unconstrained.
- The operations Append, Insert, Prepend, and Replace_Element that have a formal parameter of type Element_Type perform indefinite insertion (see A.18).
- The description of Tampering_With_Elements_Prohibited is replaced by:

  Returns True if tampering with elements is prohibited for Container, and False otherwise.

Reason: Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can't be allowed. However, a simple modification of (part of) an element is not a problem.

- Tampering_With_Cursors_Prohibited is replaced by Tampering_With_Elements_Prohibited in the postcondition for the operations Reference and Constant_Reference.

- The operations Replace_Element and Swap are omitted from the nested package Stable.

Extensions to Ada 95

- The generic package Containers.Indefinite_Doubly_Linked_Lists is new.

Inconsistencies With Ada 2012

- Corrigendum: Defined some routines to "perform indefinite insertion". This could mean that some calls to those routines would now raise Program_Error where they previously worked. However, this is extremely unlikely; see Inconsistencies With Ada 2012 in A.18.11 for details.

- Defined the Iterator_View aspect, so that the stable view is used for container element iterators. This leads to a rare situation where Program_Error will be raised in Ada 2022 for code that would have worked in Ada 2012. See Inconsistencies With Ada 2012 in A.18.11 for details.
A.18.13 The Generic Package Containers.Indefinite_Hashed_Maps

The language-defined generic package Containers.Indefinite_Hashed_Maps provides a map with the same operations as the package Containers.Hashed_Maps (see A.18.5), with the difference that the generic formal types Key_Type and Element_Type are indefinite.

Static Semantics

The declaration of the generic library package Containers.Indefinite_Hashed_Maps has the same contents and semantics as Containers.Hashed_Maps except:

- The generic formal Key_Type is indefinite.
- The generic formal Element_Type is indefinite.
- The procedure with the profile:

  ```plaintext
  procedure Insert (Container : in out Map;
                  Key       : in   Key_Type;
                  Position  : out  Cursor;
                  Inserted  : out  Boolean);
  ```

  is omitted.

  **Discussion:** This procedure is omitted because there is no way to create a default-initialized object of an indefinite type. We considered having this routine insert an empty element similar to the existing empty elements of a vector, but rejected this possibility because the semantics are fairly complex and very different from the existing case. That would make it more error-prone to convert a container from a definite type to an indefinite type; by omitting the routine completely, any problems will be diagnosed by the compiler.

- The actual Element parameter of access subprogram Process of Update_Element may be constrained even if Element_Type is unconstrained.
- The operations Include, Insert, Replace, and Replace_Element that have a formal parameter of type Element_Type perform indefinite insertion (see A.18).

  **Discussion:** Some of the named operations also have a formal of the indefinite formal type Key_Type and perform indefinite insertion using that value, but it is sufficient to mention the formal of type Element_Type to cover those.

- The description of Tampering_With_Elements_Prohibited is replaced by:

  Returns True if tampering with elements is prohibited for Container, and False otherwise.

  **Reason:** Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can't be allowed. However, a simple modification of (part of) an element is not a problem.

- Tampering_With_Cursors_Prohibited is replaced by Tampering_With_Elements_Prohibited in the postcondition for the operations Reference and Constant_Reference.

- The operations Replace and Replace_Element are omitted from the nested package Stable.

Extensions to Ada 95

The generic package Containers.Indefinite_Hashed_Maps is new.

Inconsistencies With Ada 2012

**Corrigendum:** Defined some routines to “perform indefinite insertion”. This could mean that some calls to those routines would now raise Program_Error where they previously worked. However, this is extremely unlikely; see Inconsistencies With Ada 2012 in A.18.11 for details.

The language-defined generic package Containers.Infinite_Ordered_Maps provides a map with the same operations as the package Containers.Ordered_Maps (see A.18.6), with the difference that the generic formal types Key_Type and Element_Type are indefinite.

Static Semantics

The declaration of the generic library package Containers.Infinite_Ordered_Maps has the same contents and semantics as Containers.Ordered_Maps except:

- The generic formal Key_Type is indefinite.
- The generic formal Element_Type is indefinite.
- The procedure with the profile:

  ```ada
  procedure Insert (Container : in out Map;
                  Key       : in    Key_Type;
                  Position  : out   Cursor;
                  Inserted  : out   Boolean);
  ```

  is omitted.

Discussion: This procedure is omitted because there is no way to create a default-initialized object of an indefinite type. We considered having this routine insert an empty element similar to the empty elements of a vector, but rejected this possibility because the semantics are fairly complex and very different from the existing case. That would make it more error-prone to convert a container from a definite type to an indefinite type; by omitting the routine completely, any problems will be diagnosed by the compiler.

- The actual Element parameter of access subprogram Process of Update_Element may be constrained even if Element_Type is unconstrained.
- The operations Include, Insert, Replace, and Replace_Element that have a formal parameter of type Element_Type perform indefinite insertion (see A.18).

Discussion: Some of the named operations also have a formal of the indefinite formal type Key_Type and perform indefinite insertion using that value, but it is sufficient to mention the formal of type Element_Type to cover those.

- The description of Tampering_With_Elements_Prohibited is replaced by:

  Returns True if tampering with elements is prohibited for Container, and False otherwise.

Reason: Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can't be allowed. However, a simple modification of (part of) an element is not a problem.

- Tampering_With_Cursors_Prohibited is replaced by Tampering_With_Elements_Prohibited in the postcondition for the operations Reference and Constant_Reference.

- The operations Replace and Replace_Element are omitted from the nested package Stable.

Extensions to Ada 95

The generic package Containers.Infinite_Ordered_Maps is new.
A.18.15 The Generic Package Containers.Indefinite_Hashed_Sets

The language-defined generic package Containers.Indefinite_Hashed_Sets provides a set with the same operations as the package Containers.Hashed_Sets (see A.18.8), with the difference that the generic formal type Element_Type is indefinite.

Static Semantics

The declaration of the generic library package Containers.Indefinite_Hashed_Sets has the same contents and semantics as Containers.Hashed_Sets except:

- The generic formal Element_Type is indefinite.
- The actual Element parameter of access subprogram Process of Update_Element_Preserving_Key may be constrained even if Element_Type is unconstrained.
- The operations Include, Insert, Replace, Replace_Element, and To_Set that have a formal parameter of type Element_Type perform indefinite insertion (see A.18).

Ramification: This includes the procedure Replace declared in the nested generic package Generic_Keys, as well as the routines declared directly in the Containers.Indefinite_Hashed_Sets package.

Discussion: Unlike the other containers, a Hashed_Set has no operations that tamper with elements without tampering with cursors. Modifying the contents of a element of a set can change its position in the set, so those operations tamper with cursors.

Because of this characteristic, this subclause is missing the rules that other indefinite containers have modifying the definition and use of Tampering_with_Elements, and the definition of the Stable subpackage is the same as the definite version.

Extensions to Ada 95

The generic package Containers.Indefinite_Hashed_Sets is new.

Inconsistencies With Ada 2012

Corrigendum: Defined some routines to “perform indefinite insertion”. This could mean that some calls to those routines would now raise Program_Error where they previously worked. However, this is extremely unlikely; see Inconsistencies With Ada 2012 in A.18.11 for details.

A.18.16 The Generic Package Containers.Indefinite_Ordered_Sets

The language-defined generic package Containers.Indefinite_Ordered_Sets provides a set with the same operations as the package Containers.Ordered_Sets (see A.18.9), with the difference that the generic formal type Element_Type is indefinite.

Static Semantics

The declaration of the generic library package Containers.Indefinite_Ordered_Sets has the same contents and semantics as Containers.Ordered_Sets except:

- The generic formal Element_Type is indefinite.
The actual Element parameter of access subprogram Process of Update_Element_Preserving_Key may be constrained even if Element_Type is unconstrained.

The operations Include, Insert, Replace, Replace_Element, and To_Set that have a formal parameter of type Element_Type perform indefinite insertion (see A.18).

Ramification: This includes the procedure Replace declared in the nested generic package Generic_Keys, as well as the routines declared directly in the Containers.Indefinite_Ordered_Sets package.

Discussion: Because of this characteristic, this subclause is missing the rules that other indefinite containers have modifying the definition and use of Tampering_with_Elements, and the definition of the Stable subpackage is the same as the definite version.

Extensions to Ada 95

The generic package Containers.Indefinite_Ordered_Sets is new.

Inconsistencies With Ada 2012

Corrigendum: Defined some routines to "perform indefinite insertion". This could mean that some calls to those routines would now raise Program_Error where they previously worked. However, this is extremely unlikely; see Inconsistencies With Ada 2012 in A.18.11 for details.

A.18.17 The Generic Package Containers.Indefinite_Multiway_Trees

The language-defined generic package Containers.Indefinite_Multiway_Trees provides a multiway tree with the same operations as the package Containers.Multiway_Trees (see A.18.10), with the difference that the generic formal Element_Type is indefinite.

Static Semantics

The declaration of the generic library package Containers.Indefinite_Multiway_Trees has the same contents and semantics as Containers.Multiway_Trees except:

The generic formal Element_Type is indefinite.

The procedure with the profile:

```
procedure Insert_Child (Container : in out Tree;
Parent    : in   Cursor;
Before    : in   Cursor;
Position  : out   Cursor;
Count     : in   Count_Type := 1);
```

is omitted.

Discussion: This procedure is omitted because there is no way to create a default-initialized object of an indefinite type. We considered having this routine insert an empty element similar to the empty elements of a vector, but rejected this possibility because the semantics are fairly complex and very different from the existing case. That would make it more error-prone to convert a container from a definite type to an indefinite type; by omitting the routine completely, any problems will be diagnosed by the compiler.

The actual Element parameter of access subprogram Process of Update_Element may be constrained even if Element_Type is unconstrained.

The operations Append_Child, Insert_Child, Prepend_Child, and Replace_Element that have a formal parameter of type Element_Type perform indefinite insertion (see A.18).

The description of Tampering_With_Elements_Prohibited is replaced by:

Returns True if tampering with elements is prohibited for Container, and False otherwise.
**Reason:** Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can’t be allowed. However, a simple modification of (part of) an element is not a problem.

- **AI12-0111-1**  **AI12-0112-1**  Tampering With Cursors Prohibited is replaced by Tampering With Elements Prohibited in the postcondition for the operations Reference and Constant Reference.

- **AI12-0111-1** The operations Replace_Element and Swap are omitted from the nested package Stable.

---

**Extensions to Ada 2005**

- **AI05-0136-1** The generic package Containers.Indefinite_Multiway_Trees is new.

**Inconsistencies With Ada 2012**

- **AI12-0035-1** **Corrigendum:** Defined some routines to “perform indefinite insertion”. This could mean that some calls to those routines would now raise Program_Error where they previously worked. However, this is extremely unlikely; see Inconsistencies With Ada 2012 in A.18.11 for details.

- **AI12-0111-1** Defined the Iterator_View aspect, so that the stable view is used for container element iterators. This leads to a rare situation where Program_Error will be raised in Ada 2022 for code that would have worked in Ada 2012. See Inconsistencies With Ada 2012 in A.18.11 for details.

---

**A.18.18 The Generic Package Containers.Indefinite_Holders**

- **AI05-0069-1** The language-defined generic package Containers.Indefinite_Holders provides a private type Holder and a set of operations for that type. A holder container holds a single element of an indefinite type.

- **AI05-0069-1** A holder container allows the declaration of an object that can be used like an uninitialized variable or component of an indefinite type.

- **AI05-0069-1** A holder container may be empty. An empty holder does not contain an element.

**Static Semantics**

- **AI05-0069-1** **AI05-0084-1** **AI12-0112-1**

```ada
generic
  type Element_Type (<>)
  is private;
  with function "=" (Left, Right : Element_Type) return Boolean is <>;
package Ada.Containers.Indefinite_Holders
  with Preelaborate, Remote_Types, Nonblocking, Global =>
    in out synchronized is
  pragma Preelaborate(Indefinite_Holders);
  pragma Remote_Types(Indefinite_Holders);
Discuss:

  For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects in this generic package, see the notes on the equivalent operations in the specification of the Containers.Vectors package (see A.18.2).

- **AI12-0112-1**  **AI12-0399-1**

``` ada
  type Holder is tagged private
  with Stable_Properties => (Is_Empty,
    Tampering_With_The_Element_Prohibited),
    Default Initial Condition => Is_Empty (Holder),
    pragma Preelaborable Initialization (Holder);
  Empty_Holder : constant Holder;
function Equal_Element (Left, Right : Element_Type) return Boolean
  with renames ":=";
function "=" (Left, Right : Holder) return Boolean;
function Tampering_With_The_Element_Prohibited
  with Nonblocking, Global => null, Use Formal => null;
```
{A12-0339-1} function Empty return Holder
  is (Empty_Holder)
  with Post =>
  not Tampering_With_The_Element_Prohibited (Empty'Result)
  and then Is_Empty (Empty'Result);

{A12-0112-1} function To_Holder (New_Item : Element_Type) return Holder
  with Post => not Is_Empty (To_Holder'Result);

{A12-0112-1} function Is_Empty (Container : Holder) return Boolean
  with Global => null, Use_Formal => null;

{A12-0112-1} procedure Clear (Container : in out Holder)
  with Pre => not Tampering_With_The_Element_Prohibited (Container)
  or else raise Program_Error,
  Post => Is_Empty (Container);

{A12-0112-1} function Element (Container : Holder) return Element_Type
  with Pre => not Is_Empty (Container)
  or else raise Constraint_Error,
  Global => null, Use_Formal => Element_Type;

{A12-0112-1} procedure Replace_Element (Container : in out Holder;
  New_Item : in Element_Type)
  with Pre => not Tampering_With_The_Element_Prohibited (Container)
  or else raise Program_Error,
  Post => not Is_Empty (Container);

{A12-0112-1} procedure Query_Element
  (Container : in Holder;
  Process : not null access procedure (Element : in Element_Type))
  with Pre => not Is_Empty (Container)
  or else raise Constraint_Error;

{AI05-0001-1} {A12-0112-1} procedure Update_Element
  (Container : in out Holder;
  Process : not null access procedure (Element : in out Element_Type))
  with Pre => not Is_Empty (Container)
  or else raise Constraint_Error;

{AI12-0112-1} type Constant_Reference_Type
  (Element : not null access constant Element_Type)
  is private
  with Implicit_Dereference => Element,
  Nonblocking, Global => in out synchronized,
  Default_Initial_Condition => (raise Program_Error);

{AI12-0112-1} type Reference_Type
  (Element : not null access Element_Type)
  is private
  with Implicit_Dereference => Element,
  Nonblocking, Global => in out synchronized,
  Default_Initial_Condition => (raise Program_Error);

{AI12-0112-1} function Constant_Reference (Container : aliased in Holder)
  return Constant_Reference_Type
  with Pre => not Is_Empty (Container),
  Post => Tampering_With_The_Element_Prohibited (Container),
  Nonblocking, Global => null, Use_Formal => null;

{AI12-0112-1} function Reference (Container : aliased in out Holder)
  return Reference_Type
  with Pre => not Is_Empty (Container)
  or else raise Constraint_Error,
  Post => Tampering_With_The_Element_Prohibited (Container),
  Nonblocking, Global => null, Use_Formal => null;

{AI05-0001-1} {A12-0112-1} procedure Assign (Target : in out Holder; Source : in Holder)
  with Post => (Is_Empty (Source) = Is_Empty (Target));

{AI05-0001-1} {A12-0112-1} function Copy (Source : Holder) return Holder
  with Post => (Is_Empty (Source) = Is_Empty (Copy'Result));
procedure Move (Target : in out Holder; Source : in out Holder) with Pre => (not Tampering_With_The_Element_Prohibited (Target) or else raise Program_Error) and then (not Tampering_With_The_Element_Prohibited (Source) or else raise Program_Error), Post => (if not Target'Has_Same_Storage (Source) then Is_Empty (Source) and then (not Is_Empty (Target))),

procedure Swap (Left, Right : in out Holder) with Pre => (not Tampering_With_The_Element_Prohibited (Left) or else raise Program_Error) and then (not Tampering_With_The_Element_Prohibited (Right) or else raise Program_Error), Post => Is_Empty (Left) = Is_Empty (Right)'Old and then Is_Empty (Right) = Is_Empty (Left)'Old;

private
    ... -- not specified by the language
end Ada.Containers.Indefinite_Holders;

The actual function for the generic formal function "=" on Element_Type values is expected to define a reflexive and symmetric relationship and return the same result value each time it is called with a particular pair of values. If it behaves in some other manner, the function "=" on holder values returns an unspecified value. The exact arguments and number of calls of this generic formal function by the function "=" on holder values are unspecified.

Ramification: If the actual function for "=" is not symmetric and consistent, the result returned by any of the functions defined to use "=" cannot be predicted. The implementation is not required to protect against "=" raising an exception, or returning random results, or any other "bad" behavior. And it can call "=" in whatever manner makes sense. But note that only the results of the function "=" is unspecified; other subprograms are not allowed to break if "=" is bad.

The type Holder is used to represent holder containers. The type Holder needs finalization (see 7.6).

Empty_Holder represents an empty holder object. If an object of type Holder is not otherwise initialized, it is initialized to the same value as Empty_Holder.

Some operations of this generic package have access to subprogram parameters. To ensure such operations are well-defined, they guard against certain actions by the designated subprogram. In particular, some operations check for “tampering with the element” of a container because they depend on the element of the container not being replaced. When tampering with the element is prohibited for a particular holder object H, Program_Error is propagated by the finalization of H, as well as by a call that passes H to certain of the operations of this package, as indicated by the precondition of such an operation.

Paragraphs 30 through 35 are removed as preconditions now describe these rules.

A subprogram is said to tamper with the element of a holder object H if:

- It clears the element contained by H, that is, it calls the Clear procedure with H as a parameter;
- It replaces the element contained by H, that is, it calls the Replace_Element procedure with H as a parameter;
- It calls the Move procedure with H as a parameter;
- It finalizes H.

Reason: Complete replacement of an element can cause its memory to be deallocated while another operation is holding onto a reference to it. That can’t be allowed. However, a simple modification of (part of) an element is not a problem, so Update_Element does not cause a problem.
When tampering with the element is prohibited for a particular holder object \( H \), Program_Error is propagated by a call of any language-defined subprogram that is defined to tamper with the element of \( H \), leaving \( H \) unmodified. These checks are made before any other defined behavior of the body of the language-defined subprogram.

```ada
function "=" (Left, Right : Holder) return Boolean;
```

If Left and Right denote the same holder object, then the function returns True. Otherwise, it compares the element contained in Left to the element contained in Right using the generic formal equality operator, returning the result of that operation. Any exception raised during the evaluation of element equality is propagated.

**Implementation Note:** This wording describes the canonical semantics. However, the order and number of calls on the formal equality function is unspecified, so an implementation need not call the equality function if the correct answer can be determined without doing so.

```ada
function Tampering_With_The_Element_Prohibited (Container : Holder) return Boolean
with Nonblocking, Global => null, Use_Formal => null;
```

Returns True if tampering with the element is currently prohibited for Container, and returns False otherwise.

```ada
function To_Holder (New_Item : Element_Type) return Holder
with Post => not Is_Empty (To_Holder'Result);
```

Returns a nonempty holder containing an element initialized to \( New \_\text{Item} \). To_Holder performs indefinite insertion (see A.18).

```ada
function Is_Empty (Container : Holder) return Boolean
with Global => null, Use_Formal => null;
```

Returns True if Container is empty, and False if it contains an element.

```ada
procedure Clear (Container : in out Holder)
with Pre => not Tampering_With_The_Element_Prohibited (Container)
or else raise Program_Error,
Post => Is_Empty (Container);
```

Removes the element from Container. Container is empty after a successful Clear operation.

```ada
function Element (Container : Holder) return Element_Type
with Pre => not Is_Empty (Container)
or else raise Constraint_Error,
Global => null, Use_Formal => Element_Type;
```

Returns if Container is empty, Constraint_Error is propagated. Otherwise, returns the element stored in Container.

```ada
procedure Replace_Element (Container : in out Holder;
New_Item : in Element_Type)
with Pre => not Tampering_With_The_Element_Prohibited (Container)
or else raise Program_Error,
Post => not Is_Empty (Container);
```

Replace Element assigns the value \( New \_\text{Item} \) into Container, replacing any preexisting content of Container. Replace Element performs indefinite insertion (see A.18). Container is not empty after a successful call to Replace_Element.
procedure Query_Element
(Container : in Holder;
Process   : not null access procedure (Element : in Element_Type))
with Pre => not Is_Empty (Container) or else raise Constraint_Error,
Global => null, Use Formal => null;

If Container is empty, Constraint_Error is propagated. Otherwise, Query_Element calls Process.all with the contained element as the argument. Tampering with the element of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

Implementation Note: The “tamper with the element” check is intended to prevent the Element parameter of Process from being replaced or deleted outside of Process. The check prevents data loss (if Element_Type is passed by copy) or erroneous execution (if Element_Type is an unconstrained type).

procedure Update_Element
(Container : in out Holder;
Process   : not null access procedure (Element : in out Element_Type))
with Pre => not Is_Empty (Container) or else raise Constraint_Error;

If Container is empty, Constraint_Error is propagated. Otherwise, Update_Element calls Process.all with the contained element as the argument. Tampering with the element of Container is prohibited during the execution of the call on Process.all. Any exception raised by Process.all is propagated.

Implementation Note: The Element parameter of Process.all may be constrained even if Element_Type is unconstrained.

function Constant_Reference (Container : aliased in Holder) return Constant_Reference_Type
with Pre => not Is_Empty (Container) or else raise Constraint_Error,
Post => Tampering_With_The_Element_Prohibited (Container),
Nonblocking, Global => null, Use Formal => null;

This function (combined with the Implicit Dereference aspect) provides a convenient way to gain read access to the contained element of a holder container.

The types Constant_Reference_Type and Reference_Type need finalization.

This paragraph was deleted.

The default initialization of an object of type Constant_Reference_Type or Reference_Type propagates Program_Error.

Reason: It is expected that Reference_Type (and Constant_Reference_Type) will be a controlled type, for which finalization will have some action to terminate the tampering check for the associated container. If the object is created by default, however, there is no associated container. Since this is useless, and supporting this case would take extra work, we define it to raise an exception.
function Reference (Container : aliased in out Holder)
return Reference_Type
with Post => Tampering_With_The_Element_Prohibited (Container),
Nonblocking, Global => null, Use_Formal => null;

This function (combined with the Implicit Dereference aspects) provides a convenient way to gain read and write access to the contained element of a holder container.

If Container is empty, Constraint_Error is propagated. Otherwise, Reference returns an object whose discriminant is an access value that designates the contained element. Tampering with the element of Container is prohibited while the object returned by Reference exists and has not been finalized.

procedure Assign (Target : in out Holder; Source : in Holder)
with Post => (Is_Empty (Source) = Is_Empty (Target));

If Target denotes the same object as Source, the operation has no effect. If Source is empty, Clear (Target) is called. Otherwise, Replace Element (Target, Element (Source)) is called.

procedure Move (Target : in out Holder; Source : in out Holder)
with Pre => (not Tampering_With_The_Element_Prohibited (Target),
or else raise Program_Error)
and then (not Tampering_With_The_Element_Prohibited (Source),
or else raise Program_Error),
Post => (if not Target'Has_Same_Storage (Source) then
Is_Empty (Source) and then (not Is_Empty (Target)))
and then (not Is_Empty (Right)'Old
Is_Empty (Right) = Is_Empty (Left)'Old);

procedure Swap (Left, Right : in out Holder)
with Pre => (not Tampering_With_The_Element_Prohibited (Left),
or else raise Program_Error)
and then (not Tampering_With_The_Element_Prohibited (Right),
or else raise Program_Error),
Post => Is_Empty (Left) = Is_Empty (Right)'Old and then
Is_Empty (Right) = Is_Empty (Left)'Old;

Bounded (Run-Time) Errors

It is a bounded error for the actual function associated with a generic formal subprogram, when called as part of an operation of this package, to tamper with the element of any Holder parameter of the operation. Either Program_Error is raised, or the operation works as defined on the value of the Holder either prior to, or subsequent to, some or all of the modifications to the Holder.
It is a bounded error to call any subprogram declared in the visible part of Containers.Indefinite_Holders when the associated container has been finalized. If the operation takes Container as an in out parameter, then it raises Constraint_Error or Program_Error. Otherwise, the operation either proceeds as it would for an empty container, or it raises Constraint_Error or Program_Error.

Erroneous Execution

Execution is erroneous if the holder container associated with the result of a call to Reference or Constant_Reference is finalized before the result object returned by the call to Reference or Constant_Reference is finalized.

Reason:
Each object of Reference_Type and Constant_Reference_Type probably contains some reference to the originating container. If that container is prematurely finalized (which is only possible via Unchecked_Deallocation, as accessibility checks prevent passing a container to Reference that will not live as long as the result), the finalization of the object of Reference_Type will try to access a nonexistent object. This is a normal case of a dangling pointer created by Unchecked_Deallocation; we have to explicitly mention it here as the pointer in question is not visible in the specification of the type. (This is the same reason we have to say this for invalid cursors.)

Implementation Requirements

No storage associated with a holder object shall be lost upon assignment or scope exit.

The execution of an assignment statement for a holder container shall have the effect of copying the element (if any) from the source holder object to the target holder object.

Implementation Note:
An assignment of a holder container is a “deep” copy; that is the element is copied as well as any data structures. We say “effect of” in order to allow the implementation to avoid copying the element immediately if it wishes. For instance, an implementation that avoided copying until one of the containers is modified would be allowed. (Note that this implementation would require care, see A.18.2 for more.)

Implementation Advice

Move and Swap should not copy any elements. The element, and should minimize copying of internal data structures.

Implementation Advice:
Move and Swap in Containers.Indefinite_Holders. Move should not copy any elements. The element, and should minimize copying of internal data structures.

Implementation Note:
Usually that can be accomplished simply by moving the pointer(s) to the internal data structures appropriately from the Source holder to the Target holder.

If an exception is propagated from a holder operation, no storage should be lost, nor should the element be removed from a holder container unless specified by the operation.

Implementation Advice:
If an exception is propagated from a holder operation, no storage should be lost, nor should the element be removed from a holder container unless specified by the operation.

Reason:
This is important so that programs can recover from errors. But we don't want to require heroic efforts, so we just require documentation of cases where this can't be accomplished.

Extensions to Ada 2005

The generic package Containers.Indefinite_Holders is new.

Inconsistencies With Ada 2012

Corrigendum: Defined some routines to “perform indefinite insertion”. This could mean that some calls to those routines would now raise Program_Error where they previously worked. However, this is extremely unlikely; see Inconsistencies With Ada 2012 in A.18.11 for details.

Incompatibilities With Ada 2012

A number of new subprograms and types were added to Containers.Indefinite_Holders to better support contracts and provide additional functionality. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.
Wording Changes from Ada 2012

{AI12-0110-1} Corrigendum: Clarified that tampering checks precede all other checks made by a subprogram (but come after those associated with the call).

{AI12-0111-1} Added contracts to this container. This includes describing some of the semantics with pre- and postconditions, rather than English text. Note that the preconditions can be Suppressed (see 11.5).

A.18.19 The Generic Package Containers.Bounded_Vectors

{AI05-0001-1} The language-defined generic package Containers.Bounded_Vectors provides a private type Vector and a set of operations. It provides the same operations as the package Containers.Vectors (see A.18.2), with the difference that the maximum storage is bounded.

Static Semantics

{AI05-0001-1} The declaration of the generic library package Containers.Bounded_Vectors has the same contents and semantics as Containers.Vectors except:

- {AI12-0112-1} The aspect pragma Preelaborate is replaced with aspect pragma Pure. Aspect Global is deleted.

Ramification: {AI12-0112-1} The Global aspect for a Pure package is null (see 6.1.2), so we don't need to give it explicitly.

- The type Vector is declared with a discriminant that specifies the capacity:

> type Vector (Capacity : Count_Type) is tagged private...

- {AI12-0409-1} The aspect_definition for Preelaborable_Initialization for type Vector is changed to:

> Preelaborable_Initialization =>
> Element_Type'Preelaborable_Initialization

- The type Vector needs finalization if and only if type Element_Type needs finalization.

Implementation Note: {AI05-0212-1} The type Vector cannot depend on package Ada.Finalization unless the element type depends on that package. The objects returned from the Iterator and Reference functions probably do depend on package Ada.Finalization. Restricted environments may need to avoid use of those functions and their associated types.

- {AI12-0112-1} Capacity is omitted from the Stable_Properties of type Vector.

Reason: The capacity is a discriminant here, so it can't be changed by most routines; thus including it in the stable properties adds no information.

- {AI12-0339-1} In function Empty, the postcondition is altered to:

> Post =>
> Empty'Result.Capacity = Capacity and then
> not Tampering_With_Elements_Prohibited (Empty'Result) and then
> not Tampering_With_Cursors_Prohibited (Empty'Result) and then
> Length (Empty'Result) = 0;

- {AI12-0112-1} In function Copy, the postcondition is altered to:

> if the Capacity parameter is equal to or greater than the length of Source, the vector Capacity exactly equals the value of the Capacity parameter:

> Post => Length (Copy'Result) = Length (Source) and then
> (if Capacity > Length (Source) then
> Copy'Result.Capacity = Capacity
> else Copy'Result.Capacity >= Length (Source));

- The description of Reserve_Capacity is replaced with:

> procedure Reserve_Capacity (Container : in out Vector;
> Capacity : in Count_Type)
> with Pre => Capacity <= Container.Capacity
> or else raise Capacity_Error;
ThisIf the specified Capacity is larger than the capacity of Container, then Reserve_Capacity propagates Capacity_Error. Otherwise, the operation has no effect, [other than checking the precondition].

The portion of the postcondition checking the capacity is omitted from subprograms Set_Length, Assign, Insert, Insert_Space, Prepend, Append, and Delete.

For procedures Insert, Insert_Space, Prepend, and Append, the part of the precondition reading:

\[ (<\text{some length}> <= \text{Maximum Length} - <\text{some other length}> \]
\[ \text{or else raise Constraint_Error}) \]

is replaced by:

\[ (<\text{some length}> <= \text{Maximum Length} - <\text{some other length}> \]
\[ \text{or else raise Constraint_Error}) \text{ and then} \]
\[ (<\text{some length}> <= \text{Container.Capacity} - <\text{some other length}> \]
\[ \text{or else raise Capacity_Error}) \]

Bounded (Run-Time) Errors

It is a bounded error to assign from a bounded vector object while tampering with elements [or cursors] of that object is prohibited. Either Program_Error is raised by the assignment, execution proceeds with the target object prohibiting tampering with elements [or cursors], or execution proceeds normally.

Proof: Tampering with elements includes tampering with cursors, so we only really need to talk about tampering with elements here; we mention cursors for clarity.

Erroneous Execution

When a bounded vector object V is finalized, if tampering with cursors is prohibited for V other than due to an assignment from another vector, then execution is erroneous.

Reason: This is a tampering event, but since the implementation is not allowed to use Ada.Finalization, it is not possible in a pure Ada implementation to detect this error. (There is no Finalize routine that will be called that could make the check.) Since the check probably cannot be made, the bad effects that could occur (such as an iterator going into an infinite loop or accessing a nonexistent element) cannot be prevented and we have to allow anything. We do allow re-assigning an object that only prohibits tampering because it was copied from another object as that cannot cause any negative effects.

Implementation Requirements

For each instance of Containers.Vectors and each instance of Containers.Bounded_Vectors, if the two instances meet the following conditions, then the output generated by the Vector'Output or Vector'Write subprograms of either instance shall be readable by the Vector'Input or Vector'Read of the other instance, respectively:

- the Element_Type parameters of the two instances are statically matching subtypes of the same type; and
- the output generated by Element_Type'Output or Element_Type'Write is readable by Element_Type'Input or Element_Type'Read, respectively (where Element_Type denotes the type of the two actual Element_Type parameters); and
- the preceding two conditions also hold for the Index_Type parameters of the instances.

Bounded vector objects should be implemented without implicit pointers or dynamic allocation.
Implementation Advice: Bounded vector objects should be implemented without implicit pointers or dynamic allocation.

The implementation advice for procedure Move to minimize copying does not apply.

Implementation Advice: The implementation advice for procedure Move to minimize copying does not apply to bounded vectors.

Extensions to Ada 2005

The generic package Containers.Bounded_Vectors is new.

Inconsistencies With Ada 2012

Tampering with elements is now defined to be equivalent to tampering with cursors for bounded containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

A.18.20 The Generic Package Containers.Bounded_Doubly_Linked_Lists

The language-defined generic package Containers.Bounded_Doubly_Linked_Lists provides a private type List and a set of operations. It provides the same operations as the package Containers.Doubly_Linked_Lists (see A.18.3), with the difference that the maximum storage is bounded.

Static Semantics

The declaration of the generic library package Containers.Bounded_Doubly_Linked_Lists has the same contents and semantics as Containers.Doubly_Linked_Lists except:

- The aspect pragma Preelaborate is replaced with aspect pragma Pure. Aspect Global is deleted.

Ramification: The Global aspect for a Pure package is null (see 6.1.2), so we don't need to give it explicitly.

- The type List is declared with a discriminant that specifies the capacity (maximum number of elements) as follows:

- The type List needs finalization if and only if type Element_Type needs finalization.

Implementation Note: The type List cannot depend on package Ada.Finalization unless the element type depends on that package. The objects returned from the Iterator and Reference functions probably do depend on package Ada.Finalization. Restricted environments may need to avoid use of those functions and their associated types.

The function Empty is replaced by:

16.a.1/3
17/3
A105-0001-1
The implementation advice for procedure Move to minimize copying does not apply.

17.a.1/3
A105-0160-1 A105-0184-1
Implementation Advice: The implementation advice for procedure Move to minimize copying does not apply to bounded vectors.

17.a/3
A105-0001-1 A105-0160-1 A105-0184-1
The generic package Containers.Bounded_Vectors is new.

Inconsistencies With Ada 2012

Correction: Tampering with elements is now defined to be equivalent to tampering with cursors for bounded containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

A112-0409-1
Correction: A bounded vector now only has Preelaborable_Initialization (abbreviated PI in this note) when the actual for the Element_Type has PI. If an program used a vector whose actual Element_Type does not have PI in a context when PI is required (such as a library-level object in a preelaborated unit or as a component of a type with PI), the program would be illegal in Ada 2022 but legal in original Ada 2012. This situation is unlikely, especially as some existing Ada 2012 implementations reject the instance in this case.
function Empty (Capacity : Count_Type := implementation-defined)
return List
with Post =>
   Empty'Result.Capacity = Capacity and then
   not Tampering With Elements Prohibited (Empty'Result) and then
   not Tampering With Cursors Prohibited (Empty'Result) and then
   Length (Empty'Result) = 0;

• \{AI12-0112-1\} For procedures Insert, Prepend, Append, Merge, and the three-parameter Splice whose parameter Source has type List, the part of the precondition reading: The allocation of internal storage includes a check that the capacity is not exceeded, and Capacity_Error is raised if this check fails.
   
   \((<\text{some length}> \leq \text{Count Type}'\text{Last} - <\text{some other length}>\)

   or else raise Constraint_Error).

   is replaced by:

   \((<\text{some length}> \leq \text{Count Type}'\text{Last} - <\text{some other length}>\)

   or else raise Constraint_Error) and then

   \((<\text{some length}> \leq \text{Container.Capacity} - <\text{some other length}>\)

   or else raise Capacity_Error).

• \{AI12-0112-1\} In procedure Assign, the precondition is altered to: if Source length is greater than Target capacity, then Capacity_Error is propagated.

   Pre => [not Tampering With Cursors Prohibited (Target)

   or else raise Program_Error) and then

   (Length (Source) \leq Target.Capacity

   or else raise Capacity_Error),

   • The function Copy is replaced with:

   \{AI12-0112-1\} function Copy (Source : List; Capacity : Count_Type := 0)
return List
with Pre => Capacity = 0 or else Capacity \geq Length (Source)

   or else raise Capacity_Error,

   Post =>

   Length (Copy'Result) = Length (Source) and then

   not Tampering With Elements Prohibited (Copy'Result) and then

   not Tampering With Cursors Prohibited (Copy'Result) and then

   Copy'Result.Capacity = (if Capacity = 0 then

   Length (Source) else Capacity).

   Returns a list whose elements have the same values as the elements of Source.If Capacity is 0, then the list capacity is the length of Source; if Capacity is equal to or greater than the length of Source, the list capacity equals the value of the Capacity parameter; otherwise, the operation propagates Capacity_Error.

   • This paragraph was deleted.\{AI12-0112-1\} In the three-parameter procedure Splice whose Source has type List, if the sum of the length of Target and the length of Source is greater than the capacity of Target, then Splice propagates Capacity_Error.

   • \{AI12-0112-1\} In the four-parameter procedure Splice, the precondition is altered to: if the length of Target equals the capacity of Target, then Splice propagates Capacity_Error.
A.18.20 The Generic Package Containers.Bounded_Doubly_Linked_Lists 16 October 2023 1164

Bounded (Run-Time) Errors

{AI05-0160-1} {AI05-0265-1} It is a bounded error to assign from a bounded list object while tampering with elements [or cursors] of that object is prohibited. Either Program_Error is raised by the assignment, execution proceeds with the target object prohibiting tampering with elements [or cursors], or execution proceeds normally.

Proof: Tampering with elements includes tampering with cursors, so we only really need to talk about tampering with elements here; we mention cursors for clarity.

Erroneous Execution

{AI05-0265-1} When a bounded list object L is finalized, if tampering with cursors is prohibited for L other than due to an assignment from another list, then execution is erroneous.

Reason: This is a tampering event, but since the implementation is not allowed to use Ada.Finalization, it is not possible in a pure Ada implementation to detect this error. (There is no Finalize routine that will be called that could make the check.) Since the check probably cannot be made, the bad effects that could occur (such as an iterator going into an infinite loop or accessing a nonexistent element) cannot be prevented and we have to allow anything. We do allow re-assigning an object that only prohibits tampering because it was copied from another object as that cannot cause any negative effects.

Implementation Requirements

{AI05-0184-1} {AI05-0264-1} For each instance of Containers.Doubly_Linked_Lists and each instance of Containers.Bounded_Doubly_Linked_Lists, if the two instances meet the following conditions, then the output generated by the List'Output or List'Write subprograms of either instance shall be readable by the List'Input or List'Read of the other instance, respectively:

- {AI05-0184-1} {AI05-0248-1} the Element_Type parameters of the two instances are statically matching subtypes of the same type; and
- {AI05-0184-1} the output generated by Element_Type'Output or Element_Type'Write is readable by Element_Type'Input or Element_Type'Read, respectively (where Element_Type denotes the type of the two actual Element_Type parameters).

Implementation Advice

{AI05-0001-1} Bounded list objects should be implemented without implicit pointers or dynamic allocation.

Implementation Advice: Bounded list objects should be implemented without implicit pointers or dynamic allocation.

{AI05-0001-1} The implementation advice for procedure Move to minimize copying does not apply.

Implementation Advice: The implementation advice for procedure Move to minimize copying does not apply to bounded lists.
Extensions to Ada 2005

The generic package Containers.Bounded_Doubly_Linked_Lists is new.

Inconsistencies With Ada 2012

Correction: Tampering with elements is now defined to be equivalent to tampering with cursors for bounded containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

Incompatibilities With Ada 2012

Correction: A bounded list now only has Preelaborable_Initialization (abbreviated PI in this note) when the actual for the Element_Type has PI. If an program used a list whose actual Element_Type does not have PI in a context when PI is required (such as a library-level object in a preelaborated unit or as a component of a type with PI), the program would be illegal in Ada 2022 but legal in original Ada 2012. This situation is unlikely, especially as some existing Ada 2012 implementations reject the instance in this case.

A.18.21 The Generic Package Containers.Bounded_Hashed_Maps

The language-defined generic package Containers.Bounded_Hashed_Maps provides a private type Map and a set of operations. It provides the same operations as the package Containers.Hashed_Maps (see A.18.5), with the difference that the maximum storage is bounded.

Static Semantics

The declaration of the generic library package Containers.Bounded_Hashed_Maps has the same contents and semantics as Containers.Hashed_Maps except:

- The aspect pragma Preelaborate is replaced with aspect pragma Pure. Aspect Global is deleted.

- The type Map is declared with discriminants that specify both the capacity (number of elements) and modulus (number of distinct hash values) of the hash table as follows:

  \[
  \text{type Map (Capacity : Count_Type; Modulus : Hash_Type)}\text{ is tagged private...} +
  \]

- The aspect definition for Preelaborable_Initialization for type Map is changed to:

  \[
  \text{Preelaborable Initialization =}
  \]
  \[
  \text{Element_Type'Preelaborable_Initialization and}
  \]
  \[
  \text{Key_Type'Preelaborable_Initialization}
  \]

- The type Map needs finalization if and only if type Key_Type or type Element_Type needs finalization.

  Implementation Note: The type Map cannot depend on package Ada.Finalization unless the element or key type depends on that package. The objects returned from the Iterator and Reference functions probably do depend on package Ada.Finalization. Restricted environments may need to avoid use of those functions and their associated types.

- In function Empty, the postcondition is altered to:

  \[
  \text{Post =>}
  \]
  \[
  \text{Empty'Result.Capacity = Capacity and then}
  \]
  \[
  \text{Empty'Result.Modulus = Default_Modulus (Capacity) and then}
  \]
  \[
  \text{not Tampering_With_Elements_Prohibited (Empty'Result) and then}
  \]
  \[
  \text{not Tampering_With_Cursors_Prohibited (Empty'Result) and then}
  \]
  \[
  \text{Length (Empty'Result) = 0;}
  \]

- The description of Reserve_Capacity is replaced with:
procedure Reserve_Capacity (Container : in out Map;
   Capacity : in  Count_Type);
   with Pre => Capacity <= Container.Capacity
   or else raise Capacity_Error;

This If the specified Capacity is larger than the capacity of Container, then Reserve_Capacity propagates Capacity_Error. Otherwise, the operation has no effect, [other than checking the precondition].

• An additional operation is added immediately following Reserve_Capacity:

    function Default_Modulus (Capacity : Count_Type) return Hash_Type;
    Default_Modulus returns an implementation-defined value for the number of distinct hash values to be used for the given capacity (maximum number of elements).

• For procedures Insert and Include, the part of the precondition reading:

    (<some length> <= Count_Type'Last - <some other length>
     or else raise Constraint_Error)

is replaced by:

    (<some length> <= Count_Type'Last - <some other length>
     or else raise Constraint_Error) and then
    (some length > Container.Capacity - <some other length>
     or else raise Capacity_Error)

• In procedure Assign, the precondition is altered to:

    Pre => (not Tampering_With_Cursors_Prohibited (Target)
     or else raise Program_Error) and then
    (Length (Source) <= Target.Capacity
     or else raise Capacity_Error),

• The function Copy is replaced with:

    function Copy (Source : Map;
        Capacity : Count_Type := 0;
        Modulus  : Hash_Type := 0) return Map
        with Pre => Capacity = 0 or else Capacity >= Length (Source)
        or else raise Capacity_Error,
        Post =>
        Length (Copy'Result) = Length (Source) and then
        not Tampering_With_Elements_Prohibited (Copy'Result) and then
        not Tampering_With_Cursors_Prohibited (Copy'Result) and then
        Copy'Result.Capacity = (if Capacity = 0 then
        Length (Source) else Capacity) and then
        Copy'Result.Modulus = (if Modulus = 0 then
        Default_Modulus (Capacity) else Modulus),

Returns a map with key/element pairs initialized from the values in Source. If Capacity is 0, then the map capacity is the length of Source; if Capacity is equal to or greater than the length of Source, the map capacity is the value of the Capacity parameter; otherwise, the operation propagates Capacity_Error. If the Modulus argument is 0, then the map modulus is the value returned by a call to Default_Modulus with the map capacity as its argument; otherwise, the map modulus is the value of the Modulus parameter.

Bounded (Run-Time) Errors

It is a bounded error to assign from a bounded map object while tampering with elements [or cursors] of that object is prohibited. Either Program_Error is raised by the assignment, execution proceeds with the target object prohibiting tampering with elements [or cursors], or execution proceeds normally.

Proof: Tampering with elements includes tampering with cursors, so we only really need to talk about tampering with elements here; we mention cursors for clarity.
Erroneous Execution

{AI05-0265-1} When a bounded map object \( M \) is finalized, if tampering with cursors is prohibited for \( M \) other than due to an assignment from another map, then execution is erroneous.

Reason: This is a tampering event, but since the implementation is not allowed to use Ada.Finalization, it is not possible in a pure Ada implementation to detect this error. (There is no Finalize routine that will be called that could make the check.) Since the check probably cannot be made, the bad effects that could occur (such as an iterator going into an infinite loop or accessing a nonexistent element) cannot be prevented and we have to allow anything. We do allow re-assigning an object that only prohibits tampering because it was copied from another object as that cannot cause any negative effects.

Implementation Requirements

{AI05-0184-1} {AI05-0264-1} For each instance of Containers.Hashed_Maps and each instance of Containers.Bounded_Hashed_Maps, if the two instances meet the following conditions, then the output generated by the Map'Output or Map'Write subprograms of either instance shall be readable by the Map'Input or Map'Read of the other instance, respectively:

- {AI05-0184-1} {AI05-0248-1} the Element_Type parameters of the two instances are statically matching subtypes of the same type; and
- {AI05-0184-1} the output generated by Element_Type'Output or Element_Type'Write is readable by Element_Type'Input or Element_Type'Read, respectively (where Element_Type denotes the type of the two actual Element_Type parameters); and
- {AI05-0184-1} the preceding two conditions also hold for the Key_Type parameters of the instances.

Implementation Advice

{AI05-0001-1} {AI05-0269-1} Bounded hashed map objects should be implemented without implicit pointers or dynamic allocation.

Implementation Advice: Bounded hashed map objects should be implemented without implicit pointers or dynamic allocation.

{AI05-0001-1} The implementation advice for procedure Move to minimize copying does not apply.

Implementation Advice: The implementation advice for procedure Move to minimize copying does not apply to bounded hashed maps.

Extensions to Ada 2005

{AI05-0001-1} {AI05-0160-1} {AI05-0184-1} The generic package Containers.Bounded_Hashed_Maps is new.

Inconsistencies With Ada 2012

{AI12-0111-1} Correction: Tampering with elements is now defined to be equivalent to tampering with cursors for bounded containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

Incompatibilities With Ada 2012

{AI12-0409-1} Correction: A bounded map now only has Preelaborable_Initialization (abbreviated PI in this note) when the actuals for the Element_Type and the Key_Type have PI. If an program used a map whose actual Element_Type or Key_Type does not have PI in a context when PI is required (such as a library-level object in a preelaborated unit or as a component of a type with PI), the program would be illegal in Ada 2022 but legal in original Ada 2012. This situation is unlikely, especially as some existing Ada 2012 implementations reject the instance in this case.

The language-defined generic package Containers.Bounded.Ordered.Maps provides a private type Map and a set of operations. It provides the same operations as the package Containers.Ordered.Maps (see A.18.6), with the difference that the maximum storage is bounded.

Static Semantics

The declaration of the generic library package Containers.Bounded.Ordered.Maps has the same contents and semantics as Containers.Ordered.Maps except:

- The aspect pragma Preelaborate is replaced with aspect pragma Pure. Aspect Global is deleted.
- The type Map is declared with a discriminant that specifies the capacity (maximum number of elements) as follows:
  ```
  type Map (Capacity : Count_Type) is tagged private...
  ```
- The aspect definition for Preelaborable_Initialization for type Map is changed to:
  ```
  Preelaborable_Initialization =>
    Element_Type'Preelaborable_Initialization
    and
    Key_Type'Preelaborable_Initialization
  ```
- The type Map needs finalization if and only if type Key_Type or type Element_Type needs finalization.

Implementation Note: The type Map cannot depend on package Ada.Finalization unless the element type depends on that package. The objects returned from the Iterator and Reference functions probably do depend on package Ada.Finalization. Restricted environments may need to avoid use of those functions and their associated types.

The function Empty is replaced by:

```ada
function Empty (Capacity : Count_Type := implementation-defined)
return Map
with Post =>
  Empty'Result.Capacity = Capacity
  and then
  not Tampering_With_Elements_Prohibited (Empty'Result)
  and then
  not Tampering_With_Cursors_Prohibited (Empty'Result)
  and then
  Length (Empty'Result) = 0;
```

For procedures Insert and Include, the part of the precondition reading: The allocation of internal storage includes a check that the capacity is not exceeded, and Capacity_Error is raised if this check fails.

is replaced by:

```ada
<some length> <= Count_Type'Last - <some other length>
  or else raise Constraint_Error;
```

In procedure Assign, the precondition is altered to: if Source.length is greater than Target.capacity, then Capacity_Error is propagated.

```ada
Pre => (not Tampering_With_Cursors_Prohibited (Target)
  or else raise Program_Error)
  and then
  (Length (Source) <= Target.Capacity
  or else raise Capacity_Error),
```

The function Copy is replaced with:
function Copy (Source   : Map; Capacity : Count_Type := 0) return Map
  with Pre  => Capacity = 0 or else Capacity >= Length (Source)
  or else raise Capacity_Error,
  Post =>
    Length (Copy'Result) = Length (Source) and then
    not Tampering_With_Elements_Prohibited (Copy'Result) and then
    not Tampering_With_Cursors_Prohibited (Copy'Result) and then
    Copy'Result.Capacity = (if Capacity = 0 then
      Length (Source) else Capacity);

Returns a map with key/element pairs initialized from the values in Source. If
Capacity is 0, then the map capacity is the length of Source; if Capacity is equal to or greater than
the length of Source, the map capacity is the specified value; otherwise, the operation propagates
Capacity_Error.

Bounded (Run-Time) Errors

It is a bounded error to assign from a bounded map object while
tampering with elements [or cursors] of that object is prohibited. Either Program_Error is raised by the
assignment, execution proceeds with the target object prohibiting tampering with elements [or cursors], or
execution proceeds normally.

Proof: Tampering with elements includes tampering with cursors, so we only really need to talk about tampering with
elements here; we mention cursors for clarity.

Erroneous Execution

When a bounded map object M is finalized, if tampering with cursors is prohibited for M
other than due to an assignment from another map, then execution is erroneous.

Reason: This is a tampering event, but since the implementation is not allowed to use Ada.Finalization, it is not
possible in a pure Ada implementation to detect this error. (There is no Finalize routine that will be called that
could make the check.) Since the check probably cannot be made, the bad effects that could occur (such as an iterator going
into an infinite loop or accessing a nonexistent element) cannot be prevented and we have to allow anything. We do
allow re-assigning an object that only prohibits tampering because it was copied from another object as that cannot
cause any negative effects.

Implementation Requirements

For each instance of Containers.Ordered_Maps and each instance of
Containers.Bounded_Ordered_Maps, if the two instances meet the following conditions, then the output
generated by the Map'Output or Map'Write subprograms of either instance shall be readable by the
Map'Input or Map'Read of the other instance, respectively:

• the Element_Type parameters of the two instances are statically
  matching subtypes of the same type; and

• the output generated by Element_Type'Output or Element_Type'Write is readable
  by Element_Type'Input or Element_Type'Read, respectively (where Element_Type denotes the
type of the two actual Element_Type parameters); and

• the preceding two conditions also hold for the Key_Type parameters of the
  instances.

Implementation Advice

Bounded ordered map objects should be implemented without implicit
pointers or dynamic allocation.

Implementation Advice: Bounded ordered map objects should be implemented without implicit pointers or dynamic
allocation.
The implementation advice for procedure Move to minimize copying does not apply.

Implementation Advice: The implementation advice for procedure Move to minimize copying does not apply to bounded ordered maps.

Extensions to Ada 2005


Inconsistencies With Ada 2012

Correction: Tampering with elements is now defined to be equivalent to tampering with cursors for bounded containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

A.18.23 The Generic Package Containers.Bounded_Hashed_Sets

The language-defined generic package Containers.Bounded_Hashed_Sets provides a private type Set and a set of operations. It provides the same operations as the package Containers.Hashed_Sets (see A.18.8), with the difference that the maximum storage is bounded.

Static Semantics

The declaration of the generic library package Containers.Bounded_Hashed_Sets has the same contents and semantics as Containers.Hashed_Sets except:

- The aspect pragma Preelaborate is replaced with aspect pragma Pure. Aspect Global is deleted.
- The type Set is declared with discriminants that specify both the capacity (number of elements) and modulus (number of distinct hash values) of the hash table as follows:

  ```
  type Set (Capacity : Count_Type;
   Modulus  : Hash_Type) is tagged private
  ...;
  ```

- The aspect_definition for Preelaborable_Initialization for type Set is changed to:

  ```
  Preelaborable_Initialization =>
  Element_Type'Preelaborable_Initialization
  ```

- The type Set needs finalization if and only if type Element_Type needs finalization.

  Implementation Note: The type Set cannot depend on package Ada.Finalization unless the element or key type depends on that package. The objects returned from the Iterator and Reference functions probably do depend on package Ada.Finalization. Restricted environments may need to avoid use of those functions and their associated types.

  In function Empty, the postcondition is altered to:

  ```
  Post =>
  Empty'Result.Capacity = Capacity and then
  Empty'Result.Modulus = Default_Modulus (Capacity) and then
  not Tampering_With_Cursors_Prohibited (Empty'Result) and then
  Length (Empty'Result) = 0;
  ```

- The description of Reserve_Capacity is replaced with:
procedure Reserve_Capacity (Container : in out Set; Capacity : in Count_Type) with Pre => Capacity <= Container.Capacity or else raise Capacity_Error;

This if the specified Capacity is larger than the capacity of Container, then Reserve_Capacity propagates Capacity_Error. Otherwise, the operation has no effect, [other than checking the precondition].

- An additional operation is added immediately following Reserve_Capacity:
  function Default_Modulus (Capacity : Count_Type) return Hash_Type;
  Default_Modulus returns an implementation-defined value for the number of distinct hash values to be used for the given capacity (maximum number of elements).
- For procedures Insert and Include, the part of the precondition reading:
  (<some length> <= Count_Type'Last - <some other length> or else raise Constraint_Error)
is replaced by:
  (<some length> <= Count_Type'Last - <some other length> or else raise Constraint_Error) and then
  (<some length> <= Container.Capacity - <some other length> or else raise Capacity_Error).
- In procedure Assign, the precondition is altered to:
  Pre => (not Tampering_With_Cursors_Prohibited (Target) or else raise Program_Error) and then
  (Length (Source) <= Target.Capacity or else raise Capacity_Error),
- The function Copy is replaced with:
  function Copy (Source : Set; Capacity : Count_Type := 0; Modulus : Hash_Type := 0) return Map with Pre => Capacity = 0 or else Capacity >= Length (Source) or else raise Capacity_Error,
  Post =>
  Length (Copy'Result) = Length (Source) and then
  not Tampering_With_Cursors_Prohibited (Copy'Result) and then
  Copy'Result.Capacity = (if Capacity = 0 then
  Length (Source) else Capacity) and then
  Copy'Result.Modulus = (if Modulus = 0 then
  Default_Modulus (Capacity) else Modulus);
  Returns a set with key/element pairs initialized from the values in Source. If Capacity is 0, then the set capacity is the length of Source; if Capacity is equal to or greater than the length of Source, the set capacity is the value of the Capacity parameter; otherwise, the operation propagates Capacity_Error. If the Modulus argument is 0, then the set modulus is the value returned by a call to Default_Modulus with the set capacity as its argument; otherwise, the set modulus is the value of the Modulus parameter.

Bounded (Run-Time) Errors

It is a bounded error to assign from a bounded set object while tampering with elements [or cursors] of that object is prohibited. Either Program Error is raised by the assignment, execution proceeds with the target object prohibiting tampering with elements [or cursors], or execution proceeds normally.

Proof: Tampering with elements includes tampering with cursors, so we only really need to talk about tampering with elements here; we mention cursors for clarity.
Erroneous Execution

When a bounded set object S is finalized, if tampering with cursors is prohibited for S other than due to an assignment from another set, then execution is erroneous.

Reason: This is a tampering event, but since the implementation is not allowed to use Ada.Finalization, it is not possible in a pure Ada implementation to detect this error. (There is no Finalize routine that will be called that could make the check.) Since the check probably cannot be made, the bad effects that could occur (such as an iterator going into an infinite loop or accessing a nonexistent element) cannot be prevented and we have to allow anything. We do allow re-assigning an object that only prohibits tampering because it was copied from another object as that cannot cause any negative effects.

Implementation Requirements

For each instance of Containers.Hashed_Sets and each instance of Containers.Bounded_Hashed_Sets, if the two instances meet the following conditions, then the output generated by the Set'Output or Set'Write subprograms of either instance shall be readable by the Set'Input or Set'Read of the other instance, respectively:

- the Element_Type parameters of the two instances are statically matching subtypes of the same type; and
- the output generated by Element_Type'Output or Element_Type'Write is readable by Element_Type'Input or Element_Type'Read, respectively (where Element_Type denotes the type of the two actual Element_Type parameters).

Implementation Advice

Bounded hashed set objects should be implemented without implicit pointers or dynamic allocation.

The implementation advice for procedure Move to minimize copying does not apply.

The implementation advice for procedure Move to minimize copying does not apply to bounded hashed sets.

Extensions to Ada 2005

The generic package Containers.Bounded_Hashed_Sets is new.

Incompatibilities With Ada 2012

Correction: A bounded set now only has Preelaborable_Initialization (abbreviated PI in this note) when the actual for the Element_Type has PI. If an program used a set whose actual Element_Type does not have PI in a context where PI is required (such as a library-level object in a preelaborated unit or as a component of a type with PI), the program would be illegal in Ada 2022 but legal in original Ada 2012. This situation is unlikely, especially as some existing Ada 2012 implementations reject the instance in this case.

A.18.24 The Generic Package Containers.Bounded_Ordered_Sets

The language-defined generic package Containers.Bounded_Ordered_Sets provides a private type and a set of operations. It provides the same operations as the package Containers.Ordered_Sets (see A.18.9), with the difference that the maximum storage is bounded.

Static Semantics

The declaration of the generic library package Containers.Bounded_Ordered_Sets has the same contents and semantics as Containers.Ordered_Sets except:

- The aspect pragma Preelaborate is replaced with aspect pragma Pure. Aspect Global is deleted.
• The type Set is declared with a discriminant that specifies the capacity (maximum number of elements) as follows:

  \[\{AI12-0112-1\} \quad \textbf{type} \ Set \ (\text{Capacity} : \text{Count_Type}) \textbf{is tagged private} \ldots\]

• \[\{AI12-0409-1\} \quad \textbf{The aspect definition for Preelaborable Initialization for type Set is changed to:}\]

  Preelaborable Initialization =>
  Element_Type'Preelaborable Initialization

• The type Set needs finalization if and only if type Element_Type needs finalization.

  \textbf{Implementation Note:} \[\{AI05-0212-1\} \quad \text{The type Set cannot depend on package Ada.Finalization unless the element type depends on that package. The objects returned from the Iterator and Reference functions probably do depend on package Ada.Finalization. Restricted environments may need to avoid use of those functions and their associated types.}\]

• \[\{AI12-0339-1\} \quad \textbf{The function Empty is replaced by:}\]

  \[\quad \textbf{function} \ Empty \ (\text{Capacity} : \text{Count_Type} := \text{implementation-defined}) \]
  \[\quad \textbf{return} \ Set \quad \textbf{with} \quad \textbf{Post} \Rightarrow \]
  \[\quad \text{Empty'Result.Capacity} = \text{Capacity} \quad \text{and then} \]
  \[\quad \text{not } \text{Tampering With Cursors Prohibited} \ (\text{Empty'Result}) \quad \text{and then} \]
  \[\quad \text{Length} \ (\text{Empty'Result}) = 0;\]

• \[\{AI12-0112-1\} \quad \textbf{For procedures Insert and Include, the part of the precondition reading if Insert (or Include) adds an element, a check is made that the capacity is not exceeded, and Capacity_Error is raised if this check fails.}\]

  \[\quad (\langle \text{some length} \rangle \leq \text{Count_Type}'\text{Last} - \langle \text{some other length} \rangle \]
  \[\quad \text{or else raise Constraint_Error});\]

  is replaced by:

  \[\quad (\langle \text{some length} \rangle \leq \text{Count_Type}'\text{Last} - \langle \text{some other length} \rangle \]
  \[\quad \text{or else raise Constraint_Error}) \quad \text{and then} \]
  \[\quad (\langle \text{some length} \rangle \leq \text{Container.Capacity} - \langle \text{some other length} \rangle \]
  \[\quad \text{or else raise Capacity_Error});\]

• \[\{AI12-0112-1\} \quad \textbf{In procedure Assign, the precondition is altered to: if Source length is greater than Target capacity, then Capacity_Error is propagated.}\]

  \[\quad \text{Pre} \Rightarrow \ (\text{not} \ \text{Tampering With Cursors Prohibited} \ (\text{Target}) \]
  \[\quad \text{or else raise Program_Error}) \quad \text{and then} \]
  \[\quad (\text{Length} \ (\text{Source}) \leq \text{Target.Capacity} \]
  \[\quad \text{or else raise Capacity_Error});\]

• The function Copy is replaced with:

  \[\{AI12-0112-1\} \quad \textbf{function} \ Copy \ (\text{Source} : \text{Set}; \]
  \[\quad \text{Capacity} : \text{Count_Type} := 0) \textbf{return} \text{Map} \]
  \[\quad \textbf{with} \quad \textbf{Pre} \Rightarrow \ (\text{Capacity} = 0 \quad \text{or else} \quad \text{Capacity} \geq \text{Length} \ (\text{Source}) \]
  \[\quad \text{or else raise Capacity_Error}, \]
  \[\quad \textbf{Post} \Rightarrow \]
  \[\quad \text{Length} \ (\text{Copy'Result}) = \text{Length} \ (\text{Source}) \quad \text{and then} \]
  \[\quad \text{not} \ \text{Tampering With Cursors Prohibited} \ (\text{Copy'Result}) \quad \text{and then} \]
  \[\quad \text{Copy'Result.Capacity} = (\text{if} \ \text{Capacity} = 0 \quad \text{then} \]
  \[\quad \text{Length} \ (\text{Source}) \quad \text{else} \quad \text{Capacity});\]

• \[\{AI12-0112-1\} \quad \textbf{Returns a set with key/element pairs initialized from the values in Source. If Capacity is 0, then the set capacity is the length of Source; if Capacity is equal to or greater than the length of Source, the set capacity is the specified value; otherwise, the operation propagates Capacity_Error.}\]

\textit{Bounded (Run-Time) Errors}

\[\{AI05-0160-1\} \quad \{AI05-0265-1\} \quad \text{It is a bounded error to assign from a bounded set object while tampering with elements [or cursors] of that object is prohibited. Either Program_Error is raised by the assignment, execution proceeds with the target object prohibiting tampering with elements [or cursors], or execution proceeds normally.}\]
Proof: Tampering with elements includes tampering with cursors, so we only really need to talk about tampering with elements here; we mention cursors for clarity.

Erroneous Execution

When a bounded set object $S$ is finalized, if tampering with cursors is prohibited for $S$ other than due to an assignment from another set, then execution is erroneous.

Reason: This is a tampering event, but since the implementation is not allowed to use Ada.Finalization, it is not possible in a pure Ada implementation to detect this error. (There is no Finalize routine that will be called that could make the check.) Since the check probably cannot be made, the bad effects that could occur (such as an iterator going into an infinite loop or accessing a nonexistent element) cannot be prevented and we have to allow anything. We do allow re-assigning an object that only prohibits tampering because it was copied from another object as that cannot cause any negative effects.

Implementation Requirements

For each instance of Containers.Ordered_Sets and each instance of Containers.Bounded_Ordered_Sets, if the two instances meet the following conditions, then the output generated by the Set'Output or Set'Write subprograms of either instance shall be readable by the Set'Input or Set'Read of the other instance, respectively:

- the Element_Type parameters of the two instances are statically matching subtypes of the same type; and

- the output generated by Element_Type'Output or Element_Type'Write is readable by Element_Type'Input or Element_Type'Read, respectively (where Element_Type denotes the type of the two actual Element_Type parameters).

Implementation Advice

Bounded ordered set objects should be implemented without implicit pointers or dynamic allocation.

Implementation Advice: Bounded ordered set objects should be implemented without implicit pointers or dynamic allocation.

The implementation advice for procedure Move to minimize copying does not apply.

Implementation Advice: The implementation advice for procedure Move to minimize copying does not apply to bounded ordered sets.

Extensions to Ada 2005

The generic package Containers.Bounded_Ordered_Sets is new.

Incompatibilities With Ada 2012

Correction: A bounded set now only has Preelaborable_Initialization (abbreviated PI in this note) when the actual for the Element_Type has PI. If an program used a set whose actual Element_Type does not have PI in a context when PI is required (such as a library-level object in a preelaborated unit or as a component of a type with PI), the program would be illegal in Ada 2022 but legal in original Ada 2012. This situation is unlikely, especially as some existing Ada 2012 implementations reject the instance in this case.

A.18.25 The Generic Package Containers.Bounded_Multiway_Trees

The language-defined generic package Containers.Bounded_Multiway_Trees provides a private type Tree and a set of operations. It provides the same operations as the package Containers.Multiway_Trees (see A.18.10), with the difference that the maximum storage is bounded.

Static Semantics

{AI05-0136-1} The declaration of the generic library package Containers.Bounded_Multiway_Trees has the same contents and semantics as Containers.Multiway_Trees except:

• {AI12-0112-1} The aspect pragma Preelaborate is replaced with aspect pragma Pure. Aspect Global is deleted.

• The type Tree is declared with a discriminant that specifies the capacity (maximum number of elements) as follows:

{AI12-0112-1} type Tree (Capacity : Count_Type) is tagged private...

• {AI12-0409-1} The aspect_definition for Preelaborable_Initialization for type Tree is changed to:

```
Preelaborable_Initialization =>
  Element_Type'Preelaborable_Initialization
```

• The type Tree needs finalization if and only if type Element_Type needs finalization.

Implementation Note: {AI05-0212-1} The type Tree cannot depend on package Ada.Finalization unless the element type depends on that package. The objects returned from the Iterator and Reference functions probably do depend on package Ada.Finalization. Restricted environments may need to avoid use of those functions and their associated types.

• {AI12-0339-1} The function Empty is replaced by:

```
function Empty (Capacity : Count_Type := implementation-defined)
return Tree with Post =>
  Empty'Result.Capacity = Capacity and then
  not Tampering With Elements Prohibited (Empty'Result) and then
  not Tampering With Cursors Prohibited (Empty'Result) and then
  Node_Count (Empty'Result) = 1;
```

• {AI12-0112-1} For procedures Insert_Child, Prepend_Child, and Append_Child, the initial subexpression of the precondition is replaced with The allocation of internal storage includes a check that the capacity is not exceeded, and Capacity_Error is raised if this check fails.

```
with Pre => (not Tampering With Cursors Prohibited (Container)
  or else raise Program_Error)
and then
(Node_Count (Container) - 1 <= Container.Capacity - Count
  or else raise Capacity_Error),
```

• {AI12-0112-1} In procedure Assign, the precondition is altered to: if Source length is greater than Target capacity, then Capacity_Error is propagated.

```
Pre => (not Tampering With Cursors Prohibited (Target)
  or else raise Program_Error)
and then
(Node_Count (Source) - 1 <= Target.Capacity
  or else raise Capacity_Error),
```

• Function Copy is declared as follows:

{AI12-0056-1} function Copy (Source : Tree; Capacity : Count_Type := 0)
return TreeList
with Pre => Capacity = 0 or else Capacity >= Node_Count (Source) - 1
  or else raise Capacity_Error,
Post =>
  Node_Count (Copy'Result) = Node_Count (Source) and then
  not Tampering With Elements Prohibited (Copy'Result) and then
  not Tampering With Cursors Prohibited (Copy'Result) and then
  Copy'Result.Capacity = (if Capacity = 0 then
    Node_Count (Source) - 1 else Capacity);
• \{AI12-0112-1\} In the four-parameter procedure Copy_Subtree, the last or else of the precondition is replaced by:

```
(not Is_Root (Source) or else raise Constraint_Error) and then
(Node_Count (Target) - 1 + Subtree_Node_Count (Source) <= Target.Capacity or else raise Capacity_Error),
```

• \{AI12-0112-1\} In the five-parameter procedure Copy_Subtree, the last or else of the precondition is replaced by:

```
(not Is_Root (Source, Subtree) or else raise Constraint_Error) and then
(Node_Count (Target) - 1 + Subtree_Node_Count (Source, Subtree) <= Target.Capacity or else raise Capacity_Error),
```

• \{AI12-0112-1\} In Copy_Local_Subtree, the last or else of the precondition is replaced by:

```
(not Is_Root (Source, Subtree) or else raise Constraint_Error) and then
(Node_Count (Target) - 1 + Subtree_Node_Count (Target, Source) <= Target.Capacity or else raise Capacity_Error),
```

• \{AI05-0136-1\} \{AI05-0248-1\} \{AI12-0112-1\} In the five-parameter procedure Splice_Subtree, the penultimate or else of the precondition is replaced by: if Source is not the same object as Target, and if the sum of Target.Count and Subtree_Node_Count (Position) is greater than Target.Capacity, then Splice_Subtree propagates Capacity_Error.

```
(Has_Element (Source, Position) or else raise Program_Error) and then
(Target'Has_Same_Storage (Source) or else
 Node_Count (Target) - 1 + Subtree_Node_Count (Target, Source) <= Target.Capacity or else raise Capacity_Error) and then
```

• \{AI05-0136-1\} \{AI05-0248-1\} \{AI12-0112-1\} In the five-parameter procedure Splice_Children, the penultimate elsif of the precondition is replaced by: if Source is not the same object as Target, and if the sum of Target.Count and Subtree_Node_Count (Source_Parent) - 1 is greater than Target.Capacity, then Splice_Children propagates Capacity_Error.

```
@Before = No_Element or else
 Parent (Target, Before) /= Target_Parent
 or else raise Constraint_Error) and then
 (Target'Has_Same_Storage (Source) or else
 Node_Count (Target) - 1 + Child_Count (Source, Source_Parent) <= Target.Capacity or else raise Capacity_Error) and then
```

**Bounded (Run-Time) Errors**

\{AI05-0160-1\} \{AI05-0265-1\} It is a bounded error to assign from a bounded tree object while tampering with elements [or cursors] of that object is prohibited. Either Program_Error is raised by the assignment, execution proceeds with the target object prohibiting tampering with elements [or cursors], or execution proceeds normally.

Proof: Tampering with elements includes tampering with cursors, so we only really need to talk about tampering with elements here; we mention cursors for clarity.

**Erroneous Execution**

\{AI05-0265-1\} When a bounded tree object \(T\) is finalized, if tampering with cursors is prohibited for \(T\) other than due to an assignment from another tree, then execution is erroneous.

Reason: This is a tampering event, but since the implementation is not allowed to use Ada.Finalization, it is not possible in a pure Ada implementation to detect this error. (There is no Finalize routine that will be called that could
make the check.) Since the check probably cannot be made, the bad effects that could occur (such as an iterator going into an infinite loop or accessing a nonexistent element) cannot be prevented and we have to allow anything. We do allow re-assigning an object that only prohibits tampering because it was copied from another object as that cannot cause any negative effects.

**Implementation Requirements**

{AI05-0184-1} {AI05-0264-1} For each instance of Containers.Multiway_Trees and each instance of Containers.Bounded_Multiway_Trees, if the two instances meet the following conditions, then the output generated by the Tree'Output or Tree'Write subprograms of either instance shall be readable by the Tree'Input or Tree'Read of the other instance, respectively:

- {AI05-0184-1} {AI05-0248-1} the Element_Type parameters of the two instances are statically matching subtypes of the same type; and
- {AI05-0184-1} the output generated by Element_Type'Output or Element_Type'Write is readable by Element_Type'Input or Element_Type'Read, respectively (where Element_Type denotes the type of the two actual Element_Type parameters).

**Implementation Advice**

{AI05-0136-1} Bounded tree objects should be implemented without implicit pointers or dynamic allocation.

**Implementation Advice:** Bounded tree objects should be implemented without implicit pointers or dynamic allocation.

{AI05-0136-1} The implementation advice for procedure Move to minimize copying does not apply.

**Implementation Advice:** The implementation advice for procedure Move to minimize copying does not apply to bounded trees.

**Extensions to Ada 2005**

{AI05-0136-1} {AI05-0184-1} The generic package Containers.Bounded_Multiway_Trees is new.

**Inconsistencies With Ada 2012**

{AI12-0111-1} Correction: Tampering with elements is now defined to be equivalent to tampering with cursors for bounded containers. If a program requires tampering detection to work, it might fail in Ada 2022. Needless to say, this shouldn't happen outside of test programs. See Inconsistencies With Ada 2012 in A.18.2 for more details.

**Incompatibilities With Ada 2012**

{AI12-0409-1} Correction: A bounded tree now only has Preelaborable_Initialization (abbreviated PI in this note) when the actual for the Element_Type has PI. If an program used a tree whose actual Element_Type does not have PI in a context when PI is required (such as a library-level object in a preelaborated unit or as a component of a type with PI), the program would be illegal in Ada 2022 but legal in original Ada 2012. This situation is unlikely, especially as some existing Ada 2012 implementations reject the instance in this case.

**A.18.26 Array Sorting**

{AI95-00302-03} {AI05-0001-1} The language-defined generic procedures Containers.Generic_Array_Sort and Containers.Generic_Constrained_Array_Sort provide sorting on arbitrary array types.
The generic library procedure Containers.Generic Array Sort has the following declaration:

```ada
generic
    type Index_Type is (<>);
    type Element_Type is private;
    type Array_Type is array (Index_Type range <>) of Element_Type;
with function "<" (Left, Right : Element_Type) return Boolean is <>;
procedure Ada.Containers.Generic_Array_Sort (Container : in out Array_Type);
```

Discussion: Global => null means that the only global side-effects allowed are associated with the actual generic parameters. Similarly, when Nonblocking is set to True for a generic unit, the only blocking allowed is that associated with the actual generic parameters.

Reorders the elements of Container such that the elements are sorted smallest first as determined by the generic formal "<" operator provided. Any exception raised during evaluation of "<" is propagated.

The actual function for the generic formal function "<" of Generic_Array_Sort is expected to return the same value each time it is called with a particular pair of element values. It should define a strict weak ordering relationship (see A.18), that is, be irreflexive, asymmetric, and transitive; it should not modify Container. If the actual for "<" behaves in some other manner, the behavior of the instance of Generic_Array_Sort is unspecified. The number of how many times Generic_Array_Sort calls "<" is unspecified.

Ramification: This implies swapping the elements, usually including an intermediate copy. This of course means that the elements will be copied. Since the elements are nonlimited, this usually will not be a problem. Note that there is Implementation Advice below that the implementation should use a sort that minimizes copying of elements.

The sort is not required to be stable (and the fast algorithm required will not be stable). If a stable sort is needed, the user can include the original location of the element as an extra "sort key". We considered requiring the implementation to do that, but it is mostly extra overhead -- usually there is something already in the element that provides the needed stability.

The generic library procedure Containers.Generic Constrained Array Sort has the following declaration:

```ada
generic
    type Index_Type is (<>);
    type Element_Type is private;
    type Array_Type is array (Index_Type) of Element_Type;
with function "<" (Left, Right : Element_Type) return Boolean is <>;
procedure Ada.Containers.Generic_Constrained_Array_Sort (Container : in out Array_Type);
```

Discussion: Global => null means that the only global side-effects allowed are associated with the actual generic parameters. Similarly, when Nonblocking is set to True for a generic unit, the only blocking allowed is that associated with the actual generic parameters.

Reorders the elements of Container such that the elements are sorted smallest first as determined by the generic formal "<" operator provided. Any exception raised during evaluation of "<" is propagated.

The actual function for the generic formal function "<" of Generic_Constrained_Array_Sort is expected to return the same value each time it is called with a particular pair of element values. It should define a strict weak ordering relationship (see A.18), that is, be irreflexive, asymmetric, and transitive; it should not modify Container. If the actual for
"<" behaves in some other manner, the behavior of the instance of Generic Constrained Array Sort is unspecified. The number of How many times Generic Constrained Array Sort calls "<" is unspecified.

{AI05-0001-1} The generic library procedure Containers.Generic_Sort has the following declaration:

```ada
generic
  type Index_Type is <>;
  with function Before (Left, Right : Index_Type) return Boolean;
  with procedure Swap (Left, Right : in Index_Type);
procedure Ada.Containers.Generic_Sort (First, Last : Index_Type'Base)
  with Pure, Nonblocking, Global => nullpragma Pure(Ada.Containers.Generic_Sort);
```

Discussion: Global => null means that the only global side-effects allowed are associated with the actual generic parameters. Similarly, when Nonblocking is set to True for a generic unit, the only blocking allowed is that associated with the actual generic parameters.

{AI05-0001-1} {AI05-0248-1} Reorders the elements of an indexable structure, over the range First .. Last, such that the elements are sorted in the ordering determined by the generic formal function Before; Before should return True if Left is to be sorted before Right. The generic formal Before compares the elements having the given indices, and the generic formal Swap exchanges the values of the indicated elements. Any exception raised during evaluation of Before or Swap is propagated.

The actual function for the generic formal function Before of Generic_Sort is expected to return the same value each time it is called with index values that identify a particular pair of element values. It should define a strict weak ordering relationship (see A.18); it should not modify the elements. The actual function for the generic formal Swap should exchange the values of the indicated elements. If the actual for either Before or Swap behaves in some other manner, the behavior of Generic_Sort is unspecified. The number of times the Generic_Sort calls Before or Swap is unspecified.

**Implementation Advice**

{AI95-00302-03} The worst-case time complexity of a call on an instance of Containers.Generic_Array_Sort or Containers.Generic_Constrained_Array_Sort should be $O(N^2)$ or better, and the average time complexity should be better than $O(N^2)$, where $N$ is the length of the Container parameter.

**Implementation Advice:** Containers.Generic_Array_Sort and Containers.Generic_Constrained_Array_Sort should have an average time complexity better than $O(N^2)$ and worst case no worse than $O(N^2)$.

**Discussion:** In other words, we're requiring the use of a sorting algorithm better than $O(N^2)$, such as Quicksort. No bubble sorts allowed!

{AI95-00302-03} Containers.Generic_Array_Sort and Containers.Generic_Constrained_Array_Sort should minimize copying of elements.

**Implementation Advice:** Containers.Generic_Array_Sort and Containers.Generic_Constrained_Array_Sort should minimize copying of elements.

**To be honest:** We do not mean “absolutely minimize” here; we're not intending to require a single copy for each element. Rather, we want to suggest that the sorting algorithm chosen is one that does not copy items unnecessarily. Bubble sort would not meet this advice, for instance.

{AI05-0248-1} The worst-case time complexity of a call on an instance of Containers.Generic_Sort should be $O(N^2)$ or better, and the average time complexity should be better than $O(N^2)$, where $N$ is the difference between the Last and First parameters plus 1.

**Implementation Advice:** Containers.Generic_Sort should have an average time complexity better than $O(N^2)$ and worst case no worse than $O(N^2)$. 
Implementation Advice: Containers.Generic_Sort should minimize calls to the generic formal Swap.

Extensions to Ada 95

The generic procedures Containers.Generic_Array_Sort and Containers.Generic_Constrained_Array_Sort are new.

Extensions to Ada 2005

The generic procedure Containers.Generic_Sort is new.

Wording Changes from Ada 2005

Correction: Redefined "<" actuals to require a strict weak ordering; the old definition allowed indeterminant comparisons that would not have worked in a sort.

Wording Changes from Ada 2012

Added contracts to these procedures.

A.18.27 The Generic Package Containers.Synchronized_Queue_Interfaces

The language-defined generic package Containers.Synchronized_Queue_Interfaces provides interface type Queue, and a set of operations for that type. Interface Queue specifies a first-in, first-out queue.

Static Semantics

The generic library package Containers.Synchronized_Queue_Interfaces has the following declaration:

generic
__type Element_Type is private;
package Ada.Containers.Synchronized_Queue_Interfaces is
with Pure, Nonblocking, Global => null is
pragma Pure(Synchronized_Queue_Interfaces);

Discussion: Global => null means that the only global side-effects allowed are associated with the actual generic parameters. Similarly, when Nonblocking is set to True for a generic unit, the only blocking allowed is that associated with the actual generic parameters.

type Queue is synchronized interface;

procedure Enqueue (Container : in out Queue;
                   New_Item  : in  Element_Type) is abstract
with Synchronization => By Entry,
Nonblocking => False,
Global'Class=> in out synchronized;

procedure Dequeue (Container : in out Queue;
                   Element   : out  Element_Type) is abstract
with Synchronization => By Entry,
Nonblocking => False,
Global'Class=> in out synchronized;

function Current_Use (Container : Queue) return Count_Type is abstract
with Nonblocking, Global'Class => null, Use Formal => null;
function Peak_Use (Container : Queue) return Count_Type is abstract
with Nonblocking, Global'Class => null, Use Formal => null,
Post'Class => Peak Use'Result => Current_Use (Container);

end Ada.Containers.Synchronized_Queue_Interfaces;
The subprogram behavior descriptions given below are the semantics for the corresponding callable entities found in the language-defined generic packages that have a formal package named Queue_Interfaces.

procedure Enqueue
(Container : in out Queue;
 New Item : in Element_Type) is abstract
with Synchronization => By_Entry
 Nonblocking => False,
 Global'Class=> in out synchronized;

A queue type that implements this interface is allowed to have a bounded capacity. If the queue object has a bounded capacity, and the number of existing elements equals the capacity, then Enqueue blocks until storage becomes available; otherwise, Enqueue does not block. In any case, it then copies New_Item onto the queue.

procedure Dequeue
(Container : in out Queue;
 Element   : out Element_Type) is abstract
with Synchronization => By_Entry
 Nonblocking => False,
 Global'Class=> in out synchronized;

If the queue is empty, then Dequeue blocks until an item becomes available. In any case, it then assigns the element at the head of the queue to Element, and removes it from the queue.

function Current_Use (Container : Queue) return Count_Type is abstract
with Nonblocking, Global'Class=> null, Use_Formal => null;

Returns the number of elements currently in the queue.

function Peak_Use (Container : Queue) return Count_Type is abstract
with Nonblocking, Global'Class=> null, Use_Formal => null,
 Post'Class => Peak_Use'Result => Current_Use (Container);

Returns the maximum number of elements that have been in the queue at any one time.

NOTE Unlike other language-defined containers, there are no queues whose element types are indefinite. Elements of an indefinite type can be handled by defining the element of the queue to be a holder container (see A.18.18) of the indefinite type, or to be an explicit access type that designates the indefinite type.

Reason: There are no indefinite queues, as a useful definition for Dequeue is not possible. Dequeue cannot be a function, as Ada does not have entries that are functions (thus conditional and timed calls would not be possible). Moreover, protected functions do not allow modifying the queue object (thus it doesn't work even if we decided we didn't care about conditional and timed calls). If Dequeue is an entry, then the dequeued object would have to be an out parameter and that would require the queue client to guess the tag and constraints of the value that will be dequeued (otherwise Constraint_Error would be raised), and that is rarely going to be possible.

Extensions to Ada 2005

The generic package Containers.Synchronized_Queue_Interfaces is new.

A.18.28 The Generic Package Containers.Unbounded_Synchronized_Queues

Static Semantics

The language-defined generic package Containers.Unbounded_Synchronized_Queues provides type Queue, which implements the interface type Containers.Synchronized_Queue_Interface.Queue.
with System;
with Ada.Containers.Synchronized_Queue_Interfaces;
generic
   with package Queue_Interfaces is
   new Ada.Containers.Synchronized_Queue_Interfaces (<>);
package Ada.Containers.Unbounded_Synchronized_Queues is
   with Preelaborate,
   Nonblocking, Global => in out synchronized is
   pragma Preelaborate(Unbounded_Synchronized_Queues);

Discussion: {AI12-0112-1} For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects of this generic package, see the notes on the specification of the Containers.Vectors package (see A.18.2).

package Implementation is
   ... -- not specified by the language
end Implementation;

protected type Queue
   (Ceiling : System.Any_Priority := Default_Ceiling)
   with Priority => Ceiling
   is
      new Queue_Interfaces.Queue
      with
      overriding
      entry Enqueue (New_Item : in Queue_Interfaces.Element_Type);
      overriding
      entry Dequeue (Element : out Queue_Interfaces.Element_Type);

      {AI12-0112-1} overriding
      function Current_Use return Count_Type
      with Nonblocking, Global => null, Use_Formal => null;
      overriding
      function Peak_Use return Count_Type
      with Nonblocking, Global => null, Use_Formal => null;

private
   ... -- not specified by the language
end Queue;

private
   ... -- not specified by the language
end Ada.Containers.Unbounded_Synchronized_Queues;

{AI105-0159-1} The type Queue is used to represent task-safe queues.

{AI105-0159-1} The capacity for instances of type Queue is unbounded.

Ramification: Enqueue never blocks; if more storage is needed for a new element, it is allocated dynamically. We don’t need to explicitly specify that Queue needs finalization, because it is visibly protected.

Discussion: Nested package Implementation can be used to declare the types needed to implement the protected type Queue. This nested package is necessary as types cannot be declared in the private part of a protected type, and the types have to be declared within the generic unit in order to depend on the types imported with package Queue_Interfaces. Clients should never depend on the contents of nested package Implementation.

 Extensions to Ada 2005

A.18.29 The Generic Package Containers.Bounded_Synchronized_Queues

Static Semantics

{AI105-0159-1} The language-defined generic package Containers.Bounded_Synchronized_Queue provides type Queue, which implements the interface type Containers.Synchronized_Queue_Interfaces.Queue.
{AI12-0112-1} with System;
with Ada.Containers.Synchronized_Queue_Interfaces;
generic
  with package Queue_Interfaces is
  new Ada.Containers.Synchronized_Queue_Interfaces (<>);
  Default Capacity : Count_Type;  
package Ada.Containers.Bounded_Synchronized_Queues is
  with Preelaborate,
  Nonblocking, Global => in out synchronized is
  pragma Preelaborate(Bounded_Synchronized_Queue);
Discussion: {AI12-0112-1} For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects of this generic package, see the notes on the specification of the Containers.Vectors package (see A.18.2).
package Implementation is
  ... -- not specified by the language
end Implementation;
protected type Queue
  (Capacity : Count_Type := Default_Capacity;
   Ceiling : System.Any_Priority := Default_Ceiling)
  with Priority => Ceiling is
    new Queue_Interfaces.Queue with
      overriding
      entry Enqueue (New_Item : in Queue_Interfaces.Element_Type);
      overriding
      entry Dequeue (Element : out Queue_Interfaces.Element_Type);
{AI12-0112-1}  overriding
      function Current_Use return Count_Type
        with Nonblocking, Global => null, Use_Formal => null;
      overriding
      function Peak_Use return Count_Type
        with Nonblocking, Global => null, Use_Formal => null;
private
  ... -- not specified by the language
end Queue;
private
  ... -- not specified by the language
end Ada.Containers.Bounded_Synchronized_Queue;
{AI05-0159-1} The semantics are the same as for Unbounded_Synchronized_Queue, except:
The capacity for instances of type Queue is bounded and specified by the discriminant Capacity.
Ramification: Since this type has a bounded capacity, Enqueue might block if the queue is full.
Implementation Advice
{AI05-0159-1} Bounded queue objects should be implemented without implicit pointers or dynamic allocation.
Implementation Advice: Bounded queue objects should be implemented without implicit pointers or dynamic allocation.
Extensions to Ada 2005
{AI05-0159-1} The generic package Containers.Bounded_Synchronized_Queue is new.
A.18.30 The Generic Package Containers.Unbounded_Priority_Queues

Static Semantics

{AI05-0159-1} The language-defined generic package Containers.Unbounded_Priority_Queues provides type Queue, which implements the interface type Containers.Synchronized_Queue_Interfaces.Queue.

{AI12-0112-1} with System;
with Ada.Containers.Synchronized_Queue_Interfaces;
generic
with package Queue_Interfaces is
new Ada.Containers.Synchronized_Queue_Interfaces (<>);
type Queue Priority is private;
with function Get_Priority
(Element : Queue_Interfaces.Element_Type) return Queue_Priority is <>;
with function Before
(Left, Right : Queue Priority) return Boolean is <>;
package Ada.Containers.Unbounded_Priority_Queues is
with Preelaborate,
  Nonblocking, Global => in out synchronized is
pragma Preelaborate(Unbounded_Priority_Queues);

Discussion: {AI12-0112-1} For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects of this generic package, see the notes on the specification of the Containers.Vectors package (see A.18.2).

package Implementation is
  ...
  -- not specified by the language
end Implementation;

protected type Queue
  (Ceiling : System.Any_Priority := Default_Ceiling)
    with Priority => Ceiling is
    new Queue_Interfaces.Queue with

overriding
  entry Enqueue
    (New_Item : in Queue_Interfaces.Element_Type);
  overriding
  entry Dequeue
    (Element : out Queue_Interfaces.Element_Type);

{AI05-0159-1} {AI05-0251-1} not overriding
procedure Dequeue_Only_High_Priority
  (At_Least : in Queue Priority;
  Success : out Boolean);

{AI12-0112-1} overriding
function Current Use return Count_Type
  with Nonblocking, Global => null, Use_Formal => null;
  overriding
function Peak Use return Count_Type
  with Nonblocking, Global => null, Use_Formal => null;

private
  ...
  -- not specified by the language
end Queue;

private
  ...
  -- not specified by the language
end Ada.Containers.Unbounded_Priority_Queues;

{AI05-0159-1} The type Queue is used to represent task-safe priority queues.

{AI05-0159-1} The capacity for instances of type Queue is unbounded.
Two elements \(E_1\) and \(E_2\) are equivalent if \(\text{Before(Get\_Priority(E_1), Get\_Priority(E_2))}\) and \(\text{Before(Get\_Priority(E_2), Get\_Priority(E_1))}\) both return False.

The actual functions for Get\_Priority and Before are expected to return the same value each time they are called with the same actuals, and should not modify their actuals. Before should define a strict weak ordering relationship (see A.18). If the actual functions behave in some other manner, the behavior of Unbounded\_Priority\_Queues is unspecified.

Enqueue inserts an item according to the order specified by the Before function on the result of Get\_Priority on the elements; Before should return True if Left is to be inserted before Right. If the queue already contains elements equivalent to New\_Item, then it is inserted after the existing equivalent elements.

Ramification: Enqueue never blocks; if more storage is needed for a new element, it is allocated dynamically. We don't need to explicitly specify that Queue needs finalization, because it is visibly protected.

For a call on Dequeue\_Only\_High\_Priority, if the head of the nonempty queue is \(E\), and the function \(\text{Before(At\_Least, Get\_Priority(E))}\) returns False, then \(E\) is assigned to Element and then removed from the queue, and Success is set to True; otherwise, Success is set to False and Element is unchanged.

Ramification: Unlike Dequeue, Dequeue\_Only\_High\_Priority is not blocking; it always returns immediately.

Reason: The use of Before is "backwards" so that it acts like ">=\) (it is defined similarly to ">\); thus we dequeue only when it is False.

Extensions to Ada 2005

The generic package Containers.Unbounded\_Priority\_Queues is new.

The Generic Package Containers.Bounded\_Priority\_Queues

Static Semantics

The language-defined generic package Containers.Bounded\_Priority\_Queues provides type Queue, which implements the interface type Containers.Synchronized\_Queue\_Interfaces.Queue.

```
with System;
with Ada.Containers.Synchronized\_Queue\_Interfaces;

generic
with package Queue\_Interfaces is
new Ada.Containers.Synchronized\_Queue\_Interfaces (<>);

type Queue\_Priority is private;

with function Get\_Priority (Element: Queue\_Interfaces.Element\_Type) return Queue\_Priority is <>;

with function Before (Left, Right: Queue\_Priority) return Boolean is <>;

Default Capacity : Count\_Type;

package Ada.Containers.Bounded\_Priority\_Queues is

with Preelaborate,
Nonblocking, Global => in out synchronized is
pragmas Preelaborate(Bounded\_Priority\_Queues);

Discussion: For discussion on the reasons and meaning of the specifications of the Global and Nonblocking aspects of this generic package, see the notes on the specification of the Containers.Vectors package (see A.18.2).
```

package Implementation is
... -- not specified by the language
end Implementation;
protected type Queue
  (Capacity : Count_Type := Default_Capacity;
   Ceiling  : System.Any_Priority := Default_Ceiling)
with Priority => Ceiling is
  new Queue_Interfaces.Queue with
  overriding
  entry Enqueue (New_Item : in Queue_Interfaces.Element_Type);
  overriding
  entry Dequeue (Element : out Queue_Interfaces.Element_Type);
{AI05-0159-1} {AI05-0251-1} not overriding
  procedure Dequeue Only High Priority
  with Nonblocking, Global => null, Use Formal => null;
  overriding
  function Peak Use return Count_Type
  with Nonblocking, Global => null, Use Formal => null;
{AI12-0112-1}
private
... -- not specified by the language
end Queue;
private
... -- not specified by the language
end Ada.Containers.Bounded_Priority_ Queues;
{AI05-0159-1} The semantics are the same as for Unbounded_Priority_ Queues, except:
• The capacity for instances of type Queue is bounded and specified by the discriminant Capacity.
Ramification: Since this type has a bounded capacity, Enqueue might block if the queue is full.
Implementation Advice
{AI05-0159-1} Bounded priority queue objects should be implemented without implicit pointers or
dynamic allocation.
Implementation Advice: Bounded priority queue objects should be implemented without implicit pointers or dynamic
allocation.
Extensions to Ada 2005
{AI05-0159-1} {AI05-0251-1} The generic package Containers.Bounded_Priority_ Queues is new.

A.18.32 The Generic Package Containers.Bounded_Indefinite_Holders

{AI12-0254-1} The language-defined generic package Containers.Bounded_Indefinite_Holders provides
a private type Holder and a set of operations for that type. It provides the same operations as the package
Containers.Indefinite_Holders (see A.18.18), with the difference that the maximum storage is bounded.

Static Semantics
{AI12-0254-1} The declaration of the generic library package Containers.Bounded_Indefinite_Holders has the same contents and semantics as Containers.Indefinite_Holders except:
• The following is added to the context clause:
  with System.Storage_Elements; use System.Storage_Elements;
• An additional generic parameter follows Element_Type:
   Max_Element_Size_in_Storage_Elements : Storage_Count;
**Reason:** This value is in Storage_Elements so that it can be used as a discriminant on a storage pool object in the implementation of the object; Ada doesn't allow discriminant dependent components to use formulas. This is a generic parameter as it is a property of the Element_Type; the largest possible object of Element_Type is unlikely to be different for different containers, so making it a discriminant (as Capacity is) provides no useful capability.

- **AI12-0409-1** The aspect definition for Preelaborable_Initialization for type Holder is changed to:
  ```ada```
  ```
  Preelaborable_Initialization =>
  Element_Type'Preelaborable_Initialization
  ```
  ```ada```

- **AI12-0409-1** Add to the precondition of To_Holder and Replace_Element:
  ```ada```
  ```
  and then (New_Item'Size <=
  Max_Element_Size_in_Storage_Elements * System.Storage_Unit
  or else raise Program_Error)
  ```
  ```ada```

  **Reason:** This ensures that an object that won't fit is not inserted into the container.

---

**Bounded (Run-Time) Errors**

- **AI12-0254-1** It is a bounded error to assign from a bounded holder object while tampering with elements of that object is prohibited. Either Program_Error is raised by the assignment, execution proceeds with the target object prohibiting tampering with elements, or execution proceeds normally.

---

**Implementation Requirements**

- **AI12-0254-1** For each instance of Containers.Indefinite_Holders and each instance of Containers.Bounded_Indefinite_Holders, if the two instances meet the following conditions, then the output generated by the Holder'Output or Holder'Write subprograms of either instance shall be readable by the Holder'Input or Holder'Read of the other instance, respectively:

  - the Element_Type parameters of the two instances are statically matching subtypes of the same type; and
  - the output generated by Element_Type'Output or Element_Type'Write is readable by Element_Type'Input or Element_Type'Read, respectively (where Element_Type denotes the type of the two actual Element_Type parameters).

---

**Implementation Advice**

- **AI12-0254-1** Bounded holder objects should be implemented without dynamic allocation and any finalization should be trivial unless Element_Type needs finalization.

  **Implementation Advice:** Bounded holder objects should be implemented without dynamic allocation.

  **To be honest:** Implementation of this container in Ada will probably require the use of a special storage pool. When we say "without dynamic allocation", we mean that this pool does not use heap memory and has a trivial finalization routine (that is, procedures Adjust and Finalize are null procedures). All storage pools are controlled, so we can't reasonably say that a bounded holder will not need finalization.

  **Implementation Note:** If the implementation supports discontiguous objects that require multiple calls to Allocate in a storage pool, the storage pool will need to support such allocations. The storage pool implementation can assume that all Allocate calls occur together, and similarly for Deallocate calls, thus simplifying the pool implementation so that allocation only occurs at a high-water mark location.

- **AI12-0350-1** The Implementation Advice about the Move and Swap operations is deleted for bounded holders; these operations can copy elements as necessary.

  **Reason:** The memory of a bounded indefinite holder belongs directly to the container, so it cannot be moved with the element. If the element type contains any internal pointers, moving it without calling Adjust would leave such pointers pointing to the wrong holder object. Thus, a full copy is needed, including any associated finalization and adjustments.

---

**Extensions to Ada 2012**

- **AI12-0254-1** The generic package Containers.Bounded_Indefinite_Holders is new.
The following example is an implementation of Dijkstra's shortest path algorithm in a directed graph with positive distances. The graph is represented by a map from nodes to sets of edges.

```ada
with Ada.Containers.Vectors;
with Ada.Containers.Doubly_Linked_Lists;
use Ada.Containers;

generic type Node is range <>;
package Shortest_Paths is
    type Distance is new Float range 0.0 .. Float'Last;
    type Edge is record
        To, From : Node;
        Length   : Distance;
    end record;

package Node_Maps is new Vectors (Node, Node);
-- The algorithm builds a map to indicate the node used to reach a given
-- node in the shortest distance.
package Adjacency_Lists is new Doubly_Linked_Lists (Edge);
use Adjacency_Lists;

package Graphs is new Vectors (Node, Adjacency_Lists.List);
package Paths is new Doubly_Linked_Lists (Node);

function Shortest_Path (G : Graphs.Vector; Source : Node; Target : Node) return Paths.List
    with Pre => G (Source) /= Adjacency_Lists.Empty_List;
end Shortest_Paths;

package body Shortest_Paths is

    function Shortest_Path (G : Graphs.Vector; Source : Node; Target : Node) return Paths.List
        with Pre => G (Source) /= Adjacency_Lists.Empty_List;

        use Adjacency_Lists, Node_Maps, Paths, Graphs;
        Reached : array (Node) of Boolean := (others => False);
        -- The set of nodes whose shortest distance to the source is known.
        So_Far   : array (Node) of Distance := (others => Distance'Last);
        Nearest_Distance : Distance;
        Next     : Node;

        begin
            So_Far(Source) := 0.0;
            while not Reached(Target) loop
                Nearest_Distance := Distance'Last;
                -- Find closest node not reached yet, by iterating over all nodes.
                -- A more efficient algorithm uses a priority queue for this step.
                Next := Source;
                for N in Node'First .. Node'Last loop
                    if not Reached(N) and then So_Far(N) < Nearest_Distance then
                        Nearest_Distance := So_Far(N);
                        Next := N;
                    end if;
                end loop;

            {AI05-0299-1} if Nearest_Distance = Distance'Last then
                -- No next node found, graph is not connected
                return Paths.Empty_List;
            end if;
        end loop;
```

{AI05-0299-1}
else
    Reached(Next) := True;
end if;
-- Update minimum distance to newly reachable nodes.
{AI05-0299-1} for E of G (Next) loop
    if not Reached(E.To) then
        Nearest_Distance := E.Length + So_Far(Next);
        if Nearest_Distance < So_Far(E.To) then
            Reached_From(E.To) := Next;
            So_Far(E.To) := Nearest_Distance;
        end if;
    end if;
end loop;
-- Rebuild path from target to source.
{AI12-0386-1} declare
    N : Node := Target;
    begin
        Prepend (The_Path, N);
        while N /= Source loop
            N := Reached_From(N);
            Prepend (The_Path, N);
        end loop;
        return The_Path;
    end;
end Shortest_Paths;
{AI05-0212-1} Note that the effect of the Constant_Indexing aspect (on type Vector) and the Implicit_Dereference aspect (on type Reference_Type) is that
G (Next)
{AI05-0212-1} {AI12-0426-1} is a convenient shorthand for
G.Constant_Reference (Next).Element.all
Similarly, the effect of the loop:
for E of G (Next) loop
    if not Reached(E.To) then
        end if;
end loop;
{AI05-0212-1} is the same as:
{AI12-0080-1} for C in G (Next).Iterate loop
    declare
        E : Edge renames G (Next)(C).all;
        begin
            if not Reached(E.To) then
                ...;
            end if;
    end;
end loop:
A.18.33 Example of Container Use

30/3 \{AI05-0212-1\} which is the same as:

31/4 \{AI12-0080-1\} declare

\begin{verbatim}
L : Adjacency_Lists.List renames G (Next);
C : Adjacency_Lists.Cursor := L.First;
begin
  while Has_Element (C) loop
    declare
      E : Edge renames L(C).all;
    begin
      if not Reached(E.To) then
        ...;
      end if;
    end;
    C := L.Next (C);
  end loop;
end;
\end{verbatim}

Wording Changes from Ada 2005

31.a/3 \{AI05-0212-1\} This example of container use is new.

A.19 The Package Locales

1/3 \{AI05-0127-2\}, \{AI05-0248-1\} A locale identifies a geopolitical place or region and its associated language, which can be used to determine other internationalization-related characteristics.

Static Semantics

2/3 \{AI05-0127-2\} The library package Locales has the following declaration:

3/5 \{AI12-0414-1\} package Ada.Locales is

\begin{verbatim}
with pragma Preelaborate,(Locales);
pragma Remote_Types is(Locales);
\end{verbatim}

4/4 \{AI12-0037-1\} type Language_Code is newarray String (1 .. 3)

4.a/4 with Dynamic Predicate =>

\begin{verbatim}
(for all E of Language_Code => E in of Character range 'a' .. 'z');
\end{verbatim}

4/4 type Country_Code is newarray String (1 .. 2)

4.a/4 with Dynamic Predicate =>

\begin{verbatim}
(for all E of Country_Code => E in of Character range 'A' .. 'Z');
\end{verbatim}

Discussion: \{AI12-0037-1\} These types are derived from type String so that they can easily be converted to or from type String. That's important if one of these values needs to be input or displayed (via Text_IO, perhaps). We use the predicate to ensure that only possible component values are used. Ada does not allow converting between unrelated types with components that don't statically match, so we cannot declare new types with constrained components if we want conversions to or from type String.

5/3 Language_Unknown : constant Language_Code := "und";

5/3 Country_Unknown : constant Country_Code := "ZZ";

6/3 function Language return Language_Code;

6/3 function Country return Country_Corder;

end Ada.Locales;

8/3 \{AI05-0127-2\}, \{AI05-0233-1\} The active locale is the locale associated with the partition of the current task.

Implementation Note: \{AI05-0233-1\} Some environments define both a system locale and the locale of the current user. For such environments, the active locale is that of current user if any; otherwise (as in a partition running on a server without a user), the system locale should be used.

This paragraph was deleted. \{AI05-0127-2\}, \{AI12-0446-1\} Language_Code is a lower-case string representation of an ISO 639-3 alpha-3 code that identifies a language.

This paragraph was deleted. \{AI05-0127-2\}, \{AI12-0446-1\} Country_Code is an upper-case string representation of an ISO 3166-1 alpha-2 code that identifies a country.
Function Language returns the code of the language associated with the active locale. If the Language Code associated with the active locale cannot be determined from the environment, then Language returns Language_Unknown. Otherwise, the result is a lower-case string representation of an ISO 639-3:2007 alpha-3 code that identifies a language.

Discussion: Some common language codes are: "eng" – English; "fra" – French; "deu" – German; "zho" – Chinese. These are the same codes as used by POSIX systems. We considered including constants for the most common languages, but that was rejected as the likely source of continual arguments about the constant names and which languages are important enough to include.

Function Country returns the code of the country associated with the active locale. If the Country Code associated with the active locale cannot be determined from the environment, then Country returns Country_Unknown. Otherwise, the result is an upper-case string representation of an ISO 3166-1:2020 alpha-2 code that identifies a country.

Discussion: Some common country codes are: "CA" – Canada; "FR" – France; "DE" – Germany; "IT" – Italy; "ES" – Spain; "GB" – United Kingdom; "US" – United States. These are the same codes as used by POSIX systems. We didn't include any country constants for the same reasons that we didn't include any language constants.

Extensions to Ada 2005

Package Locales is new.

Inconsistencies With Ada 2012

Corrigendum: Types Language_Code and Country_Code are defined with predicates rather than constrained components so that they can be converted to/from type String. This changes the exception raised from Constraint_Error to Assertion_Error if an assignment is attempted with an incorrect value. This could only matter if there is a handler specifically for Constraint_Error surrounding this assignment; as this exception raise is certainly caused by a bug (why would anyone want to use invalid language or country codes?), such a handler seems very unlikely. (In addition, this is a new Ada 2012 package, so there is not likely to be a lot of code using it.)
Annex B
(normative)
Interface to Other Languages

This Annex describes features for writing mixed-language programs. General interface support is presented first; then specific support for C, COBOL, and Fortran is defined, in terms of language interface packages for each of these languages.

**Ramification:** This Annex is not a “Specialized Needs” annex. Every implementation must support all nonoptional features defined here (mainly the package Interfaces).

**Language Design Principles**
Ada should have strong support for mixed-language programming.

**Implementation Requirements**

Support for interfacing to any foreign language is optional. However, an implementation shall not provide any optional aspect, attribute, library unit, or pragma having the same name as an aspect, attribute, library unit, or pragma (respectively) specified in the subclauses of this Annex unless the provided construct is either as specified in those subclauses or is more limited in capability than that required by those subclauses. A program that attempts to use an unsupported capability of this Annex shall either be identified by the implementation before run time or shall raise an exception at run time.

Discussion: The intent is that the same rules apply for the optional parts of language interfacing as apply for Specialized Needs Annexes. See 1.1.3 for a discussion of the purpose of these rules.

**Extensions to Ada 83**
Much of the functionality in this Annex is new to Ada 95.

**Wording Changes from Ada 83**
This Annex contains what used to be RM83-13.8.

**Wording Changes from Ada 2005**
Moved the clarification that interfacing to foreign languages is optional and has the same restrictions as a Specialized Needs Annex here.

### B.1 Interfacing Aspects

**Interfacing Pragmas**

An interfacing aspect is a representation aspect that is one of the aspects Import, Export, Link_Name, External_Name, or Convention.

Specifying the pragma Import aspect to have the value True is used to import an entity defined in a foreign language into an Ada program, thus allowing a foreign-language subprogram to be called from Ada, or a foreign-language variable to be accessed from Ada. In contrast, specifying the pragma Export aspect to have the value True is used to export an Ada entity to a foreign language, thus allowing an Ada subprogram to be called from a foreign language, or an Ada object to be accessed from a foreign language. The pragma Import and Export aspects are intended primarily for objects and subprograms, although implementations are allowed to support other entities. The Link_Name and External_Name aspects are used to specify the link name and external name, respectively, to be used to identify imported or exported entities in the external environment.

Aspect Description for Import: Entity is imported from another language.
Aspect Description for Export: Entity is exported to another language.

Aspect Description for External_Name: Name used to identify an imported or exported entity.

Aspect Description for Link_Name: Linker symbol used to identify an imported or exported entity.

The `pragma Convention` aspect is used to indicate that an Ada entity should use the conventions of another language. It is intended primarily for types and “callback” subprograms. For example, “`with pragma Convention => (Fortran, Matrix)`” on the declaration of an array type `Matrix` implies that `Matrix` should be represented according to the conventions of the supported Fortran implementation, namely column-major order.

Syntax

```
{AI05-0229-1} The form of a `An interfacing pragma` is a representation pragma that is one of the pragmas `Import`, `Export`, or `Convention`. Their forms, together with that of the related `pragma Linker_Options` is, are as follows:
```

```
{AI05-0229-1} `pragma Import(
    [Convention =>] convention_identifier, [Entity =>] local_name
    [,[External_Name =>] string_expression] [,[Link_Name =>] string_expression]);`
```

```
{AI05-0229-1} `pragma Export(
    [Convention =>] convention_identifier, [Entity =>] local_name
    [,[External_Name =>] string_expression] [,[Link_Name =>] string_expression]);`
```

```
{AI05-0229-1} `pragma Convention([Convention =>] convention_identifier,[Entity =>] local_name);
```

```
pragma Linker_Options(string_expression);
```

A `pragma Linker_Options` is allowed only at the place of a declarative item.

This paragraph was deleted. {8652/0058} {AI95-00036-01} {AI05-0229-1} For pragmas `Import` and `Export`, the argument for `Link_Name` shall not be given without the `pragma argument_identifier` unless the argument for `External_Name` is given.

Name Resolution Rules

```
{AI05-0229-1} The `Import` and `Export` aspects are of type Boolean.
```

```
{AI05-0229-1} The `Link_Name` and `External_Name` aspects are of expected type for a `string_expression` in an interfacing pragma or in `pragma Linker_Options` is `String`.
```

```
{AI05-0229-1} `Ramification: There is no language-defined support for external or link names of type `Wide_String`, or of other string types. Implementations may, of course, have additional `aspect pragmas` for that purpose. Note that allowing both `String` and `Wide_String` in the same `aspect_definition pragma` would cause ambiguities.`
```

```
{AI05-0229-1} The expected type for the `string_expression` in `pragma Linker_Options` is `String`.
```

Legality Rules

```
{AI05-0229-1} The `aspect Convention` shall be specified by a `convention_identifier` which is an interfacing pragma shall be the name of a `convention`. The convention names are implementation defined, except for certain language-defined ones, such as Ada and Intrinsic, as explained in 6.3.1, “Conformance`
Rules”. [Additional convention names generally represent the calling conventions of foreign languages, language implementations, or specific run-time models.] The convention of a callable entity is its calling convention.

**Implementation defined:** Implementation-defined convention names.

**Discussion:** We considered representing the convention names using an enumeration type declared in System. Then, `convention_identifier` would be changed to `convention_name`, and we would make its expected type be the enumeration type. We didn't do this because it seems to introduce extra complexity, and because the list of available languages is better represented as the list of children of package Interfaces — a more open-ended sort of list.

If $L$ is a `convention_identifier` for a language, then a type $T$ is said to be compatible with convention $L$, (alternatively, is said to be an $L$-compatible type) if any of the following conditions are met:

- $T$ is declared in a language interface package corresponding to $L$ and is defined to be $L$-compatible (see B.3, B.3.1, B.3.2, B.4, B.5),
- `{AI05-0229-1}` Convention $L$ has been specified for $T$ in a pragma `Convention`, and $T$ is eligible for convention $L$; that is:
  - `{AI12-0135-1}` $T$ is an enumeration type such that all internal codes (whether assigned by default or explicitly) are within an implementation-defined range that includes at least the range of values $0 .. 2^{15}–1$;  
- $T$ is an array type with either an unconstrained or statically-constrained first subtype, and its component type is $L$-compatible,
- $T$ is a record type that has no discriminants and that only has components with statically-constrained subtypes, and each component type is $L$-compatible,
- `{AI05-0002-1}` $T$ is an access-to-object type, and its designated type is $L$-compatible, and its designated subtype is not an unconstrained array subtype,
- $T$ is an access-to-subprogram type, and its designated profile's parameter and result types are all $L$-compatible,
- $T$ is derived from an $L$-compatible type,
- `{AI12-0207-1}` $T$ is an anonymous access type, and $T$ is eligible for convention $L$,

**Reason:** We say this so that the presence of an anonymous access component does not necessarily prevent a type from being eligible for convention $L$. We want the anonymous access type to take the convention from the enclosing type, but if we only said that, the definition would be circular (one can only portably apply the convention $L$ to a record type $R$ if the components of $R$ already have convention $L$; but the anonymous components of $R$ have to take the convention from $R$). We include the part of about $T$ being eligible for convention $L$ so that we don't force convention $L$ on some type that is incompatible with it.

- The implementation permits $T$ as an $L$-compatible type.

**Discussion:** For example, an implementation might permit Integer as a C-compatible type, though the C type to which it corresponds might be different in different environments.

 `{AI05-0229-1}` If the pragma `Convention aspect is specified for` applies to a type, then the type shall either be compatible with or eligible for the `specified` convention specified in the pragma.

**Ramification:** `{AI05-0229-1}` If a type is derived from an $L$-compatible type, the derived type is by default $L$-compatible, but it is also permitted to specify the `Convention aspect` for the derived type.

 `{AI05-0229-1}` It is permitted to specify the `Convention aspect` for an incomplete type, but in the complete declaration each component must be $L$-compatible.

 `{AI05-0229-1}` If each component of a record type is $L$-compatible, then the record type itself is only $L$-compatible if it has a specified `Convention`.

 `{AI12-0207-1}` If convention $L$ is specified for a type $T$, for each component of $T$ that has an anonymous access type, the convention of the anonymous access type is $L$. If convention $L$ is specified for an object that has an anonymous access type, the convention of the anonymous access type is $L$.  

Ramification: This applies to both anonymous access-to-object and anonymous access-to-subprogram types.

22.3 \[AI05-0229-1\] A `pragma Import` shall be the completion of a declaration. Notwithstanding any rule to the contrary, a declaration with a `pragma Import` aspect shall not have may serve as the completion of any kind of (explicit) declaration if supported by an implementation for that kind of declaration. If a completion is a `pragma Import`, then it shall appear in the same declarative part, package specification, task definition or protected definition as the declaration. For a library unit, it shall appear in the same compilation, before any subsequent compilation units other than pragmas. If the local name denotes more than one entity, then the `pragma Import` is the completion of all of them.

Discussion: \[AI05-0229-1\] For declarations of deferred constants and subprograms, we explicitly mention that no completion is allowed when aspect `pragma Import` is True explicitly as a possible completion. For other declarations that require completions, we ignore the possibility of the `pragma Import` being True. Nevertheless, if an implementation chooses to allow specifying aspect `pragma Import` to be True for complete the declaration of a task, protected type, incomplete type, private type, etc., it may do so, and the normal completion is then not allowed for that declaration.

23.3 \[AI05-0229-1\] An entity with a True specified as the Entity argument to a `pragma Import` aspect (or `pragma Export` aspect) is said to be imported (respectively, exported). An entity shall not be both imported and exported.

24 The declaration of an imported object shall not include an explicit initialization expression. [Default initializations are not performed.]

Proof: This follows from the “Notwithstanding ...” wording in the Dynamics Semantics paragraphs below.

25.3 \[AI05-0229-1\] The type of an imported or exported object shall be compatible with the specified Convention aspect, if any convention specified in the corresponding pragma.

Ramification: This implies, for example, that importing an Integer object might be illegal, whereas importing an object of type Interfaces.C.int would be permitted.

26.3 \[AI05-0229-1\] For an imported or exported subprogram, the result and parameter types shall each be compatible with the specified Convention aspect, if any convention specified in the corresponding pragma.

27.3 \[AI05-0229-1\] The `aspect definition` (if any) used to directly specify an `External_Name` or `Link_Name` aspect shall be a static expression. The `string expression` of a `pragma Linker_Options` shall be static. An `External_Name` or `Link_Name` aspect shall be specified only for an entity that is either imported or exported.

Static Semantics

Paragraphs 28 and 29 were deleted.

28.3 \[AI05-0229-1\] Import, Export, and Convention pragmas are representation pragmas that specify the convention aspect of representation. In addition, Import and Export pragmas specify the imported and exported aspects of representation, respectively.

29.3 \[AI05-0229-1\] An interfacing pragma is a program unit pragma when applied to a program unit (see 10.1.5).

30.3 \[AI05-0229-1\] An interfacing pragma defines the convention of the entity denoted by the local name. The Convention aspect convention represents the calling convention or representation convention of the entity. For an access-to-subprogram type, it represents the calling convention of designated subprograms. In addition:
• A **pragma** Import aspect indicates that the entity is defined externally (that is, outside the Ada program). This aspect is never inherited; if not directly specified, the Import aspect is False.

• A **pragma** Export aspect indicates that the entity is used externally. This aspect is never inherited; if not directly specified, the Export aspect is False.

• **For an entity with a True** A **pragma** Import or Export aspect, an optionally specifies an entity's external name, link name, or both may also be specified.

An **external name** is a string value for the name used by a foreign language program either for an entity that an Ada program imports, or for referring to an entity that an Ada program exports.

A **link name** is a string value for the name of an exported or imported entity, based on the conventions of the foreign language's compiler in interfacing with the system's linker tool.

The meaning of link names is implementation defined. If neither a link name nor the Address attribute of an imported or exported entity is specified, then a link name is chosen in an implementation-defined manner, based on the external name if one is specified.

**Implementation defined:** The meaning of link names.

**Ramification:** For example, an implementation might always prepend "_", and then pass it to the system linker.

**Implementation defined:** The manner of choosing link names when neither the link name nor the address of an imported or exported entity is specified.

**Ramification:** Normally, this will be the entity's defining name, or some simple transformation thereof.

Pragma Linker_Options has the effect of passing its string argument as a parameter to the system linker (if one exists), if the immediately enclosing compilation unit is included in the partition being linked. The interpretation of the string argument, and the way in which the string arguments from multiple Linker_Options pragmas are combined, is implementation defined.

**Implementation defined:** The effect of pragma Linker_Options.

**Dynamic Semantics**

Notwithstanding what this document says elsewhere, the elaboration of a declaration with a True Import aspect denoted by the local_name of a pragma Import does not create the entity. Such an elaboration has no other effect than to allow the defining name to denote the external entity.

**Ramification:** This implies that default initializations are skipped. (Explicit initializations are illegal.) For example, an imported access object is not initialized to null.

Note that the local_name in a pragma Import might denote more than one declaration; in that case, the entity of all of those declarations will be the external entity.

**Discussion:** This “notwithstanding” wording is better than saying “unless aspect named by a pragma Import is True” on every definition of elaboration. It says we recognize the contradiction, and this rule takes precedence.

**Erroneous Execution**

It is the programmer's responsibility to ensure that the use of interfacing aspects pragmas does not violate Ada semantics; otherwise, program execution is erroneous. For example, passing an object with mode in to imported code that modifies it causes erroneous execution. Similarly, calling an imported subprogram that is not pure from a pure package causes erroneous execution.

**Implementation Advice**

If an implementation supports **pragma** Export for a given language, then it should also allow the main subprogram to be written in that language. It should support some mechanism for
invoking the elaboration of the Ada library units included in the system, and for invoking the finalization of the environment task. On typical systems, the recommended mechanism is to provide two subprograms whose link names are "adainit" and "adafinal". Adainit should contain the elaboration code for library units. Adafinal should contain the finalization code. These subprograms should have no effect the second and subsequent time they are called.

**Implementation Advice:** If `pragma Export` is supported for a language, the main program should be able to be written in that language. Subprograms named "adainit" and "adafinal" should be provided for elaboration and finalization of the environment task.

**Ramification:** For example, if the main subprogram is written in C, it can call adainit before the first call to an Ada subprogram, and adafinal after the last.

**AI05-0229-1** {AI05-0269-1} Automatic elaboration of preelaborated packages should be provided when specifying the `pragma Export aspect as True`.

**Implementation Advice:** Automatic elaboration of preelaborated packages should be provided when specifying the `pragma Export aspect as True`.

**AI05-0229-1** {AI12-0135-1} {AI12-0444-1} For each supported convention `L` other than Intrinsic, an implementation should support specifying the `pragma Import` and `Export` `pragma` for objects of `L`-compatible types and for subprograms, and the `pragma Convention` for `L`-eligible types and for subprograms, presuming the other language has corresponding features. Specifying the `pragma Convention` should not be supported for scalar types other than enumeration types whose internal codes fall within the range `0 .. 2**15–1`, but no recommendation is made for other scalar types.

**Implementation Advice:** For each supported convention `L` other than Intrinsic, specifying the `pragma Import` and `Export` `pragma` for objects of `L`-compatible types and for subprograms, and the `pragma Convention` should be supported for `L`-eligible types and for subprograms.

**Reason:** AI05-0229-1 Specifying the `pragma Convention` is not necessary for scalar types, since the language interface packages declare scalar types corresponding to those provided by the respective foreign languages.

**Implementation Note:** AI95-00114-01 If an implementation supports interfacing to the `C++` entities not supported by B.3, it should do so via the convention identifier C_Plus_Plus (in additional to any C++-implementation-specific ones).

**Reason:** AI95-00114-01 The reason for giving the advice about `C++` is to encourage uniformity among implementations, given that the name of the language is not syntactically legal as an identifier. We place this advice in the AARM, rather than the RM95 proper, because (as of this writing) `C++` is not an international standard, and we don't want to refer to such a language from an international standard.

**NOTE 1** AI05-0229-1 AI12-0440-1 Implementations can place restrictions on interfacing `pragma`; for example, requiring each exported entity to be declared at the library level.

**Proof:** Arbitrary restrictions are allowed by 13.1.

**Ramification:** Such a restriction might be to disallow them altogether. Alternatively, the implementation might allow them only for certain kinds of entities, or only for certain conventions.

**NOTE 2** AI05-0229-1 The `pragma Convention` in combination with the `pragma Import` `aspect` indicates the conventions for accessing external entities. It is possible that the actual entity is written in assembly language, but reflects the conventions of a particular language. For example, with `Convention => Ada`, the `pragma Import(Ada, ...)` can be used to interface to an assembly language routine that obeys the Ada compiler's calling conventions.

**NOTE 3** AI05-0229-1 AI12-0440-1 To obtain “call-back” to an Ada subprogram from a foreign language environment, the `pragma Convention` `aspect` can be specified both for the access-to-subprogram type and the specific subprogram(s) to which 'Access is applied.

**Paragraphs 45 and 46 were deleted.**

**NOTE 4** AI05-0229-1 It is illegal to specify more than one of `Import`, `Export`, or `Convention` for a given entity.

**NOTE 5** AI05-0229-1 The local name in an interfacing `pragma` can denote more than one entity in the case of overloading. Such a `pragma` applies to all of the denoted entities.

**NOTE 6** AI12-0449-1 Machine code insertions can also be relevant for interfacing; see 13.8 See also 13.8, “Machine Code Insertions.”
Ramification: The Intrinsic convention (see 6.3.1) implies that the entity is somehow “built in” to the implementation. Thus, it generally does not make sense for users to specify Intrinsic along with specifying that the entity is imported in a pragma Import. The intention is that only implementations will specify Intrinsic for an imported entity in a pragma Import. The language also defines certain subprograms to be Intrinsic.

Discussion: There are many imaginable interfacing pragmas that don't make any sense. For example, setting the Convention of a protected procedure to Ada is probably wrong. Rather than enumerating all such cases, however, we leave it up to implementations to decide what is sensible.

NOTE 7 If both External_Name and Link_Name are specified for a given entity an Import or Export pragma, then the External_Name is ignored.

This paragraph was deleted.

NOTE 8 An interfacing pragma might result in an effect that violates Ada semantics.

Examples

package Fortran_Library is
  function Sqrt (X : Float) return Float
    with Import => True, Convention => Fortran;
  type Matrix is array (Natural range <>, Natural range <>) of Float
    with Convention => Fortran;
  function Invert (M : Matrix) return Matrix
    with Import => True, Convention => Fortran;
private
  pragma Import (Fortran, Sqrt);
  pragma Import (Fortran, Exp);
end Fortran_Library;

Extensions to Ada 83

Interfacing pragmas are new to Ada 95. Pragma Import replaces Ada 83’s pragma Interface. Existing implementations can continue to support pragma Interface for upward compatibility.

Wording Changes from Ada 95

{8652/0058} Corrigendum: Clarified that pragmas Import and Export work like a subprogram call; parameters cannot be omitted unless named notation is used. (Reordering is still not permitted, however.)

{AI95-00320-01} Added wording to say all bets are off if foreign code doesn't follow the semantics promised by the Ada specifications.

Incompatibilities With Ada 2005

{AI05-0002-1} Correction: Access types that designate unconstrained arrays are no longer defined to be L-compatible. Such access-to-arrays require bounds information, which is likely to be incompatible with a foreign language. The change will allow (but not require) compilers to reject bad uses, which probably will not work anyway. Note that implementations can still support any type that it wants as L-compatible, such uses will not be portable, however. As such, there should be little existing code that will be impacted (compilers probably already rejected cases that could not be translated, whether or not the language allowed doing so formally).

Extensions to Ada 2005

{AI05-0229-1} Aspects Convention, Import, Export, Link_Name, and External_Name are new; pragmas Convention, Import, and Export are now obsolescent.

Incompatibilities With Ada 2012

{AI12-0207-1} Correction: The convention of anonymous access components is that of the enclosing type (in Ada 2012, it was Ada). Similarly, the convention of the anonymous access type of an object is that of the object (again, in Ada 2012 it was Ada). While this is formally incompatible, it should be more useful in portable code; it makes little sense to have a component of an Ada access type in a record with a C convention. For most implementations, this will have no real effect as convention Ada anonymous access types were allowed as C-compatible anyway. But such code was not portable, as this was not required in Ada 2012.
**B.2 The Package Interfaces**

Package Interfaces is the parent of several library packages that declare types and other entities useful for interfacing to foreign languages. It also contains some implementation-defined types that are useful across more than one language (in particular for interfacing to assembly language).

**Implementation defined:** The contents of the visible part of package Interfaces and its language-defined descendants.

**Static Semantics**

The library package Interfaces has the following skeletal declaration:

```ada
package Interfaces is
  with pragma Pure is (Interfaces);
  type Integer_n is range -2**(n-1) .. 2**(n-1) - 1;  -- 2's complement
  type Unsigned_n is mod 2**n;
  function Shift_Left (Value : Unsigned_n; Amount : Natural)
    return Unsigned_n;
  function Shift_Right (Value : Unsigned_n; Amount : Natural)
    return Unsigned_n;
  function Shift_Right_Arithmetic (Value : Unsigned_n; Amount : Natural)
    return Unsigned_n;
  function Rotate_Left (Value : Unsigned_n; Amount : Natural)
    return Unsigned_n;
  function Rotate_Right (Value : Unsigned_n; Amount : Natural)
    return Unsigned_n;
  ...
end Interfaces;
```

**Implementation Requirements**

An implementation shall provide the following declarations in the visible part of package Interfaces:

- Signed and modular integer types of \( n \) bits, if supported by the target architecture, for each \( n \) that is at least the size of a storage element and that is a factor of the word size. The names of these types are of the form Integer_\( n \) for the signed types, and Unsigned_\( n \) for the modular types;

  **Ramification:** For example, for a typical 32-bit machine the corresponding types might be Integer_8, Unsigned_8, Integer_16, Unsigned_16, Integer_32, and Unsigned_32.

  The wording above implies, for example, that Integer_16'Size = Unsigned_16'Size = 16. Unchecked conversions between same-Sized types will work as expected.

- For each such modular type in Interfaces, shifting and rotating subprograms as specified in the declaration of Interfaces above. These subprograms are Intrinsic. They operate on a bit-by-bit basis, using the binary representation of the value of the operands to yield a binary representation for the result. The Amount parameter gives the number of bits by which to shift or rotate. For shifting, zero bits are shifted in, except in the case of Shift_Right_Arithmetic, where one bit is shifted in if Value is at least half the modulus.

  **Reason:** We considered making shifting and rotating be primitive operations of all modular types. However, it is a design principle of Ada that all predefined operations should be operators (not functions named by identifiers). (Note that an early version of Ada had "abs" as an identifier, but it was changed to a reserved word operator before standardization of Ada 83.) This is important because the implicit declarations would hide nonoverloadable declarations with the same name, whereas operators are always overloadable. Therefore, we would have had to make
shift and rotate into reserved words, which would have been upward incompatible, or else invent new operator symbols, which seemed like too much mechanism.

To be honest: \{AI12-0264-1\} “Shifting” and “rotating” have the conventional meaning. Neither of these terms is usefully defined by the usual normative references of the Reference Manual, so we provide pseudo-code here to describe the intended semantics of the above wording (all operations in these examples are using modular semantics).

```ada
function Rotate_Left (Value : Unsigned_n; Amount : Natural)
return Unsigned_n is
    Result : Unsigned_n := Value;
    Bit : Unsigned_n range 0 .. 1;
begin
    for Count in 1 .. Amount loop
        Bit := Result/2**(n-1); -- High-bit of Result
        Result := Result*2 + Bit;
    end loop;
    return Result;
end Rotate_Left;

function Rotate_Right (Value : Unsigned_n; Amount : Natural)
return Unsigned_n is
    Result : Unsigned_n := Value;
    Bit : Unsigned_n range 0 .. 1;
begin
    for Count in 1 .. Amount loop
        Bit := Result mod 2; -- Low-bit of Result
        Result := Result/2 + (Bit * 2**(n-1));
    end loop;
    return Result;
end Rotate_Right;

function Shift_Left (Value : Unsigned_n; Amount : Natural)
return Unsigned_n is
begin
    for Count in 1 .. Amount loop
        Result := Result * 2;
    end loop;
    return Result;
end Shift_Left;

function Shift_Right (Value : Unsigned_n; Amount : Natural)
return Unsigned_n is
begin
    for Count in 1 .. Amount loop
        Result := Result / 2;
    end loop;
    return Result;
end Shift_Right;

function Shift_Right_Arithmetic (Value : Unsigned_n; Amount : Natural)
return Unsigned_n is
    Neg : constant Boolean := Result/2**(n-1) = 1; -- High-bit of Result
begin
    for Count in 1 .. Amount loop
        if Neg then
            Result := Result / 2 + 2**(n-1);
        else
            Result := Result / 2;
        end if;
    end loop;
    return Result;
end Shift_Right_Arithmetic;
```

\{AI12-0264-1\} These generally correspond to machine instructions, although there may not be an exact match in terms of boundary conditions, as Ada requires the correct result to be produced for all values of Amount.

- Floating point types corresponding to each floating point format fully supported by the hardware.

Implementation Note: The names for these floating point types are not specified. However, if IEEE arithmetic is supported, then the names should be IEEE_Float_32 and IEEE_Float_64 for single and double precision, respectively.

\{AI95-00204-01\} \{AI05-0262-1\} Support for interfacing to any foreign language is optional. However, an implementation shall not provide any attribute, library unit, or pragma having the same name as an
attribute, library unit, or pragma (respectively) specified in the following clauses of this Annex unless the
provided construct is either as specified in those clauses or is more limited in capability than that required
by those clauses. A program that attempts to use an unsupported capability of this Annex shall either be
identified by the implementation before run time or shall raise an exception at run time.

Discussion: The intent is that the same rules apply for language interfacing as apply for Specialized Needs Annexes.
See 1.1.3 for a discussion of the purpose of these rules.

Implementation Permissions

An implementation may provide implementation-defined library units that are children of Interfaces, and
may add declarations to the visible part of Interfaces in addition to the ones defined above.

Implementation defined: Implementation-defined children of package Interfaces. The contents of the visible part of
package Interfaces.

A child package of package Interfaces with the name of a convention
may be provided independently of whether the convention is supported by the pragma Convention aspect
and vice versa. Such a child package should contain any declarations that would be useful for interfacing
to the language (implementation) represented by the convention. Any declarations useful for interfacing
to any language on the given hardware architecture should be provided directly in Interfaces.

Ramification: For example, package Interfaces.XYZ_Pascal might contain declarations of types that match the data
types provided by the XYZ implementation of Pascal, so that it will be more convenient to pass parameters to a
subprogram whose convention is XYZ_Pascal.

Implementation Advice

This paragraph was deleted.

For each implementation-defined convention identifier, there
should be a child package of package Interfaces with the corresponding name. This package should
contain any declarations that would be useful for interfacing to the language (implementation) represented
by the convention. Any declarations useful for interfacing to any language on the given hardware
architecture should be provided directly in Interfaces.

Ramification: For example, package Interfaces.XYZ_Pascal might contain declarations of
types that match the data types provided by the XYZ implementation of Pascal, so that it will be more convenient to pass parameters to a
subprogram whose convention is XYZ_Pascal.

Implementation Advice: If an interface to C, COBOL, or Fortran is provided, the corresponding package or packages
described in Annex B, “Interface to Other Languages” should also be provided.

Implementation Note: The intention is that an implementation might support several implementations of the foreign
language: Interfaces.This_Fortran and Interfaces.That_Fortran might both exist. The “default” implementation,
overridable by the user, should be declared as a renaming:

package Interfaces.Fortran renames Interfaces.This_Fortran;

Wording Changes from Ada 95

Clarified that interfacing to foreign languages is optional and has the same restrictions as a

Wording Changes from Ada 2005

Move the restrictions on implementations of optional features to the start of this Annex.

B.3 Interfacing with C and C++ Interfacing with C

The facilities relevant
to interfacing with the C language and the corresponding subset of the C++ language are the package
Interfaces.C and its children, and support for specifying the Import, Export, and Convention aspect pragmas with convention identifier C, and support for the Convention pragma with convention identifier C Pass By Copy, and any of the C Variadic n conventions described below.

The package Interfaces.C contains the basic types, constants, and subprograms that allow an Ada program to pass scalars and strings to C and C++ functions. When this subclause mentions a C entity, the reference also applies to the corresponding entity in C++.

Static Semantics

The library package Interfaces.C has the following declaration:

```ada
package Interfaces.C is
with pragma Pure is (C);
```

-- Declarations based on C's <limits.h>

```ada
CHAR_BIT : constant := implementation-defined; -- typically 8
SCHAR_MIN : constant := implementation-defined; -- typically –128
SCHAR_MAX : constant := implementation-defined; -- typically 127
UCHAR_MAX : constant := implementation-defined; -- typically 255
```

-- Signed and Unsigned Integers

```ada
type int is range implementation-defined;
type short is range implementation-defined;
type long is range implementation-defined;
type signed_char is range SCHAR_MIN .. SCHAR_MAX;
for signed_char'Size use CHAR_BIT;
type unsigned is mod implementation-defined;
type unsigned_short is mod implementation-defined;
type unsigned_long is mod implementation-defined;
type unsigned_char is mod (UCHAR_MAX+1);
for unsigned_char'Size use CHAR_BIT;
subtype plain_char is implementation-defined;
type ptrdiff_t is range implementation-defined;
type size_t is mod implementation-defined;
```

-- Boolean Type

```ada
type C_bool is new Boolean;
```

-- Floating Point

```ada
type C_float is digits implementation-defined;
type double is digits implementation-defined;
type long_double is digits implementation-defined;
```

-- Characters and Strings

```ada
type char is <implementation-defined character type>;
```

(8652/0060) {AI95-00037-01} nul : constant char := implementation-defined(char'First);

```ada
function To_C (Item : in Character) return char;
function To_Ada (Item : in char) return Character;
```

(233/0809-01) {AI05-0229-1} {AI05-0269-1} type char_array is array (size_t range <>) of aliased char

```ada
with Pack;
pragma Pack (char_array);
for char_array'Component_Size use CHAR_BIT;
function Is_Nul_Terminated (Item : in char_array) return Boolean;
```
function To_C (Item : in String; Append_Nul : in Boolean := True)
  return char_array;

function To_Ada (Item : in char_array; Trim_Nul : in Boolean := True)
  return String;

procedure To_C (Item : in String; Target : out char_array; Count : out size_t; Append_Nul : in Boolean := True);

procedure To_Ada (Item : in char_array; Target : out String; Count : out Natural; Trim_Nul : in Boolean := True);

-- Wide Character and Wide String

{8652/0060} {AI95-00037-01}  type wchar_t is <implementation-defined character type> implementation-defined;

{8652/0060} {AI95-00037-01}  wide_nul : constant wchar_t := implementation-defined wchar_t'First;

function To_C (Item : in Wide_Character) return wchar_t;
function To_Ada (Item : in wchar_t) return Wide_Character;

{AI05-0229-1}  type wchar_array is array (size_t range <>) of aliased wchar_t
  with Pack;

This paragraph was deleted.{AI05-0229-1}  pragma Pack(wchar_array);

function Is_Null_Terminated (Item : in wchar_array) return Boolean;

function To_C (Item : in Wide_String; Append_Nul : in Boolean := True)
  return wchar_array;

function To_Ada (Item : in wchar_array; Trim_Nul : in Boolean := True)
  return Wide_String;

procedure To_C (Item : in Wide_String; Target : out wchar_array; Count : out size_t; Append_Nul : in Boolean := True);

procedure To_Ada (Item : in wchar_array; Target : out Wide_String; Count : out Natural; Trim_Nul : in Boolean := True);

{AI95-00285-01} {AI12-0450-1}  -- ISO/IEC 10646:2003 compatible types defined by ISO/IEC TR 10769:2004

{AI95-00285-01}  type char16_t is <implementation-defined character type>;

char16_nul : constant char16_t := implementation-defined;

function To_C (Item : in Wide_Character) return char16_t;
function To_Ada (Item : in char16_t) return Wide_Character;

{AI05-0229-1}  type char16_array is array (size_t range <>) of aliased char16_t
  with Pack;

This paragraph was deleted.{AI05-0229-1}  pragma Pack(char16_array);

function Is_Null_Terminated (Item : in char16_array) return Boolean;

function To_C (Item : in Wide_String; Append_Nul : in Boolean := True)
  return char16_array;

function To_Ada (Item : in char16_array; Trim_Nul : in Boolean := True)
  return Wide_String;
procedure To_C (Item : in Wide_String;
    Target : out char16_array;
    Count : out size_t;
    Append_Nul : in Boolean := True);

procedure To_Ada (Item : in char16_array;
    Target   : out Wide_String;
    Count    : out Natural;
    Trim_Nul : in Boolean := True);

{AI95-00285-01} type char32_t is <implementation-defined character type>;
  char32_nul : constant char32_t := implementation-defined;

function To_C (Item : in Wide_Wide_Character) return char32_t;
function To_Ada (Item : in char32_t) return Wide_Wide_Character;

{AI05-0229-1} type char32_array is array (size_t range <>) of aliased char32_t
with Pack;

This paragraph was deleted.{AI05-0229-1} pragma Pack(char32_array);

function Is_Null_Terminated (Item : in char32_array) return Boolean;

function To_C (Item : in Wide_Wide_String; Append_Nul : in Boolean := True)
return char32_array;

function To_Ada (Item : in char32_array; Trim_Nul : in Boolean := True)
return Wide_Wide_String;

procedure To_C (Item : in Wide_Wide_String;
    Target     : out char32_array;
    Count      : out size_t;
    Append_Nul : in Boolean := True);

procedure To_Ada (Item : in char32_array;
    Target     : out Wide_Wide_String;
    Count      : out Natural;
    Trim_Nul   : in Boolean := True);

Terminator_Error : exception;

end Interfaces.C;

Implementation defined: The definitions of certain types and constants in Interfaces.C.

Each of the types declared in Interfaces.C is C-compatible.

{AI95-00285-01} {AI12-0411-1} The types int, short, long, unsigned, ptrdiff_t, size_t, double, char, and
wchar_t, char16_t, and char32_t correspond respectively to the C types having the same names. The types
signed_char, unsigned_short, unsigned_long, unsigned_char, C_bool, C_float, and long_double
correspond respectively to the C types signed char, unsigned short, unsigned long, unsigned char, C_bool,
float, and long double.

Discussion: The C types wchar_t and char16_t seem to be the same. However, wchar_t has an implementation-defined
size, whereas char16_t is guaranteed to be an unsigned type of at least 16 bits. Also, char16_t and char32_t are
encouraged to have UTF-16 and UTF-32 representations; that means that they are not directly the same as the Ada
types, which most likely don’t use any UTF encoding.

The type of the subtype plain_char is either signed_char or unsigned_char, depending on the C
implementation.

function To_C (Item : in Character) return char;
function To_Ada (Item : in char ) return Character;

The functions To_C and To_Ada map between the Ada type Character and the C type char.

Implementation Note: {8652/0114} {AI95-00038-01} The To_C and To_Ada functions map between corresponding
characters, not necessarily between characters with the same internal representation. Corresponding characters are
characters defined by the same enumeration literal, if such exist; otherwise, the correspondence is unspecified.

The following definition is equivalent to the above summary:
To_C (Latin_1_Char) = char'Value(Character'Image(Latin_1_Char))
provided that char'Value does not raise an exception; otherwise the result is unspecified.

To_Ada (Native_C_Char) = Character'Value(char'Image(Native_C_Char))
provided that Character'Value does not raise an exception; otherwise the result is unspecified.

function Is_Nul_Terminated (Item : in char_array) return Boolean;
The result of Is_Nul_Terminated is True if Item contains nul, and is False otherwise.

function To_C (Item : in String; Append_Nul : in Boolean := True)
return char_array;

function To_Ada (Item : in char_array; Trim_Nul : in Boolean := True)
return String;

{AI95-00258-01} The result of To_C is a char_array value of length Item'Length (if Append_Nul
is False) or Item'Length+1 (if Append_Nul is True). The lower bound is 0. For each component
Item(I), the corresponding component in the result is To_C applied to Item(I). The value nul is
appended if Append_Nul is True. If Append_Nul is False and Item'Length is 0, then To_C
propagates Constraint_Error.

The result of To_Ada is a String whose length is Item'Length (if Trim_Nul is False) or the length
of the slice of Item preceding the first nul (if Trim_Nul is True). The lower bound of the result is
1. If Trim_Nul is False, then for each component Item(I) the corresponding component in the
result is To_Ada applied to Item(I). If Trim_Nul is True, then for each component Item(I) before
the first nul the corresponding component in the result is To_Ada applied to Item(I). The function
propagates Terminator_Error if Trim_Nul is True and Item does not contain nul.

procedure To_C (Item : in String;
    Target : out char_array;
    Count : out size_t;
    Append_Nul : in Boolean := True);

procedure To_Ada (Item : in char_array;
    Target : out String;
    Count : out Natural;
    Trim_Nul : in Boolean := True);

For procedure To_C, each element of Item is converted (via the To_C function) to a char, which
is assigned to the corresponding element of Target. If Append_Nul is True, nul is then assigned to
the next element of Target. In either case, Count is set to the number of Target elements assigned.
If Target is not long enough, Constraint_Error is propagated.

For procedure To_Ada, each element of Item (if Trim_Nul is False) or each element of Item
preceding the first nul (if Trim_Nul is True) is converted (via the To_Ada function) to a
Character, which is assigned to the corresponding element of Target. Count is set to the number
of Target elements assigned. If Target is not long enough, Constraint_Error is propagated. If
Trim_Nul is True and Item does not contain nul, then Terminator_Error is propagated.

function Is_Nul_Terminated (Item : in wchar_array) return Boolean;
The result of Is_Nul_Terminated is True if Item contains wide_nul, and is False otherwise.

function To_C (Item : in Wide_Character) return wchar_t;
function To_Ada (Item : in wchar_t) return Wide_Character;

To_C and To_Ada provide the mappings between the Ada and C wide character types.
function To_C (Item : in Wide_String; 
    Append_Nul : in Boolean := True) 
return wchar_array;

function To_Ada (Item : in wchar_array; 
    Trim_Nul : in Boolean := True) 
return Wide_String;

procedure To_C (Item : in Wide_String; 
    Target : out wchar_array; 
    Count : out size_t; 
    Append_Nul : in Boolean := True); 

procedure To_Ada (Item : in wchar_array; 
    Target : out Wide_String; 
    Count : out Natural; 
    Trim_Nul : in Boolean := True);

The To_C and To_Ada subprograms that convert between Wide_String and wchar_array have analogous effects to the To_C and To_Ada subprograms that convert between String and char_array, except that wide_nul is used instead of nul.

function Is_Nul_Terminated (Item : in char16_array) return Boolean;

{AI95-00285-01} The result of Is_Nul_Terminated is True if Item contains char16_nul, and is False otherwise.

function To_C (Item : in Wide_Character) return char16_t;
function To_Ada (Item : in char16_t ) return Wide_Character;

{AI95-00285-01} To_C and To_Ada provide mappings between the Ada and C 16-bit character types.

function To_C (Item : in Wide_String; 
    Append_Nul : in Boolean := True) 
return char16_array;

function To_Ada (Item : in char16_array; 
    Trim_Nul : in Boolean := True) 
return Wide_String;

procedure To_C (Item : in Wide_String; 
    Target : out char16_array; 
    Count : out size_t; 
    Append_Nul : in Boolean := True); 

procedure To_Ada (Item : in char16_array; 
    Target : out Wide_String; 
    Count : out Natural; 
    Trim_Nul : in Boolean := True);

{AI95-00285-01} The To_C and To_Ada subprograms that convert between Wide_String and char16_array have analogous effects to the To_C and To_Ada subprograms that convert between String and char_array, except that char16_nul is used instead of nul.

function Is_Nul_Terminated (Item : in char32_array) return Boolean;

{AI95-00285-01} {AI12-0437-1} The result of Is_Nul_Terminated is True if Item contains char32_nul
char16_nul, and is False otherwise.

function To_C (Item : in Wide_Wide_Character) return char32_t;
function To_Ada (Item : in char32_t ) return Wide_Wide_Character;

{AI95-00285-01} To_C and To_Ada provide mappings between the Ada and C 32-bit character types.
function To_C (Item       : in Wide_Wide_String;
              Append_Nul : in Boolean := True)
             return char32_array;

function To_Ada (Item     : in char32_array;
                 Trim_Nul : in Boolean := True)
             return Wide_Wide_String;

procedure To_C (Item       : in Wide_Wide_String;
                Target     : out char32_array;
                Count      : out size_t;
                Append_Nul : in Boolean := True);

procedure To_Ada (Item     : in char32_array;
                  Target   : out Wide_Wide_String;
                  Count    : out Natural;
                  Trim_Nul : in Boolean := True);

{AI95-00285-01} The To_C and To_Ada subprograms that convert between Wide_Wide_String and char32_array have analogous effects to the To_C and To_Ada subprograms that convert between String and char_array, except that char32_nul is used instead of nul.

Discussion: The Interfaces.C package provides an implementation-defined character type, char, designed to model the C run-time character set, and mappings between the types char and Character.

One application of the C interface package is to compose a C string and pass it to a C function. One way to do this is for the programmer to declare an object that will hold the C array, and then pass this array to the C function. This is realized via the type char_array:

type char_array is array (size_t range <>) of Char;

The programmer can declare an Ada String, convert it to a char_array, and pass the char_array as actual parameter to the C function that is expecting a char *

An alternative approach is for the programmer to obtain a C char pointer from an Ada String (or from a char_array) by invoking an allocation function. The package Interfaces.C.Strings (see below) supplies the needed facilities, including a private type chars_ptr that corresponds to C's char *, and two allocation functions. To avoid storage leakage, a Free procedure releases the storage that was allocated by one of these allocate functions.

It is typical for a C function that deals with strings to adopt the convention that the string is delimited by a nul char. The C interface packages support this convention. A constant nul of type Char is declared, and the function Value(Chars_Ptr) in Interfaces.C.Strings returns a char_array up to and including the first nul in the array that the chars_ptr points to. The Allocate_Chars function allocates an array that is nul terminated.

Some C functions that deal with strings take an explicit length as a parameter, thus allowing strings to be passed that contain nul as a data element. Other C functions take an explicit length that is an upper bound: the prefix of the string up to the char before nul, or the prefix of the given length, is used by the function, whichever is shorter. The C Interface packages support calling such functions.

{8652/0059} {AI95-00131-01} {AI95-0229-1} The Convention aspectpragma with convention_identifier C_Pass_By_Copy shall only be specified for applied to a type.

{8652/0059} {AI95-00131-01} {AI95-00216-01} The eligibility rules in B.1 do not apply to convention C_Pass_By_Copy. Instead, a type T is eligible for convention C_Pass_By_Copy if T is an unchecked union type or if T is a record type that has no discriminants and that only has components with statically constrained subtypes, and each component is C-compatible.

{AI95-00131-01} If a type is C_Pass_By_Copy-compatible, then it is also C-compatible.

{AI12-0028-1} The identifiers C_Variadic_0, C_Variadic_1, C_Variadic_2, and so on are convention identifiers. These conventions are said to be C_Variadic. The convention C_Variadic_n is the calling convention for a variadic C function taking n fixed parameters and then a variable number of additional parameters. The C_Variadic_n convention shall only be specified as the convention aspect for a subprogram, or for an access-to-subprogram type, having at least n parameters. A type is compatible with a C_Variadic convention if and only if the type is C-compatible.
To be honest: It is implementation defined what the largest $n$ in C Variadic $n$ is supported. We don't say this because it complicates the wording and it is true for almost any convention identifier (only Ada is required to be supported by the language, all others need to be documented in order for programmers to know that they are available).

Implementation Requirements

{8652/0059} {AI95-00131-01} {AI05-0229-1} An implementation shall support specifying aspect pragma Convention with a C convention identifier for a C-eligible type (see B.1). An implementation shall support specifying aspect pragma Convention with a C Pass By Copy convention identifier for a C Pass By Copy-eligible type.

Implementation Permissions

An implementation may provide additional declarations in the C interface packages.

{AI05-0002-1} {AI05-0229-1} {AI12-0444-1} An implementation is not required to support specifying the Convention aspect with convention identifier C in the following cases:

- {AI05-0248-1} for a subprogram that has a parameter of an unconstrained array subtype, unless the Import aspect has the value True for the subprogram;
- for a function with an unconstrained array result subtype;
- for an object whose nominal subtype is an unconstrained array subtype.

Implementation Note: {AI05-0002-1} These rules ensure that an implementation never needs to create bounds for an unconstrained array that originates in C (and thus does not have bounds). An implementation can do so if it wishes, of course. Note that these permissions do not extend to passing an unconstrained array as a parameter to a C function; in this case, the bounds can simply be dropped and thus support is required.

Implementation Advice

{8652/0060} {AI95-00037-01} {AI95-00285-01} The constants nul, and wide_nul, char16_nul, and char32_nul should have a representation of zero.

Implementation Advice: The constants nul, wide nul, char16 nul, and char32 nul in package Interfaces.C should have a representation of zero.

An implementation should support the following interface correspondences between Ada and C.

- An Ada procedure corresponds to a void-returning C function.
  Discussion: The programmer can also choose an Ada procedure when the C function returns an int that is to be discarded.
- An Ada function corresponds to a non-void C function.
- {AI12-0135-1} An Ada enumeration type corresponds to a C enumeration type with corresponding enumeration literals having the same internal codes, provided the internal codes fall within the range of the C int type.
- An Ada in scalar parameter is passed as a scalar argument to a C function.
- An Ada in parameter of an access-to-object type with designated type T is passed as a t* argument to a C function, where t is the C type corresponding to the Ada type T.
- An Ada access T parameter, or an Ada out or in out parameter of an elementary type T, is passed as a t* argument to a C function, where t is the C type corresponding to the Ada type T. In the case of an elementary out or in out parameter, a pointer to a temporary copy is used to preserve by-copy semantics.
- {8652/0059} {AI95-00131-01} {AI95-00343-01} An Ada parameter of a (record) type T of convention C Pass By Copy-compatible (record) type T, of mode in, is passed as a t argument to a C function, where t is the C struct corresponding to the Ada type T.
An Ada parameter of a record type $T$, of any mode, other than an in parameter of a type of convention C Pass By Copy-compatible type, is passed as a *t argument to a C function, with the const modifier if the Ada mode is in, where t is the C struct corresponding to the Ada type T.

An Ada parameter of an array type with component type $T$, of any mode, is passed as a *t argument to a C function, with the const modifier if the Ada mode is in, where t is the C type corresponding to the Ada type T.

An Ada parameter of an access-to-subprogram type is passed as a pointer to a C function whose prototype corresponds to the designated subprogram's specification.

An Ada parameter of a private type is passed as specified for the full view of the type.

The rules of correspondence given above for parameters of mode in also apply to the return object of a function.

An implementation should provide unsigned_long_long and long_long as 64-bit modular and signed integer types (respectively) in package Interfaces.C if the C implementation supports unsigned long long and long long as 64-bit types. An Ada parameter of a private type is passed as specified for the full view of the type.

Implementation Advice: If C interfacing is supported, the interface correspondences between Ada and C should be supported.

Implementation Advice: If the C implementation supports unsigned long long, unsigned_long_long should be supported.

NOTE 1 Values of type char_array are not implicitly terminated with nul. If a char_array is to be passed as a parameter to an imported C function requiring nul termination, it is the programmer's responsibility to obtain this effect.

NOTE 2 To obtain the effect of C's sizeof(item_type), where Item_Type is the corresponding Ada type, evaluate the expression: size_t(Item_Type'Size/CHAR_BIT).

NOTE 3 There is no explicit support for C's union types. Unchecked conversions can be used to obtain the effect of C unions.

NOTE 4 A variadic C function that takes a variable number of arguments can correspond to several Ada subprograms, taking various specific numbers and types of parameters.

Examples

Example of using the Interfaces.C package:

```ada
package C renames Interfaces.C;
use type C.char_array;
-- Call <string.h>strcpy:
-- C definition of strcpy: char *strcpy(char *s1, const char *s2);
-- This function copies the string pointed to by s2 (including the terminating null character)
-- into the array pointed to by s1. If copying takes place between objects that overlap,
-- the behavior is undefined. The strcpy function returns the value of s1.
```

```ada
procedure Strcpy (Target : out C.char_array;
                  Source : in C.char_array)
  with Import => True, Convention => C, External Name => "strcpy";
```

Example of using the Interfaces.C package:

```ada
package C renames Interfaces.C;
use type C.char_array;
-- Call <string.h>strcpy:
-- C definition of strcpy: char *strcpy(char *s1, const char *s2);
-- This function copies the string pointed to by s2 (including the terminating null character)
-- into the array pointed to by s1. If copying takes place between objects that overlap,
-- the behavior is undefined. The strcpy function returns the value of s1.
```

```ada
procedure Strcpy (Target : out C.char_array;
                  Source : in C.char_array)
  with Import => True, Convention => C, External Name => "strcpy";
```
-- Call <stdio.h>printf:
-- C definition of printf: int printf (const char * format, ...);
-- This function writes the C string pointed by format to the standard output (stdout).
-- If format includes format specifiers (subsequences beginning with %), the additional
-- arguments following format are formatted and inserted in the resulting string
-- replacing their respective specifiers. If the number of arguments does not match
-- the number of format specifiers, or if the types of the arguments do not match
-- the corresponding format specifier, the behaviour is undefined. On success, the
-- printf function returns the total number of characters written to the standard output.
-- If a writing error occurs, a negative number is returned.

pragma Import(C, Strcpy, "strcpy");

-- Note: since the C function's return value is of no interest, the Ada interface is a procedure
procedure Printf (Format : in C.char_array;
Param1 : in C.char_array;
Param2 : in C.int);
with Import => True, Convention => C_Variadic_1, External_Name => "printf";
Chars1 : C.char_array(1..20);
Chars2 : C.char_array(1..20);
begin
Chars2(1..6) := "qwert" & C.nul;
Strcpy(Chars1, Chars2);
-- Now Chars1(1..6) = "qwert" & C.Nul
Printf("The String=%s, Length=%d", Chars1, Chars1'Length);
end Test;

Incompatibilities With Ada 95

Types char16_t and char32_t and their related types and operations are newly added to Interfaces.C. If Interfaces.C is referenced in a use_clause, and an entity E with the same defining_identifier as a new entity in Interfaces.C is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Extensions to Ada 95

Corrigendum: Convention C_Pass_By_Copy is new.

Wording Changes from Ada 95

Corrigendum: Clarified the intent for Nul and Wide_Nul.

Specified that an unchecked union type (see B.3.3) is eligible for convention C_Pass_By_Copy.

Specified what happens if the To_C function tries to return a null string.

Clarified that the interface correspondences also apply to private types whose full types have the specified characteristics.

Clarified that a type must have convention C_Pass_By_Copy in order to be passed by copy (not just a type that could have that convention).

Added wording to make it clear that these facilities can also be used with C++.

Incompatibilities With Ada 2005

Correction: Added a definition of correspondences for function results. Also added wording to make it clear that we do not expect the implementation to conjure bounds for unconstrained arrays out of thin air. These changes allow (but don't require) compilers to reject unreasonable uses of array types. Such uses probably didn't work anyway (and probably were rejected, no matter what the language definition said), so little existing code should be impacted.

Incompatibilities With Ada 2012

Added type C_bool and (implicitly) the enumeration literals True and False to the Interfaces.C package. Therefore, a use clause conflict is possible; see the introduction of Annex A for more on this topic.
Extensions to Ada 2012

Corrected identifiers C_Variadic_0, C_Variadic_1, and so on are new. These are classified as a correction as any implementation can add such identifiers and it is important that special conventions be available for variadic functions as typical x64 conventions are different for normal and variadic C functions.

Defined the correspondence between an Ada enumeration type and a C enumeration type; implementations should support convention C for enumeration types.

Wording Changes from Ada 2012

Added Implementation Advice that types be defined in Interfaces.C corresponding to long long and unsigned long long.

Correction: Added advice that const t* map to Ada in parameters and vice versa.

Added advice about mapping type Boolean.

B.3.1 The Package Interfaces.C.Strings

The package Interfaces.C.Strings declares types and subprograms allowing an Ada program to allocate, reference, update, and free C-style strings. In particular, the private type chars_ptr corresponds to a common use of “char *” in C programs, and an object of this type can be passed to a subprogram to which with Import => True, Convention => C pragma Import(C,...) has been specified, and for which “char *” is the type of the argument of the C function.

Static Semantics

The library package Interfaces.C.Strings has the following declaration:

```ada
{AI12-0241-1} {AI12-0302-1} package Interfaces.C.Strings with pragma Precallable, Nonblocking, Global => in out synchronized is Strings;

type char_array_access is access all char_array;

{AI95-00161-01} {AI12-0399-1} type chars_ptr is private;

{AI95-00276-01} type chars_ptr_array is array (size_t range <>) of aliased chars_ptr;

null_Ptr : constant chars_ptr;

function To_CHARS_Ptr (Item : in char_array_access; Nul_Check : in Boolean := False) return chars_ptr;

function New_Char_Array (Chars : in char_array) return chars_ptr;

function New_String (Str : in String) return chars_ptr;

procedure Free (Item : in out chars_ptr);

Dereference_Error : exception;

function Value (Item : in chars_ptr) return char_array;

function Value (Item : in chars_ptr; Length : in size_t) return char_array;

function Value (Item : in chars_ptr) return String;

function Value (Item : in chars_ptr; Length : in size_t) return String;

function Strlen (Item : in chars_ptr) return size_t;

procedure Update (Item : in chars_ptr;
    Offset : in size_t;
    Chars : in char_array;
    Check : in Boolean := True);
```
procedure Update (Item   : in chars_ptr;
          Offset : in size_t;
          Str    : in String;
          Check  : in Boolean := True);

Update_Error : exception;

private
  ... -- not specified by the language
end Interfaces.C.Strings;

Discussion: The string manipulation types and subprograms appear in a child of Interfaces.C versus being there
directly, since it is useful to have Interfaces.C specified as
pragma Pure.

Differently named functions New_String and New_Char_Array are declared, since if there were a single overloaded
function a call with a string literal as actual parameter would be ambiguous.

The type chars_ptr is C-compatible and corresponds to the use of C's “char *” for a pointer to the first
char in a char array terminated by null. When an object of type chars_ptr is declared, its value is by default
set to Null_Ptr, unless the object is imported (see B.1).

Discussion: The type char_array_access is not necessarily C-compatible, since an object of this type may carry “dope”
information. The programmer should convert from char_array_access to chars_ptr for objects imported from, exported
to, or passed to C.

function To_Chars_Ptr (Item      : in char_array_access;
          Nul_Check : in Boolean := False) return chars_ptr;

{8652/0061} {AI95-00140-01} {AI05-0264-1} If Item is null, then To_Chars_Ptr returns
Null_Ptr. If Item is not null, otherwise, if Nul_Check is True and Item.all does not contain null,
then the function propagates Terminator_Error; otherwise if Nul_Check is True and Item.all does
contain null, To_Chars_Ptr performs a pointer conversion with no allocation of memory.

function New_Char_Array (Chars   : in char_array) return chars_ptr;

This function returns a pointer to an allocated object initialized to Chars(Chars'First .. Index) &
null where
  • Index = Chars'Last if Chars does not contain null, or
  • Index is the smallest size_t value I such that Chars(I+1) = nul.

Storage_Error is propagated if the allocation fails.

function New_String (Str     : in String) return chars_ptr;

This function is equivalent to New_Char_Array(To_C(Str)).

procedure Free (Item : in out chars_ptr);

If Item is Null_Ptr, then Free has no effect. Otherwise, Free releases the storage occupied by
Value(Item), and resets Item to Null_Ptr.

function Value (Item : in chars_ptr) return char_array;

{AI05-0264-1} If Item = Null_Ptr, then Value propagates Dereference_Error. Otherwise, Value
returns the prefix of the array of chars pointed to by Item, up to and including the first null. The
lower bound of the result is 0. If Item does not point to a null-terminated string, then execution of
Value is erroneous.

function Value (Item : in chars_ptr; Length : in size_t) return char_array;

{8652/0062} {AI95-00139-01} {AI05-0264-1} If Item = Null_Ptr, then Value(Item) propagates
Dereference_Error. Otherwise, Value returns the shorter of two arrays, either the first Length
chars pointed to by Item, and Value(Item). The lower bound of the result is 0. If Length is 0, then Value propagates Constraint_Error.

**Ramification:** Value(New_Char_Array(Chars)) = Chars if Chars does not contain nul; else Value(New_Char_Array(Chars)) is the prefix of Chars up to and including the first nul.

```ada
function Value (Item : in chars_ptr) return String;
```
Equivalent to To_Ada(Value(Item), Trim_Nul=>True).

```ada
function Value (Item : in chars_ptr; Length : in size_t) return String;
```
Equivalent to To_Ada(Value(Item, Length) & nul, Trim_Nul=>True).

```ada
function Strlen (Item : in chars_ptr) return size_t;
```
Returns Val'Length–1 where Val = Value(Item); propagates Dereference_Error if Item = Null_Ptr.

**Ramification:** Strlen returns the number of chars in the array pointed to by Item, up to and including the char immediately before the first nul.

Strlen has the same possibility for erroneous execution as Value, in cases where the string has not been nul-terminated.

Strlen has the effect of C's strlen function.

```ada
procedure Update (Item   : in chars_ptr;
   Offset : in size_t;
   Chars  : in char_array;
   Check  : Boolean := True);
```
If Item = Null_Ptr, then Update propagates Dereference_Error. Otherwise, this procedure updates the value pointed to by Item, starting at position Offset, using Chars as the data to be copied into the array. Overwriting the nul terminator, and skipping with the Offset past the nul terminator, are both prevented if Check is True, as follows:

- Let N = Strlen(Item). If Check is True, then:
  - If Offset+Chars'Length>N, propagate Update_Error.
  - Otherwise, overwrite the data in the array pointed to by Item, starting at the char at position Offset, with the data in Chars.
- If Check is False, then processing is as above, but with no check that Offset+Chars'Length>N.

**Ramification:** If Chars contains nul, Update's effect may be to “shorten” the pointed-to char array.

```ada
procedure Update (Item   : in chars_ptr;
   Offset : in size_t;
   Str    : in String;
   Check  : in Boolean := True);
```
Equivalent to Update(Item, Offset, To_C(Str, Append_Nul => False), Check).

**Discussion:** To truncate the Item to the length of Str, use Update(Item, Offset, To_C(Str), Check) instead of Update(Item, Offset, Str, Check). Note that when truncating Item, Item must be longer than Str.

**Erroneous Execution**

Execution of any of the following is erroneous if the Item parameter is not null_ptr and Item does not point to a nul-terminated array of chars.

- a Value function not taking a Length parameter,
- the Free procedure,
• the Strlen function.

Execution of Free(X) is also erroneous if the chars_ptr X was not returned by New_Char_Array or New_String.

Reading or updating a freed char_array is erroneous.

Execution of Update is erroneous if Check is False and a call with Check equal to True would have propagated Update_Error.

NOTE {AI12-0440-1} New_Char_Array and New_String can
might
be implemented either through the allocation function
from the C environment (“malloc”) or through Ada dynamic memory allocation (“new”). The key points are
• {AI12-0440-1} the returned value (a chars_ptr) is represented as a C “char *” so that it can
may
be passed to C
functions;
• {AI12-0442-1} the allocated object can
should
be freed by the programmer via a call of Free, rather than by calling
not by a called C function.

Inconsistencies With Ada 95

{AI95-00242-01} Amendment Correction: Update for a String parameter is now defined to not add a nul character. It did add a nul in Ada 95. This means that programs that used this behavior of Update to truncate a string will no longer work (the string will not be truncated). This change makes Update for a string consistent with Update for a char_array (no implicit nul is added to the end of a char_array).

{AI95-00161-01} Amendment Correction: Added pragma Preelaborable_Initialization to type chars_ptr, so that it can be used in preelaborated units.

{AI95-00276-01} Amendment Correction: The components of chars_ptr_array are aliased so that it can be used to instantiate Interfaces.C.Pointers (that is its intended purpose, which is otherwise mysterious as it has no operations).

Extensions to Ada 95

{AI95-00039-01} Amendment Correction: Fixed the missing semantics of Update when Item is Null_Ptr.

Wording Changes from Ada 95

{8652/0061} {AI95-00140-01} Corrigendum: Fixed the missing semantics of To_Char_Ptr when Nul_Check is False.

{8652/0062} {AI95-00139-01} Corrigendum: Fixed the missing semantics of Value when the Length is 0.

{8652/0063} {AI95-00177-01} Corrigendum: Corrected the definition of Value to avoid raising Terminator_Error.

{8652/0064} {AI95-00039-01} Corrigendum: Fixed the missing semantics of Update when Item is Null_Ptr.

B.3.2 The Generic Package Interfaces.C.Pointers

The generic package Interfaces.C.Pointers allows the Ada programmer to perform C-style operations on pointers. It includes an access type Pointer, Value functions that dereference a Pointer and deliver the designated array, several pointer arithmetic operations, and “copy” procedures that copy the contents of a source pointer into the array designated by a destination pointer. As in C, it treats an object Ptr of type Pointer as a pointer to the first element of an array, so that for example, adding 1 to Ptr yields a pointer to the second element of the array.

{AI12-0445-1} The generic allows two styles of usage: one in which the array is terminated by a special terminator element; and another in which the programmer keeps needs to keep track of the length.

Static Semantics

The generic library package Interfaces.C.Pointers has the following declaration:
generic
  type Index is <>;
  type Element is private;
  type Element_Array is array (Index range <>) of aliased Element;
Default_Terminator : Element;
package Interfaces.C.Pointers is
  withpragma Preelaborate, Nonblocking, Global => in out synchronized
is (Pointers);
type Pointer is access all Element;
function Value(Ref : in Pointer;
  Terminator : in Element := Default_Terminator)
  return Element_Array;
function Value(Ref : in Pointer;
  Length : in ptrdiff_t)
  return Element_Array;
Pointer_Error : exception;
-- C-style Pointer arithmetic
function "+" (Left : in Pointer;   Right : in ptrdiff_t) return Pointer
  with Convention => Intrinsic;
function "+" (Left : in ptrdiff_t; Right : in Pointer) return Pointer
  with Convention => Intrinsic;
function "+" (Left : in Pointer; Right : in Pointer) return Pointer
  with Convention => Intrinsic;
function "-" (Left : in Pointer; Right : in ptrdiff_t) return Pointer
  with Convention => Intrinsic;
function "-" (Left : in Pointer; Right : in Pointer) return ptrdiff_t
  with Convention => intrinsic;
procedure Increment (Ref : in out Pointer)
  with Convention => Intrinsic;
procedure Decrement (Ref : in out Pointer)
  with Convention => intrinsic;
procedure Copy_Terminated_Array
  (Source : in Pointer;
  Target : in Pointer;
  Limit : in ptrdiff_t := ptrdiff_t'Last;
  Terminator : in Element := Default_Terminator);
procedure Copy_Array
  (Source : in Pointer;
  Target : in Pointer;
  Length : in ptrdiff_t);
end Interfaces.C.Pointers;

The type Pointer is C-compatible and corresponds to one use of C's "Element *". An object of type Pointer is interpreted as a pointer to the initial Element in an Element_Array. Two styles are supported:
  • Explicit termination of an array value with Default_Terminator (a special terminator value);
  • Programmer-managed length, with Default_Terminator treated simply as a data element.

function Value(Ref : in Pointer;
  Terminator : in Element := Default_Terminator)
  return Element_Array;
This function returns an Element_Array whose value is the array pointed to by Ref, up to and including the first Terminator; the lower bound of the array is Index'First. Interfaces.C.Strings.Dereference_Error is propagated if Ref is null.
**function** Value(Ref : in Pointer;
   Length : in ptrdiff_t)
**return** Element_Array;

This function returns an Element_Array comprising the first Length elements pointed to by Ref. The exception Interfaces.C.Strings.Dereference_Error is propagated if Ref is *null*.

The "+" and "-" functions perform arithmetic on Pointer values, based on the Size of the array elements. In each of these functions, Pointer_Error is propagated if a Pointer parameter is *null*.

**procedure** Increment (Ref : in out Pointer);

   Equivalent to Ref := Ref+1.

**procedure** Decrement (Ref : in out Pointer);

   Equivalent to Ref := Ref–1.

**function** Virtual_Length (Ref        : in Pointer;
   Terminator : in Element := Default_Terminator)
**return** ptrdiff_t;

Returns the number of Elements, up to the one just before the first Terminator, in Value(Ref, Terminator).

**procedure** Copy_Terminated_Array
   (Source     : in Pointer;
    Target     : in Pointer;
    Limit      : in ptrdiff_t := ptrdiff_t'Last;
    Terminator : in Element := Default_Terminator);

This procedure copies Value(Source, Terminator) into the array pointed to by Target; it stops either after Terminator has been copied, or the number of elements copied is Limit, whichever occurs first. Dereference_Error is propagated if either Source or Target is *null*.

**Ramification**: It is the programmer's responsibility to ensure that elements are not copied beyond the logical length of the target array.

**Implementation Note**: The implementation has to take care to check the Limit first.

**procedure** Copy_Array (Source  : in Pointer;
    Target  : in Pointer;
    Length  : in ptrdiff_t);

This procedure copies the first Length elements from the array pointed to by Source, into the array pointed to by Target. Dereference_Error is propagated if either Source or Target is *null*.

**Erroneous Execution**

It is erroneous to dereference a Pointer that does not designate an aliased Element.

**Discussion**: Such a Pointer could arise via "+", "-", Increment, or Decrement.

Execution of Value(Ref, Terminator) is erroneous if Ref does not designate an aliased Element in an Element_Array terminated by Terminator.

Execution of Value(Ref, Length) is erroneous if Ref does not designate an aliased Element in an Element_Array containing at least Length Elements between the designated Element and the end of the array, inclusive.

Execution of Virtual_Length(Ref, Terminator) is erroneous if Ref does not designate an aliased Element in an Element_Array terminated by Terminator.

Execution of Copy_Terminated_Array(Source, Target, Limit, Terminator) is erroneous in either of the following situations:
Execution of both Value(Source, Terminator) and Value(Source, Limit) are erroneous, or

Copying writes past the end of the array containing the Element designated by Target.

Execution of Copy_Array(Source, Target, Length) is erroneous if either Value(Source, Length) is erroneous, or copying writes past the end of the array containing the Element designated by Target.

NOTE To compose a Pointer from an Element_Array, use 'Access on the first element. For example (assuming appropriate instantiations):

```ada
Some_Array : Element_Array(0..5) ;
Some_Pointer : Pointer := Some_Array(0)'Access;
```

**Examples**

**Example of Interfaces.C.Pointers:**

```ada
with Interfaces.C.Pointers;
with Interfaces.C.Strings;
procedure Test_Pointers is
package C renames Interfaces.C;
package Char_Ptrs is
  new C.Pointers (Index              => C.size_t,
                   Element            => C.char,
                   Element_Array      => C.char_array,
                   Default_Terminator => C.nul);
use type Char_Ptrs.Pointer;
subtype Char_Star is Char_Ptrs.Pointer;
procedure Strcpy (Target_Ptr, Source_Ptr : Char_Star) is
  Target_Temp_Ptr : Char_Star := Target_Ptr;
  Source_Temp_Ptr : Char_Star := Source_Ptr;
  Element : C.char;
  begin
    if Target_Temp_Ptr = null or Source_Temp_Ptr = null then
      raise C.Strings.Dereference_Error;
    end if;
    loop
      Element := Source_Temp_Ptr.all;
      Target_Temp_Ptr.all := Element;
      exit when C."="(Element, C.nul) Element = C.nul;
    Char_Ptrs.Increment(Target_Temp_Ptr);
    Char_Ptrs.Increment(Source_Temp_Ptr);    
    end loop;
  end Strcpy;
begin
...
end Test_Pointers;
```

### B.3.3 Unchecked Union Types Pragmas

**Pragma Unchecked-Union**

[Specifying aspectA pragma Unchecked_Union to have the value True defines an interface correspondence between a given discriminated type and some C union. The aspect requires that the associated type shall be given a representation that allocates no space for its discriminant(s).]

Paragraphs 2 through 3 were moved to Annex J, “Obsolescent Features”.

**Syntax**

```ada
pragma Unchecked_Union (first_subtype_local_name);
```

---

**B.3.2** The Generic Package Interfaces.C.Pointers
Static Semantics

For a discriminated record type having a variant part, the following language-defined representation aspect may be specified:

Unchecked_Union

The type of aspect Unchecked_Union is Boolean. If directly specified, the aspect_definition shall be a static expression. If not specified (including by inheritance), the aspect is False.

Aspect Description for Unchecked_Union: Type is used to interface to a C union type.

Legality Rules

Paragraphs 4 and 5 were deleted.

Unchecked_Union is a representation pragma, specifying the unchecked union aspect of representation.

The first_subtype_local_name of a pragma Unchecked_Union shall denote an unconstrained discriminated record subtype having a variant_part.

A type for which aspect pragma Unchecked_Union is True applies is called an unchecked union type. A subtype of an unchecked union type is defined to be an unchecked union subtype. An object of an unchecked union type is defined to be an unchecked union object.

All component subtypes of an unchecked union type shall be C-compatible.

If a component subtype of an unchecked union type is subject to a per-object constraint, then the component subtype shall be an unchecked union subtype.

Any name that denotes a discriminant of an object of an unchecked union type shall occur within the declarative region of the type or as the selector_name of an aggregate, and shall not occur within a record_representation_clause.

The type of a component declared in a variant_part of an unchecked union type shall not need finalization. In addition to the places where Legality Rules normally apply (see 12.3), this rule also applies in the private part of an instance of a generic unit. For an unchecked union type declared within the body of a generic unit, or within the body of any of its descendant library units, no part of the type of a component declared in a variant_part of the unchecked union type shall be of a formal private type or formal private extension declared within the formal part of the generic unit have a controlled, protected, or task part.

Reason: The last part is a classic assume-the-worst rule that avoids dependence on the actuals in a generic body. We did not include this in the definition of “needs finalization” as it has a bad interaction with the use of that term for the No_Nested_Finalization restriction.

The completion of an incomplete or private type declaration having a known_discriminant_part shall not be an unchecked union type.

An unchecked union subtype shall only be passed as a generic actual parameter if the corresponding formal type has no known discriminants or is an unchecked union type.

This includes formal private types without a known_discriminant_part, formal derived types that do not inherit any discriminants (formal derived types do not have known_discriminant_parts), and formal derived types that are unchecked union types.

Static Semantics

An unchecked union type is eligible for convention C.

All objects of an unchecked union type have the same size.
Discriminants of objects of an unchecked union type are of size zero.

Any check which would require reading a discriminant of an unchecked union object is suppressed (see 11.5). These checks include:

- The check performed when addressing a variant component (that is, a component that was declared in a variant part) of an unchecked union object that the object has this component (see 4.1.3).
- Any checks associated with a type or subtype conversion of a value of an unchecked union type (see 4.6). This includes, for example, the check associated with the implicit subtype conversion of an assignment statement.
- The subtype membership check associated with the evaluation of a qualified expression (see 4.7) or an uninitialized allocator (see 4.8).

Discussion: If a suppressed check would have failed, execution is erroneous (see 11.5). An implementation is always allowed to make a suppressed check if it can somehow determine the discriminant value.

Dynamic Semantics

A view of an unchecked union object (including a type conversion or function call) has inferable discriminants if it has a constrained nominal subtype, unless the object is a component of an enclosing unchecked union object that is subject to a per-object constraint and the enclosing object lacks inferable discriminants.

An expression of an unchecked union type has inferable discriminants if it is either a name of an object with inferable discriminants or a qualified expression whose subtype_mark denotes a constrained subtype.

Program_Error is raised in the following cases:

- Evaluation of the predefined equality operator for an unchecked union type if either of the operands lacks inferable discriminants.
- Evaluation of the predefined equality operator for a type which has a subcomponent of an unchecked union type whose nominal subtype is unconstrained.
- Evaluation of an individual membership test if the subtype_mark (if any) denotes a constrained unchecked union subtype and the tested_simple_expression lacks inferable discriminants.
- Conversion from a derived unchecked union type to an unconstrained non-unchecked-union type if the operand of the conversion lacks inferable discriminants.
- Execution of the default implementation of the Write or Read attribute of an unchecked union type.
- Execution of the default implementation of the Output or Input attribute of an unchecked union type if the type lacks default discriminant values.

Implementation Permissions

An implementation may require that pragma Controlled be specified for the type of an access subcomponent of an unchecked union type.

Paragraph 29 was deleted.
NOTE \{AI95-00216-01\} The use of an unchecked union to obtain the effect of an unchecked conversion results in erroneous execution (see 11.5). Execution of the following example is erroneous even if Float’Size = Integer’Size:

\{AI05-0229-1\} type T (Flag : Boolean := False) is  
record  
  case Flag is  
    when False =>  
      F1 : Float := 0.0;  
    when True =>  
      F2 : Integer := 0;  
  end case;  
end record  
with Unchecked_Union;  
pragma Unchecked_Union (T);  
X : T;  
Y : Integer := X.F2; -- erroneous

Extensions to Ada 95

\{AI95-00216-01\} **Pragma Unchecked_Union is new.**

Incompatibilities With Ada 2005

\{AI05-0026-1\} **Correction:** The use of discriminants on Unchecked_Union types is now illegal in record_representation_clauses, as it makes no sense to specify a position for something that is not supposed to exist. It is very unlikely that this change will have any impact on existing code.

Extensions to Ada 2005

\{AI05-0229-1\} **Aspect Unchecked_Union is new; pragma Unchecked_Union is now obsolescent.**

Wording Changes from Ada 2005

\{AI05-0026-1\} **Correction:** Revised the rules to use the “needs finalization” definition, and eliminated generic contract issues.

Wording Changes from Ada 2012

\{AI05-0162-1\} **Correction:** Adjusted the wording to reflect that membership tests can have more than one expression or subtype_mark.

\{AI05-0174-1\} **Correction:** Adjusted the wording to allow named aggregates of an unchecked union type; it is clearly madness to allow positional record components in an aggregate but not named component associations.

B.4 Interfacing with COBOL

\{AI05-0229-1\} The facilities relevant to interfacing with the COBOL language are the package Interfaces.COBOL and support for specifying the Import, Export and Convention aspect pragmas with convention_identifier COBOL.

The COBOL interface package supplies several sets of facilities:

- A set of types corresponding to the native COBOL types of the supported COBOL implementation (so-called “internal COBOL representations”), allowing Ada data to be passed as parameters to COBOL programs
- \{AI12-0439-1\} A set of types and constants reflecting external data representations such as cannot be found in files or databases, allowing COBOL-generated data to be read by an Ada program, and Ada-generated data to be read by COBOL programs
- A generic package for converting between an Ada decimal type value and either an internal or external COBOL representation

Unchanged Union Types B.3.3
Static Semantics

The library package Interfaces.COBOL has the following declaration:

```ada
package Interfaces.COBOL is
  with pragma Preelaborate, Nonblocking, Global => in out synchronized is (COBOL);
end Interfaces.COBOL;
```

-- Types and operations for internal data representations

```ada
type Floating is digits implementation-defined;
type Long_Floating is digits implementation-defined;
type Binary is range implementation-defined;
type Long_Binary is range implementation-defined;
Max_Digits_Binary : constant := implementation-defined;
Max_Digits_Long_Binary : constant := implementation-defined;
```

```ada
{AI05-0229-1} type Decimal_Element is mod implementation-defined;
type Packed_Decimal is array (Positive range <>) of Decimal_Element;
pragma Pack(Packed_Decimal);

type COBOL_Character is implementation-defined character type;
Ada_To_COBOL : array (Character) of COBOL_Character := implementation-defined;
COBOL_To_Ada : array (COBOL_Character) of Character := implementation-defined;
```

```ada
{AI05-0229-1} type Alphanumeric is array (Positive range <>) of COBOL_Character;
pragma Pack(Alphanumeric);

function To_COBOL (Item : in String) return Alphanumeric;
function To_Ada   (Item : in Alphanumeric) return String;
procedure To_COBOL (Item : in String; Target : out Alphanumeric; Last : out Natural);
procedure To_Ada (Item : in Alphanumeric; Target : out String; Last : out Natural);
```

```ada
{AI05-0229-1} type Numeric is array (Positive range <>) of COBOL_Character;
pragma Pack(Numeric);
```

-- Formats for COBOL data representations

```ada
type Display_Format is private;
  Unsigned             : constant Display_Format;
  Leading_Separate     : constant Display_Format;
  Trailing_Separate    : constant Display_Format;
  Leading_Nonseparate  : constant Display_Format;
  Trailing_Nonseparate : constant Display_Format;

type Binary_Format is private;
  High_Order_First  : constant Binary_Format;
  Low_Order_First   : constant Binary_Format;
  Native_Binary     : constant Binary_Format;

{AI05-0229-1} type Packed_Format is private;
  Packed_Unsigned   : constant Packed_Format;
  Packed_Signed     : constant Packed_Format;
```

-- Types for external representation of COBOL binary data

```ada
{AI05-0229-1} type Byte is mod 2**COBOL_Character'Size;
type Byte_Array is array (Positive range <>) of Byte;
pragma Pack (Byte_Array);

Conversion_Error : exception;
```
**Ada 202y Draft 1 — Annotated Ada Reference Manual**

```Ada
generic
  type Num is delta <> digits <>;
package Decimal_Conversions is
  -- Display Formats: data values are represented as Numeric
  function Valid (Item : in Numeric; Format : in Display_Format) return Boolean;
  function Length (Format : in Display_Format) return Natural;
  function To_Decimal (Item : in Numeric; Format : in Display_Format) return Num;
  function To_Display (Item : in Num; Format : in Display_Format) return Numeric;
  -- Packed Formats: data values are represented as Packed_Decimal
  function Valid (Item : in Packed_Decimal; Format : in Packed_Format) return Boolean;
  function Length (Format : in Packed_Format) return Natural;
  function To_Decimal (Item : in Packed_Decimal; Format : in Packed_Format) return Num;
  function To_Packed (Item : in Num; Format : in Packed_Format) return Packed_Decimal;
  -- Binary Formats: external data values are represented as Byte_Array
  function Valid (Item : in Byte_Array; Format : in Binary_Format) return Boolean;
  function Length (Format : in Binary_Format) return Natural;
  function To_Decimal (Item : in Byte_Array; Format : in Binary_Format) return Num;
  function To_Binary (Item : in Num; Format : in Binary_Format) return Byte_Array;
  -- Internal Binary formats: data values are of type Binary or Long_Binary
  function To_Decimal (Item : in Binary) return Num;
  function To_Decimal (Item : in Long_Binary) return Num;
  function To_Binary (Item : in Num) return Binary;
  function To_Long_Binary (Item : in Num) return Long_Binary;
end Decimal_Conversions;
private
  ... -- not specified by the language
end Interfaces.COBOL;
```

**Implementation defined:** The types Floating, Long_Floating, Binary, Long_Binary, Decimal_Element, and COBOL_Character; and the initializations of the variables Ada_To_COBOL and COBOL_To_Ada, in Interfaces.COBOL.

Each of the types in Interfaces.COBOL is COBOL-compatible.

The types Floating and Long_Floating correspond to the native types in COBOL for data items with computational usage implemented by floating point. The types Binary and Long_Binary correspond to the native types in COBOL for data items with binary usage, or with computational usage implemented by binary.

Max_Digits_Binary is the largest number of decimal digits in a numeric value that is represented as Binary. Max_Digits_Long_Binary is the largest number of decimal digits in a numeric value that is represented as Long_Binary.

The type Packed_Decimal corresponds to COBOL's packed-decimal usage.

---

1223   16 October 2023  Interfacing with COBOL   B.4
The type COBOL_Character defines the run-time character set used in the COBOL implementation. Ada_To_COBOL and COBOL_To_Ada are the mappings between the Ada and COBOL run-time character sets.

**Reason:** The character mappings are visible variables, since the user needs the ability to modify them at run time.

Type Alphanumeric corresponds to COBOL’s alphanumeric data category.

Each of the functions To_COBOL and To_Ada converts its parameter based on the mappings Ada_To_COBOL and COBOL_To_Ada, respectively. The length of the result for each is the length of the parameter, and the lower bound of the result is 1. Each component of the result is obtained by applying the relevant mapping to the corresponding component of the parameter.

Each of the procedures To_COBOL and To_Ada copies converted elements from Item to Target, using the appropriate mapping (Ada_To_COBOL or COBOL_To_Ada, respectively). The index in Target of the last element assigned is returned in Last (0 if Item is a null array). If Item'Length exceeds Target'Length, Constraint_Error is propagated.

Type Numeric corresponds to COBOL’s numeric data category with display usage.

The types Display_Format, Binary_Format, and Packed_Format are used in conversions between Ada decimal type values and COBOL internal or external data representations. The value of the constant Native_Binary is either High_Order_First or Low_Order_First, depending on the implementation.

```ada
function Valid (Item   : in Numeric;  
               Format : in Display_Format) return Boolean;
```

The function Valid checks that the Item parameter has a value consistent with the value of Format. If the value of Format is other than Unsigned, Leading_Separate, and Trailing_Separate, the effect is implementation defined. If Format does have one of these values, the following rules apply:

- **{8652/0066} {AI95-00071-01} {AI05-0264-1}** Format=Unsigned: if Item comprises zero or more leading space characters followed by one or more decimal digit characters, then Valid returns True, else it returns False.

- **{8652/0066} {AI95-00071-01}** Format=Leading_Separate: if Item comprises zero or more leading space characters, followed by a single occurrence of the plus or minus sign character, and then one or more decimal digit characters, then Valid returns True, else it returns False.

- **{8652/0066} {AI95-00071-01}** Format=Trailing_Separate: if Item comprises zero or more leading space characters, followed by one or more decimal digit characters and finally a plus or minus sign character, then Valid returns True, else it returns False.

```ada
function Length (Format : in Display_Format) return Natural;
```

The Length function returns the minimal length of a Numeric value sufficient to hold any value of type Num when represented as Format.

```ada
function To_Decimal (Item   : in Numeric;  
                    Format : in Display_Format) return Num;
```

Produces a value of type Num corresponding to Item as represented by Format. The number of digits after the assumed radix point in Item is Num'Scale. Conversion_Error is propagated if the value represented by Item is outside the range of Num.

**Discussion:** There is no issue of truncation versus rounding, since the number of decimal places is established by Num'Scale.
function To_Display (Item: in Num; Format: in Display_Format) return Numeric;

{8652/0067} {AI95-00072-01} This function returns the Numeric value for Item, represented in accordance with Format. The length of the returned value is Length(Format), and the lower bound is 1. Conversion_Error is propagated if Num is negative and Format is Unsigned.

function Valid (Item: in Packed.Decimal; Format: in Packed.Format) return Boolean;

This function returns True if Item has a value consistent with Format, and False otherwise. The rules for the formation of Packed.Decimal values are implementation defined.

function Length (Format: in Packed.Format) return Natural;

This function returns the minimal length of a Packed.Decimal value sufficient to hold any value of type Num when represented as Format.

function To.Decimal (Item: in Packed.Decimal; Format: in Packed.Format) return Num;

Produces a value of type Num corresponding to Item as represented by Format. Num'Scale is the number of digits after the assumed radix point in Item. Conversion_Error is propagated if the value represented by Item is outside the range of Num.

function To_Packed (Item: in Num; Format: in Packed_Format) return Packed_Decimal;

{8652/0067} {AI95-00072-01} This function returns the Packed_Decimal value for Item, represented in accordance with Format. The length of the returned value is Length(Format), and the lower bound is 1. Conversion_Error is propagated if Num is negative and Format is PackedUnsigned.

function Valid (Item: in Byte_Array; Format: in Binary_Format) return Boolean;

This function returns True if Item has a value consistent with Format, and False otherwise.

Ramification: This function returns False only when the represented value is outside the range of Num.

function Length (Format: in Binary_Format) return Natural;

This function returns the minimal length of a Byte_Array value sufficient to hold any value of type Num when represented as Format.

function To_Decimal (Item: in Byte_Array; Format: in Binary_Format) return Num;

Produces a value of type Num corresponding to Item as represented by Format. Num'Scale is the number of digits after the assumed radix point in Item. Conversion_Error is propagated if the value represented by Item is outside the range of Num.

function To_Binary (Item: in Num; Format: in Binary_Format) return Byte_Array;

{8652/0067} {AI95-00072-01} This function returns the Byte_Array value for Item, represented in accordance with Format. The length of the returned value is Length(Format), and the lower bound is 1.
function To_Decimal (Item : in Binary) return Num;
function To_Decimal (Item : in Long_Binary) return Num;

These functions convert from COBOL binary format to a corresponding value of the decimal type Num. Conversion_Error is propagated if Item is too large for Num.

**Ramification:** There is no rescaling performed on the conversion. That is, the returned value in each case is a “bit copy” if Num has a binary radix. The programmer is responsible for maintaining the correct scale.

function To_Binary (Item : in Num) return Binary;
function To_Long_Binary (Item : in Num) return Long_Binary;

These functions convert from Ada decimal to COBOL binary format. Conversion_Error is propagated if the value of Item is too large to be represented in the result type.

**Discussion:** One style of interface supported for COBOL, similar to what is provided for C, is the ability to call and pass parameters to an existing COBOL program. Thus the interface package supplies types that can be used in an Ada program as parameters to subprograms whose bodies will be in COBOL. These types map to COBOL's alphanumeric and numeric data categories.

Several types are provided for support of alphanumeric data. Since COBOL's run-time character set is not necessarily the same as Ada's, Interfaces.COBOL declares an implementation-defined character type COBOL_Character, and mappings between Character and COBOL_Character. These mappings are visible variables (rather than, say, functions or constant arrays), since in the situation where COBOL_Character is EBCDIC, the flexibility of dynamically modifying the mappings is needed. Corresponding to COBOL's alphanumeric data is the string type Alphanumeric.

Numeric data may have either a “display” or “computational” representation in COBOL. On the Ada side, the data is of a decimal fixed point type. Passing an Ada decimal data item to a COBOL program requires conversion from the Ada decimal type to some type that reflects the representation expected on the COBOL side.

- **Computational Representation**
  - Floating point representation is modeled by Ada floating point types, Floating and Long_Floating. Conversion between these types and Ada decimal types is obtained directly, since the type name serves as a conversion function.
  - Binary representation is modeled by an Ada integer type, Binary, and possibly other types such as Long_Binary. Conversion between, say, Binary and a decimal type is through functions from an instantiation of the generic package Decimal_Conversions.
  - Packed decimal representation is modeled by the Ada array type Packed_Decimal. Conversion between packed decimal and a decimal type is through functions from an instantiation of the generic package Decimal_Conversions.

- **Display Representation**
  - Display representation for numeric data is modeled by the array type Numeric. Conversion between display representation and a decimal type is through functions from an instantiation of the generic package Decimal_Conversions. A parameter to the conversion function indicates the desired interpretation of the data (e.g., signed leading separate, etc.)

**Implementation Requirements**

![AI05-0229-1](ThePragma Convention of COBOL_T may be applied to a record type may be specified as COBOL_T to direct the compiler to choose a COBOL-compatible representation for objects of the type.)

The package Interfaces.COBOL allows the Ada programmer to deal with data from files (or databases) created by a COBOL program. For data that is alphanumeric, or in display or packed decimal format, the approach is the same as for passing parameters (instantiate Decimal_Conversions to obtain the needed conversion functions). For binary data, the external representation is treated as a Byte array, and an instantiation of Decimal_IO produces a package that declares the needed conversion functions. A parameter to the conversion function indicates the desired interpretation of the data (e.g., high-versus low-order byte first).

**Ramification:** An implementation supporting this package shall ensure that if the bounds of a Packed_Decimal, Alphanumeric, or Numeric variable are static, then the representation of the object comprises solely the array components (that is, there is no implicit run-time “descriptor” that is part of the object).
### Implementation Permissions

An implementation may provide additional constants of the private types Display_Format, Binary_Format, or Packed_Format.

**Reason:** This is to allow exploitation of other external formats that may be available in the COBOL implementation.

An implementation may provide further floating point and integer types in Interfaces.COBOL to match additional native COBOL types, and may also supply corresponding conversion functions in the generic package Decimal_Conversions.

### Implementation Advice

An Ada implementation should support the following interface correspondences between Ada and COBOL.

- An Ada `access T parameter is passed as a “BY REFERENCE” data item of the COBOL type corresponding to T.
- An Ada `in scalar parameter is passed as a “BY CONTENT” data item of the corresponding COBOL type.
- Any other Ada parameter is passed as a “BY REFERENCE” data item of the COBOL type corresponding to the Ada parameter type; for scalars, a local copy is used if necessary to ensure by-copy semantics.

**Implementation Advice:** If COBOL interfacing is supported, the interface correspondences between Ada and COBOL should be supported.

**Note 1** \{AI05-0229-1\} An implementation is not required to support specifying aspect `pragma Convention for access types, nor is it required to support specifying aspect `pragma Import, Export, or Convention for functions.

**Reason:** COBOL does not have a pointer facility, and a COBOL program does not return a value.

**Note 2** \{AI12-0440-1\} If an Ada subprogram is exported to COBOL, then a call from COBOL call can only specify either “BY CONTENT” or “BY REFERENCE”.

### Examples of Interfaces.COBOL:

```ada
with Interfaces.COBOL;

procedure Test_Call is
  -- Calling a foreign COBOL program
  -- Assume that a COBOL program PROG has the following declaration
  -- in its LINKAGE section:
  -- 01 Parameter-Area
  -- 05 NAME PIC X(20).
  -- 05 SSN PIC X(9).
  -- 05 SALARY PIC 99999V99 USAGE COMP.
  -- The effect of PROG is to update SALARY based on some algorithm

  package COBOL renames Interfaces.COBOL;
  type Salary_Type is delta 0.01 digits 7;

  {AI05-0229-1} type COBOL_Record is
    record
      Name   : COBOL.Numeric(1..20);
      SSN    : COBOL.Numeric(1..9);
      Salary : COBOL.Binary; -- Assume Binary = 32 bits
    end record
  end with Convention => COBOL;
  pragma Convention (COBOL, COBOL_Record);

  {AI05-0229-1} procedure Prog (Item : in out COBOL_Record)
    with Import => True, Convention => COBOL;
    pragma Import (COBOL, Prog, "PROG");
```

*1227*  16 October 2023  Interfacing with COBOL  *B.4*
package Salary_Conversions is
new COBOL.Decimal_Conversions(Salary_Type);

Some_Salary : Salary_Type := 12_345.67;
Some_Record : COBOL_Record :=
    (Name => "Johnson, John ",
    SSN => "111223333",
    Salary => Salary_Conversions.To_Binary(Some_Salary));

begin
    Prog (Some_Record);
    ...
end Test_Call;

with Interfaces.COBOL;
with COBOL_Sequential_IO;  -- Assumed to be supplied by implementation
procedure Test_External_Formats is
{AI12-0442-1}  -- Using data created by a COBOL program
    -- Assume that a COBOL program has created a sequential file with
    -- the following record structure, and that we want to
    -- process the records in an Ada program
    -- 01 EMPLOYEE-RECORD
    --  05 NAME PIC X(20).
    --  05 SSN PIC X(9).
    --  05 SALARY PIC 99999V99 USAGE COMP.
    --  05 ADJUST PIC S999V999 SIGN LEADING SEPARATE.
    -- The COMP data is binary (32 bits), high-order byte first
package COBOL renames Interfaces.COBOL;
type Salary_Type is delta 0.01 digits 7;
type Adjustments_Type is delta 0.001 digits 6;
{AI05-0229-1}  -- External representation
    type COBOL_Employee_Record_Type is
        record
            Name    : COBOL.Alphanumeric(1..20);
            SSN     : COBOL.Alphanumeric(1..9);
            Salary  : COBOL.Byte_Array(1..4);
            Adjust  : COBOL.Numeric(1..7);  -- Sign and 6 digits
        end record
with Convention => COBOL;
package COBOL_Employee_IO is
new COBOL_Sequential_IO(COBOL_Employee_Record_Type);
use COBOL_Employee_IO;
COBOL_File : File_Type;
type Ada_Employee_Record_Type is  -- Internal representation
    record
        Name    : String(1..20);
        SSN     : String(1..9);
        Salary  : Salary_Type;
        Adjust  : Adjustments_Type;
    end record;
COBOL_Record : COBOL_Employee_Record_Type;
Ada_Record   : Ada_Employee_Record_Type;
package Salary_Conversions is
new COBOL.Decimal_Conversions(Salary_Type);
use Salary_Conversions;
package Adjustments_Conversions is
new COBOL.Decimal_Conversions(Adjustments_Type);
use Adjustments_Conversions;
begin
    Open (COBOL_File, Name => "Some_File");
    loop
        Read (COBOL_File, COBOL_Record);
Ada Record.Name := COBOL>To_Ada(COBOL_Record.Name);
Ada_Record.SSN := COBOL>To_Ada(COBOL_Record.SSN);
Ada_Record.Salary := To_Decimal(COBOL_Record.Salary, COBOL.High_Order_First);
Ada_Record.Adjust := To_Decimal(COBOL_Record.Adjust, COBOL.Leading_Separate);
... -- Process Ada_Record
end loop;
exception
  when End_Error => ...
end Test_External_Formats;

Wording Changes from Ada 95

{8652/0066} {AI95-00071-01} Corrigendum: Corrected the definition of Valid to match COBOL.

{8652/0067} {AI95-00072-01} Corrigendum: Specified the bounds of the results of To_Display, To_Packed, and To_Binary.

B.5 Interfacing with Fortran

{AI05-0229-1} The facilities relevant to interfacing with the Fortran language are the package Interfaces.Fortran and support for specifying the Import, Export and Convention aspect pragmas with convention_identifier Fortran.

The package Interfaces.Fortran defines Ada types whose representations are identical to the default representations of the Fortran intrinsic types Integer, Real, Double Precision, Complex, Logical, and Character in a supported Fortran implementation. These Ada types can therefore be used to pass objects between Ada and Fortran programs.

Static Semantics

The library package Interfaces.Fortran has the following declaration:

{AI12-0414-1} with Ada.Numerics.Generic_Complex_Types; -- see G.1.1
pragma Elaborate_All(Ada.Numerics.Generic_Complex_Types);
package Interfaces.Fortran is
  with pragma Pure is(Fortran);
  type Fortran_Integer is range implementation-defined;
  type Real is digits implementation-defined;
  type Double_Precision is digits implementation-defined;
  type Logical is new Boolean;
  package Single_Precision_Complex_Types is new Ada.Numerics.Generic_Complex_Types (Real);
  type Complex is new Single_Precision_Complex_Types.Complex;
  subtype Imaginary is Single_Precision_Complex_Types.Imaginary;
  i : Imaginary renames Single_Precision_Complex_Types.i;
  j : Imaginary renames Single_Precision_Complex_Types.j;
{AI12-0058-1} package Double_Precision_Complex_Types is
  new Ada.Numerics.Generic_Complex_Types (Double_Precision);
{AI12-0058-1} type Double_Complex is new Double_Precision_Complex_Types.Complex;
{AI12-0058-1} subtype Double_Imaginary is Double_Precision_Complex_Types.Imaginary;
  type Character_Set is implementation-defined character type;
{AI05-0229-1} type Fortran_Character is array (Positive range <>) of Character_Set with Pack;
  pragma Pack (Fortran_Character);
function To_Fortran (Item : in Character) return Character_Set;
function To_Fortran (Item : in String) return Fortran_Character;
procedure To_Fortran (Item       : in String;
                     Target     : out Fortran_Character;
                     Last       : out Natural);

end Interfaces.Fortran;

Implementation defined: The types Fortran_Integer, Real, Double_Precision, and Character_Set in Interfaces.Fortran.

Ramification: {AI12-0058-1} The means by which the Complex and Double_Complex types are type is provided in Interfaces.Fortran creates a dependence of Interfaces.Fortran on Numerics.Generic_Complex_Types (see G.1.1). This dependence is intentional and unavoidable, if the Fortran-compatible Complex and Double_Complex types are to be useful in Ada code without duplicating facilities defined elsewhere.

{AI12-0058-1} The types Fortran=Integer, Real, Double_Precision, Logical, Complex, Double_Complex, Character_Set, and Fortran_Character are Fortran-compatible.

The To_Fortran and To_Ada functions map between the Ada type Character and the Fortran type Character_Set, and also between the Ada type String and the Fortran type Fortran_Character. The To_Fortran and To_Ada procedures have analogous effects to the string conversion subprograms found in Interfaces.COBOL.

Implementation Requirements

{AI05-0229-1} An implementation shall support specifying aspect pragma Convention with a Fortran convention_identifier for a Fortran-eligible type (see B.1).

Implementation Permissions

{AI12-0058-1} {AI12-0263-1} {AI12-0450-1} An implementation may add additional declarations to the Fortran interface packages. For example, declarations are permitted for the character types corresponding to Fortran character kinds 'ascii' and 'iso_10646', which in turn correspond to ISO/IEC 646:1991 and to UCS-4 as specified in ISO/IEC 10646:2020 the Fortran interface package for an implementation of Fortran 77 (ANSI X3.9-1978) that defines types like Integer*<n>, Real*<n>, Logical*<n>, and Complex*<n> may contain the declarations of types named Integer_Star_<n>, Real_Star_<n>, Logical_Star_<n>, and Complex_Star_<n>. (This convention should not apply to Character*<n>, for which the Ada analog is the constrained array subtype Fortran_Character (1..<n>).) Similarly, the Fortran interface package for an implementation of Fortran 90 that provides multiple kinds of intrinsic types, e.g. Integer (Kind=<n>), Real (Kind=<n>), Logical (Kind=<n>), Complex (Kind=<n>), and Character (Kind=<n>), may contain the declarations of types with the recommended names Integer_Kind_<n>, Real_Kind_<n>, Logical_Kind_<n>, Complex_Kind_<n>, and Character_Kind_<n>.

Reason: {AI12-0058-1} Fortran compilers are required to recognize 'ascii' and 'iso_10646' as arguments to the SELECTED_CHAR_KIND intrinsic function, but are not required to support those kinds.

Discussion: {AI12-0058-1} Implementations may add auxiliary declarations as needed to assist in the declarations of additional Fortran-compatible types. For example, if a double precision complex type is defined, then Numerics.Generic_Complex_Types may be instantiated for the double precision type. Similarly, if a wide character type is defined to match a Fortran 90 wide character type (accessible in Fortran 90 with the Kind attribute modifier), then an auxiliary character set may be declared to serve as its component type.

Implementation Advice

An Ada implementation should support the following interface correspondences between Ada and Fortran:
• An Ada procedure corresponds to a Fortran subroutine.
• An Ada function corresponds to a Fortran function.
• An Ada parameter of an elementary, array, or record type T is passed as a T_F argument to a Fortran procedure, where T_F is the Fortran type corresponding to the Ada type T, and where the INTENT attribute of the corresponding dummy argument matches the Ada formal parameter mode; the Fortran implementation's parameter passing conventions are used. For elementary types, a local copy is used if necessary to ensure by-copy semantics.
• An Ada parameter of an access-to-subprogram type is passed as a reference to a Fortran procedure whose interface corresponds to the designated subprogram's specification.

**Implementation Advice:** If Fortran interfacing is supported, the interface correspondences between Ada and Fortran should be supported.

**NOTE 1** An object of a Fortran-compatible record type, declared in a library package or subprogram, can correspond to a Fortran common block; the type also corresponds to a Fortran “derived type”.

**NOTE 2** {AI12-0224-1} For Fortran facilities not addressed by this subclause, consider using the Fortran to C interoperability features defined in ISO/IEC 1594-1:2018 along with the C interfacing features defined in B.3.

**Examples**

**Example of Interfaces.Fortran:**

```ada
with Interfaces.Fortran;
use Interfaces.Fortran;

procedure Ada_Application is

{AI05-0229-1} {AI12-0178-1} type Fortran_Matrix is
array (Fortran_Integer Integer range <>,
Fortran_Integer Integer range <>) of Double_Precision
with Convention => Fortran;
pragma Convention (Fortran, Fortran_Matrix); -- stored in Fortran's
-- column-major order

procedure Invert (Rank : in Fortran_Integer; X : in out Fortran_Matrix)
with Import => True, Convention => Fortran; -- a Fortran subroutine
pragma Import (Fortran, Invert);

Rank      : constant Fortran_Integer := 100;
My_Matrix : Fortran_Matrix (1 .. Rank, 1 .. Rank);

{AI12-0058-1} type Standard_Deviation is digits Precision
with Convention => Fortran,
Deviation : Standard_Deviation;
-- Declarations to match the following Fortran declarations:
-- integer, parameter :: precision = selected_real_kind(p=6)
-- real(precision) :: deviation

begin

... My_Matrix := ...;
... Invert (Rank, My_Matrix);
...

{AI12-0058-1} Deviation := ...
...
end Ada_Application;
```

**Wording Changes from Ada 2012**

{AI12-0058-1} **Correction:** The package Double Precision Complex Types and associated types are added to package Interfaces.Fortran. In unusual circumstances, this could cause an incompatibility; we don't document it as an incompatibility as implementations are allowed to add declarations to this package, so that risk of an incompatibility is present for any move from one version of an implementation to another (not to mention to another implementation). As such, the language-defined additions make no change in the risk of incompatibility.
Annex C
(normative)
Systems Programming

[ The Systems Programming Annex specifies additional capabilities provided for low-level programming. These capabilities are also required in many real-time, embedded, distributed, and information systems.]

This Annex is new to Ada 95.

C.1 Access to Machine Operations

Implementation defined: Implementation-defined intrinsic subprograms

Implementation Requirements

The implementation shall support machine code insertions (see 13.8) or intrinsic subprograms (see 6.3.1) (or both). The implementation-defined attributes shall be provided to allow the use of Ada entities as operands for such machine code insertions or intrinsic subprograms.

Discussion: Ada entities could be used as operands in machine code insertions and/or intrinsic subprograms using language-defined attributes (such as address), implementation-defined attributes, or could be directly allowed.

Implementation Advice

The machine code or intrinsics support should allow access to all operations normally available to assembly language programmers for the target environment, including privileged instructions, if any.

Implementation Advice: The machine code or intrinsics support should allow access to all operations normally available to assembly language programmers for the target environment.

Ramification: Of course, on a machine with protection, an attempt to execute a privileged instruction in user mode will probably trap. Nonetheless, we want implementations to provide access to them so that Ada can be used to write systems programs that run in privileged mode.

The support for interfacing aspects (see Annex B) should include support for assembly interface to assembler; the default assembler should be associated with the convention identifier Assembler.

Implementation Advice: Interface to assembler should be supported; the default assembler should be associated with the convention identifier Assembler.

If an entity is exported to assembly language, then the implementation should allocate it at an addressable location, and should ensure that it is retained by the linking process, even if not otherwise referenced from the Ada code. The implementation should assume that any call to a machine code or assembler subprogram is allowed to read or update every object that is specified as exported.

Implementation Advice: If an entity is exported to assembly language, then the implementation should allocate it at an addressable location even if not otherwise referenced from the Ada code. A call to a machine code or assembler subprogram should be treated as if it can read or update every object that is specified as exported.

Documentation Requirements

The implementation shall document the overhead associated with calling machine-code or intrinsic subprograms, as compared to a fully-inlined call, and to a regular out-of-line call.
6.2 | **Documentation Requirement:** The overhead of calling machine-code or intrinsic subprograms.

7 | The implementation shall document the types of the package System.Machine_Code usable for machine code insertions, and the attributes to be used in machine code insertions for references to Ada entities.

7.a | **Documentation Requirement:** The types and attributes used in machine code insertions.

8/3 | {AI05-0229-1} The implementation shall document the subprogram calling conventions associated with the convention identifiers available for use with the `Convention` aspect interfacing pragmas (Ada and Assembler, at a minimum), including register saving, exception propagation, parameter passing, and function value returning.

8.a/2 | **Documentation Requirement:** The subprogram calling conventions for all supported convention identifiers.

9 | For exported and imported subprograms, the implementation shall document the mapping between the Link_Name string, if specified, or the Ada designator, if not, and the external link name used for such a subprogram.

9.a/2 | **This paragraph was deleted.** Implementation defined: Implementation-defined aspects of access to machine operations.

9.b/2 | **Documentation Requirement:** The mapping between the Link_Name or Ada designator and the external link name.

Implementation Advice

10 | The implementation should ensure that little or no overhead is associated with calling intrinsic and machine-code subprograms.

10.a/2 | **Implementation Advice:** Little or no overhead should be associated with calling intrinsic and machine-code subprograms.

11 | It is recommended that intrinsic subprograms be provided for convenient access to any machine operations that provide special capabilities or efficiency and that are not otherwise available through the language constructs. Examples of such instructions include:

12/5 | • {AI12-0453-1} Atomic read-modify-write operations — for example, test and set, compare and swap, decrement and test, enqueue/dequeue.

13/5 | • {AI12-0453-1} Standard numeric functions — for example, sin, log.

14/5 | • {AI12-0453-1} String manipulation operations — for example, translate and test.

15/5 | • {AI12-0453-1} Vector operations — for example, compare vector against thresholds.

16 | Direct operations on I/O ports.

16.a/2 | **Implementation Advice:** Intrinsic subprograms should be provided to access any machine operations that provide special capabilities or efficiency not normally available.

### C.2 Required Representation Support

1/3 | {AI95-00434-01} {AI05-0299-1} This subclause specifies minimal requirements on the implementation's support for representation items and related features.

**Implementation Requirements**

2 | The implementation shall support at least the functionality defined by the recommended levels of support in Clause 13.

### C.3 Interrupt Support

1/3 | {AI05-0299-1} [This subclause specifies the language-defined model for hardware interrupts in addition to mechanisms for handling interrupts.]
Dynamic Semantics

[An interrupt represents a class of events that are detected by the hardware or the system software.] Interrupts are said to occur. An occurrence of an interrupt is separable into generation and delivery. Generation of an interrupt is the event in the underlying hardware or system that makes the interrupt available to the program. Delivery is the action that invokes part of the program as response to the interrupt occurrence. Between generation and delivery, the interrupt occurrence [(or interrupt)] is pending. Some or all interrupts may be blocked. When an interrupt is blocked, all occurrences of that interrupt are prevented from being delivered. Certain interrupts are reserved. The set of reserved interrupts is implementation defined. A reserved interrupt is either an interrupt for which user-defined handlers are not supported, or one which already has an attached handler by some other implementation-defined means. Program units can be connected to nonreserved interrupts. While connected, the program unit is said to be attached to that interrupt. The execution of that program unit, the interrupt handler, is invoked upon delivery of the interrupt occurrence.

This paragraph was deleted.

Implementation defined: Implementation-defined aspects of interrupts.

To be honest: As an obsolescent feature, interrupts may be attached to task entries by an address clause. See J.7.1.

While a handler is attached to an interrupt, it is called once for each delivered occurrence of that interrupt. While the handler executes, the corresponding interrupt is blocked.

While an interrupt is blocked, all occurrences of that interrupt are prevented from being delivered. Whether such occurrences remain pending or are lost is implementation defined.

Each interrupt has a default treatment which determines the system's response to an occurrence of that interrupt when no user-defined handler is attached. The set of possible default treatments is implementation defined, as is the method (if one exists) for configuring the default treatments for interrupts.

An interrupt is delivered to the handler (or default treatment) that is in effect for that interrupt at the time of delivery.

An exception propagated from a handler that is invoked by an interrupt has no effect.

[If the Ceiling_Locking policy (see D.3) is in effect, the interrupt handler executes with the active priority that is the ceiling priority of the corresponding protected object.]

Implementation Requirements

\{AI12-0445-1\} The implementation shall provide a mechanism to determine the minimum stack space that is necessary for each interrupt handler and to reserve that space for the execution of the handler. [This space should accommodate nested invocations of the handler where the system permits this.]

If the hardware or the underlying system holds pending interrupt occurrences, the implementation shall provide for later delivery of these occurrences to the program.

If the Ceiling_Locking policy is not in effect, the implementation shall provide means for the application to specify whether interrupts are to be blocked during protected actions.

Documentation Requirements

The implementation shall document the following items:

Discussion: This information may be different for different forms of interrupt handlers.

1. For each interrupt, which interrupts are blocked from delivery when a handler attached to that interrupt executes (either as a result of an interrupt delivery or of an ordinary call on a procedure of the corresponding protected object).
2. Any interrupts that cannot be blocked, and the effect of attaching handlers to such interrupts, if this is permitted.

3. Which run-time stack an interrupt handler uses when it executes as a result of an interrupt delivery; if this is configurable, what is the mechanism to do so; how to specify how much space to reserve on that stack.

4. {AI12-0453-1} Any implementation- or hardware-specific activity that happens before a user-defined interrupt handler gets control (for example, reading device registers, acknowledging devices).

5. Any timing or other limitations imposed on the execution of interrupt handlers.

6. The state (blocked/unblocked) of the nonreserved interrupts when the program starts; if some interrupts are unblocked, what is the mechanism a program can use to protect itself before it can attach the corresponding handlers.

7. Whether the interrupted task is allowed to resume execution before the interrupt handler returns.

8. {AI12-0453-1} The treatment of interrupt occurrences that are generated while the interrupt is blocked; that is, whether one or more occurrences are held for later delivery, or all are lost.

9. Whether predefined or implementation-defined exceptions are raised as a result of the occurrence of any interrupt, and the mapping between the machine interrupts (or traps) and the predefined exceptions.

10. On a multi-processor, the rules governing the delivery of an interrupt to a particular processor.

   **Documentation Requirement:** The treatment of interrupts.

**Implementation Permissions**

{AI95-00434-01} If the underlying system or hardware does not allow interrupts to be blocked, then no blocking is required [as part of the execution of subprograms of a protected object for which one of its subprograms is an interrupt handler].

In a multi-processor with more than one interrupt subsystem, it is implementation-defined whether (and how) interrupt sources from separate subsystems share the same Interrupt_Id type (see C.3.2). In particular, the meaning of a blocked or pending interrupt may then be applicable to one processor only.

**Discussion:** This issue is tightly related to the issue of scheduling on a multi-processor. In a sense, if a particular interrupt source is not available to all processors, the system is not truly homogeneous.

{AI12-0453-1} One way to approach this problem is to assign sub-ranges within Interrupt_Id to each interrupt subsystem, such that “similar” interrupt sources (for example, a timer) in different subsystems get a distinct id.

Implementations are allowed to impose timing or other limitations on the execution of interrupt handlers.

**Reason:** These limitations are often necessary to ensure proper behavior of the implementation.

{AI95-00434-01} {AI05-0299-1} Other forms of handlers are allowed to be supported, in which case, the rules of this subclause should be adhered to.

The active priority of the execution of an interrupt handler is allowed to vary from one occurrence of the same interrupt to another.

**Implementation Advice**

{AI95-00434-01} If the Ceiling_Locking policy is not in effect, the implementation should provide means for the application to specify which interrupts are to be blocked during protected actions, if the underlying system allows for finer-grained control of interrupt blocking.
Implementation Advice: If the Ceiling_Locking policy is not in effect and the target system allows for finer-grained control of interrupt blocking, a means for the application to specify which interrupts are to be blocked during protected actions should be provided.

NOTE 1 {AI12-0447-1} The default treatment for an interrupt can be to keep the interrupt pending or to deliver it to an implementation-defined handler. Examples of actions that an implementation-defined handler can perform include aborting the partition, ignoring (that is, discarding occurrences of) the interrupt, or queuing one or more occurrences of the interrupt for possible later delivery when a user-defined handler is attached to that interrupt.

NOTE 2 It is a bounded error to call Task_Identification.Current_Task (see C.7.1) from an interrupt handler.

NOTE 3 The rule that an exception propagated from an interrupt handler has no effect is modeled after the rule about exceptions propagated out of task bodies.

C.3.1 Protected Procedure Handlers

Paragraphs 1 through 6 were moved to Annex J, “Obsolescent Features”.

Syntax

{AI05-0229-1} The form of a pragma Interrupt_Handler is as follows:

{AI05-0229-1} interrupt_handler_name;

{AI05-0229-1} The form of a pragma Attach_Handler is as follows:

{AI05-0229-1} pragma Attach_Handler(handler_name, expression);

Name Resolution Rules

{AI05-0229-1} For the Interrupt_Handler and Attach_Handler pragmas, the handler_name shall resolve to denote a protected procedure with a parameterless profile.

{AI05-0229-1} For the Attach_Handler pragma, the expected type for the expression is Interrupts.Interrupt_Id (see C.3.2).

Static Semantics

{AI05-0229-1} For a parameterless protected procedure, the following language-defined representation aspects may be specified:

Interrupt_Handler

The type of aspect Interrupt_Handler is Boolean. If directly specified, the aspect definition shall be a static expression. [This aspect is never inherited;] if not directly specified, the aspect is False.

Aspect Description for Interrupt_Handler: Protected procedure may be attached to interrupts.

Attach_Handler

The aspect Attach_Handler is an expression, which shall be of type Interrupts.Interrupt_Id. [This aspect is never inherited.]

Aspect Description for Attach_Handler: Protected procedure is attached to an interrupt.

Legality Rules

{AI95-00434-01} {AI05-0033-1} {AI05-0229-1} If either the Attach_Handler or Interrupt_Handler aspect are specified for a protected procedure, the pragma is only allowed immediately within the protected_definition where the corresponding subprogram is declared. The corresponding protected_type_declaration or single_protected_declaration shall be a library-level declaration and shall not be declared within a generic body. In addition to the places where Legality Rules normally apply (see 12.3), this rule also applies in the private part of an instance of a generic unit.
7.a

**Discussion:** In the case of a protected_type_declaration, an object_declaration of an object of that type need not be at library level.

7.b/3

\textit{[A105-0033-1] [A105-0229-1]} We cannot allow these aspects in protected declarations in a generic body, because legality rules are not checked for instance bodies, and these should not be allowed if the instance is not at the library level. The protected types can be declared in the private part if this is desired. Note that while the ’Access to use the handler would provide the check in the case of Interrupt_Handler, there is no other check for Attach_Handler. Since these aspects are so similar, we want the rules to be the same.

8/3

This paragraph was deleted.\textit{[A105-00253-01] [A105-00303-01] [A105-0033-1]} The Interrupt_Handler pragma is only allowed immediately within the protected_definition where the corresponding subprogram is declared. The corresponding protected_type_declaration or single_protected_declaration shall be a library-level declaration. In addition, any object_declaration of such a type shall be a library-level declaration.

**Dynamic Semantics**

9/3

\textit{[A105-0229-1]} If the pragma Interrupt_Handler aspect of a protected procedure is True appears in a protected_definition, then the corresponding procedure may be attached dynamically, as a handler, to interrupts (see C.3.2). [Such procedures are allowed to be attached to multiple interrupts.]

10/3

\textit{[A105-0229-1]} The expression specified for the Attach_Handler aspect of a protected procedure \textit{P} is evaluated as part of the creation of the protected object that contains \textit{P}. The value of the expression identifies pragma [as evaluated at object creation time] specifies an interrupt. As part of the initialization of that object, \textit{P} (if the Attach_Handler pragma is specified, the handler procedure) is attached to the specified interrupt. A check is made that the corresponding interrupt is not reserved. Program_Error is raised if the check fails, and the existing treatment for the interrupt is not affected.

11/3

\textit{[A105-00434-01]} If the Ceiling Locking policy (see D.3) is in effect, then upon the initialization of a protected object that contains a protected procedure for which either the Attach_Handler aspect is specified or the Interrupt_Handler aspect is True pragma applies to one of its procedures, a check is made that the initial ceiling priority of the object defined in the protected_definition is in the range of System_INTERRUPT_Priority. If the check fails, Program_Error is raised.

12/3

\textit{[8652/0068]} \textit{[A105-00121-01]} \textit{[A105-0229-1]} When a protected object is finalized, for any of its procedures that are attached to interrupts, the handler is detached. If the handler was attached by a procedure in the Interrupts package or if no user handler was previously attached to the interrupt, the default treatment is restored. If the an Attach_Handler aspect pragma was specified and the most recently attached handler for the same interrupt is the same as the one that was attached at the time the protected_object was initialized[Otherwise, [that is, if an Attach_Handler pragma was specified], the previous handler is restored.

Discussion: \textit{[8652/0068]} \textit{[A105-00121-01]} \textit{[A105-00303-01]} \textit{[A105-0229-1]} If all protected objects for interrupt handlers are declared at the library level since only library-level protected procedures can be attached as handlers using the Interrupts package, the finalization discussed above occurs only as part of the finalization of all library-level packages in a partition. However, objects of a protected type containing procedures with an Attach_Handler aspect pragma need not be at the library level. Thus, an implementation needs to be able to restore handlers during the execution of the program. (An object with an Interrupt_Handler aspect pragma also need not be at the library level, but such a handler cannot be attached to an interrupt using the Interrupts package.)

13

When a handler is attached to an interrupt, the interrupt is blocked [(subject to the Implementation Permission in C.3)] during the execution of every protected action on the protected object containing the handler.

13.1/5

\textit{[AI12-0252-1]} If restriction No Dynamic Attachment is in effect, then a check is made that the interrupt identified by an Attach_Handler aspect does not appear in any previously elaborated Attach_Handler aspect; Program_Error is raised if this check fails.
Reason: When No Dynamic Attachment is in effect, it is not possible to call any previous handler. Therefore, the only possibility is to replace the original handler, rendering it ineffective. Having an unused handler in a program is likely a bug, so we require an exception to be raised.

Erroneous Execution

If the Ceiling Locking policy (see D.3) is in effect and an interrupt is delivered to a handler, and the interrupt hardware priority is higher than the ceiling priority of the corresponding protected object, the execution of the program is erroneous.

\{8652/0068\} \{AI95-00121-01\} \{AI05-0229-1\} If the handlers for a given interrupt attached via \texttt{aspect\_pragma} Attach\_Handler are not attached and detached in a stack-like (LIFO) order, program execution is erroneous. In particular, when a protected object is finalized, the execution is erroneous if any of the procedures of the protected object are attached to interrupts via \texttt{aspect\_pragma} Attach\_Handler and the most recently attached handler for the same interrupt is not the same as the one that was attached at the time the protected object was initialized.

Discussion: \{8652/0068\} \{AI95-00121-01\} \{AI05-0229-1\} This simplifies implementation of the Attach\_Handler \texttt{aspect\_pragma} by not requiring a check that the current handler is the same as the one attached by the initialization of a protected object.

Metrics

The following metric shall be documented by the implementation:

\{AI95-00434-01\} The worst-case overhead for an interrupt handler that is a parameterless protected procedure, in clock cycles. This is the execution time not directly attributable to the handler procedure or the interrupted execution. It is estimated as $C - (A+B)$, where $A$ is how long it takes to complete a given sequence of instructions without any interrupt, $B$ is how long it takes to complete a normal call to a given protected procedure, and $C$ is how long it takes to complete the same sequence of instructions when it is interrupted by one execution of the same procedure called via an interrupt.

Implementation Note: The instruction sequence and interrupt handler used to measure interrupt handling overhead should be chosen so as to maximize the execution time cost due to cache misses. For example, if the processor has cache memory and the activity of an interrupt handler could invalidate the contents of cache memory, the handler should be written such that it invalidates all of the cache memory.

Documentation Requirement: The metrics for interrupt handlers.

Implementation Permissions

\{AI05-0229-1\} When the \texttt{aspect\_pragma}s Attach\_Handler or Interrupt\_Handler are specified for apply to a protected procedure, the implementation is allowed to impose implementation-defined restrictions on the corresponding \texttt{protected\_type\_declaration} and \texttt{protected\_body}.

Ramification: The restrictions may be on the constructs that are allowed within them, and on ordinary calls (i.e. not via interrupts) on protected operations in these protected objects.

Implementation defined: Any restrictions on a protected procedure or its containing type when an \texttt{aspect\_pragma} Attach\_handler or Interrupt\_Handler is specified applies.

An implementation may use a different mechanism for invoking a protected procedure in response to a hardware interrupt than is used for a call to that protected procedure from a task.

Discussion: This is despite the fact that the priority of an interrupt handler (see D.1) is modeled after a hardware task calling the handler.

\{AI05-0229-1\} Notwithstanding what this subclause says elsewhere, the Attach\_Handler and Interrupt\_Handler \texttt{aspect\_pragma}s are allowed to be used for other, implementation defined, forms of interrupt handlers.
Ramification: \{AI05-0229-1\} For example, if an implementation wishes to allow interrupt handlers to have parameters, it is allowed to do so via these `aspect pragmas`; it need not invent implementation-defined `aspect pragmas` for the purpose.

Implementation defined: Any other forms of interrupt handler supported by the `Attach_Handler` and `Interrupt_Handler` `aspect pragmas`.

Implementation Advice

Whenever possible, the implementation should allow interrupt handlers to be called directly by the hardware.

Implementation Advice: Interrupt handlers should be called directly by the hardware.

Whenever practical, the implementation should detect violations of any implementation-defined restrictions before run time.

Implementation Advice: Violations of any implementation-defined restrictions on interrupt handlers should be detected before run time.

NOTE 1 \{AI05-0229-1\} \{AI12-0440-1\} The `Attach_Handler` `aspect canmay pragma` can provide static attachment of handlers to interrupts if the implementation supports preelaboration of protected objects. (See C.4.)

NOTE 2 \{AI95-00434-01\} \{AI12-0442-1\} For a protected object that has a (protected) procedure of its procedures is attached to an interrupt, the correct ceiling priority should have a ceiling priority be at least as high as the highest processor priority at which that interrupt will ever be delivered.

NOTE 3 Protected procedures can also be attached dynamically to interrupts via operations declared in the predefined package `Interrupts`.

NOTE 4 An example of a possible implementation-defined restriction is disallowing the use of the standard storage pools within the body of a protected procedure that is an interrupt handler.

Incompatibilities With Ada 95

Amendment Correction: Corrected the wording so that the rules for the use of `Attach_Handler` and `Interrupt_Handler` are identical. This means that uses of `pragma Interrupt_Handler` outside of the target protected type or single protected object are now illegal.

Corrigendum: Clarified the meaning of “the previous handler” when finalizing protected objects containing interrupt handlers.

Dropped the requirement that an object of a type containing an `Interrupt_Handler` pragma must be declared at the library level. This was a generic contract model violation. This change is not an extension, as an attempt to attach such a handler with a routine in package `Interrupts` will fail an accessibility check anyway. Moreover, implementations can retain the rule as an implementation-defined restriction on the use of the type, as permitted by the Implementation Permissions above.

Extensions to Ada 2005

Aspects `Interrupt_Handler` and `Attach_Handler` are new; `pragma Interrupt_Handler` and `Attach_Handler` are now obsolescent.

Wording Changes from Ada 2005

Correction: Added missing generic contract wording for the aspects `Attach_Handler` and `Interrupt_Handler`.

Inconsistencies With Ada 2012

Correction: Program Error might be raised if two handlers are attached when restriction `No Dynamic Attachment` is in effect (including as part of the Ravenscar profile). Original Ada 2012 would have just ignored the first handler. This is almost certainly a bug rather than an intended result.
C.3.2 The Package Interrupts

Static Semantics

The following language-defined packages exist:

\{AI05-0167-1\} \{AI12-0241-1\} \{AI12-0302-1\} with System;
\{AI05-0167-1\} \{AI12-0241-1\} \{AI12-0302-1\} with System.Multiprocessors;
package Ada.Interrupts
with Nonblocking, Global => in out synchronized is

  type Interrupt_Id is implementation-defined;
  type Parameterless_Handler is
    access protected procedure
      with Nonblocking => False;

  function Is_Reserved (Interrupt : Interrupt_Id)
    return Boolean;
  function Is_Attached (Interrupt : Interrupt_Id)
    return Boolean;
  function Current_Handler (Interrupt : Interrupt_Id)
    return Parameterless_Handler;
  procedure Attach_Handler
    (New_Handler : in Parameterless_Handler;
     Interrupt   : in Interrupt_Id);
  procedure Exchange_Handler
    (Old_Handler : out Parameterless_Handler;
     New_Handler : in Parameterless_Handler;
     Interrupt   : in Interrupt_Id);
  procedure Detach_Handler
    (Interrupt : in Interrupt_Id);
  function Reference (Interrupt : Interrupt_Id)
    return System.Address;

\{AI05-0167-1\} function Get_CPU (Interrupt : Interrupt_Id)
    return System.Multiprocessors.CPU_Range;

private
  ... -- not specified by the language
end Ada.Interrupts;

\{AI12-0302-1\} package Ada.Interrupts.Names
with Nonblocking, Global => null is
  implementation-defined : constant Interrupt_Id :=
    implementation-defined;

  implementation-defined : constant Interrupt_Id :=
    implementation-defined;
end Ada.Interrupts.Names;

Dynamic Semantics

The Interrupt_Id type is an implementation-defined discrete type used to identify interrupts.

The Is_Reserved function returns True if and only if the specified interrupt is reserved.

The Is_Attached function returns True if and only if a user-specified interrupt handler is attached to the interrupt.

\{8652/0069\} \{AI95-00166-01\} The Current_Handler function returns a value that represents the attached handler of the interrupt. If no user-defined handler is attached to the interrupt, Current_Handler returns \texttt{null} a value that designates the default treatment; calling Attach_Handler or Exchange_Handler with this value restores the default treatment.
The Attach_Handler procedure attaches the specified handler to the interrupt, overriding any existing treatment (including a user handler) in effect for that interrupt. If New_Handler is null, the default treatment is restored. If New_Handler designates a protected procedure for which the Interrupt_Handler aspect pragma is False, Program_Error is raised. In this case, the operation does not modify the existing interrupt treatment.

The Exchange_Handler procedure operates in the same manner as Attach_Handler with the addition that the value returned in Old_Handler designates the previous treatment for the specified interrupt. If the previous treatment is not a user-defined handler, null is returned.

Ramification: Calling Attach_Handler or Exchange_Handler with this value for New_Handler restores the previous handler.

If the application uses only parameterless procedures as handlers (other types of handlers may be provided by the implementation, but are not required by the standard), then if Old_Handler is not null, it may be called to execute the previous handler. This provides a way to cascade application interrupt handlers. However, the default handler cannot be cascaded this way (Old_Handler must be null for the default handler).

The Detach_Handler procedure restores the default treatment for the specified interrupt.

For all operations defined in this package that take a parameter of type Interrupt_Id, with the exception of Is_Reserved and Reference, a check is made that the specified interrupt is not reserved. Program_Error is raised if this check fails.

If, by using the Attach_Handler, Detach_Handler, or Exchange_Handler procedures, an attempt is made to detach a handler that was attached statically (using the aspect pragma Attach_Handler), the handler is not detached and Program_Error is raised.

The Reference function returns a value of type System.Address that can be used to attach a task entry via an address clause (see J.7.1) to the interrupt specified by Interrupt. This function raises Program_Error if attaching task entries to interrupts (or to this particular interrupt) is not supported.

The function Get_CPU returns the processor on which the handler for Interrupt is executed. If the handler can execute on more than one processor the value System.Multiprocessors.Not_A_Specific_CPU is returned.

At no time during attachment or exchange of handlers shall the current handler of the corresponding interrupt be undefined.

If implementation-defined forms of interrupt handler procedures are supported, such as protected procedures with parameters, then for each such form of a handler, a type analogous to Parameterless_Handler should be specified in a child package of Interrupts, with the same operations as in the predefined package Interrupts.
**Implementation Advice:** If implementation-defined forms of interrupt handler procedures are supported, then for each such form of a handler, a type analogous to Parameterless_Handler should be specified in a child package of Interrupts, with the same operations as in the predefined package Interrupts.

NOTE The package Interrupts.Names contains implementation-defined names (and constant values) for the interrupts that are supported by the implementation.

**Examples**

Example of interrupt handlers:

```ada
{AI05-0229-1} {AI12-0178-1} Device_Priority : constant array (Ada.Interrupts.Interrupt_Id range 1..5) of System.Interrupt_Priority := ( ... );

protected type Device_Interface (Int_Id : Ada.Interrupts.Interrupt_Id)
  with Interrupt_Priority => Device_Priority(Int_Id)
is
  procedure Handler with Attach_Handler => Int_Id;

  pragma Attach_Handler(Handler, Int_Id);
...

  pragma Interrupt_Priority(Device_Priority(Int_Id));

end Device_Interface;
...

Device_1_Driver : Device_Interface(1);
...

Device_5_Driver : Device_Interface(5);
...
```

**Wording Changes from Ada 95**

{8652/0069} {AI95-00166-01} **Corrigendum:** Clarified that the value returned by Current_Handler and Exchange_Handler for the default treatment is null.

**Incompatibilities With Ada 2005**

{AI05-0167-1} Function Get_CPU is added to Interrupts. If Interrupts is referenced in a use_clause, and an entity E with a defining_identifier of Get_CPU is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

**C.4 Preelaboration Requirements**

{AI05-0299-1} {AI12-0417-1} [This subclause specifies additional implementation and documentation requirements for the Preelaborate aspect (see 10.2.1.).]

**Implementation Requirements**

The implementation shall not incur any run-time overhead for the elaboration checks of subprograms and protected_bodies declared in preelaborated library units.

The implementation shall not execute any memory write operations after load time for the elaboration of constant objects declared immediately within the declarative region of a preelaborated library package, so long as the subtype and initial expression (or default initial expressions if initialized by default) of the object_declaration satisfy the following restrictions. The meaning of load time is implementation defined.

**Discussion:** On systems where the image of the partition is initially copied from disk to RAM, or from ROM to RAM, prior to starting execution of the partition, the intention is that “load time” consist of this initial copying step. On other systems, load time and run time might actually be interspersed.

- Any subtype_mark denotes a statically constrained subtype, with statically constrained subcomponents, if any;
- {AI95-00161-01} no subtype_mark denotes a controlled type, a private type, a private extension, a generic formal private type, a generic formal derived type, or a descendant of such a type;
Reason: For an implementation that uses the registration method of finalization, a controlled object will require some code executed to register the object at the appropriate point. The other types are those that might have a controlled component. None of these types were allowed in preelaborated units in Ada 95. These types are covered by the Implementation Advice, of course, so they should still execute as little code as possible.

- any constraint is a static constraint;
- any allocator is for an access-to-constant type;
- any uses of predefined operators appear only within static expressions;
- any primaries that are names, other than attribute_references for the Access or Address attributes, appear only within static expressions;

Ramification: This cuts out attribute_references that are not static, except for Access and Address.

{AI12-0368-1} any name that is not part of a static expression is an expanded name or direct_name that statically names some entity;

Ramification: {AI12-0368-1} This cuts out function_calls and type_conversions that are not static, including calls on attribute functions like 'Image and 'Value. We do allow components if those components don't require any evaluation or checks.

- any discrete_choice of an array_aggregate is static;
- no language-defined check associated with the elaboration of the object_declaration can fail.

Reason: {AI95-00114-01} The intent is that aggregates all of whose scalar subcomponents are static, and all of whose access subcomponents are null, allocators for access-to-constant types, or X'Access, will be supported with no run-time code generated.

Documentation Requirements

12 The implementation shall document any circumstances under which the elaboration of a preelaborated package causes code to be executed at run time.

12.a/2 Documentation Requirement: Any circumstances when the elaboration of a preelaborated package causes code to be executed.

13 The implementation shall document whether the method used for initialization of preelaborated variables allows a partition to be restarted without reloading.

13.a/2 Documentation Requirement: Whether a partition can be restarted without reloading.

This paragraph was deleted. Implementation defined: Implementation-defined aspects of preelaboration.

13.b/2 Discussion: {AI95-00114-01} This covers the issue of the run-time system RTS itself being restartable, so that need not be a separate Documentation Requirement.

Implementation Advice

14 It is recommended that preelaborated packages be implemented in such a way that there should be little or no code executed at run time for the elaboration of entities not already covered by the Implementation Requirements.

14.a/2 Implementation Advice: Preelaborated packages should be implemented such that little or no code is executed at run time for the elaboration of entities.

Wording Changes from Ada 95

{AI95-00161-01} Added wording to exclude the additional kinds of types allowed in preelaborated units from the Implementation Requirements.

Wording Changes from Ada 2012

{AI12-0368-1} Added wording to allow components so long as no evaluation or checks are required for the reference.
C.5 Aspect Discard_Names

Pragma Discard_Names

{AI12-0072-1} [Specifying the aspect pragma Discard_Names can be used to request a reduction in storage used for the names of certain entities with runtime name text.]

Static Semantics

{AI12-0072-1} An entity with runtime name text is a nonderived enumeration first subtype, a tagged first subtype, or an exception.

{AI12-0072-1} For an entity with runtime name text, the following language-defined representation aspect may be specified:

Discard_Names

The type of aspect Discard_Names is Boolean. If directly specified, the aspect definition shall be a static expression. If not specified (including by inheritance), the aspect is False.

Aspect Description for Discard_Names: Requests a reduction in storage for names associated with an entity.

Syntax

The form of a pragma Discard_Names is as follows:

pragma Discard_Names[[[On => ] local_name]];

A pragma Discard_Names is allowed only immediately within a declarative_part, immediately within a package_specification, or as a configuration pragma.

Legality Rules

{AI12-0072-1} The local_name (if present) shall denote an entity with runtime name text: a nonderived enumeration [first] subtype, a tagged [first] subtype, or an exception. The pragma specifies that the aspect Discard_Names for applies to the type or exception has the value True. Without a local_name, the pragma specifies that applies to all such entities with runtime name text declared after the pragma, within the same declarative region have the value True for aspect Discard_Names. Alternatively, the pragma can be used as a configuration pragma. If the configuration pragma Discard_Names applies to a compilation unit, all entities with runtime name text declared in the compilation unit have the value True for the aspect Discard_Names. If the pragma applies to a type, then it applies also to all descendants of the type.

Ramification: {AI12-0072-1} If the aspect is specified for a type, then it is inherited by all descendants of the type. The aspect cannot be specified as False on a derived type (because specifying the aspect is not allowed on derived enumeration types, and by rule applying to all aspects for other types (see 13.1.1)).

Static Semantics

If a local_name is given, then a pragma Discard_Names is a representation pragma.

This paragraph was deleted. Ramification: {AI05-0229-1} {AI12-0072-1} Representation pragmas automatically specify aspects of the same name, so Discard_Names can be used as an aspect mark in an aspect specification instead of using the pragmas on individual entities.

{AI95-00285-01} {AI95-00440-01} {AI12-0072-1} If the aspect Discard_Names is True for pragma applies to an enumeration type, then the semantics of the Wide_Wide_Image and Wide_Wide_Value attributes are implementation defined for that type; the semantics of Image, Wide_.. and Value and Wide_Value are still defined in terms of Wide_Wide_Image and Wide_Wide_Value. In addition, the semantics of Text_IO.Enumeration_IO are implementation defined. If the aspect Discard_Names is True for pragma applies to a tagged type, then the semantics of the Tags.Wide_Wide_Expanded_Name function are implementation defined for that type; the semantics of Tags.Expanded_Name and Tags.-
Wide Expanded_Name are still defined in terms of Tags.Wide_Wide_Expanded_Name. If the aspect Discard_Names is True for pragma applies to an exception, then the semantics of the Exceptions.Wide_Wide_Exception_Name.Exception_Name function are implementation defined for that exception; the semantics of Exceptions.Exception_Name and Exceptions.Wide_Exception_Name are still defined in terms of Exceptions.Wide_Wide_Exception_Name.

Implementation defined: The semantics of some attributes and functions of an entity for which aspect pragma Discard_Names is True.

Ramification: The Width attribute is still defined in terms of Image.

\{AI95-00285-01\} \{AI12-0072-1\} The semantics of S'Wide_Wide_Image.Wide_Image and S'Wide_Wide_Value.Wide_Value are implementation defined for any subtype of an enumeration type for which the aspect is True for pragma applies. (The pragma, if used, actually names the first subtype, of course.)

Implementation Advice

If the aspect Discard_Names is True for pragma applies to an entity, then the implementation should reduce the amount of storage used for storing names associated with that entity.

Reason: A typical implementation of the Image attribute for enumeration types is to store a table containing the names of all the enumeration literals. Aspect pragma Discard_Names allows the implementation to avoid storing such a table without having to prove that the Image attribute is never used (which can be difficult in the presence of separate compilation).

We did not specify the semantics of the Image attribute when aspect Discard_Names is True in the presence of this pragma because different semantics might be desirable in different situations. In some cases, it might make sense to use the Image attribute to print out a useful value that can be used to identify the entity given information in compiler-generated listings. In other cases, it might make sense to get an error at compile time or at run time. In cases where memory is plentiful, the simplest implementation makes sense: ignore the aspect pragma. Implementations that are capable of avoiding the extra storage in cases where the Image attribute is never used might also wish to ignore the aspect pragma.

The same applies to the Tags.Expanded_Name and Exceptions.Exception_Name functions.

Wording Changes from Ada 95

\{AI95-00285-01\} \{AI95-00400-01\} Updated the wording to reflect that the double wide image and value functions are now the master versions that the others are defined from.

Wording Changes from Ada 2012

\{AI12-0072-1\} Corrigendum: Defined the pragma in terms of the aspect Discard_Names, and added a missing definition of the meaning of the configuration pragma. This is not intended to make any semantic change (Ada 2012 has an aspect Discard_Names defined via blanket rules for representation pragmas in 13.1 and 13.1.1), just to clarify the meaning.

C.6 Shared Variable Control

This subclause defines representation aspects pragmas that control the use of shared variables.

Paragraphs 2 through 6 were moved to Annex J, “Obsolescent Features”.

Syntax

\{AI05-0229-1\} \{AI05-0299-1\} The form for pragmas Atomic, Volatile, Atomic_Components, and Volatile_Components is as follows:

`pragma Atomic(local_name);`

`pragma Volatile(local_name);`
pragma Atomic_Components(array_local_name);
pragma Volatile_Components(array_local_name);

Static Semantics

{AI05-0229-1} {AI12-0282-1} For an object declaration, a component declaration, or a full type declaration, or a formal complete type declaration, the following representation aspects may be specified:

Atomic

The type of aspect Atomic is Boolean.

Aspect Description for Atomic: Declare that a type, object, or component is atomic.

Independent

The type of aspect Independent is Boolean.

Aspect Description for Independent: Declare that a type, object, or component is independently addressable.

Volatile

The type of aspect Volatile is Boolean.

Aspect Description for Volatile: Declare that a type, object, or component is volatile.

{AI12-0363-1} Full_Access_Only

The type of aspect Full_Access_Only is Boolean.

Aspect Description for Full_Access_Only: Declare that a volatile type, object, or component is full access.

{AI05-0229-1} {AI12-0282-1} For a full type declaration of an array type, (including the anonymous type of an object declaration for an object of an anonymous array type, or the formal complete type declaration of a formal array type of an anonymous array object), the following representation aspects may be specified:

Atomic_Components

The type of aspect Atomic_Components is Boolean.

Aspect Description for Atomic_Components: Declare that the components of an array type or object are atomic.

Volatile_Components

The type of aspect Volatile_Components is Boolean.

Aspect Description for Volatile_Components: Declare that the components of an array type or object are volatile.

{AI05-0229-1} {AI12-0282-1} For a full type declaration of a composite type, (including the anonymous type of an object declaration for an object of an anonymous composite type, or the formal complete type declaration of a formal composite type of an anonymous array object), the following representation aspect may be specified:

Independent_Components

The type of aspect Independent_Components is Boolean.

Aspect Description for Independent_Components: Declare that the components of an array or record type, or an array object, are independently addressable.

{AI05-0229-1} {AI12-0363-1} If any of these aspects are directly specified, the aspect definition shall be a static expression. If not specified for a type (including by inheritance), the Atomic, Atomic_Components, and Full_Access_Only aspects are False. If any of these aspects are specified True for a type, then the corresponding aspect is True for all objects of the type. If the Atomic aspect is specified True, then the aspects Volatile, Independent, and Volatile_Component (if defined) are True; if the Atomic_Components aspect is specified True, then the aspects Volatile, Volatile_Components, and Independent_Components are True. If the Volatile aspect is specified True, then the Volatile_Components aspect (if defined) is True, and vice versa. When not determined by one of
the other aspects, or for an object by its type, the Volatile, Volatile Components, Independent, and Independent Components aspects are False.

**Ramification:** \{AI12-0363-1\} Aspects Volatile and Volatile Components (when defined) are equivalent. We provide the Volatile Components aspect only to give symmetry with Atomic Components and Independent Components aspects.

An atomic type is one **forte** which the aspect pragma Atomic is True applies. An atomic object (including a component) is one **forte** which the aspect pragma Atomic is True applies, or a component of an array **forte** which the aspect pragma Atomic_Components is True for the associated type applies, or any object of an atomic type, other than objects obtained by evaluating a slice.

**Ramification:** \{AI95-00272-01\} A slice of an atomic array object is not itself atomic. That's necessary as executing a read or write of a dynamic number of components in a single instruction is not possible on many targets.

A volatile type is one **forte** which the aspect pragma Volatile is True applies. A volatile object (including a component) is one **forte** which the aspect pragma Volatile is True applies, or a component of an array **forte** which the aspect pragma Volatile_Components is True for the associated type applies, or any object of a volatile type. In addition, every atomic type or object is also defined to be volatile. Finally, if an object is volatile, then so are all of its subcomponents [(the same does not apply to atomic)].

When True, the aspects Independent and Independent Components specify as independently addressable the named object or component(s), or in the case of a type, all objects or components of that type. All atomic objects and aliased objects are considered to be specified as independently addressable.

**Ramification:** If the compiler cannot guarantee that an object (including a component) for which aspect Independent or aspect Independent_Components is True is independently addressable from any other nonoverlapping object, then the aspect specification must be rejected.

Similarly, an atomic object (including atomic components) is always independently addressable from any other nonoverlapping object. Any representation item which would prevent this from being true should be rejected, notwithstanding what this Standard says elsewhere (specifically, in the Recommended Level of Support).

The Full_Access Only aspect shall not be specified unless the associated type or object is volatile [(or atomic)]. A full access type is any atomic type, or a volatile type for which the aspect Full_Access Only is True. A full access object (including a component) is any atomic object, or a volatile object for which the aspect Full_Access Only is True for the object [or its type]. A Full_Access Only aspect is illegal if any subcomponent of the object or type is a full access object or is of a generic formal type.

**Ramification:** \{AI12-0363-1\} This last rule breaks privacy, but that is considered OK for representation clauses when there is no clear alternative. Note that atomic objects may be nested, so long as the outer atomic object does not have the Full_Access Only aspect True.

**Reason:** \{AI12-0363-1\} We disallow subcomponents of a generic formal type in a Full_Access Only object or type as the actual to a formal type can be a full access type. We could have had a less restrictive rule, but such a use is unlikely as full access only objects are intended to be used to access memory-mapped devices with access restrictions, and those will need a concrete mapping not possible for generic formal types.

**Name Resolution Rules**

The local name in an Atomic or Volatile pragma shall resolve to denote either an object declaration, a noninherited component declaration, or a full type declaration. The array local name in an Atomic_Components or Volatile_Components pragma shall resolve to denote the declaration of an array type or an array object of an anonymous type.
Legality Rules

\{AI05-0229-1\} If aspect Independent_Components is specified for a full_type_declaration, the declaration shall be that of an array or record type.

\{AI05-0229-1\} \{AI12-0001-1\} It is illegal to specify either of the aspect\_pragma Atomic or Atomic\_Components to have the value True for an object or type if the implementation cannot support the indivisible and independent reads and updates required by the aspect\_pragma (see below).

\{AI12-0001-1\} It is illegal to specify the Size attribute of an atomic object, the Component\_Size attribute for an array type with atomic components, or the layout attributes of an atomic component, in a way that prevents the implementation from performing the required indivisible and independent reads and updates.

\{AI05-0142-4\} \{AI05-0218-1\} \{AI12-0363-1\} If an atomic object is passed as a parameter, then the type of the formal parameter shall either have an atomic type or allow pass by copy (that is, not be a nonatomic by-reference type). If an atomic object is used as an actual for a generic formal object of mode in out, then the type of the generic formal object shall be atomic. If the prefix of an attribute\_reference for an Access attribute denotes an atomic object (including a component), then the designated type of the resulting access type shall be atomic. If an atomic type is used as an actual for a generic formal derived type, then the ancestor of the formal type shall be atomic. Corresponding rules apply to volatile objects and to full access object types.

**Ramification:** \{AI05-0142-4\} A formal parameter allows pass by copy if it is not aliased and it is of a type that allows pass by copy (that is, is not a by-reference type).

\{AI12-0128-1\} \{AI12-0363-1\} If a nonatomic subcomponent of a full access object is passed as an actual parameter in a call then the formal parameter shall allow pass by copy (and, at run time, the parameter shall be passed by copy). A nonatomic subcomponent of a full access object shall not be used as an actual for a generic formal derived type, then the ancestor of the formal type shall be atomic. A corresponding rule applies to volatile types and similarly to full access types: a volatile type is used as an actual for a generic formal array type, then the element type of the formal type shall be volatile.

\{AI12-0363-1\} If a type with volatile components is used as an actual for a generic formal array type, then the components of the formal type shall be volatile. Furthermore, if the actual type has atomic components and the formal array type has aliased components, then the components of the formal array type shall also be atomic. A corresponding rule applies when the actual type has volatile full access components.

**Reason:** \{AI12-0363-1\} The limitations on formal array types are separate for volatile and atomic because of the fact that only volatility is carried down to all subcomponents of a volatile object, while atomicity is not. The goal of both limitations is that we don't want 'Access for an access type to produce a value that designates an object whose atomicity and volatility don't agree with that of the designated type of the access type. The above rules ensure that the generic "sees" the relevant volatility and atomicity.

\{AI05-0229-1\} If an aspect\_pragma Volatile, Volatile\_Components, Atomic, or Atomic\_Components is directly specified to have the value True for an aspect\_pragma to a stand-alone constant object, then the aspect\_pragma Import shall also be specified as True for apply to it.

**Ramification:** Hence, no initialization expression is allowed for such a constant. Note that a constant that is atomic or volatile because of its type is allowed.

**Reason:** Stand-alone constants that are explicitly specified as Atomic or Volatile only make sense if they are being manipulated outside the Ada program. From the Ada perspective the object is read-only. Nevertheless, if imported and
atomic or volatile, the implementation should presume it might be altered externally. For an imported stand-alone
constant that is not atomic or volatile, the implementation can assume that it will not be altered.

To be honest: \{AI05-0218-1\} Volatile Components and Atomic Components actually are aspects of the anonymous
array type; this rule only applies when the aspect is specified directly on the constant object and not when the (named)
array type has the aspect.

\{AI05-0009-1\} \{AI05-0229-1\} It is illegal to specify the aspect Independent or Independent Components
as True for a component, object or type if the implementation cannot provide the independent
addressability required by the aspect (see 9.10).

\{AI05-0009-1\} \{AI05-0229-1\} It is illegal to specify a representation aspect for a component, object or
type for which the aspect Independent or Independent Components is True, in a way that prevents the
implementation from providing the independent addressability required by the aspect.

Paragraph 14 was moved to Annex J, “Obsolescent Features”.

Static Semantics

\{AI05-0229-1\} These pragmas are representation pragmas (see 13.1).

Dynamic Semantics

For an atomic object (including an atomic component) all reads and updates of the object as a whole are
indivisible.

\{AI05-0117-1\} \{AI05-0275-1\} All tasks of the program (on all processors) that read or update volatile
variables see the same order of updates to the variables. A use of an atomic variable or other mechanism
may be necessary to avoid erroneous execution and to ensure that access to nonatomic volatile variables is
sequential (see 9.10). For a volatile object all reads and updates of the object as a whole are performed
directly to memory.

Implementation Note: \{AI05-0117-1\} \{AI05-0275-1\} To ensure this, on a multiprocessor, any read or update of an
atomic object may require the use of an appropriate memory barrier. This precludes any use of register temporaries,
caches, and other similar optimizations for that object.

Discussion: \{AI05-0275-1\} From 9.10 it follows that (in non-erroneous programs) accesses to variables, including
those shared by multiple tasks, are always sequential. This guarantees that no task will ever see partial updates of any
variable. For volatile variables (including atomic variables), the above rule additionally specifies that all tasks see the
same order of updates.

\{AI05-0275-1\} If for a shared variable $X$, a read of $X$ occurs sequentially after an update of $X$, then the read will return
the updated value if $X$ is volatile or atomic, but may or may not return the updated value if $X$ is nonvolatile. For
nonvolatile accesses, a signaling action is needed in order to share the updated value.

\{AI05-0275-1\} Because accesses to the same atomic variable by different tasks establish a sequential order between
the actions of those tasks, implementations may be required to emit memory barriers around such updates or use
atomic instructions that imply such barriers.

Two actions are sequential (see 9.10) if each is the read or update of the same atomic object.

If a type is atomic or volatile and it is not a by-copy type, then the type is defined to be a by-reference
type. If any subcomponent of a type is atomic or volatile, then the type is defined to be a by-reference
type.

If an actual parameter is atomic or volatile, and the corresponding formal parameter is not, then the
parameter is passed by copy.

Implementation Note: Note that in the case where such a parameter is normally passed by reference, a copy of the
actual will have to be produced at the call-site, and a pointer to the copy passed to the formal parameter. If the actual is
atomic, any copying has to use indivisible read on the way in, and indivisible write on the way out.

Reason: It has to be known at compile time whether an atomic or a volatile parameter is to be passed by copy or by
reference. For some types, it is unspecified whether parameters are passed by copy or by reference. The above rules
further specify the parameter passing rules involving atomic and volatile types and objects.
All reads of or writes to any nonatomic subcomponent of a full access object are performed by reading and/or writing all of the nearest enclosing full access object.

**Implementation Note:** For example, if a 32-bit record object has four nonatomic components, each occupying one byte, then an assignment to one of those components might normally be implemented on some target machines via some sort of store_byte instruction; if the record object is an atomic full access object then instead a 32-bit read-modify-write must be performed. That read-modify-write need not be atomic, although the read and the write must each separately be atomic. Note that it doesn't matter whether the store_byte instruction would have executed atomically. This rule is needed in some cases for memory-mapped device registers.

**Discussion:** The atomic reads and writes associated with accesses to nonatomic components of a full access object that is atomic are normal atomic operations — all of the rules that apply to other atomic operations apply to these as well. In particular, these atomic reads and writes are sequential if they apply to the same object.

**Implementation Requirements**

The external effect of a program is defined to include each read and update of a volatile or atomic object. The implementation shall not generate any memory reads or updates of atomic or volatile objects other than those specified by the program. However, there may be target-dependent cases where reading or writing a volatile but nonatomic object (typically a component) necessarily involves reading and/or writing neighboring storage, and that neighboring storage can overlap a volatile object.

**Discussion:** The presumption is that volatile or atomic objects might reside in an “active” part of the address space where each read has a potential side effect, and at the very least might deliver a different value.

The rule above and the definition of external effect are intended to prevent (at least) the following incorrect optimizations, where V is a volatile variable:

- X:= V; Y:=V; cannot be allowed to be translated as Y:=V; X:=V;
- Deleting redundant loads: X:= V; X:= V; shall read the value of V from memory twice.
- Deleting redundant stores: V:= X; V:= X; shall write into V twice.
- Extra stores: V:= X+Y; should not translate to something like V:= X; V:= V+Y;
- Extra loads: X:= V; Y:= X+Z; X:=X+B; should not translate to something like Y:= V+Z; X:= V+B;
- Reordering of loads from volatile variables: X:= V1; Y:= V2; (whether or not V1 = V2) should not translate to Y:= V2; X:= V1;
- Reordering of stores to volatile variables: V1:= X; V2:= X; should not translate to V2:=X; V1:= X;

The part about “target-dependent cases” is intended to let compilers use a read-modify-write operation when a volatile component has a size that cannot be directly read or written with the available machine instructions. (For instance, writing a Boolean component with size 1 in a volatile packed array of Boolean requires a pre-read on most existing machines.)

This paragraph was deleted.

If the pragma Pack aspect is True for a type any of whose subcomponents are atomic, the implementation shall not pack the atomic subcomponents more tightly than that for which it can support indivisible reads and updates.

This paragraph was deleted.

**Implementation Permissions**

Within the body of an instance of a generic unit that has a formal type T that is not atomic and an actual type that is atomic, if an object O of type T is declared and explicitly specified as atomic, the implementation may introduce an additional copy on passing O to a subprogram with a parameter of type T that is normally passed by reference. A corresponding permission applies to volatile parameter passing.
Implementation Advice

A load or store of a volatile object whose size is a multiple of System.Storage_Unit and whose alignment is nonzero, should be implemented by accessing exactly the bits of the object and no others, except in the case of a volatile but nonatomic subcomponent of an atomic object.

Implementation Advice: A load or store of a volatile object whose size is a multiple of System.Storage_Unit and whose alignment is nonzero, should be implemented by accessing exactly the bits of the object and no others.

Reason: Since any object can be a volatile object, including packed array components and bit-mapped record components, we require the above only when it is reasonable to assume that the machine can avoid accessing bits outside of the object. The exception is needed so this advice doesn’t conflict with other rules of this subclause.

Ramification: This implies that the load or store of a volatile object that meets the above requirement should not be combined with that of any other object, nor should it access any bits not belonging to any other object. This means that the suitability of the implementation for memory-mapped I/O can be determined from its documentation, as any cases where the implementation does not follow Implementation Advice must be documented.

A load or store of an atomic object should, where possible, be implemented by a single load or store instruction.

Implementation Advice: A load or store of an atomic object should be implemented by a single load or store instruction.

NOTE 1 An imported volatile or atomic constant behaves as a constant (i.e. read-only) with respect to other parts of the Ada program, but can still be modified by an “external source”.

NOTE 2 Specifying the Pack aspect cannot override the effect of specifying an Atomic or Atomic_Components aspect.

NOTE 3 When mapping an Ada object to a memory-mapped hardware register, the Ada object can be declared atomic to ensure that the compiler will read and write exactly the bits of the register as specified in the source code and no others.

Discussion: This is especially important for a write-only hardware register, as in such a case a read-modify-write cycle will not work. The only time the language guarantees such a cycle will not happen is when writing an entire atomic object. If one wants to write individual components of a write-only hardware register (assuming the hardware supports that), those also need to be declared atomic.

Incompatibilities With Ada 83

Pragma Atomic replaces Ada 83’s pragma Shared. The name “Shared” was confusing, because the pragma was not used to mark variables as shared.

Wording Changes from Ada 95

Added Implementation Advice to clarify the meaning of Atomic and Volatile in machine terms. The documentation that this advice applies will make the use of Ada implementations more predictable for low-level (such as device register) programming.

Added wording to clarify that a slice of an object of an atomic type is not atomic, just like a component of an atomic type is not (necessarily) atomic.

Incompatibilities With Ada 2005

Correction: Plugged a hole involving volatile components of formal types when the formal type's component has a nonvolatile type. This was done by making certain actual types illegal for formal derived and formal array types; these types were allowed for Ada 95 and Ada 2005.

Extensions to Ada 2005

Aspects Independent and Independent_Components are new; they eliminate ambiguity about independent addressability.

Aspects Atomic, Atomic_Components, Volatile, and Volatile_Components are new; pragmas Atomic, Atomic_Components, Volatile, and Volatile_Components are now obsolescent.
Wording Changes from Ada 2005

{AI05-0117-1} {AI05-0275-1} Revised the definition of volatile to eliminate overspecification and simply focus on the root requirement (that all tasks see the same view of volatile objects). This is not an inconsistency; "memory" arguably includes on-chip caches so long as those are kept consistent. Moreover, it is difficult to imagine a program that could tell the difference.

{AI05-0142-4} Added wording to take explicitly aliased parameters (see 6.1) into account when determining the legality of parameter passing of volatile and atomic objects.

Inconsistencies With Ada 2012

{AI12-0128-1} Required that nonatomic components of a atomic object use a read-modify-write cycle, as well as clarifying that such a cycle is allowed for volatile objects that aren't exactly the size of a machine scalar. That can introduce a read-modify-write cycle where one was not used previously (for instance, if the components are exactly byte-sized on most machines); it is thought that this will more often fix bugs with access to hardware than it will cause them. If this is an issue, declaring the components themselves as atomic will restore the previous behavior.

Extensions to Ada 2012

{AI12-0282-1} These aspects now can be specified for generic formal types.

{AI12-0363-1} Aspect Full Access Only is new; it can be used to guarantee access to a complete device register for any operation even when the register is mapped to a number of components.

Wording Changes from Ada 2012

{AI12-0001-1} Corrigendum: Clarified that aliased objects are considered to be specified as independently addressable, and also eliminated an unnecessary rule.


{AI12-0234-1} The language-defined package System.Atomic_Operations is the parent of a set of child units that provide facilities for manipulating objects of atomic types and for supporting lock-free synchronization. The subprograms of this subsystem are Intrinsic subprograms (see 6.3.1) in order to provide convenient access to machine operations that can provide these capabilities if they are available in the target environment.

Static Semantics

{AI12-0234-1} The library package System.Atomic_Operations has the following declaration:

```ada
package System.Atomic_Operations
   with Pure, Nonblocking is
end System.Atomic_Operations;
```

{AI12-0234-1} System.Atomic_Operations serves as the parent of other language-defined library units that manipulate atomic objects; its declaration is empty.

{AI12-0234-1} A call to a subprogram is said to be lock-free if the subprogram is guaranteed to return from the call while keeping the processor of the logical thread of control busy for the duration of the call.

{AI12-0234-1} In each child package, a function Is_Lock_Free(...) is provided to check whether the operations of the child package can all be provided lock-free for a given object. Is_Lock_Free returns True if operations defined in the child package are lock-free when applied to the object denoted by Item, and Is_Lock_Free returns False otherwise.

Extensions to Ada 2012

{AI12-0234-1} This package is new.

The language-defined generic package System.Atomic_Operations.Exchange provides the following operations:

- To atomically compare the value of two atomic objects, and update the first atomic object with a desired value if both objects were found to be equal, or otherwise update the second object with the value of the first object.
- To atomically update the value of an atomic object, and then return the value that the atomic object had just prior to the update.

Static Semantics

The generic library package System.Atomic_Operations.Exchange has the following declaration:

```ada
package System.Atomic_Operations.Exchange with Pure, Nonblocking is
  function Atomic_Exchange (Item : aliased in out Atomic_Type; Value : Atomic_Type) return Atomic_Type with Convention => Intrinsic;
  function Atomic_Compare_And_Exchange (Item : aliased in out Atomic_Type; Prior : aliased in out Atomic_Type; Desired : Atomic_Type) return Boolean with Convention => Intrinsic;
  function Is_Lock_Free (Item : aliased Atomic_Type) return Boolean with Convention => Intrinsic;
```

Atomic_Exchange atomically assigns the value of Value to Item, and returns the previous value of Item.

Atomic_Compare_And_Exchange first evaluates the value of Prior. Atomic_Compare_And_Exchange then performs the following steps as part of a single indivisible operation:

- evaluates the value of Item;
- compares the value of Item with the value of Prior;
- if equal, assigns Item the value of Desired;
- otherwise, makes no change to the value of Item.

After these steps, if the value of Item and Prior did not match, Prior is assigned the original value of Item, and the function returns False. Otherwise, Prior is unaffected and the function returns True.

Examples

```ada
type Atomic_Boolean is new Boolean with Atomic;
package Exchange is new Atomic_Operations.Exchange (Atomic_Type => Atomic_Boolean);
Lock : aliased Atomic_Boolean := False;
...```

Example of a spin lock using Atomic_Exchange:
begin -- Some critical section, trying to get the lock:
  -- Obtain the lock
  while Exchange.Atomic_Exchange (Item => Lock, Value => True) loop
    null;
  end loop;
  ... -- Do stuff
  Lock := False; -- Release the lock
end;

C.6.3 The Package System.Atomic_Operations.Test_and_Set

The language-defined package System.Atomic_Operations.Test_And_Set provides an operation to atomically set and clear an atomic flag object.

Static Semantics

The library package System.Atomic_Operations.Test_And_Set has the following declaration:

```ada
package System.Atomic_Operations.Test_And_Set
  with Pure, Nonblocking is
  type Test_And_Set_Flag is mod implementation-defined
    with Atomic, Default_Value => 0, Size => implementation-defined;

  function Atomic_Test_And_Set
    (Item : aliased in out Test_And_Set_Flag) return Boolean
    with Convention => Intrinsic;

  procedure Atomic_Clear
    (Item : aliased in out Test_And_Set_Flag)
    with Convention => Intrinsic;

  function Is_Lock_Free
    (Item : aliased Test_And_Set_Flag) return Boolean
    with Convention => Intrinsic;
end System.Atomic_Operations.Test_And_Set;
```

Implementation defined: The modulus and size of Test_and_Set_Flag.

Test_And_Set_Flag represents the state of an atomic flag object. An atomic flag object can either be considered to be set or cleared.

Atomic_Test_And_Set performs an atomic test-and-set operation on Item. Item is set to some implementation-defined nonzero value. The function returns True if the previous contents were nonzero, and otherwise returns False.

Implementation defined: The value used to represent the set value for Atomic_Test_And_Set.

Atomic_Clear performs an atomic clear operation on Item. After the operation, Item contains 0. This call should be used in conjunction with Atomic_Test_And_Set.
The Package System.Atomic_Operations.Integer_Arithmetic

The language-defined generic package System.Atomic_Operations.Integer_Arithmetic provides operations to perform arithmetic atomically on objects of integer types.

Static Semantics

The generic library package System.Atomic_Operations.Integer_Arithmetic has the following declaration:

```ada
generic
  type Atomic_Type is range <> with Atomic;
package System.Atomic_Operations.Integer_Arithmetic
  with Pure, Nonblocking is
  procedure Atomic_Add (Item : aliased in out Atomic_Type;
                        Value : Atomic_Type)
                                with Convention => Intrinsic;
  procedure Atomic_Subtract (Item : aliased in out Atomic_Type;
                            Value : Atomic_Type)
                                with Convention => Intrinsic;
  function Atomic_Fetch_And_Add (Item : aliased in out Atomic_Type;
                                Value : Atomic_Type)
                                return Atomic_Type
                                with Convention => Intrinsic;
  function Atomic_Fetch_And_Subtract (Item : aliased in out Atomic_Type;
                                Value : Atomic_Type)
                                return Atomic_Type
                                with Convention => Intrinsic;
  function Is_Lock_Free (Item : aliased Atomic_Type)
                      return Boolean
                      with Convention => Intrinsic;
end System.Atomic_Operations.Integer_Arithmetic;
```

The operations of this package are defined as follows:

```ada
procedure Atomic_Add (Item : aliased in out Atomic_Type;
                      Value : Atomic_Type)
                      with Convention => Intrinsic;
  { AI12-0321-1 } Atomically performs: Item := Item + Value;

procedure Atomic_Subtract (Item : aliased in out Atomic_Type;
                          Value : Atomic_Type)
                          with Convention => Intrinsic;
  { AI12-0321-1 } Atomically performs: Item := Item - Value;

function Atomic_Fetch_And_Add (Item : aliased in out Atomic_Type;
                                Value : Atomic_Type)
                                return Atomic_Type
                                with Convention => Intrinsic;
  { AI12-0321-1 } Atomically performs: Tmp := Item; Item := Item + Value;
  return Tmp;

function Atomic_Fetch_And_Subtract (Item : aliased in out Atomic_Type;
                                      Value : Atomic_Type)
                                      return Atomic_Type
                                      with Convention => Intrinsic;
  { AI12-0321-1 } Atomically performs: Tmp := Item; Item := Item - Value;
  return Tmp;
```

C.6.5 The Package System.Atomic_Operations.Modular_Arithmetic

{AI12-0364-1} The language-defined generic package System.Atomic_Operations.Modular_Arithmetic provides operations to perform arithmetic atomically on objects of modular types.

Static Semantics

{AI12-0364-1} The generic library package System.Atomic_Operations.Modular_Arithmetic has the following declaration:

generic
  type Atomic_Type is mod <> with Atomic;
package System.Atomic_Operations.Modular_Arithmetic
  with Pure, Nonblocking is
  procedure Atomic_Add (Item : aliased in out Atomic_Type; Value : Atomic_Type)
    with Convention => Intrinsic;
  procedure Atomic_Subtract (Item : aliased in out Atomic_Type; Value : Atomic_Type)
    with Convention => Intrinsic;
  function Atomic_Fetch_And_Add (Item : aliased in out Atomic_Type; Value : Atomic_Type)
    return Atomic_Type
    with Convention => Intrinsic;
  function Atomic_Fetch_And_Subtract (Item : aliased in out Atomic_Type; Value : Atomic_Type)
    return Atomic_Type
    with Convention => Intrinsic;
  function Is_Lock_Free (Item : aliased Atomic_Type) return Boolean
    with Convention => Intrinsic;
end System.Atomic_Operations.Modular_Arithmetic;

{AI12-0364-1} The operations of this package are defined as follows:

procedure Atomic_Add (Item : aliased in out Atomic_Type; Value : Atomic_Type)
  with Convention => Intrinsic;

{AI12-0364-1} Atomically performs: Item := Item + Value;

procedure Atomic_Subtract (Item : aliased in out Atomic_Type; Value : Atomic_Type)
  with Convention => Intrinsic;

{AI12-0364-1} Atomically performs: Item := Item - Value;

function Atomic_Fetch_And_Add (Item : aliased in out Atomic_Type; Value : Atomic_Type)
  with Convention => Intrinsic;

{AI12-0364-1} Atomically performs: Tmp := Item; Item := Item + Value;
return Tmp;
function Atomic_Fetch_And_Subtract
(Item : aliased in out Atomic_Type;
Value : Atomic_Type) return Atomic_Type
with Convention => Intrinsic;

{AI12-0364-1} Atomically performs: Tmp := Item; Item := Item - Value;
return Tmp;

Extensions to Ada 2012

C.7 Task Information
Task Identification and Attributes

{AI95-00266-02} {AI05-0299-1} [This subclause describes operations and attributes that can be used to obtain the identity of a task. In addition, a package that associates user-defined information with a task is defined. Finally, a package that associates termination procedures with a task or set of tasks is defined.]

Wording Changes from Ada 95

{AI95-00266-02} {AI05-0299-1} The title and text here were updated to reflect the addition of task termination procedures to this subclause.

C.7.1 The Package Task_Identification

Static Semantics

The following language-defined library package exists:

package Ada.Task_Identification is
withpragma Preelaborate, Nonblocking, Global => in out synchronized;

type Task_Id is private
withpragma Preelaborable_Initialization (Task_Id);

Null_Task_Id : constant Task_Id;
function "=" (Left, Right : Task_Id) return Boolean;
function Image (T : Task_Id) return String;
function Current_Task return Task_Id;
function Environment_Task return Task_Id;
procedure Abort_Task (T : in out Task_Id) with Nonblocking => False;

{AI05-0189-1} function Is_Terminated (T : Task_Id) return Boolean;
function Is_Callable (T : Task_Id) return Boolean;
function Activation_Is_Complete (T : Task_Id) return Boolean;

private
... -- not specified by the language
end Ada.Task_Identification;

Dynamic Semantics

A value of the type Task_Id identifies an existent task. The constant Null_Task_Id does not identify any task. Each object of the type Task_Id is default initialized to the value of Null_Task_Id.

The function "=" returns True if and only if Left and Right identify the same task or both have the value Null_Task_Id.

The function Image returns an implementation-defined string that identifies T. If T equals Null_Task_Id, Image returns an empty string.
The function `Current_Task` returns a value that identifies the calling task.

**Ramification:** {AI12-0005-1} The logical threads of control associated with the execution of a given parallel construct all execute as part of the execution of one task (see 9, “Tasks and Synchronization”). Thus, the result returned by a call to `Task_Identification.Current_Task` is independent of whether the call takes place during the execution of a parallel construct.

{AI05-0189-1} The function `Environment_Task` returns a value that identifies the environment task.

{AI12-0454-1} The effect of `Abort_Task` is the same as the `abort_statement` for the task identified by `T`. [In addition, if `T` identifies the environment task, the entire partition is aborted, see See E.1.]

The functions `Is_Terminated` and `Is_Callable` return the value of the corresponding attribute of the task identified by `T`.

**Ramification:** {8652/0115} {AI95-00206-01} These routines can be called with an argument identifying the environment task. `Is_Terminated` will always be False for such a call, but `Is_Callable` (usually True) could be False if the environment task is waiting for the termination of dependent tasks. Thus, a dependent task can use `Is_Callable` to determine if the main subprogram has completed.

{AI05-0189-1} The function `Activation_Is_Complete` returns True if the task identified by `T` has completed its activation (whether successfully or not). It returns False otherwise. If `T` identifies the environment task, `Activation_Is_Complete` returns True after the elaboration of the library items of the partition has completed.

For a prefix `T` that is of a task type [{after any implicit dereference}], the following attribute is defined:

`T'Identity` Yields a value of the type `Task_Id` that identifies the task denoted by `T`.

For a prefix `E` that denotes an `entry_declaration`, the following attribute is defined:

`E'Caller` {AI05-0262-1} Yields a value of the type `Task_Id` that identifies the task whose call is now being serviced. Use of this attribute is allowed only inside an `entry_body` or `accept_statement` or `entry_body` after the `entry_barrier` corresponding to the `entry_declaration` denoted by `E`.

{AI12-0231-1} `Abort_Task` is a potentially blocking operation (see 9.5.1).

**Bounded (Run-Time) Errors**

{AI95-00237-01} {AI05-0004-1} It is a bounded error to call the `Current_Task` function from an `entry_body` or an interrupt handler, or finalization of a task attribute. `Program_Error` is raised, or an implementation-defined value of the type `Task_Id` is returned.

**Implementation defined:** The value of `Current_Task` when in a protected entry, or interrupt handler, or finalization of a task attribute.

**Implementation Note:** This value could be `Null_Task_Id`, or the ID of some user task, or that of an internal task created by the implementation.

**Ramification:** {AI95-00237-01} An `entry_barrier` is syntactically part of an `entry_body`, so a call to `Current_Task` from an `entry_barrier` is also covered by this rule.

**Erroneous Execution**

If a value of `Task_Id` is passed as a parameter to any of the operations declared in this package (or any language-defined child of this package), and the corresponding task object no longer exists, the execution of the program is erroneous.
C.7.1 The Package Task_Identification

Documentation Requirements

The implementation shall document the effect of calling Current_Task from an entry body or interrupt handler.

Implementation defined: The effect of calling Current_Task from an entry body or interrupt handler.

Documentation Requirement: The effect of calling Current_Task from an entry body or interrupt handler.

NOTE 1 This package is intended for use in writing user-defined task scheduling packages and constructing server tasks. Current_Task can be used in conjunction with other operations requiring a task as an argument such as Set_Priority (see D.5).

NOTE 2 The function Current_Task and the attribute Caller can return a Task_Id value that identifies the environment task.

Extensions to Ada 95

{AI95-00362-01} Task_Identification is now preelaborated, so it can be used in preelaborated units.

Wording Changes from Ada 95

{8652/0070} {AI95-00101-01} Corrigendum: Corrected the mode of the parameter to Abort_Task to in.

{AI95-00237-01} Corrected the wording to include finalization of a task attribute in the bounded error case; we don't want to specify which task does these operations.

Incompatibilities With Ada 2005

{AI05-0189-1} Functions Environment_Task and Activation_Is_Complete are added to Task_Identification. If Task_Identification is referenced in a use_clause, and an entity E with a defining_identifier of Environment_Task or Activation_Is_Complete is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Wording Changes from Ada 2012

{AI12-0231-1} Correction: Defined what happens if Null_Task_Id is passed to Activation_Is_Complete.

C.7.2 The Package Task_Attributes

Static Semantics

The following language-defined generic library package exists:

```ada
{AI12-0241-1} {AI12-0302-1} with Ada.Task_Identification; use
Ada.Task_Identification;
generic
    type Attribute is private;
    Initial_Value : in Attribute;
package Ada.Task_Attributes
    with Nonblocking, Global => in out synchronized is
    type Attribute_Handle is access all Attribute;
    function Value(T : Task_Id := Current_Task)
        return Attribute;
    function Reference(T : Task_Id := Current_Task)
        return Attribute_Handle;
    procedure Set_Value(Val : in Attribute;
        T : in Task_Id := Current_Task);
    procedure Reinitialize(T : in Task_Id := Current_Task);
end Ada.Task_Attributes;
```

Dynamic Semantics

When an instance of Task_Attributes is elaborated in a given active partition, an object of the actual type corresponding to the formal type Attribute is implicitly created for each task (of that partition) that exists
and is not yet terminated. This object acts as a user-defined attribute of the task. A task created previously in the partition and not yet terminated has this attribute from that point on. Each task subsequently created in the partition will have this attribute when created. In all these cases, the initial value of the given attribute is Initial_Value.

The Value operation returns the value of the corresponding attribute of T.

The Reference operation returns an access value that designates the corresponding attribute of T.

The Set_Value operation performs any finalization on the old value of the attribute of T and assigns Val to that attribute (see 5.2 and 7.6).

The effect of the Reinitialize operation is the same as Set_Value where the Val parameter is replaced with Initial_Value.

**Implementation Note:** In most cases, the attribute memory can be reclaimed at this point.

For all the operations declared in this package, Tasking_Error is raised if the task identified by T is terminated. Program_Error is raised if the value of T is Null_Task_Id.

{AI95-00237-01} After a task has terminated, all of its attributes are finalized, unless they have been finalized earlier. When the master of an instantiation of Ada.Task_Attributes is finalized, the corresponding attribute of each task is finalized, unless it has been finalized earlier.

**Reason:** This is necessary so that a task attribute does not outlive its type. For instance, that's possible if the instantiation is nested, and the attribute is on a library-level task.

**Ramification:** The task owning an attribute cannot, in general, finalize that attribute. That's because the attributes are finalized after the task is terminated; moreover, a task may have attributes as soon as it is created; the task may never even have been activated.

**Bounded (Run-Time) Errors**

{8652/0071} {AI95-00165-01} If the package Ada.Task_Attributes is instantiated with a controlled type and the controlled type has user-defined Adjust or Finalize operations that in turn access task attributes by any of the above operations, then a call of Set_Value of the instantiated package constitutes a bounded error. The call may perform as expected or may result in forever blocking the calling task and subsequently some or all tasks of the partition.

**Erroneous Execution**

It is erroneous to dereference the access value returned by a given call on Reference after a subsequent call on Reinitialize for the same task attribute, or after the associated task terminates.

**Reason:** This allows the storage to be reclaimed for the object associated with an attribute upon Reinitialize or task termination.

If a value of Task_Id is passed as a parameter to any of the operations declared in this package and the corresponding task object no longer exists, the execution of the program is erroneous.

{8652/0071} {AI95-00165-01} {AI95-00237-01} An access to a task attribute is erroneous if executed concurrently with another such access elsewhere or a call with calls of any of the operations declared in package Task_Attributes. An access to a task attribute is erroneous if executed concurrently with or after the finalization of the task attribute.

**Reason:** There is no requirement of atomicity on accesses via a value of type Attribute_Handle.

**Ramification:** A task attribute can only be accessed after finalization through a value of type Attribute_Handle. Operations in package Task_Attributes cannot be used to access a task attribute after finalization, because either the master of the instance has been or is in the process of being left (in which case the instance is out of scope and thus cannot be called), or the associated task is already terminated (in which case Tasking_Error is raised for any attempt to call a task attribute operation).
Implementation Requirements

For a given attribute of a given task, the implementation shall perform the operations declared in this package, each of the above operations for a given attribute of a given task atomically with respect to any of these operations of other of the above operations for the same attribute of the same task. The granularity of any locking mechanism necessary to achieve such atomicity is implementation defined.

Implementation defined: Granularity of locking for Task_Attributes.

Ramification: Hence, other than by dereferencing an access value returned by Reference, an attribute of a given task can be safely read and updated concurrently by multiple tasks.

After a task attributes are finalized or terminates, the implementation shall finalize all attributes of the task, and reclaim any other storage associated with the attributes.

Documentation Requirements

The implementation shall document the limit on the number of attributes per task, if any, and the limit on the total storage for attribute values per task, if such a limit exists.

In addition, if these limits can be configured, the implementation shall document how to configure them.

This paragraph was deleted. Implementation defined: Limits on the number and size of task attributes, and how to configure them. Implementation-defined aspects of Task_Attributes.

Documentation Requirement: For package Task_Attributes, limits on the number and size of task attributes, and how to configure any limits.

Metrics

The implementation shall document the following metrics: A task calling the following subprograms shall execute in a sufficiently high priority as to not be preempted during the measurement period. This period shall start just before issuing the call and end just after the call completes. If the attributes of task T are accessed by the measurement tests, no other task shall access attributes of that task during the measurement period. For all measurements described here, the Attribute type shall be a scalar type whose size is equal to the size of the predefined type Integer integer size. For each measurement, two cases shall be documented: one where the accessed attributes are of the calling task [(that is, the default value for the T parameter is used)], and the other, where T identifies another, nonterminated, task.

The following calls (to subprograms in the Task_Attributes package) shall be measured:

• a call to Value, where the return value is Initial_Value;
• a call to Value, where the return value is not equal to Initial_Value;
• a call to Reference, where the return value designates a value equal to Initial_Value;
• a call to Reference, where the return value designates a value not equal to Initial_Value;
• {AI95-00434-01} a call to Set_Value where the Val parameter is not equal to Initial_Value and the old attribute value is equal to Initial_Value;
• a call to Set_Value where the Val parameter is not equal to Initial_Value and the old attribute value is not equal to Initial_Value.

Documentation Requirement: The metrics for the Task_Attributes package.

Implementation Permissions

An implementation can avoid actually creating the object corresponding to a task attribute until its value is set to something other than that of Initial_Value, or until Reference is called for the task attribute. Similarly, when the value of the attribute is to be reinitialized to that of Initial_Value, the object may instead be finalized and its storage reclaimed, to be recreated when needed.
later. While the object does not exist, the function \texttt{Value} may simply return \texttt{Initial Value}, rather than implicitly creating the object.

\textbf{Discussion}: The effect of this permission can only be observed if the assignment operation for the corresponding type has side effects.

\textbf{Implementation Note}: \{AI95-00114-01\} This permission means that even though every task has every attribute, storage need only be allocated for those attributes for which function \texttt{Reference} has been invoked or set to a value other than that of \texttt{Initial Value}.

An implementation is allowed to place restrictions on the maximum number of attributes a task may have, the maximum size of each attribute, and the total storage size allocated for all the attributes of a task.

\textbf{Implementation Advice}

\{AI95-00434-01\} \{AI12-0438-1\} Some implementations are targeted to domains in which memory use at run time must be completely deterministic. For such implementations, it is recommended that the storage for task attributes will be pre-allocated statically and not from the heap. This can be accomplished by either placing restrictions on the number and the size of the task's attributes of a task, or by using the pre-allocated storage for the first N attribute objects, and the heap for the others. In the latter case, N should be documented.

\textbf{Implementation Advice}: If the target domain requires deterministic memory use at run time, storage for task attributes should be pre-allocated statically and the number of attributes pre-allocated should be documented.

\textbf{Discussion}: We don't mention "restrictions on the size and number" (that is, limits) in the text for the Annex, because it is covered by the Documentation Requirement above, and we try not to repeat requirements in the Annex (they're enough work to meet without having to do things twice).

\{AI95-00237-01\} Finalization of task attributes and reclamation of associated storage should be performed as soon as possible after task termination.

\textbf{Implementation Advice}: Finalization of task attributes and reclamation of associated storage should be performed as soon as possible after task termination.

\textbf{Reason}: \{AI95-00237-01\} This is necessary because the normative wording only says that attributes are finalized “after” task termination. Without this advice, waiting until the instance is finalized would meet the requirements (it is after termination, but may be a very long time after termination). We can’t say anything more specific than this, as we do not want to require the overhead of an interaction with the tasking system to be done at a specific point.

\textbf{NOTE 1} \{AI12-0442-1\} An attribute always exists (after instantiation), and has the initial value. An implementation can avoid using \texttt{It need not occupy memory to store the attribute value} until the first operation that potentially changes the attribute value. The same holds true after Reinitialize.

\textbf{NOTE 2} \{AI12-0442-1\} The result of the \texttt{Reference} function should be used with care; it is always safe to use that result in the task body whose attribute is being accessed. However, when the result is being used by another task, the programmer \texttt{will want to make sure that the task whose attribute is being accessed is not yet terminated}. Failing to do so \texttt{can make the program execution erroneous}.

\textbf{NOTE 3} \{AI95-00434-01\} As specified in C.7.1, if the parameter \texttt{T} (in a call on a subprogram of an instance of this package) identifies a nonexistent task, the execution of the program is erroneous.

\textbf{Wording Changes from Ada 95}

\{8652/0071\} \{AI95-00165-01\} Corrigendum: Clarified that use of task attribute operations from within a task attribute operation (by an \texttt{Adjust} or \texttt{Finalize} call) is a bounded error, and that concurrent use of attribute handles is erroneous.

\{AI95-00237-01\} Clarified the wording so that the finalization takes place after the termination of the task or when the instance is finalized (whichever is sooner).
The Package Task_Termination

Static Semantics

The following language-defined library package exists:

```ada
with Ada.Task_Identification;
with Ada.Exceptions;
package Ada.Task_Termination is
    withpragma Prelaborate, Nonblocking, Global => in out synchronized
    is(Task_Termination);

    type Cause_Of_Termination is (Normal, Abnormal, Unhandled_Exception);

    type Termination_Handler is access protected procedure
        (Cause : in Cause_Of_Termination;
        T     : in Ada.Task_Identification.Task_Id;
        X     : in Ada.Exceptions.Exception_Occurrence);

    procedure Set_Dependents_Fallback_Handler
        (Handler: in Termination_Handler);

    function Current_Task_Fallback_Handler return Termination_Handler;

    procedure Set_Specific_Handler
        (T       : in Ada.Task_Identification.Task_Id;
        Handler : in Termination_Handler);

    function Specific_Handler (T : Ada.Task_Identification.Task_Id)
        return Termination_Handler;

end Ada.Task_Termination;
```

Dynamic Semantics

The type Termination_Handler identifies a protected procedure to be executed by the implementation when a task terminates. Such a protected procedure is called a handler. In all cases T identifies the task that is terminating. If the task terminates due to completing the last statement of its body, or as a result of waiting on a terminate alternative, and the finalization of the task completes normally, then Cause is set to Normal and X is set to Null_Occurrence. If the task terminates because it is being aborted, then Cause is set to Abnormal and X is set to Null_Occurrence if the finalization of the task completes normally. If the task terminates because of an exception raised by the execution of its task_body, then Cause is set to Unhandled_Exception and X is set to the associated exception occurrence if the finalization of the task completes normally. Independent of how the task completes, if finalization of the task propagates an exception, then Cause is either Unhandled_Exception or Abnormal, and X is an exception occurrence that identifies the Program_Error exception.

Each task has two termination handlers, a fall-back handler and a specific handler. The specific handler applies only to the task itself, while the fall-back handler applies only to the dependent tasks of the task. A handler is said to be set if it is associated with anonnull value of type Termination_Handler, and cleared otherwise. When a task is created, its specific handler and fall-back handler are cleared.

The procedure Set_Dependents_Fallback_Handler changes the fall-back handler for the calling task; if Handler is null, that fall-back handler is cleared; otherwise, it is set to be Handler.all. If a fall-back handler had previously been set it is replaced.

The function Current_Task_Fallback_Handler returns the fall-back handler that is currently set for the calling task, if one is set; otherwise, it returns null.

The procedure Set_Specific_Handler changes the specific handler for the task identified by T; if Handler is null, that specific handler is cleared; otherwise, it is set to be Handler.all. If a specific handler had previously been set it is replaced.
Ramification: {AI05-0005-1} This package cannot portably be used to set a handler on the program as a whole. It is possible to call Set_Specific_Handler with the environment task's ID. But any call to the handler would necessarily be a Bounded (Run-Time) Error, as the handler is called after the task's finalization has completed. In the case of the environment task, that includes any possible protected objects, and calling a protected object after it is finalized is a Bounded (Run-Time) Error (see 9.4). This might work in a particular implementation, but it cannot be depended upon.

{AI95-00266-02} {AI05-0264-1} The function Specific_Handler returns the specific handler that is currently set for the task identified by T, if one is set; otherwise, it returns null.

{AI95-00266-02} As part of the finalization of a task_body, after performing the actions specified in 7.6 for finalization of a master, the specific handler for the task, if one is set, is executed. If the specific handler is cleared, a search for a fall-back handler proceeds by recursively following the master relationship for the task. If a task is found whose fall-back handler is set, that handler is executed; otherwise, no handler is executed.

{AI95-00266-02} For Set_Specific_Handler or Specific_Handler, Tasking_Error is raised if the task identified by T has already terminated. Program_Error is raised if the value of T is Ada.Task_Identification.Null_Task_Id.

{AI95-00266-02} An exception propagated from a handler that is invoked as part of the termination of a task has no effect.

Erroneous Execution

{AI95-00266-02} For a call of Set_Specific_Handler or Specific_Handler, if the task identified by T no longer exists, the execution of the program is erroneous.

Extensions to Ada 95

{AI95-00266-02} Package Task_Termination is new.

Wording Changes from Ada 2005

{AI05-0202-1} Correction: Specified what is passed to the handler if the finalization of the task fails after it is completed. This was not specified at all in Ada 2005, so there is a possibility that some program depended on some other behavior of an implementation. But as this case is very unlikely (and only occurs when there is already a significant bug in the program - so should not occur in fielded systems), we're not listing this as an inconsistency.
Annex D
(normative)
Real-Time Systems

This Annex specifies additional characteristics of Ada implementations intended for real-time systems software. To conform to this Annex, an implementation shall also conform to Annex C, “Systems Programming”.

Metrics

The metrics are documentation requirements; an implementation shall document the values of the language-defined metrics for at least one configuration [of hardware or an underlying system] supported by the implementation, and shall document the details of that configuration.

This paragraph was deleted. Implementation defined: Values of all Metrics.

Documentation Requirement: The details of the configuration used to generate the values of all metrics.

Reason: The actual values of the metrics are likely to depend on hardware configuration details that are variable and generally outside the control of a compiler vendor.

The metrics do not necessarily yield a simple number. [For some, a range is more suitable, for others a formula dependent on some parameter is appropriate, and for others, it may be more suitable to break the metric into several cases.] Unless specified otherwise, the metrics in this annex are expressed in processor clock cycles. For metrics that require documentation of an upper bound, if there is no upper bound, the implementation shall report that the metric is unbounded.

Discussion: There are several good reasons to specify metrics in seconds; there are however equally good reasons to specify them in processor clock cycles. In defining the metrics, we have tried to strike a balance on a case-by-case basis.

It has been suggested that all metrics should be given names, so that “data-sheets” could be formulated and published by vendors. However the paragraph number can serve that purpose.

NOTE 1 The specification of the metrics makes a distinction between upper bounds and simple execution times. Where something is just specified as “the execution time of” a piece of code, this leaves one the freedom to choose a nonpathological case. This kind of metric is of the form “there exists a program such that the value of the metric is V”. Conversely, the meaning of upper bounds is “there is no program such that the value of the metric is greater than V”. This kind of metric can only be partially tested, by finding the value of V for one or more test programs.

NOTE 2 The metrics do not cover the whole language; they are limited to features that are specified in Annex C, “Systems Programming” and in this Annex. The metrics are intended to provide guidance to potential users as to whether a particular implementation of such a feature is going to be adequate for a particular real-time application. As such, the metrics are aimed at known implementation choices that can result in significant performance differences.

NOTE 3 The purpose of the metrics is not necessarily to provide fine-grained quantitative results or to serve as a comparison between different implementations on the same or different platforms. Instead, their goal is rather qualitative; to define a standard set of approximate values that can be measured and used to estimate the general suitability of an implementation, or to evaluate the comparative utility of certain features of an implementation for a particular real-time application.

Extensions to Ada 83

This Annex is new to Ada 95.

D.1 Task Priorities

This subclause specifies the priority model for real-time systems. In addition, the methods for specifying priorities are defined.

Paragraphs 2 through 6 were moved to Annex J, “Obsolescent Features”.

1267  16 October 2023  Real-Time Systems  D
### Syntax

The form of a `pragma Priority` is as follows:

```ada
pragma Priority(expression);
```

The form of a `pragma Interrupt_Priority` is as follows:

```ada
pragma Interrupt_Priority((expression));
```

### Name Resolution Rules

The expected type for the expression in a `Priority` or `Interrupt_Priority` pragma is `Integer`.

### Static Semantics

For a task type (including the anonymous type of a `single_task_declaration`), protected type (including the anonymous type of a `single_protected_declaration`), or subprogram, the following language-defined representation aspects may be specified:

#### Priority

The aspect `Priority` is an `expression`, which shall be of type `Integer`.

**Aspect Description for Priority:** Priority of a task object or type, or priority of a protected object or type; the priority is not in the interrupt range.

#### Interrupt_Priority

The aspect `Interrupt_Priority` is an `expression`, which shall be of type `Integer`.

**Aspect Description for Interrupt_Priority:** Priority of a task object or type, or priority of a protected object or type; the priority is in the interrupt range.

### Legality Rules

This paragraph was deleted. A `Priority` pragma is allowed only immediately within a `task_definition`, a `protected_definition`, or the `declarative_part` of a `subprogram_body`. An `Interrupt_Priority` pragma is allowed only immediately within a `task_definition` or a `protected_definition`. At most one such pragma shall appear within a given construct.

If the `Priority` aspect is specified for a subprogram pragma that appears in the `declarative_part` of a `subprogram_body`, the `expression` shall be static, and its value shall be in the range of `System.Priority`.

**Reason:** This value is needed before it gets elaborated, when the environment task starts executing.

At most one of the `Priority` and `Interrupt_Priority` aspects may be specified for a given entity.

**Ramification:** This includes specifying via pragmas (see J.15.11). Note that 13.1 prevents multiple specifications of a single representation aspect by any means.

Neither of the `Priority` or `Interrupt_Priority` aspects shall be specified for a synchronized interface type.

### Static Semantics

The following declarations exist in package `System`:

```ada
subtype Any_Priority is Integer range implementation-defined;
subtype Priority is Any_Priority range Any_Priority'First .. Any_Priority'Last;
subtype Interrupt_Priority is Any_Priority range Priority'Last+1 .. Any_Priority'Last;
```

```ada
Default_Priority : constant Priority := (Priority'First + Priority'Last)/2;
```

**Implementation defined:** The declarations of `Any_Priority` and `Priority`.
The full range of priority values supported by an implementation is specified by the subtype `Any_Priority`. The subrange of priority values that are high enough to require the blocking of one or more interrupts is specified by the subtype `Interrupt_Priority`. [The subrange of priority values below `System.Interrupt_Priority'First` is specified by the subtype `System.Priority`.

This paragraph was deleted.\{AI05-0229-1\} The priority specified by a `Priority` or `Interrupt_Priority` pragma is the value of the expression in the pragma, if any. If there is no expression in an `Interrupt_Priority` pragma, the priority value is `Interrupt_Priority'Last`.

Dynamic Semantics

\{AI05-0229-1\} The `Priority` aspect pragma has no effect if it occurs in the declarative_part of the subprogram_body of a subprogram other than the main subprogram; the `Priority` value is not associated with any task.

\{AI12-0404-1\} A task priority is an integer value that indicates a degree of urgency and is the basis for resolving competing demands of tasks for resources. Unless otherwise specified, whenever tasks compete for processors or other implementation-defined resources, the resources are allocated to the task with the highest priority value. The base priority of a task is the priority with which it was created, or to which it was later set by `Dynamic_Priorities.Set_Priority` (see D.5). At all times, a task also has an active priority, which generally reflects its base priority unless as well as any priority it inherits from other sources. Priority inheritance is the process by which the priority of a task or other entity (for example, a protected object; see D.3) is used in the evaluation of another task's active priority.

Implementation defined: Implementation-defined execution resources.

\{AI05-0229-1\} The effect of specifying a `Priority` or `Interrupt_Priority` aspect for a protected type or single_protected_declaration such a pragma in a protected_definition is discussed in D.3.

\{AI05-0229-1\} \{AI12-0081-1\} The expression specified for the `Priority` or `Interrupt_Priority` aspect of a task type pragma that appears in a task_definition is evaluated for each time a task object of the task type is created (see 9.1). For the `Priority` aspect pragma, the value of the expression is converted to the subtype `Priority`; for the `Interrupt_Priority` aspect pragma, this value is converted to the subtype `Any_Priority`. The priority value is then associated with the task object whose task_declaration specifies the aspect_definition contains the pragma.

\{AI05-0229-1\} Likewise, the priority value is associated with the environment task if the aspect is specified for a pragma that appears in the declarative_part of the main subprogram.

\{AI05-0229-1\} The initial value of a task's base priority is specified by default or by means of a `Priority` or `Interrupt_Priority` aspect. After a task is created, its base priority can be changed only by a call to `Dynamic_Priorities.Set_Priority` (see D.5).] The initial base priority of a task in the absence of an aspect is the base priority of the task that creates it at the time of creation (see 9.1). If the aspect pragma `Priority` is not specified for the main subprogram, the initial base priority of the environment task is `System.Default_Priority`. [The task's active priority is used when the task competes for processors. Similarly, the task's active priority is used to determine the task's position in any queue when `Priority_Queuing` is specified (see D.4).]

\{AI95-00357-01\} At any time, the active priority of a task is the maximum of all the priorities the task is inheriting at that instant. For a task that is not held (see D.11), its base priority is always a source of priority inheritance, unless otherwise specified for a particular task dispatching policy. Other sources of priority inheritance are specified under the following conditions:

**Discussion:** Other parts of the annex, e.g. D.11, define other sources of priority inheritance.

- \{8652/0072\} \{AI95-00092-01\} During activation, a task being activated inherits the active priority of its activator (see 9.2) had at the time the activation was initiated.
During rendezvous, the task accepting the entry call inherits the active priority of the entry caller (see 9.5.3 and D.4).

While starting a protected action on a protected object when the FIFO_Spinning admission policy is in effect, a task inherits the ceiling priority of the protected object (see 9.5, D.3, and D.4.1).

Priority inheritance is needed for FIFO_Spinning to ensure that lower priority tasks that initiate spin waiting earlier than other higher priority tasks continue to spin to ensure that they can be granted the resource when it becomes available in order to support FIFO ordering. Note that this rule only matters when tasks that can initiate a protected action on an object P can be on a different processor than P. In particular, this rule does not matter on a monoprocessor.

While a task executes a protected action on a protected object, the task inherits the ceiling priority of the protected object (see 9.5 and D.3).

In all of these cases, the priority ceases to be inherited as soon as the condition calling for the inheritance no longer exists.

The range of System.Priority shall include at least 30 values.

The range of System.Interrupt_Priority shall include at least one value.

The priority expression can include references to discriminants of the enclosing type.

It is a consequence of the active priority rules that at the point when a task stops inheriting a priority from another source, its active priority is re-evaluated. This is in addition to other instances described in this Annex for such re-evaluation.

An implementation may provide a nonstandard mode in which tasks inherit priorities under conditions other than those specified above.

The use of a Priority or Interrupt_Priority aspect pragma does not require the package System to be named in a with_clause for the enclosing compilation_unit.

The priority of a task is per-object and not per-type.

Priorities need not be static anymore (except for the main subprogram).

The description of the Priority pragma has been moved to this annex.

Corrigendum: Clarified that dynamic priority changes are not transitive - that is, they don't apply to tasks that are being activated by or in rendezvous with the task that had its priority changed.

Generalized the definition of priority inheritance to take into account the differences between the existing and new dispatching policies.

Aspects Priority and Interrupt_Priority are new; pragmas Priority and Interrupt_Priority are now obsolescent.

Clarified when the Priority and Interrupt_Priority aspect expressions are evaluated.

Added an additional case of priority inheritance when the new admission policy FIFO_Spinning is in effect.
D.2 Priority Scheduling

{AI95-00321-01} {AI05-0299-1} [This subclause describes the rules that determine which task is selected for execution when more than one task is ready (see 9.2). The rules have two parts: the task dispatching model (see D.2.1), and a specific task dispatching policy (see D.2.2).]

Wording Changes from Ada 95

{AI95-00321-01} {AI05-0299-1} This introduction is simplified in order to reflect the rearrangement and expansion of this subclause.

D.2.1 The Task Dispatching Model

{AI95-00321-01} [The task dispatching model specifies task preemptive scheduling, based on conceptual priority-ordered ready queues.]

Static Semantics

{AI95-00355-01} The following language-defined library package exists:

{AI05-0166-1} {AI12-0241-1} {AI12-0302-1} package Ada.Dispatching is
    withpragma PreelaboratePure, Nonblocking, Global => in out synchronized
    is Dispatching;
    Dispatching.Policy_Error : exception;
    end Ada.Dispatching;

{AI95-00355-01} {AI05-0166-1} {AI12-0241-1} {AI12-0302-1} procedure Yield
    with Nonblocking => False;
    end Ada.Dispatching;

Dispatching serves as the parent of other language-defined library units concerned with task dispatching.

{AI12-0279-1} For a noninstance subprogram (including a generic formal subprogram), a generic subprogram, or an entry, the following language-defined aspect may be specified with an aspect specification (see 13.1.1):

Yield

The type of aspect Yield is Boolean.

Aspect Description for Yield: Ensures that a callable entity includes a task dispatching point.

If directly specified, the aspect definition shall be a static expression. If not specified (including by inheritance), the aspect is False.

{AI12-0279-1} {AI12-0294-1} If a Yield aspect is specified True for a primitive subprogram \( S \) of a type \( T \), then the aspect is inherited by the corresponding primitive subprogram of each descendant of \( T \).

Legality Rules

{AI12-0279-1} {AI12-0294-1} If the Yield aspect is specified for a dispatching subprogram that inherits the aspect, the specified value shall be confirming.

{AI12-0279-1} {AI12-0294-1} If the Nonblocking aspect (see 9.5) of the associated callable entity is statically True, the Yield aspect shall not be specified as True. For a callable entity that is declared within a generic body, this rule is checked assuming that any nonstatic Nonblocking attributes in the expression of the Nonblocking aspect of the entity are statically True.

Reason: {AI12-0294-1} The second sentence here is an assume-the-worst rule. The only Nonblocking attributes that are nonstatic are those that depend, directly or indirectly, on the nonblocking aspect of a generic formal parameter. We have to assume these might in fact have the value True if given an appropriate actual entity.
In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

Dynamic Semantics

A task can become a running task only if it is ready (see Clause 99.2) and the execution resources required by that task are available. Processors are allocated to tasks based on each task's active priority.

It is implementation defined whether, on a multiprocessor, a task that is waiting for access to a protected object keeps its processor busy.

Implementation defined: Whether, on a multiprocessor, a task that is waiting for access to a protected object keeps its processor busy.

Task dispatching is the process by which a logical thread of control associated with a ready task is selected for execution on a processor. This selection is done at certain points during the execution of such a logical thread of control, at certain points called task dispatching points. Such a logical thread of control reaches a task dispatching point whenever it becomes blocked, and when its associated task terminates whenever it becomes ready. In addition, the completion of an accept_statement (see 9.5.2), and task termination are task dispatching points for the executing task. [Other task dispatching points are defined throughout this Annex for specific policies.]

Below we talk in terms of tasks, but in the context of a parallel construct, a single task can be represented by multiple logical threads of control, each of which can appear separately on a ready queue.

Ramification: On multiprocessor systems, more than one task can be chosen, at the same time, for execution on more than one processor, as explained below.

Task dispatching policies are specified in terms of conceptual ready queues and task states, and task preemption. A ready queue is an ordered list of ready tasks. The first position in a queue is called the head of the queue, and the last position is called the tail of the queue. A task is ready if it is in a ready queue, or if it is running. Each processor has one ready queue for each priority value. At any instant, each ready queue of a processor contains exactly the set of tasks of that priority that are ready for execution on that processor, but are not running on any processor; that is, those tasks that are ready, are not running on any processor, and can be executed using that processor and other available resources. A task can be on the ready queues of more than one processor.

Discussion: The core language defines a ready task as one that is not blocked. Here we refine this definition and talk about ready queues.

Each processor also has one running task, which is the task currently being executed by that processor. Whenever a task running on a processor reaches a task dispatching point it goes back to one or more ready queues; a one task (possibly the same task) is then selected to run on that processor. The task selected is the one at the head of the highest priority nonempty ready queue; this task is then removed from all ready queues to which it belongs.

Discussion: There is always at least one task to run, if we count the idle task.

A preemptible resource is a resource that while allocated to one task can be allocated (temporarily) to another instead. Processors are preemptible resources. Access to a protected object (see 9.5.1) is a nonpreemptible resource. When a higher-priority task is dispatched to the processor, and the previously running task is placed on the appropriate ready queue, the latter task is said to be preempted. A call of Yield and a delay statement are task dispatching points for all language-defined policies point. Yield is a potentially blocking operation (see 9.5.1).
A processor that is executing a task is available to execute tasks of higher priority, within the set of tasks that that processor is able to execute. Write access to a protected object, on the other hand, cannot be granted to a new task before the old task has released it.

A new running task is also selected whenever there is a nonempty ready queue with a higher priority than the priority of the running task, or when the task dispatching policy requires a running task to go back to a ready queue. [These are also task dispatching points.] If the Yield aspect has the value True, then a call to procedure Yield is included within the body of the associated callable entity, and invoked immediately prior to returning from the body if and only if no other task dispatching points were encountered during the execution of the body.

An implementation may place implementation-defined restrictions on tasks whose active priority is in the Interrupt_Priority range.

Implementation defined: The effect of implementation-defined execution resources on task dispatching.

An example of a possible implementation-defined execution resource is a page of physical memory, which must be loaded with a particular page of virtual memory before a task can continue execution.

NOTE 1 Clause 9 specifies under which circumstances a task becomes ready. The ready state is affected by the rules for task activation and termination, delay statements, and entry calls. When a task is not ready, it is said to be blocked.

NOTE 2 An example of a possible implementation-defined execution resource is a page of physical memory, which must be loaded with a particular page of virtual memory before a task can continue execution.

NOTE 3 The ready queues are purely conceptual; there is no requirement that such lists physically exist in an implementation.

NOTE 4 While a task is running, it is not on any ready queue. Any time the task that is running on a processor is added to a ready queue, a new running task is selected for that processor.

NOTE 5 In a multiprocessor system, a task can be on the ready queues of more than one processor. At the extreme, if several processors share the same set of ready tasks, the contents of their ready queues is identical, and so they can be viewed as sharing one ready queue, and can be implemented that way. [Thus, the dispatching model covers multiprocessors where dispatching is implemented using a single ready queue, as well as those with separate dispatching domains.]

NOTE 6 The priority of a task is determined by rules specified in this subclause, and under D.1, “Task Priorities”, D.3, “Priority Ceiling Locking”, and D.5, “Dynamic Priorities”.

NOTE 7 The setting of a task's base priority as a result of a call to Set_Priority does not always take effect immediately when Set_Priority is called. The effect of setting the task's base priority is deferred while the affected task performs a protected action.
Wording Changes from Ada 95

17.a/3 \{AI95-00321-01\} \{AI05-0005-1\} This description is simplified to describe only the parts of the dispatching model common to all policies. In particular, rules about preemption are moved elsewhere. This makes it easier to add other policies (which might not involve preemption).

Incompatibilities With Ada 2005

17.b/3 \{AI05-0166-1\} Procedure Yield is added to Dispatching. If Dispatching is referenced in a use_clause, and an entity \(E\) with a defining_identifier of Yield is defined in a package that is also referenced in a use_clause, the entity \(E\) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

17.c/4 \{AI05-0166-1\} \{AI12-0005-1\} Package Dispatching was a Pure package, but now is Preelaborated with the addition of Yield. This is incompatible as Dispatching can no longer be depended upon from a Pure package. This should happen rarely in practice as the only contents was the exception Dispatching_Policy_Error and none of the child packages that could raise that exception are pure.

Inconsistencies With Ada 2012

17.d/5 \{AI12-0299-1\} Correction: Substantially reduced the Implementation Permission that used to allow “altering” task dispatching points to only allow adding task dispatching points. If an implementation was using this permission to remove task dispatching points, and a program depended on that behavior to work, it could fail when used with Ada 2022. We are not aware of any such implementations, and such behavior was never portable to other implementations, so we do not expect this to matter in practice.

Extensions to Ada 2012

17.e/5 \{AI12-0279-1\} \{AI12-0294-1\} Aspect Yield is new.

Wording Changes from Ada 2012

17.f/5 \{AI12-0119-1\} Redid the description of task dispatching to include the separate threads of control that can be started by a parallel construct.

D.2.2 Task Dispatching Pragmas

The Standard Task Dispatching Policy

0.1/3 \{AI95-00355-01\} \{AI05-00299-1\} [This subclause allows a single task dispatching policy to be defined for all priorities, or the range of priorities to be split into subranges that are assigned individual dispatching policies.]

Syntax

1 The form of a pragma Task_Dispatching_Policy is as follows:

2 \begin{verbatim}
pragma Task_Dispatching_Policy(policy_identifier);
\end{verbatim}

2.1/2 \{AI95-00355-01\} The form of a pragma Priority_Specific_Dispatching is as follows:

2.2/2 \begin{verbatim}
pragma Priority_Specific_Dispatching (
        policy_identifier, first_priority_expression, last_priority_expression);
\end{verbatim}

Name Resolution Rules

2.3/2 \{AI95-00355-01\} The expected type for first_priority_expression and last_priority_expression is Integer.

Legality Rules

3/2 \{AI95-00321-01\} \{AI95-00355-01\} The policy_identifier used in a pragma Task_Dispatching_Policy shall be the name of a task dispatching policy shall either be FIFO_Within_Priorities or an implementation-defined identifier.
Implementation defined: Implementation defined policy identifiers allowed in a pragma Task_Dispatching_Policy.

{AI95-00355-01} The policy identifier used in a pragma Priority_Specific_Dispatching shall be the name of a task dispatching policy.

{AI95-00355-01} Both first_priority_expression and last_priority_expression shall be static expressions in the range of System.Any_Priority; last_priority_expression shall have a value greater than or equal to first_priority_expression.

Static Semantics

{AI95-00355-01} Pragma Task_Dispatching_Policy specifies the single task dispatching policy.

{AI95-00355-01} Pragma Priority_Specific_Dispatching specifies the task dispatching policy for the specified range of priorities. Tasks with base priorities within the range of priorities specified in a Priority_Specific_Dispatching pragma have their active priorities determined according to the specified dispatching policy. Tasks with active priorities within the range of priorities specified in a Priority_Specific_Dispatching pragma are dispatched according to the specified dispatching policy.

Reason: {AI95-00355-01} Each ready queue is managed by exactly one policy. Anything else would be chaos. The ready queue is determined by the active priority. However, how the active priority is calculated is determined by the policy; in order to break out of this circle, we have to say that the active priority is calculated by the method determined by the policy of the base priority.

{AI95-00355-01} {AI05-0262-1} If a partition contains one or more Priority_Specific_Dispatching pragmas, the dispatching policy for priorities not covered by any Priority_Specific_Dispatching pragmas is FIFO_Within_Priorities.

Post-Compilation Rules

{AI95-00355-01} A Task_Dispatching_Policy pragma is a configuration pragma. A Priority_Specific_Dispatching pragma is a configuration pragma.

{AI95-00355-01} The priority ranges specified in more than one Priority_Specific_Dispatching pragma within the same partition shall not be overlapping.

{AI95-00355-01} If a partition contains one or more Priority_Specific_Dispatching pragmas it shall not contain a Task_Dispatching_Policy pragma.

This paragraph was deleted {AI95-00333-01} If the FIFO_Within_Priorities policy is specified for a partition, then the Ceiling_Locking policy (see D.3) shall also be specified for the partition.

Dynamic Semantics

{AI95-00355-01} A task dispatching policy specifies the details of task dispatching that are not covered by the basic task dispatching model. These rules govern when tasks are inserted into and deleted from the ready queues, and whether a task is inserted at the head or the tail of the queue for its active priority.] A single task dispatching policy is specified by a Task_Dispatching_Policy configuration pragma. Pragma Priority_Specific_Dispatching assigns distinct dispatching policies to subranges of System.Any_Priority. If no such pragma appears in any of the program units comprising a partition, the task dispatching policy for that partition is unspecified.

{AI95-00355-01} If neither pragma applies to any of the program units comprising a partition, the task dispatching policy for that partition is unspecified.

{AI95-00355-01} {AI05-0262-1} If a partition contains one or more Priority_Specific_Dispatching pragmas, a task dispatching point occurs for the currently running task of a processor whenever there is a nonempty ready queue for that processor with a higher priority than the priority of the running task.
Discussion: {AI05-0005-1} If we have priority specific dispatching then we want preemption across the entire range of priorities. That prevents higher priority tasks from being blocked by lower priority tasks that have a different policy. On the other hand, if we have a single policy for the entire partition, we might not require any preemption. Note that policy Non_Preemptive_FIFO_Within_Priorities is not allowed in a priority specific dispatching pragma.

{AI95-00355-01} A task that has its base priority changed may move from one dispatching policy to another. It is immediately subject to the new dispatching policy.

Ramification: Once subject to the new dispatching policy, it may be immediately preempted or dispatched, according the rules of the new policy.

Paragraphs 7 through 13 were moved to D.2.3.

{AI95-00321-01} The language defines only one task dispatching policy, FIFO_Within_Priorities; when this policy is in effect, modifications to the ready queues occur only as follows:

- {AI95-00321-01} When a blocked task becomes ready, it is added at the tail of the ready queue for its active priority.
- {AI95-00321-01} When the active priority of a ready task that is not running changes, or the setting of its base priority takes effect, the task is removed from the ready queue for its old active priority and is added at the tail of the ready queue for its new active priority, except in the case where the active priority is lowered due to the loss of inherited priority, in which case the task is added at the head of the ready queue for its new active priority.
- {AI95-00321-01} When the setting of the base priority of a running task takes effect, the task is added to the tail of the ready queue for its active priority.
- {AI95-00321-01} When a task executes a delay_statement that does not result in blocking, it is added to the tail of the ready queue for its active priority.
  
Ramification: If the delay does result in blocking, the task moves to the “delay queue”, not to the ready queue.

- {AI95-00321-01} Each of the events specified above is a task dispatching point (see D.2.1).
- {AI95-00321-01} In addition, when a task is preempted, it is added at the head of the ready queue for its active priority.

Implementation Requirements

13.1/2 {AI95-00333-01} {AI95-00355-01} An implementation shall allow, for a single partition, both the locking policy (see D.3) to be specified as Ceiling Locking and also one or more Priority_Specific_Dispatching pragmas to be given.

Documentation Requirements

Paragraphs 14 through 16 were moved to D.2.3.

{AI95-00321-01} Priority inversion is the duration for which a task remains at the head of the highest priority ready queue while the processor executes a lower priority task. The implementation shall document:

- {AI95-00321-01} The maximum priority inversion a user task can experience due to activity of the implementation (on behalf of lower priority tasks), and
- {AI95-00321-01} whether execution of a task can be preempted by the implementation processing of delay expirations for lower priority tasks, and if so, for how long.

This paragraph was deleted. Implementation defined: Implementation defined aspects of priority inversion.
Implementation Permissions

{AI95-00256-01} {AI12-0444-1} Implementations are allowed to define other task dispatching policies, but are not required to support specifying more than one task dispatching policy per partition.

{AI95-00355-01} {AI12-0444-1} An implementation is not required to support pragma Priority_Specific_Dispatching if it is infeasible to support it in the target environment. [For optimization purposes, an implementation may alter the points at which task dispatching occurs, in an implementation defined manner. However, a delay_statement always corresponds to at least one task dispatching point.]

Implementation defined: Implementation defined task dispatching policies.

Paragraphs 19 through 21 were deleted.

NOTE 1 {AI95-00321-01} If the active priority of a running task is lowered due to loss of inherited priority (as it is on completion of a protected operation) and there is a ready task of the same active priority that is not running, the running task continues to run (provided that there is no higher priority task).

NOTE 2 {AI95-00321-01} The setting of a task’s base priority as a result of a call to Set_Priority does not always take effect immediately when Set_Priority is called. The effect of setting the task’s base priority is deferred while the affected task performs a protected action.

NOTE 3 {AI95-00321-01} Setting the base priority of a ready task causes the task to move to the end of the queue for its active priority, regardless of whether the active priority of the task actually changes.

Extensions to Ada 95

{AI95-00333-01} Amendment Correction: It is no longer required to specify Ceiling_Locking with the language-defined task dispatching policies; we only require that implementations allow them to be used together.

{AI95-00355-01} {AI05-0005-1} Pragma Priority_Specific_Dispatching is new; it allows the specification of different policies for different priorities.

Wording Changes from Ada 95

{AI95-00256-01} Clarified that an implementation need support only one task dispatching policy (of any kind, language-defined or otherwise) per partition.

{AI95-00321-01} {AI05-0005-1} This description is simplified to describe only the rules for the Task_Dispatching_Policy pragma that are common to all policies. In particular, rules about preemption are moved elsewhere. This makes it easier to add other policies (which might not involve preemption).

D.2.3 Preemptive Dispatching

{AI95-00321-01} {AI05-0299-1} [This subclause defines a preemptive task dispatching policy.]

Static Semantics

{AI95-00355-01} The policy identifier FIFO_Within_Priorities is a task dispatching policy.

Dynamic Semantics

{AI95-00321-01} When FIFO Within_Priorities is in effect, modifications to the ready queues occur only as follows:

- {AI95-00321-01} When a blocked task becomes ready, it is added at the tail of the ready queue for its active priority.

- When the active priority of a ready task that is not running changes, or the setting of its base priority takes effect, the task is removed from the ready queue for its old active priority and is added at the tail of the ready queue for its new active priority, except in the case where the active priority is lowered due to the loss of inherited priority, in which case the task is added at the head of the ready queue for its new active priority.
When the setting of the base priority of a running task takes effect, the task is added to the tail of the ready queue for its active priority.

When a task executes a delay_statement that does not result in blocking, it is added to the tail of the ready queue for its active priority.

**Ramification:** If the delay does result in blocking, the task moves to the “delay queue”, not to the ready queue.

### Implementation Requirements

An implementation shall allow, for a single partition, both the task dispatching policy to be specified as FIFO Within Priorities and also the locking policy (see D.3) to be specified as Ceiling_Locking.

**Reason:** This is the preferred combination of the FIFO Within Priorities policy with a locking policy, and we want that combination to be portable.

### Documentation Requirements

**Priority inversion** is the duration for which a task remains at the head of the highest priority nonempty ready queue while the processor executes a lower priority task. The implementation shall document:

- The maximum priority inversion a user task can experience due to activity of the implementation (on behalf of lower priority tasks), and

**Documentation Requirement:** The maximum priority inversion a user task can experience from the implementation.

- whether execution of a task can be preempted by the implementation processing of delay expirations for lower priority tasks, and if so, for how long.

**Documentation Requirement:** The amount of time that a task can be preempted for processing on behalf of lower-priority tasks.

**NOTE 1** If the active priority of a running task is lowered due to loss of inherited priority (as it is on completion of a protected operation) and there is a ready task of the same active priority that is not running, the running task continues to run (provided that there is no higher priority task).

**NOTE 2** Setting the base priority of a ready task causes the task to move to the tail of the queue for its active priority, regardless of whether the active priority of the task actually changes.

### Wording Changes from Ada 95

This subclause is new; it mainly consists of text that was found in D.2.1 and D.2.2 in Ada 95. This was separated out so the definition of additional policies was easier.

We require that implementations allow this policy and Ceiling_Locking together.

We explicitly defined FIFO_Within_Priorities to be a task dispatching policy.

## D.2.4 Non-Preemptive Dispatching

### Implementation Requirements

[This subclause defines a non-preemptive task dispatching policy.]

1/3
Static Semantics

{AI95-00298-01} {AI95-00355-01} The policy identifier Non Preemptive FIFO Within Priorities is a task dispatching policy.

{AI05-0166-1} The following language-defined library package exists:

{AI12-0241-1} {AI12-0302-1} package Ada.Dispatching.Non Preemptive is
withpragma Preelaborate, NonBlocking, Global => in out synchronized
is (Non Preemptive);
procedure Yield To Higher;
procedure Yield To Same Or Higher renames Yield;
end Ada.Dispatching.Non Preemptive;

{AI05-0166-1} {AI05-0264-1} A call of Yield To Higher is a task dispatching point for this policy. If the task at the head of the highest priority ready queue has a higher active priority than the calling task, then the calling task is preempted.

Ramification: For language-defined policies other than Non Preemptive FIFO Within Priorities, a higher priority task should never be on a ready queue while a lower priority task is executed. Thus, for such policies, Yield To Higher does nothing.

Yield To Higher is not a potentially blocking operation; it can be used during a protected operation. That is allowed, as under the predefined Ceiling Locking policy any task with a higher priority than the protected operation cannot call the operation (that would violate the locking policy). An implementation-defined locking policy may need to define the semantics of Yield To Higher differently.

Legality Rules

{AI95-00355-01} Non Preemptive FIFO Within Priorities shall not be specified as the policy identifier of pragma Priority Specific Dispatching (see D.2.2).

Reason: The non-preemptive nature of this policy could cause the policies of higher priority tasks to malfunction, missing deadlines and having unlimited priority inversion. That would render the use of such policies impotent and misleading. As such, this policy only makes sense for a complete system.

Dynamic Semantics

{AI95-00298-01} When Non Preemptive FIFO Within Priorities is in effect, modifications to the ready queues occur only as follows:

- {AI95-00298-01} When a blocked task becomes ready, it is added at the tail of the ready queue for its active priority.
- When the active priority of a ready task that is not running changes, or the setting of its base priority takes effect, the task is removed from the ready queue for its old active priority and is added at the tail of the ready queue for its new active priority.
- When the setting of the base priority of a running task takes effect, the task is added to the tail of the ready queue for its active priority.
- When a task executes a delay_statement that does not result in blocking, it is added to the tail of the ready queue for its active priority.

Ramification: If the delay does result in blocking, the task moves to the “delay queue”, not to the ready queue.

{AI05-0166-1} For this policy, blocking or termination of a task, a non-blocking delay_statement, a call to Yield To Higher, and a call to Yield To Same Or Higher or Yield are is the only non-blocking event that is a task dispatching point (see D.2.1).

Ramification: {AI05-0166-1} A delay statement is always a task dispatching point even if it is not blocking. Similarly, a call to Yield To Higher is never blocking, but it is a task dispatching point. In each of these cases, they can cause the current task to stop running (it is still ready). Otherwise, the running task continues to run until it is blocked.

{AI12-0299-1} This rule supersedes the Implementation Permission of D.2.1; an implementation that adds additional task dispatching points to this policy is incorrect.
Implementation Requirements

{AI95-00333-01} An implementation shall allow, for a single partition, both the task dispatching policy to be specified as Non_Preemptive_FIFO_Within_Priorities and also the locking policy (see D.3) to be specified as Ceiling_Locking.

Reason: This is the preferred combination of the Non_Preemptive_FIFO_Within_Priorities policy with a locking policy, and we want that combination to be portable.

Implementation Permissions

{AI95-00298-01} {AI05-0229-1} {AI05-0269-1} Since implementations are allowed to round all ceiling priorities in subrange System.Priority to System.Priority'Last (see D.3), an implementation may allow a task of a partition using the Non_Preemptive_FIFO_Within_Priorities policy to execute within a protected object without raising its active priority provided the associated protected unit does not contain any subprograms with aspects Interrupt_Handler or Attach_Handler specified, nor does the unit have aspectpragma Interrupt_Priority specified. When the locking policy (see D.3) is Ceiling_Locking, an implementation taking advantage of this permission shall ensure that a call to Yield_to_Higher that occurs within a protected action uses the ceiling priority of the protected object (rather than the active priority of the task) when determining whether to preempt the task, Interrupt_Handler, or Attach_Handler.

Reason: {AI05-0269-1} We explicitly require that the ceiling priority be used in calls to Yield_to_Higher in order to prevent a risk of priority inversion and consequent loss of mutual exclusion when Yield_to_Higher is used in a protected object. This requirement might lessen the value of the permission (as the current Ceiling_Priority will have to be maintained in the TCB), but loss of mutual exclusion cannot be tolerated. The primary benefit of the permission (eliminating the need for preemption at the end of a protected action) is still available. As noted above, an implementation-defined locking policy will need to specify the semantics of Yield_to_Higher, including this case.

Extensions to Ada 95

{AI95-00298-01} {AI95-00355-01} Policy Non_Preemptive_FIFO_Within_Priorities is new.

Extensions to Ada 2005

{AI05-0166-1} Package Dispatching.Non_Preemptive is new.

D.2.5 Round Robin Dispatching

{AI95-00355-01} {AI05-0299-1} [This subclause defines the task dispatching policy Round_Robin_Within_Priorities and the package Round_Robin.]
When task dispatching policy Round Robin Within Priorities is the single policy in effect for a partition, each task with priority in the range of System.Interrupt_Priority is dispatched according to policy FIFO Within Priorities.

**Dynamic Semantics**

The procedures Set_Quantum set the required Quantum value for a single priority level Pri or a range of priority levels Low .. High. If no quantum is set for a Round Robin priority level, Default Quantum is used.

The function Actual_Quantum returns the actual quantum used by the implementation for the priority level Pri.

The function Is_Round_Robin returns True if priority Pri is covered by task dispatching policy Round_Robin_Within_Priorities; otherwise, it returns False.

A call of Actual_Quantum or Set_Quantum raises exception Dispatching.Dispatching_Policy_Error if a predefined policy other than Round_Robin_Within_Priorities applies to the specified priority or any of the priorities in the specified range.

For Round_Robin_Within_Priorities, the dispatching rules for FIFO_Within_Priorities apply with the following additional rules:

- When a task is added or moved to the tail of the ready queue for its base priority, it has an execution time budget equal to the quantum for that priority level. This will also occur when a blocked task becomes executable again.

- When a task is preempted (by a higher priority task) and is added to the head of the ready queue for its priority level, it retains its remaining budget.

- While a task is executing, its budget is decreased by the amount of execution time it uses. The accuracy of this accounting is the same as that for execution time clocks (see D.14).

  **Ramification:** Note that this happens even when the task is executing at a higher, inherited priority, and even if that higher priority is dispatched by a different policy than round robin.

- When a task has exhausted its budget and is without an inherited priority (and is not executing within a protected operation), it is moved to the tail of the ready queue for its priority level. This is a task dispatching point.

  **Ramification:** In this case, it will be given a budget as described in the first bullet. The rules for FIFO_Within_Priority (to which these bullets are added) say that a task that has its base priority set to a Round Robin priority is moved to the tail of the ready queue for its new priority level, and then will be given a budget as described in the first bullet. That happens whether or not the task's original base priority was a Round Robin priority.

**Implementation Requirements**

An implementation shall allow, for a single partition, both the task dispatching policy to be specified as Round Robin Within Priorities and also the locking policy (see D.3) to be specified as Ceiling_Locking.

**Reason:** This is the preferred combination of the Round_Robin_Within_Priorities policy with a locking policy, and we want that combination to be portable.

**Documentation Requirements**

An implementation shall document the quantum values supported.

**Documentation Requirement:** The quantum values supported for round robin dispatching.
An implementation shall document the accuracy with which it detects the exhaustion of the budget of a task.

**Documentation Requirement:** The accuracy of the detection of the exhaustion of the budget of a task for round robin dispatching.

**NOTE 1** {AI95-00355-01} {AI12-0442-1} Due to implementation constraints, the quantum value returned by `Actual_Quantum` can differ from that set with `Set_Quantum`.

**NOTE 2** {AI95-00355-01} A task that executes continuously with an inherited priority will not be subject to round robin dispatching.

---

**D.2.6 Earliest Deadline First Dispatching**

The deadline of a task is an indication of the urgency of the task; it represents a point on an ideal physical time line. The deadline might affect how resources are allocated to the task.

This subclause presents `Dispatching.EDF`, a package for representing the deadline of a task and a dispatching policy that defines Earliest Deadline First (EDF) dispatching. The `Relative_Deadline` aspect is provided to assign an initial deadline to a task. A configuration pragma `Generate_Deadlines` is provided to specify that a task’s deadline is recomputed whenever it is made ready.

This paragraph was deleted.

**Discussion:** {AI95-00355-01} {AI12-0442-1} This aspect pragma is the only way of assigning an initial deadline to a task so that its activation can be controlled by EDF scheduling. This is similar to the way `Priority` is used to give an initial priority to a task.

**Language Design Principles**

This paragraph was deleted.

To predict the behavior of a multi-tasking program it is necessary to control access to the processor which is preemptive, and shared objects which are usually non-preemptive and embodied in protected objects. Two common dispatching policies for the processor are fixed priority and EDF. The most effective control over shared objects is via preemption levels. With a pure priority scheme a single notion of priority is used for processor dispatching and preemption levels. With EDF and similar schemes priority is used for preemption levels (only), with another measure used for dispatching. T.P. Baker showed (Real-Time Systems, March 1991, vol. 3, num. 1, Stack Based Scheduling of Realtime Processes) that for EDF a newly released task should only preempt the currently running task if it has an earlier deadline and a higher preemption level than any currently “locked” protected object. The rules of this subclause implement this scheme including the case where the newly released task should execute before some existing tasks but not preempt the currently executing task.

---

**Syntax**

```
pragma Relative_Deadline (relative_deadline_expression);
```

**Name Resolution Rules**

The expected type for `relative_deadline_expression` is `Real_Time.Time_Span`.

---

**Legality Rules**

A `Relative_Deadline` pragma is allowed only immediately within a task definition or the declarative part of a subprogram body. At most one such pragma shall appear within a given construct.
The policy identifier EDF_Within_PrioritiesEDF_Across_Priorities is a task dispatching policy.

The following language-defined library package exists:

```ada
with Ada.Real_Time;
with Ada.Task_Identification;
package Ada.Dispatching.EDF with Nonblocking, Global => in out synchronized is

type Deadline is Ada.Real_Time.Time;
subtype Relative Deadline is Ada.Real_Time.Time_Span;
constant Default_Deadline : Deadline := Ada.Real_Time.Time_Last;
constant Default_Relative_Deadline : Relative Deadline := Ada.Real_Time.Time_Span_Last;
procedure Set_Deadline
(D : in Deadline;
function Get_Deadline
procedure Set_Relative_Deadline
(D : in Relative Deadline;
function Get_Relative_Deadline
procedure Delay_Until_And_Set_Deadline
(Delay_Until_Time : in Ada.Real_Time.Time;
Deadline_Offset : in Ada.Real_Time.Time_Span) with Nonblocking => False;
```

For a subprogram, a task type (including the anonymous type of a single_task_declaration), or a protected type (including the anonymous type of a single_protected_declaration), the following language-defined representation aspect may be specified:

Relative Deadline

The aspect Relative Deadline is an expression, which shall be of type Ada.Real_Time.Time_Span.

Aspect Description for Relative Deadline: Task or protected type parameter used in Earliest Deadline First Dispatching.

The form of pragma Generate_Deadlines is as follows:

pragma Generate_Deadlines;

The Generate_Deadlines pragma is a configuration pragma.
Legality Rules

{AI05-0229-1} {AI12-0230-1} The Relative_Deadline aspect shall not be specified on a task or protected interface type. If the Relative_Deadline aspect is specified for a subprogram, the aspect_definition shall be a static expression.

Post-Compilation Rules

{AI95-00357-01} {AI12-0230-1} If the EDF_Within_PrioritiesEDF_Across_Priorities policy is specified for a partition, then the Ceiling_Locking policy (see D.3) shall also be specified for the partition.

{AI95-00357-01} {AI12-0230-1} If the EDF_Within_PrioritiesEDF_Across_Priorities policy appears in a Priority_Specific_Dispatching pragma (see D.2.2) in a partition, then the Ceiling_Locking policy (see D.3) shall also be specified for the partition.

Reason: Unlike the other language-defined dispatching policies, the semantic description of EDF_Within_PrioritiesEDF_Across_Priorities assumes Ceiling_Locking (and a ceiling priority) in order to make the mapping between deadlines and priorities work. Thus, we require both policies to be specified if EDF is used in the partition.

Dynamic Semantics

{AI95-00357-01} {AI05-0229-1} The Relative_Deadline aspect pragma has no effect if it is specified for an occurrence in the declarative_part of the subprogram_body of a subprogram other than the main subprogram.

{AI112-0230-1} If pragma Generate_Deadlines is in effect, the deadline of a task is recomputed each time it becomes ready. The new deadline is the value of Real_Time.Clock at the time the task is added to a ready queue plus the value returned by Get_Relative_Deadline.

{AI95-00357-01} {AI05-0229-1} {AI12-0230-1} The initial absolute deadline for a task with a specified for which aspect containing pragma Relative_Deadline is specified is the result of adding the value returned by a call of Real_Time.Clock to the value of the expression specified as the Relative_Deadline that is the value of the aspect_relative_deadline_expression, where this entire computation, including the call of Real_Time.Clock, is performed between task creation and the start of its activation. If the aspect there is no Relative_Deadline is not specified pragma then the initial absolute deadline of a task is the value of Default_Deadline (Ada.Real_Time.Time_Last). The environment task is also given an initial deadline by this rule, using the value of the Relative_Deadline aspect of the main subprogram (if any).

Proof: The environment task is a normal task by 10.2, so of course this rule applies to it.

{AI112-0230-1} The effect of specifying a Relative_Deadline aspect for a protected type or single_protected_declaration is discussed in D.3.

{AI95-00357-01} {AI112-0230-1} A task has both an active and a base absolute deadline. These are the same except when the task is inheriting a relative deadline during activation or a rendezvous (see below) or within a protected action (see D.3). The procedure Set_Deadline changes the (base) absolute deadline of the task to D. The function Get_Deadline returns the (base) absolute deadline of the task.

{AI112-0230-1} The procedure Set_Relative_Deadline changes the relative deadline of the task to D. The function Get_Relative_Deadline returns the relative deadline of the task.

{AI112-0230-1} The function Get_Last_Release_Time returns the time, as provided by Real_Time.Clock, when the task was last made ready (that is, was added to a ready queue).

{AI95-00357-01} {AI112-0230-1} The procedure Delay_Until_And_Set_Deadline delays the calling task until time Delay_Until_Time. When the task becomes ready again it will have deadline Delay_Until_Time + Deadline_Offset.
On a system with a single processor, the setting of the deadline of a task to the new value occurs immediately at the first point that is outside the execution of a protected action. If the task is currently on a ready queue it is removed and re-entered onto the ready queue determined by the rules defined below.

When EDF Within PrioritiesEDF Across Priorities is specified for a priority, the range Low..High all ready queue for that priority is queues in this range are ordered by deadline. The task at the head of a queue is the one with the earliest deadline.

A task dispatching point occurs for the currently running task $T$ to which policy EDF Within PrioritiesEDF Across Priorities applies:

- when a change to the base (absolute) deadline of $T$ occurs;
- there is a task on the ready queue for the active priority of $T$ with a deadline earlier than the deadline of $T$;
- there is a nonempty ready queue for that processor with a higher priority than the active priority of the running task;
- there is a ready task with the same priority as $T$ but with an earlier absolute deadline.

In these cases, the currently running task is said to be preempted and is returned to the ready queue for its active priority, at a position determined by its active (absolute) deadline.

For a task $T$ to which policy EDF Across Priorities applies, the base priority is not a source of priority inheritance; the active priority when first activated or while it is blocked is defined as the maximum of the following:

- the lowest priority in the range specified as EDF Across Priorities that includes the base priority of $T$;
- the priorities, if any, currently inherited by $T$;
- the highest priority $P$, if any, less than the base priority of $T$ such that one or more tasks are executing within a protected object with ceiling priority $P$ and task $T$ has an earlier deadline than all such tasks; and furthermore $T$ has an earlier deadline than all other tasks on ready queues with priorities in the given EDF Across Priorities range that are strictly less than $P$.

Ramification: The active priority of $T$ might be lower than its base priority.

When a task $T$ is first activated or becomes unblocked, it is added to the ready queue corresponding to this active priority. Until it becomes blocked again, the active priority of $T$ remains no less than this value; it will exceed this value only while it is inheriting a higher priority.

Discussion: These rules ensure that a task executing in a protected object is preempted only by a task with a shorter deadline and a higher base priority. This matches the traditional preemption level description without the need to define a new kind of protected object locking.

When the setting of the base priority of a ready task takes effect and the new priority is in a range specified as EDF Within PrioritiesEDF Across Priorities, the task is added to the ready queue, at a position determined by its active deadline corresponding to its new active priority, as determined above.

For all the operations defined in Dispatching EDF, Tasking Error is raised if the task identified by $T$ has terminated. Program Error is raised if the value of $T$ is Null Task Id.

If two tasks with priority designated as EDF Within Priorities rendezvous then the deadline for the execution of the accept statement is the earlier of the deadlines of the two tasks.
D.2.6 Earliest Deadline First Dispatching

29.2/5 \{AI12-0230-1\} During activation, a task being activated inherits the deadline that its activator (see 9.2) had at the time the activation was initiated.

Bounded (Run-Time) Errors

30/5 \{AI95-00357-01\} \{AI12-0230-1\} If EDF_Across_Priorities is specified for priority range Low..High, it is a bounded error to declare a protected object with ceiling priority Low or to assign the value Low to attribute 'Priority. In either case either Program_Error is raised or the ceiling of the protected object is assigned the value Low+1.

Paragraph 30 was deleted.

Erroneous Execution

31/2 \{AI95-00357-01\} If a value of Task_Id is passed as a parameter to any of the subprograms of this package and the corresponding task object no longer exists, the execution of the program is erroneous.

Documentation Requirements

32/2 \{AI95-00357-01\} On a multiprocessor, the implementation shall document any conditions that cause the completion of the setting of the deadline of a task to be delayed later than what is specified for a single processor.

32.a/2 Documentation Requirement: Any conditions that cause the completion of the setting of the deadline of a task to be delayed for a multiprocessor.

33/5 NOTE \{AI95-00357-01\} \{AI05-0264-1\} \{AI12-0230-1\} If two distinct priorities adjacent priority ranges, A..B and B+1..C are specified to have policy EDF_Within_Priorities|EDF_Across_Priorities, then tasks from the higher priority always run before tasks of the lower priority, regardless of deadlines; this is not equivalent to this policy being specified for the single range, A..C.

This paragraph was deleted.

34/5 NOTE \{AI95-00357-01\} \{AI12-0230-1\} The above rules implement the preemption-level protocol (also called Stack Resource Policy protocol) for resource sharing under EDF dispatching. The preemption-level for a task is denoted by its base priority. The definition of a ceiling preemption-level for a protected object follows the existing rules for ceiling locking.

34.a/2 Implementation Note: \{AI95-00357-01\} An implementation may support additional dispatching policies by replacing absolute deadline with an alternative measure of urgency.

Extensions to Ada 95

34.b/2 \{AI95-00357-01\} Policy EDF_Across_Priorities and package Dispatching.EDF are new.

Extensions to Ada 2005

34.c/3 \{AI05-0229-1\} Aspect Relative_Deadline is new; pragma Relative_Deadline is now obsolescent.

Wording Changes from Ada 2005

34.d/3 \{AI05-0055-1\} Correction: Corrected definition of active priority to avoid deadline inversion in an unusual case.

Incompatibilities With Ada 2012

34.e/5 \{AI12-0005-1\} \{AI12-0230-1\} The policy EDF_Across_Priorities was replaced by EDF_Within_Priorities. A program using EDF_Across_Priorities could fail to compile. However, we are not aware of any implementations of EDF_Across_Priorities, so it seems unlikely that any such programs exist outside of books and papers.

D.3 Priority Ceiling Locking

1/3 \{AI05-0299-1\} [This subclause specifies the interactions between priority task scheduling and protected object ceilings. This interaction is based on the concept of the ceiling priority of a protected object.]
Syntax

The form of a pragma Locking_Policy is as follows:

```
pragma Locking_Policy(policy_identifier);
```

Legality Rules

The `policy_identifier` shall either be Ceiling_Locking or an implementation-defined identifier.

**Implementation defined:** Implementation-defined `policy_identifier` allowed in a `pragma Locking_Policy`.

Post-Compilation Rules

A Locking_Policy pragma is a configuration pragma.

Dynamic Semantics

{8652/0073} {AI95-00091-01} {AI95-00327-01} [A locking policy specifies the details of protected object locking. All protected objects have a priority. The locking policy specifies the meaning of the priority of a protected object, which specifies whether or not protected objects have priorities, and the relationships between these priorities and task priorities. In addition, the policy specifies the state of a task when it executes a protected action, and how its active priority is affected by the locking.] The locking policy is specified by a Locking_Policy pragma. For implementation-defined locking policies, the meaning of the priority of a protected object is implementation defined. If no Locking_Policy pragma applies to a protected object, the initial priority is specified by the locking policy.

**Implementation defined:** The locking policy if no Locking_Policy pragma applies to any unit of a partition.

{AI95-00327-01} {AI05-0229-1} The expression specified for the Priority aspect (see D.1) is evaluated as part of the creation of the corresponding protected object and converted to the subtype System.Any_Priority or System.Interrupt_Priority, respectively. The value of the expression is the initial priority of the corresponding protected object. If no Priority or Interrupt_Priority aspect is specified for a protected object, the initial priority is specified by the locking policy.

There is one predefined locking policy, Ceiling_Locking; this policy is defined as follows:

- **AI95-00327-01** {AI05-0229-1} Every protected object has a ceiling priority, which is determined by either a Priority or Interrupt_Priority aspect as defined in D.1, or by assignment to the Priority attribute as described in D.5.2. The ceiling priority of a protected object (or ceiling, for short) is an upper bound on the active priority a task can have when it calls methods of that protected object.

- **AI95-00327-01** The initial ceiling priority of a protected object is equal to the initial priority of that object and converted to the subtype System.Any_Priority or System.Interrupt_Priority, respectively. The value of the expression is the ceiling priority of the corresponding protected object.

- **AI95-00327-01** {AI12-0051-1} If an Interrupt_Handler or Attach_Handler aspect (see C.3.1) is specified for a protected subprogram of a protected type that does not have either the appears in a protected_definition without an Priority or Interrupt_Priority aspect specified pragma, the initial ceiling priority of protected objects of that type is implementation defined, but in the range of the subtype System.Interrupt_Priority.

**Implementation defined:** Default ceiling priorities.
If neither aspect **pragma Priority** nor **Interrupt_Priority**, **Interrupt_Handler**, or **Attach_Handler** is specified for a protected type, and no protected subprogram of the type has aspect **Interrupt_Handler** or **Attach_Handler** specified in the **protected_definition**, then the **initial** priority of the corresponding protected object is **System.Priority'Last**.

While a task executes a protected action, it inherits the **ceiling** priority of the corresponding protected object.

When a task calls a protected operation, a check is made that its active priority is not higher than the priority of the corresponding protected object; **Program_Error** is raised if this check fails.

**Every** protected object has a **relative deadline**, which is determined by a **Relative Deadline** aspect as defined in D.2.6, or by assignment to the **Relative Deadline** attribute as described in D.5.2. The relative deadline of a protected object represents a lower bound on the relative deadline a task may have when it calls a protected operation of that protected object.

If aspect **Relative_Deadline** is not specified for a protected type then the initial relative deadline of the corresponding protected object is **Ada.Real_Time.Time_Span_Zero**.

While a task executes a protected action on a protected object **P**, it inherits the relative deadline of **P**. In this case, let **DF** be 'now' ('now' is obtained via a call on **Ada.Real_Time.Clock** at the start of the action) plus the deadline floor of **P**. If the active deadline of the task is later than **DF**, its active deadline is reduced to **DF**; the active deadline is unchanged otherwise.

When a task calls a protected operation, a check is made that its active deadline minus its last release time is not less than the relative deadline of the corresponding protected object; **Program_Error** is raised if this check fails.

**Bounded (Run-Time) Errors**

Following any change of priority, it is a bounded error for the active priority of any task with a call queued on an entry of a protected object to be higher than the ceiling priority of the protected object. In this case one of the following applies:

1. **AI12-0404-I** at any time prior to executing the entry body, **Program_Error** is raised in the calling task;
2. **AI12-0404-I** when the entry is open, the entry body is executed at the ceiling priority of the protected object;
3. **AI12-0404-I** when the entry is open, the entry body is executed at the ceiling priority of the protected object and then **Program_Error** is raised in the calling task; or
4. **AI12-0404-I** when the entry is open, the entry body is executed at the ceiling priority of the protected object that was in effect when the entry call was queued.

**Ramification:** Note that the error is “blamed” on the task that did the entry call, not the task that changed the priority of the task or protected object. This seems to make sense for the case of changing the priority of a task blocked on a call, since if the **Set_Priority** had happened a little bit sooner, before the task queued a call, the entry-calling task would get the error. Similarly, there is no reason not to raise the priority of a task that is executing in an abortable part, so long as its priority is lowered before it gets to the end and needs to cancel the call. The priority might need to be lowered to allow it to remove the call from the entry queue, in order to avoid violating the ceiling. This seems relatively harmless, since there is an error, and the task is about to start raising an exception anyway.

**Implementation Permissions**

The implementation is allowed to round all ceilings in a certain subrange of **System.Priority** or **System.Interrupt_Priority** up to the top of that subrange, uniformly.
Discussion: For example, an implementation might use Priority’Last for all ceilings in Priority, and Interrupt_Priority’Last for all ceilings in Interrupt_Priority. This would be equivalent to having two ceiling priorities for protected objects, “nonpreemptible” and “noninterruptible”, and is an allowed behavior.

Note that the implementation cannot choose a subrange that crosses the boundary between normal and interrupt priorities.

Implementations are allowed to define other locking policies, but are not required to support specifying more than one locking policy per partition.

[Since implementations are allowed to place restrictions on code that runs at an interrupt-level active priority (see C.3.1 and D.2.1), the implementation may implement a language feature in terms of a protected object with an implementation-defined ceiling, but the ceiling shall be no less than Priority’Last.]

Implementation defined: The ceiling of any protected object used internally by the implementation.

Proof: This permission follows from the fact that the implementation can place restrictions on interrupt handlers and on any other code that runs at an interrupt-level active priority.

The implementation might protect a storage pool with a protected object whose ceiling is Priority’Last, which would cause allocators to fail when evaluated at interrupt priority. Note that the ceiling of such an object has to be at least Priority’Last, since there is no permission for allocators to fail when evaluated at a noninterrupt priority.

Implementation Advice

The implementation should use names that end with “_Locking” for implementation-defined locking policies.

Implementation Advice: Names that end with “_Locking” should be used for implementation-defined locking policies.

NOTE 1 While a task executes in a protected action, it can be preempted only by tasks whose active priorities are higher than the ceiling priority of the protected object.

NOTE 2 If a protected object has a ceiling priority in the range of Interrupt_Priority, certain interrupts are blocked while protected actions of that object execute. In the extreme, if the ceiling is Interrupt_Priority’Last, all blockable interrupts are blocked during that time.

NOTE 3 As described in C.3.1, whenever an interrupt is handled by one of the protected procedures of a protected object, a check is made that its ceiling priority is at least as high as the highest active priority at which tasks can be executing when they call protected operations of that object. In determining this value the following factors, which can affect active priority, are relevant:

- the effect of Set_Priority, 
- nested protected operations, 
- entry calls, 
- task activation, 
- and other implementation-defined factors.

NOTE 4 Attaching a protected procedure whose ceiling is below the interrupt hardware priority to an interrupt causes the execution of the program to be erroneous (see C.3.1).

NOTE 5 On a single processor implementation, the ceiling priority rules guarantee that there is no possibility of deadlock involving only protected subprograms (excluding the case where a protected operation calls another protected operation on the same protected object).

Extensions to Ada 95

All protected objects now have a priority, which is the value of the Priority attribute of D.5.2. How this value is interpreted depends on the locking policy; for instance, the ceiling priority is derived from this value when the locking policy is Ceiling_Locking.

Wording Changes from Ada 95

Corrected the wording to reflect that pragma Locking_Policy cannot be inside of a program unit.

Clarified that an implementation need support only one locking policy (of any kind, language-defined or otherwise) per partition.

The bounded error for the priority of a task being higher than the ceiling of an object it is currently in was moved here from D.5, so that it applies no matter how the situation arises.
Wording Changes from Ada 2005

23.a/3 | {AI05-0229-1} Revised to use aspects Priority and Interrupt_Priority as pragmas Priority and Interrupt_Priority are now obsolescent.

Extensions to Ada 2012

23.f/5 | {AI12-0230-1} All protected objects now have a relative deadline, which is the value of the Relative_Deadline attribute of D.5.2. How this value is interpreted depends on the locking policy.

Wording Changes from Ada 2012

23.g/4 | {AI12-0051-1} Corrigendum: Clarified that the Priority aspect can be used to set the initial ceiling priority of a protected object that contains an interrupt handler.

D.4 Entry Queuing Policies

1/5 | {8652/0074} {AI95-00068-01} {AI05-0299-1} {AI12-0324-1} This subclause specifies a mechanism for a user to choose an entry queuing policy. It also defines three such policies. Other policies are implementation defined.

Implementation defined: Implementation-defined queuing policies.

Syntax

2 The form of a pragma Queuing_Policy is as follows:

3 ```
pragma Queuing_Policy(policy_identifier);
``` 

Legality Rules

4/5 | {AI12-0183-1} The policy_identifier shall be either FIFO_Queuing, Ordered_FIFO_Queuing, Priority_Queuing or an implementation-defined identifier.

Post-Compilation Rules

5 A Queuing_Policy pragma is a configuration pragma.

Dynamic Semantics

6 [A queuing policy governs the order in which tasks are queued for entry service, and the order in which different entry queues are considered for service.] The queuing policy is specified by a Queuing_Policy pragma.

Ramification: The queuing policy includes entry queuing order, the choice among open alternatives of a selective_accept, and the choice among queued entry calls of a protected object when more than one entry_barrier condition is True.

7/5 | {AI95-00355-01} {AI12-0163-1} {AI12-0183-1} Three queuing policies, FIFO_Queuing, Ordered_FIFO_Queuing, and Priority_Queuing, are language defined. If no Queuing_Policy pragma applies to any of the program units comprising the partition, the queuing policy for that partition is FIFO_Queuing. The rules for this policy are specified in 9.5.3 and 9.7.1.

7.1/5 | {AI12-0163-1} The Ordered_FIFO_Queuing policy is defined as follows:

7.2/5 | Calls are selected on a given entry queue in order of arrival.

7.3/5 | When more than one condition of an entry_barrier of a protected object becomes True, and more than one of the respective queues is nonempty, the call that arrived first is selected.

7.4/5 | If the expiration time of two or more open delay_alternatives is the same and no other accept_alternatives are open, the sequence of statements of the delay_alternative that is first in textual order in the selective_accept is executed.
The Priority_Queueing policy is defined as follows:

- **When more than one alternative of a selective_accept is open and has queued calls, the alternative whose queue has the call that arrived first is selected.**

  **Implementation Note:** A possible implementation for this policy would be to assign a sequence number to each queued entry call, where the sequence number is incremented globally across all queues associated with the protected object or selective_accept.

  **Reason:** It would have been marginally easier to use textual order for the case when multiple queues are selectable. But textual order can lead to unfair queue servicing, since the queues in earlier textual order will end up starving the later ones if calls arrive fast enough. Applying arrival first as the selector provides fairness for this policy.

- The calls to an entry ([including a member of an entry family]) are queued in an order consistent with the priorities of the calls. The priority of an entry call is initialized from the active priority of the calling task at the time the call is made, but can change later. Within the same priority, the order is consistent with the calling (or requeuing, or priority setting) time (that is, a FIFO order).

- **{8652/0075} {AI95-00205-01}** After a call is first queued, changes to the active priority of a task do not affect the priority of the call, unless the base priority of the task is set while the task is blocked on an entry call.

- When the base priority of a task is set (see D.5), if the task is blocked on an entry call, and the call is queued, the priority of the call is updated to the new active priority of the calling task. This causes the call to be removed from and then reinserted in the queue at the new active priority.

  **Reason:** A task is blocked on an entry call if the entry call is simple, conditional, or timed. If the call came from the triggering_statement of an asynchronous_select, or a requeue thereof, then the task is not blocked on that call; such calls do not have their priority updated. Thus, there can exist many queued calls from a given task (caused by many nested ATC’s), but a task can be blocked on only one call at a time.

  A previous version of Ada 9X required queue reordering in the asynchronous_select case as well. If the call corresponds to a “synchronous” entry call, then the task is blocked while queued, and it makes good sense to move it up in the queue if its priority is raised.

  However, if the entry call is “asynchronous”, that is, it is due to an asynchronous_select whose triggering_statement is an entry call, then the task is not waiting for this entry call, so the placement of the entry call on the queue is irrelevant to the rate at which the task proceeds.

  Furthermore, when an entry is used for asynchronous_selects, it is almost certain to be a “broadcast” entry or have only one caller at a time. For example, if the entry is used to notify tasks of a mode switch, then all tasks on the entry queue would be signaled when the mode changes. Similarly, if it is indicating some interrupting event such as a control-C, all tasks sensitive to the interrupt will want to be informed that the event occurred. Hence, the order on such a queue is essentially irrelevant.

  Given the above, it seems an unnecessary semantic and implementation complexity to specify that asynchronous queued calls are moved in response to dynamic priority changes. Furthermore, it is somewhat inconsistent, since the call was originally queued based on the active priority of the task, but dynamic priority changes are changing the base priority of the task, and only indirectly the active priority. We say explicitly that asynchronous queued calls are not affected by normal changes in active priority during the execution of an abortable_part. Saying that, if a change in the base priority affects the active priority, then we do want the calls reordered, would be inconsistent. It would also require the implementation to maintain a readily accessible list of all queued calls which would not otherwise be necessary.

  Several rules were removed or simplified when we changed the rules so that calls due to asynchronous_selects are never moved due to intervening changes in active priority, be they due to protected actions, some other priority inheritance, or changes in the base priority.

- **When more than one condition of an entry_barrier of a protected object becomes True, and more than one of the respective queues is nonempty, the call with the highest priority is selected.** If more than one such call has the same priority, the call that is queued on the entry whose declaration is first in textual order in the protected_definition is selected. For members of the same entry family, the one with the lower family index is selected.

- **If the expiration time of two or more open delay_alternatives is the same and no other accept_alternatives are open, the sequence_of_statements of the delay_alternative that is first in textual order in the selective_accept is executed.**
• When more than one alternative of a `selective_accept` is open and has queued calls, an alternative whose queue has the highest-priority call at its head is selected. If two or more open alternatives have equal-priority queued calls, then a call on the entry in the `accept_alternative` that is first in textual order in the `selective_accept` is selected.

**Implementation Permissions**

{AI95-00256-01} {AI12-0444-1} Implementations are allowed to define other queuing policies, but are not required to support specifying more than one queuing policy per partition.

Discussion: 8652/0116 {AI95-00069-01} {AI95-00256-01} This rule is really redundant, as 10.1.5 allows an implementation to limit the use of configuration pragmas to an empty environment. In that case, there would be no way to have multiple policies in a partition. In any case, the wording here really ought to be "...more than one queuing policy per partition," since this part of the rule applies to all queuing policies, not just implementation-defined ones.

{AI95-00188-02} Implementations are allowed to defer the reordering of entry queues following a change of base priority of a task blocked on the entry call if it is not practical to reorder the queue immediately.

Reason: Priority change is immediate, but the effect of the change on entry queues can be deferred. That is necessary in order to implement priority changes on top of a non-Ada kernel.

Discussion: The reordering should occur as soon as the blocked task can itself perform the reinsertion into the entry queue.

**Implementation Advice**

The implementation should use names that end with "_Queuing" for implementation-defined queuing policies.

Implementation Advice: Names that end with "_Queuing" should be used for implementation-defined queuing policies.

**Static Semantics**

{AI12-0164-1} For a task type (including the anonymous type of a `single_task_declaration`), protected type (including the anonymous type of a `single_protected_declaration`), or an entry declaration, the following language-defined representation aspect may be specified:

Max_Entry_Queue_Length

The type of aspect `Max_Entry_Queue_Length` is `Integer`.

Aspect Description for `Max_Entry_Queue_Length`: The maximum entry queue length for a task type, protected type, or entry.

If directly specified, the aspect definition shall be a static expression no less than -1. If not specified, the aspect has value -1 (representing no additional restriction on queue length).

**Legality Rules**

{AI12-0164-1} {AI12-0388-1} If the `Max_Entry_Queue_Length` aspect for a type has a nonnegative value, the `Max_Entry_Queue_Length` aspect for every individual entry of that type shall not be greater than the value of the aspect for the type. The `Max_Entry_Queue_Length` aspect of a type is nonoverridable (see 13.1.1).

Ramification: Aspect `Max_Entry_Queue_Length` can specify less than the partition-wide or type-wide default, but it can't expand the length of a queue.

**Post-Compilation Rules**

{AI12-0164-1} If a restriction `Max_Entry_Queue_Length` applies to a partition, any value specified for the `Max_Entry_Queue_Length` aspect specified for the declaration of a type or entry in the partition shall not be greater than the value of the restriction.
Ramification: 13.12(6) says that the restriction value has to be static, so this is statically checkable. But the restriction does not have to be in the same compilation as the aspect, so the check cannot, in general, be done until link time.

Dynamic Semantics

{AI12-0164-1} If a nonconfirming value is specified for Max_Entry_Queue_Length for a type, and an entry call or requeue would cause the queue for any entry of the type to become longer than the specified value, then Program_Error is raised at the point of the call or requeue.

{AI12-0164-1} If a nonconfirming value is specified for Max_Entry_Queue_Length for an entry, and an entry call or requeue would cause the queue for an entry to become longer than the specified value, then Program_Error is raised at the point of the call or requeue.

Wording Changes from Ada 95

{8652/0074} {AI95-00068-01} Corrigendum: Corrected the number of queuing policies defined.

{8652/0075} {AI95-00205-01} Corrigendum: Corrected so that a call of Set_Priority in an abortable part does not change the priority of the triggering entry call.

{AI95-00188-02} Added a permission to defer queue reordering when the base priority of a task is changed. This is a counterpart to stronger requirements on the implementation of priority change.

{AI95-00256-01} Clarified that an implementation need support only one queuing policy (of any kind, language-defined or otherwise) per partition.

{AI95-00355-01} Fixed wording to make clear that pragma never appears inside of a unit; rather it “applies to” the unit.

Extensions to Ada 2012

{AI12-0163-1} Defined the new queuing policy Ordered_FIFO_Queueing.

{AI12-0164-1} Defined the new aspect Max_Entry_Queue_Length.

D.4.1 Admission Policies

{AI12-0276-1} [This subclause specifies a mechanism for a user to choose an admission policy. It also defines one such policy. Other policies are implementation defined.]

Implementation defined: Implementation-defined admission policies.

Syntax

{AI12-0276-1} The form of a pragma Admission_Policy is as follows:

pragmatischeadmission_policy(policy_identifier);

Legality Rules

{AI12-0276-1} The policy_identifier shall be either FIFO_Spinning or an implementation-defined identifier.

Post-Compilation Rules

{AI12-0276-1} An Admission_Policy pragma is a configuration pragma.

Dynamic Semantics

{AI12-0276-1} An admission policy governs the order in which competing tasks are evaluated for acquiring the execution resource associated with a protected object. The admission policy is specified by an Admission_Policy pragma.

{AI12-0276-1} One admission policy, FIFO_Spinning, is language defined. If FIFO_Spinning is in effect, and starting a protected action on a protected object involves busy-waiting, then calls are selected...
for acquiring the execution resource of the protected object in the order in which the busy-wait was
initiated; otherwise the FIFO_Spinning policy has no effect. If no Admission_Policy pragma applies to
any of the program units in the partition, the admission policy for that partition is implementation defined.

Discussion: {AI12-0005-1} Busy-waiting might be used for protected objects that can be called from tasks running on
other processors than the one the protected object is on. It is unnecessary if all of the tasks that can call a protected
object are on the same processor as the object; in particular, it would not be used on a monoprocessor. Aspect CPU
(see D.16) can be used to ensure that busy-waiting is not needed.

Implementation Note: A possible implementation for this policy would be to apply the abstraction of a ticketing
system by assigning two sequence number values to each protected object. One sequence number represents the next
available ticket number, and the other sequence number represents the ticket number currently being serviced by the
protected object. The next available ticket number is incremented and assigned to a task when the task initiates a busy-
wait for acquiring the execution resource associated with the protected object. The ticket number currently being
serviced is incremented when a task releases this execution resource. As part of acquiring the execution resource, a
busy-wait task waits until its assigned ticket number equals the protected object's value for the ticket number currently
being serviced. While a task busy-waits, it monitors the active priority of the protected object in order to inherit any
modifications to the protected object's active priority.

Implementation Permissions

Discussion: {AI12-0276-1} {AI12-0444-1} Implementations are allowed to define other admission policies, but are
not required to support specifying more than one admission policy per partition.

Discussion: This rule is in fact redundant, as 10.1.5 allows an implementation to limit the use of configuration pragmas
to an empty environment. In that case, there would be no way to have multiple policies in a partition.

Extensions to Ada 2012

{AI12-0276-1} Admission Policies and the specific policy FIFO_Spinning are new.

D.5 Dynamic Priorities

This subclause describes how the priority of an entity can be modified or queried at run time.

Wording Changes from Ada 95

This subclause is turned into two subclauses. This subclause introduction is new.

D.5.1 Dynamic Priorities for Tasks

This subclause describes how the base priority of a task can be modified or queried at run time.

Static Semantics

The following language-defined library package exists:

```ada
package Ada.Dynamic_Priorities is
  withpragma Preelaborate, Nonblocking, Global => in out synchronized
  with System;
  with Ada.Task_Identification; -- See C.7.1
  procedure Set_Priority(Priority : in System.Any_Priority;
      T : in Ada.Task_Identification.Task_Id :=
      Ada.Task_Identification.Current_Task);
  function Get_Priority (T : Ada.Task_Identification.Task_Id :=
      return System.Any_Priority;
end Ada.Dynamic_Priorities;
```

D.4.1 Admission Policies
The procedure `Set_Priority` sets the base priority of the specified task to the specified `Priority` value. `Set_Priority` has no effect if the task is terminated.

The function `Get_Priority` returns T’s current base priority. `Tasking_Error` is raised if the task is terminated.

**Reason:** There is no harm in setting the priority of a terminated task. A previous version of Ada 9X made this a run-time error. However, there is little difference between setting the priority of a terminated task, and setting the priority of a task that is about to terminate very soon; neither case should be an error. Furthermore, the runtime check is not necessarily feasible to implement on all systems, since priority changes might be deferred due to inter-processor communication overhead, so the error might not be detected until after `Set_Priority` has returned.

However, we wish to allow implementations to avoid storing “extra” information about terminated tasks. Therefore, we make `Get_Priority` of a terminated task raise an exception; the implementation need not continue to store the priority of a task that has terminated.

`Program_Error` is raised by `Set_Priority` and `Get_Priority` if T is equal to `Null_Task_Id`.

\{AI95-00188-02\} On a system with a single processor, the setting of `Set_Priority` the task’s base priority of a task T to the new value occurs immediately at the first point when T is outside the execution of an entry. As soon as is practical but not while the task is performing a protected action. This setting occurs no later than the next abort completion point of the task T (see 9.8).

**Implementation Note:** \{AI95-00188-02\} The priority change is immediate if the target task is on a delay queue or a ready queue outside of a protected action. However, consider when `Set_Priority` is called by a task T1 to set the priority of T2, if T2 is blocked, waiting on an entry call queued on a protected object, the entry queue needs to be reordered. Since T1 might have a priority that is higher than the ceiling of the protected object, T1 cannot, in general, do the reordering. One way to implement this is to wake T2 up and have T2 do the work. This is similar to the disentangling of queues that needs to happen when a high-priority task aborts a lower-priority task, which might have a call queued on a protected object with a low ceiling. We have an Implementation Permission in D.4 to allow this implementation. We could have required an immediate priority change if on a ready queue during a protected action, but that would have required extra checks for ceiling violations to meet Bounded (Run-Time) Error requirements of D.3 and potentially could cause a protected action to be abandoned in the middle (by raising `Program_Error`). That seems bad.

**Reason:** A previous version of Ada 9X made it a run-time error for a high-priority task to set the priority of a lower-priority task that has a queued call on a protected object with a low ceiling. This was changed because:

- The check was not feasible to implement on all systems, since priority changes might be deferred due to inter-processor communication overhead. The calling task would continue to execute without finding out whether the operation succeeded or not.
- The runtime check would tend to cause intermittent system failures — how is the caller supposed to know whether the other task happens to have a queued call at any given time? Consider for example an interrupt that needs to trigger a priority change in some task. The interrupt handler could not safely call `Set_Priority` without knowing exactly what the other task is doing, or without severely restricting the ceilings used in the system. If the interrupt handler wants to hand the job off to a third task whose job is to call `Set_Priority`, this won’t help, because one would normally want the third task to have high priority.

**Bounded (Run-Time) Errors**

\{AI95-00327-01\} If a task is blocked on a protected entry call, and the call is queued, it is a bounded error to raise its base priority above the ceiling priority of the corresponding protected object. When an entry call is cancelled, it is a bounded error if the priority of the calling task is higher than the ceiling priority of the corresponding protected object. In either of these cases, either `Program_Error` is raised in the task that called the entry, or its priority is temporarily lowered, or both, or neither.

**Ramification:** Note that the error is “blamed” on the task that did the entry call, not the task that called `Set_Priority`. This seems to make sense for the case of a task blocked on a call, since if the `Set_Priority` had happened a little bit sooner, before the task queued a call, the entry calling task would get the error. In the other case, there is no reason not to raise the priority of a task that is executing in an abortable part, so long as its priority is lowered before it gets to the end and needs to cancel the call. The priority might need to be lowered to allow it to remove the call from the entry queue, in order to avoid violating the ceiling. This seems relatively harmless, since there is an error, and the task is about to start raising an exception anyway.
Paragraph 11 was deleted.

**Erroneous Execution**

12 If any subprogram in this package is called with a parameter T that specifies a task object that no longer exists, the execution of the program is erroneous.

12.a **Ramification:** Note that this rule overrides the above rule saying that Program_Error is raised on Get_Priority of a terminated task. If the task object still exists, and the task is terminated, Get_Priority raises Program_Error. However, if the task object no longer exists, calling Get_Priority causes erroneous execution.

**Documentation Requirements**

12.1/2 `{AI95-00188-02}` On a multiprocessor, the implementation shall document any conditions that cause the completion of the setting of the priority of a task to be delayed later than what is specified for a single processor.

12.a/2 **Documentation Requirement:** Any conditions that cause the completion of the setting of the priority of a task to be delayed for a multiprocessor.

**Metrics**

13 The implementation shall document the following metric:

14 • The execution time of a call to Set_Priority, for the nonpreempting case, in processor clock cycles. This is measured for a call that modifies the priority of a ready task that is not running (which cannot be the calling one), where the new base priority of the affected task is lower than the active priority of the calling task, and the affected task is not on any entry queue and is not executing a protected operation.

14.a/2 **Documentation Requirement:** The metrics for Set_Priority.

15/2 **Note 1 `{AI95-00321-01}`** Setting a task's base priority affects task dispatching. First, it can change the task's active priority. Second, under the FIFO Within Priorities standard task dispatching policy it always causes the task to move to the tail of the ready queue corresponding to its active priority, even if the new base priority is unchanged.

16 **Note 2** Under the priority queuing policy, setting a task's base priority has an effect on a queued entry call if the task is blocked waiting for the call. That is, setting the base priority of a task causes the priority of a queued entry call from that task to be updated and the call to be removed and then reinserted in the entry queue at the new priority (see D.4), unless the call originated from the triggering statement of an asynchronous select.

17 **Note 3** The effect of two or more Set_Priority calls executed in parallel on the same task is defined as executing these calls in some serial order.

17.a **Proof:** This follows from the general reentrancy requirements stated near the beginning of Annex A, “Predefined Language Environment”.

18/5 **Note 4 `{AI05-0092-1}` `{AI12-0447-1}` The rule for when Tasking_Error is raised for Set_Priority or Get_Priority is different from the rule for when Tasking_Error is raised on an entry call (see 9.5.3). In particular, setting or querying the priority of a completed or an abnormal task can be queried/is allowed, so long as the task is not yet terminated, and setting the priority of a task can be set is allowed for any task state (including for terminated tasks).

19/5 **Note 5 `{AI12-0442-1}`** Changing the priorities of a set of tasks can be performed by a series of calls to Set_Priority for each task separately. This can be done For this to work reliably, it should be done within a protected operation that has high enough ceiling priority to guarantee that the operation completes without being preempted by any of the affected tasks.

**Extensions to Ada 95**

19.a/2 `{AI95-00188-02}` **Amendment Correction:** Priority changes are now required to be done immediately so long as the target task is not on an entry queue.

19.b/2 `{AI95-00362-01}` **Dynamic Priorities is now Preelaborated, so it can be used in preelaborated units.**

**Wording Changes from Ada 95**

19.c/3 `{AI95-00327-01}` `{AI05-0299-1}` This Ada 95 subclause was moved down a level turned into a subclause. The paragraph numbers are the same as those for D.5 in Ada 95.
There is no “standard” policy anymore, so that phrase was replaced by the name of a specific policy in the notes.

The bounded error for the priority of a task being higher than the ceiling of an object it is currently in was moved to D.3, so that it applies no matter how the situation arises.

D.5.2 Dynamic Priorities for Protected Objects

This subclause specifies how the priority of a protected object can be modified or queried at run time.

The following attributes are defined for a prefix P that denotes a protected object:

- **P'Priority**
  - Denotes a non-aliased component of the protected object P. This component is of type System.Any_Priority and its value is the priority of P. P'Priority denotes a variable if and only if P denotes a variable. A reference to this attribute shall appear only within the body of P.

- **P'Relative_Deadline**
  - Denotes a non-aliased component of the protected object P. This component is of type Ada.Real_Time.Time_Span and its value is the relative deadline of P. P'Relative_Deadline denotes a variable if and only if P denotes a variable. A reference to this attribute shall appear only within the body of P.

The initial value of the attribute Priority is determined by the initial value of the priority of the protected object (see D.3), and can be changed by an assignment. The initial value of the attribute Relative_Deadline is determined by the initial value of the relative deadline of the protected object (see D.3), and can be changed by an assignment.

If the locking policy Ceiling_Locking (see D.3) is in effect, then the ceiling priority of a protected object \( P \) is set to the value of \( P'\text{Priority} \) at the end of each protected action of \( P \).

If the locking policy Ceiling_Locking is in effect, then for a protected object \( P \) with either an Attach_Handler or Interrupt_Handler aspect specified for one of its procedures, a check is made that the value to be assigned to \( P'\text{Priority} \) is in the range System.Interrupt_Priority. If the check fails, Program_Error is raised.

The implementation shall document the following metric:

- The difference in execution time of calls to the following procedures in protected object \( P \):
  ```ada
  protected P is
    procedure Do_Not_Set_Ceiling (Pr : System.Any_Priority);
    procedure Set_Ceiling (Pr : System.Any_Priority);
  end P;
  ```
protected body P is
  procedure Do_Not_Set_Ceiling (Pr : System.Any_Priority) is
  begin
    null;
  end;
  procedure Set_Ceiling (Pr : System.Any_Priority) is
  begin
    P'Priority := Pr;
  end;
end P;

Documentation Requirement: The metrics for setting the priority of a protected object.

NOTE \{AI95-00327-01\} Since P'Priority is a normal variable, the value following an assignment to the attribute immediately reflects the new value even though its impact on the ceiling priority of P is postponed until completion of the protected action in which it is executed.

Extensions to Ada 95

\{AI95-00327-01\} \{AI95-00445-01\} The ability to dynamically change and query the priority of a protected object is new.

Extensions to Ada 2012

\{AI12-0230-1\} The ability to dynamically change and query the relative deadline of a protected object is new.

D.6 Preemptive Abort

\{AI05-0299-1\} [This subclause specifies requirements on the immediacy with which an aborted construct is completed.]

Dynamic Semantics

On a system with a single processor, an aborted construct is completed immediately at the first point that is outside the execution of an abort-deferred operation.

Documentation Requirements

On a multiprocessor, the implementation shall document any conditions that cause the completion of an aborted construct to be delayed later than what is specified for a single processor.

Implementation defined: On a multiprocessor, any conditions that cause the completion of an aborted construct to be delayed later than what is specified for a single processor.

Documentation Requirement: On a multiprocessor, any conditions that cause the completion of an aborted construct to be delayed later than what is specified for a single processor.

Metrics

The implementation shall document the following metrics:

- The execution time, in processor clock cycles, that it takes for an abort_statement to cause the completion of the aborted task. This is measured in a situation where a task T2 preempts task T1 and aborts T1. T1 does not have any finalization code. T2 shall verify that T1 has terminated, by means of the Terminated attribute.

- On a multiprocessor, an upper bound in seconds, on the time that the completion of an aborted task can be delayed beyond the point that it is required for a single processor.

- \{AI95-00114-01\} An upper bound on the execution time of an asynchronous_select, in processor clock cycles. This is measured between a point immediately before a task T1 executes a protected operation Pr.Set that makes the condition of an entry_barrier Pr.Wait True, and the point where task T2 resumes execution immediately after an entry call to Pr.Wait in an asynchronous_select. T1 preempts T2 while T2 is executing the abortable part, and then blocks itself so that T2 can execute. The execution time of T1 is measured separately, and subtracted.
• An upper bound on the execution time of an asynchronous select, in the case that no asynchronous transfer of control takes place. This is measured between a point immediately before a task executes the asynchronous select with a nonnull abortable part, and the point where the task continues execution immediately after it. The execution time of the abortable part is subtracted.

**Documentation Requirement:** The metrics for aborts.

**Implementation Advice**

Even though the abort statement is included in the list of potentially blocking operations (see 9.5.1), it is recommended that this statement be implemented in a way that never requires the task executing the abort statement to block.

**Implementation Advice:** The abort statement should not require the task executing the statement to block.

On a multi-processor, the delay associated with aborting a task on another processor should be bounded; the implementation should use periodic polling, if necessary, to achieve this.

**Implementation Advice:** On a multi-processor, the delay associated with aborting a task on another processor should be bounded.

**NOTE 1** Abortion does not change the active or base priority of the aborted task.

**NOTE 2** Abortion cannot be more immediate than is allowed by the rules for deferral of abortion during finalization and in protected actions.

### D.7 Tasking Restrictions

{AI05-0299-1} [This subclause defines restrictions that can be used with a pragma Restrictions (see 13.12) to facilitate the construction of highly efficient tasking run-time systems.]

**Static Semantics**

{AI12-0290-1} {AI12-0369-1} A scalar expression within a protected unit is said to be pure-barrier-eligible if it is one of the following:

• a static expression;
• a name that statically names (see 4.9) a scalar subcomponent of the immediately enclosing protected unit;
• a Count attribute reference whose prefix statically denotes an entry declaration of the immediately enclosing unit;
• a call to a predefined relational operator or boolean logical operator (and, or, xor, not), where each operand is pure-barrier-eligible;
• a membership test whose tested simple expression is pure-barrier-eligible, and whose membership choice list meets the requirements for a static membership test (see 4.9);
• a short-circuit control form both of whose operands are pure-barrier-eligible;
• a conditional expression all of whose conditions, selecting expressions, and dependent expressions are pure-barrier-eligible; or
• a pure-barrier-eligible expression enclosed in parentheses.

The following restriction identifiers are language defined:

{AI05-0013-1} {AI05-0216-1} No Task Hierarchy No task depends on a master other than the library-level master. All (nonenvironment) tasks depend directly on the environment task of the partition.
Ramification: {AI05-0013-1} This is equivalent to saying “no task depends on a master other than the master that is the execution of the body of the environment task of the partition”, but it is much easier to understand. This is a post-compilation check, which can be checked at compile-time.

This paragraph was deleted. Ramification: {8652/0042} {AI95-00130-01} Note that protected types with entries and interrupt-handling protected types have nontrivial finalization actions. However, this restriction does not restrict those things.

The second sentence prevents the declaration of objects of access types which would require nested finalization. It also prevents the declarations of coextensions that need finalization in a nested scope. The latter cannot be done by preventing the declaration of the objects, as it is not necessarily known if the coextension type needs finalization (it could be a limited view).

No_Implicit_Heap_Allocations
There are no operations that implicitly require heap storage allocation to be performed by the implementation. The operations that implicitly require heap storage allocation are implementation defined.

Implementation defined: Any operations that implicitly require heap storage allocation.

There are no semantic dependences on the package Dynamic_Priorities, and no occurrences of the attribute Priority.

There is no use of a name denoting call to any of the operations defined in package Interrupts (Is Reserved, Is Attached, Current Handler, Attach Handler, Exchange Handler, Detach Handler, and Reference) are no semantic dependences on the package Asynchronous_Task_Control.

Ramification: {AI05-0013-1} This includes ‘Access’ and ‘Address of any of these operations, as well as inherited versions of these operations.

No.Dynamic_CPU_Assignment
No task has the CPU aspect specified to be a non-static expression. Each task (including the environment task) that has the CPU aspect specified as Not A Specific CPU will be assigned to a particular implementation-defined CPU. The same is true for the environment
task when the CPU aspect is not specified. [Any other task without a CPU aspect will activate and execute on the same processor as its activating task.]

**Proof:** The processor of a task without a CPU aspect is defined in D.16, and this restriction guarantees that the activator always has a CPU assigned.

**Reason:** This restriction prevents any migration of tasks.

**Ramification:** If no CPU aspects are specified, then the program will run on a single CPU, as all of the tasks will be activated directly or indirectly by the environment task, and the rules require the same CPU to be used as the activating task.

**Implementation defined:** When restriction No Dynamic CPU Assignment applies to a partition, the processor on which a task with a CPU value of a Not A Specific CPU will execute.

{AI95-00305-01} {AI05-0013-1} No Local Protected Objects
Protected objects are shall be declared only at library level.

{AI95-00297-01} {AI05-0013-1} No Local Timing_Events
Timing_Events are shall be declared only at library level.

{AI95-00305-01} No Protected Type Allocators
There are no allocators for protected types or types containing protected type subcomponents.

{AI05-0224-1} In the case of an initialized allocator of an access type whose designated type is class-wide and limited, a check is made that the specific type of the allocated object has no protected subcomponents. Program_Error is raised if this check fails.

{AI95-00305-01} {AI05-0211-1} No Relative_Delay
There are no delay_relative_statements, and there is no use of a name that denotes the Timing_Events.Set_Handler subprogram that has a Time_Span parameter.

{AI95-00305-01} No Requeue_Statements
There are no requeue_statements.

{AI95-00305-01} No Select_Statements
There are no select_statements.

{AI95-00394-01} {AI05-0211-1} No Specific Termination_Handlers
There is no use of a name denoting no calls to the Set Specific Handler and Specific Handler subprograms in Task Termination.

{AI12-0117-1} No Tasks Unassigned To CPU
The CPU aspect is specified for the environment task. No CPU aspect is specified to be statically equal to Not A Specific CPU. If aspect CPU is specified (dynamically) to the value Not_A_Specific_CPU, then Program_Error is raised. If Set_CPU or Delay Until And Set_CPU are called with the CPU parameter equal to Not A Specific CPU, then Program_Error is raised.

**Ramification:** If this restriction is used in a context for which restriction No Dynamic CPU Assignment is in effect, then no runtime check is needed when specifying the CPU aspect. If the restriction is used with the Ravenscar profile, no runtime checks are needed.

{AI12-0290-1} Pure_Barrriers
The Boolean expression in each protected entry barrier is pure-barrier-eligible.

{AI95-00305-01} {AI05-0013-1} {AI12-0369-1} Simple_Barrriers
The Boolean expression in each entry barrier is shall be either a static Boolean expression or a name that statically names (see 4.9) denotes a Boolean subcomponent of the enclosing protected object.

The following restriction_parameter_identifiers are language defined:

Max_Select_Alternatives
Specifies the maximum number of alternatives in a selective_accept.
Max_Task_Entries
Specifies the maximum number of entries per task. The bounds of every entry family of a task unit shall be static, or shall be defined by a discriminant of a subtype whose corresponding bound is static. [A value of zero indicates that no rendezvous are possible.]

Max_Protected_Entries
Specifies the maximum number of entries per protected type. The bounds of every entry family of a protected unit shall be static, or shall be defined by a discriminant of a subtype whose corresponding bound is static.

Dynamic Semantics

The following restriction identifier is language defined:

If the following restrictions are violated, the behavior is implementation defined. If an implementation chooses to detect such a violation, Storage_Error should be raised.

No_Task_Termination
All tasks are nonterminating. It is implementation-defined what happens if a task attempts to terminate. If there is a fall-back handler (see C.7.3) set for the partition it should be called when the first task attempts to terminate.

Implementation defined: When restriction No_Task_Termination applies to a partition, what happens when a task terminates.

The following restriction parameter identifiers are language defined:

Max_Storage_At_Blocking
Specifies the maximum portion [(in storage elements)] of a task's Storage_Size that can be retained by a blocked task. If an implementation chooses to detect a violation of this restriction, Storage_Error should be raised; otherwise, the behavior is implementation defined.

Implementation defined: The behavior when restriction Max_Storage_At_Blocking is violated.

Max_Asynchronous_Select_Nesting
Specifies the maximum dynamic nesting level of asynchronous_selects. A value of zero prevents the use of any asynchronous_select and, if a program contains an asynchronous_select, it is illegal. If an implementation chooses to detect a violation of this restriction for values other than zero, Storage_Error should be raised; otherwise, the behavior is implementation defined.

Implementation defined: The behavior when restriction Max_Asynchronous_Select_Nesting is violated.

Max_Tasks
Specifies the maximum number of task creations that may be executed over the lifetime of a partition, not counting the creation of the environment task. A value of zero prevents any task creation and, if a program contains a task creation, it is illegal. If an implementation chooses to detect a violation of this restriction, Storage_Error should be raised; otherwise, the behavior is implementation defined.

Ramification: Note that this is not a limit on the number of tasks active at a given time; it is a limit on the total number of task creations that occur.

Implementation Note: We envision an implementation approach that places TCBs or pointers to them in a fixed-size table, and never reuses table elements.

Implementation defined: The behavior when restriction Max_Tasks is violated.

Max_Entry_Queue_Length
Max_Entry_Queue_Length defines the maximum number of calls that are queued on an entry. Violation of this restriction results in the raising of Program_Error at the point of the call or requeue.

No_Standard_Allocators_After_Elaboration
Specifies that an allocator using a standard storage pool (see 13.11) shall not occur within a parameterless library subprogram.
nor within the handled_sequence_of_statements of a task body. For the purposes of this rule, an allocator of a type derived from a formal access type does not use a standard storage pool.

\{AI05-0189-1\} \{AI05-0262-1\} At run time, Storage_Error is raised if an allocator using a standard storage pool is evaluated after the elaboration of the library items of the partition has completed.

It is implementation defined whether the use of pragma Restrictions results in a reduction in executable program size, storage requirements, or execution time. If possible, the implementation should provide quantitative descriptions of such effects for each restriction.

**Implementation defined:** Whether the use of implementation-defined aspects of pragma Restrictions results in a reduction in program code or data size or execution time.

**Implementation Advice**

When feasible, the implementation should take advantage of the specified restrictions to produce a more efficient implementation.

**Implementation Advice:** When feasible, specified restrictions should be used to produce a more efficient implementation.

**NOTE** The above Storage Checks can be suppressed with pragma Suppress.

**Incompatibilities With Ada 95**

\{AI95-00360-01\} **Amendment Correction:** The No_Nested_Finalization is now defined in terms of types that need finalization. These types include a variety of language-defined types that might be implemented with a controlled type. If the restriction No_Nested_Finalization (see D.7) applies to the partition, and one of these language-defined types does not have a controlled part, it will not be allowed in local objects in Ada 2005 whereas it would be allowed in original Ada 95. Such code is not portable, as other Ada compilers may have had a controlled part, and thus would be illegal under the restriction.

**Extensions to Ada 95**

\{AI95-00297-01\} \{AI95-00305-01\} \{AI95-00394-01\} Restrictions No_Dynamic_Attachment, No_Local_Protected_Objects, No_Protected_Type_Allocators, No_Local_Timing_Events, No_Relative_Delay, No_Requeue_Statement, No_Select_Statements, No_Specific_Termination_Handlers, No_Task_Termination, Max_Entry_Queue_Length, and Simple_Barrriers are newly added to Ada.

**Wording Changes from Ada 95**

\{8652/0042\} \{AI95-00130-01\} **Corrigendum:** Clarified that No_Nested_Finalization covered task and protected parts as well.

\{8652/0076\} \{AI95-00067-01\} **Corrigendum:** Changed the description of Max_Tasks and Max_Async_Control to eliminate conflicts with the High Integrity Annex (see H.4).

\{AI95-00327-01\} Added using of the new Priority attribute to the restriction No_Dynamic_Priorities.

\{AI95-00394-01\} **Restriction** No_Async_Control is now obsolescent.

**Incompatibilities With Ada 2005**

\{AI05-0013-1\} **Correction:** Changed so that coextensions of types that require nested finalization are also prohibited; this is done by prohibiting allocators rather than objects of specific access types. It seems unlikely that any program depending on this restriction would violate it in this blatant manner, so it is expected that very few programs will be affected by this change.

\{AI05-0211-1\} **Correction:** The restriction No_Relative_Delay was changed to include the Timing_Events routine that uses a relative delay. This means that a program that uses that routine and this restriction will now be rejected. However, such a program violates the spirit and intent of the restriction and as such the program should never have been allowed. Moreover, it is unlikely that any program depending on this restriction would violate it in such an obvious manner, so it is expected that very few programs will be affected by this change.

\{AI05-0211-1\} **Correction:** A number of restrictions were changed from "no calls" on some subprogram to "no use of a name that denotes" that subprogram. This closes a hole where renames, uses as the prefix of 'Access, and the like, would not be rejected by the restriction, possibly allowing backdoor access to the prohibited subprogram. A program
that uses one of these restrictions and using such backdoor access will now be rejected; however, it is extremely unlikely that any program that relies on these restrictions would also use an end-run around the restriction, so it is expected that very few programs will be affected by this change.

Extensions to Ada 2005

{AI05-0189-1} Restriction No Standard Allocators After Elaboration is newly added to Ada.

Wording Changes from Ada 2005

{AI05-0013-1} {AI05-0216-1} Correction: Improved the wording of various restrictions to make it clearer that they prohibit things that would otherwise be legal, and to word them as definitions, not Legality Rules.

{AI05-0192-1} Correction: Added wording to explain how No Task Allocators and No Protected Type Allocators are checked for class-wide types. This might be an extension if the compiler assumed the worst in the past (it is now a runtime check).

Extensions to Ada 2012

{AI12-0055-1} Corrigendum: Restriction No Dynamic CPU Assignment is newly added to Ada, for use as part of the Ravenscar profile (see D.13).

{AI12-0117-1} Corrigendum: Restriction No Tasks Unassigned To CPU is newly added to Ada; it ensures that no task is running on an implementation-defined CPU so that task scheduling can be analyzed.

{AI12-0290-1} {AI12-0369-1} Restriction Pure Barriers is newly added to Ada; it allows the Jorvik profile to use more expressive barriers than the Ravenscar profile without having to worry about exceptions or side-effects.

{AI12-0369-1} Restriction Simple Barriers (which is part of the Ravenscar profile) is extended to allow statically named record and array subcomponents; this allows common static analysis patterns to be used with Ravenscar.

D.8 Monotonic Time

{AI05-0299-1} [This subclause specifies a high-resolution, monotonic clock package.]

Static Semantics

The following language-defined library package exists:

{AI12-0241-1} {AI12-0302-1} package Ada.Real_Time

with Nonblocking, Global => in out synchronized is

type Time is private;
  Time_First : constant Time;
  Time_Last : constant Time;
  Time_Unit : constant : = implementation-defined-real-number;

type Time_Span is private;
  Time_Span_First : constant Time_Span;
  Time_Span_Last : constant Time_Span;
  Time_Span_Zero : constant Time_Span;
  Time_Span_Unit : constant Time_Span;

  Tick : constant Time_Span;

function Clock return Time;

function "+" (Left : Time; Right : Time_Span) return Time;
function "+" (Left : Time_Span; Right : Time) return Time;
function "-" (Left : Time; Right : Time_Span) return Time;
function "-" (Left : Time; Right : Time) return Time_Span;

function ";=" (Left, Right : Time) return Boolean;
function ";=" (Left, Right : Time_Span) return Boolean;
function ";=" (Left, Right : Time_Span) return Boolean;
function ";=" (Left, Right : Time) return Boolean;

10/3

10/4

10/5

10/6

10/7

10/8
In this Annex, real time is defined to be the physical time as observed in the external environment. The type Time is a time type as defined by 9.6; [values of this type may be used in a delay_until_statement.] Values of this type represent segments of an ideal time line. The set of values of the type Time corresponds one-to-one with an implementation-defined range of mathematical integers.

Discussion: Informally, real time is defined to be the International Atomic Time (TAI) which is monotonic and nondecreasing. We use it here for the purpose of discussing rate of change and monotonic behavior only. It does not imply anything about the absolute value of Real_Time.Clock, or about Real_Time.Time being synchronized with TAI. It is also used for real time in the metrics, for comparison purposes.

Implementation Note: The specification of TAI as "real time" does not preclude the use of a simulated TAI clock for simulated execution environments.

The Time value I represents the half-open real time interval that starts with E+I*Time_Unit and is limited by E+(I+1)*Time_Unit, where Time_Unit is an implementation-defined real number and E is an unspecified origin point, the epoch, that is the same for all values of the type Time. It is not specified by the language whether the time values are synchronized with any standard time reference. [For example, E can correspond to the time of system initialization or it can correspond to the epoch of some time standard.]

Discussion: E itself does not have to be a proper time value.

This half-open interval I consists of all real numbers R such that E+I*Time_Unit <= R < E+(I+1)*Time_Unit.

Values of the type Time_Span represent length of real time duration. The set of values of this type corresponds one-to-one with an implementation-defined range of mathematical integers. The Time_Span value corresponding to the integer I represents the real-time duration I*Time_Unit.

Reason: The purpose of this type is similar to Standard.Duration; the idea is to have a type with a higher resolution.

Discussion: We looked at many possible names for this type: Real_Time.Duration, Fine_Duration, Interval, Time_Interval_Length, Time_Measure, and more. Each of these names had some problems, and we've finally settled for Time_Span.
Time_First and Time_Last are the smallest and largest values of the Time type, respectively. Similarly, Time_Span_First and Time_Span_Last are the smallest and largest values of the Time_Span type, respectively.

A value of type Seconds_Count represents an elapsed time, measured in seconds, since the epoch.

Dynamic Semantics

Time_Unit is the smallest amount of real time representable by the Time type; it is expressed in seconds. Time_Span_Unit is the difference between two successive values of the Time type. It is also the smallest positive value of type Time_Span. Time_Unit and Time_Span_Unit represent the same real time duration. A clock tick is a real time interval during which the clock value (as observed by calling the Clock function) remains constant. Tick is the average length of such intervals.

\[\text{TI95-00432-01}\] The function To_Duration converts the value TS to a value of type Duration. Similarly, the function To_Time_Span converts the value D to a value of type Time_Span. For To_Duration operations, the result is rounded to the nearest value of type Duration exactly representable value (away from zero if exactly halfway between two exactly representable values). If the result is outside the range of Duration, Constraint_Error is raised. For To_Time_Span, the value of D is first rounded to the nearest integral multiple of Time_Unit, away from zero if exactly halfway between two multiples. If the rounded value is outside the range of Time_Span, Constraint_Error is raised. Otherwise, the value is converted to the type Time_Span.

To_Duration(Time_Span_Zero) returns 0.0, and To_Time_Span(0.0) returns Time_Span_Zero.

\[\text{TI95-00386-01} \quad \text{TI95-00432-01}\] The functions Nanoseconds, Microseconds, and Milliseconds, Seconds, and Minutes convert the input parameter to a value of the type Time_Span. NS, US, and MS, S, and M are interpreted as a number of nanoseconds, microseconds, and milliseconds, seconds, and minutes respectively. The input parameter is first converted to seconds and rounded to the nearest integral multiple of Time_Unit. The result is rounded to the nearest exactly representable value (away from zero if exactly halfway between two multiples. If the rounded value is outside the range of Time_Span, Constraint_Error is raised. Otherwise, the rounded value is converted to the type Time_Span exactly representable values). This paragraph was deleted. \[\text{Discussion-\{TI95-00432-01\}}\] The above does not imply that the Time_Span type will have to accommodate Integer’Last of milliseconds; Constraint_Error is allowed to be raised.

The effects of the operators on Time and Time_Span are as for the operators defined for integer types.

Implementation Note: Though time values are modeled by integers, the types Time and Time_Span need not be implemented as integers.

The function Clock returns the amount of time since the epoch.

The effects of the Split and Time_Of operations are defined as follows, treating values of type Time, Time_Span, and Seconds_Count as mathematical integers. The effect of Split(T,SC,TS) is to set SC and TS to values such that T*Time_Unit = SC*1.0 + TS*Time_Unit, and 0.0 <= TS*Time_Unit < 1.0. The value returned by Time_Of(SC,TS) is the value T such that T*Time_Unit = SC*1.0 + TS*Time_Unit.

Implementation Requirements

The range of Time values shall be sufficient to uniquely represent the range of real times from program start-up to 50 years later. Tick shall be no greater than 1 millisecond. Time_Unit shall be less than or equal to 20 microseconds.

Implementation Note: The required range and accuracy of Time are such that 32-bits worth of seconds and 32-bits worth of ticks in a second could be used as the representation.

\[\text{AI12-0451-1}\] The value of Time_Span_First in seconds shall be no greater than −3600 seconds, and the value of Time_Span_Last in seconds shall be no less than 3600 seconds.
A clock jump is the difference between two successive distinct values of the clock (as observed by calling the Clock function). There shall be no backward clock jumps.

**Documentation Requirements**

The implementation shall document the values of Time_First, Time_Last, Time_Span_First, Time_Span_Last, Time_Span_Unit, and Tick.

**Documentation Requirement:** The values of Time_First, Time_Last, Time_Span_First, Time_Span_Last, Time_Span_Unit, and Tick for package Real_Time.

The implementation shall document the properties of the underlying time base used for the clock and for type Time, such as the range of values supported and any relevant aspects of the underlying hardware or operating system facilities used.

**Documentation Requirement:** The properties of the underlying time base used in package Real_Time.

**Discussion:** If there is an underlying operating system, this might include information about which system call is used to implement the clock. Otherwise, it might include information about which hardware clock is used.

The implementation shall document whether or not there is any synchronization with external time references, and if such synchronization exists, the sources of synchronization information, the frequency of synchronization, and the synchronization method applied.

**Documentation Requirement:** Any synchronization of package Real_Time with external time references.

\{AI05-0299-1\} \{AI12-0439-1\} The implementation shall document any aspects of the external environment that can could interfere with the clock behavior as defined in this subclause.

**Documentation Requirement:** Any aspects of the external environment that can could interfere with package Real_Time.

**Discussion:** For example, the implementation is allowed to rely on the time services of an underlying operating system, and this operating system clock can implement time zones or allow the clock to be reset by an operator. This dependence has to be documented.

**Metrics**

\{AI05-0299-1\} For the purpose of the metrics defined in this subclause, real time is defined to be the International Atomic Time (TAI).

The implementation shall document the following metrics:

- An upper bound on the real-time duration of a clock tick. This is a value D such that if \( t_1 \) and \( t_2 \) are any real times such that \( t_1 < t_2 \) and \( \text{Clock}_{t_1} = \text{Clock}_{t_2} \) then \( t_2 - t_1 \leq D \).

- An upper bound on the size of a clock jump.

- An upper bound on the drift rate of Clock with respect to real time. This is a real number D such that

\[
E(1-D) \leq (\text{Clock}_{t} - \text{Clock}) \leq E(1+D)
\]

provided that: \( \text{Clock} + E(1+D) \leq \text{Time}_\text{Last} \).

- where Clock is the value of Clock at time \( t \), and \( E \) is a real time duration not less than 24 hours. The value of \( E \) used for this metric shall be reported.

**Reason:** This metric is intended to provide a measurement of the long term (cumulative) deviation; therefore, 24 hours is the lower bound on the measurement period. On some implementations, this is also the maximum period, since the language does not require that the range of the type Duration be more than 24 hours. On those implementations that support longer-range Duration, longer measurements should be performed.

- An upper bound on the execution time of a call to the Clock function, in processor clock cycles.
• Upper bounds on the execution times of the operators of the types Time and Time_Span, in processor clock cycles.

**Implementation Note:** A fast implementation of the Clock function involves repeated reading until you get the same value twice. It is highly improbable that more than three reads will be necessary. Arithmetic on time values should not be significantly slower than 64-bit arithmetic in the underlying machine instruction set.

**Documentation Requirement:** The metrics for package Real_Time.

**Implementation Permissions**

{AI12-0444-1} Implementations targeted to machines with word size smaller than 32 bits may omit support for the full range and granularity of the Time and Time_Span types.

**Discussion:** These requirements are based on machines with a word size of 32 bits.

**Implementation Note:** The supported values need to be documented.

**Implementation Advice**

When appropriate, implementations should provide configuration mechanisms to change the value of Tick.

**Reason:** This is often needed when the compilation system was originally targeted to a particular processor with a particular interval timer, but the customer uses the same processor with a different interval timer.

**Discussion:** Tick is a deferred constant and not a named number specifically for this purpose.

**Implementation Note:** This can be achieved either by pre-run-time configuration tools, or by having Tick be initialized (in the package private part) by a function call residing in a board specific module.

It is recommended that Calendar.Clock and Real_Time.Clock be implemented as transformations of the same time base.

**Implementation Advice:** Calendar.Clock and Real_Time.Clock should be transformations of the same time base.

It is recommended that the “best” time base which exists in the underlying system be available to the application through Clock. “Best” may mean highest accuracy or largest range.

**Implementation Advice:** The “best” time base which exists in the underlying system should be available to the application through Real_Time.Clock.

NOTE 1: {AI05-0299-1} The rules in this subclause do not imply that the implementation can protect the user from operator or installation errors that could result in the clock being set incorrectly.

NOTE 2: Time_Unit is the granularity of the Time type. In contrast, Tick represents the granularity of Real_Time.Clock. There is no requirement that these be the same.

**Incompatibilities With Ada 95**

{AI95-00386-01} {AI05-0005-1} Functions Seconds and Minutes are newly added to Real_Time. If Real_Time is referenced in a use_clause, and an entity E with a defining identifier of Seconds or Minutes is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

**Wording Changes from Ada 95**

{AI95-00432-01} Added wording explaining how and when many of these functions can raise Constraint_Error. While there always was an intent to raise Constraint_Error if the values did not fit, there never was any wording to that effect, and since Time_Span was a private type, the normal numeric type rules do not apply to it.

**D.9 Delay Accuracy**

{AI05-0299-1} This subclause specifies performance requirements for the delay_statement. The rules apply both to delay_relative_statement and to delay_until_statement. Similarly, they apply equally to a simple delay_statement and to one which appears in a delay_alternative.
Dynamic Semantics

The effect of the delay_statement for Real_Time.Clock:

- If \( C_1 \) is a value of Clock read before a task executes a delay_relative_statement with duration \( D \), and \( C_2 \) is a value of Clock read after the task resumes execution following that delay_statement, then \( C_2 - C_1 \geq D \).

- If \( C \) is a value of Clock read after a task resumes execution following a delay_until_statement with Real_Time.Clock value \( T \), then \( C \geq T \).

A simple delay_statement with a negative or zero value for the expiration time does not cause the calling task to be blocked; it is nevertheless a potentially blocking operation (see 9.5.1).

\{AI05-0004-1\} When a delay_statement appears in a delay_alternative of a timed_entry_call the selection of the entry call is attempted, regardless of the specified expiration time. When a delay_statement appears in a select_alternative,selective_accept_alternative, and a call is queued on one of the open entries, the selection of that entry call proceeds, regardless of the value of the delay expression.

Ramification: The effect of these requirements is that one has to always attempt a rendezvous, regardless of the value of the delay expression. This can be tested by issuing a timed_entry_call with an expiration time of zero, to an open entry.

Documentation Requirements

The implementation shall document the minimum value of the delay expression of a delay_relative_statement that causes the task to actually be blocked.

Documentation Requirement: The minimum value of the delay expression of a delay_relative_statement that causes a task to actually be blocked.

The implementation shall document the minimum difference between the value of the delay expression of a delay_until_statement and the value of Real_Time.Clock, that causes the task to actually be blocked.

This paragraph was deleted. Implementation defined: Implementation-defined aspects of delay_statements.

Documentation Requirement: The minimum difference between the value of the delay expression of a delay_until_statement and the value of Real_Time.Clock, that causes the task to actually be blocked.

Metrics

The implementation shall document the following metrics:

- An upper bound on the execution time, in processor clock cycles, of a delay_relative_statement whose requested value of the delay expression is less than or equal to zero.

- An upper bound on the execution time, in processor clock cycles, of a delay_until_statement whose requested value of the delay expression is less than or equal to the value of Real_Time.Clock at the time of executing the statement. Similarly, for Calendar.Clock.

\{AI12-0445-1\} An upper bound on the lateness of a delay_relative_statement, for a positive value of the delay expression, in a situation where the task has sufficient priority to preempt the processor as soon as it becomes ready, and can proceed without waitingdoes not need to wait for any other execution resources. The upper bound is expressed as a function of the value of the delay expression. The lateness is obtained by subtracting the value of the delay expression from the actual duration. The actual duration is measured from a point immediately before a task executes the delay_statement to a point immediately after the task resumes execution following this statement.

\{AI12-0445-1\} An upper bound on the lateness of a delay_until_statement, in a situation where the value of the requested expiration time is after the time the task begins executing the statement, the task has sufficient priority to preempt the processor as soon as it becomes ready, and it can
proceed without waiting does not need to wait for any other execution resources. The upper bound is expressed as a function of the difference between the requested expiration time and the clock value at the time the statement begins execution. The lateness of a delay_until_statement is obtained by subtracting the requested expiration time from the real time that the task resumes execution following this statement.

Documentation Requirement: The metrics for delay statements.

NOTE {AI95-00355-01} The execution time of a delay_statement that does not cause the task to be blocked (e.g., “delay 0.0;”) is of interest in situations where delays are used to achieve voluntary round-robin task dispatching among equal-priority tasks.

Wording Changes from Ada 83

The rules regarding a timed_entry_call with a very small positive Duration value, have been tightened to always require the check whether the rendezvous is immediately possible.

Wording Changes from Ada 95

{AI95-00355-01} The note about “voluntary round-robin”, while still true, has been deleted as potentially confusing as it is describing a different kind of round-robin than is defined by the round-robin dispatching policy.

D.10 Synchronous Task Control

{AI05-0299-1} [This subclause describes a language-defined private semaphore (suspension object), which can be used for two-stage suspend operations and as a simple building block for implementing higher-level queues.]

Static Semantics

The following language-defined package exists:

```ada
withpragma Preelaborate, Nonblocking, Global => in out synchronized
is
package Ada.Synchronous_Task_Control is
  type Suspension_Object is limited private;
  procedure Set_True(S : in out Suspension_Object);
  procedure Set_False(S : in out Suspension_Object);
  function Current_State(S : Suspension_Object) return Boolean;
  procedure Suspend_Until_True(S : in out Suspension_Object)
    with Nonblocking => False;
private
... -- not specified by the language
end Ada.Synchronous_Task_Control;
```

The type Suspension_Object is a by-reference type.

Implementation Note: {AI95-00318-02} The implementation can ensure this by, for example, making the full view an explicitly limited record type.

{AI05-0168-1} The following language-defined package exists:

```ada
with Ada.Real_Time;
package Ada.Synchronous_Task_Control.EDF with Nonblocking, Global => in out synchronized is
  procedure Suspend_Until_True_And_Set_Deadline
    (S  : in out Suspension_Object;
     TS : in Ada.Real_Time.Time_Span)
    with Nonblocking => False;
end Ada.Synchronous_Task_Control.EDF;
```

Dynamic Semantics

{AI95-00114-01} An object of the type Suspension_Object has two visible states: True and False. Upon initialization, its value is set to False.
Discussion: This object is assumed to be private to the declaring task, i.e. only that task will call Suspend_Until_True on this object, and the count of callers is at most one. Other tasks can, of course, change and query the state of this object.

\{AI95-00114-01\} The operations Set_True and Set_False are atomic with respect to each other and with respect to Suspend_Until_True; they set the state to True and False respectively.

Current_State returns the current state of the object.

\{AI95-00114-01\} The procedure Suspend_Until_True blocks the calling task until the state of the object S is True; at that point the task becomes ready and the state of the object becomes False.

\{AI12-0241-1\} Program_Error is raised upon calling Suspend_Until_True if another task is already waiting on that suspension object. Suspend_Until_True is a potentially blocking operation (see 9.5.1).

\{AI05-0168-1\} \{AI05-0269-1\} \{AI12-0241-1\} The procedure Suspend_Until_True_And_Set_Deadline blocks the calling task until the state of the object S is True; at that point the task becomes ready with a deadline of Ada.Real_Time.Clock + TS, and the state of the object becomes False. Program_Error is raised upon calling Suspend_Until_True_And_Set_Deadline if another task is already waiting on that suspension object. Suspend_Until_True_And_Set_Deadline is a potentially blocking operation.

Bounded (Run-Time) Errors

\{AI12-0171-1\} \{AI12-0439-1\} It is a bounded error for two or more tasks to call Suspend_Until_True on the same Suspension_Object concurrently. For each task, Program_Error can be raised, the task can proceed without suspending, or the task can suspend, potentially indefinitely. The state of the suspension object can end up either True or False.

Implementation Requirements

The implementation is required to allow the calling of Set_False and Set_True during any protected action, even one that has its ceiling priority in the Interrupt_Priority range.

\{AI05-0168-1\} More complex schemes, such as setting the deadline relative to when Set_True is called, can be programmed using a protected object.

Extensions to Ada 95

\{AI95-00362-01\} Synchronous_Task_Control is now Preelaborated, so it can be used in preelaborated units.

Extensions to Ada 2005

\{AI05-0168-1\} Child package Ada.Synchronous_Task_Control.EDF is new.

Wording Changes from Ada 2012

\{AI12-0171-1\} Correction: Clarified that Suspend_Until_True should only be called from a single task, and what happens if that is violated.

D.10.1 Synchronous Barriers

\{AI05-0174-1\} \{AI05-0299-1\} This subclause introduces a language-defined package to synchronously release a group of tasks after the number of blocked tasks reaches a specified count value.

Static Semantics

\{AI05-0174-1\} The following language-defined library package exists:

\{AI12-0241-1\} \{AI12-0302-1\} package Ada.Synchronous_Barrriers is

withpragma Preelaborate, Nonblocking, Global => in out synchronized
is (Synchronous_Barrriers);

1311 16 October 2023 Synchronous Task Control D.10
subtype Barrier Limit is Positive range 1 .. implementation-defined;

Implementation defined: The value of Barrier Limit'Last in Synchronous Barriers.

type Synchronous_Barrier (Release_Threshold : Barrier Limit) is limited private;

{AI12-0241-1} procedure Wait_For_Release (The_Barrier : in out Synchronous_Barrier;
Notified    : out Boolean)
with Nonblocking => False;

private
-- not specified by the language
end Ada.Synchronous_Barriers;

{AI05-0174-1} Type Synchronous Barrier needs finalization (see 7.6).

Dynamic Semantics

{AI05-0174-1} Each call to Wait_For_Release blocks the calling task until the number of blocked tasks associated with the Synchronous_Barrier object is equal to Release_Threshold, at which time all blocked tasks are released. Notified is set to True for one of the released tasks, and set to False for all other released tasks.

{AI05-0174-1} The mechanism for determining which task sets Notified to True is implementation defined.

{AI05-0174-1} Once all tasks have been released, a Synchronous_Barrier object may be reused to block another Release_Threshold number of tasks.

{AI05-0174-1} As the first step of the finalization of a Synchronous_Barrier, each blocked task is unblocked and Program_Error is raised at the place of the call to Wait_For_Release.

{AI05-0174-1} It is implementation defined whether an abnormal task which is waiting on a Synchronous_Barrier object is aborted immediately or aborted when the tasks waiting on the object are released.

Implementation defined: When an aborted task that is waiting on a Synchronous_Barrier is aborted.

This paragraph was deleted.

{AI05-0174-1} {AI12-0241-1} Wait_For_Release is a potentially blocking operation (see 9.5.1).

Bounded (Run-Time) Errors

{AI05-0174-1} It is a bounded error to call Wait_For_Release on a Synchronous_Barrier object after that object is finalized. If the error is detected, Program_Error is raised. Otherwise, the call proceeds normally, which may leave a task blocked forever.

Extensions to Ada 2005

{AI05-0174-1} The package Ada.Synchronous_Barriers is new.

D.11 Asynchronous Task Control

{AI05-0299-1} [This subclause introduces a language-defined package to do asynchronous suspend/resume on tasks. It uses a conceptual held priority value to represent the task's held state.]

Static Semantics

The following language-defined library package exists:
package Ada.Asynchronous_Task_Control is
withpragma Preelaborate, Nonblocking, Global => in out synchronized
is
procedure Hold(T : in Ada.Task_Identification.Task_Id);
procedure Continue(T : in Ada.Task_Identification.Task_Id);
function Is_Held(T : Ada.Task_Identification.Task_Id)
return Boolean;
end Ada.Asynchronous_Task_Control;

Dynamic Semantics

After the Hold operation has been applied to a task, the task becomes held. For each processor there is a conceptual idle task, which is always ready. The base priority of the idle task is below System.Any_Priority'First. The held priority is a constant of the type Integer whose value is below the base priority of the idle task.

Discussion: The held state should not be confused with the blocked state as defined in 9.2; the task is still ready.

For any priority below System.Any_Priority'First, the task dispatching policy is FIFO Within Priorities.

To be honest: This applies even if a Task Dispatching Policy specifies the policy for all of the priorities of the partition.

Ramification: A task at the held priority never runs, so it is not necessary to implement FIFO Within Priorities for systems that have only one policy (such as EDF Across Priorities).

The Hold operation sets the state of T to held. For a held task, the active priority is reevaluated as if the base priority of the task were the held priority; the task's own base priority does not constitute an inheritance source (see D.1), and the value of the held priority is defined to be such a source instead.

Ramification: For example, if T is currently inheriting priorities from other sources (e.g. it is executing in a protected action), its active priority does not change, and it continues to execute until it leaves the protected action.

The Continue operation resets the state of T to not-held; its active priority is then reevaluated as determined by the task dispatching policy associated with its base priority described in D.1.

The Is_Held function returns True if and only if T is in the held state.

Discussion: Note that the state of T can be changed immediately after Is_Held returns.

As part of these operations, a check is made that the task identified by T is not terminated. Tasking_Error is raised if the check fails. Program_Error is raised if the value of T is Null_Task_Id.

Erroneous Execution

If any operation in this package is called with a parameter T that specifies a task object that no longer exists, the execution of the program is erroneous.

Implementation Permissions

An implementation may omit need not support for Asynchronous_Task_Control if it is infeasible to support it in the target environment.

Reason: A direct implementation of the Asynchronous_Task_Control semantics using priorities is not necessarily efficient enough. Thus, we envision implementations that use some other mechanism to set the “held” state. If there is no other such mechanism, support for Asynchronous_Task_Control might be infeasible, because an implementation in terms of priority would require one idle task per processor. On some systems, programs are not supposed to know how many processors are available, so creating enough idle tasks would be problematic.

NOTE 1 It is a consequence of the priority rules that held tasks cannot be dispatched on any processor in a partition (unless they are inheriting priorities) since their priorities are defined to be below the priority of any idle task.
NOTE 2   The effect of calling Get_Priority and Set_Priority on a Held task is the same as on any other task.

NOTE 3   Calling Hold on a held task or Continue on a non-held task has no effect.

NOTE 4   The rules affecting queuing are derived from the above rules, in addition to the normal priority rules:

- When a held task is on the ready queue, its priority is so low as to never reach the top of the queue as long as there are other tasks on that queue.
- If a task is executing in a protected action, inside a rendezvous, or is inheriting priorities from other sources (e.g. when activated), it continues to execute until it is no longer executing the corresponding construct.
- If a task becomes held while waiting (as a caller) for a rendezvous to complete, the active priority of the accepting task is not affected.
- If a task becomes held while waiting in a selective_accept, and an entry call is issued to one of the open entries, the corresponding accept_alternative_accept_body executes. When the rendezvous completes, the active priority of the accepting task is lowered to the held priority (unless it is still inheriting from other sources), and the task does not execute until another Continue.
- The same holds if the held task is the only task on a protected entry queue whose barrier becomes open. The corresponding entry body executes.

Extensions to Ada 95

{AI95-00362-01}  Asynchronous Task Control is now Preelaborated, so it can be used in preelaborated units.

Wording Changes from Ada 95

{8652/0077}  {AI95-00111-01}  Corrigendum: Corrected to eliminate the use of the undefined term “accept body”.

{AI95-00357-01}  The description of held tasks was changed to reflect that the calculation of active priorities depends on the dispatching policy of the base priority. Thus, the policy of the held priority was specified in order to avoid surprises (especially when using the EDF policy).

D.12 Other Optimizations and Determinism Rules

{AI05-0299-1}  [This subclause describes various requirements for improving the response and determinism in a real-time system.]

Implementation Requirements

1 If the implementation blocks interrupts (see C.3) not as a result of direct user action (e.g. an execution of a protected action) there shall be an upper bound on the duration of this blocking.

2. a. Ramification: The implementation shall not allow itself to be interrupted when it is in a state where it is unable to support all the language-defined operations permitted in the execution of interrupt handlers. (see 9.5.1).

3 The implementation shall recognize entry-less protected types. The overhead of acquiring the execution resource of an object of such a type (see 9.5.1) shall be minimized. In particular, there should not be any overhead due to evaluating entry_barrier conditions.

3.a. Implementation Note: Ideally the overhead should just be a spin-lock.

4 Unchecked_Deallocation shall be supported for terminated tasks that are designated by access types, and shall have the effect of releasing all the storage associated with the task. This includes any run-time system or heap storage that has been implicitly allocated for the task by the implementation.

Documentation Requirements

5 The implementation shall document the upper bound on the duration of interrupt blocking caused by the implementation. If this is different for different interrupts or interrupt priority levels, it should be documented for each case.

5.a/2 This paragraph was deleted. Implementation defined: The upper bound on the duration of interrupt blocking caused by the implementation.

5.b/2 Documentation Requirement: The upper bound on the duration of interrupt blocking caused by the implementation.
The implementation shall document the following metric:

- The overhead associated with obtaining a mutual-exclusive access to an entry-less protected object. This shall be measured in the following way:

  For a protected object of the form:
  
  ```ada
  protected Lock is
    procedure Set;
    function Read return Boolean;
  private
    Flag : Boolean := False;
  end Lock;
  
  protected body Lock is
    procedure Set is
      begin
        Flag := True;
      end Set;
    function Read return Boolean
      begin
        return Flag;
      end Read;
  end Lock;
  
  The execution time, in processor clock cycles, of a call to Set. This shall be measured between the point just before issuing the call, and the point just after the call completes. The function Read shall be called later to verify that Set was indeed called (and not optimized away). The calling task shall have sufficiently high priority as to not be preempted during the measurement period. The protected object shall have sufficiently high ceiling priority to allow the task to call Set.

  For a multiprocessor, if supported, the metric shall be reported for the case where no contention (on the execution resource) exists [from tasks executing on other processors].

  **Documentation Requirement:** The metrics for entry-less protected objects.

---

**D.13 The Ravenscar and Jorvik Profiles**

Paragraphs 2 and 3 were moved to 13.12, “Pragma Restrictions and Pragma Profile”.

**Syntax**

The form of a pragma Profile is as follows:

```
pragma Profile (profile_identifier, profile pragma argument association);
```

**Legality Rules**

The `profile_identifier` Ravenscar and `profile_identifier` Jorvik arcis a usage profile (see 13.12). For usage profile Ravenscar and Jorvik, there shall be noshall be the name of a run-time profile. The semantics of any `profile pragma argument - associations` are defined by the run-time profile specified by the `profile_identifier`.

**Static Semantics**

The usage profile Ravenscar is equivalent to the following set of pragmas: A profile is equivalent to the set of configuration pragmas that is defined for each run-time profile.
The Ravenscar profile is named for the location of the meeting that defined its initial version. The name is now in widespread use, so we stick with existing practice, rather than using a more descriptive name.

The Jorvik profile is named for the city of York, UK, near where the Ravenscar profile was created. "Jorvik" (pronounced "Yorvick") was the Viking name for York.

The usage profile Jorvik is equivalent to the following set of pragmas:

```ada
pragma Task_Dispatching_Policy (FIFO_Within_Priorities);
pragma Locking_Policy (Ceiling_Locking);
pragma Detect_Blocking;
pragma Restrictions (No Abort Statements,
                      No Dynamic Attachment,
                      No Dynamic CPU Assignment,
                      No dynamic Priorities,
                      No Implicit Heap Allocations,
                      No Local Protected Objects,
                      No Local Timing Events,
                      No Protected Type Allocators,
                      No Relative Delay,
                      No Requeue Statements,
                      No Select Statements,
                      No Specific Termination Handlers,
                      No Task Allocators,
                      No Task Hierarchy,
                      No Task Termination,
                      Simple Barriers,
                      Max Entry Queue Length => 1,
                      Max Protected Entries => 1,
                      Max Task Entries => 0,
                      No Dependence => Ada.Asynchronous_Task_Control,
                      No Dependence => Ada.Calendar,
                      No Dependence => Ada.Execution_Time.Group_Budgets,
                      No Dependence => Ada.Execution_Time.Timers,
                      No Dependence => Ada.Synchronous_Barriers,
                      No Dependence => Ada.Task_Attributes,
                      No Dependence => System.Multiprocessors.Dispatching_Domains);
```

Discussion: The Jorvik profile removes a number of restrictions from the Ravenscar profile to allow additional applications to benefit from predictability and low overhead. Specifically, the following restrictions are removed:

No_Implicit_Heap_Allocations
No_Relative_Delay
Max_Entry_Queue_Length => 1
Max_Protected_Entries => 1
No_Dependence => Ada.Calendar
No_Dependence => Ada.Synchronous_Barriers

Jorvik also replaces restriction Simple_Barriers with Pure_Barriers (a weaker requirement than Simple_Barriers).

Post-Compilation Rules

\\{AI95-00249-01} \{AI05-0246-1\} A pragma Profile is a configuration pragma. There may be more than one pragma Profile for a partition.

Paragraph 7 and 8 were deleted.

Implementation Requirements

\\{AI05-0171-1} \{AI05-0229-1\} \{AI12-0055-1\} A task shall only be on the ready queues of one processor, and the processor to which a task belongs shall be defined statically. Whenever a task running on a processor reaches a task dispatching point, it goes back to the ready queues of the same processor. A task with a CPU value of Not_A_Specific_CPU will execute on an implementation defined processor. [A task without a CPU aspect will activate and execute on the same processor as its activating task.]

Proof: The processor of a task without a CPU aspect is defined in D.16.

Implementation Advice

\\{AI05-0171-1} \{AI12-0291-1\} On a multiprocessor system, an implementation should support a fully partitioned approach if one of these profiles is specified. Each processor should have separate and disjoint ready queues.

Implementation Advice: On a multiprocessor system, each processor should have a separate and disjoint ready queue.

\text{NOTE 1} \ \{AI95-00249-01\} \{AI05-0246-1\} \{AI12-0055-1\} \text{For the Ravenscar profile, the effect of the restriction Max_Entry_Queue_Length => 1 applies only to protected entry queues due to the accompanying restriction of Max_Task_Entries => 0. The restriction Max_Entry_Queue_Length is not applied by the Jorvik profile.}

\text{NOTE 2} \ \{AI12-0055-1\} \{AI12-0291-1\} \text{When the Ravenscar or Jorvik profile is in effect (via the effect of the No Dynamic CPU Assignment restriction), all of the tasks in the partition will execute on a single CPU unless the programmer explicitly uses aspect CPU to specify the CPU assignments for tasks. The use of multiple CPUs requires care, as many guarantees of single CPU scheduling no longer apply.}

\text{NOTE 3} \ \{AI12-0055-1\} \{AI12-0291-1\} \text{It is not recommended to specify the CPU of a task to be Not_A_Specific_CPU when the Ravenscar or Jorvik profile is in effect. How a partition executes strongly depends on the assignment of tasks to CPUs.}

\text{NOTE 4} \ \{AI12-0291-1\} Any unit that meets the requirements of the Ravenscar profile also meets the requirements of the Jorvik profile.

Extensions to Ada 95

\\{AI95-00249-01} \{AI05-0246-1\} The Ravenscar profile is new; it was moved here by Ada 2012.

Wording Changes from Ada 2005

\\{AI05-0171-1\} How Ravenscar behaves on a multiprocessor system is now defined.

Incompatibilities With Ada 2012

\\{AI05-0073-1\} \textbf{Corrigendum:} The Ravenscar profile no longer allows the use of package Synchronous_Barriers, as this package violates the fundamental Ravenscar requirement that each waiting point can only block (and release) a single task. This is incompatible with the published Ada 2012 standard, but it is unlikely that any existing Ravenscar runtime ever usefully supported barriers.

\\{AI05-0055-1\} \textbf{Corrigendum:} The Ravenscar profile (via the effect of the new restriction No_Dynamic_CPU_Assignment) no longer allows setting the CPU aspect of a task to a non-static value. While this...
was allowed, an implementation would have had to come up with a creative interpretation of the Ada 2012 requirement to define the association of tasks to processors statically. As such, the new check is more likely to catch bugs than break a working program.

**Extensions to Ada 2012**

The Jorvik profile is new.

### D.14 Execution Time

This subclause describes a language-defined package to measure execution time.

**Static Semantics**

The following language-defined library package exists:

```ada
package Ada.Execution_Time
    with Nonblocking, Global => in out synchronized is
    type CPU_Time is private;
    CPU_Time_First : constant CPU_Time;
    CPU_Time_Last : constant CPU_Time;
    CPU_Time_Unit : constant := implementation-defined-real-number;
    CPU_Tick : constant Time_Span;

    function "+" (Left : CPU_Time; Right : Time_Span) return CPU_Time;
    function "+" (Left : Time_Span; Right : CPU_Time) return CPU_Time;
    function "-" (Left : CPU_Time; Right : Time_Span) return CPU_Time;
    function "-" (Left : CPU_Time; Right : CPU_Time) return Time_Span;
    function "<" (Left, Right : CPU_Time) return Boolean;
    function "<=" (Left, Right : CPU_Time) return Boolean;
    function ">" (Left, Right : CPU_Time) return Boolean;
    function ">=" (Left, Right : CPU_Time) return Boolean;
    procedure Split (T : CPU_Time; SC : out Seconds_Count; TS : out Time_Span);

    function Time_Of (SC : Seconds_Count; TS : Time_Span := Time_Span_Zero) return CPU_Time;

    Interrupt_Clocks_Supported : constant Boolean := implementation-defined;
    Separate_Interrupt_Clocks_Supported : constant Boolean := implementation-defined;
    function Clock_For_Interrupts return CPU_Time;

private
    -- not specified by the language
end Ada.Execution_Time;
```

The execution time or CPU time of a given task is defined as the time spent by the system executing that task, including the time spent executing run-time or system services on its behalf. The mechanism used to measure execution time is implementation defined. The Boolean constant Interrupt_Clocks_Supported is set to True if the implementation separately accounts for the execution time of interrupt handlers. If it is set to False it is implementation defined which task, if any, is charged the execution time that is consumed by interrupt handlers. The Boolean constant Separate_Interrupt_Clocks_Supported is set to True if the implementation separately accounts.
for the execution time of individual interrupt handlers (see D.14.3) and run-time services on behalf of the system.

Discussion: The implementation-defined properties above and of the values declared in the package are repeated in Documentation Requirements, so we don't mark them as implementation-defined.

\{AI95-00307-01\} The type CPU_Time represents the execution time of a task. The set of values of this type corresponds one-to-one with an implementation-defined range of mathematical integers.

\{AI95-00307-01\} The CPU_Time value I represents the half-open execution-time interval that starts with I*CPU_Time_Unit and is limited by (I+1)*CPU_Time_Unit, where CPU_Time_Unit is an implementation-defined real number. For each task, the execution time value is set to zero at the creation of the task.

Ramification: Since it is implementation-defined which task is charged execution time for system services, the execution time value may become nonzero even before the start of the activation of the task.

\{AI95-00307-01\} CPU_Time_First and CPU_Time_Last are the smallest and largest values of the CPU_Time type, respectively.

\{AI05-0170-1\} The execution time value for the function Clock_For_Interrupts is initialized to zero.

Dynamic Semantics

\{AI95-00307-01\} CPU_Time_Unit is the smallest amount of execution time representable by the CPU_Time type; it is expressed in seconds. A CPU clock tick is an execution time interval during which the clock value (as observed by calling the Clock function) remains constant. CPU_Tick is the average length of such intervals.

\{AI95-00307-01\} The effects of the operators on CPU_Time and Time_Span are as for the operators defined for integer types.

\{AI95-00307-01\} The function Clock returns the current execution time of the task identified by T; Tasking_Error is raised if that task has terminated; Program_Error is raised if the value of T is Task_Identification.Null_Task_Id.

\{AI95-00307-01\} The effects of the Split and Time_Of operations are defined as follows, treating values of type CPU_Time, Time_Span, and Seconds_Count as mathematical integers. The effect of Split (T, SC, TS) is to set SC and TS to values such that T*CPU_Time_Unit = SC*1.0 + TS*CPU_Time_Unit, and 0.0 <= TS*CPU_Time_Unit < 1.0. The value returned by Time_Of(SC,TS) is the execution-time value T such that T*CPU_Time_Unit=SC*1.0 + TS*CPU_Time_Unit.

\{AI05-0170-1\} The function Clock_For_Interrupts returns the total cumulative time spent executing within all interrupt handlers. This time is not allocated to any task execution time clock. If Interrupt_Clocks_Supported is set to False the function raises Program_Error.

Erroneous Execution

\{AI95-00307-01\} For a call of Clock, if the task identified by T no longer exists, the execution of the program is erroneous.

Implementation Requirements

\{AI95-00307-01\} The range of CPU_Time values shall be sufficient to uniquely represent the range of execution times from the task start-up to 50 years of execution time later. CPU_Tick shall be no greater than 1 millisecond.
Documentation Requirements

The implementation shall document the values of CPU_Time_First, CPU_Time_Last, CPU_Time_Unit, and CPU_Tick.

**Documentation Requirement:** The values of CPU_Time_First, CPU_Time_Last, CPU_Time_Unit, and CPU_Tick of package Execution_Time.

The implementation shall document the properties of the underlying mechanism used to measure execution times, such as the range of values supported and any relevant aspects of the underlying hardware or operating system facilities used.

**Documentation Requirement:** The properties of the mechanism used to implement package Execution_Time, including the values of the constants defined in the package.

Metrics

The implementation shall document the following metrics:

- An upper bound on the execution-time duration of a clock tick. This is a value D such that if t₁ and t₂ are any execution times of a given task such that t₁ < t₂ and \( \text{Clock}_t = \text{Clock}_{t₂} \), then \( t₂ - t₁ <= D \).
- An upper bound on the size of a clock jump. A clock jump is the difference between two successive distinct values of an execution-time clock (as observed by calling the Clock function with the same Task_Id).
- An upper bound on the execution time of a call to the Clock function, in processor clock cycles.
- Upper bounds on the execution times of the operators of the type CPU_Time, in processor clock cycles.

**Documentation Requirement:** The metrics for execution time.

Implementation Permissions

Implementations targeted to machines with word size smaller than 32 bits may omit support for the full range and granularity of the CPU_Time type.

Implementation Advice

When appropriate, implementations should provide configuration mechanisms to change the value of CPU_Tick.

**Implementation Advice:** When appropriate, implementations should provide configuration mechanisms to change the value of Execution_Time.CPU_Tick.

Extensions to Ada 95

The package Execution_Time is new.

Incompatibilities With Ada 2005

Function Clock_For_Interrupts, and constants Interrupt_Clocks_Supported and Separate_Interrupt_Clocks_Supported are added to Execution_Time. If Execution_Time is referenced in a use_clause, and an entity \( E \) with a defining identifier of one of the added entities is defined in a package that is also referenced in a use_clause, the entity \( E \) may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

Wording Changes from Ada 2005

If Interrupt_Clocks_Supported is True, it is now possible to determine the execution time of interrupt handlers. This is not an inconsistency, as not charging any task for such time was a legitimate implementation for Ada 2005.
D.14.1 Execution Time Timers

This subclause describes a language-defined package that provides a facility for calling a handler when a task has used a defined amount of CPU time.

Static Semantics

The following language-defined library package exists:

```ada
package Ada.Execution_Time.Timers
  with Nonblocking, Global => in out synchronized is
  type Timer (T : not null access constant Ada.Task_Identification.Task_Id) is
    tagged limited private;
  type Timer_Handler is
    access protected procedure (TM : in out Timer)
      with Nonblocking => False;
  Min_Handler_Ceiling : constant System.Any_Priority :=
    implementation-defined;
  procedure Set_Handler (TM      : in out Timer;
                          In_Time : in Time_Span;
                          Handler : in Timer_Handler);
  procedure Set_Handler (TM      : in out Timer;
                          At_Time : in CPU_Time;
                          Handler : in Timer_Handler);
  function Current_Handler (TM : Timer) return Timer_Handler;
  procedure Cancel_Handler (TM        : in out Timer;
                           Cancelled : out Boolean);
  function Time_Remaining (TM : Timer) return Time_Span;
  Timer_Resource_Error : exception;
private
  ... -- not specified by the language
end Ada.Execution_Time.Timers;
```

The type Timer represents an execution-time event for a single task and is capable of detecting execution-time overruns. The access discriminant T identifies the task concerned. The type Timer needs finalization (see 7.6).

An object of type Timer is said to be set if it is associated with a nonnull value of type Timer_Handler and cleared otherwise. All Timer objects are initially cleared.

The type Timer_Handler identifies a protected procedure to be executed by the implementation when the timer expires. Such a protected procedure is called a handler.

Discussion: Type Timer is tagged. This makes it possible to share a handler between several events. In simple cases, access can be used to compare the parameter with a specific timer object (this works because a tagged type is a by-reference type). In more complex cases, a type extension of type Timer can be declared; a double type conversion can be used to access the extension data. An example of how this can be done can be found for the similar type Timing_Event, see D.15.

Dynamic Semantics

When a Timer object is created, or upon the first call of a Set_Handler procedure with the timer as parameter, the resources required to operate an execution-time timer based on the associated execution-time clock are allocated and initialized. If this operation would exceed the available resources, Timer_Resource_Error is raised.
The procedures Set_Handler associate the handler Handler with the timer TM; if Handler is null, the timer is cleared; otherwise, it is set. The first procedure Set_Handler loads the timer TM with an interval specified by the Time_Span parameter. In this mode, the timer TM expires when the execution time of the task identified by TM.T.all has increased by In_Time; if In_Time is less than or equal to zero, the timer expires immediately. The second procedure Set_Handler loads the timer TM with the absolute value specified by At_Time. In this mode, the timer TM expires when the execution time of the task identified by TM.T.all reaches At_Time; if the value of At_Time has already been reached when Set_Handler is called, the timer expires immediately.

Implementation Note: Since an access-to-constant can designate a variable, the Task_Id value designated by the discriminant of a Timer object can be changed after the object is created. Thus, an implementation cannot use the value of the Task_Id other than where this Reference Manual specifies. For instance, the Task_Id should be read when the timer is set, but it should not be used when the timer expires (as it may designate a different task at that point).

A call of a procedure Set_Handler for a timer that is already set replaces the handler and the (absolute or relative) execution time; if Handler is not null, the timer remains set.

When a timer expires, the associated handler is executed, passing the timer as parameter. The initial action of the execution of the handler is to clear the event.

The function Current_Handler returns the handler associated with the timer TM if that timer is set; otherwise, it returns null.

The procedure Cancel_Handler clears the timer if it is set. Cancelled is assigned True if the timer was set prior to it being cleared; otherwise, it is assigned False.

The function Time_Remaining returns the execution time interval that remains until the timer TM would expire, if that timer is set; otherwise, it returns Time_Span_Zero.

The constant Min_Handler_Ceiling is the minimum ceiling priority required for a protected object with a handler to ensure that no ceiling violation will occur when that handler is invoked.

As part of the finalization of an object of type Timer, the timer is cleared.

For all the subprograms defined in this package, Tasking_Error is raised if the task identified by TM.T.all has terminated, and Program_Error is raised if the value of TM.T.all is Task_Identification.Null_Task_Id.

An exception propagated from a handler invoked as part of the expiration of a timer has no effect.

Erroneous Execution

For a call of any of the subprograms defined in this package, if the task identified by TM.T.all no longer exists, the execution of the program is erroneous.

Implementation Requirements

For a given Timer object, the implementation shall perform the operations declared in this package atomically with respect to any of these operations on the same Timer object. The replacement of a handler by a call of Set_Handler shall be performed atomically with respect to the execution of the handler.

Reason: This prevents various race conditions. In particular it ensures that if an event occurs when Set_Handler is changing the handler then either the new or old handler is executed in response to the appropriate event. It is never possible for a new handler to be executed in response to an old event.

When an object of type Timer is finalized, the system resources used by the timer shall be deallocated.
Implementation Permissions

{AI95-00307-01} {AI05-0264-1} Implementations may limit the number of timers that can be defined for each task. If this limit is exceeded, then Timer_Resource_Error is raised.

NOTE {AI95-00307-01} A Timer_Handler can be associated with several Timer objects.

Extensions to Ada 95

{AI95-00307-01} The package Execution_Time.Timers is new.

D.14.2 Group Execution Time Budgets

{AI95-00354-01} {AI05-0299-1} This subclause describes a language-defined package to assign execution time budgets to groups of tasks.

Static Semantics

{AI95-00354-01} The following language-defined library package exists:

{AI05-0169-1} {AI12-0302-1} with System;

package Ada.Execution_Time.Group_Budgets with Nonblocking, Global => in out synchronized is

{AI12-0241-1} {AI12-0302-1} type Group_Budget(CPU : System.Multiprocessors.CPU := System.Multiprocessors.CPU'First) is tagged limited private;

{AI12-0241-1} type Group_Budget_Handler is access
protected procedure (GB : in out Group_Budget)
with Nonblocking => False;

{AI12-0241-1} type Task_Array is array (Positive range <>) of Ada.Task_Identification.Task_Id;

Min_Handler_Ceiling : constant System.Any_Priority := implementation-defined;

procedure Add_Task (GB : in out Group_Budget; T  : in Ada.Task_Identification.Task_Id);
procedure Remove_Task (GB: in out Group_Budget; T  : in Ada.Task_Identification.Task_Id);
function Is_Member (GB : Group_Budget; T : Ada.Task_Identification.Task_Id) return Boolean;
function Is_A_Group_Member (T : Ada.Task_Identification.Task_Id) return Boolean;
function Members (GB : Group_Budget) return Task_Array;
function Budget_Has_Expired (GB : Group_Budget) return Boolean;
function Budget_Remaining (GB : Group_Budget) return Time_Span;
procedure Set_Handler (GB      : in out Group_Budget; Handler : in Group_Budget_Handler);
procedure Replenish (GB : in out Group_Budget; To : in Time_Span);
procedure Add (GB : in out Group_Budget; Interval : in Time_Span);
function Handle (GB : Group_Budget) return Task_Array;
function Cancel_Handler (GB : in out Group_Budget;
 Cancelled : out Boolean);

Group_Budget_Error : exception

private
   -- not specified by the language
end Ada.Execution_Time.Group_Budgets;
The type Group_Budget represents an execution time budget to be used by a group of tasks. The type Group_Budget needs finalization (see 7.6). A task can belong to at most one group. Tasks of any priority can be added to a group.

An object of type Group_Budget has an associated nonnegative value of type Time_Span known as its budget, which is initially Time_Span_Zero. The type Group_Budget_Handler identifies a protected procedure to be executed by the implementation when the budget is exhausted, that is, reaches zero. Such a protected procedure is called a handler.

An object of type Group_Budget also includes a handler, which is a value of type Group_Budget_Handler. The handler of the object is said to be set if it is not null and cleared otherwise. The handler of all Group_Budget objects is initially cleared.

Discussion: Type Group_Budget is tagged. This makes it possible to share a handler between several events. In simple cases, 'Access can be used to compare the parameter with a specific group budget object (this works because a tagged type is a by-reference type). In more complex cases, a type extension of type Group_Budget can be declared; a double type conversion can be used to access the extension data. An example of how this can be done can be found for the similar type Timing_Event, see D.15.

Dynamic Semantics

The procedure Add_Task adds the task identified by T to the group GB; if that task is already a member of some other group, Group_Budget_Error is raised.

The procedure Remove_Task removes the task identified by T from the group GB; if that task is not a member of the group GB, Group_Budget_Error is raised. After successful execution of this procedure, the task is no longer a member of any group.

The function Is_Member returns True if the task identified by T is a member of the group GB; otherwise, it returns False.

The function Is_A_Group_Member returns True if the task identified by T is a member of some group; otherwise, it returns False.

The function Members returns an array of values of type Task_Identification.Task_Id identifying the members of the group GB. The order of the components of the array is unspecified.

The procedure Replenish loads the group budget GB with To as the Time_Span value. The exception Group_Budget_Error is raised if the Time_Span value To is nonpositive. Any execution on CPU of any member of the group of tasks results in the budget counting down, unless exhausted. When the budget becomes exhausted (reaches Time_Span_Zero), the associated handler is executed if the handler of group budget GB is set. Nevertheless, the tasks continue to execute.

The procedure Add modifies the budget of the group GB. A positive value for Interval increases the budget. A negative value for Interval reduces the budget, but never below Time_Span_Zero. A zero value for Interval has no effect. A call of procedure Add that results in the value of the budget going to Time_Span_Zero causes the associated handler to be executed if the handler of the group budget GB is set.

The function Budget_Has_Expired returns True if the budget of group GB is exhausted (equal to Time_Span_Zero); otherwise, it returns False.

The function Budget_Remaining returns the remaining budget for the group GB. If the budget is exhausted it returns Time_Span_Zero. This is the minimum value for a budget.

The procedure Set_Handler associates the handler Handler with the Group_Budget GB; if Handler is null, the handler of Group_Budget is cleared, otherwise, it is set.
A call of Set_Handler for a Group_Budget that already has a handler set replaces the handler; if Handler is not null, the handler for Group_Budget remains set.

The function Current_Handler returns the handler associated with the group budget GB if the handler for that group budget is set; otherwise, it returns null.

The procedure Cancel_Handler clears the handler for the group budget if it is set. Cancelled is assigned True if the handler for the group budget was set prior to it being cleared; otherwise, it is assigned False.

The constant Min_Handler_Ceiling is the minimum ceiling priority required for a protected object with a handler to ensure that no ceiling violation will occur when that handler is invoked.

The precision of the accounting of task execution time to a Group_Budget is the same as that defined for execution-time clocks from the parent package.

As part of the finalization of an object of type Group_Budget all member tasks are removed from the group identified by that object.

If a task is a member of a Group_Budget when it terminates, then as part of the finalization of the task it is removed from the group.

For all the operations defined in this package, Tasking_Error is raised if the task identified by T has terminated, and Program_Error is raised if the value of T is Task_Identification.Null_Task_Id.

An exception propagated from a handler invoked when the budget of a group of tasks becomes exhausted has no effect.

Erroneous Execution

For a call of any of the subprograms defined in this package, if the task identified by T no longer exists, the execution of the program is erroneous.

Implementation Requirements

For a given Group_Budget object, the implementation shall perform the operations declared in this package atomically with respect to any of these operations on the same Group_Budget object. The replacement of a handler, by a call of Set_Handler, shall be performed atomically with respect to the execution of the handler.

Reason: This prevents various race conditions. In particular it ensures that if the budget is exhausted when Set_Handler is changing the handler then either the new or old handler is executed and the exhausting event is not lost.

NOTE 1: Clearing or setting of the handler of a group budget does not change the current value of the budget. Exhaustion or loading of a budget does not change whether the handler of the group budget is set or cleared.

NOTE 2: A Group_Budget_Handler can be associated with several Group_Budget objects.

Extensions to Ada 95

The package Execution_Time.Group_Budgets is new.

Inconsistencies With Ada 2005

A Group_Budget is now defined to work on a single processor. If an implementation managed to make this package work for programs running on a multiprocessor system, and a program depends on that fact, it could fail when ported to Ada 2012. We believe it is unlikely that such an implementation exists because of the difficulty of signalling other processors when the time reaches zero; in any case, depending on such an implementation is not portable.
D.14.3 **Execution Time of Interrupt Handlers**

This subclause describes a language-defined package to measure the execution time of interrupt handlers.

### Static Semantics

The following language-defined library package exists:

```ada
package Ada.Interrupts;

    function Clock (Interrupt : Ada.Interrupts.Interrupt_Id) return CPU_Time;
    function Supported (Interrupt : Ada.Interrupts.Interrupt_Id) return Boolean;

end Ada.Interrupts;
```

The execution time or CPU time of a given interrupt Interrupt is defined as the time spent by the system executing interrupt handlers identified by Interrupt, including the time spent executing run-time or system services on its behalf. The mechanism used to measure execution time is implementation defined. Time spent executing interrupt handlers is distinct from time spent executing any task.

**Discussion:** The implementation-defined mechanism here is the same as that covered by the Documentation Requirements of D.14, so we don't repeat that requirement here.

For each interrupt, the execution time value is initially set to zero.

### Dynamic Semantics

The function Clock returns the current cumulative execution time of the interrupt identified by Interrupt. If Separate Interrupt Clocks Supported is set to False the function raises Program_Error.

The function Supported returns True if the implementation is monitoring the execution time of the interrupt identified byInterrupt; otherwise, it returns False. For any Interrupt_Id Interrupt for which Supported(Interrupt) returns False, the function Clock(Interrupt) will return a value equal to Ada.Execution_Time.Time_Of(0).

### Extensions to Ada 2005

The package Execution_Time.Interrupts is new.

---

D.15 **Timing Events**

This subclause describes a language-defined package to allow user-defined protected procedures to be executed at a specified time without the use of a task or a delay statement.

### Static Semantics

The following language-defined library package exists:

```ada
package Ada.Real_Time.Timing_Events

    type Timing_Event is tagged limited private;
    type Timing_Event_Handler is access protected procedure (Event : in out Timing_Event) with Nonblocking => False;

end Ada.Real_Time.Timing_Events;
```

---
The type `Timing_Event` represents a time in the future when an event is to occur. The type `Timing_Event` needs finalization (see 7.6).

An object of type `Timing_Event` is said to be `set` if it is associated with a nonnull value of type `Timing_Event_Handler` and `cleared` otherwise. All `Timing_Event` objects are initially cleared.

The type `Timing_Event_Handler` identifies a protected procedure to be executed by the implementation when the timing event occurs. Such a protected procedure is called a `handler`.

**Discussion:** Type `Timing_Event` is tagged. This makes it possible to share a handler between several events. In simple cases, `Access` can be used to compare the parameter with a specific timing event object (this works because a tagged type is a by-reference type). In more complex cases, a type extension of type `Timing_Event` can be declared; a double type conversion can be used to access the extension data. For example:

```ada
type Toaster_Timing_Event is new Timing_Event with record
   Slot : Natural;
end record;

protected body Toaster is
   procedure Timer (Event : in out Timing_Event)
      begin
         Pop_Up_Toast (Toaster_Timing_Event(Timing_Event'Class(Event)).Slot);
      end Timer;
   ...
end Toaster;
```

The extra conversion to the class-wide type is necessary to make the conversions legal. While this usage is clearly ugly, we think that the need for this sort of usage will be rare, so we can live with it. It's certainly better than having no way to associate data with an event.

**Dynamic Semantics**

The procedures `Set_Handler` associate the handler `Handler` with the event `Event`; if `Handler` is `null`, the event is cleared; otherwise, it is set. The first procedure `Set_Handler` sets the execution time for the event to be `At_Time`. The second procedure `Set_Handler` sets the execution time for the event to be `Real_Time.Clock + In_Time`.

A call of a procedure `Set_Handler` for an event that is already set replaces the handler and the time of execution; if `Handler` is not `null`, the event remains set.

As soon as possible after the time set for the event, the handler is executed, passing the event as parameter. The handler is only executed if the timing event is in the set state at the time of execution. The initial action of the execution of the handler is to clear the event.

**Reason:** The second sentence of this paragraph is because of a potential race condition. The time might expire and yet before the handler is executed, some task could call `Cancel_Handler` (or equivalently call `Set_Handler` with a `null` parameter) and thus clear the handler.
If the Ceiling Locking policy (see D.3) is in effect when a procedure Set_Handler is called, a check is made that the ceiling priority of Handler.all is Interrupt Priority'Last. If the check fails, Program_Error is raised.

If a procedure Set_Handler is called with zero or negative In_Time or with At_Time indicating a time in the past, then the handler is executed as soon as possible after the completion of immediately by the task executing the call of Set_Handler. The timing event Event is cleared.

Ramification: The handler will still be executed. Under no circumstances is a scheduled call of a handler lost.

Discussion: We say “as soon as possible” so that we do not deadlock if we are executing the handler when Set_Handler is called. In that case, the current invocation of the handler must complete before the new handler can start executing.

The function Current_Handler returns the handler associated with the event Event if that event is set; otherwise, it returns null.

The procedure Cancel_Handler clears the event if it is set. Cancelled is assigned True if the event was set prior to it being cleared; otherwise, it is assigned False.

The function Time_Of_Event returns the time of the event if the event is set; otherwise, it returns Real_Time.Time_First.

As part of the finalization of an object of type Timing_Event, the Timing_Event is cleared.

Implementation Note: This is the only finalization defined by the language that has a visible effect; but an implementation may have other finalization that it needs to perform. Implementations need to ensure that the event is cleared before anything else is finalized that would prevent a set event from being triggered.

If several timing events are set for the same time, they are executed in FIFO order of being set.

An exception propagated from a handler invoked by a timing event has no effect.

For a given Timing_Event object, the implementation shall perform the operations declared in this package atomically with respect to any of these operations on the same Timing_Event object. The replacement of a handler by a call of Set_Handler shall be performed atomically with respect to the execution of the handler.

Reason: This prevents various race conditions. In particular it ensures that if an event occurs when Set_Handler is changing the handler then either the new or old handler is executed in response to the appropriate event. It is never possible for a new handler to be executed in response to an old event.

The implementation shall document the following metric:

- An upper bound on the lateness of the execution of a handler. That is, the maximum time between the time specified for the event and when a handler is actually invoked assuming no other handler or task is executing during this interval executed and the time specified when the event was set.

Documentation Requirement: The metrics for timing events.

The protected handler procedure should be executed directly by the real-time clock interrupt mechanism.
Implementation Advice: For a timing event, the handler should be executed directly by the real-time clock interrupt mechanism.

NOTE 1  {AI95-00297-01} Since a call of Set_Handler is not a potentially blocking operation, it can be called from within a handler.

NOTE 2  {AI95-00297-01} A Timing_Event_Handler can be associated with several Timing_Event objects.

Extensions to Ada 95

{AI95-00297-01} The package Real_Time.Timing_Events is new.

Wording Changes from Ada 2005

{AI05-0094-1} Correction: Reworded to eliminate a deadlock condition if the event time is in the past and a handler is currently executing. This is technically an inconsistency, but only if a program is depending on deadlocking; since it is impossible to imagine how that could be useful, we have not documented this as an inconsistency.

{AI05-0210-1} Correction: Clarified the metric for lateness of a timing event to exclude interference from other handlers and tasks. This change might change the documentation of an implementation, but not the implementation itself, so there is no inconsistency.

D.16 Multiprocessor Implementation

{AI05-0171-1} {AI05-0299-1} This subclause allows implementations on multiprocessor platforms to be configured.

Static Semantics

{AI12-0241-1} {AI12-0302-1} package System.Multiprocessors is
withpragma Preelaborate, Nonblocking, Global => in out synchronized
is
type CPU_Range is range 0 .. implementation-defined;
Not_A_Specific_CPU : constant CPU_Range := 0;
subtype CPU is CPU_Range range 1 .. CPU_Range'Last;

Implementation defined: The value of CPU_Range'Last in System.Multiprocessors.

function Number_Of_CPUs return CPU;
end System.Multiprocessors;

{AI05-0171-1} {AI05-0229-1} A call of Number_Of_CPUs returns the number of processors available to the program. Within a given partition, each call on Number_Of_CPUs will return the same value.

{AI12-0281-1} For a task type (including the anonymous type of a single task declaration), protected type (including the anonymous type of a single protected declaration), or subprogram, the following language-defined representation aspect may be specified:

CPU
The aspect CPU is an expression, which shall be of type System.Multiprocessors.CPU_Range.

Aspect Description for CPU: Processor on which a given task, or calling task for a protected operation, should run.

Legality Rules

{AI05-0171-1} {AI05-0229-1} If the CPU aspect is specified for a subprogram, the expression shall be static.

{AI05-0229-1} {AI12-0281-1} The CPU aspect shall not be specified on a task or protected interface type.
Dynamic Semantics

The expression specified for the CPU aspect of a task or protected type is evaluated for each time an task object of the corresponding task type is created (see 9.1 and 9.4). The CPU value is then associated with the task object whose task declaration specifies the aspect.

The CPU aspect has no effect if it is specified for a subprogram other than the main subprogram; the CPU value is not associated with any task.

The CPU value is associated with the environment task if the CPU aspect is specified for the main subprogram. If the CPU aspect is not specified for the main subprogram it is implementation defined on which processor the environment task executes.

Implementation defined: The processor on which the environment task executes in the absence of a value for the aspect CPU.

For a task, the CPU value determines the processor on which the task will activate and execute; the task is said to be assigned to that processor. If the CPU value is Not_A_Specific_CPU, then the task is not assigned to a processor. A task without a CPU aspect specified will activate and execute on the same processor as its activating task if the activating task is assigned a processor. If the CPU value is not in the range of System.Multiprocessors.CPU_Range or is greater than Number_Of_CPUs the task is defined to have failed, and it becomes a completed task (see 9.2).

For a protected type, the CPU value determines the processor on which calling tasks will execute; the protected object is said to be assigned to that processor. If the CPU value is Not_A_Specific_CPU, then the protected object is not assigned to a processor. A call to a protected object that is assigned to a processor from a task that is not assigned a processor or is assigned a different processor raises Program_Error.

Discussion: When a protected object is assigned to a CPU, only tasks also assigned to that CPU can call it. In contrast, a protected object that is not assigned to a specific CPU can be called by any task on any processor (subject, of course, to visibility and ceiling priority restrictions). As noted below, when the tasks and protected object are necessarily on the same CPU, a simpler implementation can be used.

Implementation Advice

Starting a protected action on a protected object statically assigned to a processor should be implemented without busy-waiting.

Reason: Busy-waiting is a form of lock and can be a source of deadlock. Busy-waiting is typically needed for starting protected actions on multiprocessors, but if all tasks calling a protected object execute on the same CPU, this locking isn't needed and the source of deadlock and associated overhead can be eliminated.

Implementation Advice: Starting a protected action on a protected object statically assigned to a processor should not use busy-waiting.

Extensions to Ada 2005

The package System.Multiprocessors and the CPU aspect are new.

Extensions to Ada 2012

Aspect CPU can now be applied to protected types, in order to avoid the overhead and deadlock potential of multiprocessor execution.

Wording Changes from Ada 2012

Corrigendum: Clarified when the CPU aspect expression is evaluated.
D.16.1 Multiprocessor Dispatching Domains

This subclause allows implementations on multiprocessor platforms to be partitioned into distinct dispatching domains during program startup.

Static Semantics

The following language-defined library package exists:

```ada
with Ada.Real_Time;
with Ada.Task_Identification;
package System.Multiprocessors.Dispatching_Domains
with Nonblocking, Global => in out synchronized is
  Dispatching_Domain_Error : exception;
  type Dispatching_Domain (<> is limited private;
  System_Dispatching_Domain : constant Dispatching_Domain;
  function Create (First, Last : CPU; Last : CPU_Range) return Dispatching_Domain;
  function Get_First_CPU (Domain : Dispatching_Domain) return CPU;
  function Get_Last_CPU  (Domain : Dispatching_Domain) return CPU_Range;
  type CPU_Set is array (CPU range <>) of Boolean;
  function Create (Set : CPU_Set) return Dispatching_Domain;
  function Get_CPU_Set (Domain : Dispatching_Domain) return CPU_Set;
  function Get_Dispatching_Domain
    return Dispatching_Domain;
  procedure Assign_Task
    (Domain : in out Dispatching_Domain;
    CPU    : in CPU_Range := Not_A_Specific_CPU;
  procedure Set_CPU
    (CPU : in CPU_Range;
  function Get_CPU
    return CPU_Range;
  procedure Delay_Until_And_Set_CPU
    (Delay_Until_Time : in Ada.Real_Time.Time; CPU : in CPU_Range);
private
  -- not specified by the language
end System.Multiprocessors.Dispatching_Domains;
```

A dispatching domain represents a set series of processors on which a task may execute. Each processor is contained within exactly one dispatching domain. A task is assigned to a dispatching domain. An object of type Dispatching_Domain identifies a dispatching domain. System Dispatching_Domain identifies a domain that contains the processor or processors on which the environment task executes. At program start-up, all processors are contained within this domain.

For a task type (including the anonymous type of a single task declaration), the following language-defined representation aspect may be specified:
Dispatching_Domain

The value of aspect Dispatching_Domain is an expression, which shall be of type Dispatching Domains.Dispatching_Domain. This aspect is the domain to which the task (or all objects of the task type) are assigned.

Aspect Description for Dispatching_Domain: Domain (group of processors) on which a given task should run.

Legality Rules

\{AI05-0167-1\} The Dispatching_Domain aspect shall not be specified for a task interface.

Dynamic Semantics

\{AI05-0167-1\} \{AI12-0033-1\} The expression specified for the Dispatching_Domain aspect of a task type is evaluated each time an object of the task type is created for each task object (see 9.1). If the identified dispatching domain is empty, then Dispatching_Domain_Error is raised; otherwise the newly created task is assigned to the domain identified by the value of the expression. The Dispatching_Domain value is then associated with the task object whose task declaration specifies the aspect.

\{AI05-0167-1\} If a task is not explicitly assigned to any domain, it is assigned to that of the activating task. A task always executes on some CPU in its domain.

\{AI05-0167-1\} \{AI12-0082-1\} If both the dispatching domain and CPU are specified for a task, and the CPU value is not contained within the setrange of processors for the domain (and is not Not_A_Specific_CPU), the activation of the task is defined to have failed, and it becomes a completed task (see 9.2).

\{AI05-0167-1\} \{AI12-0033-1\} The function Create with First and Last parameters creates and returns a dispatching_domain containing all the processors in the range First .. Last. The function Create with a Set parameter creates and returns a dispatching domain containing the processors for which Set(I) is True. These processors are removed from System_Dispatching_Domain. A call of Create will raise Dispatching_Domain_Error if any designated processor is not currently in System_Dispatching_Domain, or if the system cannot support a distinct domain over the processors identified, or if a processor has a task assigned to it, or if the allocation would leave System_Dispatching_Domain empty. A call of Create will raise Dispatching_Domain_Error if the calling task is not the environment task, or if Create is called after the call to the main subprogram.

\{AI05-0167-1\} \{AI12-0033-1\} The function Get_First_CPU returns the first CPU in Domain, or CPU'First if Domain is empty; Get_Last_CPU returns the last CPU in Domain, or CPU_Range'First if Domain is empty. The function Get_CPU_Set(D) returns an array whose low bound is Get_First_CPU(D), whose high bound is Get_Last_CPU(D), with True values in the Set corresponding to the CPUs that are in the given Domain one.

\{AI05-0167-1\} \{AI12-0082-1\} The function Get_Dispatching_Domain returns the dispatching_domain on which the task is assigned.

\{AI05-0167-1\} \{AI12-0033-1\} \{AI12-0033-1\} A call of the procedure Assign_Task assigns task T to the CPU within the dispatching_domain Domain. Task T can now execute only on CPU, unless CPU designates Not_A_Specific_CPU, in which case it can execute on any processor within Domain. The exception Dispatching_Domain_Error is propagated if Domain is empty, T is already assigned to a dispatching_domain other than System_Dispatching_Domain, or if CPU is not one of the processors of Domain (and is not Not_A_Specific_CPU). A call of Assign_Task is a task dispatching point for task T unless T is inside of a protected action, in which case the effect on task T is delayed until its next task dispatching point. If T is the Current_Task the effect is immediate if T is not inside a protected action, otherwise the effect is as soon as practical. Assigning a task already assigned to System_Dispatching_Domain that is already assigned to that domain has no effect.
A call of procedure Set_CPU assigns task T to the CPU. Task T can now execute only on CPU, unless CPU designates Not_A_Specific_CPU, in which case it can execute on any processor within its dispatching_domain. The exception Dispatching_Domain_Error is propagated if CPU is not one of the processors of the dispatching_domain on which T is assigned (and is not Not_A_Specific_CPU). A call of Set_CPU is a task dispatching point for task T unless T is inside of a protected action, in which case the effect on task T is delayed until its next task dispatching point. If T is the Current_Task the effect is immediate if T is not inside a protected action, otherwise the effect is as soon as practical.

The function Get_CPU returns the processor assigned to task T, or Not_A_Specific_CPU if the task is not assigned to a processor.

A call of Delay_Until_And_Set_CPU delays the calling task for the designated time and then assigns the task to the specified processor when the delay expires. The exception Dispatching_Domain_Error is propagated if P is not one of the processors of the calling task's dispatching_domain (and is not Not_A_Specific_CPU).

The implementation shall perform the operations Assign_Task, Set_CPU, Get_CPU and Delay_Until_And_Set_CPU atomically with respect to any of these operations on the same dispatching_domain, processor or task.

Any task that belongs to the system dispatching domain can execute on any CPU within that domain, unless the assignment of the task has been specified.

Reason: This ensures that priorities and deadlines are respected within the system dispatching domain. There is no such guarantee between different domains.

We only need to talk about the system dispatching domain here, because Assign_Task and Set_CPU already have such wording for tasks that are assigned explicitly to a dispatching domain and specify Not_A_Specific_CPU.

Ramification: If no dispatching domains are created, all tasks can execute on all processors. (As always, implementation-defined dispatching policies may have other rules, so a partition that does not specify any language-defined dispatching policy may do anything at all and in particular does not need to follow this rule.

Discussion: A task can be assigned to a specific CPU by specifying the aspect CPU for a task, or by calling a dynamic operation like Set_CPU or Assign_Task.

Implementation Advice: Each dispatching domain should have separate and disjoint ready queues.

Implementation Advice: Each dispatching domain should have separate and disjoint ready queues.

To be honest: "Ready queue" here doesn't mean the conceptual "ready queue" as defined in D.2.1 (one per processor); this rule is talking about the ready queues used by the implementation.

The implementation shall document the processor(s) on which the clock interrupt is handled and hence where delay queue and ready queue manipulations occur. For any Interrupt_Id whose handler can execute on more than one processor the implementation shall also document this set of processors.

Documentation Requirement: The processor(s) on which the clock interrupt is handled; the processors on which each Interrupt_Id can be handled.

An implementation may limit the number of dispatching domains that can be created and raise Dispatching_Domain_Error if an attempt is made to exceed this number.
The implementation may defer the effect of a Set_CPU or an Assign_Task operation until the specified task leaves an ongoing parallel construct.

**Reason:**
These operations can change the set of CPUs that a parallel operation is allowed to use. This could require the ability to move or suspend one or more threads to execute them on a different CPU. However, parallel constructs are primarily intended to improve performance of code, and the overhead needed to support such a rarely used operation could be substantial. Therefore, rather than requiring support we allow the implementation to wait to implement these operations until the parallel construct (and thus the extra threads) have completed.

**Extensions to Ada 2005**

The package System.Multiprocessors.Dispatching_Domains and the aspect Dispatching_Domains are new.

**Inconsistencies With Ada 2012**

Corrigendum: We now explicitly allow empty dispatching domains, as it would be difficult to avoid declaring them when a system is configured at runtime. Therefore, assigning a task to an empty domain now raises Dispatching_Domain_Error; creating such a domain should not raise Dispatching_Domain_Error. If an implementation does something different in these cases, and a program depends on that difference, the program could malfunction. This seems very unlikely (if no exception is ever raised, the task assigned to the empty domain could never run; if the exception is raised earlier, the program can't do anything useful).

**Incompatibilities With Ada 2012**

Corrigendum: The subtypes of the parameter or result of several routines were changed to support empty domains. These changes will cause rules requiring subtype conformance to fail on these routines (such as 'Access). We believe such uses are unlikely. In addition, type CPU_Set and function Get_CPU_Set, along with an overloaded Create are newly added to this package. As such, a use_clause conflict is possible; see the introduction of Annex A for more on this topic. If Multiprocessors.Dispatching_Domains is referenced in a use_clause, and an entity E with the same defining_identifier as a new entity in this package is defined in a package that is also referenced in a use_clause, the entity E may no longer be use-visible, resulting in errors. This should be rare and is easily fixed if it does occur.

**Wording Changes from Ada 2012**

Corrigendum: Added wording to clarify that all tasks can execute on all CPUs of the system dispatching domain by default.

Corrigendum: Added a definition to clarify that a "dispatching domain" is a concept which is identified by an object of type Dispatching_Domain; more than one object might identify the same dispatching domain (for instance, the result of function GetDispatching_Domain is a different object but identifies the same dispatching domain).
Annex E
(normative)
Distributed Systems

[This Annex defines facilities for supporting the implementation of distributed systems using multiple partitions working cooperatively as part of a single Ada program.]

Extensions to Ada 83

This Annex is new to Ada 95.

Post-Compilation Rules

A distributed system is an interconnection of one or more processing nodes (a system resource that has both computational and storage capabilities), and zero or more storage nodes (a system resource that has only storage capabilities, with the storage addressable by one or more processing nodes).

A distributed program comprises one or more partitions that execute independently (except when they communicate) in a distributed system.

The process of mapping the partitions of a program to the nodes in a distributed system is called configuring the partitions of the program.

Implementation Requirements

The implementation shall provide means for explicitly assigning library units to a partition and for the configuring and execution of a program consisting of multiple partitions on a distributed system; the means are implementation defined.

Implementation defined: The means for creating and executing distributed programs.

Implementation Permissions

An implementation may require that the set of processing nodes of a distributed system be homogeneous.

NOTE 1 The partitions comprising a program can be executed on differently configured distributed systems or on a nondistributed system without requiring recompilation. A distributed program can be partitioned differently from the same set of library units without recompilation. The resulting execution is semantically equivalent.

NOTE 2 A distributed program retains the same type safety as the equivalent single partition program.

E.1 Partitions

[The partitions of a distributed program are classified as either active or passive.]
An active partition shall be configured on a processing node. A passive partition shall be configured either on a storage node or on a processing node.

The configuration of the partitions of a program onto a distributed system shall be consistent with the possibility for data references or calls between the partitions implied by their semantic dependences. Any reference to data or call of a subprogram across partitions is called a *remote access*.

**Discussion:** For example, an active partition that includes a unit with a semantic dependence on the declaration of another RCI package of some other active partition has to be connected to that other partition by some sort of a message passing mechanism.

A passive partition that is accessible to an active partition should have its storage addressable to the processor(s) of the active partition. The processor(s) should be able to read and write from/to that storage, as well as to perform “read-modify-write” operations (in order to support entry-less protected objects).

**Ramification:** *{AI12-0359-1} A passive partition has no execution resources of its own, so while a call of a subprogram in a passive partition is a remote access to that subprogram, it is *not* a remote subprogram call (see E.4). The calling active partition executes the body of the subprogram of the passive partition.*

**Dynamic Semantics**

A *library_item* is elaborated as part of the elaboration of each partition that includes it. If a normal library unit (see E.2) has state, then a separate copy of the state exists in each active partition that elaborates it. [The state evolves independently in each such partition.]

**Ramification:** Normal library units cannot be included in passive partitions.

[A active partition *terminates* when its environment task terminates.] A partition becomes *inaccessible* if it terminates or if it is *aborted*. An active partition is aborted when its environment task is aborted. In addition, if a partition fails during its elaboration, it becomes inaccessible to other partitions. Other implementation-defined events can also result in a partition becoming inaccessible.

**Implementation defined:** Any events that can result in a partition becoming inaccessible.

For a *prefix* D that denotes a library-level declaration, excepting a declaration of or within a declared-pure library unit, the following attribute is defined:

**Bounded (Run-Time) Errors**

*{AI95-00226-01} It is a bounded error for there to be cyclic elaboration dependences between the active partitions of a single distributed program. The possible effects, in each of the partitions involved, are deadlock during elaboration, or the raising of Communication_Error or Program_Error in one or all of the active partitions involved.*

**Implementation Permissions**

An implementation may allow multiple active or passive partitions to be configured on a single processing node, and multiple passive partitions to be configured on a single storage node. In these cases, the scheduling policies, treatment of priorities, and management of shared resources between these partitions are implementation defined.

**Implementation defined:** The scheduling policies, treatment of priorities, and management of shared resources between partitions in certain cases.

An implementation may allow separate copies of an active partition to be configured on different processing nodes, and to provide appropriate interactions between the copies to present a consistent state of the partition to other active partitions.
Ramification: The language does not specify the nature of these interactions, nor the actual level of consistency preserved.

{AI12-0444-1} In an implementation, the partitions of a distributed program may need not be loaded and elaborated at different times all at the same time; they may be loaded and elaborated one at a time over an extended period of time. An implementation may provide facilities to abort and reload a partition during the execution of a distributed program.

An implementation may allow the state of some of the partitions of a distributed program to persist while other partitions of the program terminate and are later reinvoked.

NOTE 1 {AI12-0417-1} Library units are grouped into partitions after compile time, but before run time. At compile time, only the relevant library unit properties are identified using categorization aspects pragmas.

NOTE 2 The value returned by the Partition_Id attribute can be used as a parameter to implementation-provided subprograms in order to query information about the partition.

Wording Changes from Ada 95

{AI95-00226-01} Corrected wording so that a partition that has an elaboration problem will either deadlock or raise an exception. While an Ada 95 implementation could allow some partitions to continue to execute, they could be accessing unelaborated data, which is very bad (and erroneous in a practical sense). Therefore, this isn't listed as an inconsistency.

E.2 Categorization of Library Units

Library units can be categorized according to the role they play in a distributed program. Certain restrictions are associated with each category to ensure that the semantics of a distributed program remain close to the semantics for a nondistributed program.

{AI05-0243-1} {AI12-0417-1} A categorization aspect A categorization pragma is a library unit pragma (see 10.1.5) that specifies a corresponding categorization aspect. A categorization aspect restricts the declarations, child units, or semantic dependencies of the library unit to which it applies. A categorized library unit is a library unit that has a categorization aspect that is True to which a categorization pragma applies.

{AI05-0243-1} {AI12-0417-1} The aspects pragmas Shared Passive, Remote Types, and Remote Call Interface are categorization aspects pragmas, and the associated aspects are categorization aspects. In addition, for the purposes of this Annex, the aspect Pure (see 10.2.1) is considered a categorization aspect and the pragma Pure (see 10.2.1) is considered a categorization pragma.

{8652/0078} {AI95-00048-01} {AI05-0243-1} [ A library package or generic library package is called a shared passive library unit if the Shared Passive aspect of the unit is True pragma applies to it. A library package or generic library package is called a remote types library unit if the Remote Types aspect of the unit is True pragma applies to it. A library unit package or generic library package is called a remote call interface if the Remote Call Interface aspect of the unit is True pragma applies to it.] A normal library unit is one for which no categorization aspect is True pragma applies.

Proof: {AI05-0243-1} {AI05-0299-1} These terms (other than “normal library unit”) are really defined in the following subclauses.

Ramification: {8652/0078} {AI95-00048-01} A library subprogram can be a remote call interface, but it cannot be a remote types or shared passive library unit.

{AI05-0206-1} {AI05-0243-1} {AI05-0269-1} {AI05-0299-1} [The various categories of library units and the associated restrictions are described in this and the following clause and its subclauses. The categories are related hierarchically in that the library units of one category can depend semantically only on library units of that category or an earlier one in the hierarchy, except that the body of a remote types or remote call interface library unit is unrestricted. The declaration of a remote types or remote call
interface library unit may depend on preelaborated normal library units that are mentioned only in private with clauses, and all categories can depend on limited views.

6/3 \{AI05-0243-1\} \{AI05-0269-1\} The overall hierarchy (including declared pure) is as follows, with a lower-numbered category being “earlier in the hierarchy” in the sense of the previous paragraph:

6.1/3 1. Declared Pure
6.2/3 2. Shared Passive
6.3/3 3. Remote Types
6.4/3 4. Remote Call Interface
6.5/3 5. Normal (no restrictions)

Paragraphs 7 through 11 were deleted.

7/3 \{AI05-0243-1\} Declared Pure
Can depend only on other declared pure library units;

8/3 \{AI05-0243-1\} Shared Passive
Can depend only on other shared passive or declared pure library units;

9/3 \{AI05-0206-1\} \{AI05-0243-1\} Remote Types
The declaration of the library unit can depend only on other remote types library units, or one of the above library unit categories, or limited views, or preelaborated normal library units that are mentioned only in private with clauses; the body of the library unit is unrestricted;

10/3 \{AI05-0206-1\} \{AI05-0243-1\} Remote Call Interface
The declaration of the library unit can depend only on other remote call interfaces, or one of the above; the body of the library unit is unrestricted;

11/3 \{AI05-0243-1\} Normal
Unrestricted.

12 Declared pure and shared passive library units are preelaborated. The declaration of a remote types or remote call interface library unit is required to be preelaborable.

Implementation Requirements

13/1 \{8652/0079\} \{AI95-00208-01\} For a given library-level type declared in a preelaborated library unit or in the declaration of a remote types or remote call interface library unit, the implementation shall choose the same representation for the type upon each elaboration of the type’s declaration for different partitions of the same program.

Paragraph 13 and 14 were deleted.

Implementation Permissions

14/5 \{AI12-0417-1\} Implementations are allowed to define other categorization pragmas.

Wording Changes from Ada 95

14.a/2 \{8652/0078\} \{AI05-00048-01\} Corrigendum: Clarified that a library subprogram can be a remote call interface unit.

14.b/2 \{8652/0079\} \{AI95-00208-01\} Corrigendum: Removed the requirement that types be represented the same in all partitions, because it prevents the definition of heterogeneous distributed systems and goes much further than required.

Wording Changes from Ada 2005

14.c/3 \{AI05-0206-1\} \{AI05-0299-1\} We now allow private withs of preelaborated units in Remote Types and Remote Call Interface units; this is documented as an extension in the subclauses where this is defined normatively.
We have introduced categorization aspects; these are documented as extensions in the subclauses where they actually are defined.

**Wording Changes from Ada 2012**

Categorization pragmas are now obsolescent.

### E.2.1 Shared Passive Library Units

A shared passive library unit is used for managing global data shared between active partitions. The restrictions on shared passive library units prevent the data or tasks of one active partition from being accessible to another active partition through references implicit in objects declared in the shared passive library unit.

**Language Design Principles**

The restrictions governing a shared passive library unit are designed to ensure that objects and subprograms declared in the package can be used safely from multiple active partitions, even though the active partitions live in different address spaces, and have separate run-time systems.

**Syntax**

The form of a `pragma Shared_Passive` is as follows:

```
pragma Shared_Passive(library_unit_name);
```

Paragraphs 2 and 3 were moved to Annex J, “Obsolescent Features”.

**Legality Rules**

When the library unit aspect (see 13.1.1) a `pragma Shared_Passive` of is used to specify that a library unit is True, the library unit is a shared passive library unit, namely that the is a library unit to which a `Shared_Passive` aspect of the library unit is True pragma applies. The following restrictions apply to such a library unit:

**Aspect Description for Shared_Passive:** A given package is used to represent shared memory in a distributed system.

- **[it shall be preelaborable (see 10.2.1);]**

  **Ramification:** It cannot contain library-level declarations of protected objects with entries, nor of task objects. Task objects are disallowed because passive partitions don't have any threads of control of their own, nor any run-time system of their own. Protected objects with entries are disallowed because an entry queue contains references to calling tasks, and that would require in effect a pointer from a passive partition back to a task in some active partition.

- **{AI05-0243-1}** it shall depend semantically only upon declared pure or shared passive `library_item`library units;

  **Reason:** Shared passive packages cannot depend semantically upon remote types packages because the values of an access type declared in a remote types package refer to the local heap of the active partition including the remote types package.

  **Ramification:** {AI05-0243-1} We say `library_item` here, so that limited views are allowed; those are not `library_units`, but they are `library_item`.

- **{8652/0080}** {AI95-00003-01} {AI12-0038-1} {AI12-0320-1} it shall not contain a library-level declaration of an access type that designates a class wide type, nor a type with a part that is of a task type, or protected type with `entry_declaration`; if the shared passive library unit is generic, it shall not contain a declaration for such an access type unless the declaration is nested within a body other than a `package_body`.

  **Reason:** These kinds of access types are disallowed because the object designated by an access value of such a type could contain an implicit reference back to the active partition on whose behalf the designated object was created.

- **{AI12-0320-1}** of an access type that designates a class-wide type;

  **Reason:**

- **{AI12-0320-1}** of a type with a part that is of a task type;
7.3/5
- \{AI12-0320-1\} of a type with a part that is of a protected type with entry declarations; or

7.4/5
- \{AI12-0038-1\} \{AI12-0320-1\} it shall not contain a library-level declaration that contains a name that denotes a type declared within a declared-pure package, if that type has a part that is of an access type; for the purposes of this rule, the parts considered include those of the full views of any private types or private extensions.

7.b/4

Reason: This rule breaks privacy by looking into the full views of private types. Avoiding privacy breakage here would have required disallowing the use in a shared passive package of any private type declared in a declared-pure package, which would have been severely incompatible.

Notwithstanding the definition of accessibility given in 3.10.2, the declaration of a library unit \(P_1\) is not accessible from within the declarative region of a shared passive library unit \(P_2\), unless the shared passive library unit \(P_2\) depends semantically on \(P_1\).

Discussion: We considered a more complex rule, but dropped it. This is the simplest rule that recognizes that a shared passive package may outlive some other library package, unless it depends semantically on that package. In a nondistributed program, all library packages are presumed to have the same lifetime.

\{AI12-0417-1\} Implementations may define additional aspects or pragmas that force two library packages to be in the same partition, or to have the same lifetime, which would allow this rule to be relaxed in the presence of such aspects or pragmas.

Static Semantics

A shared passive library unit is preelaborated.

Post-Compilation Rules

A shared passive library unit shall be assigned to at most one partition within a given program.

Notwithstanding the rule given in 10.2, a compilation unit in a given partition does not need (in the sense of 10.2) the shared passive library units on which it depends semantically to be included in that same partition; they will typically reside in separate passive partitions.

To be honest: \{AI12-0359-1\} This rule is necessary so that the shared data of a shared passive partition is not duplicated in each partition. It does not imply a particular implementation; in particular, code can be replicated in each active partition.

Implementation Note: \{AI12-0359-1\} One possible implementation for a shared passive partition is as a shared library that is mapped into the address space of each active partition. In such case, both the code and the data of the passive partition would be mapped into the active partitions and directly called/accessed from each active partition. For instance, on Microsoft Windows a DLL has the correct semantics.

Alternatively, the shared data can be represented as a file or persistent memory, with the shared code being replicated in each active partition. Code replication is an as-if optimization; it should be impossible to tell where the code lives since no elaboration is necessary.

Wording Changes from Ada 95

\{8652/0080\} \{AI95-00003-01\} Corrigendum: Corrected the wording to allow access types in blocks in shared passive generic packages.

Extensions to Ada 2005

\{AI05-0243-1\} \{AI12-0417-1\} Shared Passive is now a categorization aspect, so it can be specified by an aspect specification — although the pragma is still preferred by the Reference Manual.

Incompatibilities With Ada 2012

\{AI12-0038-1\} Corrigendum: Uses of access types declared in declared-pure units are not allowed in library-level shared passive packages. These were allowed by Ada 2005 and Ada 2012, but it is unlikely that they work properly, as active partitions could disappear before the shared-passive partition. As such, the new errors are more likely to catch bugs than to cause them.
Wording Changes from Ada 2012

{AI12-0417-1} The pragma Shared Passive is now obsolescent.

E.2.2 Remote Types Library Units

[A remote types library unit supports the definition of types intended for use in communication between active partitions.]

Language Design Principles

The restrictions governing a remote types package are similar to those for a declared pure package. However, the restrictions are relaxed deliberately to allow such a package to contain declarations that violate the stateless property of pure packages, though it is presumed that any state-dependent properties are essentially invisible outside the package.

Syntax

{AI12-0417-1} The form of a pragma Remote_Types is as follows:

`pragma Remote_Types(library_unit_name);`

Paragraphs 2 and 3 were moved to Annex J, “Obsolescent Features”.

Legality Rules

{AI05-0243-1} {AI12-0417-1} When the library unit aspect (see 13.1.1) of a pragma Remote_Types is used to specify that a library unit is True, the library unit is a remote types library unit, namely that the library unit to which the pragma Remote_Types aspect of the library unit is True applies. The following restrictions apply to such a library unit:

Aspect Description for Remote_Types: Types in a given package may be used in remote procedure calls.

- [it shall be preelaborable;]
- {AI05-0206-1} {AI05-0243-1} it shall depend semantically only on declared pure library items, shared passive library units, or other remote types library units, or preelaborated normal library units that are mentioned only in private with clauses;
  Ramification: {AI05-0243-1} We say declared pure library item here, so that (all) limited views are allowed; those are not library units, but they are declared pure library items.
- it shall not contain the declaration of any variable within the visible part of the library unit;
  Reason: This is essentially a “methodological” restriction. A separate copy of a remote types package is included in each partition that references it, just like a normal package. Nevertheless, a remote types package is thought of as an “essentially pure” package for defining types to be used for interpartition communication, and it could be misleading to declare visible objects when no remote data access is actually being provided.
- {AI95-00240-01} {AI95-00366-01} if the full view of each type declared in the visible part of the library unit that has any available stream attributes shall support external streaming (see 13.13.2) has a part that is of a nonremote access type, then that access type, or the type of some part that includes the access type subcomponent, shall have user-specified Read and Write attributes.
  Reason: This is to prevent the use of the predefined Read and Write attributes of an access type as part of the Read and Write attributes of a visible type.
  Ramification: {AI95-00366-01} Types that do not have available stream attributes are excluded from this rule; that means that attributes do not need to be specified for most limited types. It is only necessary to specify attributes for nonlimited types that have a part that is of any access type, and for extensions of limited types with available stream attributes where the record_extension_part includes a subcomponent of an access type, where the access type does not have specified attributes.

{8652/0082} {AI95-00164-01} {AI05-0060-1} A named access type declared in the visible part of a remote types or remote call interface library unit is called a remote access type. Such a type shall be:
either an access-to-subprogram type or a general access type that designates a class-wide limited private type.

- {8652/0082} {AI95-00164-01} an access-to-subprogram type, or

- {8652/0082} {AI95-00164-01} {AI05-0060-1} a general access type that designates a class-wide limited private type, a class-wide limited interface type, or a class-wide private type extension all of whose ancestors are either private type-extensions, limited interface types, or limited private types.

- {8652/0081} {AI95-00004-01} A type that is derived from a remote access type is also a remote access type.

- {AI12-0283-1} A remote access-to-subprogram type shall not be nonblocking (see 9.5).

  **Reason:** All calls on remote subprograms are considered potentially blocking, so they cannot statically be allowed in nonblocking code.

  **Ramification:** The type declaration of a remote type is illegal if the Nonblocking aspect is True, either implicitly by inheritance or by explicit specification.

The following restrictions apply to the use of a remote access-to-subprogram type:

- {AI95-00431-01} A value of a remote access-to-subprogram type shall be converted only to or from another (subtype-conformant) remote access-to-subprogram type;

- The prefix of an Access attribute_reference that yields a value of a remote access-to-subprogram type shall statically denote a (subtype-conformant) remote subprogram.

The following restrictions apply to the use of a remote access-to-class-wide type:

- {8652/0083} {AI95-00047-01} {AI95-00240-01} {AI95-00366-01} {AI05-0060-1} {AI05-0101-1} The primitive subprograms of the corresponding specific limited private type shall only have access parameters if they are controlling formal parameters. The primitive functions of the corresponding specific type shall only have an access result if it is a controlling access result. Each noncontrolling formal parameter of the types of all the noncontrolling formal parameters and noncontrolling result type shall support external streaming (see 13.13.2); have either a nonlimited type or a type with Read and Write attributes specified via an attribute_definition_clause;

- {AI05-0060-1} {AI05-0215-1} {AI05-0269-1} The corresponding specific type shall not have a primitive procedure with the Synchronization aspect specified unless the synchronization_kind is Optional (see 9.5);

- A value of a remote access-to-class-wide type shall be explicitly converted only to another remote access-to-class-wide type;

- {AI12-0034-1} A value of a remote access-to-class-wide type shall be dereferenced (or implicitly converted to an anonymous access type) only as part of a dispatching call to a primitive operation of the designated type where the value designates a controlling operand of the call (see E.4, “Remote Subprogram Calls”);

  **Ramification:** {AI12-0034-1} Stream attributes of the designated type are not primitive operations of the designated type, and thus remote calls to them are prohibited by this rule. This is good, as the access parameter of a stream attribute does not have external streaming, and thus cannot be a parameter of a remote call.

- {AI05-0101-1} A controlling access result value for a primitive function with any controlling operands of the corresponding specific type shall either be explicitly converted to a remote access-to-class-wide type or be part of a dispatching call where the value designates a controlling operand of the call;

- {AI95-00366-01} {AI12-0085-1} The Storage_Pool attribute is not defined for a remote access-to-class-wide type; the expected type for an allocator shall not be a remote access-to-class-wide type. A remote access-to-class-wide type shall not be an
actual parameter for a generic formal access type. The Storage_Size attribute of a remote access-to-class-wide type yields 0; it is not allowed in an attribute_definition_clause. The Storage_Pool and Storage_Size aspects shall not be specified for a remote access-to-class-wide type.

**Reason:** {AI05-0005-1} All three of these restrictions are because there is no storage pool associated with a remote access-to-class-wide type. The Storage_Size is defined to be 0 so that there is no conflict with the rules for pure units.

**Ramification:** {AI12-0085-1} The prohibition against specifying the Storage_Size aspect for an access-to-class-wide type applies to any method of doing that, including via either an aspect specification or an attribute_definition_clause.

### Erroneous Execution

{AI12-0076-1} Execution is erroneous if some operation (other than the initialization or finalization of the object) modifies the value of a constant object declared in the visible part of a remote types package.

**Discussion:** {AI12-0005-1} This could be accomplished via a self-referencing pointer or via squirrelling away a writable pointer to a controlled object.

**NOTE 1** {AI12-0442-1} A remote types library unit is not necessarily need not be pure, and the types it defines cannot include levels of indirection implemented by using access types. User-specified Read and Write attributes (see 13.13.2) provide for sending values of such a type between active partitions, with Write marshalling the representation, and Read unmarshalling any levels of indirection.

**NOTE 2** {AI05-0060-1} The value of a remote access-to-class-wide limited interface can designate an object of a nonlimited type derived from the interface.

**NOTE 3** {AI05-0060-1} {AI12-0440-1} A remote access type can designate a class-wide synchronized, protected, or task interface type.

**Proof:** Synchronized, protected, and task interfaces are all considered limited interfaces, see 3.9.4.

### Incompatibilities With Ada 95

{AI95-00240-01} {AI05-0248-1} **Amendment Correction:** The wording was changed from “user-specified” to “available” read and write attributes. (This was then further changed, see below.) This means that an access type with the attributes specified in the private part would originally have been sufficient to allow the access type to be used in a remote type, but that is no longer allowed. Similarly, the attributes of a remote type that has access components have to be specified in the visible part. These changes were made so that the rules were consistent with the rules introduced for the Corrigendum for stream attributes; moreover, legality should not depend on the contents of the private part.

### Extensions to Ada 95

{AI95-00366-01} {AI05-0005-1} Remote types that cannot be streamed (that is, have no available stream attributes) do not require the specification of stream attributes. This is necessary so that most extensions of Limited_Controlled do not need stream attributes defined (otherwise there would be a significant incompatible with Limited_Controlled would need stream attributes, and then all extensions of it also would need stream attributes).

### Wording Changes from Ada 95

{8652/0081} {AI95-00004-01} **Corrigendum:** Added missing wording so that a type derived from a remote access type is also a remote access type.

{8652/0083} {AI95-00047-01} **Corrigendum:** Clarified that user-defined Read and Write attributes are required for the primitive subprograms corresponding to a remote access-to-class-wide type.

{8652/0082} {AI95-00164-01} **Corrigendum:** Added missing wording so that a remote access type can designate an appropriate private extension.

{AI95-00366-01} Changed the wording to use the newly defined term type that supports external streaming, so that various issues with access types in pure units and implicitly declared attributes for type extensions are properly handled.

{AI95-00366-01} Defined Storage_Size to be 0 for remote access-to-class-wide types, rather than having it undefined. This eliminates issues with pure units requiring a defined storage size.

{AI95-00431-01} Corrected the wording so that a value of a local access-to-subprogram type cannot be converted to a remote access-to-subprogram type, as intended (and required by the ACATS).
Incompatibilities With Ada 2005

Correction: Added rules about the returning of remote access-to-class-wide access class-wide types; this had been missed in the past. While programs that returned unstreamable types from RCI functions were legal, it is not clear what they could have done (as the results could not be marshalled). Similarly, RCI functions that return remote controlling access types could try to save those values, but it is unlikely that a compiler would know how to do that usefully. Thus, it seems unlikely that any real programs will be impacted by these changes.

E.2.2 Remote Types Library Units

[Remote call interface library units can be used as an interface for remote procedure calls (RPCs) (or remote function calls) between active partitions.]

Language Design Principles

The restrictions governing a remote call interface library unit are intended to ensure that the values of the actual parameters in a remote call can be meaningfully sent between two active partitions.

Syntax

The form of a pragma Remote_Call_Interface is as follows:

\{AI12-0417-1\} \{AI12-0005-1\} \{AI12-0005-1\} \{AI12-0005-1\} \{AI12-0005-1\} \{AI12-0005-1\} \{AI12-0005-1\} The form of a pragma Remote_Call_Interface is as follows:

\{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} The form of a pragma All_Calls_Remote is as follows:

\{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} \{AI12-0047-1\} A pragma All_Calls_Remote is a library unit pragma.

Paragraphs 2 through 6 were moved to Annex J, “Obsolescent Features”.

Legality Rules

When the library unit aspect (see 13.1.1) A pragma Remote_Call_Interface of is used to specify that a library unit is True, the library unit is a remote
call interface (RCI), namely that the is a library unit to which the pragma Remote_Call_Interface aspect of the library unit is True applies. A subprogram declared in the visible part of such a library unit, or declared by such a library unit, is called a remote subprogram.

**Aspect Description for Remote_Call_Interface:** Subprograms in a given package may be used in remote procedure calls.

\{AI05-0206-I\} \{AI05-0243-I\} The declaration of an RCI library unit shall be preelaborable (see 10.2.1), and shall depend semantically only upon declared pure library items, shared passive library units, remote types library units, or other remote call interface library units or preelaborated normal library units that are mentioned only in private with clauses.

**Ramification:** \{AI05-0243-I\} We say declared pure library item here, so that (all) limited views are allowed; those are not library units, but they are declared pure library items.

\{8652/0078\} \{AI95-00048-01\} In addition, the following restrictions apply to the visible part of an RCI library unit:

- \{8652/0078\} \{AI95-00048-01\} its visible part shall not contain the declaration of a variable;
  - **Reason:** \{8652/0078\} \{AI95-00048-01\} Remote call interface units do not provide remote data access. A shared passive package has to be used for that.

- \{8652/0078\} \{AI95-00048-01\} its visible part shall not contain the declaration of a limited type;
  - **Reason:** \{AI95-00048-01\} We disallow the declaration of task and protected types, since calling an entry or a protected subprogram implicitly passes an object of a limited type (the target task or protected object). We disallow other limited types since we require that such types have available defined Read and Write attributes, but we certainly don't want the Read and Write attributes themselves to involve remote calls (thereby defeating their purpose of marshalling the value for remote calls).

- \{8652/0078\} \{AI95-00048-01\} its visible part shall not contain a nested generic_declaration;
  - **Reason:** This is disallowed because the body of the nested generic would presumably have access to data inside the body of the RCI package, and if instantiated in a different partition, remote data access might result, which is not supported.

- \{8652/0078\} \{AI95-00048-01\} \{AI05-0229-I\} it shall not be, nor shall its visible part contain, the declaration of a subprogram for which aspect pragma Inline is True applies;
  - **Reason:** All such subprograms are remote subprograms, and all calls on remote subprograms are considered potentially blocking, so they cannot statically be allowed in nonblocking code.

- \{AI12-0283-I\} it shall not be, nor shall its visible part contain, the declaration of a subprogram that is nonblocking (see 9.5);
  - **Reason:** The type declaration of a remote subprogram is illegal if the Nonblocking aspect is True, either implicitly by inheritance or by explicit specification.
  - **Ramification:** The type declaration of a remote subprogram is illegal if the Nonblocking aspect is True, either implicitly by inheritance or by explicit specification.

- \{8652/0078\} \{AI95-00048-01\} \{AI95-00240-01\} \{AI95-00366-01\} \{AI05-0101-I\} it shall not be, nor shall its visible part contain, a subprogram (or access-to-subprogram) declaration whose profile has an access parameter or a parameter or result of a type that does not support external streaming (see 13.13.2) an access parameter, or a formal parameter of a limited type unless that limited type has user specified Read and Write attributes;
  - **Ramification:** \{AI05-0101-I\} No anonymous access types support external streaming, so they are never allowed as parameters or results of RCI subprograms.

- any public child of the library unit shall be a remote call interface library unit.
  - **Reason:** \{AI12-0417-I\} No restrictions apply to the private part of an RCI package, and since a public child can “see” the private part of its parent, such a child must itself have a Remote_Call_Interface pragma, and be assigned to the same partition (see below).
  - **Discussion:** \{AI12-0417-I\} We considered making the public child of an RCI package implicitly RCI, but it seemed better to require an explicit pragma to avoid any confusion.
  - Note that there is no need for a private child to be an RCI package, since it can only be seen from the body of its parent or its siblings, all of which are required to be in the same active partition.
Specification of a stream-oriented attribute is illegal in the specification of a remote call interface library unit. In addition to the places where Legality Rules normally apply (see 12.3), this rule applies also in the private part of an instance of a generic unit.

**Ramification:** This applies whether the stream-oriented attribute is specified with an attribute_definition_clause or with an aspect_specification.

**Reason:** Stream-oriented attributes are intended to be used locally (to marshall values), while subprograms in a remote call interface are intended to be used remotely. We resolve the conflict by banning the local use routines. The type should be included in a remote types package and imported into the remote call interface package.

If a pragma All_Calls_Remote sets the All_Calls_Remote is a library unit representation aspect of the applies to a library unit to which the pragma applies to the value True, the library unit shall be a remote call interface.

**Aspect Description for All_Calls_Remote:** All indirect or dispatching remote subprogram calls, and all direct remote subprogram procedure calls, should use the Partition Communication Subsystem, even if they are local.

**Post-Compilation Rules**

A remote call interface library unit shall be assigned to at most one partition of a given program. A remote call interface library unit whose parent is also an RCI library unit shall be assigned only to the same partition as its parent.

**Implementation Note:** The declaration of an RCI unit package, with a calling-stub body, is automatically included in all active partitions with compilation units that depend on it. However the whole RCI library unit, including its (non-stub) body, will only be in one of the active partitions.

Notwithstanding the rule given in 10.2, a compilation unit in a given partition that semantically depends on the declaration of an RCI library unit, needs (in the sense of 10.2) only the declaration of the RCI library unit, not the body, to be included in that same partition. [Therefore, the body of an RCI library unit is included only in the partition to which the RCI library unit is explicitly assigned.]

**Implementation Requirements**

If aspect pragma All_Calls_Remote is True for a given RCI library unit package, then the implementation shall route any of the following calls from outside the declarative region of the unit package through the Partition Communication Subsystem (PCS); see E.5. Calls to such subprograms from within the declarative region of the unit package are defined to be local and shall not go through the PCS.

- **AI12-0031-1** A direct call to a subprogram of the RCI unit from outside the declarative region of the unit;
- **AI12-0031-1** An indirect call through a remote access-to-subprogram value that designates a subprogram of the RCI unit;
- **AI12-0031-1** A dispatching call with a controlling operand designated by a remote access-to-class-wide value whose tag identifies a type declared in the RCI unit.

**Discussion:** Without this pragma, it is presumed that most implementations will not make direct calls through the PCS if the call originates in the same partition as that of the RCI unit package. When this aspect is True, all indirect or dispatching remote subprogram calls to the RCI unit, and all direct calls from outside the subsystem rooted at the RCI unit package, are treated like calls from outside the partition, ensuring that the PCS is involved in all such calls (for debugging, redundancy, etc.).

**Reason:** There is no point in forcing local direct calls (including calls from children) to go through the PCS, since on the target system, these calls are always local, and all the units are in the same active partition.
Implementation Permissions

\{AI05-0243-1\}  \{AI12-0417-1\}  \{AI12-0444-1\} An implementation may omit, need not support, or the Remote_Call_Interface pragma or aspect or the All Calls Remote aspect pragma. [Explicit message-based communication between active partitions can be supported as an alternative to RPC.]

Ramification: (AI12-0417-1) Of course, it is pointless to support the All_Calls_Remote aspect pragma if the Remote_Call_Interface aspect pragma (or some approximate equivalent) is not supported.

Incompatibilities With Ada 95

\{AI95-00240-01\}  \{AI05-0248-1\} Amendment Correction: The wording was changed from “user-specified” to “available” read and write attributes. (This was then further changed, see below.) This means that a type with the attributes specified in the private part would originally have been allowed as a formal parameter of an RCI subprogram, but that is no longer allowed. This change was made so that the rules were consistent with the rules introduced for the Corrigendum for stream attributes; moreover, legality should not depend on the contents of the private part.

Wording Changes from Ada 95

\{8652/0078\}  \{AI95-00048-01\} Corrigendum: Changed the wording to allow a library subprogram to be a remote call interface unit.

\{AI95-00366-01\} Changed the wording to use the newly defined term type that supports external streaming, so that various issues with access types in pure units and implicitly declared attributes for type extensions are properly handled.

Incompatibilities With Ada 2005

\{AI10-0101-1\} Correction: Added a rule to ensure that function results are streamable; this was missing in previous versions of Ada. While programs that returned unstreamable types from RCI functions were legal, it is not clear what they could have done (as the results could not be marshalled). Thus, it seems unlikely that any real programs will be impacted by this change.

Extensions to Ada 2005

\{AI05-0206-1\} Added wording to allow private withs of preelaborated normal units in the specification of a remote call interface unit.

\{AI05-0229-1\} All Calls Remote is now a representation aspect, so it can be specified by an aspect specification — although the pragma is still preferred by the Reference Manual.

\{AI05-0243-1\} Remote_Call_Interface is now a categorization aspect, so it can be specified by an aspect specification — although the pragma is still preferred by the Reference Manual.

Inconsistencies With Ada 2012

\{AI12-0031-1\} Corrigendum: Redefined when indirect and dispatching remote calls have to be remote for a unit for which the aspect All Calls Remote is True. With the new rules, a local target called indirectly or via dispatching will be routed through the PCS, while that was not necessarily true in earlier Ada. If a program depended on local targets not being routed through the PCS even when All Calls Remote is used, then it might behave differently or fail in corrected Ada 2012 as corrected with this refinement. This is highly unlikely as the PCS is going to be able to communicate with any part of the program, including the local partition.

Incompatibilities With Ada 2012

\{AI12-0002-1\} Correction: Specifying user-defined stream-oriented attributes is now illegal in an RCI unit. If a program contains such attributes, they and their associated type will need to be moved to a remote types package (which is then imported into the RCI unit).

Wording Changes from Ada 2012

\{AI12-0283-1\} Added a rule to ensure that potentially blocking remote calls are not considered nonblocking.

\{AI12-0417-1\} The pragmas Remote_Call_Interface and All_Calls_Remote are now obsolescent.
E.3 Consistency of a Distributed System

Language Design Principles

The rules guarantee that remote call interface and shared passive library units are consistent among all partitions prior to the execution of a distributed program, so that the semantics of the distributed program are well defined.

Static Semantics

For a prefix P that statically denotes a program unit, the following attributes are defined:

- **P'Version** Yields a value of the predefined type String that identifies the version of the compilation unit that contains the declaration of the program unit.
- **P'Body_Version** Yields a value of the predefined type String that identifies the version of the compilation unit that contains the body (but not any subunits) of the program unit.

The version of a compilation unit changes whenever the version changes for any–compilation unit changes in a semantically significant way. This document does not define the exact meaning of "semantically significant" on which it depends semantically. The version also changes whenever the compilation unit itself changes in a semantically significant way. It is implementation defined whether there are other events (such as recompilation) that result in the version of a compilation unit changing.

If P is not a library unit, and P has no completion, then P'Body_Version returns the Body_Version of the innermost program unit enclosing the declaration of P. If P is a library unit, and P has no completion, then P'Body_Version returns a value that is different from Body_Version of any version of P that has a completion.

Bounded (Run-Time) Errors

In a distributed program, a library unit is consistent if the same version of its declaration is used throughout. It is a bounded error to elaborate a partition of a distributed program that contains a compilation unit that depends on a different version of the declaration of a shared passive or RCI library unit than that included in the partition to which the shared passive or RCI library unit was assigned. As a result of this error, Program_Error can be raised in one or both partitions during elaboration; in any case, the partitions become inaccessible to one another.

Ramification: Because a version changes if anything on which it depends undergoes a version change, requiring consistency for shared passive and remote call interface library units is sufficient to ensure consistency for the declared pure and remote types library units that define the types used for the objects and parameters through which interpartition communication takes place.

Note that we do not require matching Body_Versions; it is irrelevant for shared passive and remote call interface packages, since only one copy of their body exists in a distributed program (in the absence of implicit replication), and we allow the bodies to differ for declared pure and remote types packages from partition to partition, presuming that the differences are due to required error corrections that took place during the execution of a long-running distributed program. The Body_Version attribute provides a means for performing stricter consistency checks.

Wording Changes from Ada 95

Corrigendum: Clarified the meaning of `Version` and `Body_Version`. 

---

E.3 Consistency of a Distributed System 16 October 2023 1348
E.4 Remote Subprogram Calls

{AI12-0359-1} A remote subprogram call is a subprogram call that invokes the execution of a subprogram in another (active) partition. The partition that originates the remote subprogram call is the calling partition, and the partition that executes the corresponding subprogram body is the called partition. Some remote procedure calls are allowed to return prior to the completion of subprogram execution. These are called asynchronous remote procedure calls.

Discussion: {AI12-0359-1} Remote subprogram calls are always between active partitions; a passive partition has no execution resources of its own and thus cannot execute anything, while a remote subprogram call is always executed by the called partition.

There are three different ways of performing a remote subprogram call:

- As a direct call on a (remote) subprogram explicitly declared in a remote call interface;
- As an indirect call through a value of a remote access-to-subprogram type;
- As a dispatching call with a controlling operand designated by a value of a remote access-to-class-wide type.

The first way of calling corresponds to a static binding between the calling and the called partition. The latter two ways correspond to a dynamic binding between the calling and the called partition.

{AI05-0101-1} Remote types library units (see E.2.2) and remote call interface library units (see E.2.3) define the remote subprograms or remote access types used for remote subprogram calls.

Language Design Principles
Remote subprogram calls are standardized since the RPC paradigm is widely-used, and establishing an interface to it in the annex will increase the portability and reusability of distributed programs.

Legality Rules
In a dispatching call with two or more controlling operands, if one controlling operand is designated by a value of a remote access-to-class-wide-type, then all shall be.

{AI12-0283-1} A nonblocking program unit shall not contain, other than within nested units with Nonblocking specified as statically False, a dispatching call with a controlling operand designated by a value of a remote access-to-class-wide-type.

Reason: Such a dispatching call is a potentially blocking call (see below) even if the called subprogram is nonblocking, so we must not assert that no blocking is possible.

Ramification: The calls is illegal if the Nonblocking aspect of the containing unit is True, either implicitly by inheritance or by explicit specification.

Dynamic Semantics
For the execution of a remote subprogram call, subprogram parameters (and later the results, if any) are passed using a stream-oriented representation (see 13.13.1) [which is suitable for transmission between partitions]. This action is called marshalling. Unmarshalling is the reverse action of reconstructing the parameters or results from the stream-oriented representation. [Marshalling is performed initially as part of the remote subprogram call in the calling partition; unmarshalling is done in the called partition. After the remote subprogram completes, marshalling is performed in the called partition, and finally unmarshalling is done in the calling partition.]

A calling stub is the sequence of code that replaces the subprogram body of a remotely called subprogram in the calling partition. A receiving stub is the sequence of code (the “wrapper”) that receives a remote subprogram call on the called partition and invokes the appropriate subprogram body.
Remote subprogram calls are executed at most once, that is, if the subprogram call returns normally, then the called subprogram's body was executed exactly once.

The task executing a remote subprogram call blocks until the subprogram in the called partition returns, unless the call is asynchronous. For an asynchronous remote procedure call, the calling task can become ready before the procedure in the called partition returns.

If a construct containing a remote call is aborted, the remote subprogram call is cancelled. Whether the execution of the remote subprogram is immediately aborted as a result of the cancellation is implementation defined.

Implementation defined: Whether the execution of the remote subprogram is immediately aborted as a result of cancellation.

If a remote subprogram call is received by a called partition before the partition has completed its elaboration, the call is kept pending until the called partition completes its elaboration (unless the call is cancelled by the calling partition prior to that).

If an exception is propagated by a remotely called subprogram, and the call is not an asynchronous call, the corresponding exception is reraised at the point of the remote subprogram call. For an asynchronous call, if the remote procedure call returns prior to the completion of the remotely called subprogram, any exception is lost.

The exception Communication_Error (see E.5) is raised if a remote call cannot be completed due to difficulties in communicating with the called partition.

Reason: Asynchronous remote procedure calls are potentially blocking since the implementation may require waiting for the availability of shared resources to initiate the remote call.

Program_Error is raised if this check fails. In a remote function call which returns a class-wide type, the same check is made on the function result.

Discussion: This check makes certain that the specific type passed or returned in an RPC satisfies the rules for a "communicable" type. Normally this is guaranteed by the compile-time restrictions on remote call interfaces. However, with class-wide types, it is possible to pass an object whose tag identifies a type declared outside the "safe" packages. This is considered an accessibility check since only the types declared in "safe" packages are considered truly "global" (cross-partition). Other types are local to a single partition. This is analogous to the "accessibility" of global vs. local declarations in a single-partition program.

This rule replaces a rule from an early version of Ada 9X which was given in the subclause on Remote Types Library Units (now E.2.2, “Remote Types Library Units”). That rule tried to prevent "bad" types from being sent by arranging for their tags to mismatch between partitions. However, this interfered with other uses of tags. The new rule allows tags to agree in all partitions, even for those types which are not "safe" to pass in an RPC.

In a dispatching call with two or more controlling operands that are designated by values of a remote access-to-class-wide type, a check is made [(in addition to the normal Tag_Check — see 11.5)] that all the remote access-to-class-wide values originated from Access attribute references that were evaluated by tasks of the same active partition. Constraint_Error is raised if this check fails.

Implementation Note: When a remote access-to-class-wide value is created by an Access attribute_reference, the identity of the active partition that evaluated the attribute_reference should be recorded in the representation of the remote access value.
The implementation of remote subprogram calls shall conform to the PCS interface as defined by the specification of the language-defined package System.RPC (see E.5). The calling stub shall use the Do_RPC procedure unless the remote procedure call is asynchronous in which case Do_APC shall be used. On the receiving side, the corresponding receiving stub shall be invoked by the RPC-receiver.

**Implementation Note:** One possible implementation model is as follows:

The code for calls to subprograms declared in an RCI package is generated normally, that is, the call-site is the same as for a local subprogram call. The code for the remotely callable subprogram bodies is also generated normally. Subprogram's prologue and epilogue are the same as for a local call.

When compiling the specification of an RCI package, the compiler generates calling stubs for each visible subprogram. Similarly, when compiling the body of an RCI package, the compiler generates receiving stubs for each visible subprogram together with the appropriate tables to allow the RPC-receiver to locate the correct receiving stub.

For the statically bound remote calls, the identity of the remote partition is statically determined (it is resolved at configuration/link time).

The calling stub operates as follows:

- It allocates (or reuses) a stream of Params_Stream_Type of Initial_Size, and initializes it by repeatedly calling Write operations, first to identify which remote subprogram in the receiving partition is being called, and then to pass the incoming value of each of the in and out parameters of the call.

- 

- [AI05-0229-1] It allocates (or reuses) a stream for the Result, unless an aspect pragma Asynchronous is specified as True for applied to the procedure.

- [AI05-0229-1] It calls Do_RPC unless an aspect pragma Asynchronous is specified as True for applied to the procedure in which case it calls Do_APC. An access value designating the message stream allocated and initialized above is passed as the Params parameter. An access value designating the Result stream is passed as the Result parameter.

- [AI05-0229-1] If the aspectpragma Asynchronous is not specified for the procedure, Do_RPC blocks until a reply message arrives, and then returns to the calling stub. The stub returns after extracting from the Result stream, using Read operations, the in and out parameters or the function result. If the reply message indicates that the execution of the remote subprogram propagated an exception, the exception is propagated from Do_RPC to the calling stub, and thence to the point of the original remote subprogram call. If Do_RPC detects that communication with the remote partition has failed, it propagates Communication_Error.

On the receiving side, the RPC-receiver procedure operates as follows:

- It is called from the PCS when a remote-subprogram-call message is received. The call originates in some remote call receiver task executed and managed in the context of the PCS.

- It extracts information from the stream to identify the appropriate receiving stub.

- The receiving stub extracts the in and out parameters using Read from the stream designated by the Params parameter.

- The receiving stub calls the actual subprogram body and, upon completion of the subprogram, uses Write to insert the results into the stream pointed to by the Result parameter. The receiving stub returns to the RPC-receiver procedure which in turn returns to the PCS. If the actual subprogram body propagates an exception, it is propagated by the RPC-receiver to the PCS, which handles the exception, and indicates in the reply message that the execution of the subprogram body propagated an exception. The exception occurrence can be represented in the reply message using the Write attribute of Ada.Exceptions.Exception_Occurrence.

For remote access-to-subprogram types:

A value of a remote access-to-subprogram type can be represented by the following components: a reference to the remote partition, an index to the package containing the remote subprogram, and an index to the subprogram within the package. The values of these components are determined at run time when the remote access value is created. These three components serve the same purpose when calling Do_APC/RPC, as in the statically bound remote calls; the only difference is that they are evaluated dynamically.

For remote access-to-class-wide types:

For each remote access-to-class-wide type, a calling stub is generated for each dispatching operation of the designated type. In addition, receiving stubs are generated to perform the remote dispatching operations in the called partition. The appropriate subprogram_body is determined as for a local dispatching call once the receiving stub has been reached.
A value of a remote access-to-class-wide type can be represented with the following components: a reference to the remote partition, an index to a table (created one per each such access type) containing addresses of all the dispatching operations of the designated type, and an access value designating the actual remote object.

Alternatively, a remote access-to-class-wide value can be represented as a normal access value, pointing to a "stub" object which in turn contains the information mentioned above. A call on any dispatching operation of such a stub object does the remote call, if necessary, using the information in the stub object to locate the target partition, etc. This approach has the advantage that less special-casing is required in the compiler. All access values can remain just a simple address.

For a call to Do_RPC or Do_APC: The partition ID of all controlling operands are checked for equality (a Constraint_Error is raised if this check fails). The partition ID value is used for the Partition parameter. An index into the tagged-type-descriptor is created. This index points to the receiving stub of the class-wide operation. This index and the index to the table (described above) are written to the stream. Then, the actual parameters are marshalled into the message stream. For a controlling operand, only the access value designating the remote object is required (the other two components are already present in the other parameters).

On the called partition (after the RPC-receiver has transferred control to the appropriate receiving stub) the parameters are first unmarshalled. Then, the tags of the controlling operands (obtained by dereferencing the pointer to the object) are checked for equality. If the check fails Constraint_Error is raised and propagated back to the calling partition, unless it is a result of an asynchronous call. Finally, a dispatching call to the specific subprogram (based on the controlling object's tag) is made. Note that since this subprogram is not in an RCI package, no specific stub is generated for it, it is called normally from the dispatching stub.

With respect to shared variables in shared passive library units, the execution of the corresponding subprogram body of a synchronous remote procedure call is considered to be part of the execution of the calling task. The execution of the corresponding subprogram body of an asynchronous remote procedure call proceeds in parallel with the calling task and does not signal the next action of the calling task (see 9.10).

NOTE 1 A given active partition can both make and receive remote subprogram calls. Thus, an active partition can act as both a client and a server.

NOTE 2 If a given exception is propagated by a remote subprogram call, but the exception does not exist in the calling partition, the exception can be handled by an others choice or be propagated to and handled by a third partition.

Discussion: This situation can happen in a case of dynamically nested remote subprogram calls, where an intermediate call executes in a partition that does not include the library unit that defines the exception.

Wording Changes from Ada 95

{8652/0086} Corrigendum: Added rules so that tasks can safely access shared passive objects.

{8652/0085} Corrigendum: Clarified that the check on class-wide types also applies to values returned from remote subprogram call functions.

Wording Changes from Ada 2005

{AI05-0101-1} Correction: Corrected the text to note that remote access types can be defined in remote types units.

Wording Changes from Ada 2012

{AI12-0283-1} Added a rule to ensure that potentially blocking remote calls are not considered nonblocking.

{AI12-0359-1} Clarified that remote subprogram calls are always to active partitions.

E.4.1 Asynchronous Remote Calls

Pragma Asynchronous

[This subclause introduces the aspect pragma Asynchronous which can be specified to allow a remote subprogram call to return prior to completion of the execution of the corresponding remote subprogram body.]

Paragraphs 2 through 7 were deleted.

Syntax

{AI05-0229-1} The form of a pragma Asynchronous is as follows:
pragma Asynchronous(local_name);

Legality Rules

{AI05-0229-1} The local_name of a pragma Asynchronous shall denote either:

• One or more remote procedures; the formal parameters of the procedure(s) shall all be of mode in;
• The first subtype of a remote access to procedure type; the formal parameters of the designated profile of the type shall all be of mode in;
• The first subtype of a remote access to class-wide type.

Static Semantics

{AI05-0229-1} For a remote procedure, the following language-defined representation aspect may be specified: A pragma Asynchronous is a representation pragma. When applied to a type, it specifies the type-related asynchronous aspect of the type.

Asynchronous
The type of aspect Asynchronous is Boolean. If directly specified, the aspect_definition shall be a static expression. If not specified, the aspect is False.

Aspect Description for Asynchronous: Remote procedure calls are asynchronous; the caller continues without waiting for the call to return.

{AI05-0229-1} For a remote access type, the following language-defined representation aspect may be specified:

Asynchronous
The type of aspect Asynchronous is Boolean. If directly specified, the aspect_definition shall be a static expression. If not specified (including by inheritance), the aspect is False.

Legality Rules

{AI05-0229-1} If aspect Asynchronous is specified for a remote procedure, the formal parameters of the procedure shall all be of mode in.

{AI05-0229-1} If aspect Asynchronous is specified for a remote access type, the type shall be a remote access-to-class-wide type, or the type shall be a remote access-to-procedure type with the formal parameters of the designated profile of the type all of mode in.

Dynamic Semantics

{AI05-0229-1} A remote call is asynchronous if it is a call to a procedure, or a call through a value of an access-to-procedure type, for which aspect pragma Asynchronous is True applies. In addition, if aspect pragma Asynchronous is True for applies to a remote access-to-class-wide type, then a dispatching call on a procedure with a controlling operand designated by a value of the type is asynchronous if the formal parameters of the procedure are all of mode in.

Implementation Requirements

Asynchronous remote procedure calls shall be implemented such that the corresponding body executes at most once as a result of the call.

To be honest: It is not clear that this rule can be tested or even defined formally.

Extensions to Ada 2005

{AI05-0229-1} Aspect Asynchronous is new; pragma Asynchronous is now obsolescent.
E.4.2 Example of Use of a Remote Access-to-Class-Wide Type

Example of using a remote access-to-class-wide type to achieve dynamic binding across active partitions:

```ada
{AI12-0414-1} package Tapes is
  with pragma Pure is(Tapes);
  type Tape is abstract tagged limited private;
  -- Primitive dispatching operations where
  -- Tape is controlling operand
  procedure Copy (From, To : access Tape;
      Num_Recs : in Natural) is abstract;
  procedure Rewind (T : access Tape) is abstract;
  -- More operations

  private
  type Tape is ...
  end Tapes;
{AI12-0414-1} with Tapes;

package Name_Server is
  with pragma Remote_Call_Interface is;
  -- Dynamic binding to remote operations is achieved
  -- using the access-to-limited-class-wide type Tape_Ptr
  type Tape_Ptr is access all Tapes.Tape'Class;
  -- The following statically bound remote operations
  -- allow for a name-server capability in this example
  function Find     (Name : String) return Tape_Ptr;
  procedure Register (Name : in String; T : in Tape_Ptr);
  procedure Remove   (T : in Tape_Ptr);
  -- More operations
  end Name_Server;

package Tape_Driver is
  -- Declarations are not shown, they are irrelevant here
  end Tape_Driver;
{AI12-0347-1} with Tapes, Name_Server;

package body Tape_Driver is
  type New_Tape is new Tapes.Tape with ...
  overriding
  procedure Rewind (T : access New_Tape);
  overriding
  procedure Copy
      (From, To : access New_Tape; Num_Recs: in Natural) is
  begin
      . . .
  end Copy;

procedure Rewind (T : access New_Tape) is
  begin
      . . .
  end Rewind;
  -- Objects remotely accessible through use
  -- of Name_Server operations
  Tape1, Tape2 : aliased New_Tape;
  begin
      Name_Server.Register ("NINE-TRACK", Tape1'Access);
      Name_Server.Register ("SEVEN-TRACK", Tape2'Access);
  end Tape_Driver;
```
with Tapes, Name_Server;
-- Tape_Driver is not needed and thus not mentioned in the with_clause
procedure Tape_Client is
   T1, T2 : Name_Server.Tape_Ptr;
begin
   T1 := Name_Server.Find ("NINE-TRACK");
   T2 := Name_Server.Find ("SEVEN-TRACK");
   Tapes.Rewind (T1);
   Tapes.Rewind (T2);
   Tapes.Copy (T1, T2, 3);
end Tape_Client;

{AI12-0452-1} Discussion of Notes on the example:

Discussion: The example does not show the case where tapes are removed from or added to the system. In the former case, an appropriate exception needs to be defined to instruct the client to use another tape. In the latter, the Name_Server should have a query function visible to the clients to inform them about the availability of the tapes in the system.

This paragraph was deleted.

- The package Tapes provides the necessary declarations of the type and its primitive operations.
- Name_Server is a remote call interface package and is elaborated in a separate active partition to provide the necessary naming services (such as Register and Find) to the entire distributed program through remote subprogram calls.
- Tape_Driver is a normal package that is elaborated in a partition configured on the processing node that is connected to the tape device(s). The abstract operations are overridden to support the locally declared tape devices (Tape1, Tape2). The package is not visible to its clients, but it exports the tape devices (as remote objects) through the services of the Name_Server. This allows for tape devices to be dynamically added, removed or replaced without requiring the modification of the clients' code.
- {AI12-0442-1} The Tape_Client procedure references only declarations in the Tapes and Name_Server packages. Before using a tape for the first time, it will needs to query the Name_Server for a system-wide identity for that tape. From then on, it can use that identity to access the tape device.
- Values of remote access type Tape_Ptr include the necessary information to complete the remote dispatching operations that result from dereferencing the controlling operands T1 and T2.

E.5 Partition Communication Subsystem

{AI95-00273-01} [The Partition Communication Subsystem (PCS) provides facilities for supporting communication between the active partitions of a distributed program. The package System.RPC is a language-defined interface to the PCS.] An implementation conforming to this Annex shall use the RPC interface to implement remote subprogram calls.

Reason: The prefix RPC is used rather than RSC because the term remote procedure call and its acronym are more familiar.

Static Semantics

The following language-defined library package exists:

{AI12-0241-1} {AI12-0302-1} with Ada.Streams; -- see 13.13.1
package System.RPC
  with Nonblocking => False, Global => in out synchronized is
   type Partition_Id is range 0 .. implementation-defined;
   Communication_Error : exception;
type Params_Stream_Type (Initial_Size : Ada.Streams.Stream_Element_Count) is new Ada_streams.Root_Stream_Type with private;

procedure Read(
    Stream : in out Params_Stream_Type;
    Item : out Ada.Streams.Stream_Element_Array;
    Last : out Ada.Streams.Stream_Element_Offset);

procedure Write(
    Stream : in out Params_Stream_Type;
    Item : in Ada.Streams.Stream_Element_Array);

-- Synchronous call
procedure Do_RPC(
    Partition : in Partition_Id;
    Params : access Params_Stream_Type;
    Result : access Params_Stream_Type);

-- Asynchronous call
procedure Do_APC(
    Partition : in Partition_Id;
    Params : access Params_Stream_Type);

-- The handler for incoming RPCs

private
    ... -- not specified by the language
end System.RPC;

A value of the type Partition_Id is used to identify a partition.

Implementation defined: The range of type System.RPC.Partition_Id.

An object of the type Params_Stream_Type is used for identifying the particular remote subprogram that is being called, as well as marshalling and unmarshalling the parameters or result of a remote subprogram call, as part of sending them between partitions.

[The Read and Write procedures override the corresponding abstract operations for the type Params_Stream_Type.]

Dynamic Semantics

The Do_RPC and Do_APC procedures send a message to the active partition identified by the Partition parameter.

Implementation Note: It is assumed that the RPC interface is above the message-passing layer of the network protocol stack and is implemented in terms of it.

After sending the message, Do_RPC blocks the calling task until a reply message comes back from the called partition or some error is detected by the underlying communication system in which case Communication_Error is raised at the point of the call to Do_RPC.

Reason: Only one exception is defined in System.RPC, although many sources of errors might exist. This is so because it is not always possible to distinguish among these errors. In particular, it is often impossible to tell the difference between a failing communication link and a failing processing node. Additional information might be associated with a particular Exception_Occurrence for a Communication_Error.

Do_APC operates in the same way as Do_RPC except that it is allowed to return immediately after sending the message.
Upon normal return, the stream designated by the Result parameter of Do_RPC contains the reply message.

The procedure System.RPC.Establish_RPC_Receiver is called once, immediately after elaborating the library units of an active partition (that is, right after the elaboration of the partition) if the partition includes an RCI library unit, but prior to invoking the main subprogram, if any. The Partition parameter is the Partition_Id of the active partition being elaborated. The Receiver parameter designates an implementation-provided procedure called the RPC-receiver which will handle all RPCs received by the partition from the PCS. Establish_RPC_Receiver saves a reference to the RPC-receiver; when a message is received at the called partition, the RPC-receiver is called with the Params stream containing the message. When the RPC-receiver returns, the contents of the stream designated by Result is placed in a message and sent back to the calling partition.

**Implementation Note:** It is defined by the PCS implementation whether one or more threads of control should be available to process incoming messages and to wait for their completion.

**Implementation Note:** At link-time, the linker provides the RPC-receiver and the necessary tables to support it. A call on Establish_RPC_Receiver is inserted just before the call on the main subprogram.

**Reason:** The interface between the PCS (the System.RPC package) and the RPC-receiver is defined to be dynamic in order to allow the elaboration sequence to notify the PCS that all packages have been elaborated and that it is safe to call the receiving stubs. It is not guaranteed that the PCS units will be the last to be elaborated, so some other indication that elaboration is complete is needed.

If a call on Do_RPC is aborted, a cancellation message is sent to the called partition, to request that the execution of the remotely called subprogram be aborted.

**To be honest:** The full effects of this message are dependent on the implementation of the PCS.

This paragraph was deleted. The subprograms declared in System.RPC are potentially blocking operations.

**Implementation Requirements**

The implementation of the RPC-receiver shall be reentrant, thereby allowing concurrent calls on it from the PCS to service concurrent remote subprogram calls into the partition.

**Reason:** There seems no reason to allow the implementation of RPC-receiver to be nonreentrant, even though we don't require that every implementation of the PCS actually perform concurrent calls on the RPC-receiver.

An implementation shall not restrict the replacement of the body of System.RPC. An implementation shall not restrict children of System.RPC. [The related implementation permissions in the introduction to Annex A do not apply.]

**Reason:** The point of System.RPC is to let the user tailor the communications mechanism without requiring changes to or other cooperation from the compiler. However, implementations can restrict the replacement of language-defined units. This requirement overrides that permission for System.RPC.

If the implementation of System.RPC is provided by the user, an implementation shall support remote subprogram calls as specified.

**Discussion:** If the implementation takes advantage of the implementation permission to use a different specification for System.RPC, it still needs to use it for remote subprogram calls, and allow the user to replace the body of System.RPC. It just isn't guaranteed to be portable to do so in Ada 2005 - an advantage which was more theoretical than real anyway.

**Documentation Requirements**

The implementation of the PCS shall document whether the RPC-receiver is invoked from concurrent tasks. If there is an upper limit on the number of such tasks, this limit shall be documented as well, together with the mechanisms to configure it (if this is supported).

This paragraph was deleted. Implementation defined: Implementation-defined aspects of the PCS.
Documentation Requirement: Whether the RPC-receiver is invoked from concurrent tasks, and if so, the number of such tasks.

Implementation Permissions

The PCS is allowed to contain implementation-defined interfaces for explicit message passing, broadcasting, etc. Similarly, it is allowed to provide additional interfaces to query the state of some remote partition (given its partition ID) or of the PCS itself, to set timeouts and retry parameters, to get more detailed error status, etc. These additional interfaces should be provided in child packages of System.RPC.

Implementation defined: Implementation-defined interfaces in the PCS.

{AI12-0444-1} A body for the package System.RPC is not required to need not be supplied by the implementation.

Reason: It is presumed that a body for the package System.RPC might be extremely environment specific. Therefore, we do not require that a body be provided by the (compiler) implementation. The user will have to write a body, or acquire one, appropriate for the target environment.

{AI95-00273-01} {AI05-0299-1} An alternative declaration is allowed for package System.RPC as long as it provides a set of operations that is substantially equivalent to the specification defined in this subclauseclause.

Reason: Experience has proved that the definition of System.RPC given here is inadequate for interfacing to existing distribution mechanisms (such as CORBA), especially on heterogeneous systems. Rather than mandate a change in the mechanism (which would break existing systems), require implementations to support multiple mechanisms (which is impractical), or prevent the use of Annex E facilities with existing systems (which would be silly), we simply make this facility optional.

One of the purposes behind System.RPC was that knowledgeable users, rather than compiler vendors, could create this package tailored to their networks. Experience has shown that users get their RPC from vendors anyway; users have not taken advantage of the flexibility provided by this defined interface. Moreover, one could compare this defined interface to requiring Ada compilers to use a defined interface to implement tasking. No one thinks that the latter is a good idea, why should anyone believe that the former is?

Therefore, this subclauseclause is made optional. We considered deleting the subclauseclause outright, but we still require that users may replace the package (whatever its interface). Also, it still provides a useful guide to the implementation of this feature.

Implementation Advice

Whenever possible, the PCS on the called partition should allow for multiple tasks to call the RPC-receiver with different messages and should allow them to block until the corresponding subprogram body returns.

{AI95-00273-01} {AI05-0299-1} The System.RPC.Write operation should raise Storage_Error if it runs out of space when writing an item.

NOTE The package System.RPC is not designed for direct calls by user programs. It is instead designed for use in the implementation of remote subprograms calls, being called by the calling stubs generated for a remote call interface library unit to initiate a remote call, and in turn calling back to an RPC-receiver that dispatches to the receiving stubs generated for the body of a remote call interface, to handle a remote call received from elsewhere.
Incompatibilities With Ada 95

\{AI95-00273-01\} The specification of System.RPC can now be tailored for an implementation. If a program replaces the body of System.RPC with a user-defined body, it might not compile in a given implementation of Ada 2005 (if the specification of System.RPC has been changed).

Wording Changes from Ada 95

\{8652/0087\} \{AI95-00082-01\} Corrigendum: Clarified that the user can replace System.RPC.
Annex F
(normative)
Information Systems

This Annex provides a set of facilities relevant to Information Systems programming. These fall into several categories:

- an attribute definition clause specifying Machine_Radix for a decimal subtype;
- the package Decimal, which declares a set of constants defining the implementation's capacity for decimal types, and a generic procedure for decimal division; and
- the child packages Text_IO.Editing and Wide_Text_IO.Editing, which support formatted and localized output of decimal data, based on “picture String” values.

Other relevant facilities can be found in

The character and string handling packages in Annex A, “Predefined Language Environment” are also relevant for Information Systems.

Implementation Advice

If COBOL (respectively, C) is widely supported in the target environment, implementations supporting the Information Systems Annex should provide the child package Interfaces.COBOL (respectively, Interfaces.C) specified in Annex B and should support a convention_identifier of COBOL (respectively, C) for in the Convention aspect interfacing pragmas (see Annex B), thus allowing Ada programs to interface with programs written in that language.

Implementation Advice: If COBOL (respectively, C) is supported in the target environment, then interfacing to COBOL (respectively, C) should be supported as specified in Annex B.

Extensions to Ada 83

This Annex is new to Ada 95.

Wording Changes from Ada 95

Added a mention of Wide Text IO.Editing, part of the support for 32-bit characters.

F.1 Machine_Radix Attribute Definition Clause

Static Semantics

The representation attribute Machine_Radix may be specified for a decimal first subtype (see 3.5.9) via an attribute_definition_clause; the expression of such a clause shall be static, and its value shall be 2 or 10. A value of 2 implies a binary base range; a value of 10 implies a decimal base range.

Ramification: In the absence of a Machine_Radix clause, the choice of 2 versus 10 for S'Machine_Radix is not specified.

Aspect Description for Machine_Radix: Radix (2 or 10) that is used to represent a decimal fixed point type.
Implementation Advice

Packed decimal should be used as the internal representation for objects of subtype S when S'Machine_Radix = 10.

Discussion: {AI05-0229-1} The intent of a decimal Machine_Radix attribute definition clause is to allow the programmer to declare an Ada decimal data object whose representation matches a particular COBOL implementation's representation of packed decimal items. The Ada object may then be passed to an interfaced COBOL program that takes a packed decimal data item as a parameter, assuming that convention COBOL has been specified for the Ada object's type with an aspect in a pragma Convention.

Additionally, the Ada compiler may choose to generate arithmetic instructions that exploit the packed decimal representation.

Examples

Example of Machine_Radix attribute definition clause:

```ada
type Money is delta 0.01 digits 15;
for Money'Machine_Radix use 10;
```

Wording Changes from Ada 2012

{AI12-0272-1} Clarified that Machine_Radix is a representation aspect.

F.2 The Package Decimal

Static Semantics

The library package Decimal has the following declaration:

```ada
{AI12-0414-1} package Ada.Decimal is
  with pragma Pure is (Decimal);
  constant Max_Scale := implementation-defined;
  constant Min_Scale := implementation-defined;
  constant Min_Delta := 10.0**(-Max_Scale);
  constant Max_Delta := 10.0**(-Min_Scale);
  constant Max_Decimal_Digits := implementation-defined;

  generic
  type Dividend_Type is delta <> digits <>;
  type Divisor_Type is delta <> digits <>;
  type Quotient_Type is delta <> digits <>;
  type Remainder_Type is delta <> digits <>;
  procedure Divide (Dividend : in Dividend_Type;
                   Divisor : in Divisor_Type;
                   Quotient : out Quotient_Type;
                   Remainder : out Remainder_Type)
      withConvention => Intrinsic;
      pragma Convention (Intrinsic, Divide);
end Ada.Decimal;
```

Implementation defined: The values of named numbers in the package Decimal.

Max_Scale is the largest N such that 10.0**(-N) is allowed as a decimal type's delta. Its type is universal_integer.

Min_Scale is the smallest N such that 10.0**(-N) is allowed as a decimal type's delta. Its type is universal_integer.

Min_Delta is the smallest value allowed for delta in a decimal_fixed_point_definition. Its type is universal_real.
Max_Delta is the largest value allowed for delta in a decimal_fixed_point_definition. Its type is universal_real.

Max_Decimal_Digits is the largest value allowed for digits in a decimal_fixed_point_definition. Its type is universal_integer.

Reason: The name is Max_Decimal_Digits versus Max_Digits, in order to avoid confusion with the named number System.Max_Digits relevant to floating point.

Static Semantics
The effect of Divide is as follows. The value of Quotient is Quotient_Type(Dividend/Divisor). The value of Remainder is Remainder_Type(Intermediate), where Intermediate is the difference between Dividend and the product of Divisor and Quotient; this result is computed exactly.

Implementation Requirements
Decimal.Max_Decimal_Digits shall be at least 18.
Decimal.Max_Scale shall be at least 18.
Decimal.Min_Scale shall be at most 0.

NOTE The effect of division yielding a quotient with control over rounding versus truncation is obtained by applying either the function attribute Quotient_Type’Round or the conversion Quotient_Type to the expression Dividend/Divisor.

F.3 Edited Output for Decimal Types

The child packages Text_IO.Editing, and Wide_Text_IO.Editing, and Wide_Wide_Text_IO.Editing provide localizable formatted text output, known as edited output, for decimal types. An edited output string is a function of a numeric value, program-specifiable locale elements, and a format control value. The numeric value is of some decimal type. The locale elements are:

- the currency string;
- the digits group separator character;
- the radix mark character; and
- the fill character that replaces leading zeros of the numeric value.

For Text_IO.Editing the edited output and currency strings are of type String, and the locale characters are of type Character. For Wide_Text_IO.Editing their types are Wide_String and Wide_Character, respectively. For Wide_Wide_Text_IO.Editing their types are Wide_Wide_String and Wide_Wide_Character, respectively.

Each of the locale elements has a default value that can be replaced or explicitly overridden.

A format-control value is of the private type Picture; it determines the composition of the edited output string and controls the form and placement of the sign, the position of the locale elements and the decimal digits, the presence or absence of a radix mark, suppression of leading zeros, and insertion of particular character values.

A Picture object is composed from a String value, known as a picture String, that serves as a template for the edited output string, and a Boolean value that controls whether a string of all space characters is produced when the number's value is zero. A picture String comprises a sequence of one- or two-Character symbols, each serving as a placeholder for a character or string at a corresponding position in the edited output string. The picture String symbols fall into several categories based on their effect on the edited output string:
Decimal Digit:  '9'
Radix Control:  ','  'V'
Sign Control:  '+',  '–',  '<',  '>',  'CR',  'DB'
Currency Control:  '$',  '#'
Zero Suppression:  'Z',  '*'
Simple Insertion:  '_',  'B',  '0',  '/'

The entries are not case-sensitive. Mixed- or lower-case forms for "CR" and "DB", and lower-case forms for 'V', 'Z', and 'B', have the same effect as the upper-case symbols shown.

An occurrence of a '9' Character in the picture String represents a decimal digit position in the edited output string.

A radix control Character in the picture String indicates the position of the radix mark in the edited output string: an actual character position for '1', or an assumed position for 'V'.

A sign control Character in the picture String affects the form of the sign in the edited output string. The '<' and '>' Character values indicate parentheses for negative values. A Character '+', '–', or '<' appears either singly, signifying a fixed-position sign in the edited output, or repeated, signifying a floating-position sign that is preceded by zero or more space characters and that replaces a leading 0.

A currency control Character in the picture String indicates an occurrence of the currency string in the edited output string. The '$' Character represents the complete currency string; the '#' Character represents one character of the currency string. A '$' Character appears either singly, indicating a fixed-position currency string in the edited output, or repeated, indicating a floating-position currency string that occurs in place of a leading 0. A sequence of '#' Character values indicates either a fixed- or floating-position currency string, depending on context.

A zero suppression Character in the picture String allows a leading zero to be replaced by either the space character (for 'Z') or the fill character (for '*').

A simple insertion Character in the picture String represents, in general, either itself (if '/') or '0'), the space character (if 'B'), or the digits group separator character (if '_'). In some contexts it is treated as part of a floating sign, floating currency, or zero suppression string.

18/2 | \{AI95-00434-01\} An example of a picture String is "<####Z ZZ9.99>". If the currency string is "kr\$FF", the separator character is ',', and the radix mark is '.', then the edited output string values for the decimal values 32.10 and −5432.10 are "bbkr\$F bbb32.10b" and "(-bbkr\$F 5,432.10)" respectively, where 'b' indicates the space character.

19/2 | \{AI95-00285-01\} The generic packages Text_IO.Decimal_IO, and Wide_Text_IO.Decimal_IO (see A.10.9, “Input-Output for Real Types”) provide text input and nonedited text output for decimal types.

20/2 | NOTE \{AI95-00285-01\} A picture String is of type Standard.String, for all of Text_IO.Editing, and Wide_Text_IO.Editing.

Wording Changes from Ada 95

F.3.1 Picture String Formation

\{AI05-0299-1\} A well-formed picture String, or simply picture String, is a String value that conforms to the syntactic rules, composition constraints, and character replication conventions specified in this subclause.
Dynamic Semantics

This paragraph was deleted.

picture_string ::=  
  fixed_$_picture_string  
  | fixed.tencent#_picture_string  
  | floating_currency_picture_string  
  | non_currency_picture_string

fixed_$_picture_string ::=  
  [fixed_LHS_sign] fixed_$_char {direct_insertion} [zero_suppression]  
    number [RHS_sign]  
  | [fixed_LHS_sign {direct_insertion};] [zero_suppression]  
    number fixed_$_char {direct_insertion} [RHS_sign]  
  | floating_LHS_sign number fixed_$_char {direct_insertion} [RHS_sign]  
  | [fixed_LHS_sign] fixed_$_char {direct_insertion}  
    all_zero_suppression_number {direct_insertion} [RHS_sign]  
  | [fixed_LHS_sign {direct_insertion};] all_zero_suppression_number {direct_insertion}  
    fixed_$_char {direct_insertion} [RHS_sign]  
  | all_sign_number {direct_insertion} fixed_$_char {direct_insertion} [RHS_sign]

fixed.tencent#_picture_string ::=  
  [fixed_LHS_sign] single_#_currency {direct_insertion}  
    [zero_suppression] number [RHS_sign]  
  | [fixed_LHS_sign] multiple_#_currency {direct_insertion}  
    zero_suppression number [RHS_sign]  
  | [fixed_LHS_sign {direct_insertion};] [zero_suppression]  
    number fixed_#_currency {direct_insertion} [RHS_sign]  
  | floating_LHS_sign number fixed_#_currency {direct_insertion} [RHS_sign]  
  | [fixed_LHS_sign] single_#_currency {direct_insertion}  
    all_zero_suppression_number {direct_insertion} [RHS_sign]  
  | [fixed_LHS_sign] multiple_#_currency {direct_insertion}  
    all_zero_suppression_number {direct_insertion} [RHS_sign]  
  | [fixed_LHS_sign {direct_insertion};] all_zero_suppression_number {direct_insertion}  
    fixed_#_currency {direct_insertion} [RHS_sign]  
  | all_sign_number {direct_insertion} fixed_#_currency {direct_insertion} [RHS_sign]
floating_currency_picture_string ::= 
  [fixed_LHS_sign] {direct_insertion} floating_$_currency number [RHS_sign]
  | [fixed_LHS_sign] {direct_insertion} floating_#_currency number [RHS_sign]
  | [fixed_LHS_sign] {direct_insertion} all_currency_number {direct_insertion} [RHS_sign]

non_currency_picture_string ::= 
  [fixed_LHS_sign {direct_insertion}] zero_suppression number [RHS_sign]
  | [floating_LHS_sign] number [RHS_sign]
  | [fixed_LHS_sign {direct_insertion}] all_zero_suppression_number {direct_insertion} [RHS_sign]
  | all_sign_number {direct_insertion}
  | fixed_LHS_sign direct_insertion {direct_insertion} number [RHS_sign]

fixed_LHS_sign ::= LHS_Sign
LHS_Sign ::= + | – | <

fixed_$_char ::= $

direct_insertion ::= simple_insertion
simple_insertion ::= _ | B | 0 | /

zero_suppression ::= Z {Z | context_sensitive_insertion} | fill_string
context_sensitive_insertion ::= simple_insertion

fill_string ::= * {* | context_sensitive_insertion}

number ::= 
  fore_digits [radix [aft_digits] {direct_insertion}]
  | radix aft_digits {direct_insertion}
fore_digits ::= 9 {9 | direct_insertion}
aft_digits ::= {9 | direct_insertion} 9
radix ::= . | V

RHS_sign ::= + | – | > | CR | DB

floating_LHS_sign ::= 
  LHS_Sign {context_sensitive_insertion} LHS_Sign {LHS_Sign | context_sensitive_insertion}

single_#_currency ::= #
multiple_#_currency ::= ## {#}
fixed_#_currency ::= single_#_currency | multiple_#_currency

floating_$_currency ::= $ {context_sensitive_insertion} $ {$ | context_sensitive_insertion}

floating_#_currency ::= # {context_sensitive_insertion} # {# | context_sensitive_insertion}

all_sign_number ::= all_sign_fore [radix [all_sign_aft]] [>

all_sign_fore ::= sign_char {context_sensitive_insertion} sign_char {sign_char | context_sensitive_insertion}

all_sign_aft ::= {all_sign_aft_char} sign_char

all_sign_aft_char ::= sign_char | context_sensitive_insertion

sign_char ::= + | – | <

all_currency_number ::= all_currency_fore [radix [all_currency_aft]]

all_currency_fore ::= currency_char {context_sensitive_insertion}

all_currency_aft ::= {all_currency_aft_char} currency_char

all_currency_aft_char ::= currency_char | context_sensitive_insertion

currency_char ::= $ | #

all_zero_suppression_number ::= all_zero_suppression_fore [ radix [all_zero_suppression_aft]]

all_zero_suppression_fore ::= zero_suppression_char {zero_suppression_char | context_sensitive_insertion}

all_zero_suppression_aft ::= {all_zero_suppression_aft_char} zero_suppression_char

all_zero_suppression_aft_char ::= zero_suppression_char | context_sensitive_insertion

zero_suppression_char ::= Z | *

The following composition constraints apply to a picture String:
• A floating_LHS_sign does not have occurrences of different LHS_Sign Character values.
• If a picture String has '<' as fixed_LHS_sign, then it has '>' as RHS_sign.
• If a picture String has '<' in a floating_LHS_sign or in an all_sign_number, then it has an occurrence of '>'.
• {8652/0088} {AI95-00153} If a picture String has '+' or '-' as fixed_LHS_sign, in a floating_LHS_sign, or in an all_sign_number, then it has no RHS_sign or '>' character.
• An instance of all_sign_number does not have occurrences of different sign_char Character values.
• An instance of `all_currency_number` does not have occurrences of different `currency_char` Character values.

• An instance of `all_zero_suppression_number` does not have occurrences of different `zero-suppression_char` Character values, except for possible case differences between 'Z' and 'z'.

A replicable Character is a Character that, by the above rules, can occur in two consecutive positions in a picture String.

A Character replication is a String

\[ \text{char} \& \ (' \& \text{spaces} \& \text{count_string} \& ') \]

where `char` is a replicable Character, `spaces` is a String (possibly empty) comprising only space Character values, and `count_string` is a String of one or more decimal digit Character values. A Character replication in a picture String has the same effect as (and is said to be equivalent to) a String comprising \( n \) consecutive occurrences of `char`, where \( n = \text{Integer'Value(count_string)} \).

An expanded picture String is a picture String containing no Character replications.

Discussion: Since 'B' is not allowed after a RHS sign, there is no need for a special rule to disallow "9.99DB(2)" as an abbreviation for "9.99DBB".

NOTE Although a sign to the left of the number can float, a sign to the right of the number is in a fixed position.

Wording Changes from Ada 95

{8652/0088} {AI95-00153-01} Corrigendum: The picture string rules for numbers were tightened.

### F.3.2 Edited Output Generation

**Dynamic Semantics**

The contents of an edited output string are based on:

• A value, `Item`, of some decimal type `Num`,

• An expanded picture String `Pic_String`,

• A Boolean value, `Blank_When_Zero`,

• A Currency string,

• A Fill character,

• A Separator character, and

• A Radix_Mark character.

The combination of a True value for `Blank_When_Zero` and a '*' character in `Pic_String` is inconsistent; no edited output string is defined.

Reason: {AI95-00114-01} Such a `Pic_String` is invalid, and any attempt to use such a string will raise Picture_Error.

A layout error is identified in the rules below if leading nonzero digits of `Item`, character values of the Currency string, or a negative sign would be truncated; in such cases no edited output string is defined.

The edited output string has lower bound 1 and upper bound \( N \) where \( N = \text{Pic_String'}\text{Length} + \text{Currency-Length_Adjustment} - \text{Radix_Adjustment} \), and

- `Currency-Length_Adjustment = Currency'Length - 1` if there is some occurrence of '$' in `Pic_String`, and 0 otherwise.

- `Radix_Adjustment = 1` if there is an occurrence of 'V' or 'v' in `Pic_Str`, and 0 otherwise.
Let the magnitude of Item be expressed as a base-10 number \( I_p \cdots I_1. F_1 \cdots F_q \), called the displayed magnitude of Item, where:

- \( q = \min(\max(\text{Num'Scale}, 0), n) \) where \( n \) is 0 if Pic_String has no radix and is otherwise the number of digit positions following radix in Pic_String, where a digit position corresponds to an occurrence of '9', a zero_suppression_char (for an all_zero_suppression_number), a currency_char (for an all_currency_number), or a sign_char (for an all_sign_number).
- \( I_p \neq 0 \) if \( p > 0 \).

If \( n < \text{Num'Scale} \), then the above number is the result of rounding (away from 0 if exactly midway between values).

If Blank_When_Zero = True and the displayed magnitude of Item is zero, then the edited output string comprises all space character values. Otherwise, the picture String is treated as a sequence of instances of syntactic categories based on the rules in F.3.1, and the edited output string is the concatenation of string values derived from these categories according to the following mapping rules.

\{AI12-0451-1\} Table F.1F-1 shows the mapping from a sign control symbol to a corresponding character or string in the edited output. In the columns showing the edited output, a lower-case 'b' represents the space character. If there is no sign control symbol but the value of Item is negative, a layout error occurs and no edited output string is produced.

<table>
<thead>
<tr>
<th>Sign Control Symbol</th>
<th>Edited Output for Nonnegative Number</th>
<th>Edited Output for Negative Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>'+'</td>
<td>'+'</td>
<td>'-'</td>
</tr>
<tr>
<td>'-'</td>
<td>'b'</td>
<td>'</td>
</tr>
<tr>
<td>'&lt;'</td>
<td>'b'</td>
<td>'('</td>
</tr>
<tr>
<td>'&gt;'</td>
<td>'b'</td>
<td>')'</td>
</tr>
<tr>
<td>&quot;CR&quot;</td>
<td>&quot;bb&quot;</td>
<td>&quot;CR&quot;</td>
</tr>
<tr>
<td>&quot;DB&quot;</td>
<td>&quot;bb&quot;</td>
<td>&quot;DB&quot;</td>
</tr>
</tbody>
</table>

\{AI12-0451-1\} An instance of fixed_LHS_sign maps to a character as shown in Table F.1F-1.

An instance of fixed_$_char maps to Currency.

An instance of direct_insertion maps to Separator if direct_insertion = '\_', and to the direct_insertion Character otherwise.

An instance of number maps to a string \( \text{integer_part} \& \text{radix_part} \& \text{fraction_part} \) where:

- The string for \( \text{integer_part} \) is obtained as follows:
  1. Occurrences of '9' in fore_digits of number are replaced from right to left with the decimal digit character values for \( I_1, ..., I_p \), respectively.
  2. Each occurrence of '9' in fore_digits to the left of the leftmost '9' replaced according to rule 1 is replaced with '0'.
  3. If \( p \) exceeds the number of occurrences of '9' in fore_digits of number, then the excess leftmost digits are eligible for use in the mapping of an instance of zero_suppression,
floating_LHS_sign, floating_${ currency}, or floating_#_currency to the left of number; if there is no such instance, then a layout error occurs and no edited output string is produced.

- The *radix_part* is:
  - "" if number does not include a radix, if radix = 'V', or if radix = 'v'
  - Radix_Mark if number includes '.' as radix

- The string for *fraction_part* is obtained as follows:
  1. Occurrences of '9' in *aft_digits* of number are replaced from left to right with the decimal digit character values for F₁, ... Fₚ.
  2. Each occurrence of '9' in *aft_digits* to the right of the rightmost '9' replaced according to rule 1 is replaced by '0'.

An instance of *zero_suppression* maps to the string obtained as follows:

1. The rightmost 'Z', 'z', or '*' Character values are replaced with the excess digits (if any) from the *integer_part* of the mapping of the number to the right of the *zero_suppression* instance,
2. A context_sensitive_insertion Character is replaced as though it were a direct_insertion Character, if it occurs to the right of some 'Z', 'z', or '*' in *zero_suppression* that has been mapped to an excess digit,
3. Each Character to the left of the leftmost Character replaced according to rule 1 above is replaced by:
   - the space character if the zero suppression Character is 'Z' or 'z', or
   - the Fill character if the zero suppression Character is '*'.
4. A layout error occurs if some excess digits remain after all 'Z', 'z', and '*' Character values in *zero_suppression* have been replaced via rule 1; no edited output string is produced.

An instance of *RHS_sign* maps to a character or string as shown in Table F.1.

An instance of floating_LHS_sign maps to the string obtained as follows.

1. Up to all but one of the rightmost LHS_Sign Character values are replaced by the excess digits (if any) from the *integer_part* of the mapping of the number to the right of the *floating_LHS_sign* instance,
2. The next Character to the left is replaced with the character given by the entry in Table F.1F-1 corresponding to the LHS_Sign Character.
3. A context_sensitive_insertion Character is replaced as though it were a direct_insertion Character, if it occurs to the right of the leftmost LHS_Sign character replaced according to rule 1.
4. Any other Character is replaced by the space character.
5. A layout error occurs if some excess digits remain after replacement via rule 1; no edited output string is produced.

An instance of fixed_#_currency maps to the Currency string with n space character values concatenated on the left (if the instance does not follow a radix) or on the right (if the instance does follow a radix), where n is the difference between the length of the fixed_#_currency instance and Currency'Length. A layout error occurs if Currency'Length exceeds the length of the fixed_#_currency instance; no edited output string is produced.

An instance of floating_${ currency} maps to the string obtained as follows:
1. Up to all but one of the rightmost 'S' Character values are replaced with the excess digits (if any) from the integer_part of the mapping of the number to the right of the floating_$_currency instance.

2. The next Character to the left is replaced by the Currency string.

3. A context_sensitive_insertion Character is replaced as though it were a direct_insertion Character, if it occurs to the right of the leftmost 'S' Character replaced via rule 1.

4. Each other Character is replaced by the space character.

5. A layout error occurs if some excess digits remain after replacement by rule 1; no edited output string is produced.

An instance of floating_$_currency maps to the string obtained as follows:

1. Up to all but one of the rightmost '#' Character values are replaced with the excess digits (if any) from the integer_part of the mapping of the number to the right of the floating_$_currency instance.

2. The substring whose last Character occurs at the position immediately preceding the leftmost Character replaced via rule 1, and whose length is Currency'Length, is replaced by the Currency string.

3. A context_sensitive_insertion Character is replaced as though it were a direct_insertion Character, if it occurs to the right of the leftmost '#' replaced via rule 1.

4. Any other Character is replaced by the space character.

5. A layout error occurs if some excess digits remain after replacement rule 1, or if there is no substring with the required length for replacement rule 2; no edited output string is produced.

An instance of all_zero_suppression_number maps to:

- a string of all spaces if the displayed magnitude of Item is zero, the zero_suppression_char is 'Z' or 'z', and the instance of all_zero_suppression_number does not have a radix at its last character position;

- a string containing the Fill character in each position except for the character (if any) corresponding to radix, if zero_suppression_char = '*' and the displayed magnitude of Item is zero;

- otherwise, the same result as if each zero_suppression_char in all_zero_suppression_aft were '9', interpreting the instance of all_zero_suppression_number as either zero_suppression_number (if a radix and all_zero_suppression_aft are present), or as zero_suppression otherwise.

An instance of all_sign_number maps to:

- a string of all spaces if the displayed magnitude of Item is zero and the instance of all_sign_number does not have a radix at its last character position;

- otherwise, the same result as if each sign_char in all_sign_number_aft were '9', interpreting the instance of all_sign_number as either floating_LHS_sign_number (if a radix and all_sign_number_aft are present), or as floating_LHS_sign otherwise.

An instance of all_currency_number maps to:

- a string of all spaces if the displayed magnitude of Item is zero and the instance of all_currency_number does not have a radix at its last character position;

- otherwise, the same result as if each currency_char in all_currency_number_aft were '9', interpreting the instance of all_currency_number as floating_$_currency number or
floating_#_currency number (if a radix and all_currency_number_aft are present), or as floating_$_currency or floating_#_currency otherwise.

Examples

<table>
<thead>
<tr>
<th>Item:</th>
<th>Picture and Result Strings:</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456.78</td>
<td>Picture: &quot;-### *** **9.99&quot;</td>
</tr>
<tr>
<td></td>
<td>Result: &quot;bbF***123,456,78&quot; (currency = &quot;F&quot;, separator = &quot;,&quot;, radix mark = &quot;,&quot;)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item:</th>
<th>Picture and Result Strings:</th>
</tr>
</thead>
</table>
| 0.0   | Picture: 
|       | Result: "bbbbbbbbbb" |
| 0.20  | Picture: 
|       | Result: "bbbbbb8.20" |
| -1234.565 | Picture: "<<< <<< <<< " |
|         | Result: "bb(1,234.57DMb)" (currency = "DM") |
| 12345.67 | Picture: "### ### ### **9.99" |
|         | Result: "bbCHF12,345.67" (currency = "CHF") |

Wording Changes from Ada 95

Corrigendum: Corrected the picture string example.

F.3.3 The Package Text_IO.Editing

The package Text_IO.Editing provides a private type Picture with associated operations, and a generic package Decimal_Output. An object of type Picture is composed from a well-formed picture String (see F.3.1) and a Boolean item indicating whether a zero numeric value will result in an edited output string of all space characters. The package Decimal_Output contains edited output subprograms implementing the effects defined in F.3.2.

Static Semantics

The library package Text_IO.Editing has the following declaration:

```ada
with Nonblocking, Global => in out synchronized is

type Picture is private;

function Valid (Pic_String      : in String; 
  Blank_When_Zero : in Boolean := False) return Boolean;

function To_Picture (Pic_String      : in String; 
  Blank_When_Zero : in Boolean := False) 
  return Picture;

function Pic_String      (Pic : in Picture) return String;
function Blank_When_Zero (Pic : in Picture) return Boolean;

Max_Picture_Length : constant := implementation_defined;

Picture_Error       : exception;
```

F.3.2 Edited Output Generation
Default_Currency : constant String := "$";
Default_Fill      : constant Character := '*';
Default_Separator : constant Character := ',';
Default_Radix_Mark: constant Character := '.';

generic
    type Num is delta <> digits <>;
    Default_Currency : in String := Text_IO.Editing.Default_Currency;
    Default_Fill      : in Character := Text_IO.Editing.Default_Fill;
    Default_Separator : in Character := Text_IO.Editing.Default_Separator;
    Default_Radix_Mark: in Character := Text_IO.Editing.Default_Radix_Mark;

package Decimal_Output is
    function Length (Pic      : in Picture;
                     Currency : in String := Default_Currency)
        return Natural;
    function Valid (Item     : in Num;
                    Pic      : in Picture;
                    Currency : in String := Default_Currency)
        return Boolean;
    function Image (Item       : in Num;
                    Pic        : in Picture;
                    Currency   : in String    := Default_Currency;
                    Fill       : in Character := Default_Fill;
                    Separator  : in Character := Default_Separator;
                    Radix_Mark : in Character := Default_Radix_Mark)
        return String;

    {AI12-0241-1} procedure Put (File       : in File_Type;
                                  Item       : in Num;
                                  Pic        : in Picture;
                                  Currency   : in String    := Default_Currency;
                                  Fill       : in Character := Default_Fill;
                                  Separator  : in Character := Default_Separator;
                                  Radix_Mark : in Character := Default_Radix_Mark)
        with Nonblocking => False;

    {AI12-0241-1} procedure Put (Item     : in Num;
                                  Pic        : in Picture;
                                  Currency   : in String    := Default_Currency;
                                  Fill       : in Character := Default_Fill;
                                  Separator  : in Character := Default_Separator;
                                  Radix_Mark : in Character := Default_Radix_Mark)
        with Nonblocking => False;

    procedure Put (To         : out String;
                   Item       : in Num;
                   Pic        : in Picture;
                   Currency   : in String    := Default_Currency;
                   Fill       : in Character := Default_Fill;
                   Separator  : in Character := Default_Separator;
                   Radix_Mark : in Character := Default_Radix_Mark);

end Decimal_Output;
private
    ... -- not specified by the language
end Ada.Text_IO.Editing;

Implementation defined: The value of Max_Picture_Length in the package Text_IO.Editing
The exception Constraint_Error is raised if the Image function or any of the Put procedures is invoked
with a null string for Currency.
function Valid (Pic_String : in String; Blank_When_Zero : in Boolean := False) return Boolean;

Valid returns True if Pic_String is a well-formed picture String (see F.3.1) the length of whose expansion does not exceed Max_Picture_Length, and if either Blank_When_Zero is False or Pic_String contains no '*'.

function To_Picture (Pic_String : in String; Blank_When_Zero : in Boolean := False) return Picture;

To_Picture returns a result Picture such that the application of the function Pic_String to this result yields an expanded picture String equivalent to Pic_String, and such that Blank_When_Zero applied to the result Picture is the same value as the parameter Blank_When_Zero. Picture_Error is raised if not Valid(Pic_String, Blank_When_Zero).

function Pic_String (Pic : in Picture) return String;

function Blank_When_Zero (Pic : in Picture) return Boolean;

If Pic is To_Picture(String_Item, Boolean_Item) for some String_Item and Boolean_Item, then:

- Pic_String(Pic) returns an expanded picture String equivalent to String_Item and with any lower-case letter replaced with its corresponding upper-case form, and
- Blank_When_Zero(Pic) returns Boolean_Item.

If Pic_1 and Pic_2 are objects of type Picture, then ""(Pic_1, Pic_2) is True when

- Pic_String(Pic_1) = Pic_String(Pic_2), and
- Blank_When_Zero(Pic_1) = Blank_When_Zero(Pic_2).

function Length (Pic : in Picture; Currency : in String := Default_Currency) return Natural;

Length returns Pic_String(Pic)'Length + Currency_Length_Adjustment – Radix_Adjustment where

- Currency_Length_Adjustment =
  - Currency'Length – 1 if there is some occurrence of '$' in Pic_String(Pic), and
  - 0 otherwise.
- Radix_Adjustment =
  - 1 if there is an occurrence of 'V' or 'v' in Pic_String(Pic), and
  - 0 otherwise.

function Valid (Item : in Num; Pic : in Picture; Currency : in String := Default_Currency) return Boolean;

Valid returns True if Image(Item, Pic, Currency) does not raise Layout_Error, and returns False otherwise.

function Image (Item : in Num; Pic : in Picture; Currency : in String := Default_Currency; Fill : in Character := Default_Fill; Separator : in Character := Default_Separator; Radix_Mark : in Character := Default_Radix_Mark) return String;
Image returns the edited output String as defined in F.3.2 for Item, Pic_String(Pic), Blank_When_Zero(Pic), Currency, Fill, Separator, and Radix_Mark. If these rules identify a layout error, then Image raises the exception Layout_Error.

**procedure** Put (File : in File_Type;
Item       : in Num;
Pic        : in Picture;
Currency   : in String := Default_Currency;
Fill       : in Character := Default_Fill;
Separator  : in Character := Default_Separator;
Radix_Mark : in Character := Default_Radix_Mark);

Each of these Put procedures outputs Image(Item, Pic, Currency, Fill, Separator, Radix_Mark) consistent with the conventions for Put for other real types in case of bounded line length (see A.10.6, “Get and Put Procedures”).

**procedure** Put (Item       : in Num;
Pic        : in Picture;
Currency   : in String := Default_Currency;
Fill       : in Character := Default_Fill;
Separator  : in Character := Default_Separator;
Radix_Mark : in Character := Default_Radix_Mark);

{AI05-0264-1} Put copies Image(Item, Pic, Currency, Fill, Separator, Radix_Mark) to the given string, right justified. Otherwise, unassigned Character values in To are assigned the space character. If To’Length is less than the length of the string resulting from Image, then Layout_Error is raised.

**Implementation Requirements**

Max_Picture_Length shall be at least 30. The implementation shall support currency strings of length up to at least 10, both for Default_Currency in an instantiation of Decimal_Output, and for Currency in an invocation of Image or any of the Put procedures.

**Discussion**: This implies that a picture string with character replications need not be supported (i.e., To_Picture will raise Picture_Error) if its expanded form exceeds 30 characters.

**NOTE 1** {AI12-0450-1} The rules for edited output are based on COBOL (ANSI X3.23:1985, endorsed by ISO as ISO 1989-1985), with the following differences:

- The COBOL provisions for picture string localization and for 'P' format are absent from Ada.
- The following Ada facilities are not in COBOL:
  - currency symbol placement after the number,
  - localization of edited output string for multi-character currency string values, including support for both length-preserving and length-expanding currency symbols in picture strings
  - localization of the radix mark, digits separator, and fill character, and
  - parenthesization of negative values.

{AI12-0450-1} The value of 30 for Max_Picture_Length is the same limit as in COBOL.

**Discussion**: {AI12-0450-1} The rules for edited output were based on the 1985 version of COBOL (ANSI X3.23:1985, endorsed by ISO as ISO 1989-1985), with the following differences:

- The COBOL provisions for picture string localization and for 'P' format are absent from Ada.
- The following Ada facilities are not in the 1985 version of COBOL:
  - currency symbol placement after the number,
F.3.3 The Package Text_IO.Editing

Static Semantics

The child package Text_IO.Editing has the same contents as Text_IO, except that:

- each occurrence of Character is replaced by Wide_Character,
- each occurrence of Text_IO is replaced by Wide_Text_IO,
- the subtype of Default_Currency is Wide_String rather than String, and
- each occurrence of String in the generic package Decimal_Output is replaced by Wide_String.

Implementation defined: The value of Max_Picture_Length in the package Text_IO.Editing

NOTE Each of the functions Text_IO.Editing.Valid, To_Picture, and Pic_String has String (versus Wide_String) as its parameter or result subtype, since a picture String is not localizable.

F.3.4 The Package Wide_Text_IO.Editing

Static Semantics

The child package Wide_Text_IO.Editing has the same contents as Text_IO.Editing, except that:

- each occurrence of Character is replaced by Wide_Character,
- each occurrence of Text_IO is replaced by Wide_Text_IO,
- the subtype of Default_Currency is Wide_String rather than String, and
- each occurrence of String in the generic package Decimal_Output is replaced by Wide_String.

Implementation defined: The value of Max_Picture_Length in the package Wide_Text_IO.Editing

NOTE Each of the functions Wide_Text_IO.Editing.Valid, To_Picture, and Pic_String has String (versus Wide_String) as its parameter or result subtype, since a picture String is not localizable.

F.3.5 The Package Wide_Wide_Text_IO.Editing

Static Semantics

The child package Wide_Wide_Text_IO.Editing has the same contents as Text_IO.Editing, except that:

- each occurrence of Character is replaced by Wide_Wide_Character,
- each occurrence of Text_IO is replaced by Wide_Wide_Text_IO,
- the subtype of Default_Currency is Wide_Wide_String rather than String, and
- each occurrence of String in the generic package Decimal_Output is replaced by Wide_Wide_String.

Implementation defined: The value of Max_Picture_Length in the package Wide_Wide_Text_IO.Editing

NOTE Each of the functions Wide_Wide_Text_IO.Editing.Valid, To_Picture, and Pic_String has String (versus Wide_Wide_String) as its parameter or result subtype, since a picture String is not localizable.

Extensions to Ada 95

Package Wide_Wide_Text_IO.Editing is new; it supports 32-bit character strings. (Shouldn't it have been "Widest_Text_IO.Editing"? :-)

52.e/5
- localization of edited output string for multi-character currency string values, including support for both length-preserving and length-expanding currency symbols in picture strings;
52.f/5
- localization of the radix mark, digits separator, and fill character; and
52.g/5
- parenthesization of negative values.
52.h/5

{AI12-0450-1} The value of 30 for Max_Picture_Length is the same limit as in COBOL.

Reason: There are several reasons we have not adopted the COBOL-style permission to provide a single-character replacement in the picture string for the ´$´ as currency symbol, or to interchange the roles of ´.´ and ´,´ in picture strings

- It would have introduced considerable complexity into Ada, as well as confusion between run-time and compile-time character interpretation, since picture Strings are dynamically computable in Ada, in contrast with COBOL
- Ada's rules for real literals provide a natural interpretation of ´.´ as digits separator and ´,´ for radix mark; it is not essential to allow these to be localized in picture strings, since Ada does not allow them to be localized in real literals.
- The COBOL restriction for the currency symbol in a picture string to be replaced by a single character currency symbol is a compromise solution. For general international usage a mechanism is needed to localize the edited output to be a multi-character currency string. Allowing a single-Character localization for the picture Character, and a multiple-character localization for the currency string, would be an unnecessary complication.

52.i

52.j

52.k

52.l

Annex G
(normative)
Numerics

The Numerics Annex specifies

- features for complex arithmetic, including complex I/O;
- a mode (“strict mode”), in which the predefined arithmetic operations of floating point and fixed point types and the functions and operations of various predefined packages have to provide guaranteed accuracy or conform to other numeric performance requirements, which the Numerics Annex also specifies;
- \{AI12-0445-1\} a mode (“relaxed mode”), in which there are no accuracy or other numeric performance requirements to be satisfied, as for implementations not conforming to the Numerics Annex;
- \{AI95-00296-01\} models of floating point and fixed point arithmetic on which the accuracy requirements of strict mode are based; and
- \{AI95-00296-01\} the definitions of the model-oriented attributes of floating point types that apply in the strict mode; and
- \{AI95-00296-01\} features for the manipulation of real and complex vectors and matrices.

Implementation Advice

\{AI05-0229-1\} If Fortran (respectively, C) is widely supported in the target environment, implementations supporting the Numerics Annex should provide the child package Interfaces.Fortran (respectively, Interfaces.C) specified in Annex B and should support a convention_identifier of Fortran (respectively, C) for in the Convention aspect interfacing pragmas (see Annex B), thus allowing Ada programs to interface with programs written in that language.

Implementation Advice: If Fortran (respectively, C) is supported in the target environment, then interfacing to Fortran (respectively, C) should be supported as specified in Annex B.

Extensions to Ada 83

This Annex is new to Ada 95.

G.1 Complex Arithmetic

Types and arithmetic operations for complex arithmetic are provided in Generic_Complex_Types, which is defined in G.1.1. Implementation-defined approximations to the complex analogs of the mathematical functions known as the “elementary functions” are provided by the subprograms in Generic_Complex_Elementary_Functions, which is defined in G.1.2. Both of these library units are generic children of the predefined package Numerics (see A.5). Nongeneric equivalents of these generic packages for each of the predefined floating point types are also provided as children of Numerics.

Implementation defined: The accuracy actually achieved by the complex elementary functions and by other complex arithmetic operations.

Discussion: Complex arithmetic is defined in the Numerics Annex, rather than in the core, because it is considered to be a specialized need of (some) numeric applications.
G.1.1 Complex Types

Static Semantics

The generic library package Numerics.Generic_Complex_Types has the following declaration:

```ada
package Ada.Numerics.Generic_Complex_Types is
withpragma Pure, Nonblocking is(Generic_Complex_Types);

type Complex is
  record
    Re, Im : Real'Base;
  end record;

withpragma Preelaborable_Initialization(Imaginary);

i : constant Imaginary;
withpragma Preelaborable_Initialization(Imaginary);

j : constant Imaginary;

function Re (X : Complex) return Real'Base;
function Im (X : Complex) return Real'Base;
function Im (X : Imaginary) return Real'Base;

procedure Set_Re (X  : in out Complex;
  Re : in Real'Base);
procedure Set_Im (X  : in out Complex;
  Im : in Real'Base);
procedure Set_Im (X  : out Imaginary;
  Im : in Real'Base);

function Compose_From_Cartesian (Re, Im : Real'Base) return Complex;
function Compose_From_Cartesian (Re : Real'Base) return Complex;
function Compose_From_Cartesian (Im : Imaginary) return Complex;

function Modulus (X : Complex) return Real'Base;
function "abs" (Right : Complex) return Real'Base renames Modulus;
function Argument (X : Complex) return Real'Base;
function Argument (X : Complex;
  Cycle : Real'Base) return Real'Base;

function Compose_From_Polar (Modulus, Argument : Real'Base) return Complex;
function Compose_From_Polar (Modulus, Argument, Cycle : Real'Base) return Complex;

function "+" (Right : Complex) return Complex;
function "+" (Right : Complex) return Complex;
function Conjugate (X : Complex) return Complex;

function "+" (Left, Right : Complex) return Complex;
function "+" (Left, Right : Complex) return Complex;
function "**" (Left, Right : Complex) return Complex;
function "/" (Left, Right : Complex) return Complex;

function "***" (Left : Complex; Right : Integer) return Complex;

function "+" (Right : Imaginary) return Imaginary;
function "-" (Right : Imaginary) return Imaginary;
function Conjugate (X : Imaginary) return Imaginary renames "+-";
function "abs" (Right : Imaginary) return Real'Base;

function "+" (Left, Right : Imaginary) return Imaginary;
function "+" (Left, Right : Imaginary) return Imaginary;
function "+" (Left, Right : Imaginary) return Real'Base;
function "+" (Left, Right : Imaginary) return Real'Base;

function "***" (Left : Imaginary; Right : Integer) return Complex;
```
type Imaginary is new Real'Base;  
i : constant Imaginary := 1.0;  
j : constant Imaginary := 1.0;  
end Ada.Numerics.Generic_Complex_Types;  

The library package Numerics.Complex_Types is declared pure and 
defines the same types, constants, and subprograms as Numerics.Generic_Complex_Types, except that 
the predefined type Float is systematically substituted for Real'Base throughout. Nongeneric equivalents 
of Numerics.Generic_Complex_Types for each of the other predefined floating point types are defined 
similarly, with the names Numerics.Short_Complex_Types, Numerics.Long_Complex_Types, etc.

Reason: The nongeneric equivalents are provided to allow the programmer to construct simple mathematical 
applications without being required to understand and use generics. 

Reason: The nongeneric equivalents all export the types Complex and Imaginary and the constants i and j (rather than 
uniquely named types and constants, such as Short_Complex, Long_Complex, etc.) to preserve their equivalence to 
actual instantiations of the generic package and to allow the programmer to change the precision of an application 
globally by changing a single context clause.

Ramification: A pure unit is always nonblocking, so we don't need to talk about the Nonblocking 
aspect of these packages. Similarly, a pure unit always has the Global aspect set to null, so we don't need to talk about 
that, either.

Complex is a visible type with Cartesian components.

Reason: The Cartesian representation is far more common than the polar representation, in practice. The 
accuracy of the results of the complex arithmetic operations and of the complex elementary functions is dependent on 
the representation; thus, implementers need to know that representation. The type is visible so that complex “literals” 
can be written in aggregate notation, if desired.

Imaginary is a private type; its full type is derived from Real'Base.

Reason: The Imaginary type and the constants i and j are provided for two reasons:

- They allow complex “literals” to be written in the alternate form of \( a + b^*i \) (or \( a + b^*j \)), if desired. Of course, 
in some contexts the sum will need to be parenthesized.
When an Ada binding to ISO/IEC 60559:2020 that provides (signed) infinities as the result of operations that overflow becomes available, it will be important to allow arithmetic between pure-imaginary and complex operands without requiring the former to be represented as (or promoted to) complex values with a real component of zero. For example, the multiplication of \( a + b^* i \) by \( d^* i \) should yield \(-b \cdot d + a \cdot d^* i \), but if one cannot avoid representing the pure-imaginary value \( d^* i \) as the complex value \( 0.0 + d^* i \), then a NaN ("Not-a-Number") could be produced as the result of multiplying \( a \) by \( 0.0 \) (for example, when \( a \) is infinite); the NaN could later trigger an exception. Providing the Imaginary type and overloading of the arithmetic operators for mixtures of Imaginary and Complex operands gives the programmer the same control over avoiding premature coercion of pure-imaginary values to complex as is already provided for pure-real values.

**Reason:** The Imaginary type is private, rather than being visibly derived from Real'Base, for two reasons:

- to preclude implicit conversions of real literals to the Imaginary type (such implicit conversions would make many common arithmetic expressions ambiguous); and
- to suppress the implicit derivation of the multiplication, division, and absolute value operators with Imaginary operands and an Imaginary result (the result type would be incorrect).

**Reason:** The base subtype Real'Base is used for the component type of Complex, the parent type of Imaginary, and the parameter and result types of some of the subprograms to maximize the chances of being able to pass meaningful values into the subprograms and receive meaningful results back. The generic formal parameter Real therefore plays only one role, that of providing the precision to be maintained in complex arithmetic calculations. Thus, the subprograms in Numerics.Generic_Complex_Types share with those in Numerics.Generic_Elementary_Functions, and indeed even with the predefined arithmetic operations (see 4.5), the property of being free of range checks on input and output, that is, of being able to exploit the base range of the relevant floating point type fully. As a result, the user loses the ability to impose application-oriented bounds on the range of values that the components of a complex variable can acquire; however, it can be argued that few, if any, applications have a naturally square domain (as opposed to a circular domain) anyway.

The arithmetic operations and the Re, Im, Modulus, Argument, and Conjugate functions have their usual mathematical meanings. When applied to a parameter of pure-imaginary type, the “imaginary-part” function Im yields the value of its parameter, as the corresponding real value. The remaining subprograms have the following meanings:

**Reason:** The middle case can be understood by considering the parameter of pure-imaginary type to represent a complex value with a zero real part.

- The Set_Re and Set_Im procedures replace the designated component of a complex parameter with the given real value; applied to a parameter of pure-imaginary type, the Set_Im procedure replaces the value of that parameter with the imaginary value corresponding to the given real value.

- The Compose_From_Cartesian function constructs a complex value from the given real and imaginary components. If only one component is given, the other component is implicitly zero.

- The Compose_From_Polar function constructs a complex value from the given modulus (radius) and argument (angle). When the value of the parameter Modulus is positive (resp., negative), the result is the complex value represented by the point in the complex plane lying at a distance from the origin given by the absolute value of Modulus and forming an angle measured counterclockwise from the positive (resp., negative) real axis given by the value of the parameter Argument.

When the Cycle parameter is specified, the result of the Argument function and the parameter Argument of the Compose_From_Polar function are measured in units such that a full cycle of revolution has the given value; otherwise, they are measured in radians.

The computed results of the mathematically multivalued functions are rendered single-valued by the following conventions, which are meant to imply the principal branch:

- The result of the Modulus function is nonnegative.

- The result of the Argument function is in the quadrant containing the point in the complex plane represented by the parameter X. This may be any quadrant (I through IV); thus, the range of the Argument function is approximately \(-\pi\) to \(\pi\) (–Cycle/2.0 to Cycle/2.0, if the parameter Cycle is
specified). When the point represented by the parameter X lies on the negative real axis, the result approximates

- $\pi$ (resp., $-\pi$) when the sign of the imaginary component of X is positive (resp., negative), if Real'Signed_Zeros is True;
- $\pi$, if Real'Signed_Zeros is False.

- Because a result lying on or near one of the axes may not be exactly representable, the approximation inherent in computing the result may place it in an adjacent quadrant, close to but on the wrong side of the axis.

Dynamic Semantics

The exception Numerics.Argument_Error is raised by the Argument and Compose_From_Polar functions with specified cycle, signaling a parameter value outside the domain of the corresponding mathematical function, when the value of the parameter Cycle is zero or negative.

The exception Constraint_Error is raised by the division operator when the value of the right operand is zero, and by the exponentiation operator when the value of the left operand is zero and the value of the exponent is negative, provided that Real'Machine_Overflows is True; when Real'Machine_Overflows is False, the result is unspecified. [Constraint_Error can also be raised when a finite result overflows (see G.2.6).]

Discussion: \{AI12-0437-1\} It is anticipated that an Ada binding to ISO/IEC 60559:2020 will be developed in the future. As part of such a binding, the Machine_Overflows attribute of a conformant floating point type will be specified to yield False, which will permit implementations of the complex arithmetic operations to deliver results with infinite components (and set the zero-divide flag defined by the binding) instead of raising Constraint_Error in overflow situations, when traps are disabled. Similarly, it is appropriate for the complex arithmetic operations to deliver results with infinite components (and set the zero-divide flag defined by the binding) instead of raising Constraint_Error in the situations defined above, when traps are disabled. Finally, such a binding should also specify the behavior of the complex arithmetic operations, when sensible, given operands with infinite components.

Implementation Requirements

In the implementation of Numerics.Generic_Complex_Types, the range of intermediate values allowed during the calculation of a final result shall not be affected by any range constraint of the subtype Real.

Implementation Note: Implementations of Numerics.Generic_Complex_Types written in Ada should therefore avoid declaring local variables of subtype Real; the subtype Real'Base should be used instead.

In the following cases, evaluation of a complex arithmetic operation shall yield the prescribed result, provided that the preceding rules do not call for an exception to be raised:

- The results of the Re, Im, and Compose_From_Cartesian functions are exact.
- The real (resp., imaginary) component of the result of a binary addition operator that yields a result of complex type is exact when either of its operands is of pure-imaginary (resp., real) type.
  
  Ramification: The result of the addition operator is exact when one of its operands is of real type and the other is of pure-imaginary type. In this particular case, the operator is analogous to the Compose_From_Cartesian function; it performs no arithmetic.

- The real (resp., imaginary) component of the result of a binary subtraction operator that yields a result of complex type is exact when its right operand is of pure-imaginary (resp., real) type.

- The real component of the result of the Conjugate function for the complex type is exact.

- When the point in the complex plane represented by the parameter X lies on the nonnegative real axis, the Argument function yields a result of zero.

Discussion: Argument(X + i*Y) is analogous to EF.ArcTan(Y, X), where EF is an appropriate instance of Numerics.Generic_Elementary_Functions, except when X and Y are both zero, in which case the former yields the value zero while the latter raises Numerics.Argument_Error.
• When the value of the parameter Modulus is zero, the Compose_From_Polar function yields a
result of zero.
• When the value of the parameter Argument is equal to a multiple of the quarter cycle, the result
of the Compose_From_Polar function with specified cycle lies on one of the axes. In this case,
one of its components is zero, and the other has the magnitude of the parameter Modulus.
• Exponentiation by a zero exponent yields the value one. Exponentiation by a unit exponent yields
the value of the left operand. Exponentiation of the value one yields the value one. Exponentiation
of the value zero yields the value zero, provided that the exponent is nonzero. When the left operand
is of pure-imaginary type, one component of the result of the exponentiation operator is zero.

When the result, or a result component, of any operator of Numerics.Generic_Complex_Types has a
mathematical definition in terms of a single arithmetic or relational operation, that result or result
component exhibits the accuracy of the corresponding operation of the type Real.

Other accuracy requirements for the Modulus, Argument, and Compose_From_Polar functions, and
accuracy requirements for the multiplication of a pair of complex operands or for division by a complex
operand, all of which apply only in the strict mode, are given in G.2.6.

The sign of a zero result or zero result component yielded by a complex arithmetic operation or function
is implementation defined when Real'Signed_Zeros is True.

Implementation defined: The sign of a zero result (or a component thereof) from any operator or function in
Numerics.Generic_Complex_Types, when Real'Signed_Zeros is True.

Implementation Permissions

{AI12-0444-1} The nongeneric equivalent packages can may, but need not, be actual instantiations of the
generic package for the appropriate predefined type, though that is not required.

{8652/0091} {AI95-00434-01} Implementations may obtain the result of exponentiation of a complex or
pure-imaginary operand by repeated complex multiplication, with arbitrary association of the factors and
with a possible final complex reciprocation (when the exponent is negative). Implementations are also
permitted to obtain the result of exponentiation of a complex operand, but not of a pure-imaginary
operand, by converting the left operand to a polar representation; exponentiating the modulus by the
given exponent; multiplying the argument by the given exponent, when the exponent is positive, or
dividing the argument by the absolute value of the given exponent, when the exponent is negative; and
reconverting to a Cartesian representation. Because of this implementation freedom, no accuracy
requirement is imposed on complex exponentiation (except for the prescribed results given above, which
apply regardless of the implementation method chosen).

Implementation Advice

{AI12-0437-1} Because the usual mathematical meaning of multiplication of a complex operand and a
real operand is that of the scaling of both components of the former by the latter, an implementation
should not perform this operation by first promoting the real operand to complex type and then
performing a full complex multiplication. In systems that, in the future, support an Ada binding to
ISO/IEC 60559:2020/IEC 559:1989, the latter technique will not generate the required result when one of
the components of the complex operand is infinite. (Explicit multiplication of the infinite component by
the zero component obtained during promotion yields a NaN that propagates into the final result.)
Analogous advice applies in the case of multiplication of a complex operand and a pure-imaginary
operand, and in the case of division of a complex operand by a real or pure-imaginary operand.

Implementation Advice: Mixed real and complex operations (as well as pure-imaginary and complex operations)
should not be performed by converting the real (resp. pure-imaginary) operand to complex.
Likewise, because the usual mathematical meaning of addition of a complex operand and a real operand is that the imaginary operand remains unchanged, an implementation should not perform this operation by first promoting the real operand to complex type and then performing a full complex addition. In implementations in which the Signed_Zeroes attribute of the component type is True (and which therefore conform to ISO/IEC 60559:2020 in regard to the handling of the sign of zero in predefined arithmetic operations), the latter technique will not generate the required result when the imaginary component of the complex operand is a negatively signed zero. (Explicit addition of the negative zero to the zero obtained during promotion yields a positive zero.) Analogous advice applies in the case of addition of a complex operand and a pure-imaginary operand, and in the case of subtraction of a complex operand and a real or pure-imaginary operand.

Implementations in which Real'Signed_Zeroes is True should attempt to provide a rational treatment of the signs of zero results and result components. As one example, the result of the Argument function should have the sign of the imaginary component of the parameter X when the point represented by that parameter lies on the positive real axis; as another, the sign of the imaginary component of the Compose_From_Polar function should be the same as (resp., the opposite of) that of the Argument parameter when that parameter has a value of zero and the Modulus parameter has a nonnegative (resp., negative) value.

**Implementation Advice:** If Real'Signed_Zeroes is True for Numerics.Generic_Complex_Types, a rational treatment of the signs of zero results and result components should be provided.

The semantics of Numerics.Generic_Complex_Types differs from Generic_Complex_Types as defined in ISO/IEC CD 13813 (for Ada 83) in the following ways:

- The generic package is a child of the package defining the Argument_Error exception.
- The nongeneric equivalents export types and constants with the same names as those exported by the generic package, rather than with names unique to the package.
- Implementations are not allowed to impose an optional restriction that the generic actual parameter associated with Real be unconstrained. (In view of the ability to declare variables of subtype Real'Base in implementations of Numerics.Generic_Complex_Types, this flexibility is no longer needed.)
- The dependence of the Argument function on the sign of a zero parameter component is tied to the value of Real'Signed_Zeroes.
- Conformance to accuracy requirements is conditional.

**Extensions to Ada 95**

**Amendment Correction:** Added a pragma Preelaborable_Initialization to type Imaginary, so that it can be used in preelaborated units.

**Corrigendum:** Explicitly stated that the nongeneric equivalents of Generic_Complex_Types are pure.

### G.1.2 Complex Elementary Functions

**Static Semantics**

The generic library package Numerics.Generic_Complex_Elementary_Functions has the following declaration:

```
with Ada.Numerics.Generic_Complex_Types;
generic
with package Complex_Types is
new Ada.Numerics.Generic_Complex_Types (<>);
use Complex_Types;
package Ada.Numerics.Generic_Complex_Elementary_Functions is
withpragma Pure, Nonblocking is (Generic_Complex_Elementary_Functions);
function Sqrt (X : Complex) return Complex;
function Log  (X : Complex) return Complex;
function Exp  (X : Complex) return Complex;
function Exp  (X : Imaginary) return Complex;
function "**" (Left : Complex;   Right : Complex) return Complex;
function "**" (Left : Complex;   Right : Real'Base) return Complex;
function "**" (Left : Real'Base; Right : Complex) return Complex;
function Sin (X : Complex) return Complex;
function Cos (X : Complex) return Complex;
function Tan (X : Complex) return Complex;
function Cot (X : Complex) return Complex;
function Arcsin (X : Complex) return Complex;
function Arccos (X : Complex) return Complex;
function Arctan (X : Complex) return Complex;
function Arccot (X : Complex) return Complex;
function Sinh (X : Complex) return Complex;
function Cosh (X : Complex) return Complex;
function Tanh (X : Complex) return Complex;
function Coth (X : Complex) return Complex;
function Arcsinh (X : Complex) return Complex;
function Arccosh (X : Complex) return Complex;
function Arctanh (X : Complex) return Complex;
function Arccoth (X : Complex) return Complex;
end Ada.Numerics.Generic_Complex_Elementary_Functions;

The library package Numerics.Complex_Elementary_Functions is declared pure and defines the same subprograms as Numerics.Generic_Complex_Elementary_Functions, except that the predefined type Float is systematically substituted for Real'Base, and the Complex and Imaginary types exported by Numerics.Complex_Types are systematically substituted for Complex and Imaginary, throughout. Nongeneric equivalents of Numerics.Generic_Complex_Elementary_Functions corresponding to each of the other predefined floating point types are defined similarly, with the names Numerics.Short_Complex_Elementary_Functions, Numerics.Long_Complex_Elementary_Functions, etc.

Reason: The nongeneric equivalents are provided to allow the programmer to construct simple mathematical applications without being required to understand and use generics.

The overloading of the Exp function for the pure-imaginary type is provided to give the user an alternate way to compose a complex value from a given modulus and argument. In addition to Compose_From_Polar(Rho, Theta) (see G.1.1), the programmer may write Rho * Exp(i * Theta).

The imaginary (resp., real) component of the parameter X of the forward hyperbolic (resp., trigonometric) functions and of the Exp function (and the parameter X, itself, in the case of the overloading of the Exp function for the pure-imaginary type) represents an angle measured in radians, as does the imaginary (resp., real) component of the result of the Log and inverse hyperbolic (resp., trigonometric) functions.

The functions have their usual mathematical meanings. However, the arbitrariness inherent in the placement of branch cuts, across which some of the complex elementary functions exhibit discontinuities, is eliminated by the following conventions:

- The imaginary component of the result of the Sqrt and Log functions is discontinuous as the parameter X crosses the negative real axis.
• The result of the exponentiation operator when the left operand is of complex type is discontinuous as that operand crosses the negative real axis.

• \{AI95-00185-01\} The real (resp., imaginary) component of the result of the Arcsin, and Arccos (resp., and Arctanh) functions is discontinuous as the parameter \( X \) crosses the real axis to the left of \(-1.0\) or the right of \(1.0\).

• \{AI95-00185-01\} The real (resp., imaginary) component of the result of the Arctan and (resp., Arcsinh functions) function is discontinuous as the parameter \( X \) crosses the imaginary axis below \(-i\) or above \(i\).

• \{AI95-00185-01\} The real component of the result of the Arccot function is discontinuous as the parameter \( X \) crosses the imaginary axis below \(-i\) or above \(i\).

• The imaginary component of the Arcsinh function is discontinuous as the parameter \( X \) crosses the real axis to the left of \(1.0\).

• The imaginary component of the result of the Arccoth function is discontinuous as the parameter \( X \) crosses the real axis between \(-1.0\) and \(1.0\).

Discussion: \{AI95-00185-01\} The branch cuts come from the fact that the functions in question are really multi-valued in the complex domain, and that we have to pick one principal value to be the result of the function. Evidently we have much freedom in choosing where the branch cuts lie. However, we are adhering to the following principles which seem to lead to the more natural definitions:

• A branch cut should not intersect the real axis at a place where the corresponding real function is well-defined (in other words, the complex function should be an extension of the corresponding real function).

• Because all the functions in question are analytic, to ensure power series validity for the principal value, the branch cuts should be invariant by complex conjugation.

• For odd functions, to ensure that the principal value remains an odd function, the branch cuts should be invariant by reflection in the origin.

\{AI95-00185-01\} The computed results of the mathematically multivalued functions are rendered single-valued by the following conventions, which are meant to imply that the principal branch is an analytic continuation of the corresponding real-valued function in Numerics.Generic_Elementary_Functions. (For Arctan and Arccot, the single-argument function in question is that obtained from the two-argument version by fixing the second argument to be its default value.):

• The real component of the result of the Sqrt and Arccosh functions is nonnegative.

• The same convention applies to the imaginary component of the result of the Log function as applies to the result of the natural-cycle version of the Argument function of Numerics.Generic_Complex_Types (see G.1.1).

• The range of the real (resp., imaginary) component of the result of the Arcsin and Arctan (resp., Arcsinh and Arctanh) functions is approximately \(-\pi/2.0\) to \(\pi/2.0\).

• The real (resp., imaginary) component of the result of the Arcos and Arccot (resp., Arccoth) functions ranges from \(0.0\) to approximately \(\pi\).

• The range of the imaginary component of the result of the Arcosh function is approximately \(-\pi\) to \(\pi\).

In addition, the exponentiation operator inherits the single-valuedness of the Log function.

Dynamic Semantics

The exception Numerics.Argument_Error is raised by the exponentiation operator, signaling a parameter value outside the domain of the corresponding mathematical function, when the value of the left operand is zero and the real component of the exponent (or the exponent itself, when it is of real type) is zero.
The exception Constraint_Error is raised, signaling a pole of the mathematical function (analogous to dividing by zero), in the following cases, provided that Complex_Types.Real'Machine_Overflows is True:

- by the Log, Cot, and Coth functions, when the value of the parameter X is zero;
- by the exponentiation operator, when the value of the left operand is zero and the real component of the exponent (or the exponent itself, when it is of real type) is negative;
- by the Arctan and Arccot functions, when the value of the parameter X is \( \pm i \);
- by the Arctanh and Arccoth functions, when the value of the parameter X is \( \pm 1.0 \).

[Constraint_Error can also be raised when a finite result overflows (see G.2.6); this may occur for parameter values sufficiently near poles, and, in the case of some of the functions, for parameter values having components of sufficiently large magnitude.] When Complex_Types.Real'Machine_Overflows is False, the result at poles is unspecified.

**Reason:** The purpose of raising Constraint_Error (rather than Numerics.Argument_Error) at the poles of a function, when Float_Type'Machine_Overflows is True, is to provide continuous behavior as the actual parameters of the function approach the pole and finally reach it.

**Discussion:** \{AI12-0437-1\} It is anticipated that an Ada binding to ISO/IEC 60559:2020/IEC 559:1989 will be developed in the future. As part of such a binding, the Machine_Overflows attribute of a conformant floating point type will be specified to yield False, which will permit implementations of the complex elementary functions to deliver results with an infinite component (and set the overflow flag defined by the binding) instead of raising Constraint_Error in overflow situations, when traps are disabled. Similarly, it is appropriate for the complex elementary functions to deliver results with an infinite component (and set the zero-divide flag defined by the binding) instead of raising Constraint_Error at poles, when traps are disabled. Finally, such a binding should also specify the behavior of the complex elementary functions, when sensible, given parameters with infinite components.

**Implementation Requirements**

In the implementation of Numerics.Generic_Complex_Elementary_Functions, the range of intermediate values allowed during the calculation of a final result shall not be affected by any range constraint of the subtype Complex_Types.Real.

**Implementation Note:** Implementations of Numerics.Generic_Complex_Elementary_Functions written in Ada should therefore avoid declaring local variables of subtype Complex_Types.Real; the subtype Complex_Types.Real'Base should be used instead.

In the following cases, evaluation of a complex elementary function shall yield the prescribed result (or a result having the prescribed component), provided that the preceding rules do not call for an exception to be raised:

- When the parameter X has the value zero, the Sqrt, Sin, Arcsin, Tan, Arctan, Sinh, Arcsinh, Tanh, and Arctanh functions yield a result of zero; the Exp, Cos, and Cosh functions yield a result of one; the Arccos and Arccot functions yield a real result; and the Arccoth function yields an imaginary result.
- When the parameter X has the value one, the Sqrt function yields a result of one; the Log, Arccos, and Arccosh functions yield a result of zero; and the Arcsin function yields a real result.
- When the parameter X has the value \( -1.0 \), the Sqrt function yields the result
  - \( i \) (resp., \(-i\)), when the sign of the imaginary component of X is positive (resp., negative), if Complex_Types.Real'Signed_Zeros is True;
  - \( i \), if Complex_Types.Real'Signed_Zeros is False;
- \{AI95-00434-01\} When the parameter X has the value \( -1.0 \), the Log function yields an imaginary result; and the Arcsin and Arccos functions yield a real result.
- When the parameter X has the value \( \pm i \), the Log function yields an imaginary result.
Exponentiation by a zero exponent yields the value one. Exponentiation by a unit exponent yields the value of the left operand (as a complex value). Exponentiation of the value one yields the value one. Exponentiation of the value zero yields the value zero.

**Discussion:** It is possible to give many other prescribed results restricting the result to the real or imaginary axis when the parameter X is appropriately restricted to easily testable portions of the domain. We follow the proposed ISO/IEC standard for Generic_Complex_Elementary_Functions (for Ada 83), CD 13813, in not doing so, however.

Other accuracy requirements for the complex elementary functions, which apply only in the strict mode, are given in G.2.6.

The sign of a zero result or zero result component yielded by a complex elementary function is implementation defined when Complex_Types.Real'Signed_Zeros is True.

**Implementation defined:** The sign of a zero result (or a component thereof) from any operator or function in Numerics.Generic_Complex_Elementary_Functions, when Complex_Types.Real'Signed_Zeros is True.

**Implementation Permissions**

The exponentiation operator may be implemented in terms of the Exp and Log functions. Because this implementation yields poor accuracy in some parts of the domain, no accuracy requirement is imposed on complex exponentiation.

The implementation of the Exp function of a complex parameter X is allowed to raise the exception Constraint_Error, signaling overflow, when the real component of X exceeds an unspecified threshold that is approximately \log(Complex_Types.Real'Safe_Last). This permission recognizes the impracticality of avoiding overflow in the marginal case that the exponential of the real component of X exceeds the safe range of Complex_Types.Real but both components of the final result do not. Similarly, the Sin and Cos (resp., Sinh and Cosh) functions are allowed to raise the exception Constraint_Error, signaling overflow, when the absolute value of the imaginary (resp., real) component of the parameter X exceeds an unspecified threshold that is approximately \log(Complex_Types.Real'Safe_Last) + \log(2.0). This permission recognizes the impracticality of avoiding overflow in the marginal case that the hyperbolic sine or cosine of the imaginary (resp., real) component of X exceeds the safe range of Complex_Types.Real but both components of the final result do not.

**Implementation Advice**

Implementations in which Complex_Types.Real'Signed_Zeros is True should attempt to provide a rational treatment of the signs of zero results and result components. For example, many of the complex elementary functions have components that are odd functions of one of the parameter components; in these cases, the result component should have the sign of the parameter component at the origin. Other complex elementary functions have zero components whose sign is opposite that of a parameter component at the origin, or is always positive or always negative.

**Implementation Advice:** If Complex_Types.Real'Signed_Zeros is True for Numerics.Generic_Complex_Elementary_Functions, a rational treatment of the signs of zero results and result components should be provided.

**Wording Changes from Ada 83**

The semantics of Numerics.Generic_Complex_Elementary_Functions differs from Generic_Complex_Elementary_Functions as defined in ISO/IEC CD 13814 (for Ada 83) in the following ways:

- The generic package is a child unit of the package defining the Argument_Error exception.
- The proposed Generic_Complex_Elementary_Functions standard (for Ada 83) specified names for the nongeneric equivalents, if provided. Here, those nongeneric equivalents are required.
The generic package imports an instance of Numerics.Generic_Complex_Types rather than a long list of individual types and operations exported by such an instance.

The dependence of the imaginary component of the Sqrt and Log functions on the sign of a zero parameter component is tied to the value of Complex_Types.Real'Signed_Zeros.

Conformance to accuracy requirements is conditional.

Wording Changes from Ada 95

\{8652/0020\} \{AI95-00126-01\} Corrigendum: Explicitly stated that the nongeneric equivalents of Generic_Complex_Elementary_Functions are pure.

\{AI95-00185-01\} Corrected various inconsistencies in the definition of the branch cuts.

G.1.3 Complex Input-Output

The generic package Text_IO.Complex_IO defines procedures for the formatted input and output of complex values. The generic actual parameter in an instantiation of Text_IO.Complex_IO is an instance of Numerics.Generic_Complex_Types for some floating point subtype. Exceptional conditions are reported by raising the appropriate exception defined in Text_IO.

Implementation Note: An implementation of Text_IO.Complex_IO can be built around an instance of Text_IO.Float_IO for the base subtype of Complex_Types.Real, where Complex_Types is the generic formal package parameter of Text_IO.Complex_IO. There is no need for an implementation of Text_IO.Complex_IO to parse real values.

Static Semantics

The generic library package Text_IO.Complex_IO has the following declaration:

Ramification: Because this is a child of Text_IO, the declarations of the visible part of Text_IO are directly visible within it.

\{AI12-0302-1\} with Ada.Numerics.Generic_Complex_Types;
generic
with package Complex_Types is
new Ada.Numerics.Generic_Complex_Types (<>);
package Ada.Text_IO.Complex_IO
   with Global => in out synchronized is
   use Complex_Types;
   Default_Fore : Field := 2;
   Default_Aft  : Field := Real'Digits - 1;
   Default_Exp  : Field := 3;
   procedure Get (File  : in File_Type;
                   Item  : out Complex;
                   Width : in Field := 0);
   procedure Get (Item  : out Complex;
                   Width : in Field := 0);
   procedure Put (File : in File_Type;
                  Item : in Complex;
                  Fore : in Field := Default_Fore;
                  Aft : in Field := Default_Aft;
                  Exp : in Field := Default_Exp);
   procedure Put (Item : in Complex;
                  Fore : in Field := Default_Fore;
                  Aft : in Field := Default_Aft;
                  Exp : in Field := Default_Exp);
procedure Get (From : in String;  
    Item : out Complex;  
    Last : out Positive)  
    with Nonblocking;  
procedure Put (To   : out String;  
    Item : in Complex;  
    Aft  : in Field := Default_Aft;  
    Exp  : in Field := Default_Exp)  
    with Nonblocking;

end Ada.Text_IO.Complex_IO;

The library package Complex_Text_IO defines the same subprograms as Text_IO.Complex_IO, except that the predefined type Float is systematically substituted for Real, and the type Numerics.Complex_Types.Complex is systematically substituted for Complex throughout. Nongeneric equivalents of Text_IO.Complex_IO corresponding to each of the other predefined floating point types are defined similarly, with the names Short_Complex_Text_IO, Long_Complex_Text_IO, etc.

Reason: The nongeneric equivalents are provided to allow the programmer to construct simple mathematical applications without being required to understand and use generics.

The semantics of the Get and Put procedures are as follows:

procedure Get (File  : in File_Type;  
    Item  : out Complex;  
    Width : in Field := 0);
procedure Get (Item  : out Complex;  
    Width : in Field := 0);

{8652/0092} {AI95-00029-01} The input sequence is a pair of optionally signed real literals representing the real and imaginary components of a complex value. These components have the format defined for the corresponding Get procedure of an instance of Text_IO.Float_IO (see A.10.9) for the base subtype of Complex_Types.Real. The optionally the pair of components may be separated by a comma and/or surrounded by a pair of parentheses or both. Blanks are freely allowed before each of the components and before the parentheses and comma, if either is used. If the value of the parameter Width is zero, then

- line and page terminators are also allowed in these places;
- the components shall be separated by at least one blank or line terminator if the comma is omitted; and
- reading stops when the right parenthesis has been read, if the input sequence includes a left parenthesis, or when the imaginary component has been read, otherwise.

If a nonzero value of Width is supplied, then

- the components shall be separated by at least one blank if the comma is omitted; and
- exactly Width characters are read, or the characters (possibly none) up to a line terminator, whichever comes first (blanks are included in the count).

Reason: The parenthesized and comma-separated form is the form produced by Put on output (see below), and also by list-directed output in Fortran. The other allowed forms match several common styles of edit-directed output in Fortran, allowing most preexisting Fortran data files containing complex data to be read easily. When such files contain complex values with no separation between the real and imaginary components, the user will have to read those components separately, using an instance of Text_IO.Float_IO.

Returns, in the parameter Item, the value of type Complex that corresponds to the input sequence.

The exception Text_IO.Data_Error is raised if the input sequence does not have the required syntax or if the components of the complex value obtained are not of the base subtype of Complex_Types.Real.
procedure Put (File : in File_Type;
    Item : in Complex;
    Fore : in Field := Default_Fore;
    Aft : in Field := Default_Aft;
    Exp : in Field := Default_Exp);
procedure Put (Item : in Complex;
    Fore : in Field := Default_Fore;
    Aft : in Field := Default_Aft;
    Exp : in Field := Default_Exp);

Outputs the value of the parameter Item as a pair of decimal literals representing the real and imaginary components of the complex value, using the syntax of an aggregate. More specifically,

- outputs a left parenthesis;
- outputs the value of the real component of the parameter Item with the format defined by the corresponding Put procedure of an instance of Text_IO.Float_IO for the base subtype of Complex_Types.Real, using the given values of Fore, Aft, and Exp;
- outputs a comma;
- outputs the value of the imaginary component of the parameter Item with the format defined by the corresponding Put procedure of an instance of Text_IO.Float_IO for the base subtype of Complex_Types.Real, using the given values of Fore, Aft, and Exp;
- outputs a right parenthesis.

Discussion: If the file has a bounded line length, a line terminator may be output implicitly before any element of the sequence itemized above.

Discussion: The option of outputting the complex value as a pair of reals without additional punctuation is not provided, since it can be accomplished by outputting the real and imaginary components of the complex value separately.

procedure Get (From : in String;
    Item : out Complex;
    Last : out Positive);

{AI95-00434-01} Reads a complex value from the beginning of the given string, following the same rule as the Get procedure that reads a complex value from a file, but treating the end of the string as a file line terminator. Returns, in the parameter Item, the value of type Complex that corresponds to the input sequence. Returns in Last the index value such that From(Last) is the last character read.

The exception Text_IO.Data_Error is raised if the input sequence does not have the required syntax or if the components of the complex value obtained are not of the base subtype of Complex_Types.Real.

procedure Put (To   : out String;
    Item : in Complex;
    Aft  : in Field := Default_Aft;
    Exp  : in Field := Default_Exp);

Outputs the value of the parameter Item to the given string as a pair of decimal literals representing the real and imaginary components of the complex value, using the syntax of an aggregate. More specifically,

- a left parenthesis, the real component, and a comma are left justified in the given string, with the real component having the format defined by the Put procedure (for output to a file) of an instance of Text_IO.Float_IO for the base subtype of Complex_Types.Real, using a value of zero for Fore and the given values of Aft and Exp;
- the imaginary component and a right parenthesis are right justified in the given string, with the imaginary component having the format defined by the Put procedure (for output
to a file) of an instance of Text_IO.Float_IO for the base subtype of Complex_Types.Real, using a value for Fore that completely fills the remainder of the string, together with the given values of Aft and Exp.

**Reason:** This rule is the one proposed in LSN-1051. Other rules were considered, including one that would have read "Outputs the value of the parameter Item to the given string, following the same rule as for output to a file, using a value for Fore such that the sequence of characters output exactly fills, or comes closest to filling, the string; in the latter case, the string is filled by inserting one extra blank immediately after the comma." While this latter rule might be considered the closest analogue to the rule for output to a string in Text_IO.Float_IO, it requires a more difficult and inefficient implementation involving special cases when the integer part of one component is substantially longer than that of the other and the string is too short to allow both to be preceded by blanks. Unless such a special case applies, the latter rule might produce better columnar output if several such strings are ultimately output to a file, but very nearly the same output can be produced by outputting to the file directly, with the appropriate value of Fore; in any case, it might validly be assumed that output to a string is intended for further computation rather than for display, so that the precise formatting of the string to achieve a particular appearance is not the major concern.

The exception Text_IO.Layout_Error is raised if the given string is too short to hold the formatted output.

**Implementation Permissions**

Other exceptions declared (by renaming) in Text_IO may be raised by the preceding procedures in the appropriate circumstances, as for the corresponding procedures of Text_IO.Float_IO.

**Extensions to Ada 95**

{AI95-00328-01} Nongeneric equivalents for Text_IO.Complex_IO are added, to be consistent with all other language-defined Numerics generic packages.

**Wording Changes from Ada 95**

{8652/0092} {AI95-0029-01} **Corrigendum:** Clarified that the syntax of values read by Complex_IO is the same as that read by Text_IO.Float_IO.

---

**G.1.4 The Package Wide_Text_IO.Complex_IO**

**Static Semantics**

Implementations shall also provide the generic library package Wide_Text_IO.Complex_IO. Its declaration is obtained from that of Text_IO.Complex_IO by systematically replacing Text_IO by Wide_Text_IO and String by Wide_String; the description of its behavior is obtained by additionally replacing references to particular characters (commas, parentheses, etc.) by those for the corresponding wide characters.

**G.1.5 The Package Wide_Wide_Text_IO.Complex_IO**

**Static Semantics**

{AI95-00285-01} Implementations shall also provide the generic library package Wide_Wide_Text_IO.Complex_IO. Its declaration is obtained from that of Text_IO.Complex_IO by systematically replacing Text_IO by Wide_Wide_Text_IO and String by Wide_Wide_String; the description of its behavior is obtained by additionally replacing references to particular characters (commas, parentheses, etc.) by those for the corresponding wide characters.

**Extensions to Ada 95**

{AI95-00285-01} **Package Wide_Wide_Text_IO.Complex_IO is new.** (At least it wasn't called Incredibly_Wide_Text_IO.Complex_IO; maybe next time.)
G.2 Numeric Performance Requirements

Implementation Requirements

Implementations shall provide a user-selectable mode in which the accuracy and other numeric performance requirements detailed in the following subclauses are observed. This mode, referred to as the strict mode, may or may not be the default mode; it directly affects the results of the predefined arithmetic operations of real types and the results of the subprograms in children of the Numerics package, and indirectly affects the operations in other language defined packages. Implementations shall also provide the opposing mode, which is known as the relaxed mode.

Reason: On the assumption that the users of an implementation that does not support the Numerics Annex have no particular need for numerical performance, such an implementation has no obligation to meet any particular requirements in this area. On the other hand, users of an implementation that does support the Numerics Annex are provided with a way of ensuring that their programs achieve a known level of numerical performance and that the performance is portable to other such implementations. The relaxed mode is provided to allow implementers to offer an efficient but not fully accurate alternative in the case that the strict mode entails a time overhead that some users may find excessive. In some of its areas of impact, the relaxed mode may be fully equivalent to the strict mode.

Implementation Note: The relaxed mode may, for example, be used to exploit the implementation of (some of) the elementary functions in hardware, when available. Such implementations often do not meet the accuracy requirements of the strict mode, or do not meet them over the specified range of parameter values, but compensate in other ways that may be important to the user, such as their extreme speed.

Ramification: For implementations supporting the Numerics Annex, the choice of mode has no effect on the selection of a representation for a real type or on the values of attributes of a real type.

Implementation Permissions

Either mode may be the default mode.

Implementation defined: Whether the strict mode or the relaxed mode is the default.

The two modes can be one and the same need not actually be different.

Extensions to Ada 83

The choice between strict and relaxed numeric performance was not available in Ada 83.

G.2.1 Model of Floating Point Arithmetic

In the strict mode, the predefined operations of a floating point type shall satisfy the accuracy requirements specified here and shall avoid or signal overflow in the situations described. This behavior is presented in terms of a model of floating point arithmetic that builds on the concept of the canonical form (see A.5.3).

Static Semantics

Associated with each floating point type is an infinite set of model numbers. The model numbers of a type are used to define the accuracy requirements that have to be satisfied by certain predefined operations of the type; through certain attributes of the model numbers, they are also used to explain the meaning of a user-declared floating point type declaration. The model numbers of a derived type are those of the parent type; the model numbers of a subtype are those of its type.

The model numbers of a floating point type T are zero and all the values expressible in the canonical form (for the type T), in which mantissa has T'Model_Mantissa digits and exponent has a value greater than or equal to T'Model_Emin. (These attributes are defined in G.2.2.)

Discussion: The model is capable of describing the behavior of most existing hardware that has a mantissa-exponent representation. As applied to a type T, it is parameterized by the values of T'Machine_Radix, T'Model_Mantissa,
T'Model_Emin, T'Safe_First, and T'Safe_Last. The values of these attributes are determined by how, and how well, the hardware behaves. They in turn determine the set of model numbers and the safe range of the type, which figure in the accuracy and range (overflow avoidance) requirements.

\{AI12-0453-1\} In hardware that is free of arithmetic anomalies, T'Model_Mantissa, T'Model_Emin, T'Safe_First, and T'Safe_Last will yield the same values as T'Machine_Mantissa, T'Machine_Emin, T'Base'First, and T'Base'Last, respectively, and the model numbers in the safe range of the type T will coincide with the machine numbers of the type T. In less perfect hardware, it is not possible for the model-oriented attributes to have these optimal values, since the hardware, by definition, and therefore the implementation, cannot conform to the stringencies of the resulting model; in this case, the values yielded by the model-oriented attributes have to be made more conservative (that is, have to be penalized), with the result that the model numbers are more widely separated than the machine numbers, and the safe range is a subrange of the base range. The implementation will then be able to conform to the requirements of the weaker model defined by the sparser set of model numbers and the smaller safe range.

A model interval of a floating point type is any interval whose bounds are model numbers of the type. The model interval of a type T associated with a value v is the smallest model interval of T that includes v. (The model interval associated with a model number of a type consists of that number only.)

Implementation Requirements

The accuracy requirements for the evaluation of certain predefined operations of floating point types are as follows.

**Discussion:** This subclause does not cover the accuracy of an operation of a static expression; such operations have to be evaluated exactly (see 4.9). It also does not cover the accuracy of the predefined attributes of a floating point subtype that yield a value of the type; such operations also yield exact results (see 3.5.8 and A.5.3).

An operand interval is the model interval, of the type specified for the operand of an operation, associated with the value of the operand.

For any predefined arithmetic operation that yields a result of a floating point type T, the required bounds on the result are given by a model interval of T (called the result interval) defined in terms of the operand values as follows:

- The result interval is the smallest model interval of T that includes the minimum and the maximum of all the values obtained by applying the (exact) mathematical operation to values arbitrarily selected from the respective operand intervals.

The result interval of an exponentiation is obtained by applying the above rule to the sequence of multiplications defined by the exponent, assuming arbitrary association of the factors, and to the final division in the case of a negative exponent.

The result interval of a conversion of a numeric value to a floating point type T is the model interval of T associated with the operand value, except when the source expression is of a fixed point type with a small that is not a power of T'Machine_Radix or is a fixed point multiplication or division either of whose operands has a small that is not a power of T'Machine_Radix; in these cases, the result interval is implementation defined.

**Implementation defined:** The result interval in certain cases of fixed-to-float conversion.

For any of the foregoing operations, the implementation shall deliver a value that belongs to the result interval when both bounds of the result interval are in the safe range of the result type T, as determined by the values of T'Safe_First and T'Safe_Last; otherwise,

- if T'Machine_Overflows is True, the implementation shall either deliver a value that belongs to the result interval or raise Constraint_Error;
- if T'Machine_Overflows is False, the result is implementation defined.

**Implementation defined:** The result of a floating point arithmetic operation in overflow situations, when the Machine_Overflows attribute of the result type is False.
For any predefined relation on operands of a floating point type T, the implementation may deliver any value (that is, either True or False) obtained by applying the (exact) mathematical comparison to values arbitrarily chosen from the respective operand intervals.

The result of a membership test is defined in terms of comparisons of the operand value with the lower and upper bounds of the given range or type mark (the usual rules apply to these comparisons).

Implementation Permissions

If the underlying floating point hardware implements division as multiplication by a reciprocal, the result interval for division (and exponentiation by a negative exponent) is implementation defined.

Implementation defined: The result interval for division (or exponentiation by a negative exponent), when the floating point hardware implements division as multiplication by a reciprocal.

Wording Changes from Ada 83

The Ada 95 model numbers of a floating point type that are in the safe range of the type are comparable to the Ada 83 safe numbers of the type. There is no analog of the Ada 83 model numbers. The Ada 95 model numbers, when not restricted to the safe range, are an infinite set.

Inconsistencies With Ada 83

Giving the model numbers the hardware radix, instead of always a radix of two, allows (in conjunction with other changes) some borderline declared types to be represented with less precision than in Ada 83 (that is, with single precision, whereas Ada 83 would have used double precision). Because the lower precision satisfies the requirements of the model (and did so in Ada 83 as well), this change is viewed as a desirable correction of an anomaly, rather than a worrisome inconsistency. (Of course, the wider representation chosen in Ada 83 also remains eligible for selection in Ada 95.)

As an example of this phenomenon, assume that Float is represented in single precision and that a double precision type is also available. Also assume hexadecimal hardware with clean properties, for example certain IBM hardware. Then,

```ada
type T is digits Float'Digits range -Float'Last .. Float'Last;
```

results in T being represented in double precision in Ada 83 and in single precision in Ada 95. The latter is intuitively correct; the former is counterintuitive. The reason why the double precision type is used in Ada 83 is that Float has model and safe numbers (in Ada 83) with 21 binary digits in their mantissas, as is required to model the hypothesized hexadecimal hardware using a binary radix; thus Float'Last, which is not a model number, is slightly outside the range of safe numbers of the single precision type, making that type ineligible for selection as the representation of T even though it provides adequate precision. In Ada 95, Float'Last (the same value as before) is a model number and is in the safe range of Float on the hypothesized hardware, making Float eligible for the representation of T.

Extensions to Ada 83

Giving the model numbers the hardware radix allows for practical implementations on decimal hardware.

Wording Changes from Ada 83

The wording of the model of floating point arithmetic has been simplified to a large extent.

G.2.2 Model-Oriented Attributes of Floating Point Types

In implementations that support the Numerics Annex, the model-oriented attributes of floating point types shall yield the values defined here, in both the strict and the relaxed modes. These definitions add conditions to those in A.5.3.

Static Semantics

For every subtype S of a floating point type T:

Yields the number of digits in the mantissa of the canonical form of the model numbers of T (see A.5.3). The value of this attribute shall be greater than or equal to \( \lceil d - \log(10) \rceil \).
\log(T'\text{Machine\_Radix}) + 1, \text{ where } d \text{ is the requested decimal precision of } T. \text{ In addition, it shall be less than or equal to the value of } T'\text{Machine\_Mantissa}. \text{ This attribute yields a value of the type } \text{universal\_integer}.

\left\lfloor d \cdot \log(10) / \log(T'\text{Machine\_Radix}) \right\rfloor + g 

\text{where } d \text{ is the requested decimal precision of } T, \text{ and } g \text{ is 0 if } T'\text{Machine\_Radix} \text{ is a positive power of } 10 \text{ and 1 otherwise. In addition, } T'\text{Model\_Mantissa} \text{ shall be less than or equal to the value of } T'\text{Machine\_Mantissa}. \text{ This attribute yields a value of the type } \text{universal\_integer}.

**Ramification:** \text{S'\text{Model\_Epsilon}}, which is defined in terms of \text{S'\text{Model\_Mantissa}} (see A.5.3), yields the absolute value of the difference between one and the next model number of the type \( T \) above one. It is equal to or larger than the absolute value of the difference between one and the next machine number of the type \( T \) above one.

\text{S'\text{Model\_Emin}}

Yields the minimum exponent of the canonical form of the model numbers of \( T \) (see A.5.3). The value of this attribute shall be greater than or equal to the value of \( T'\text{Machine\_Emin} \). This attribute yields a value of the type \( \text{universal\_integer} \).

**Ramification:** \text{S'\text{Model\_Small}}, which is defined in terms of \text{S'\text{Model\_Emin}} (see A.5.3), yields the smallest positive (nonzero) model number of the type \( T \).

\text{S'\text{Safe\_First}}

Yields the lower bound of the safe range of \( T \). The value of this attribute shall be a model number of \( T \) and greater than or equal to the lower bound of the base range of \( T \). In addition, if \( T \) is declared by a floating_point_definition or is derived from such a type, and the floating_point_definition includes a real_range_specification specifying a lower bound of \( lb \), then the value of this attribute shall be less than or equal to \( lb \); otherwise, it shall be less than or equal to \( -10.0 \cdot 10^{d} \), where \( d \) is the requested decimal precision of \( T \). This attribute yields a value of the type \( \text{universal\_real} \).

\text{S'\text{Safe\_Last}}

Yields the upper bound of the safe range of \( T \). The value of this attribute shall be a model number of \( T \) and less than or equal to the upper bound of the base range of \( T \). In addition, if \( T \) is declared by a floating_point_definition or is derived from such a type, and the floating_point_definition includes a real_range_specification specifying an upper bound of \( ub \), then the value of this attribute shall be greater than or equal to \( ub \); otherwise, it shall be greater than or equal to \( 10.0 \cdot 10^{d} \), where \( d \) is the requested decimal precision of \( T \). This attribute yields a value of the type \( \text{universal\_real} \).

\text{S'\text{Model}}

Denotes a function (of a parameter \( X \)) whose specification is given in A.5.3. If \( X \) is a model number of \( T \), the function yields \( X \); otherwise, it yields the value obtained by rounding or truncating \( X \) to either one of the adjacent model numbers of \( T \). Constraint Error is raised if the resulting model number is outside the safe range of \( S \). A zero result has the sign of \( X \) when \( S'\text{Signed\_Zeros} \) is True.

Subject to the constraints given above, the values of \text{S'\text{Model\_Mantissa}} and \text{S'\text{Safe\_Last}} are to be maximized, and the values of \text{S'\text{Model\_Emin}} and \text{S'\text{Safe\_First}} minimized, by the implementation as follows:

- First, \text{S'\text{Model\_Mantissa}} is set to the largest value for which values of \text{S'\text{Model\_Emin}}, \text{S'\text{Safe\_First}}, and \text{S'\text{Safe\_Last}} can be chosen so that the implementation satisfies the strict-mode requirements of G.2.1 in terms of the model numbers and safe range induced by these attributes.
- Next, \text{S'\text{Model\_Emin}} is set to the smallest value for which values of \text{S'\text{Safe\_First}} and \text{S'\text{Safe\_Last}} can be chosen so that the implementation satisfies the strict-mode requirements of G.2.1 in terms of the model numbers and safe range induced by these attributes and the previously determined value of \text{S'\text{Model\_Mantissa}}.
- \text{[AI05-0092-1]} Finally, \text{S'\text{Safe\_First}} and \text{S'\text{Safe\_Last}} are set (in either order) to the smallest and largest values, respectively, for which the implementation satisfies the strict-mode
requirements of G.2.1 in terms of the model numbers and safe range induced by these attributes and the previously determined values of S'Model_Mantissa and S'Model_Emin.

11.a/5  Ramification: \{AI12-0437-1\} The following table shows appropriate attribute values for IEEE basic single and double precision types (ANSI/IEEE Std 754-1985, ISO/IEC 60559:2020\cite{ISOIEC60559}). Here, we use the names IEEE_Float_32 and IEEE_Float_64, the names that would typically be declared in package Interfaces, in an implementation that supports IEEE arithmetic. In such an implementation, the attributes would typically be the same for Standard.Float and Long_Float, respectively.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>IEEE_Float_32</th>
<th>IEEE_Float_64</th>
</tr>
</thead>
<tbody>
<tr>
<td>'Machine_Radix</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>'Machine_Mantissa</td>
<td>24</td>
<td>53</td>
</tr>
<tr>
<td>'Machine_Emin</td>
<td>-125</td>
<td>-1021</td>
</tr>
<tr>
<td>'Machine_Emax</td>
<td>128</td>
<td>1024</td>
</tr>
<tr>
<td>'Denorm</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>'Machine_Rounds</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>'Machine_Oversflows</td>
<td>True/False</td>
<td>True/False</td>
</tr>
<tr>
<td>'Signed_Zeros</td>
<td>should be True</td>
<td>should be True</td>
</tr>
<tr>
<td>'Model_Mantissa</td>
<td>(same as 'Machine_Mantissa)</td>
<td>(same as 'Machine_Mantissa)</td>
</tr>
<tr>
<td>'Model_Emin</td>
<td>(same as 'Machine_Emin)</td>
<td>(same as 'Machine_Emin)</td>
</tr>
<tr>
<td>'Model_Epsilon</td>
<td>2.0**(-23)</td>
<td>2.0**(-52)</td>
</tr>
<tr>
<td>'Model_Small</td>
<td>2.0**(-126)</td>
<td>2.0**(-1022)</td>
</tr>
<tr>
<td>'Safe_First</td>
<td>-2.0<strong>128*(1.0-2.0</strong>(-24))</td>
<td>-2.0<strong>1024*(1.0-2.0</strong>(-53))</td>
</tr>
<tr>
<td>'Safe_Last</td>
<td>2.0<strong>128*(1.0-2.0</strong>(-24))</td>
<td>2.0<strong>1024*(1.0-2.0</strong>(-53))</td>
</tr>
<tr>
<td>'Digits</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>'Base' Digits</td>
<td>(same as 'Digits')</td>
<td>(same as 'Digits')</td>
</tr>
<tr>
<td>'First</td>
<td>(same as 'Safe_First')</td>
<td>(same as 'Safe_First')</td>
</tr>
<tr>
<td>'Last</td>
<td>(same as 'Safe_Last')</td>
<td>(same as 'Safe_Last')</td>
</tr>
<tr>
<td>'Size'</td>
<td>32</td>
<td>64</td>
</tr>
</tbody>
</table>

Note: 'Machine_Oversflows can be True or False, depending on whether the Ada implementation raises Constraint_Error or delivers a signed infinity in overflow and zero divide situations (and at poles of the elementary functions).

Wording Changes from Ada 95

11.b/2  \{AI95-00256-01\} Corrected the definition of Model_Mantissa to match that given in 3.5.8.

G.2.3 Model of Fixed Point Arithmetic

In the strict mode, the predefined arithmetic operations of a fixed point type shall satisfy the accuracy requirements specified here and shall avoid or signal overflow in the situations described.

Implementation Requirements

The accuracy requirements for the predefined fixed point arithmetic operations and conversions, and the results of relations on fixed point operands, are given below.

Discussion: This subclause does not cover the accuracy of an operation of a static expression; such operations have to be evaluated exactly (see 4.9).

The operands of the fixed point adding operators, absolute value, and comparisons have the same type. These operations are required to yield exact results, unless they overflow.

Multiplications and divisions are allowed between operands of any two fixed point types; the result has to be (implicitly or explicitly) converted to some other numeric type. For purposes of defining the accuracy rules, the multiplication or division and the conversion are treated as a single operation whose accuracy depends on three types (those of the operands and the result). For decimal fixed point types, the attribute T'Round may be used to imply explicit conversion with rounding (see 3.5.10).

When the result type is a floating point type, the accuracy is as given in G.2.1. For some combinations of the operand and result types in the remaining cases, the result is required to belong to a small set of values called the perfect result set; for other combinations, it is required merely to belong to a generally larger and implementation-defined set of values called the close result set. When the result type is a decimal
fixed point type, the perfect result set contains a single value; thus, operations on decimal types are always fully specified.

**Implementation defined:** The definition of close result set, which determines the accuracy of certain fixed point multiplications and divisions.

\{AI12-0453-1\} When one operand of a fixed-fixed multiplication or division is of type universal_real, that operand is not implicitly converted in the usual sense, since the context does not determine a unique target type, but the accuracy of the result of the multiplication or division (that is, whether the result has to belong to the perfect result set or merely the close result set) depends on the value of the operand of type universal_real and on the types of the other operand and of the result.

**Discussion:** \{AI12-0453-1\} We need not consider here the multiplication or division of two such operands, since in that case either the operation is evaluated exactly (that is, it is an operation of a static expression all of whose operators are of a root numeric type) or it is considered to be an operation of a floating point type.

For a fixed point multiplication or division whose (exact) mathematical result is \(v\), and for the conversion of a value \(v\) to a fixed point type, the perfect result set and close result set are defined as follows:

- If the result type is an ordinary fixed point type with a small of \(s\),
  - if \(v\) is an integer multiple of \(s\), then the perfect result set contains only the value \(v\);
  - otherwise, it contains the integer multiple of \(s\) just below \(v\) and the integer multiple of \(s\) just above \(v\).

The close result set is an implementation-defined set of consecutive integer multiples of \(s\) containing the perfect result set as a subset.

- If the result type is a decimal type with a small of \(s\),
  - if \(v\) is an integer multiple of \(s\), then the perfect result set contains only the value \(v\);
  - otherwise, if truncation applies, then it contains only the integer multiple of \(s\) in the direction toward zero, whereas if rounding applies, then it contains only the nearest integer multiple of \(s\) (with ties broken by rounding away from zero).

The close result set is an implementation-defined set of consecutive integer multiples of \(s\) containing the perfect result set as a subset.

**Ramification:** As a consequence of subsequent rules, this case does not arise when the operand types are also decimal types.

- If the result type is an integer type,
  - if \(v\) is an integer, then the perfect result set contains only the value \(v\);
  - otherwise, it contains the integer nearest to the value \(v\) (if \(v\) lies equally distant from two consecutive integers, the perfect result set contains the one that is further from zero).

The close result set is an implementation-defined set of consecutive integers containing the perfect result set as a subset.

\{AI12-0453-1\} The result of a fixed point multiplication or division shall belong either to the perfect result set or to the close result set, as described below, if overflow does not occur. In the following cases, if the result type is a fixed point type, let \(s\) be its small; otherwise, that is, when the result type is an integer type, let \(s\) be 1.0.

- \{AI12-0453-1\} For a multiplication or division neither of whose operands is of type universal_real, let \(l\) and \(r\) be the smalls of the left and right operands. For a multiplication, if \((l \cdot r) / s\) is an integer or the reciprocal of an integer (the smalls are said to be “compatible” in this case), the result shall belong to the perfect result set; otherwise, it belongs to the close result set. For a division, if \(l / (r \cdot s)\) is an integer or the reciprocal of an integer (that is, the smalls are...
compatible), the result shall belong to the perfect result set; otherwise, it belongs to the close result set.

21.a

Ramification: When the operand and result types are all decimal types, their smalls are necessarily compatible; the same is true when they are all ordinary fixed point types with binary smalls.

22

• For a multiplication or division having one universal_real operand with a value of v, note that it is always possible to factor v as an integer multiple of a “compatible” small, but the integer multiple may be “too big”. If there exists a factorization in which that multiple is less than some implementation-defined limit, the result shall belong to the perfect result set; otherwise, it belongs to the close result set.

22.a

Implementation defined: Conditions on a universal_real operand of a fixed point multiplication or division for which the result shall be in the perfect result set.

23/5 [AI12-0300-1] A multiplication P * Q of an operand of a fixed point type F by an operand of type Integer, or vice-versa, and a division P / Q of an operand of a fixed point type F by an operand of type Integer, are also allowed. In these cases, the result has then a type of F; explicit conversion of the result is never required. The accuracy required in these cases is the same as that required for a multiplication F(P * Q) or a division F(P / Q) obtained by interpreting the operand of the integer type to have a fixed point type with a small of 1.0.

24

The accuracy of the result of a conversion from an integer or fixed point type to a fixed point type, or from a fixed point type to an integer type, is the same as that of a fixed point multiplication of the source value by a fixed point operand having a small of 1.0 and a value of 1.0, as given by the foregoing rules. The result of a conversion from a floating point type to a fixed point type shall belong to the close result set. The result of a conversion of a universal_real operand to a fixed point type shall belong to the perfect result set.

25

The possibility of overflow in the result of a predefined arithmetic operation or conversion yielding a result of a fixed point type T is analogous to that for floating point types, except for being related to the base range instead of the safe range. If all of the permitted results belong to the base range of T, then the implementation shall deliver one of the permitted results; otherwise,

26

• if T'Machine_Overflows is True, the implementation shall either deliver one of the permitted results or raise Constraint_Error;

27

• if T'Machine_Overflows is False, the result is implementation defined.

27.a

Implementation defined: The result of a fixed point arithmetic operation in overflow situations, when the Machine_Overflows attribute of the result type is False.

Inconsistencies With Ada 83

27.b

Since the values of a fixed point type are now just the integer multiples of its small, the possibility of using extra bits available in the chosen representation for extra accuracy rather than for increasing the base range would appear to be removed, raising the possibility that some fixed point expressions will yield less accurate results than in Ada 83. However, this is partially offset by the ability of an implementation to choose a smaller default small than before. Of course, if it does so for a type T then T'Small will have a different value than it previously had.

27.c

The accuracy requirements in the case of incompatible smalls are relaxed to foster wider support for nonbinary smalls. If this relaxation is exploited for a type that was previously supported, lower accuracy could result; however, there is no particular incentive to exploit the relaxation in such a case.

Wording Changes from Ada 83

27.d

The fixed point accuracy requirements are now expressed without reference to model or safe numbers, largely because the full generality of the former model was never exploited in the case of fixed point types (particularly in regard to operand perturbation). Although the new formulation in terms of perfect result sets and close result sets is still verbose, it can be seen to distill down to two cases:

27.e

• a case where the result must be the exact result, if the exact result is representative, or, if not, then either one of the adjacent values of the type (in some subcases only one of those adjacent values is allowed);
• a case where the accuracy is not specified by the language.

Wording Changes from Ada 2012

{AI12-0300-1} Correction: Reworded the fixed*integer accuracy requirements to clarify that the only allowed integer type in such operations is Standard.Integer. We make this correction as readers of the Reference Manual have been confused on this point.

G.2.4 Accuracy Requirements for the Elementary Functions

In the strict mode, the performance of Numerics.Generic_Elementary_Functions shall be as specified here.

Implementation Requirements

When an exception is not raised, the result of evaluating a function in an instance EF of Numerics.Generic_Elementary_Functions belongs to a result interval, defined as the smallest model interval of EF.Float_Type that contains all the values of the form \( f \cdot (1.0 + d) \), where \( f \) is the exact value of the corresponding mathematical function at the given parameter values, \( d \) is a real number, and \( |d| \) is less than or equal to the function's maximum relative error. The function delivers a value that belongs to the result interval when both of its bounds belong to the safe range of EF.Float_Type; otherwise,

• if EF.Float_Type'Machine_Overflows is True, the function either delivers a value that belongs to the result interval or raises Constraint_Error, signaling overflow;

• if EF.Float_Type'Machine_Overflows is False, the result is implementation defined.

Implementation defined: The result of an elementary function reference in overflow situations, when the Machine_Overflows attribute of the result type is False.

The maximum relative error exhibited by each function is as follows:

• \( 2.0 \cdot EF.Float_Type'Model_Epsilon, \) in the case of the Sqrt, Sin, and Cos functions;

• \( 4.0 \cdot EF.Float_Type'Model_Epsilon, \) in the case of the Log, Exp, Tan, Cot, and inverse trigonometric functions; and

• \( 8.0 \cdot EF.Float_Type'Model_Epsilon, \) in the case of the forward and inverse hyperbolic functions.

The maximum relative error exhibited by the exponentiation operator, which depends on the values of the operands, is \( (4.0 + |Right \cdot \log(Left)| / 32.0) \cdot EF.Float_Type'Model_Epsilon. \)

The maximum relative error given above applies throughout the domain of the forward trigonometric functions when the Cycle parameter is specified. When the Cycle parameter is omitted, the maximum relative error given above applies only when the absolute value of the angle parameter X is less than or equal to some implementation-defined angle threshold, which shall be at least EF.Float_Type'Machine_Radix \( \lceil EF.Float_Type'Machine_Mantissa/2 \rceil \). Beyond the angle threshold, the accuracy of the forward trigonometric functions is implementation defined.

Implementation defined: The value of the angle threshold, within which certain elementary functions, complex arithmetic operations, and complex elementary functions yield results conforming to a maximum relative error bound.

Implementation defined: The accuracy of certain elementary functions for parameters beyond the angle threshold.

Implementation Note: The angle threshold indirectly determines the amount of precision that the implementation has to maintain during argument reduction.

{AI95-00434-01} {AI12-0451-1} The prescribed results specified in A.5.1 for certain functions at particular parameter values take precedence over the maximum relative error bounds; effectively, they narrow to a single value the result interval allowed by the maximum relative error bounds. Additional rules with a similar effect are given by the Table below for the inverse trigonometric functions, at particular parameter values for which the mathematical result is possibly not a model number.
of \(EF\).\text{Float\_Type}\) (or is, indeed, even transcendental). In each table entry, the values of the parameters are such that the result lies on the axis between two quadrants; the corresponding accuracy rule, which takes precedence over the maximum relative error bounds, is that the result interval is the model interval of \(EF\).\text{Float\_Type}\) associated with the exact mathematical result given in the table.

This paragraph was deleted.

The last line of the table is meant to apply when \(EF\).\text{Float\_Type}'\text{Signed\_Zeros}\) is False; the two lines just above it, when \(EF\).\text{Float\_Type}'\text{Signed\_Zeros}\) is True and the parameter \(Y\) has a zero value with the indicated sign.

<table>
<thead>
<tr>
<th>Function</th>
<th>Value of X</th>
<th>Value of Y</th>
<th>Exact Result when Cycle Specified</th>
<th>Exact Result when Cycle Omitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arcsin</td>
<td>1.0</td>
<td>n.a.</td>
<td>Cycle/4.0</td>
<td>(\pi/2.0)</td>
</tr>
<tr>
<td>Arcsin</td>
<td>–1.0</td>
<td>n.a.</td>
<td>–Cycle/4.0</td>
<td>–(\pi/2.0)</td>
</tr>
<tr>
<td>Arccos</td>
<td>0.0</td>
<td>n.a.</td>
<td>Cycle/4.0</td>
<td>(\pi/2.0)</td>
</tr>
<tr>
<td>Arccos</td>
<td>–1.0</td>
<td>n.a.</td>
<td>Cycle/2.0</td>
<td>(\pi)</td>
</tr>
<tr>
<td>Arctan and Arccot</td>
<td>0.0</td>
<td>positive</td>
<td>Cycle/4.0</td>
<td>(\pi/2.0)</td>
</tr>
<tr>
<td>Arctan and Arccot</td>
<td>0.0</td>
<td>negative</td>
<td>–Cycle/4.0</td>
<td>–(\pi/2.0)</td>
</tr>
<tr>
<td>Arctan and Arccot</td>
<td>negative</td>
<td>+0.0</td>
<td>Cycle/2.0</td>
<td>(\pi)</td>
</tr>
<tr>
<td>Arctan and Arccot</td>
<td>negative</td>
<td>–0.0</td>
<td>–Cycle/2.0</td>
<td>–(\pi)</td>
</tr>
<tr>
<td>Arctan and Arccot</td>
<td>negative</td>
<td>0.0</td>
<td>Cycle/2.0</td>
<td>(\pi)</td>
</tr>
</tbody>
</table>

The amount by which the result of an inverse trigonometric function is allowed to spill over into a quadrant adjacent to the one corresponding to the principal branch, as given in A.5.1, is limited. The rule is that the result belongs to the smallest model interval of \(EF\).\text{Float\_Type}\) that contains both boundaries of the quadrant corresponding to the principal branch. This rule also takes precedence over the maximum relative error bounds, effectively narrowing the result interval allowed by them.

Finally, the following specifications also take precedence over the maximum relative error bounds:

- The absolute value of the result of the Sin, Cos, and Tanh functions never exceeds one.
- The absolute value of the result of the Coth function is never less than one.
- The result of the Cosh function is never less than one.

**Implementation Advice**

The versions of the forward trigonometric functions without a Cycle parameter should not be implemented by calling the corresponding version with a Cycle parameter of 2.0*\text{Numerics.Pi}, since this will not provide the required accuracy in some portions of the domain. For the same reason, the version of Log without a Base parameter should not be implemented by calling the corresponding version with a Base parameter of \text{Numerics.e}.
Implementation Advice: For elementary functions, the forward trigonometric functions without a Cycle parameter should not be implemented by calling the corresponding version with a Cycle parameter. Log without a Base parameter should not be implemented by calling Log with a Base parameter.

Wording Changes from Ada 83
The semantics of Numerics.Generic_Elementary_Functions differs from Generic_Elementary_Functions as defined in ISO/IEC DIS 11430 (for Ada 83) in the following ways related to the accuracy specified for strict mode:

- The maximum relative error bounds use the Model_Epsilon attribute instead of the Base'Epsilon attribute.
- The accuracy requirements are expressed in terms of result intervals that are model intervals. On the one hand, this facilitates the description of the required results in the presence of underflow; on the other hand, it slightly relaxes the requirements expressed in ISO/IEC DIS 11430.

G.2.4 Performance Requirements for Random Number Generation

In the strict mode, the performance of Numerics.Float_Random and Numerics.Discrete_Random shall be as specified here.

Implementation Requirements

Two different calls to the time-dependent Reset procedure shall reset the generator to different states, provided that the calls are separated in time by at least one second and not more than fifty years.

The implementation's representations of generator states and its algorithms for generating random numbers shall yield a period of at least $2^{31}$–2; much longer periods are desirable but not required.

\{AI12-0453-1\} The implementations of Numerics.Float_Random.Random and Numerics.Discrete_Random.Random shall pass at least 85% of the individual trials in a suite of statistical tests. For Numerics.Float_Random, the tests are applied directly to the floating point values generated (that is, they are not converted to integers first), while for Numerics.Discrete_Random they are applied to the generated values of various discrete types. Each test suite performs 6 different tests, with each test repeated 10 times, yielding a total of 60 individual trials. An individual trial is deemed to pass if the chi-square value (or other statistic) calculated for the observed counts or distribution falls within the range of values corresponding to the 2.5 and 97.5 percentage points for the relevant degrees of freedom (that is, it shall be neither too high nor too low). For the purpose of determining the degrees of freedom, measurement categories are combined whenever the expected counts are fewer than 5.

Implementation Note: In the floating point random number test suite, the generator is reset to a time-dependent state at the beginning of the run. The test suite incorporates the following tests, adapted from D. E. Knuth, *The Art of Computer Programming, vol. 2: Seminumerical Algorithms*. In the descriptions below, the given number of degrees of freedom is the number before reduction due to any necessary combination of measurement categories with small expected counts; it is one less than the number of measurement categories.

- Proportional Distribution Test (a variant of the Equidistribution Test). The interval 0.0 .. 1.0 is partitioned into $K$ subintervals. $K$ is chosen randomly between 4 and 25 for each repetition of the test, along with the boundaries of the subintervals (subject to the constraint that at least 2 of the subintervals have a width of 0.001 or more). 5000 random floating point numbers are generated. The counts of random numbers falling into each subinterval are tallied and compared with the expected counts, which are proportional to the widths of the subintervals. The number of degrees of freedom for the chi-square test is $K$–1.
- Gap Test. The bounds of a range $A .. B$, with 0.0 ≤ $A < B$ ≤ 1.0, are chosen randomly for each repetition of the test, subject to the constraint that 0.2 ≤ $B–A$ ≤ 0.6. Random floating point numbers are generated until 5000 falling into the range $A .. B$ have been encountered. Each of these 5000 is preceded by a “gap” (of length greater than or equal to 0) of consecutive random numbers not falling into the range $A .. B$. The counts of gaps of each length from 0 to 15, and of all lengths greater than 15 lumped together, are tallied and compared with the expected counts. Let $P = B–A$. The probability that a gap has a length of $L$ is $(1–P)^{K}$. The number of degrees of freedom for the chi-square test is 16.
- Permutation Test. 5000 tuples of 4 different random floating point numbers are generated. (An entire 4-tuple is discarded in the unlikely event that it contains any two exactly equal components.) The counts of each of the $4! = 24$ possible relative orderings of the components of the 4-tuples are tallied and compared with the
expected counts. Each of the possible relative orderings has an equal probability. The number of degrees of freedom for the chi-square test is 23.

- Increasing-Runs Test. Random floating point numbers are generated until 5000 increasing runs have been observed. An “increasing run” is a sequence of random numbers in strictly increasing order; it is followed by a random number that is strictly smaller than the preceding random number. (A run under construction is entirely discarded in the unlikely event that one random number is followed immediately by an exactly equal random number.) The decreasing random number that follows an increasing run is discarded and not included with the next increasing run. The counts of increasing runs of each length from 1 to 4, and of all lengths greater than 4 lumped together, are tallied and compared with the expected counts. The probability that an increasing run has a length of \( L \) is \( 1/L! - 1/(L+1)! \) for \( L \leq 4 \), while the probability that an increasing run has a length of 5 or more is \( 1/5! \). The number of degrees of freedom for the chi-square test is 4.

- Decreasing-Runs Test. The test is similar to the Increasing Runs Test, but with decreasing runs.

- Maximum-of-\( t \) Test (with \( t = 5 \)). 5000 tuples of 5 random floating point numbers are generated. The maximum of the components of each 5-tuple is determined and raised to the 5th power. The uniformity of the resulting values over the range 0.0 .. 1.0 is tested as in the Proportional Distribution Test.

Implementation Note: In the discrete random number test suite, Numerics.Discrete_Random is instantiated as described below. The generator is reset to a time-dependent state after each instantation. The test suite incorporates the following tests, adapted from D. E. Knuth (op. cit.) and other sources. The given number of degrees of freedom for the chi-square test is reduced by any necessary combination of measurement categories with small expected counts, as described above.

- Equidistribution Test. In each repetition of the test, a number \( R \) between 2 and 30 is chosen randomly, and Numerics.Discrete_Random is instantiated with an integer subtype whose range is \( 1 \ldots R \). 5000 integers are generated randomly from this range. The counts of occurrences of each integer in the range are tallied and compared with the expected counts, which have equal probabilities. The number of degrees of freedom for the chi-square test is \( R-1 \).

- Simplified Poker Test. Numerics.Discrete_Random is instantiated once with an enumeration subtype representing the 13 denominations (Two through Ten, Jack, Queen, King, and Ace) of an infinite deck of playing cards. 2000 “poker” hands (5-tuples of values of this subtype) are generated randomly. The counts of hands containing exactly \( K \) different denominations (\( 1 \leq K \leq 5 \)) are tallied and compared with the expected counts. The probability that a hand contains exactly \( K \) different denominations is given by a formula in Knuth. The number of degrees of freedom for the chi-square test is 4.

- Coupon Collector's Test. Numerics.Discrete_Random is instantiated in each repetition of the test with an integer subtype whose range is \( 1 \ldots R \), where \( R \) varies systematically from 2 to 11. Integers are generated randomly from this range until each value in the range has occurred, and the number \( K \) of integers generated is recorded. This constitutes a “coupon collector's segment” of length \( K \). 2000 such segments are generated. The counts of segments of each length from \( R \) to \( R+29 \), and of all lengths greater than \( R+29 \), are tallied and compared with the expected counts. The probability that a segment has any given length is given by formulas in Knuth. The number of degrees of freedom for the chi-square test is 30.

- Craps Test (Lengths of Games). Numerics.Discrete_Random is instantiated once with an integer subtype whose range is \( 1 \ldots 6 \) (representing the six numbers on a die). 5000 craps games are played, and their lengths are recorded. (The length of a craps game is the number of rolls of the pair of dice required to produce a win or a loss. A game is won on the first roll if the dice show 7 or 11; it is lost if they show 2, 3, or 12. If the dice show some other sum on the first roll, it is called the point, and the game is won if and only if the point is rolled again before a 7 is rolled.) The counts of games of each length from 1 to 18, and of all lengths greater than 18 lumped together, are tallied and compared with the expected counts. For \( 2 \leq S \leq 12 \), let \( D_S \) be the probability that a roll of a pair of dice shows the sum \( S \), and let \( Q_{D}(L) = D_1 \cdot (1 - (D_2 + D_3))^{L-1} \cdot (D_4 + D_5) \). Then, the probability that a game has a length of 1 is \( D_1 \cdot D_{11} + D_2 \cdot D_{12} + D_3 \cdot D_{13} \), and, for \( L \geq 1 \), the probability that a game has a length of \( L \) is \( Q_{D}(L) + Q_{D}(L) + Q_{D}(L) + Q_{D}(L) + Q_{D}(L) + Q_{D}(L) \). The number of degrees of freedom for the chi-square test is 18.

- Craps Test (Lengths of Passes). This test is similar to the last, but enough craps games are played for 3000 losses to occur. A string of wins followed by a loss is called a pass, and its length is the number of wins preceding the loss. The counts of passes of each length from 0 to 7, and of all lengths greater than 7 lumped together, are tallied and compared with the expected counts. For \( L \geq 0 \), the probability that a pass has a length of \( L \) is \( W^S \cdot (1-W) \), where \( W \), the probability that a game ends in a win, is 244.0/495.0. The number of degrees of freedom for the chi-square test is 8.

- Collision Test. Numerics.Discrete_Random is instantiated once with an integer or enumeration type representing binary bits. 15 successive calls on the Random function are used to obtain the bits of a 15-bit binary integer between 0 and 32767. 3000 such integers are generated, and the number of collisions (integers previously generated) is counted and compared with the expected count. A chi-square test is not used to assess the number of collisions; rather, the limits on the number of collisions, corresponding to the 2.5 and 97.5 percentage points, are (from formulas in Knuth) 112 and 154. The test passes if and only if the number of collisions is in this range.
G.2.6 Accuracy Requirements for Complex Arithmetic

In the strict mode, the performance of Numerics.Generic_Complex_Types and Numerics.Generic_Complex_Elementary_Functions shall be as specified here.

Implementation Requirements

{AI12-0453-1} When an exception is not raised, the result of evaluating a real function of an instance CT of Numerics.Generic_Complex_Types (that is, a function that yields a value of subtype CT.Real'Base or CT.Imaginary) belongs to a result interval defined as for a real elementary function (see G.2.4).

{AI12-0453-1} When an exception is not raised, each component of the result of evaluating a complex function of such an instance, or of an instance of Numerics.Generic_Complex_Elementary_Functions obtained by instantiating the latter with CT (that is, a function that yields a value of subtype CT.Complex), also belongs to a result interval. The result intervals for the components of the result are either defined by a maximum relative error bound or by a maximum box error bound. When the result interval for the real (resp., imaginary) component is defined by maximum relative error, it is defined as for that of a real function, relative to the exact value of the real (resp., imaginary) part of the result of the corresponding mathematical function. When defined by maximum box error, the result interval for a component of the result is the smallest model interval of CT.Real that contains all the values of the corresponding part of \( f \cdot (1.0 + d) \), where \( f \) is the exact complex value of the corresponding mathematical function at the given parameter values, \( d \) is complex, and |\( d \)| is less than or equal to the given maximum box error. The function delivers a value that belongs to the result interval (or a value both of whose components belong to their respective result intervals) when both bounds of the result interval(s) belong to the safe range of CT.Real; otherwise,

- Discussion: The maximum relative error could be specified separately for each component, but we do not take advantage of that freedom here.

- Discussion: Note that \( f \cdot (1.0 + d) \) defines a small circular region of the complex plane centered at \( f \), and the result intervals for the real and imaginary components of the result define a small rectangular box containing that circle.

- Reason: Box error is used when the computation of the result risks loss of significance in a component due to cancellation.

- Ramification: The components of a complex function that exhibits bounded relative error in each component have to have the correct sign. In contrast, one of the components of a complex function that exhibits bounded box error may have the wrong sign, since the dimensions of the box containing the result are proportional to the modulus of the mathematical result and not to either component of the mathematical result individually. Thus, for example, the box containing the computed result of a complex function whose mathematical result has a large modulus but lies very close to the imaginary axis might well straddle that axis, allowing the real component of the computed result to have the wrong sign. In this case, the distance between the computed result and the mathematical result is, nevertheless, a small fraction of the modulus of the mathematical result.

- if CT.Real'Machine_Overflows is True, the function either delivers a value that belongs to the result interval (or a value both of whose components belong to their respective result intervals) or raises Constraint_Error, signaling overflow;

- if CT.Real'Machine_Overflows is False, the result is implementation defined.

Implementation defined: The result of a complex arithmetic operation or complex elementary function reference in overflow situations, when the Machine_Overflows attribute of the corresponding real type is False.

{AI95-00434-01} The error bounds for particular complex functions are tabulated in Table G.2 below. In the table, the error bound is given as the coefficient of CT.Real'Model_Epsilon.

This paragraph was deleted.

Table G.2G-2: Error Bounds for Particular Complex Functions
<table>
<thead>
<tr>
<th>Function or Operator</th>
<th>Nature of Result</th>
<th>Nature of Bound</th>
<th>Error Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modulus</td>
<td>real</td>
<td>max. rel. error</td>
<td>3.0</td>
</tr>
<tr>
<td>Argument</td>
<td>real</td>
<td>max. rel. error</td>
<td>4.0</td>
</tr>
<tr>
<td>Compose_From_Polar</td>
<td>complex</td>
<td>max. rel. error</td>
<td>3.0</td>
</tr>
<tr>
<td>&quot;*&quot; (both operands complex)</td>
<td>complex</td>
<td>max. box error</td>
<td>5.0</td>
</tr>
<tr>
<td>&quot;/&quot; (right operand complex)</td>
<td>complex</td>
<td>max. box error</td>
<td>13.0</td>
</tr>
<tr>
<td>Sqrt</td>
<td>complex</td>
<td>max. rel. error</td>
<td>6.0</td>
</tr>
<tr>
<td>Log</td>
<td>complex</td>
<td>max. box error</td>
<td>13.0</td>
</tr>
<tr>
<td>Exp (complex parameter)</td>
<td>complex</td>
<td>max. rel. error</td>
<td>7.0</td>
</tr>
<tr>
<td>Exp (imaginary parameter)</td>
<td>complex</td>
<td>max. rel. error</td>
<td>2.0</td>
</tr>
<tr>
<td>Sin, Cos, Sinh, and Cosh</td>
<td>complex</td>
<td>max. rel. error</td>
<td>11.0</td>
</tr>
<tr>
<td>Tan, Cot, Tanh, and Coth</td>
<td>complex</td>
<td>max. rel. error</td>
<td>35.0</td>
</tr>
<tr>
<td>inverse trigonometric</td>
<td>complex</td>
<td>max. rel. error</td>
<td>14.0</td>
</tr>
<tr>
<td>inverse hyperbolic</td>
<td>complex</td>
<td>max. rel. error</td>
<td>14.0</td>
</tr>
</tbody>
</table>

The maximum relative error given above applies throughout the domain of the Compose_From_Polar function when the Cycle parameter is specified. When the Cycle parameter is omitted, the maximum relative error applies only when the absolute value of the parameter Argument is less than or equal to the angle threshold (see G.2.4). For the Exp function, and for the forward hyperbolic (resp., trigonometric) functions, the maximum relative error given above likewise applies only when the absolute value of the imaginary (resp., real) component of the parameter X (or the absolute value of the parameter itself, in the case of the Exp function with a parameter of pure-imaginary type) is less than or equal to the angle threshold. For larger angles, the accuracy is implementation defined.

8.a Implementation defined: The accuracy of certain complex arithmetic operations and certain complex elementary functions for parameters (or components thereof) beyond the angle threshold.

9 The prescribed results specified in G.1.2 for certain functions at particular parameter values take precedence over the error bounds; effectively, they narrow to a single value the result interval allowed by the error bounds for a component of the result. Additional rules with a similar effect are given below for certain inverse trigonometric and inverse hyperbolic functions, at particular parameter values for which a component of the mathematical result is transcendental. In each case, the accuracy rule, which takes precedence over the error bounds, is that the result interval for the stated result component is the model interval of $\text{CT}.\text{Real}$ associated with the component's exact mathematical value. The cases in question are as follows:

- When the parameter X has the value zero, the real (resp., imaginary) component of the result of the Arcscot (resp., Arccoth) function is in the model interval of $\text{CT}.\text{Real}$ associated with the value $\pi/2.0$.
- When the parameter X has the value one, the real component of the result of the Arcscin function is in the model interval of $\text{CT}.\text{Real}$ associated with the value $\pi/2.0$.
- When the parameter X has the value $-1.0$, the real component of the result of the Arcscin (resp., Arccos) function is in the model interval of $\text{CT}.\text{Real}$ associated with the value $-\pi/2.0$ (resp., $\pi$).

Discussion: It is possible to give many other prescribed results in which a component of the parameter is restricted to a similar model interval when the parameter X is appropriately restricted to an easily testable portion of the domain. We
follow the proposed ISO/IEC standard for Generic_Complex_Elementary_Functions (for Ada 83) in not doing so, however.

{A195-00434-01} The amount by which a component of the result of an inverse trigonometric or inverse hyperbolic function is allowed to spill over into a quadrant adjacent to the one corresponding to the principal branch, as given in G.1.2, is limited. The rule is that the result belongs to the smallest model interval of CT.Real that contains both boundaries of the quadrant corresponding to the principal branch. This rule also takes precedence over the maximum error bounds, effectively narrowing the result interval allowed by them.

Finally, the results allowed by the error bounds are narrowed by one further rule: The absolute value of each component of the result of the Exp function, for a pure-imaginary parameter, never exceeds one.

Implementation Advice

The version of the Compose_From_Polar function without a Cycle parameter should not be implemented by calling the corresponding version with a Cycle parameter of 2.0*Numerics.Pi, since this will not provide the required accuracy in some portions of the domain.

G.3 Vector and Matrix Manipulation

{A195-00296-01} Types and operations for the manipulation of real vectors and matrices are provided in Generic_Real_Arrays, which is defined in G.3.1. Types and operations for the manipulation of complex vectors and matrices are provided in Generic_Complex_Arrays, which is defined in G.3.2. Both of these library units are generic children of the predefined package Numerics (see A.5). Nongeneric equivalents of these packages for each of the predefined floating point types are also provided as children of Numerics.

Discussion: Vector and matrix manipulation is defined in the Numerics Annex, rather than in the core, because it is considered to be a specialized need of (some) numeric applications.

These packages provide facilities that are similar to and replace those found in ISO/IEC 13813:1998 Information technology — Programming languages — Generic packages of real and complex type declarations and basic operations for Ada (including vector and matrix types). (The other facilities provided by that Standard were already provided in Ada 95.) In addition to the main facilities of that Standard, these packages also include subprograms for the solution of linear equations, matrix inversion, determinants, and the determination of the eigenvalues and eigenvectors of real symmetric matrices and Hermitian matrices.

Extensions to Ada 95

{A195-00296-01} {A105-0299-1} This subclause provides an introduction to the following subclauses.
G.3.1 Real Vectors and Matrices

Static Semantics

{AI95-00296-01; AI95-00418-01} The generic library package Numerics.Generic_Real_Arrays has the following declaration:

{AI12-0241-1}
generic type Real is digits <>;
package Ada.Numerics.Generic_Real_Arrays is
  withpragma Pure, Nonblocking is(Generic_Real_Arrays);

-- Types

type Real_Vector is array (Integer range <>) of Real'Base;

-- Subprograms for Real_Vector types

-- Real_Vector arithmetic operations

function "+" (Right : Real_Vector) return Real_Vector;
function "+" (Left, Right : Real_Vector) return Real_Vector;
function "abs" (Right : Real_Vector) return Real_Vector;

function "+" (Left : Real'Base; Right : Real_Vector) return Real_Vector;
function "+" (Left : Real_Vector; Right : Real'Base) return Real_Vector;
function "+" (Left : Real_Vector; Right : Real_Vector) return Real_Vector;
function "+" (Left : Real_Vector; Right : Real_Vector) return Real_Vector;

function "/" (Left : Real_Vector; Right : Real'Base) return Real_Vector;

function Unit_Vector (Index : Integer; Order : Positive; First : Integer := 1) return Real_Vector;

-- Subprograms for Real_Matrix types

-- Real_Matrix arithmetic operations

function "+" (Right : Real_Matrix) return Real_Matrix;
function "+" (Right : Real_Matrix) return Real_Matrix;
function "abs" (Right : Real_Matrix) return Real_Matrix;
function Transpose (X : Real_Matrix) return Real_Matrix;
function "+" (Left, Right : Real_Matrix) return Real_Matrix;
function "+" (Left : Real_Matrix; Right : Real_Vector) return Real_Vector;
function "+" (Left : Real_Matrix; Right : Real_Vector) return Real_Vector;

function "*" (Left : Real_Vector; Right : Real_Matrix) return Real_Vector;
function "*" (Left : Real_Matrix; Right : Real_Vector) return Real_Vector;
function "/" (Left : Real_Matrix; Right : Real'Base) return Real_Matrix;

function "/" (Left : Real_Matrix; Right : Real'Base) return Real_Matrix;
-- Real Matrix inversion and related operations

function Solve (A : Real_Matrix; X : Real_Vector) return Real_Vector;
function Solve (A, X : Real_Matrix) return Real_Matrix;
function Inverse (A : Real_Matrix) return Real_Matrix;
function Determinant (A : Real_Matrix) return Real'Base;

-- Eigenvalues and vectors of a real symmetric matrix

function Eigenvalues (A : Real_Matrix) return Real_Vector;

procedure Eigensystem (A       : in Real_Matrix;
                       Values  : out Real_Vector;
                       Vectors : out Real_Matrix);

-- Other Real Matrix operations

function Unit_Matrix (Order            : Positive;
                   First_1, First_2 : Integer := 1) return Real_Matrix;

end Ada.Numerics.Generic_Real_Arrays;

{AI95-00296-01} The library package Numerics.Real_Arrays is declared pure and defines the same types and subprograms as Numerics.Generic Real Arrays, except that the predefined type Float is systematically substituted for Real'Base throughout. Nongeneric equivalents for each of the other predefined floating point types are defined similarly, with the names Numerics.Short_Real_Arrays, Numerics.Long_Real_Arrays, etc.

**Reason:** The nongeneric equivalents are provided to allow the programmer to construct simple mathematical applications without being required to understand and use generics, and to be consistent with other Numerics packages.

{AI95-00296-01} Two types are defined and exported by Numerics.Generic Real Arrays. The composite type Real_Vector is provided to represent a vector with components of type Real; it is defined as an unconstrained, one-dimensional array with an index of type Integer. The composite type Real_Matrix is provided to represent a matrix with components of type Real; it is defined as an unconstrained, two-dimensional array with indices of type Integer.

{AI95-00296-01} The effect of the various subprograms is as described below. In most cases the subprograms are described in terms of corresponding scalar operations of the type Real; any exception raised by those operations is propagated by the array operation. Moreover, the accuracy of the result for each individual component is as defined for the scalar operation unless stated otherwise.

{AI95-00296-01} In the case of those operations which are defined to involve an inner product, Constraint Error may be raised if an intermediate result is outside the range of Real'Base even though the mathematical final result would not be.

function "+" (Right : Real_Vector) return Real_Vector;
function "-" (Right : Real_Vector) return Real_Vector;
function "abs" (Right : Real_Vector) return Real_Vector;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation of the type Real to each component of Right. The index range of the result is Right'Range.

function "+" (Left, Right : Real_Vector) return Real_Vector;
function "-" (Left, Right : Real_Vector) return Real_Vector;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation of the type Real to each component of Left and the matching component of Right. The index range of the result is Left'Range. Constraint Error is raised if Left'Length is not equal to Right'Length.

function "*" (Left, Right : Real_Vector) return Real'Base;

{AI95-00296-01} This operation returns the inner product of Left and Right. Constraint Error is raised if Left'Length is not equal to Right'Length. This operation involves an inner product.
function "abs" (Right : Real_Vector) return Real'Base;

{AI95-00418-01} This operation returns the L2-norm of Right (the square root of the inner product of the vector with itself).

Discussion: Normalization of vectors is a frequent enough operation that it is useful to provide the norm as a basic operation. Furthermore, implementing the norm is not entirely straightforward, because the inner product might overflow while the final norm does not. An implementation cannot merely return \(\sqrt{X^2}\), it has to cope with a possible overflow of the inner product.

Implementation Note: While the definition is given in terms of an inner product, the norm doesn't "involve an inner product" in the technical sense. The reason is that it has accuracy requirements substantially different from those applicable to inner products; and that cancellations cannot occur, because all the terms are positive, so there is no possibility of intermediate overflow.

function "*" (Left : Real'Base; Right : Real_Vector) return Real_Vector;

{AI95-00296-01} This operation returns the result of multiplying each component of Right by the scalar Left using the "*" operation of the type Real. The index range of the result is Right'Range.

function "/" (Left : Real_Vector; Right : Real'Base) return Real_Vector;

function "+" (Right : Real_Matrix) return Real_Matrix;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation of the type Real to each component of Left and to the scalar Right. The index range of the result is Left'Range.

function Unit_Vector (Index : Integer; Order : Positive; First : Integer := 1) return Real_Vector;

{AI95-00296-01} This function returns a unit vector with Order components and a lower bound of First. All components are set to 0.0 except for the Index component which is set to 1.0. Constraint_Error is raised if Index < First, Index > First + Order – 1 or if First + Order – 1 > Integer'Last.

function Transpose (X : Real_Matrix) return Real_Matrix;

{AI95-00296-01} This function returns the transpose of a matrix X. The first and second index ranges of the result are X'Range(2) and X'Range(1) respectively.

function "+" (Left, Right : Real_Matrix) return Real_Matrix;

function "-" (Left, Right : Real_Matrix) return Real_Matrix;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation of the type Real to each component of Left and the matching component of Right. The index ranges of the result are those of Right.

function "*" (Left, Right : Real_Matrix) return Real_Matrix;

{AI95-00296-01} This operation provides the standard mathematical operation for matrix multiplication. The first and second index ranges of the result are Left'Range(1) and Right'Range(2) respectively. Constraint_Error is raised if Left'Length(2) is not equal to Right'Length(1) or Left'Length(2) is not equal to Right'Length(2).
function "*" (Left, Right : Real_Vector) return Real_Matrix;
{AI95-00296-01} This operation returns the outer product of a (column) vector Left by a (row) vector Right using the operation "*" of the type Real for computing the individual components. The first and second index ranges of the result are Left'Range and Right'Range respectively.

function "*" (Left : Real_Vector; Right : Real_Matrix) return Real_Vector;
{AI95-00296-01} This operation provides the standard mathematical operation for multiplication of a (row) vector Left by a matrix Right. The index range of the (row) vector result is Right'Range(2). Constraint_Error is raised if Left'Length is not equal to Right'Length(1). This operation involves inner products.

function "*" (Left : Real_Matrix; Right : Real_Vector) return Real_Vector;
{AI95-00296-01} This operation provides the standard mathematical operation for multiplication of a matrix Left by a (column) vector Right. The index range of the (column) vector result is Left'Range(1). Constraint_Error is raised if Left'Length(2) is not equal to Right'Length. This operation involves inner products.

function "*" (Left : Real'Base; Right : Real_Matrix) return Real_Matrix;
{AI95-00296-01} This operation returns the result of multiplying each component of Right by the scalar Left using the "*" operation of the type Real. The index ranges of the result are those of Right.

function "*" (Left : Real_Matrix; Right : Real'Base) return Real_Matrix;

function "/" (Left : Real_Matrix; Right : Real'Base) return Real_Matrix;
{AI95-00296-01} Each operation returns the result of applying the corresponding operation of the type Real to each component of Left and to the scalar Right. The index ranges of the result are those of Left.

function Solve (A : Real_Matrix; X : Real_Vector) return Real_Vector;
{AI95-00296-01} This function returns a vector Y such that X is (nearly) equal to A * Y. This is the standard mathematical operation for solving a single set of linear equations. The index range of the result is A'Range(2). Constraint_Error is raised if A'Length(1), A'Length(2), and X'Length are not equal. Constraint_Error is raised if the matrix A is ill-conditioned.

Discussion: The text says that Y is such that “X is (nearly) equal to A * Y” rather than “X is equal to A * Y” because rounding errors may mean that there is no value of Y such that X is exactly equal to A * Y. On the other hand it does not mean that any old rough value will do. The algorithm given under Implementation Advice should be followed. The requirement to raise Constraint_Error if the matrix is ill-conditioned is really a reflection of what will happen if the matrix is ill-conditioned. See Implementation Advice. We do not make any attempt to define ill-conditioned formally.

These remarks apply to all versions of Solve and Inverse.

function Solve (A, X : Real_Matrix) return Real_Matrix;
{AI95-00296-01} This function returns a matrix Y such that X is (nearly) equal to A * Y. This is the standard mathematical operation for solving several sets of linear equations. The index ranges of the result are A'Range(2) and X'Range(2). Constraint_Error is raised if A'Length(1), A'Length(2), and X'Length(1) are not equal. Constraint_Error is raised if the matrix A is ill-conditioned.

function Inverse (A : Real_Matrix) return Real_Matrix;
{AI95-00296-01} This function returns a matrix B such that A * B is (nearly) equal to the unit matrix. The index ranges of the result are A'Range(2) and A'Range(1). Constraint_Error is raised if A'Length(1) is not equal to A'Length(2). Constraint_Error is raised if the matrix A is ill-conditioned.
function Determinant (A : Real_Matrix) return Real'Base;

{AI95-00296-01} This function returns the determinant of the matrix A. Constraint Error is raised if A'Length(1) is not equal to A'Length(2).

function Eigenvalues(A : Real_Matrix) return Real_Vector;

{AI95-00296-01} This function returns the eigenvalues of the symmetric matrix A as a vector sorted into order with the largest first. Constraint Error is raised if A'Length(1) is not equal to A'Length(2). The index range of the result is A'Range(1). Argument_Error is raised if the matrix A is not symmetric.

procedure Eigensystem(A       :
in Real_Matrix;
Values  :
out Real_Vector;
Vectors :
out Real_Matrix);

{AI95-00296-01} {AI05-0047-1} This procedure computes both the eigenvalues and eigenvectors of the symmetric matrix A. The out parameter Values is the same as that obtained by calling the function Eigenvalues. The out parameter Vectors is a matrix whose columns are the eigenvectors of the matrix A. The order of the columns corresponds to the order of the eigenvalues. The eigenvectors are normalized and mutually orthogonal (they are orthonormal), including when there are repeated eigenvalues. Constraint Error is raised if A'Length(1) is not equal to A'Length(2), or if Values'Range is not equal to A'Range(1), or if the parameter Vectors are not equal to those of A. Argument_Error is raised if the matrix A is not symmetric. Constraint_Error is also raised in implementation-defined circumstances if the algorithm used does not converge quickly enough.

Ramification: {AI05-0047-1} There is no requirement on the absolute direction of the returned eigenvectors. Thus they might be multiplied by -1. It is only the ratios of the components that matter. This is standard practice.

function Unit_Matrix (Order            : Positive;
First_1, First_2 : Integer := 1) return Real_Matrix;

{AI95-00296-01} This function returns a square unit matrix with Order**2 components and lower bounds of First_1 and First_2 (for the first and second index ranges respectively). All components are set to 0.0 except for the main diagonal, whose components are set to 1.0. Constraint_Error is raised if First_1 + Order – 1 > Integer'Last or First_2 + Order – 1 > Integer'Last.

Implementation Requirements

{AI95-00296-01} Accuracy requirements for the subprograms Solve, Inverse, Determinant, Eigenvalues and Eigensystem are implementation defined.

Implementation defined: The accuracy requirements for the subprograms Solve, Inverse, Determinant, Eigenvalues and Eigensystem for type Real_Matrix.

For operations not involving an inner product, the accuracy requirements are those of the corresponding operations of the type Real in both the strict mode and the relaxed mode (see G.2).

For operations involving an inner product, no requirements are specified in the relaxed mode. In the strict mode the modulus of the absolute error of the inner product $X^*Y$ shall not exceed $g\cdot\text{abs}(X)\cdot\text{abs}(Y)$ where $g$ is defined as

$$g = X'\text{Length} \times \text{Real'Machine_Radix}^{(1 – \text{Real'Model_Mantissa})}$$

{AI95-00418-01} For the L2-norm, no accuracy requirements are specified in the relaxed mode. In the strict mode the relative error on the norm shall not exceed $g / 2.0 + 3.0 \times \text{Real'Model_Epsilon}$ where $g$ is defined as above.
Reason: This is simply the combination of the error on the inner product with the error on Sqrt. A first order computation would lead to 2.0 * Real'Model_Epsilon above, but we are adding an extra Real'Model_Epsilon to account for higher order effects.

Documentation Requirements

Documentation Requirement: Any techniques used to reduce cancellation errors in Numerics.Generic_Real_Arrays shall be documented.

Implementation Note: The above accuracy requirement is met by the canonical implementation of the inner product by multiplication and addition using the corresponding operations of type Real'Base and performing the cumulative addition using ascending indices. Note however, that some hardware provides special operations for the computation of the inner product and although these may be fast they may not meet the accuracy requirement specified. See Accuracy and Stability of Numerical Algorithms by N J Higham (ISBN 0-89871-355-2), Section 3.1.

Implementation Permissions

The nongeneric equivalent packages can but need not, be actual instantiations of the generic package for the appropriate predefined type, though that is not required.

Implementation Advice

Implementation should implement the Solve and Inverse functions using established techniques such as LU decomposition with row interchanges followed by back and forward substitution. Implementations are recommended to refine the result by performing an iteration on the residuals; if this is done, then it should be documented.

Implementation Advice: Solve and Inverse for Numerics.Generic_Real_Arrays should be implemented using established techniques such as LU decomposition and the result should be refined by an iteration on the residuals.

It is not the intention that any special provisions should be made to determine whether a matrix is ill-conditioned or not. The naturally occurring overflow (including division by zero) which will result from executing these functions with an ill-conditioned matrix and thus raise Constraint_Error is sufficient.

Discussion: There isn’t any advice for the implementation to document with this paragraph.

The test that a matrix is symmetric should be performed by using the equality operator to compare the relevant components.

Implementation Advice: The equality operator should be used to test that a matrix in Numerics.Generic_Real_Arrays is symmetric.

An implementation should minimize the circumstances under which the algorithm used for Eigenvalues and Eigensystem fails to converge.

Implementation Advice: An implementation should minimize the circumstances under which the algorithm used for Numerics.Generic_Real_Arrays.Eigenvalues and Numerics.Generic_Real_Arrays.Eigensystem fails to converge.


Extensions to Ada 95

The package Numerics.Generic_Real_Arrays and its nongeneric equivalents are new.
Wording Changes from Ada 2005

Correction: Corrected various accuracy and definition issues.

G.3.2 Complex Vectors and Matrices

Static Semantics

The generic library package Numerics.Generic_Complex_Arrays has the following declaration:

```ada
with Ada.Numerics.Generic_Real_Arrays,
     Ada.Numerics.Generic_Complex_Types;

generic
with package Real_Arrays is new
     Ada.Numerics.Generic_Real_Arrays   (<>);
use Real_Arrays;

with package Complex_Types is new
     Ada.Numerics.Generic_Complex_Types (Real);
use Complex_Types;
package Ada.Numerics.Generic_Complex_Arrays is

   withpragma Pure, Nonblocking is (Generic_Complex_Arrays);

   -- Types
   type Complex_Vector is array (Integer range <>) of Complex;
   type Complex_Matrix is array (Integer range <>,
                                Integer range <>) of Complex;

   -- Subprograms for Complex_Vector types
   -- Complex_Vector selection, conversion and composition operations
   function Re (X : Complex_Vector) return Real_Vector;
   function Im (X : Complex_Vector) return Real_Vector;
   procedure Set_Re (X  : in out Complex_Vector;
                     Re : in Real_Vector);
   procedure Set_Im (X  : in out Complex_Vector;
                     Im : in Real_Vector);
   function Compose_From_Cartesian (Re     : Real_Vector)
                        return Complex_Vector;
   function Compose_From_Cartesian (Re, Im : Real_Vector)
                        return Complex_Vector;
   function Modulus  (X     : Complex_Vector)
                        return Real_Vector;
   function "abs"    (Right : Complex_Vector)
                    return Real'BaseComplex;
   function Argument (X     : Complex_Vector;
                      Cycle : Real'Base) return Real_Vector;
   function Compose_From_Polar (Modulus, Argument : Real_Vector)
                        return Complex_Vector;
   function Compose_From_Polar (Modulus, Argument : Real_Vector;
                                  Cycle             : Real'Base)
                        return Complex_Vector;

   -- Complex_Vector arithmetic operations
   function "+"       (Right  : Complex_Vector)
                   return Complex_Vector;
   function "+"  (Left, Right : Complex_Vector)
                   return Complex_Vector;
   function Conjugate (X      : Complex_Vector)
                        return Complex_Vector;
   function "-"       (Right  : Complex_Vector)
                   return Complex_Vector;
   function "-"  (Left, Right : Complex_Vector)
                   return Complex_Vector;
   function "*"       (Left, Right : Complex_Vector)
                   return Complex;
   function "+" (Left, Right : Complex_Vector)
             return Complex;

   {AI05-0047-1} function "abs" (Right : Complex_Vector)
                   return Real'BaseComplex;

   -- Mixed Real_Vector and Complex_Vector arithmetic operations
```
function "+" (Left : Real_Vector; Right : Complex_Vector) return Complex_Vector;
function "+" (Left : Complex_Vector; Right : Real_Vector) return Complex_Vector;
function "-" (Left : Real_Vector; Right : Complex_Vector) return Complex_Vector;
function "-" (Left : Complex_Vector; Right : Real_Vector) return Complex_Vector;
function "*" (Left : Real_Vector; Right : Complex_Vector) return Complex;
function "*" (Left : Complex_Vector; Right : Real_Vector) return Complex;
function "/" (Left : Complex_Vector; Right : Complex) return Complex_Vector;
function "*" (Left : Real'Base; Right : Complex_Vector) return Complex_Vector;
function "*" (Left : Complex_Vector; Right : Real'Base) return Complex_Vector;
function "/" (Left : Complex_Vector; Right : Real'Base) return Complex_Vector;

-- Complex Vector scaling operations
function "*" (Left : Complex; Right : Complex_Vector) return Complex_Vector;
function "*" (Left : Complex_Vector; Right : Complex) return Complex_Vector;

-- Other Complex Vector operations
function Unit_Vector (Index : Integer; Order : Positive; First : Integer := 1) return Complex_Vector;

-- Subprograms for Complex Matrix types
function Re (X : Complex_Matrix) return Real_Matrix;
function Im (X : Complex_Matrix) return Real_Matrix;
procedure Set_Re (X : in out Complex_Matrix; Re : in Real_Matrix);
procedure Set_Im (X : in out Complex_Matrix; Im : in Real_Matrix);
function Compose_From_Cartesian (Re : Real_Matrix) return Complex_Matrix;
function Compose_From_Cartesian (Re, Im : Real_Matrix) return Complex_Matrix;
function Modulus (X : Complex_Matrix) return Real_Matrix;
function "abs" (Right : Complex_Matrix) return Real_Matrix
renames Modulus;
function Argument (X : Complex_Matrix) return Real_Matrix;
function Argument (X : Complex_Matrix; Cycle : Real'Base) return Real_Matrix;
function Compose_From_Polar (Modulus, Argument : Real_Matrix) return Complex_Matrix;
function Compose_From_Polar (Modulus, Argument : Real_Matrix; Cycle : Real'Base) return Complex_Matrix;

-- Complex Matrix arithmetic operations
function "+" (Right : Complex_Matrix) return Complex_Matrix;
function "-" (Right : Complex_Matrix) return Complex_Matrix;
function Conjugate (X : Complex_Matrix) return Complex_Matrix;
function Transpose (X : Complex_Matrix) return Complex_Matrix;
function "+" (Left, Right : Complex_Matrix) return Complex_Matrix;
function "+" (Left : Complex_Matrix; Right : Complex Matrix) return Complex_Matrix;
function "*" (Left : Complex Vector; Right : Complex Matrix) return Complex_Vector;
function "*" (Left : Complex Vector; Right : Complex Matrix) return Complex_Vector;

-- Mixed Real Matrix and Complex Matrix arithmetic operations

function "+" (Left : Complex Matrix; Right : Complex Matrix) return Complex_Matrix;
function "+" (Left : Complex Matrix; Right : Real Matrix) return Complex_Matrix;
function "+" (Left : Real Matrix; Right : Complex Matrix) return Complex_Matrix;
function "+" (Left : Real Matrix; Right : Real Matrix) return Complex_Matrix;

function "-" (Left : Complex Matrix; Right : Complex Matrix) return Complex_Matrix;
function "-" (Left : Complex Matrix; Right : Real Matrix) return Complex_Matrix;
function "-" (Left : Real Matrix; Right : Complex Matrix) return Complex_Matrix;
function "-" (Left : Real Matrix; Right : Real Matrix) return Complex_Matrix;

function "*" (Left : Complex Vector; Right : Complex Matrix) return Complex_Vector;
function "*" (Left : Complex Vector; Right : Real Matrix) return Complex_Vector;
function "*" (Left : Real Vector; Right : Complex Vector) return Complex_Matrix;
function "*" (Left : Real Vector; Right : Complex Matrix) return Complex_Vector;

-- Complex Matrix scaling operations

function "/" (Left : Complex; Right : Complex Matrix) return Complex_Matrix;
function "/" (Left : Complex Matrix; Right : Complex) return Complex_Matrix;
function "/" (Left : Complex Matrix; Right : Real'Base) return Complex_Matrix;
function "/" (Left : Real'Base; Right : Complex Matrix) return Complex_Matrix;

-- Complex Matrix inversion and related operations

function Solve (A : Complex_Matrix; X : Complex_Vector) return Complex_Vector;
function Solve (A, X : Complex Matrix) return Complex_Matrix;
function Inverse (A : Complex_Matrix) return Complex_Matrix;
function Determinant (A : Complex_Matrix) return Complex;
function Unit_Matrix (Order : Positive;
First_1, First_2 : Integer := 1)
return Complex_Matrix;
end Ada.Numerics.Generic_Complex_Arrays;

{AI95-00296-01} The library package Numerics.Complex_Arrays is declared pure and defines the same types and subprograms as Numerics.Generic_Complex_Arrays, except that the predefined type Float is systematically substituted for Real'Base, and the Real Vector and Real Matrix types exported by Numerics.Real_Arrays are systematically substituted for Real_Vector and Real_Matrix, and the Complex type exported by Numerics.Complex_Types is systematically substituted for Complex, throughout. Nongeneric equivalents for each of the other predefined floating point types are defined similarly, with the names Numerics.Short_Complex_Arrays, Numerics.Long_Complex_Arrays, etc.

{AI95-00296-01} Two types are defined and exported by Numerics.Generic_Complex_Arrays. The composite type Complex_Vector is provided to represent a vector with components of type Complex; it is defined as an unconstrained one-dimensional array with an index of type Integer. The composite type Complex_Matrix is provided to represent a matrix with components of type Complex; it is defined as an unconstrained, two-dimensional array with indices of type Integer.

{AI95-00296-01} The effect of the various subprograms is as described below. In many cases they are described in terms of corresponding scalar operations in Numerics.Generic_Complex_Types. Any exception raised by those operations is propagated by the array subprogram. Moreover, any constraints on the parameters and the accuracy of the result for each individual component are as defined for the scalar operation.

{AI95-00296-01} In the case of those operations which are defined to involve an inner product, Constraint_Error may be raised if an intermediate result has a component outside the range of Real'Base even though the final mathematical result would not.

Discussion: {AI05-0047-1} An inner product never involves implicit complex conjugation. If the product of a vector with the conjugate of another (or the same) vector is required, then this has to be stated explicitly by writing for example X * Conjugate(Y). This mimics the usual mathematical notation.

function Re (X : Complex_Vector) return Real_Vector;
function Im (X : Complex_Vector) return Real_Vector;

{AI95-00296-01} Each function returns a vector of the specified Cartesian components of X. The index range of the result is X'Range.

procedure Set_Re (X  : in out Complex_Vector; Re : in Real_Vector);
procedure Set_Im (X  : in out Complex_Vector; Im : in Real_Vector);

{AI95-00296-01} Each procedure replaces the specified (Cartesian) component of each of the components of X by the value of the matching component of Re or Im; the other (Cartesian) component of each of the components is unchanged. Constraint_Error is raised if X'Length is not equal to Re'Length or Im'Length.

function Compose_From_Cartesian (Re : Real_Vector)
return Complex_Vector;
function Compose_From_Cartesian (Re, Im : Real_Vector)
return Complex_Vector;

{AI95-00296-01} Each function constructs a vector of Complex results (in Cartesian representation) formed from given vectors of Cartesian components; when only the real components are given, imaginary components of zero are assumed. The index range of the result is Re'Range. Constraint_Error is raised if Re'Length is not equal to Im'Length.
function Modulus (X     : Complex_Vector) return Real_Vector;
function "abs" (Right : Complex_Vector) return Real_Vector;
renames Modulus;
function Argument (X     : Complex_Vector) return Real_Vector;
function Argument (X     : Complex_Vector;
                    Cycle : Real'Base) return Real_Vector;

{AI95-00296-01} Each function calculates and returns a vector of the specified polar components of X or Right using the corresponding function in numerics.generic_complex_types. The index range of the result is X'Range or Right'Range.

function Compose_From_Polar (Modulus, Argument : Real_Vector) return Complex_Vector;
function Compose_From_Polar (Modulus, Argument : Real_Vector;
                              Cycle             : Real'Base) return Complex_Vector;

{AI95-00296-01} Each function constructs a vector of Complex results (in Cartesian representation) formed from given vectors of polar components using the corresponding function in numerics.generic_complex_types on matching components of Modulus and Argument. The index range of the result is Modul us'Range. Constraint_Error is raised if Modulus'Length is not equal to Argument'Length.

function "+" (Right : Complex_Vector) return Complex_Vector;
function "-" (Right : Complex_Vector) return Complex_Vector;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation in numerics.generic_complex_types to each component of Right. The index range of the result is Right'Range.

function Conjugate (X : Complex_Vector) return Complex_Vector;

{AI95-00296-01} This function returns the result of applying the appropriate function Conjugate in numerics.generic_complex_types to each component of X. The index range of the result is X'Range.

function "+" (Left, Right : Complex_Vector) return Complex_Vector;
function "-" (Left, Right : Complex_Vector) return Complex_Vector;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation in numerics.generic_complex_types to each component of Left and the matching component of Right. The index range of the result is Left'Range. Constraint_Error is raised if Left'Length is not equal to Right'Length.

function "*" (Left, Right : Complex_Vector) return Complex;

{AI95-00296-01} This operation returns the inner product of Left and Right. Constraint_Error is raised if Left'Length is not equal to Right'Length. This operation involves an inner product.

{AI05-0047-1} function "abs" (Right : Complex_Vector) return Real'BaseComplex;

{AI95-00418-01} This operation returns the Hermitian L2-norm of Right (the square root of the inner product of the vector with its conjugate).

Implementation Note: While the definition is given in terms of an inner product, the norm doesn't "involve an inner product" in the technical sense. The reason is that it has accuracy requirements substantially different from those applicable to inner products; and that cancellations cannot occur, because all the terms are positive, so there is no possibility of intermediate overflow.
function "+" (Left : Real_Vector; Right : Complex_Vector) return Complex_Vector;
function "+" (Left : Complex_Vector; Right : Real_Vector) return Complex_Vector;
function "+" (Left : Real_Vector; Right : Complex_Vector) return Complex_Vector;
function "+" (Left : Complex_Vector; Right : Real_Vector) return Complex_Vector;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation in numerics.generic_complex_types to each component of Left and the matching component of Right. The index range of the result is Left'Range. Constraint_Error is raised if Left'Length is not equal to Right'Length.

function "*" (Left : Real_Vector; Right : Complex_Vector) return Complex;
function "*" (Left : Complex_Vector; Right : Real_Vector) return Complex;

{AI95-00296-01} Each operation returns the inner product of Left and Right. Constraint_Error is raised if Left'Length is not equal to Right'Length. These operations involve an inner product.

function "*" (Left : Complex; Right : Complex_Vector) return Complex_Vector;
function "*" (Left : Complex_Vector; Right : Complex) return Complex_Vector;

{AI95-00296-01} This operation returns the result of multiplying each component of Right by the complex number Left using the appropriate operation "+" in numerics.generic_complex_types. The index range of the result is Right'Range.

function "/" (Left : Complex_Vector; Right : Complex) return Complex_Vector;
function "/" (Left : Real'Base; Right : Complex_Vector) return Complex_Vector;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation in numerics.generic_complex_types to each component of the vector Left and the complex number Right. The index range of the result is Left'Range.

function "/" (Left : Complex_Vector; Right : Real'Base) return Complex_Vector;
function "/" (Left : Real'Base; Right : Complex Vector) return Complex_Vector;

{AI95-00296-01} Each operation returns the result of multiplying each component of Right by the real number Left using the appropriate operation "+" in numerics.generic_complex_types. The index range of the result is Right'Range.

function Unit_Vector (Index : Integer; Order : Positive; First : Integer := 1) return Complex_Vector;

{AI95-00296-01} This function returns a unit vector with Order components and a lower bound of First. All components are set to (0.0, 0.0) except for the Index component which is set to (1.0, 0.0). Constraint_Error is raised if Index < First, Index > First + Order – 1, or if First + Order – 1 > Integer'Last.

function Re (X : Complex_Matrix) return Real_Matrix;
function Im (X : Complex_Matrix) return Real_Matrix;

{AI95-00296-01} Each function returns a matrix of the specified Cartesian components of X. The index ranges of the result are those of X.
procedure Set_Re (X : in out Complex_Matrix; Re : in Real_Matrix);
procedure Set_Im (X : in out Complex_Matrix; Im : in Real_Matrix);

Each procedure replaces the specified (Cartesian) component of each of the
components of X by the value of the matching component of Re or Im; the other (Cartesian)
component of each of the components is unchanged. Constraint_Error is raised if X'Length(1) is
not equal to Re'Length(1) or Im'Length(1) or if X'Length(2) is not equal to Re'Length(2) or
Im'Length(2).

function Compose_From_Cartesian (Re : Real_Matrix) return Complex_Matrix;
function Compose_From_Cartesian (Re, Im : Real_Matrix) return Complex_Matrix;

Each function constructs a matrix of Complex results (in Cartesian
representation) formed from given matrices of Cartesian components; when only the real
components are given, imaginary components of zero are assumed. The index ranges of the result
are those of Re. Constraint_Error is raised if Re'Length(1) is not equal to Im'Length(1) or
Re'Length(2) is not equal to Im'Length(2).

function Modulus  (X     : Complex_Matrix) return Real_Matrix;
function "abs"    (Right : Complex_Matrix) return Real_Matrix
renames Modulus;
function Argument (X     : Complex_Matrix; Cycle : Real'Base) return Real_Matrix;

Each function calculates and returns a matrix of the specified polar components
of X or Right using the corresponding function in numerics.generic_complex_types. The index
ranges of the result are those of X or Right.

function Compose_From_Polar (Modulus, Argument : Real_Matrix)
return Complex_Matrix;
function Compose_From_Polar (Modulus, Argument : Real_Matrix;
Cycle             : Real'Base) return Complex_Matrix;

Each function constructs a matrix of Complex results (in Cartesian
representation) formed from given matrices of polar components using the corresponding
function in numerics.generic_complex_types on matching components of Modulus and
Argument. The index ranges of the result are those of Modulus. Constraint_Error is raised if
Modulus'Length(1) is not equal to Argument'Length(1) or Modulus'Length(2) is not equal to
Argument'Length(2).

function "+" (Right : Complex_Matrix) return Complex_Matrix;
function "+" (Right : Complex_Matrix) return Complex_Matrix;

Each operation returns the result of applying the corresponding operation in
numerals.generic_complex_types to each component of Right. The index ranges of the result are
those of Right.

function Conjugate (X : Complex_Matrix) return Complex_Matrix;

This function returns the result of applying the appropriate function Conjugate
in numerics.generic_complex_types to each component of X. The index ranges of the result are
those of X.

function Transpose (X : Complex_Matrix) return Complex_Matrix;

This function returns the transpose of a matrix X. The first and second index
ranges of the result are X'Range(2) and X'Range(1) respectively.
function "+" (Left, Right : Complex_Matrix) return Complex_Matrix;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation in numerics.generic_complex_types to each component of Left and the matching component of Right. The index ranges of the result are those of Left. Constraint_Error is raised if Left'Length(1) is not equal to Right'Length(1) or Left'Length(2) is not equal to Right'Length(2).

function "-" (Left, Right : Complex_Matrix) return Complex_Matrix;

function "*" (Left, Right : Complex_Matrix) return Complex_Matrix;

{AI95-00296-01} This operation provides the standard mathematical operation for matrix multiplication. The first and second index ranges of the result are Left'Range(1) and Right'Range(2) respectively. Constraint_Error is raised if Left'Length(2) is not equal to Right'Length(1). This operation involves inner products.

function "*" (Left, Right : Complex_Vector) return Complex_Matrix;

{AI95-00296-01} This operation returns the outer product of a (column) vector Left by a (row) vector Right using the appropriate operation "*" in numerics.generic_complex_types for computing the individual components. The first and second index ranges of the result are Left'Range and Right'Range respectively.

function "*" (Left : Complex_Vector; Right : Complex_Matrix) return Complex_Vector;

{AI95-00296-01} This operation provides the standard mathematical operation for multiplication of a (row) vector Left by a matrix Right. The index range of the (row) vector result is Right'Range(2). Constraint_Error is raised if Left'Length is not equal to Right'Length(1). This operation involves inner products.

function "*" (Left : Complex_Matrix; Right : Complex_Vector) return Complex_Vector;

{AI95-00296-01} This operation provides the standard mathematical operation for multiplication of a matrix Left by a (column) vector Right. The index range of the (column) vector result is Left'Range(1). Constraint_Error is raised if Left'Length(2) is not equal to Right'Length. This operation involves inner products.

function "+" (Left : Real_Matrix; Right : Complex_Matrix) return Complex_Matrix;

function "-" (Left : Real_Matrix; Right : Complex_Matrix) return Complex_Matrix;

function "+" (Left : Complex_Matrix; Right : Real_Matrix) return Complex_Matrix;

function "-" (Left : Complex_Matrix; Right : Real_Matrix) return Complex_Matrix;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation in numerics.generic_complex_types to each component of Left and the matching component of Right. The index ranges of the result are those of Left. Constraint_Error is raised if Left'Length(1) is not equal to Right'Length(1) or Left'Length(2) is not equal to Right'Length(2).

function "*" (Left : Real_Matrix; Right : Complex_Matrix) return Complex_Matrix;

function "*" (Left : Complex_Matrix; Right : Real_Matrix) return Complex_Matrix;

{AI95-00296-01} Each operation provides the standard mathematical operation for matrix multiplication. The first and second index ranges of the result are Left'Range(1) and Right'Range(2) respectively. Constraint_Error is raised if Left'Length(2) is not equal to Right'Length(1). These operations involve inner products.
function "*" (Left : Real_Vector; Right : Complex_Vector) return Complex_Matrix;
function "*" (Left : Complex_Vector; Right : Real_Vector) return Complex_Matrix;

{AI95-00296-01} Each operation returns the outer product of a (column) vector Left by a (row) vector Right using the appropriate operation "*" in numerics.generic_complex_types for computing the individual components. The first and second index ranges of the result are Left'Range and Right'Range respectively.

function "*" (Left : Real_Vector; Right : Complex_Matrix) return Complex_Vector;
function "*" (Left : Complex_Vector; Right : Real_Matrix) return Complex_Vector;

{AI95-00296-01} Each operation provides the standard mathematical operation for multiplication of a (row) vector Left by a matrix Right. The index range of the (row) vector result is Right'Range(2). Constraint_Error is raised if Left'Length is not equal to Right'Length(1). These operations involve inner products.

function "*" (Left : Real_Matrix; Right : Complex_Vector) return Complex_Vector;
function "*" (Left : Complex_Matrix; Right : Real_Vector) return Complex_Vector;

{AI95-00296-01} Each operation provides the standard mathematical operation for multiplication of a matrix Left by a (column) vector Right. The index range of the (column) vector result is Left'Range(1). Constraint_Error is raised if Left'Length(2) is not equal to Right'Length. These operations involve inner products.

function "*" (Left : Complex; Right : Complex_Matrix) return Complex_Matrix;
function "*" (Left : Complex_Matrix; Right : Complex) return Complex_Matrix;

{AI95-00296-01} This operation returns the result of multiplying each component of Right by the complex number Left using the appropriate operation "*" in numerics.generic_complex_types. The index ranges of the result are those of Right.

function "*" (Left : Complex_Matrix; Right : Complex) return Complex_Matrix;

{AI95-00296-01} This operation returns the result of applying the corresponding operation in numerics.generic_complex_types to each component of the matrix Left and the complex number Right. The index ranges of the result are those of Left.

function "*" (Left : Real'Base; Right : Complex_Matrix) return Complex_Matrix;

{AI95-00296-01} This operation returns the result of multiplying each component of Right by the real number Left using the appropriate operation "*" in numerics.generic_complex_types. The index ranges of the result are those of Right.

function "*" (Left : Complex Matrix; Right : Real'Base) return Complex_Matrix;
function "/" (Left : Complex Matrix; Right : Real'Base) return Complex Matrix;

{AI95-00296-01} Each operation returns the result of applying the corresponding operation in numerics.generic_complex_types to each component of the matrix Left and the real number Right. The index ranges of the result are those of Left.

function Solve (A : Complex_Matrix; X : Complex_Vector) return Complex_Vector;

{AI95-00296-01} This function returns a vector Y such that X is (nearly) equal to A * Y. This is the standard mathematical operation for solving a single set of linear equations. The index range
of the result is $A'\text{Range(2)}$. Constraint Error is raised if $A'\text{Length(1)}$, $A'\text{Length(2)}$, and $X'\text{Length}$ are not equal. Constraint Error is raised if the matrix $A$ is ill-conditioned.

**Discussion:** The text says that $Y$ is such that “$X$ is (nearly) equal to $A \ast Y$” rather than “$X$ is equal to $A \ast Y$” because rounding errors may mean that there is no value of $Y$ such that $X$ is exactly equal to $A \ast Y$. On the other hand it does not mean that any old rough value will do. The algorithm given under Implementation Advice should be followed.

The requirement to raise Constraint Error if the matrix is ill-conditioned is really a reflection of what will happen if the matrix is ill-conditioned. See Implementation Advice. We do not make any attempt to define ill-conditioned formally.

These remarks apply to all versions of Solve and Inverse.

**function Solve (A, X : Complex_Matrix) return Complex_Matrix;**

{AI95-00296-01} This function returns a matrix $Y$ such that $X$ is (nearly) equal to $A \ast Y$. This is the standard mathematical operation for solving several sets of linear equations. The index ranges of the result are $A'\text{Range(2)}$ and $X'\text{Range(2)}$. Constraint Error is raised if $A'\text{Length(1)}$, $A'\text{Length(2)}$, and $X'\text{Length(1)}$ are not equal. Constraint Error is raised if the matrix $A$ is ill-conditioned.

**function Inverse (A : Complex_Matrix) return Complex_Matrix;**

{AI95-00296-01} This function returns a matrix $B$ such that $A \ast B$ is (nearly) equal to the unit matrix. The index ranges of the result are $A'\text{Range(2)}$ and $A'\text{Range(1)}$. Constraint Error is raised if $A'\text{Length(1)}$ is not equal to $A'\text{Length(2)}$. Constraint Error is raised if the matrix $A$ is ill-conditioned.

**function Determinant (A : Complex_Matrix) return Complex;**

{AI95-00296-01} This function returns the determinant of the matrix $A$. Constraint Error is raised if $A'\text{Length(1)}$ is not equal to $A'\text{Length(2)}$.

**function Eigenvalues(A : Complex_Matrix) return Real_Vector;**

{AI95-00296-01} This function returns the eigenvalues of the Hermitian matrix $A$ as a vector sorted into order with the largest first. Constraint Error is raised if $A'\text{Length(1)}$ is not equal to $A'\text{Length(2)}$. The index range of the result is $A'\text{Range(1)}$. Argument Error is raised if the matrix $A$ is not Hermitian.

**Discussion:** A Hermitian matrix is one whose transpose is equal to its complex conjugate. The eigenvalues of a Hermitian matrix are always real. We only support this case because algorithms for solving the general case are inherently unstable.

**procedure Eigensystem(A : in Complex_Matrix;**

Values : out Real_Vector;

Vectors : out Complex_Matrix);**

{AI95-00296-01} {AI05-0047-1} This procedure computes both the eigenvalues and eigenvectors of the Hermitian matrix $A$. The out parameter Values is the same as that obtained by calling the function Eigenvalues. The out parameter Vectors is a matrix whose columns are the eigenvectors of the matrix $A$. The order of the columns corresponds to the order of the eigenvalues. The eigenvectors are mutually orthonormal, including when there are repeated eigenvalues. Constraint Error is raised if $A'\text{Length(1)}$ is not equal to $A'\text{Length(2)}$, or if Values'Range is not equal to $A'\text{Range(1)}$, or if the index ranges of the parameter Vectors are not equal to those of $A$. Argument Error is raised if the matrix $A$ is not Hermitian. Constraint Error is also raised in implementation-defined circumstances if the algorithm used does not converge quickly enough.

**Ramification: (AI05-0047-1)** There is no requirement on the absolute direction of the returned eigenvectors. Thus they might be multiplied by any complex number whose modulus is 1. It is only the ratios of the components that matter. This is standard practice.
function Unit_Matrix (Order : Positive; First_1, First_2 : Integer := 1) return Complex_Matrix;

{AI95-00296-01} This function returns a square unit matrix with Order**2 components and lower bounds of First_1 and First_2 (for the first and second index ranges respectively). All components are set to (0.0, 0.0) except for the main diagonal, whose components are set to (1.0, 0.0). Constraint Error is raised if First_1 + Order – 1 > Integer'Last or First_2 + Order – 1 > Integer'Last.

Implementation Requirements

{AI95-00296-01} Accuracy requirements for the subprograms Solve, Inverse, Determinant, Eigenvalues and Eigensystem are implementation defined.

Implementation defined: The accuracy requirements for the subprograms Solve, Inverse, Determinant, Eigenvalues and Eigensystem for type Complex_Matrix.

{AI95-00296-01} For operations not involving an inner product, the accuracy requirements are those of the corresponding operations of the type Real'Base and Complex in both the strict mode and the relaxed mode (see G.2).

{AI95-00296-01} For operations involving an inner product, no requirements are specified in the relaxed mode. In the strict mode the modulus of the absolute error of the inner product X*Y shall not exceed $g \ast \text{abs}(X) \ast \text{abs}(Y)$ where $g$ is defined as

$$g = X'\text{Length} \ast \text{Real'Machine\_Radix}^{\ast}(1 – \text{Real'Model\_Mantissa})$$

for mixed complex and real operands

$$g = \sqrt{2.0} \ast X'\text{Length} \ast \text{Real'Machine\_Radix}^{\ast}(1 – \text{Real'Model\_Mantissa})$$

for two complex operands

{AI95-00418-01} For the L2-norm, no accuracy requirements are specified in the relaxed mode. In the strict mode the relative error on the norm shall not exceed $g / 2.0 + 3.0 \ast \text{Real'Model\_Epsilon}$ where $g$ has the definition appropriate for two complex operands.

Documentation Requirements

{AI95-00296-01} Implementations shall document any techniques used to reduce cancellation errors such as extended precision arithmetic.

Documentation Requirement: Any techniques used to reduce cancellation errors in Numerics.Generic_Complex_Arrays shall be documented.

Implementation Note: The above accuracy requirement is met by the canonical implementation of the inner product by multiplication and addition using the corresponding operations of type Complex and performing the cumulative addition using ascending indices. Note however, that some hardware provides special operations for the computation of the inner product and although these may be fast they may not meet the accuracy requirement specified. See Accuracy and Stability of Numerical Algorithms by N J Higham (ISBN 0-89871-355-2), Sections 3.1 and 3.6.

Implementation Permissions

{AI95-00296-01} {AI12-0444-1} The nongeneric equivalent packages can may, but need not, be actual instantiations of the generic package for the appropriate predefined type, though that is not required.

{AI95-00296-01} {AI12-0444-1} Although many operations are defined in terms of operations from Numerics.Generic_Complex_Types, numerics.generic_complex_types, they cannot need not be implemented by other operations that have the same effect.
Implementation Advice

{AI95-00296-01} {AI05-0264-1} Implementations should implement the Solve and Inverse functions using established techniques. Implementations are recommended to refine the result by performing an iteration on the residuals; if this is done, then it should be documented.

**Implementation Advice:** Solve and Inverse for Numerics.Generic.Complex.Arrays should be implemented using established techniques and the result should be refined by an iteration on the residuals.

{AI95-00296-01} It is not the intention that any special provision should be made to determine whether a matrix is ill-conditioned or not. The naturally occurring overflow (including division by zero) which will result from executing these functions with an ill-conditioned matrix and thus raise Constraint_Error is sufficient.

**Discussion:** There isn’t any advice for the implementation to document with this paragraph.

{AI95-00296-01} The test that a matrix is Hermitian should use the equality operator to compare the real components and negation followed by equality to compare the imaginary components (see G.2.1).

**Implementation Advice:** The equality and negation operators should be used to test that a matrix is Hermitian.

An implementation should minimize the circumstances under which the algorithm used for Eigenvalues and Eigensystem fails to converge.


{AI95-00296-01} Implementations should not perform operations on mixed complex and real operands by first converting the real operand to complex.

**Implementation Advice:** Mixed real and complex operations should not be performed by converting the real operand to complex.

**Extensions to Ada 95**

{AI95-00296-01} The package Numerics.Generic.Complex.Arrays and its nongeneric equivalents are new.

**Wording Changes from Ada 2005**

{AI05-0047-1} Correction: Corrected various accuracy and definition issues.
Annex H
High Integrity SystemsSafety and Security

This Annex addresses requirements for high integrity systems (including safety-critical systems and having security-critical systems) constraints. It provides facilities and specifies documentation requirements that relate to several needs:

- Understanding program execution;
- Reviewing object code;
- Restricting language constructs whose usage can complicate the demonstration of program correctness.

Execution understandability is supported by pragma Normalize_Scalars, and also by requirements for the implementation to document the effect of a program in the presence of a bounded error or where the language rules leave the effect unspecified.

The pragmas Reviewable and Restrictions relate to the other requirements addressed by this Annex.

NOTE The Valid attribute (see 13.9.2) is also useful in addressing these needs, to avoid problems that otherwise arise from scalars that have values outside their declared range constraints.

Discussion: The Annex tries to provide high assurance rather than language features. However, it is not possible, in general, to test for high assurance. For any specific language feature, it is possible to demonstrate its presence by a functional test, as in the ACVC. One can also check for the presence of some documentation requirements, but it is not easy to determine objectively that the documentation is “adequate”.

Extensions to Ada 83

This Annex is new to Ada 95.

Wording Changes from Ada 95

The title of this annex was changed to better reflect its purpose and scope. High integrity systems has become the standard way of identifying systems that have high reliability requirements; it subsumes terms such as safety and security. Moreover, the annex does not include any security specific features and as such the previous title is somewhat misleading.

### H.1 Pragma Normalize_Scalars

This pragma ensures that an otherwise uninitialized scalar object is set to a predictable value, but out of range if possible.

Discussion: The goal of the pragma is to reduce the impact of a bounded error that results from a reference to an uninitialized scalar object, by having such a reference violate a range check and thus raise Constraint_Error.

Syntax

The form of a pragma Normalize_Scalars is as follows:

`pragma Normalize_Scalars;`

Post-Compilation Rules

Pragma Normalize_Scalars is a configuration pragma. It applies to all compilation_units included in a partition.
Documentation Requirements

5/2 {AI95-00434-01} If a pragma Normalize_Scalars applies, the implementation shall document the implicit initial values for scalar subtypes, and shall identify each case in which such a value is used and is not an invalid representation.

5.a/2 Documentation Requirement: If a pragma Normalize_Scalars applies, the implicit initial values of scalar subtypes shall be documented. Such a value should be an invalid representation when possible; any cases when is it not shall be documented.

5.b To be honest: It's slightly inaccurate to say that the value is a representation, but the point should be clear anyway.

5.c Discussion: By providing a type with a size specification so that spare bits are present, it is possible to force an implementation of Normalize_Scalars to use an out of range value. This can be tested for by ensuring that Constraint_Error is raised. Similarly, for an unconstrained integer type, in which no spare bit is surely present, one can check that the initialization takes place to the value specified in the documentation of the implementation. For a floating point type, spare bits might not be available, but a range constraint can provide the ability to use an out of range value.

5.d If it is difficult to document the general rule for the implicit initial value, the implementation might choose instead to record the value on the object code listing or similar output produced during compilation.

Implementation Advice

6/2 {AI95-00434-01} Whenever possible, the implicit initial values for a scalar subtype should be an invalid representation (see 13.9.1).

6.a Discussion: When an out of range value is used for the initialization, it is likely that constraint checks will detect it. In addition, it can be detected by the Valid attribute.

6.b/2 This rule is included in the documentation requirements, and thus does not need a separate summary item.

NOTE 1 The initialization requirement applies to uninitialized scalar objects that are subcomponents of composite objects, to allocated objects, and to stand-alone objects. It also applies to scalar out parameters. Scalar subcomponents of composite out parameters are initialized to the corresponding part of the actual, by virtue of 6.4.1.

NOTE 2 The initialization requirement does not apply to a scalar for which pragma Import has been specified, since initialization of an imported object is performed solely by the foreign language environment (see B.1).

NOTE 3 {AI12-0440-1} The use of pragma Normalize_Scalars in conjunction with Pragma Restrictions(No_Exceptions) can result in erroneous execution (see H.4).

9.a Discussion: Since the effect of an access to an out of range value will often be to raise Constraint_Error, it is clear that suppressing the exception mechanism could result in erroneous execution. In particular, the assignment to an array, with the array index out of range, will result in a write to an arbitrary store location, having unpredictable effects.

H.2 Documentation of Implementation Decisions

Documentation Requirements

1/5 {AI12-0439-1} The implementation shall document the range of effects for each situation that the language rules identify as either a bounded error or as having an unspecified effect. If the implementation can constrain the effects of erroneous execution for a given construct, then it shall document such constraints. [The documentation may be provided either independently of any compilation unit or partition, or as part of an annotated listing for a given unit or partition. See also 1.1.3, and 1.1.2.]

1.a/2 This paragraph was deleted. Implementation defined: Information regarding bounded errors and erroneous execution.

1.b/2 Documentation Requirement: The range of effects for each bounded error and each unspecified effect. If the effects of a given erroneous construct are constrained, the constraints shall be documented.

2 NOTE: Among the situations to be documented are the conventions chosen for parameter passing, the methods used for the management of run-time storage, and the method used to evaluate numeric expressions if this involves extended range or extra precision.

2.a Discussion: Look up “unspecified” and “erroneous execution” in the index for a list of the cases.
The management of run-time storage is particularly important. For safety applications, it is often necessary to show that a program cannot raise Storage_Error, and for security applications that information cannot leak via the run-time system. Users are likely to prefer a simple storage model that can be easily validated.

The documentation could helpfully take into account that users may well adopt a subset to avoid some forms of erroneous execution, for instance, not using the abort statement, so that the effects of a partly completed assignment_statement do not have to be considered in the validation of a program (see 9.8). For this reason documentation linked to an actual compilation may be most useful. Similarly, an implementation may be able to take into account use of the Restrictions pragma.

H.3 Reviewable Object Code

Object code review and validation are supported by pragmas Reviewable and Inspection_Point.

H.3.1 Pragma Reviewable

This pragma directs the implementation to provide information to facilitate analysis and review of a program's object code, in particular to allow determination of execution time and storage usage and to identify the correspondence between the source and object programs.

**Discussion:** Since the purpose of this pragma is to provide information to the user, it is hard to objectively test for conformity. In practice, users want the information in an easily understood and convenient form, but neither of these properties can be easily measured.

**Syntax**

The form of a **pragma** Reviewable is as follows:

```plaintext
pragma Reviewable;
```

**Post-Compilation Rules**

Pragma Reviewable is a configuration pragma. It applies to all compilation_units included in a partition.

**Implementation Requirements**

The implementation shall provide the following information for any compilation unit to which such a pragma applies:

**Discussion:** The list of requirements can be checked for, even if issues like intelligibility are not addressed.

- Where compiler-generated runtime checks remain;
  **Discussion:** A constraint check which is implemented via a check on the upper and lower bound should clearly be indicated. If a check is implicit in the form of machine instructions used (such an overflow checking), this should also be covered by the documentation. It is particularly important to cover those checks which are not obvious from the source code, such as that for stack overflow.

- An identification of any construct with a language-defined check that is recognized prior to run time as certain to fail if executed (even if the generation of runtime checks has been suppressed);
  **Discussion:** In this case, if the compiler determines that a check must fail, the user should be informed of this. However, since it is not in general possible to know what the compiler will detect, it is not easy to test for this. In practice, it is thought that compilers claiming conformity to this Annex will perform significant optimizations and therefore will detect such situations. Of course, such events could well indicate a programmer error.

- `{AI95-00209-01}` For each **read_of_reference** to a scalar object, an identification of the **read_of_reference** as either “known to be initialized”, or “possibly uninitialized”, independent of whether pragma Normalize_Scalars applies;
  **Discussion:** This issue again raises the question as to what the compiler has determined. A lazy implementation could clearly mark all scalars as “possibly uninitialized”, but this would be very unhelpful to the user. It should be possible to analyze a range of scalar uses and note the percentage in each class. Note that an access marked “known to be initialized” does not imply that the value is in range, since the initialization could be from an (erroneous) call of unchecked conversion, or by means external to the Ada program.
• Where run-time support routines are implicitly invoked;

  **Discussion:** Validators will need to know the calls invoked in order to check for the correct functionality. For instance, for some safety applications, it may be necessary to ensure that certain sections of code can execute in a particular time.

• An object code listing, including:

  • Machine instructions, with relative offsets;

    **Discussion:** The machine instructions should be in a format that is easily understood, such as the symbolic format of the assembler. The relative offsets are needed in numeric format, to check any alignment restrictions that the architecture might impose.

• Where each data object is stored during its lifetime;

  **Discussion:** This requirement implies that if the optimizer assigns a variable to a register, this needs to be evident.

• Correspondence with the source program, including an identification of the code produced per declaration and per statement.

  **Discussion:** This correspondence will be quite complex when extensive optimization is performed. In particular, address calculation to access some data structures could be moved from the actual access. However, when all the machine code arising from a statement or declaration is in one basic block, this must be indicated by the implementation.

• An identification of each construct for which the implementation detects the possibility of erroneous execution;

  **Discussion:** This requirement is quite vague. In general, it is hard for compilers to detect erroneous execution and therefore the requirement will be rarely invoked. However, if the pragma Suppress is used and the compiler can show that a predefined exception will be raised, then such an identification would be useful.

• For each subprogram, block, task, or other construct implemented by reserving and subsequently freeing an area on a run-time stack, an identification of the length of the fixed-size portion of the area and an indication of whether the non-fixed size portion is reserved on the stack or in a dynamically-managed storage region.

  **Discussion:** This requirement is vital for those requiring to show that the storage available to a program is sufficient. This is crucial in those cases in which the internal checks for stack overflow are suppressed (perhaps by `pragma Restrictions(No_Exceptions)`).

The implementation shall provide the following information for any partition to which the pragma applies:

• An object code listing of the entire partition, including initialization and finalization code as well as run-time system components, and with an identification of those instructions and data that will be relocated at load time;

  **Discussion:** The object code listing should enable a validator to estimate upper bounds for the time taken by critical parts of a program. Similarly, by an analysis of the entire partition, it should be possible to ensure that the storage requirements are suitably bounded, assuming that the partition was written in an appropriate manner.

• A description of the run-time model relevant to the partition.

  **Discussion:** For example, a description of the storage model is vital, since the Ada language does not explicitly define such a model.

The implementation shall provide control- and data-flow information, both within each compilation unit and across the compilation units of the partition.

  **Discussion:** This requirement is quite vague, since it is unclear what control and data flow information the compiler has produced. It is really a plea not to throw away information that could be useful to the validator. Note that the data flow information is relevant to the detection of “possibly uninitialized” objects referred to above.

**Implementation Advice**

The implementation should provide the above information in both a human-readable and machine-readable form, and should document the latter so as to ease further processing by automated tools.
Implementation Advice: The information produced by pragma Reviewable should be provided in both a human-readable and machine-readable form, and the latter form should be documented.

Object code listings should be provided both in a symbolic format and also in an appropriate numeric format (such as hexadecimal or octal).

Implementation Advice: Object code listings should be provided both in a symbolic format and in a numeric format.

Reason: This is to enable other tools to perform any analysis that the user needed to aid validation. The format should be in some agreed form.

NOTE The order of elaboration of library units will be documented even in the absence of pragma Reviewable (see 10.2).

Discussion: There might be some interactions between pragma Reviewable and compiler optimizations. For example, an implementation may disable some optimizations when pragma Reviewable is in force if it would be overly complicated to provide the detailed information to allow review of the optimized object code. See also pragma Optimize (2.8).

Wording Changes from Ada 95

|AI95-00209-01| The wording was clarified that pragma Reviewable applies to each read of an object, as it makes no sense to talk about the state of an object that will immediately be overwritten.

H.3.2 Pragma Inspection_Point

An occurrence of a pragma Inspection_Point identifies a set of objects each of whose values is to be available at the point(s) during program execution corresponding to the position of the pragma in the compilation unit. The purpose of such a pragma is to facilitate code validation.

Discussion: Inspection points are a high level equivalent of break points used by debuggers.

Syntax

The form of a pragma Inspection_Point is as follows:

```
pragma Inspection_Point((object_name {, object_name}));
```

Legality Rules

A pragma Inspection_Point is allowed wherever a declarative_item or statement is allowed. Each object_name shall statically denote the declaration of an object.

Discussion: The static denotation is required, since no dynamic evaluation of a name is involved in this pragma.

Static Semantics

\{8652/0093\} \{AI95-00207-01\} \{AI95-00434-01\} An inspection point is a point in the object code corresponding to the occurrence of a pragma Inspection_Point in the compilation unit. An object is inspectable at an inspection point if the corresponding pragma Inspection_Point either has an argument denoting that object, or has no arguments and the declaration of the object is visible at the inspection point.

Ramification: If a pragma Inspection_Point is in an in-lined subprogram, there might be numerous inspection points in the object code corresponding to the single occurrence of the pragma in the source; similar considerations apply if such a pragma is in a generic, or in a loop that has been “unrolled” by an optimizer.

\{8652/0093\} \{AI95-00207-01\} The short form of the pragma is a convenient shorthand for listing all objects which could be explicitly made inspectable by the long form of the pragma; thus only visible objects are made inspectable by it. Objects that are not visible at the point of the pragma are not made inspectable by the short form pragma. This is necessary so that implementations need not keep information about (or prevent optimizations on) a unit simply because some other unit might contain a short form Inspection_Point pragma.

Discussion: \{8652/0093\} \{AI95-00207-01\} If the short form of the pragma is used, then all visible objects are inspectable. This implies that global objects from other compilation units are out of scope at the point of the pragma are inspectable. A good interactive debugging system could provide information similar to a post-mortem dump at such
inspection points. The annex does not require that any inspection facility is provided, merely that the information is available to understand the state of the machine at those points.

Dynamic Semantics

Execution of a pragma Inspection_Point has no effect.

Discussion: [AI95-00114-01] Although an inspection point has no (semantic) effect, the removal or adding of a new point could change the machine code generated by the compiler.

Implementation Requirements

Reaching an inspection point is an external interaction with respect to the values of the inspectable objects at that point (see 1.1.3).

Ramification: The compiler is inhibited from moving an assignment to an inspectable variable past an inspection point for that variable. On the other hand, the evaluation of an expression that might raise an exception may be moved past an inspection point (see 11.6).

Documentation Requirements

For each inspection point, the implementation shall identify a mapping between each inspectable object and the machine resources (such as memory locations or registers) from which the object's value can be obtained.

This paragraph was deleted. **Implementation defined:** Implementation-defined aspects of pragma Inspection_Point.

**Documentation Requirement:** For each inspection point, a mapping between each inspectable object and the machine resources where the object's value can be obtained shall be provided.

NOTE 1 [AI95-00209-01] [AI12-0447-1] Because reaching an inspection point is considered an external interaction relative to the values of the inspectable variables, the implementation cannot be allowed to perform "dead store elimination" on the last assignment to such a variable prior to an inspection point at a point where the variable is inspectable. Thus an inspection point has the effect of an implicit read of reference to each of its inspectable objects.

NOTE 2 Inspection points are useful in maintaining a correspondence between the state of the program in source code terms, and the machine state during the program's execution. Assertions about the values of program objects can be tested in machine terms at inspection points. Object code between inspection points can be processed by automated tools to verify programs mechanically.

Discussion: Although it is not a requirement of the annex, it would be useful if the state of the stack and heap could be interrogated. This would allow users to check that a program did not have a 'storage leak'.

NOTE 3 [AI12-0447-1] The identification of the mapping from source program objects to machine resources can be in the form of an annotated object listing, in human-readable or tool-processable form.

Discussion: In principle, it is easy to check an implementation for this pragma, since one merely needs to check the content of objects against those values known from the source listing. In practice, one needs a tool similar to an interactive debugger to perform the check.

Wording Changes from Ada 95

{8652/0093} [AI95-00207-01] **Corrigendum:** Corrected the definition of the Inspection_Point pragma to apply to only variables visible at the point of the pragma. Otherwise, the compiler would have to assume that some other code somewhere could have a pragma Inspection_Point, preventing many optimizations (such as unused object elimination).

H.4 High Integrity Restrictions Safety and Security Restrictions

{AI05-0299-1} This subclause defines restrictions that can be used with pragma Restrictions (see 13.12); these facilitate the demonstration of program correctness by allowing tailored versions of the runtime system.

Discussion: [AI95-0005-1] Note that the restrictions are absolute. If a partition has 100 library units and just one needs Unchecked_Conversion, then the pragma cannot be used to ensure the other 99 units do not use Unchecked_Conversion. Note also that these are restrictions on all Ada code within a partition, and therefore it might not be evident from the specification of a package whether a restriction can be imposed.
Static Semantics

This paragraph was deleted. {AI95-00347-01} {AI95-00394-01} The following restrictions, the same as in D.7, apply in this Annex: No_Task_Hierarchy, No_Abort_Statement, No_Implicit_Heap_Allocation, Max_Task_Entries is 0, Max_Asynchronous_Select_Nesting is 0, and Max_Tasks is 0. [The last three restrictions are checked prior to program execution.]

{AI95-00394-01} The following restriction identifiers are language defined: additional restrictions apply in this Annex.

Tasking-related restrictions:

No_Protected_Types
There are no declarations of protected types or protected objects.

Memory-management related restrictions:

No_Allocators
There are no occurrences of an allocator.

{8652/0042} {AI95-00130} No_Local_Allocators Allocators are prohibited in subprograms, generic subprograms, tasks, and entry bodies; instantiations of generic packages are also prohibited in these contexts.

Ramification: Thus allocators are permitted only in expressions whose evaluation can only be performed before the main subprogram is invoked.

This paragraph was deleted. Reason: {8652/0042} {AI95-00130} The reason for the prohibition against instantiations of generic packages is to avoid contract model violations. An alternative would be to prohibit allocators from generic packages, but it seems preferable to allow generality on the defining side and then place the restrictions on the usage (instantiation), rather than inhibiting what can be in the generic while liberalizing where they can be instantiated.

{AI05-0152-1} {AI05-0262-1} No_Anonymous_Allocators There are no allocators of anonymous access types.

{AI05-0190-1} No_Coextensions
There are no coextensions. See 3.10.2.

{AI05-0190-1} No_Access_Parameter_Allocators
Allocators are not permitted as the actual parameter to an access parameter. See 6.1.

Immediate_Reclamation
Except for storage occupied by objects created by allocators and not deallocated via unchecked deallocation, any storage reserved at run time for an object is immediately reclaimed when the object no longer exists.

Discussion: Immediate reclamation would apply to storage created by the compiler, such as for a return value from a function whose size is not known at the call site.

Exception-related restriction:

{AI12-0344-1} No_Exceptions
Raise_statements and exception_handlers are not allowed. No language-defined runtime checks are generated; however, a runtime check performed automatically by the hardware is permitted. The callable entity associated with a procedural_iterator (see 5.5.3) is considered to not allow exit, independent of the value of its Allows_Exit aspect.

Discussion: This restriction mirrors a method of working that is quite common in the safety area. The programmer is required to show that exceptions cannot be raised. Then a simplified run-time system is used without exception
handling. However, some hardware checks may still be enforced. If the software check would have failed, or if the hardware check actually fails, then the execution of the program is unpredictable. There are obvious dangers in this approach, but it is similar to programming at the assembler level.

### Other restrictions:

**No_Floating_Point**  
Uses of predefined floating point types and operations, and declarations of new floating point types, are not allowed.

**Discussion:**  
{AI95-00114-01} The intention is to avoid the use of floating point hardware at run time, but this is expressed in language terms. It is conceivable that floating point is used implicitly in some contexts, say fixed point type conversions of high accuracy. However, the Implementation Requirements below make it clear that the restriction would apply to the “run-time system” and hence not be allowed. This restriction parameter could be used to inform a compiler that a variant of the architecture is being used which does not have floating point instructions.

**No_Fixed_Point**  
Uses of predefined fixed point types and operations, and declarations of new fixed point types, are not allowed.

**Discussion:**  
This restriction would have the side effect of prohibiting the `delay_relative_statement`. As with the No_Floating_Point restriction, this might be used to avoid any question of rounding errors. Unless an Ada run-time is written in Ada, it seems hard to rule out implicit use of fixed point, since at the machine level, fixed point is virtually the same as integer arithmetic.

**No_Access_Subprograms**  
The declaration of access-to-subprogram types is not allowed.

**Discussion:**  
Most critical applications would require some restrictions or additional validation checks on uses of access-to-subprogram types. If the application does not require the functionality, then this restriction provides a means of ensuring the design requirement has been satisfied. The same applies to several of the following restrictions, and to restriction No_Dependence => Ada.Unchecked_Conversion.

**No_Unchecked_Access**  
The Unchecked_Access attribute is not allowed.

**No_Dispatch**  
Occurrences of T’Class are not allowed, for any (tagged) subtype T.

**Discussion:**  
{AI95-00285-01} {AI12-0318-1} No_IO  
Semantic dependence on any of the library units Sequential_IO, Direct_IO, Text_IO, Wide_Text_IO, Wide_Wide_Text_IO, or Stream_IO, or Directories is not allowed.

**Discussion:**  
Excluding the input-output facilities of an implementation may be needed in those environments which cannot support the supplied functionality. A program in such an environment is likely to require some low level facilities or a call on a non-Ada feature.

**No_Delay**  
Delay_Statements and semantic dependence on package Calendar are not allowed.

**Discussion:**  
This implies that delay_alternatives in a select_statement are prohibited.

**Ramification:**  
The purpose of this restriction is to avoid the need for timing facilities within the run-time system.

**No_Recursion**  
As part of the execution of a subprogram, the same subprogram is not invoked.

**No_Recentrancy**  
During the execution of a subprogram by a task, no other task invokes the same subprogram.
No Unspecified Globals

No library-level entity shall have a Global aspect of Unspecified, either explicitly or by default. No library-level entity shall have a Global'Class aspect of Unspecified, explicitly or by default, if it is used as part of a dispatching call.

Ramification: Global'Class need not be specified on an operation if there are no dispatching calls to the operation, or if all of the dispatching calls are covered by dispatching_operation_specifiers for operations with such calls (see H.7).

No Hidden Indirect Globals

When within a context where an applicable global aspect is neither Unspecified nor in out all, any execution within such a context does neither of the following:

- Update (or return a writable reference to) a variable that is reachable via a sequence of zero or more dereferences of access-to-object values from a parameter of a visibly access-to-constant type, from a part of a non-access-type formal parameter of mode in (after any overriding – see H.7), or from a global that has mode in or is not within the applicable global variable set, unless the initial dereference is of a part of a formal parameter or global that is visibly of an access-to-variable type;

- Read (or return a readable reference to) a variable that is reachable via a sequence of zero or more dereferences of access-to-object values from a global that is not within the applicable global variable set, unless the initial dereference is of a part of a formal parameter or global that is visibly of an access-to-object type.

Ramification: The above two rules specify that any hidden indirect references are covered by the global or formal parameter modes that apply, and are not subject to alternative paths of access (such as aliasing) that could result in conflicts. On the other hand, any visible access-to-object parts are allowed to designate objects that are accessible via other means, and side-effects on such objects are permitted if the value is visibly of an access-to-variable type. Such effects do not need to be covered by the applicable global aspect(s), but are rather for the caller to worry about.

For the purposes of the above rules:

- a part of an object is visibly of an access type if the type of the object is declared immediately within the visible part of a package specification, and at the point of declaration of the type the part is visible and of an access type;

- a function returns a writable reference to V if it returns a result with a part that is visibly of an access-to-variable type designating V; similarly, a function returns a readable reference to V if it returns a result with a part that is visibly of an access-to-constant type designating V;

- if an applicable global variable set includes a package name, and the collection of some pool-specific access type (see 7.6.1) is implicitly declared in a part of the declarative region of the package included within the global variable set, then all objects allocated from that collection are considered included within the global variable set.

The consequences of violating the No Hidden Indirect Globals restriction is implementation-defined. Any aspects or other means for identifying such violations prior to or during execution are implementation-defined.

Implementation defined: The consequences of violating No Hidden Indirect Globals.

Discussion: We do not make violations automatically erroneous, because if the implementation chooses to never fully trust it, there is nothing erroneous that can happen. If an implementation chooses to trust the restriction, and performs some optimization as a result of the restriction, the implementation would define such a violation as erroneous. Such an implementation might also endeavor to detect most violations, perhaps by providing additional aspects, thereby reducing the situations which result in erroneous execution. Implementations might detect some but not all violations of the restrictions. Implementations that completely ignore the restriction should treat the restriction as an unsupported capability of Annex H, “High Integrity Systems”.

Dynamic Semantics

The following restriction parameter identifier is language defined:
Max_Image_Length

Specifies the maximum length for the result of an Image, Wide_Image, or Wide_Wide_Image attribute. Violation of this restriction results in the raising of Program_Error at the point of the invocation of an image attribute.

Implementation Requirements

{AI95-00394-01} An implementation of this Annex shall support:

- the restrictions defined in this subclause; and
- {AI05-0189-1} the following restrictions defined in D.7: No Task Hierarchy, No Abort Statement, No Standard Allocators After Elaboration; and
- {AI95-00347-01} the pragma Profile(Ravenscar); and

Discussion: {AI95-00347-01} The reference to pragma Profile(Ravenscar) is intended to show that properly restricted tasking is appropriate for use in high integrity systems. The Ada 95 Annex seemed to suggest that tasking was inappropriate for such systems.

- the following uses of restriction parameter identifiers defined in D.7[, which are checked prior to program execution]:
  - Max_Task_Entries => 0,
  - Max_Asynchronous_Select_Nesting => 0, and
  - Max_Tasks => 0.

{AI12-0020-1} {AI12-0340-1} If a Max_Image_Length restriction applies to any compilation unit in the partition, then for any subtype S, S'Image, S'Wide_Image, and S'Wide_Wide_Image shall be implemented within that partition without any dynamic allocation.

Implementation Note: {AI12-0340-1} {AI12-0384-2} This can be accomplished by using an object of the Text_Buffers.Bounded.Buffer_Type with the maximum characters as specified in the Max_Image_Length restriction, with a raise of Program_Error afterward if Text_Truncated (Buf) is True after the call on Put_Image (Buf, Arg).

{AI05-0263-1} {AI05-0272-1} {AI12-0308-1} If an implementation supports pragma Restrictions for a particular argument, then except for the restrictions No_Unchecked_Deallocation, No_Unchecked_Conversion, No_Access_Subprograms, and No_Unchecked_Access, No_Specification_of_Aspect, No_Use_of_Attribute, No_Use_of_Pragma, No_Dependency => Ada.Unchecked_Conversion, and the equivalent use of No_Dependency => Ada.Unchecked_Deallocation, the associated restriction applies to the run-time system.

Reason: Permission is granted for the run-time system to use the specified otherwise-restricted features, since the use of these features may simplify the run-time system by allowing more of it to be written in Ada.

Discussion: The restrictions that are applied to the partition are also applied to the run-time system. For example, if No_Floating_Point is specified, then an implementation that uses floating point for implementing the delay statement (say) would require that No_Floating_Point is only used in conjunction with No_Delay. It is clearly important that restrictions are effective so that Max_Tasks=0 does imply that tasking is not used, even implicitly (for input-output, say).

An implementation of tasking could be produced based upon a run-time system written in Ada in which the rendezvous was controlled by protected types. In this case, No_Protected_Types could only be used in conjunction with Max_Task_Entries=0. Other implementation dependencies could be envisaged.

If the run-time system is not written in Ada, then the wording needs to be applied in an appropriate fashion.

{AI05-0263-1} {AI12-0308-1} "the equivalent use of No_Dependency" refers to No_Dependency => Ada.Unchecked_Conversion and the like, not all uses of No_Dependency.
Documentation Requirements

If a pragma Restrictions(No_Exceptions) is specified, the implementation shall document the effects of all constructs where language-defined checks are still performed automatically (for example, an overflow check performed by the processor).

This paragraph was deleted.

Implementation defined: Implementation defined aspects of pragma Restrictions.

Documentation Requirement: If a pragma Restrictions(No Exceptions) is specified, the effects of all constructs where language-defined checks are still performed.

Discussion: {AI95-00114-01} The documentation requirements here are quite difficult to satisfy. One method is to review the object code generated and determine the checks that are still present, either explicitly, or implicitly within the architecture. As another example from that of overflow, consider the question of dereferencing a null pointer. This could be undertaken by a memory access trap when checks are performed. When checks are suppressed via the argument No_Exceptions, it would not be necessary to have the memory access trap mechanism enabled.

Erroneous Execution

Program execution is erroneous if pragma Restrictions(No_Exceptions) has been specified and the conditions arise under which a generated language-defined runtime check would fail.

Discussion: The situation here is very similar to the application of pragma Suppress. Since users are removing some of the protection the language provides, they had better be careful!

Program execution is erroneous if pragma Restrictions(No_Recursion) has been specified and a subprogram is invoked as part of its own execution, or if pragma Restrictions(No_Reentrancy) has been specified and during the execution of a subprogram by a task, another task invokes the same subprogram.

Discussion: {AI05-0005-1} In practice, many implementations might not exploit the absence of recursion or need for reentrancy, in which case the program execution would be unaffected by the use of recursion or reentrancy, even though the program is still formally erroneous.

This paragraph was deleted.

Implementation defined: Any restrictions on pragma Restrictions.

NOTE {AI95-00394-01} {AI95-0040-1} Uses of restriction parameter identifier No Dependence defined in 13.12.1: No Dependence => Ada.Unchecked_Deallocation and No Dependence => Ada.Unchecked_Conversion can be appropriate for high-integrity systems. Other uses of No_Dependence can also be appropriate for high-integrity systems.

Discussion: The specific mention of these two uses is meant to replace the identifiers now banished to J.13, “Dependence Restriction Identifiers”.

Restriction No Dependence => Ada.Unchecked_Deallocation would be useful in those contexts in which heap storage is needed on program start-up, but need not be increased subsequently. The danger of a dangling pointer can therefore be avoided.

Extensions to Ada 95

{8652/0042} {AI95-00130-01} No_Local_Allocators no longer prohibits generic instantiations.

Wording Changes from Ada 95

{AI95-00285-01} Wide Wide Text IO (which is new) is added to the No IO restriction.

{AI95-00347-01} {AI95-0299-1} The title of this subclause was changed to match the change to the Annex title. Pragma Profile(Ravenscar) is part of this annex.

{AI95-00394-01} Restriction No Dependence is used instead of special restriction_identifiers. The old names are banished to Obsolescent Features (see J.13).

{AI95-00394-01} The bizarre wording “apply in this Annex” (which no one quite can explain the meaning of) is banished.

Extensions to Ada 2005

{AI95-0152-1} {AI95-0190-1} Restrictions No Anonymous Allocators, No Coextensions, and No Access Parameter Allocators are new.
Wording Changes from Ada 2005

AI05-0189-1 New restriction No Standard Allocators After Elaboration is added to the list of restrictions that are required by this annex.

AI05-0263-1 Correction: Ada 2005 restriction No Dependence is added where needed (this was missed in Ada 2005).

AI05-0272-1 Restrictions against individual aspects, pragmas, and attributes do not apply to the run-time system, in order that an implementation can use whatever aspects, pragmas, and attributes are needed to do the job. For instance, attempting to write a run-time system for Linux that does not use the Import aspect would be very difficult and probably is not what the user is trying to prevent anyway.

Incompatibilities With Ada 2012

AI12-0318-1 Correction: Restriction No_IO now excludes use of Ada.Directories. If a program using No_IO used Ada.Directories, it would be legal in Ada 2012 and illegal in Ada 2022. However, given the role of Ada.Directories as a support package for the other packages that are excluded by No_IO, it seems unlikely that any use of the restriction would use this package (and it's possible that implementations wouldn't support its use with No_IO anyway).

Extensions to Ada 2012

AI12-0020-1 Restriction Max Image Length is new.

AI12-0079-3 Restrictions No Unspecified Globals and No Hidden Indirect Globals are new.

H.4.1 Aspect No_Controlled_Parts

Static Semantics

AI12-0256-1 AI12-0403-1 For a type, the following type-related, operational aspect may be specified:

AI12-0256-1 No_Controlled_Parts

The type of this aspect is Boolean. If True, the type and any descendants shall not have any controlled parts. If specified, the value of the expression shall be static. If not specified, the value of this aspect is False.

Aspect Description for No_Controlled_Parts: A specification that a type and its descendants do not have controlled parts.

AI12-0256-1 The No_Controlled_Parts aspect is nonoverridable (see 13.1.1).

Discussion: Since this is a Boolean-valued aspect, the blanket restrictions defined by 13.1.1 apply to the specification of Boolean-valued aspects on descendants of types with such aspects. But we still need rules about inheritance from progenitors and about hiding the aspect; it would be too painful to repeat those rules here (and have future maintenance fixes not get applied to this aspect).

Legality Rules

AI12-0256-1 AI12-0407-1 If No_Controlled_Parts is True for a type, no component of the type shall have a controlled part nor shall the type itself be controlled. For the purposes of this rule, a type has a controlled part if its full type has a controlled part; this is applied recursively. In addition to the places where Legality Rules normally apply (see 12.3), this rule also applies in the private part of an instance of a generic unit.

Discussion: This check breaks privacy by looking at the full definition of all of the types involved. This is more like a representation aspect than an operational aspect, but representation aspects are not allowed on partial views and we need this aspect to be visible to clients.

AI12-0256-1 AI12-0407-1 When enforcing the above rule within a generic body G or within the body of a generic unit declared within the declarative region of generic unit G, a generic formal private type of G and a generic formal derived type of G whose ancestor is a tagged type whose No_Controlled_Parts aspect is False are considered to have a controlled part.

Reason: This is a typical generic assume-the-worst rule.
To be honest: {AI12-0407-1} If the ancestor of the generic derived type is class-wide, the aspect in question belongs to the specific type associated with the class-wide type.

Extensions to Ada 2012

{AI12-0256-1} {AI12-0407-1} Aspect No_Controlled_Parts is new.

H.5 Pragma Detect_Blocking

{AI95-00305-01} {AI12-0267-1} The following pragma requires forces an implementation to detect potentially blocking operations during the execution of within a protected operation or a parallel construct.

Syntax

{AI95-00305-01} The form of a pragma Detect_Blocking is as follows:

pragma Detect_Blocking;

Post-Compilation Rules

{AI95-00305-01} A pragma Detect_Blocking is a configuration pragma.

Dynamic Semantics

{AI95-00305-01} {AI12-0247-1} {AI12-0267-1} An implementation is required to detect a potentially blocking operation that occurs during the execution of within a protected operation or a parallel construct defined within a compilation unit to which the pragma applies, and to raise Program_Error (see 9.59.5.1).

Implementation Permissions

{AI95-00305-01} {AI12-0267-1} An implementation is allowed to reject a compilation unit to which a pragma Detect_Blocking applies if a potentially blocking operation is present directly within an entry body, or the body of a protected subprogram, or a parallel construct occurring within the compilation unit.

NOTE {AI95-00305-01} {AI12-0442-1} An operation that causes a task to be blocked within a foreign language domain is not defined to be potentially blocking, and is unlikely to need not be detected.

Extensions to Ada 95

{AI95-00305-01} Pragma Detect_Blocking is new.

Extensions to Ada 2012

{AI12-0267-1} Pragma Detect_Blocking now applies to parallel constructs as well as protected actions.

H.6 Pragma Partition_Elaboration_Policy

{AI95-00265-01} {AI05-0299-1} This subclause defines a pragma for user control over elaboration policy.

Syntax

{AI95-00265-01} The form of a pragma Partition_Elaboration_Policy is as follows:

pragma Partition_Elaboration_Policy (policy_identifier);

The policy_identifier shall be either Sequential, Concurrent or an implementation-defined identifier.

Implementation defined: Implementation-defined policy identifiers allowed in a pragma Partition_Elaboration_Policy.
Ramiﬁcation: Note that the Ravenscar proﬁle (see D.13) has nothing to say about which Partition Elaboration Policy is used. This was intentionally omitted from the proﬁle, as there was no agreement as to whether the Sequential policy should be required for Ravenscar programs. As such it was deﬁned separately.

Post-Compilation Rules

{AI95-00265-01} A pragma Partition Elaboration Policy is a conﬁguration pragma. It speciﬁes the elaboration policy for a partition. At most one elaboration policy shall be speciﬁed for a partition.

{AI95-00265-01} {AI05-0264-1} If the Sequential policy is speciﬁed for a partition, then pragma Restrictions (No_Task_Hierarchy) shall also be speciﬁed for the partition.

Dynamic Semantics

{AI95-00265-01} Notwithstanding what this document says elsewhere, this pragma allows partition elaboration rules concerning task activation and interrupt attachment to be changed. If the policy identiﬁer is Concurrent, or if there is no pragma Partition Elaboration Policy deﬁned for the partition, then the rules deﬁned elsewhere in this Reference Manual apply.

{AI95-00265-01} {AI95-00421-01} If the partition elaboration policy is Sequential, then task activation and interrupt attachment are performed in the following sequence of steps:

1. The activation of all library-level tasks and the attachment of interrupt handlers are deferred until all library units are elaborated.
2. The interrupt handlers are attached by the environment task.
3. The environment task is suspended while the library-level tasks are activated.
4. The environment task executes the main subprogram (if any) concurrently with these executing tasks.

{AI95-00265-01} {AI95-00421-01} If several dynamic interrupt handler attachments for the same interrupt are deferred, then the most recent call of Attach_Handler or Exchange_Handler determines which handler is attached.

{AI95-00265-01} {AI95-00421-01} If any deferred task activation fails, Tasking Error is raised at the beginning of the sequence of statements of the body of the environment task prior to calling the main subprogram.

Implementation Advice

{AI95-00265-01} {AI05-0264-1} If the partition elaboration policy is Sequential and the Environment task becomes permanently blocked during elaboration, then the partition is deadlocked and it is recommended that the partition be immediately terminated.

Implementation Advice: If the partition elaboration policy is Sequential and the Environment task becomes permanently blocked during elaboration, then the partition should be immediately terminated.

Implementation Permissions

{AI95-00265-01} {AI05-0264-1} If the partition elaboration policy is Sequential and any task activation fails, then an implementation may immediately terminate the active partition to mitigate the hazard posed by continuing to execute with a subset of the tasks being active.

NOTE {AI95-00421-01} {AI12-0440-1} If any deferred task activation fails, the environment task is unable to handle the Tasking Error exception and completes immediately. By contrast, if the partition elaboration policy is Concurrent, then this exception cannot be handled within a library unit.

Extensions to Ada 95

{AI95-00265-01} {AI95-00421-01} Pragma Partition Elaboration Policy is new.
H.7 Extensions to Global and Global'Class Aspects

{AI12-0079-3} In addition to the entities specified in 6.1.2, the Global aspect may be specified for a subtype (including a formal subtype), formal package, formal subprogram, and formal object of an anonymous access-to-subprogram type.

Syntax

{AI12-0079-3} The following additional syntax is provided to override the mode of a formal parameter to reflect indirect effects on variables reachable from the formal parameter by one or more access-value dereferences:

extended_global_mode ::= overriding basic_global_mode

Name Resolution Rules

{AI12-0079-3} The object name that is associated with an overriding mode shall resolve to statically denote a formal object, or a formal parameter of the associated entity.

Static Semantics

{AI12-0079-3} The presence of the reserved word overriding in a global mode indicates that the specification is overriding the mode of a formal parameter with another mode to reflect the overall effect of an invocation of the callable entity on the state associated with the corresponding actual parameter.

{AI12-0380-1} [As described in 6.1.2, the following rules are defined in terms of operations that are performed by or on behalf of an entity.]

{AI12-0079-3} {AI12-0431-1} {AI12-0439-1} The Global aspect for a subtype identifies the global variables that can be referenced during default initialization, adjustment as part of assignment, finalization of an object of the subtype, or conversion to the subtype, including the evaluation of any assertion expressions that apply. If not specified for the first subtype of a derived type, the aspect defaults to that of the ancestor subtype; if not specified for a nonderived composite first subtype the aspect defaults to that of the enclosing library unit; if not specified for a nonderived elementary first subtype (or scalar base subtype), the aspect defaults to null in the absence of a predicate (or when the predicate is statically True), and to that of the enclosing library unit otherwise. If not specified for a nonfirst subtype $S$, the Global aspect defaults to that of the subtype identified in the subtype indication defining $S$.

{AI12-0079-3} The Global'Class aspect may be specified for the first subtype of a tagged type $T$, indicating an upper bound on the Global aspect of any descendant of $T$. If not specified, it defaults to Unspecified.

Legality Rules

{AI12-0079-3} For a tagged subtype $T$, each mode of its Global aspect shall identify a subset of the variables identified either by the corresponding mode, or by the in out mode, of the Global'Class aspect of the first subtype of any ancestor of $T$.

Extensions to Ada 2012

{AI12-0079-3} {AI12-0380-1} These extensions to the Global aspect are new.
H.7.1 **The Use_Formal and Dispatching Aspects**

{AI12-0380-1} The Use Formal and Dispatching aspects are provided to more precisely describe the use of generic formal parameters and dispatching calls within the execution of an operation, enabling more precise checking of conformance with the Nonblocking and global aspects that apply at the point of invocation of the operation.

{AI12-0079-3} {AI12-0380-1} For any declaration within a generic unit for which a global or Nonblocking aspect may be specified, other than a generic formal parameter declaration, the following aspect may be specified to indicate which generic formal parameters are used by the associated entity:

{AI12-0380-1} **Use_Formal**

The aspect is specified with a **formal_parameter_set**, with the following form:

**Aspect Description for Use_Formal:** Generic formal parameters used in the implementation of an entity.

```
formal_parameter_set ::= 
    formal_group_designator
    | formal_parameter_name
    | (formal_parameter_name, formal_parameter_name)
```

```
formal_group_designator ::= null | all
```

```
formal_parameter_name ::= 
    formal_subtype_mark
    | formal_subprogram_name
    | formal_access_to_subprogram_object_name
```

{AI12-0079-3} {AI12-0380-1} For any declaration for which a global or Nonblocking aspect may be specified, other than for a library package, a generic library package, or a generic formal, the following aspect may be specified:

{AI12-0380-1} **Dispatching**

The aspect is specified with a **dispatching_operation_set**, with the following form:

**Aspect Description for Dispatching:** Generic formal parameters used in the implementation of an entity.

```
dispatching_operation_set ::= 
    dispatching_operation_specifier
    | (dispatching_operation_specifier, dispatching_operation_specifier)
```

```
dispatching_operation_specifier ::= 
    dispatching_operation_name (object_name)
```

**Name Resolution Rules**

{AI12-0380-1} A **formal_parameter_name** in a Use_Formal aspect shall resolve to statically denote a formal subtype, a formal subprogram, or a formal object of an anonymous access-to-subprogram type of an enclosing generic unit or visible formal package.

{AI12-0380-1} The **object_name** of a dispatching_operation_specifier shall resolve to statically name an object (including possibly a formal parameter) of a tagged class-wide type **T**Class, or of an access type designating a tagged class-wide type **T**Class; the **dispatching_operation_name** of the dispatching_operation_specifier shall resolve to statically denote a dispatching operation associated with **T**.
The formal parameter set is identified by a set of formal parameter names. Alternatively, the reserved word null may be used to indicate none of the generic formal parameters, or all to indicate all of the generic formal parameters, of any enclosing generic unit (or visible formal package) can be used within the execution of the operation. If there is no formal parameter set specified for an entity declared within a generic unit, it defaults to all.

The dispatching operation set is identified by a set of dispatching_operation_specifiers. It indicates that the Nonblocking and global effects of dispatching calls that match one of the specifiers, rather than being accounted for by the Nonblocking or global aspect, are instead to be accounted for by the invoker of the operation. A dispatching call matches a dispatching_operation_specifier if the name or prefix of the call statically denotes the same operation(s) as that of the dispatching_operation_specifier, and at least one of the objects controlling the call is denoted by, or designated by, a name that statically names the same object as that denoted by the object name of the dispatching_operation_specifier.

Ramification: The object "controlling the call" is not necessarily a controlling parameter of the call if the call is a function with a controlling result or has parameters that is such a function. It is one of the objects that provide the dispatching tag used for the call; that could, for example, be a parameter of a function used as a parameter to the call, or an object being assigned to, or a parameter of an enclosing call.

In the absence of any dispatching_operation_specifiers, or if none of them match a dispatching call C within an operation P, Nonblocking and global aspects checks are performed at the point of the call C within P using the Nonblocking and Global'Class aspects that apply to the dispatching operation named in call C. If there is a match, any global access or potential blocking within the subprogram body invoked by the call C is ignored at the point of call within P. Instead, when the operation P itself is invoked, Nonblocking and global aspect checks are performed presuming each named dispatching operation is called at least once (with the named object controlling the call), but similarly ignoring those dispatching calls that would match a dispatching_operation_specifier applicable at the point of invocation of P.

Within an operation to which a Use_Formal aspect applies, if the formal parameter set is anything but all, then the only generic formal subtypes that may be used, the only formal subprograms that may be called, and the only formal objects of an anonymous access-to-subprogram type that may be dereferenced as part of a call or passed as the actual for an access parameter, are those included in the formal parameter set.

When an operation (or instance thereof) to which a Use_Formal aspect applies is invoked, Nonblocking and global aspect checks are performed presuming each generic formal parameter (or corresponding actual parameter) of the formal parameter set is used at least once.

An example of use of the Dispatching aspect:

```ada
procedure My_Write(  
    Stream : not null access Ada.Streams.Root_Stream_Type'Class; 
    Item   : My_Integer'Base) 
with Dispatching => Write(Stream); 
for My_Integer'Write use My_Write;
```

For examples of use of the Use_Formal aspect, see the Element functions of Hashed_Sets in A.18.8.
The aspects Use_Formal and Dispatching are new.
Annex J
(normative)
Obsolescent Features

{AI95-00368-01} [ This Annex contains descriptions of features of the language whose functionality is largely redundant with other features defined by this Reference Manual. Use of these features is not recommended in newly written programs. Use of these features can be prevented by using pragma Restrictions (No_Obsolescent_Features), see 13.12.1.]

Ramification: These features are still part of the language, and have to be implemented by conforming implementations. The primary reason for putting these descriptions here is to get redundant features out of the way of most readers. The designers of the next version of Ada after Ada 95 will have to assess whether or not it makes sense to drop these features from the language.

Wording Changes from Ada 83

The following features have been removed from the language, rather than declared to be obsolescent:

- The package Low_Level_IO (see A.6).
- The Epsilon, Mantissa, Emax, Small, Large, Safe_Emax, Safe_Small, and Safe_Large attributes of floating point types (see A.5.3).
- This paragraph was deleted {AI95-00284-02} The pragma Interface (see B.1).
- The pragmas System_Name, Storage_Unit, and Memory_Size (see 13.7).
- The pragma Shared (see C.6).

Implementations can continue to support the above features for upward compatibility.

Wording Changes from Ada 95

{AI95-00368-01} A mention of the No_Obsolescent_Features restriction was added.

Wording Changes from Ada 2005

{AI05-0229-1} Pragma Controlled has been removed from the language, rather than declared to be obsolescent. No existing implementation gives it any effect. An implementation could continue to support the pragma as an implementation-defined pragma for upward compatibility.

J.1 Renamings of Library Units

Renamings of Ada 83 Library Units

Static Semantics

The following library_unit_renaming_declarations exist:

```adatrue
with Ada.Unchecked_Conversion;
generic function Unchecked_Conversion renames Ada.Unchecked_Conversion;
with Ada.Unchecked_Deallocation;
generic procedure Unchecked_Deallocation renames Ada.Unchecked_Deallocation;
with Ada.Sequential_IO;
generic package Sequential_IO renames Ada.Sequential_IO;
with Ada.Direct_IO;
generic package Direct_IO renames Ada.Direct_IO;
with Ada.Text_IO;
package Text_IO renames Ada.Text_IO;
with Ada.IO_Exceptions;
package IO_Exceptions renames Ada.IO_Exceptions;
with Ada.Calendar;
package Calendar renames Ada.Calendar;
```
with System.Machine_Code;

Discussion: {AI05-0004-1} These library units correspond to those declared in Ada 83, which did not have the child unit concept or the parent package Ada.

Implementation Requirements

The implementation shall allow the user to replace these renamings.

J.2 Allowed Replacements of Characters

Syntax

The following replacements are allowed for the vertical line, number sign, and quotation mark characters:

- A vertical line character (|) can be replaced by an exclamation mark (!) where used as a delimiter.
- The number sign characters (#) of a based_literal can be replaced by colons (:) provided that the replacement is done for both occurrences.
- The quotation marks (") used as string brackets at both ends of a string literal can be replaced by percent signs (%) provided that the enclosed sequence of characters contains no quotation mark, and provided that both string brackets are replaced. Any percent sign within the sequence of characters shall then be doubled and each such doubled percent sign is interpreted as a single percent sign character value.

These replacements do not change the meaning of the program.

Reason: The original purpose of this feature was to support hardware (for example, teletype machines) that has long been obsolete. The feature is no longer necessary for that reason. Another use of the feature has been to replace the vertical line character (|) when using certain hardware that treats that character as a (non-English) letter. The feature is no longer necessary for that reason, either, since Ada 95 has full support for international character sets. Therefore, we believe this feature is no longer necessary.

Users of equipment that still uses | to represent a letter will continue to do so. Perhaps by the time Ada is revised, such equipment will no longer be in use.

Note that it was never legal to use this feature as a convenient method of including double quotes in a string without doubling them — the string literal:

```verbatim"This is quoted.""```

is not legal in Ada (and never was legal)83, nor will it be in Ada 95. One has to write:

```verbatim""This is quoted.""```

J.3 Reduced Accuracy Subtypes

A digits_constraint may be used to define a floating point subtype with a new value for its requested decimal precision, as reflected by its Digits attribute. Similarly, a delta_constraint may be used to define an ordinary fixed point subtype with a new value for its delta, as reflected by its Delta attribute.

Discussion: It might be more direct to make these attributes specifiable via an attribute_definition_clause, and eliminate the syntax for these _constraint.

Syntax

```verbatim
{AI12-0152-1} delta_constraint ::= delta static simple_expression expression [range_constraint]
```
Name Resolution Rules

\{AI12-0152-1\} The \texttt{simple_expression} of a \texttt{delta_constraint} is expected to be of any real type.

Legality Rules

\{AI12-0152-1\} The \texttt{simple_expression} of a \texttt{delta_constraint} shall be static.

For a \texttt{subtype_indication} with a \texttt{delta_constraint}, the \texttt{subtype_mark} shall denote an ordinary fixed point subtype.

For a \texttt{subtype_indication} with a \texttt{digits_constraint}, the \texttt{subtype_mark} shall denote either a decimal fixed point subtype or a floating point subtype (notwithstanding the rule given in 3.5.9 that only allows a decimal fixed point subtype).

\textit{This paragraph was deleted} \textbf{Discussion:} \{AI95-00114-01\} We may need a better way to deal with obsolescent features with rules that contradict those of the nonobsolescent parts of the standard.

Static Semantics

\{AI12-0152-1\} A \texttt{subtype_indication} with a \texttt{subtype_mark} that denotes an ordinary fixed point subtype and a \texttt{delta_constraint} defines an ordinary fixed point subtype with a \texttt{delta} given by the value of the \texttt{simple_expression} of the \texttt{delta_constraint}. If the \texttt{delta_constraint} includes a \texttt{range_constraint}, then the ordinary fixed point subtype is constrained by the \texttt{range_constraint}.

\{AI12-0152-1\} A \texttt{subtype_indication} with a \texttt{subtype_mark} that denotes a floating point subtype and a \texttt{digits_constraint} defines a floating point subtype with a requested decimal precision (as reflected by its \texttt{Digits} attribute) given by the value of the \texttt{simple_expression} of the \texttt{digits_constraint}. If the \texttt{digits_constraint} includes a \texttt{range_constraint}, then the floating point subtype is constrained by the \texttt{range_constraint}.

Dynamic Semantics

\{AI12-0152-1\} A \texttt{delta_constraint} is \textit{compatible} with an ordinary fixed point subtype if the value of the \texttt{simple_expression} is no less than the \texttt{delta} of the subtype, and the \texttt{range_constraint}, if any, is compatible with the subtype.

\{AI12-0152-1\} A \texttt{digits_constraint} is \textit{compatible} with a floating point subtype if the value of the \texttt{simple_expression} is no greater than the requested decimal precision of the subtype, and the \texttt{range_constraint}, if any, is compatible with the subtype.

The elaboration of a \texttt{delta_constraint} consists of the elaboration of the \texttt{range_constraint}, if any.

\textbf{Reason:} A numeric subtype is considered “constrained” only if a range constraint applies to it. The only effect of a \texttt{digits_constraint} or a \texttt{delta_constraint} without a \texttt{range_constraint} is to specify the value of the corresponding \texttt{Digits} or \texttt{Delta} attribute in the new subtype. The set of values of the subtype is not “constrained” in any way by such \_\texttt{constraints}.

Wording Changes from Ada 83

In Ada 83, a \texttt{delta_constraint} is called a \texttt{fixed_point_constraint}, and a \texttt{digits_constraint} is called a \texttt{floating_point_constraint}. We have adopted other terms because \texttt{digits_constraints} apply primarily to decimal fixed point types now (they apply to floating point types only as an obsolescent feature).

Wording Changes from Ada 2012

\{AI12-0152-1\} \textbf{Corrigendum:} Changed the syntax so that the value following \texttt{delta} in a \texttt{delta_constraint} is a \texttt{simple_expression}. This is compatible as any expressions that would require extra parentheses are already illegal. The change is necessary to eliminate syntax ambiguities in \texttt{derived_type_definition}s. The similar change for \texttt{digits_constraint} is documented in 3.5.9.
J.4 The Constrained Attribute

Static Semantics

For every private subtype \( S \), the following attribute is defined:

\[ S'\text{Constrained} \]

Yields the value \( \text{False} \) if \( S \) denotes an unconstrained nonformal private subtype with discriminants; also yields the value \( \text{False} \) if \( S \) denotes a generic formal private subtype, and the associated actual subtype is either an unconstrained subtype with discriminants or an unconstrained array subtype; yields the value \( \text{True} \) otherwise. The value of this attribute is of the predefined subtype Boolean.

Reason: Because Ada 95 has unknown_d Discriminant_ Parts, the Constrained attribute of private subtypes is obsolete. This is fortunate, since its Ada 83 definition was confusing, as explained below. Because this attribute is obsolete, we do not bother to extend its definition to private extensions.

The Constrained attribute of an object is not obsolete.

Note well: \( S'\text{Constrained} \) matches the Ada 95 definition of “constrained” only for composite subtypes. For elementary subtypes, \( S'\text{Constrained} \) is always true, whether or not \( S \) is constrained. (The Constrained attribute of an object does not have this problem, as it is only defined for objects of a discriminated type.) So one should think of its designator as being ′Constrained Or _Elementary.

J.5 ASCII

Static Semantics

The following declaration exists in the declaration of package Standard:

\[ \text{package ASCII is} \]

\[ \quad \text{-- Control characters:} \]

\[ \quad \text{NUL} : \text{constant Character} := \text{nul}; \quad \text{SOH} : \text{constant Character} := \text{soh}; \]
\[ \quad \text{STX} : \text{constant Character} := \text{stx}; \quad \text{ETX} : \text{constant Character} := \text{etx}; \]
\[ \quad \text{EOT} : \text{constant Character} := \text{eot}; \quad \text{ENQ} : \text{constant Character} := \text{eng}; \]
\[ \quad \text{ACK} : \text{constant Character} := \text{ack}; \quad \text{BEL} : \text{constant Character} := \text{bel}; \]
\[ \quad \text{BS} : \text{constant Character} := \text{bs}; \quad \text{HT} : \text{constant Character} := \text{ht}; \]
\[ \quad \text{LF} : \text{constant Character} := \text{lf}; \quad \text{VT} : \text{constant Character} := \text{vt}; \]
\[ \quad \text{FF} : \text{constant Character} := \text{ff}; \quad \text{CR} : \text{constant Character} := \text{cr}; \]
\[ \quad \text{SO} : \text{constant Character} := \text{so}; \quad \text{SI} : \text{constant Character} := \text{si}; \]
\[ \quad \text{DLE} : \text{constant Character} := \text{dle}; \quad \text{DC1} : \text{constant Character} := \text{dc1}; \]
\[ \quad \text{DC2} : \text{constant Character} := \text{dc2}; \quad \text{DC3} : \text{constant Character} := \text{dc3}; \]
\[ \quad \text{DC4} : \text{constant Character} := \text{dc4}; \quad \text{NAK} : \text{constant Character} := \text{nak}; \]
\[ \quad \text{SYN} : \text{constant Character} := \text{syn}; \quad \text{ETB} : \text{constant Character} := \text{etb}; \]
\[ \quad \text{CAN} : \text{constant Character} := \text{can}; \quad \text{EM} : \text{constant Character} := \text{em}; \]
\[ \quad \text{SUB} : \text{constant Character} := \text{sub}; \quad \text{ESC} : \text{constant Character} := \text{esc}; \]
\[ \quad \text{FS} : \text{constant Character} := \text{fs}; \quad \text{GS} : \text{constant Character} := \text{gs}; \]
\[ \quad \text{RS} : \text{constant Character} := \text{rs}; \quad \text{US} : \text{constant Character} := \text{us}; \]
\[ \quad \text{DEL} : \text{constant Character} := \text{del}; \]

\[ \quad \text{-- Other characters:} \]

\[ \quad \text{Exclam} : \text{constant Character} := '!'; \quad \text{Quotation} : \text{constant Character} := \text{"}; \]
\[ \quad \text{Sharp} : \text{constant Character} := '\#'; \quad \text{Dollar} : \text{constant Character} := '\$'; \]
\[ \quad \text{Percent} : \text{constant Character} := '\%'; \quad \text{Ampersand} : \text{constant Character} := '\&'; \]
\[ \quad \text{Colon} : \text{constant Character} := '\:'; \quad \text{Semicolon} : \text{constant Character} := '\;'; \]
\[ \quad \text{Query} : \text{constant Character} := '\?'; \quad \text{At_Sign} : \text{constant Character} := '@'; \]
\[ \quad \text{L_Bracket} : \text{constant Character} := '\['; \quad \text{Back_Slash} : \text{constant Character} := '\\'; \]
\[ \quad \text{R_Bracket} : \text{constant Character} := '\]'; \quad \text{Circumflex} : \text{constant Character} := '\^'; \]
\[ \quad \text{Underline} : \text{constant Character} := '\_'; \quad \text{Grave} : \text{constant Character} := '\\'; \]
\[ \quad \text{L_Brake} : \text{constant Character} := '\{'; \quad \text{Bar} : \text{constant Character} := '\|'; \]
\[ \quad \text{R_Brake} : \text{constant Character} := '\}'; \quad \text{Tilde} : \text{constant Character} := '\~'; \]
-- Lower case letters:
LC_A: constant Character:= 'a';
...
LC_Z: constant Character:= 'z';
end ASCII;

J.6 Numeric_Error

Static Semantics

The following declaration exists in the declaration of package Standard:

Numeric_Error : exception renames Constraint_Error;

Discussion: This is true even though it is not shown in A.1.
Reason: In Ada 83, it was unclear which situations should raise Numeric_Error, and which should raise Constraint_Error. The permissions of RM83-11.6 could often be used to allow the implementation to raise Constraint_Error in a situation where one would normally expect Numeric_Error. To avoid this confusion, all situations that raise Numeric_Error in Ada 83 are changed to raise Constraint_Error in Ada 95. Numeric_Error is changed to be a renaming of Constraint_Error to avoid most of the upward compatibilities associated with this change.
In new code, Constraint_Error should be used instead of Numeric_Error.

J.7 At Clauses

Syntax

at_clause ::= for direct_name use at expression;

Static Semantics

An at_clause of the form “for x use at y;” is equivalent to an attribute_definition_clause of the form “for x'Address use y;”.

Reason: The preferred syntax for specifying the address of an entity is an attribute_definition_clause specifying the Address attribute. Therefore, the special-purpose at_clause syntax is now obsolete.
The above equivalence implies, for example, that only one at_clause is allowed for a given entity. Similarly, it is illegal to give both an at_clause and an attribute_definition_clause specifying the Address attribute.

Extensions to Ada 83

We now allow to define the address of an entity using an attribute_definition_clause. This is because Ada 83's at_clause is so hard to remember: programmers often tend to write “for X'Address use...;”.

Wording Changes from Ada 83

Ada 83's address_clause is now called an at_clause to avoid confusion with the new term “Address clause” (that is, an attribute_definition_clause for the Address attribute).

J.7.1 Interrupt Entries

[Implementations are permitted to allow the attachment of task entries to interrupts via the address clause. Such an entry is referred to as an interrupt entry.
The address of the task entry corresponds to a hardware interrupt in an implementation-defined manner. (See Ada.Interrupts.Reference in C.3.2.])

Static Semantics

The following attribute is defined:
For any task entry X:

X'Address For a task entry whose address is specified (an interrupt entry), the value refers to the corresponding hardware interrupt. For such an entry, as for any other task entry, the meaning of this value is implementation defined. The value of this attribute is of the type of the subtype System.Address.

Address may be specified for single entries via an attribute_definition_clause.

Reason: Because of the equivalence of at_clauses and attribute_definition_clauses, an interrupt entry may be specified via either notation.

Dynamic Semantics

As part of the initialization of a task object, the address clause for an interrupt entry is elaborated[, which evaluates the expression of the address clause]. A check is made that the address specified is associated with some interrupt to which a task entry may be attached. If this check fails, Program_Error is raised. Otherwise, the interrupt entry is attached to the interrupt associated with the specified address.

Upon finalization of the task object, the interrupt entry, if any, is detached from the corresponding interrupt and the default treatment is restored.

While an interrupt entry is attached to an interrupt, the interrupt is reserved (see C.3).

An interrupt delivered to a task entry acts as a call to the entry issued by a hardware task whose priority is in the System.Interrupt_Priority range. It is implementation defined whether the call is performed as an ordinary entry call, a timed entry call, or a conditional entry call; which kind of call is performed can depend on the specific interrupt.

Bounded (Run-Time) Errors

It is a bounded error to evaluate E'Caller (see C.7.1) in an accept_statement for an interrupt entry. The possible effects are the same as for calling Current_Task from an entry body.

Documentation Requirements

The implementation shall document to which interrupts a task entry may be attached.

Documentation Requirement: The interrupts to which a task entry may be attached.

The implementation shall document whether the invocation of an interrupt entry has the effect of an ordinary entry call, conditional call, or a timed call, and whether the effect varies in the presence of pending interrupts.

Documentation Requirement: The type of entry call invoked for an interrupt entry.

Implementation Permissions

The support for this subclause is optional.

Interrupts to which the implementation allows a task entry to be attached may be designated as reserved for the entire duration of program execution[, that is, not just when they have an interrupt entry attached to them].

Interrupt entry calls may be implemented by having the hardware execute directly the appropriate accept_statement.accept_body. Alternatively, the implementation is allowed to provide an internal interrupt handler to simulate the effect of a normal task calling the entry.

The implementation is allowed to impose restrictions on the specifications and bodies of tasks that have interrupt entries.

It is implementation defined whether direct calls (from the program) to interrupt entries are allowed.
If a select_statement contains both a terminate_alternative and an accept_alternative for an interrupt entry, then an implementation is allowed to impose further requirements for the selection of the terminate_alternative in addition to those given in 9.3.

NOTE 1 {8652/0077} {AI95-00111-01} Queued interrupts correspond to ordinary entry calls. Interrupts that are lost if not immediately processed correspond to conditional entry calls. It is a consequence of the priority rules that an accept_statement/accept_body executed in response to an interrupt can be executed with the active priority at which the hardware generates the interrupt, taking precedence over lower priority tasks, without a scheduling action.

NOTE 2 Control information that is supplied upon an interrupt can be passed to an associated interrupt entry as one or more parameters of mode in.

Examples

Example of an interrupt entry:

```
task Interrupt_Handler is
  entry Done;
  for Done'Address use Ada.Interrupts.Reference(Ada.Interrupts.Names.Device_Done);
end Interrupt_Handler;
```

Wording Changes from Ada 83

{AI95-00114-01} RM83-13.5.1 did not adequately address the problems associated with interrupts. This feature is now obsolescent and is replaced by the Ada 95 interrupt model as specified in the Systems Programming Annex.

Wording Changes from Ada 95

{8652/0077} {AI95-00111-01} Corrigendum: The undefined term accept body was replaced by accept_statement.

J.8 Mod Clauses

Syntax

```
mod_clause ::= at mod static_expression;
```

Static Semantics

A record_representation_clause of the form:

```
{AI05-0092-1} for r use
record at mod a;
...
end record;
```

is equivalent to:

```
for r'Alignment use a;
for r use
record
...
end record;
```

Reason: The preferred syntax for specifying the alignment of an entity is an attribute_definition_clause specifying the Alignment attribute. Therefore, the special-purpose mod_clause syntax is now obsolete.

The above equivalence implies, for example, that it is illegal to give both a mod_clause and an attribute_definition_clause specifying the Alignment attribute for the same type.

Wording Changes from Ada 83

Ada 83’s alignment_clause is now called a mod_clause to avoid confusion with the new term “Alignment clause” (that is, an attribute_definition_clause for the Alignment attribute).
J.9 The Storage_Size Attribute

Static Semantics

For any task subtype T, the following attribute is defined:

\[ T\text{'Storage_Size} \]

Denotes an implementation-defined value of type \textit{universal_integer} representing the number of storage elements reserved for a task of the subtype T.

\textbf{To be honest:} \{\textit{AI05-0229-1}\} T\text{'Storage_Size} cannot be particularly meaningful in the presence of the specification of the \textbf{pragma} \textit{Storage_Size}, especially when the expression is dynamic, or depends on a discriminant of the task, because the Storage_Size will be different for different objects of the type. Even without such a \textbf{specification pragma}, the Storage_Size can be different for different objects of the type, and in any case, the value is implementation defined. Hence, it is always implementation defined.

\{\textit{AI95-00345-01}\} \{\textit{AI05-0229-1}\} Storage_Size may be specified for a task first subtype that is not an interface via an attribute_definition_clause. When the attribute is specified, the Storage_Size aspect is specified to be the value of the given expression.

\textbf{Ramification:} \{\textit{AI05-0229-1}\} When this attribute is specified with an attribute_definition_clause, the associated aspect is set to the value of the expression given in the attribute_definition_clause, rather than the expression itself. This value is therefore the same for all objects of the type; in particular, it is not re-evaluated when objects are created. This is different than when the aspect is specified with an \textbf{aspect specification} (see 13.3).

Wording Changes from Ada 95

\{\textit{AI95-00345-01}\} We don't allow specifying Storage_Size on task interfaces. We don't need to mention class-wide task types, because these cannot be a first subtype.

J.10 Specific Suppression of Checks

\{\textit{AI95-00224-01}\} Pragma Suppress can be used to suppress checks on specific entities.

Syntax

\{\textit{AI95-00224-01}\} The form of a specific Suppress \textbf{pragma} is as follows:

\[
\texttt{pragma Suppress(identifier, [On => name]);}
\]

Legality Rules

\{\textit{AI95-00224-01}\} The identifier shall be the name of a check (see 11.5). The name shall statically denote some entity.

\{\textit{AI95-00224-01}\} For a specific Suppress \textbf{pragma} that is immediately within a package specification, the name shall denote an entity (or several overloaded subprograms) declared immediately within the package specification.

Static Semantics

\{\textit{AI95-00224-01}\} A specific Suppress \textbf{pragma} applies to the named check from the place of the \textbf{pragma} to the end of the innermost enclosing declarative region, or, if the \textbf{pragma} is given in a package specification, to the end of the scope of the named entity. The \textbf{pragma} applies only to the named entity, or, for a subtype, on objects and values of its type. A specific Suppress \textbf{pragma} suppresses the named check for any entities to which it applies (see 11.5). Which checks are associated with a specific entity is not defined by this document.

\textbf{Discussion:} The language doesn't specify exactly which entities control whether a check is performed. For example, in

\[
\texttt{pragma Suppress (Range_Check, On => A); A := B;}
\]
whether or not the range check is performed is not specified. The compiler may require that checks are suppressed on B or on the type of A in order to omit the range check.

Implementation Permissions

\{AI95-00224-01\} An implementation is allowed to place restrictions on specific Suppress pragmas.

NOTE \{AI95-00224-01\} \{AI12-0440-1\} An implementation can support a similar On parameter on pragma Unsuppress (see 11.5).

Wording Changes from Ada 95

\{AI95-00224-01\} \{AI95-0299-1\} This subclause is new. This feature was moved here because it is important for pragma Unsuppress that there be an unambiguous meaning for each checking pragma. For instance, in the example

\begin{verbatim}
pragma Suppress (Range Check);
pragma Unsuppress (Range Check, On => A);
A := B;
\end{verbatim}

the user needs to be able to depend on the range check being made on the assignment. But a compiler survey showed that the interpretation of this feature varied widely; trying to define this carefully was likely to cause a lot of user and implementer pain. Thus the feature was moved here, to emphasize that its use is not portable.

J.11 The Class Attribute of Untagged Incomplete Types

Static Semantics

\{AI95-00326-01\} For the first subtype S of a type T declared by an incomplete_type_declaration that is not tagged, the following attribute is defined:

\{AI95-00326-01\} S'Class

Denotes the first subtype of the incomplete class-wide type rooted at T. The completion of T shall declare a tagged type. Such an attribute reference shall occur in the same library unit as the incomplete_type_declaration.

Reason: \{AI95-00326-01\} This must occur in the same unit to prevent children from imposing requirements on their ancestor library units for deferred incomplete types.

Wording Changes from Ada 95

\{AI95-00326-01\} \{AI95-0299-1\} This subclause is new. This feature was moved here because the tagged incomplete type provides a better way to provide this capability (it doesn't put requirements on the completion based on uses that could be anywhere). Pity we didn't think of it in 1994.

J.12 Pragma Interface

Syntax

\{AI95-00284-02\} In addition to an identifier, the reserved word interface is allowed as a pragma name, to provide compatibility with a prior edition of this Reference Manual.

Implementation Note: \{AI95-00284-02\} All implementations need to at least recognize and ignore this pragma. A syntax error is not an acceptable implementation of this pragma.

Wording Changes from Ada 95

\{AI95-00326-01\} \{AI95-0299-1\} This subclause is new. This is necessary as interface is now a reserved word, which would prevent pragma Interface from being an implementation-defined pragma. We don't define any semantics for this pragma, as we expect that implementations will continue to use whatever they currently implement - requiring any changes would be counter-productive.
J.13 Dependence Restriction Identifiers

\{[AI95-00394-01]\} The following restrictions involve dependence on specific language-defined units. The more general restriction No_Dependence (see 13.12.1) should be used for this purpose.

Static Semantics

\{[AI95-00394-01]\} The following restriction identifiers exist:

\{[AI95-00394-01]\} No_Asynchronous_Control

Semantic dependence on the predefined package Asynchronous_Task_Control is not allowed.

\{[AI95-00394-01]\} No_Unchecked_Conversion

Semantic dependence on the predefined generic function Unchecked_Conversion is not allowed.

\{[AI95-00394-01]\} No_Unchecked_Deallocation

Semantic dependence on the predefined generic procedure Unchecked_Deallocation is not allowed.

Wording Changes from Ada 95

\{[AI95-00394-01]\} \{[AI05-0299-1]\} This subclause is new. These restrictions are replaced by the more general No_Dependence (see 13.12.1).

J.14 Character and Wide_Character Conversion Functions

Static Semantics

\{[AI95-00395-01]\} The following declarations exist in the declaration of package Ada.Characters.Handling:

\function Is_Character \{Item : in Wide_Character\} return Boolean renames Conversions.Is_Character;

\function Is_String \{Item : in Wide_String\} return Boolean renames Conversions.Is_String;

\function To_Character \{Item : in Wide_Character; Substitute : in Character := ' '} return Character renames Conversions.To_Character;

\function To_String \{Item : in Wide_String; Substitute : in Character := ' '} return String renames Conversions.To_String;

\function To_Wide_Character \{Item : in Character\} return Wide_Character renames Conversions.To_Wide_Character;

\function To_Wide_String \{Item : in String\} return Wide_String renames Conversions.To_Wide_String;

Wording Changes from Ada 95

\{[AI95-00394-01]\} \{[AI05-0299-1]\} This subclause is new. These subprograms were moved to Characters.Conversions (see A.3.4).

J.15 Aspect-related Pragmas

\{[AI05-0229-1]\} Pragmas can be used as an alternative to aspect specifications to specify certain aspects.
Name Resolution Rules

\{AI12-0417-1\} Certain pragmas are defined to be program unit pragmas. A name given as the argument of a program unit pragma shall resolve to denote the declarations or renamings of one or more program units that occur immediately within the declarative region or compilation in which the pragma immediately occurs, or it shall resolve to denote the declaration of the immediately enclosing program unit (if any); the pragma applies to the denoted program unit(s). If there are no names given as arguments, the pragma applies to the immediately enclosing program unit.

**Ramification:** The fact that this is a Name Resolution Rule means that the pragma will not apply to declarations from outer declarative regions.

Legality Rules

\{AI12-0417-1\} A program unit pragma shall appear in one of these places:

- \{AI12-0417-1\} At the place of a compilation unit, in which case the pragma shall immediately follow in the same compilation (except for other pragmas) a library unit declaration that is a subprogram declaration, generic subprogram declaration, or generic instantiation, and the pragma shall have an argument that is a name denoting that declaration.

  **Ramification:** The name has to denote the immediately preceding library unit declaration.

- \{8652/0033\} \{AI95-00136-01\} \{AI12-0417-1\} Immediately within the visible part of a program unit and before any nested declaration (but not within a generic formal part), in which case the argument, if any, shall be a direct name that denotes the immediately enclosing program unit declaration.

  **Ramification:** The argument is optional in this case.

- \{AI12-0417-1\} At the place of a declaration other than the first, of a declarative part or program unit declaration, in which case the pragma shall have an argument, which shall be a direct name that denotes one or more of the following (and nothing else): a subprogram declaration, a generic subprogram declaration, or a generic instantiation, of the same declarative part or program unit declaration.

  **Ramification:** If you want to denote a subprogram body that is not a completion, or a package declaration, for example, you have to put the pragma inside.

\{AI05-0132-1\} \{AI12-0417-1\} Certain program unit pragmas are defined to be library unit pragmas. If a library unit pragma applies to a program unit, the program unit shall be The name, if any, in a library unit pragma shall denote the declaration of a library unit.

**Ramification:** This, together with the rules for program unit pragmas above, implies that if a library unit pragma applies to a subprogram declaration (and similar things), it has to appear immediately after the compilation unit, whereas if the pragma applies to a package declaration, a subprogram body that is not a completion (and similar things), it has to appear inside, as the first declarative item.

Static Semantics

\{8652/0034\} \{AI95-00041-01\} \{AI12-0417-1\} A library unit pragma that applies to a generic unit does not apply to its instances, unless a specific rule for the pragma specifies the contrary.

Implementation Advice

\{8652/0034\} \{AI95-00041-01\} \{AI12-0417-1\} When applied to a generic unit, a program unit pragma that is not a library unit pragma should apply to each instance of the generic unit for which there is not an overriding pragma applied directly to the instance.

**Implementation Advice:** When applied to a generic unit, a program unit pragma that is not a library unit pragma should apply to each instance of the generic unit for which there is not an overriding pragma applied directly to the instance.
J.15.1 Pragma Inline

Syntax

The form of a pragma Inline, which is a program unit pragma (see 10.1.5), is as follows:

```
pragma Inline (name{, name});
```

Legality Rules

The pragma shall apply to one or more callable entities or generic subprograms.

Static Semantics

Pragma Inline specifies that the Inline aspect (see 6.3.2) for each entity denoted by each name given in the pragma has the value True.

Ramification: Note that inline expansion is desired no matter what name is used in the call. This allows one to request inlining for only one of several overloaded subprograms as follows:

```
package IO is
  procedure Put(X : in Integer);
  procedure Put(X : in String);
  procedure Put(X : in Character);
private
  procedure Character_Put(X : in Character) renames Put;
pragma Inline(Character_Put);
end IO;
```

```
with IO; use IO;
procedure Main IO is
  I : Integer;
  C : Character;
begin
  ... Put(C); -- Inline expansion is desired.
  Put(I); -- Inline expansion is NOT desired.
end Main;
```

Implementation Permissions

An implementation may allow a pragma Inline that has an argument which is a direct_name denoting a subprogram_body of the same declarative_part.

Reason: This is allowed for Ada 83 compatibility. This is only a permission as this usage was considered obsolescent even for Ada 95.

Discussion: We only need to allow this in declarative_parts, because a body is only allowed in another body, and these all have declarative_parts.

NOTE: The name in a pragma Inline can only denote more than one entity in the case of overloading. Such a pragma applies to all of the denoted entities.
Incompatibilities With Ada 83

{AI95-00309-01} {AI05-0229-1} A pragma Inline cannot refer to a subprogram_body outside of that body. The pragma can be given inside of the subprogram body. Ada 2005 adds an Implementation Permission to allow this usage for compatibility (and Ada 95 implementations also can use this permission), but implementations do not have to allow such pragmas.

Extensions to Ada 83

{AI05-0229-1} A pragma Inline is allowed inside a subprogram body if there is no corresponding subprogram declaration. This is for uniformity with other program unit pragmas.

Extensions to Ada 95

{AI95-00309-01} {AI05-0229-1} Amendment Correction: Implementations are allowed to let Pragma Inline apply to a subprogram_body.

Wording Changes from Ada 2005

{AI05-0229-1} {AI05-0299-1} This subclause is new. Pragma Inline was moved here from 6.3.2; aspect Inline lives there now.

J.15.2 Pragma No_Return

Syntax

{AI05-0229-1} The form of a pragma No_Return, which is a representation pragma (see 13.1), is as follows:

{AI12-0269-1} pragma No_Return (subprogram local name, procedure local name, {, subprogram local name, procedure local name});

Legality Rules

{AI05-0229-1} {AI12-0269-1} Each subprogram local name procedure local name shall denote one or more subprograms procedures or generic subprograms procedures [The subprogram local name procedure local name shall not denote a null procedure nor an instance of a generic unit.]

Static Semantics

{AI05-0229-1} {AI12-0269-1} Pragma No_Return specifies that the No_Return aspect (see 6.5.1) for each subprogram procedure denoted by each local name given in the pragma has the value True.

Wording Changes from Ada 2005

{AI05-0229-1} {AI05-0299-1} This subclause is new. Pragma No_Return was moved here from 6.5.1; aspect No_Return lives there now.

Wording Changes from Ada 2012

{AI12-0269-1} This subclause is new. Pragma No_Return was moved here from 6.5.1; aspect No_Return lives there now.

J.15.3 Pragma Pack

Syntax

{AI05-0229-1} The form of a pragma Pack, which is a representation pragma (see 13.1), is as follows:

pragma Pack (first subtype local name);
Legality Rules

\{AI05-0229-1\} The first subtype local name of a pragma Pack shall denote a composite subtype.

Static Semantics

\{AI05-0229-1\} Pragma Pack specifies that the Pack aspect (see 13.2) for the type denoted by first subtype local name has the value True.

Wording Changes from Ada 2005

\{AI05-0229-1\} \{AI05-0299-1\} This subclause is new. Pragma Pack was moved here from 13.2; aspect Pack lives there now.

J.15.4 Pragma Storage Size

Syntax

\{AI05-0229-1\} The form of a pragma Storage Size is as follows:

```
pragma Storage_Size (expression);
```

\{AI05-0229-1\} A pragma Storage Size is allowed only immediately within a task_definition.

Name Resolution Rules

\{AI05-0229-1\} The expression of a pragma Storage_Size is expected to be of any integer type.

Static Semantics

\{AI05-0229-1\} The pragma Storage_Size sets the Storage Size aspect (see 13.3) of the type defined by the immediately enclosing task_definition to the value of the expression of the pragma.

Wording Changes from Ada 2005

\{AI05-0229-1\} \{AI05-0299-1\} This subclause is new. Pragma Storage Size was moved here from 13.3; aspect Storage_Size lives there now.

J.15.5 Interfacing Pragmas

Syntax

\{AI05-0229-1\} An interfacing pragma is a representation pragma that is one of the pragmas Import, Export, or Convention. Their forms are as follows:

```
pragma Import(
  [Con\text{\textunderscore}vention =>] convention\_identifier, [Entity =>] local\_name
  [, [External\_Name =>] external\_name\_string\_expression]
  [, [Link\_Name =>] link\_name\_string\_expression]);
```

```
pragma Export(
  [Con\text{\textunderscore}vention =>] convention\_identifier, [Entity =>] local\_name
  [, [External\_Name =>] external\_name\_string\_expression]
  [, [Link\_Name =>] link\_name\_string\_expression]);
```

```
pragma Convention([Con\text{\textunderscore}vention =>] convention\_identifier,[Entity =>] local\_name);
```

\{AI05-0229-1\} For pragmas Import and Export, the argument for Link_Name shall not be given without the pragma_argument_identifier unless the argument for External_Name is given.
Name Resolution Rules

The expected type for an external name string expression and a link name string expression in an interfacing pragma is String.

Legality Rules

The convention identifier of an interfacing pragma shall be the name of a convention (see B.1).

A pragma Import shall be the completion of a declaration. Notwithstanding any rule to the contrary, a pragma Import may serve as the completion of any kind of (explicit) declaration if supported by an implementation for that kind of declaration. If a completion is a pragma Import, then it shall appear in the same declarative part, package specification, task definition, or protected definition as the declaration. For a library unit, it shall appear in the same compilation, before any subsequent compilation units other than pragmas. If the local name denotes more than one entity, then the pragma Import is the completion of all of them.

The external name string expression and link name string expression of a pragma Import or Export shall be static.

The local name of each of these pragmas shall denote a declaration that may have the similarly named aspect specified.

Static Semantics

An interfacing pragma specifies various aspects of the entity denoted by the local name as follows:

- The Convention aspect (see B.1) is convention identifier.
- A pragma Import specifies that the Import aspect (see B.1) is True.
- A pragma Export specifies that the Export aspect (see B.1) is True.
- For both pragma Import and Export, if an external name is given in the pragma, the External Name aspect (see B.1) is specified to be external name string expression. If a link name is given in the pragma, the Link Name aspect (see B.1) is specified to be the link name string expression.

Wording Changes from Ada 2005

This subclause is new. Pragmas Import, Export, and Convention were moved here from B.1; aspects Import, Export, Convention, Link_Name, and External_Name live there now.

J.15.6 Pragma Unchecked_Union

Syntax

The form of a pragma Unchecked_Union, which is a representation pragma (see 13.1), is as follows:

pragma Unchecked_Union (first_subtype local_name);

Legality Rules

The first subtype local name of a pragma Unchecked_Union shall denote an unconstrained discriminated record subtype having a variant part.
Static Semantics

\{AI05-0229-1\} A **pragma** Unchecked_Union specifies that the Unchecked_Union aspect (see B.3.3) for the type denoted by `first_subtype local_name` has the value True.

Wording Changes from Ada 2005

\{AI05-0229-1\} \{AI05-0299-1\} This subclause is new. Pragma Unchecked_Union was moved here from B.3.3; aspect Unchecked_Union lives there now.

**J.15.7 Pragmas Interrupt_Handler and Attach_Handler**

**Syntax**

\{AI05-0229-1\} The form of a **pragma** Interrupt_Handler is as follows:

\begin{verbatim}
pragma Interrupt_Handler (handler_name);
\end{verbatim}

\{AI05-0229-1\} The form of a **pragma** Attach_Handler is as follows:

\begin{verbatim}
pragma Attach_Handler (handler_name, expression);
\end{verbatim}

**Name Resolution Rules**

\{AI05-0229-1\} For the Interrupt_Handler and Attach_Handler pragmas, the `handler_name` shall resolve to denote a protected procedure with a parameterless profile.

\{AI05-0229-1\} For the Attach_Handler pragma, the expected type for the `expression` is `Interruption.Interrupt_Id` (see C.3.2).

**Legality Rules**

\{AI05-0033-1\} \{AI05-0229-1\} The Attach_Handler and Interrupt_Handler pragmas are only allowed immediately within the protected definition where the corresponding subprogram is declared. The corresponding `protected_type_declaration` or `single_protected_declaration` shall be a library-level declaration, and shall not be declared within a generic body. In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

**Discussion:** In the case of a `protected_type_declaration`, an `object_declaration` of an object of that type need not be at library level.

\{AI05-0033-1\} We cannot allow these pragmas in a generic body, because legality rules are not checked for instance bodies, and these should not be allowed if the instance is not at the library level. The protected types can be declared in the private part if this is desired. Note that while the `Access to use the handler` would provide the check in the case of Interrupt_Handler, there is no other check for Attach_Handler. Since these pragmas are so similar, we want the rules to be the same.

**Static Semantics**

\{AI05-0229-1\} For an implementation that supports Annex C, a **pragma** Interrupt_Handler specifies the Interrupt_Handler aspect (see C.3.1) for the protected procedure `handler_name` to have the value True. For an implementation that supports Annex C, a **pragma** Attach_Handler specifies the Attach_Handler aspect (see C.3.1) for the protected procedure `handler_name` to have the value of the given `expression` (as evaluated at object creation time).

Incompatibilities With Ada 2005

\{AI05-0033-1\} **Correction:** Added missing generic contract wording for the **pragma** Attach_Handler and **pragma** Interrupt_Handler. This means that nested instances with these pragmas in the private part are now illegal. This is not likely to occur in practice.
Wording Changes from Ada 2005

{AI05-0229-1} {AI05-0299-1} This subclause is new. Pragmas Interrupt_Handler and Attach_Handler were moved here from C.3.1; aspects Interrupt_Handler and Attach_Handler live there now.

J.15.8 Shared Variable Pragmas

Syntax

{AI05-0229-1} {AI12-0425-1} The following form for pragmas are defined with the given forms Atomic, Volatile, Independent, Atomic_Components, and Volatile_Components, and Independent_Components is as follows:

pragma Atomic (local_name);
pragma Volatile (local_name);
pragma Independent (component_local_name);
pragma Atomic_Components (array_local_name);
pragma Volatile_Components (array_local_name);
pragma Independent_Components (local_name);

Discussion: {AI05-0009-1} {AI05-0229-1} Pragmas Independent and Independent_Components are born obsolete; they are defined to provide consistency with the existing shared variable pragmas. As with all obsolete features, these pragmas are not optional; all Ada implementations need to implement them. Also note that these pragmas were defined as a Correction; as such, they are expected to be implemented as part of Ada 2005 implementations (and they would not be obsolete there).

Name Resolution Rules

{AI05-0009-1} {AI05-0229-1} The local_name in an Atomic or Volatile pragma shall resolve to denote either an object_declaration, a noninherited component_declaration, or a full_type_declaration. The component_local_name in an Independent pragma shall resolve to denote a noninherited component_declaration. The array_local_name in an Atomic_Components or Volatile_Components pragma shall resolve to denote the declaration of an array type or an array object of an anonymous type. The local_name in an Independent_Components pragma shall resolve to denote the declaration of an array or record type or an array object of an anonymous type.

Static Semantics

{AI05-0229-1} These pragmas are representation pragmas (see 13.1). Each of these pragmas specifies that the similarly named aspect (see C.6) of the type, object, or component denoted by its argument is True.

Legality Rules

{AI05-0229-1} The local_name of each of these pragmas shall denote a declaration that may have the similarly named aspect specified.

Wording Changes from Ada 2005

{AI05-0229-1} {AI05-0299-1} This subclause is new. These pragmas were moved here from C.6; various aspects live there now.
J.15.9 Pragma CPU

Discussion: {AI05-0229-1} This pragma is born obsolescent; it is defined to provide consistency with existing real-time pragmas. As with all obsolescent features, this pragma is not optional; all Ada implementations need to implement it.

Syntax

{AI05-0229-1} The form of a pragma CPU is as follows:

```
pragma CPU (expression);
```

Name Resolution Rules

{AI05-0229-1} The expected type for the expression of a pragma CPU is System.Multiprocessors.CPU_Range.

Legality Rules

{AI05-0229-1} {AI12-0281-1} A CPU pragma is allowed only immediately within a task_definition, protected_definition, or the declarative_part of a subprogram_body.

{AI05-0229-1} For a CPU pragma that appears in the declarative_part of a subprogram_body, the expression shall be static.

Static Semantics

{AI05-0229-1} {AI12-0281-1} For an implementation that supports Annex D, a pragma CPU specifies the value of the CPU aspect (see D.16). If the pragma appears in a task_definition, the expression is associated with the aspect for the task type or single_task_declaration that contains the pragma. If the pragma appears in a protected_definition, the expression is associated with the aspect for the protected type or single_protected_declaration that contains the pragma. Otherwise, otherwise, the expression is associated with the aspect for the subprogram that contains the pragma.

Extensions to Ada 2005

{AI05-0009-1} Pragma CPU is new.

J.15.10 Pragma Dispatching_Domain

Discussion: {AI05-0167-1} This pragma is born obsolescent; it is defined to provide consistency with existing real-time pragmas. As with all obsolescent features, this pragma is not optional; all Ada implementations need to implement it.

Syntax

{AI05-0167-1} The form of a pragma Dispatching_Domain is as follows:

```
pragma Dispatching_Domain (expression);
```

Name Resolution Rules

{AI05-0167-1} The expected type for the expression is System.Multiprocessors.Dispatching_Domains DISPATCHING_DOMAIN.

Legality Rules

{AI05-0167-1} A Dispatching_Domain pragma is allowed only immediately within a task_definition.
Static Semantics

\{AI05-0167-1\} For an implementation that supports Annex D, a pragma Dispatching_Domain specifies the value of the Dispatching_Domain aspect (see D.16.1). The expression is associated with the aspect for the task type or single_task_declaration that contains the pragma.

Extensions to Ada 2005

\{AI05-0009-1\} Pragma Dispatching_Domain is new.

J.15.11 Pragmas Priority and Interrupt_Priority

Syntax

\{AI05-0229-1\} The form of a pragma Priority is as follows:

pragma Priority (expression);

\{AI05-0229-1\} The form of a pragma Interrupt_Priority is as follows:

pragma Interrupt_Priority [(expression);]

Name Resolution Rules

\{AI05-0229-1\} The expected type for the expression in a Priority or Interrupt_Priority pragma is Integer.

Legality Rules

\{AI05-0229-1\} A Priority pragma is allowed only immediately within a task_definition, a protected_definition, or the declarative_part of a subprogram body. An Interrupt_Priority pragma is allowed only immediately within a task_definition or a protected_definition.

\{AI05-0229-1\} For a Priority pragma that appears in the declarative_part of a subprogram body, the expression shall be static, and its value shall be in the range of System.Priority.

Static Semantics

\{AI05-0229-1\} For an implementation that supports Annex D, a pragma Priority specifies the value of the Priority aspect (see D.1) and a pragma Interrupt_Priority specifies the value of the Interrupt_Priority aspect as follows:

- If the pragma appears in a task_definition, the expression is associated with the aspect for the task type or single_task_declaration that contains the pragma;
- If the pragma appears in a protected_definition, the expression is associated with the aspect for the protected type or single_protected_declaration that contains the pragma;
- If the pragma appears in the declarative_part of a subprogram body, the expression is associated with the aspect for the subprogram that contains the pragma.

\{AI05-0229-1\} If there is no expression in an Interrupt_Priority pragma, the Interrupt_Priority aspect has the value Interrupt_Priority'Last.

Wording Changes from Ada 2005

\{AI05-0229-1\} {AI05-0299-1\} This subclause is new. Pragmas Interrupt_Priority and Priority were moved here from D.1; aspects Interrupt_Priority and Priority live there now.
J.15.12 **Pragma Relative_Deadline**

**Syntax**

\{AI05-0229-1\} The form of a pragma Relative_Deadline is as follows:

```
pragma Relative_Deadline (relative_deadline_expression);
```

**Name Resolution Rules**

\{AI05-0229-1\} The expected type for a relative_deadline_expression is Real_Time.Time_Span.

**Legality Rules**

\{AI05-0229-1\} A Relative_Deadline pragma is allowed only immediately within a task_definition or the declarative_part of a subprogram_body.

**Static Semantics**

\{AI05-0229-1\} For an implementation that supports Annex D, a pragma Relative_Deadline specifies the value of the Relative_Deadline aspect (see D.2.6). If the pragma appears in a task_definition, the expression is associated with the aspect for the task type or single_task_declaration that contains the pragma; otherwise, the expression is associated with the aspect for the subprogram that contains the pragma.

**Wording Changes from Ada 2005**

\{AI05-0229-1\} \{AI05-0299-1\} This subclause is new. Pragma Relative_Deadline was moved here from D.2.6; aspect Relative_Deadline lives there now.

J.15.13 **Pragma Asynchronous**

**Syntax**

\{AI05-0229-1\} The form of a pragma Asynchronous, which is a representation pragma (see 13.1), is as follows:

```
pragma Asynchronous (local_name);
```

**Static Semantics**

\{AI05-0229-1\} For an implementation that supports Annex E, a pragma Asynchronous specifies that the Asynchronous aspect (see E.4.1) for the procedure or type denoted by local_name has the value True.

**Legality Rules**

\{AI05-0229-1\} The local_name of a pragma Asynchronous shall denote a declaration that may have aspect Asynchronous specified.

**Wording Changes from Ada 2005**

\{AI05-0229-1\} \{AI05-0299-1\} This subclause is new. Pragma Asynchronous was moved here from E.4.1; aspect Asynchronous lives there now.

J.15.14 **Elaboration Control Pragmas**

\{AI12-0409-1\} This subclause defines pragmas that specify aspects that help control the elaboration order of library_items.
Discussion:  \{AI12-0417-1\} Pragmas that do not have associated aspects still appear in 10.2.1. These pragmas are presented in the order that the aspects are defined in 10.2.1.

Syntax

\{AI12-0417-1\} The following pragmas are defined with the given forms:

- \texttt{pragma Preelaborate\left(library unit name\right)};
- \texttt{pragma Preelaborable\_Initialization\left(direct name\right)};
- \texttt{pragma Pure\left(library unit name\right)};
- \texttt{pragma Elaborate\_Body\left(library unit name\right)};

\{AI12-0417-1\} Pragmas Preelaborate, Pure, and Elaborate\_Body are library unit pragmas.

Ramification: Pragma Preelaborable\_Initialization is not a library unit pragma.

Static Semantics

\{AI12-0417-1\} A pragma Preelaborate specifies that a library unit is preelaborated, namely that the Preelaborate aspect (see 10.2.1) of the library unit is True.

\{AI12-0417-1\} A pragma Pure specifies that a library unit is declared pure, namely that the Pure aspect (see 10.2.1) of the library unit is True.

\{AI12-0417-1\} A pragma Elaborate\_Body specifies that [a library unit requires a completion, namely that] the Elaborate\_Body aspect (see 10.2.1) of the library unit is True.

Legality Rules

\{AI12-0409-1\} A pragma Preelaborable\_Initialization specifies that the Preelaborable\_Initialization aspect (see 10.2.1) for a composite type is True. This pragma shall appear in the visible part of a package or generic package.

\{AI12-0409-1\} If the pragma appears in the first declaration list of a package\_specification, then the direct name shall denote the first subtype of a composite type, and the type shall be declared immediately within the same package as the pragma. The composite type shall be one for which the Preelaborable\_Initialization aspect can be directly specified as True. In addition to the places where Legality Rules normally apply (see 12.3), these rules also apply in the private part of an instance of a generic unit.

\{AI12-0409-1\} If the pragma appears in a generic\_formal\_part, then the direct name shall denote a type declared in the same generic\_formal\_part as the pragma, and be one for which the Preelaborable\_Initialization aspect can be directly specified as True.

NOTE  \{AI12-0409-1\} Pragmas Elaborate and Elaborate\_All, which do not have associated aspects, are found in 10.2.1.

Wording Changes from Ada 2012

\{AI12-0409-1\} This subclause is new. These pragmas were moved here from 10.2.1.

J.15.15 Distribution Pragmas

\{AI12-0417-1\} This subclause defines pragmas that specify properties of units for distributed systems.

Discussion:  \{AI12-0417-1\} These pragmas are presented in the order that the aspects are defined in Annex E.

Syntax

\{AI12-0417-1\} The following pragmas are defined with the given forms:
pragma Shared_Passive(library_unit_name);
pragma Remote_Types(library_unit_name);
pragma Remote_Call_Interface(library_unit_name);
pragma All_Calls_Remote(library_unit_name);

{AI12-0417-1} Each of these pragmas is a library unit pragma.

Static Semantics

{AI12-0417-1} A categorization pragma is a pragma that specifies a corresponding categorization aspect.

{AI12-0417-1} The pragmas Shared_Passive, Remote_Types, and Remote_Call_Interface are categorization pragmas. In addition, the pragma Pure (see J.15.14) is considered a categorization pragma.

{AI12-0417-1} A pragma Shared_Passive specifies that a library unit is a shared passive library unit, namely that the Shared_Passive aspect (see E.2.1) of the library unit is True.

{AI12-0417-1} A pragma Remote_Types specifies that a library unit is a remote types library unit, namely that the Remote_Types aspect (see E.2.2) of the library unit is True.

{AI12-0417-1} A pragma Remote_Call_Interface specifies that a library unit is a remote call interface, namely that the Remote_Call_Interface aspect (see E.2.3) of the library unit is True.

A pragma All_Calls_Remote specifies that the All_Calls_Remote aspect (see E.2.3) of the library unit is True.

Wording Changes from Ada 2012

{AI12-0417-1} This subclause is new. These pragmas were moved here from Annex E, “Distributed Systems”.
Annex K
(informative)

Language-Defined Aspects and Attributes

This annex summarizes the definitions given elsewhere of the language-defined aspects and attributes. Some aspects have corresponding attributes, as noted.

K.1 Language-Defined Aspects

This subclause summarizes the definitions given elsewhere of the language-defined aspects. Aspects are properties of entities that can be specified by the Ada program; unless otherwise specified below, aspects can be specified using an aspect_specification.

Address
Machine address of an entity. See 13.3.

Aggregate
Mechanism to define user-defined aggregates. See 4.3.5.

Alignment (object)
Alignment of an object. See 13.3.

Alignment (subtype)
Alignment of a subtype. See 13.3.

All_Calls_Remote
All indirect or dispatching remote subprogram calls, and all direct remote subprogramprocedure calls, should use the Partition Communication Subsystem even if they are local. See E.2.3.

Allows_Exit
An indication of whether a subprogram will operate correctly for arbitrary transfers of control. See 5.5.3.

Asynchronous
Remote procedure calls are asynchronous; the caller continues without waiting for the call to return. See E.4.1.

Atomic
Declare that a type, object, or component is atomic. See C.6.

Atomic_Components
Declare that the components of an array type or object are atomic. See C.6.

Attach_Handler
Protected procedure is attached to an interrupt. See C.3.1.

Bit_Order
Order of bit numbering in a record_representation_clause. See 13.5.3.

Coding
Internal representation of enumeration literals. Specified by an enumeration_representation_clause, not by an aspect_specification. See 13.4.

Component_Size
Size in bits of a component of an array type. See 13.3.

Constant_Indexing
Defines function(s) to implement user-defined indexed_components. See 4.1.6.

Convention
Calling convention or other convention used for interfacing to other languages. See B.1.
<table>
<thead>
<tr>
<th>Page</th>
<th>Term</th>
<th>Definition</th>
<th>See Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>15/5</td>
<td>CPU</td>
<td>Processor on which a given task, or calling task for a protected operation, should run.</td>
<td>D.16.</td>
</tr>
<tr>
<td>16/3</td>
<td>Default_Component_Value</td>
<td>Default value for the components of an array-of-scalar subtype. See 3.6.</td>
<td></td>
</tr>
<tr>
<td>16.1/5</td>
<td>Default_Initial_Condition</td>
<td>A condition that will hold true after the default initialization of an object. See 7.3.3.</td>
<td></td>
</tr>
<tr>
<td>17/3</td>
<td>Default_Iterator</td>
<td>Default iterator to be used in for loops. See 5.5.1.</td>
<td></td>
</tr>
<tr>
<td>18/3</td>
<td>Default_Storage_Pool</td>
<td>Default storage pool for a generic instance. See 13.11.3.</td>
<td></td>
</tr>
<tr>
<td>19/3</td>
<td>Default_Value</td>
<td>Default value for a scalar subtype. See 3.5.</td>
<td></td>
</tr>
<tr>
<td>19.1/4</td>
<td>Discard_Names</td>
<td>Requests a reduction in storage for names associated with an entity. See C.5.</td>
<td></td>
</tr>
<tr>
<td>19.2/5</td>
<td>Dispatching</td>
<td>Generic formal parameters used in the implementation of an entity. See H.7.1.</td>
<td></td>
</tr>
<tr>
<td>20/3</td>
<td>Dispatching_Domain</td>
<td>Domain (group of processors) on which a given task should run. See D.16.1.</td>
<td></td>
</tr>
<tr>
<td>21/5</td>
<td>Dynamic_Predicate</td>
<td>Condition that will hold true for objects of a given subtype; the subtype is not static. See 3.2.4.</td>
<td></td>
</tr>
<tr>
<td>22/5</td>
<td>Elaborate_Body</td>
<td>A given package will have a body, and that body is elaborated immediately after the declaration. See 10.2.1.</td>
<td></td>
</tr>
<tr>
<td>22.1/4</td>
<td>Exclusive_Functions</td>
<td>Specifies mutual exclusion behavior of protected functions in a protected type. See 9.5.1.</td>
<td></td>
</tr>
<tr>
<td>23/3</td>
<td>Export</td>
<td>Entity is exported to another language. See B.1.</td>
<td></td>
</tr>
<tr>
<td>24/3</td>
<td>External_Name</td>
<td>Name used to identify an imported or exported entity. See B.1.</td>
<td></td>
</tr>
<tr>
<td>25/3</td>
<td>External_Tag</td>
<td>Unique identifier for a tagged type in streams. See 13.3.</td>
<td></td>
</tr>
<tr>
<td>25.1/5</td>
<td>Full_Access_Only</td>
<td>Declare that a volatile type, object, or component is full access. See C.6.</td>
<td></td>
</tr>
<tr>
<td>25.2/5</td>
<td>Global</td>
<td>Global object usage contract. See 6.1.2.</td>
<td></td>
</tr>
<tr>
<td>25.3/5</td>
<td>Global'Class</td>
<td>Global object usage contract inherited on derivation. See 6.1.2.</td>
<td></td>
</tr>
<tr>
<td>26/3</td>
<td>Implicit_Dereference</td>
<td>Mechanism for user-defined implicit.all. See 4.1.5.</td>
<td></td>
</tr>
<tr>
<td>27/3</td>
<td>Import</td>
<td>Entity is imported from another language. See B.1.</td>
<td></td>
</tr>
<tr>
<td>28/3</td>
<td>Independent</td>
<td>Declare that a type, object, or component is independently addressable. See C.6.</td>
<td></td>
</tr>
<tr>
<td>29/3</td>
<td>Independent_Components</td>
<td>Declare that the components of an array or record type, or an array object, are independently addressable. See C.6.</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inline</td>
<td>For efficiency, Inline calls are requested for a subprogram. See 6.3.2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input</td>
<td>Function to read a value from a stream for a given type, including any bounds and discriminants. See 13.13.2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input'Class</td>
<td>Function to read a value from a stream for a the class-wide type associated with a given type, including any bounds and discriminants. See 13.13.2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integer_Literal</td>
<td>Defines a function to implement user-defined integer literals. See 4.2.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interrupt_Handler</td>
<td>Protected procedure may be attached to interrupts. See C.3.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interrupt_Priority</td>
<td>Priority of a task object or type, or priority of a protected object or type; the priority is in the interrupt range. See D.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iterator_Element</td>
<td>Element type to be used for user-defined iterators. See 5.5.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iterator_View</td>
<td>An alternative type to used for container element iterators. See 5.5.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layout (record)</td>
<td>Layout of record components. Specified by a record representation clause, not by an aspect specification. See 13.5.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link_Name</td>
<td>Linker symbol used to identify an imported or exported entity. See B.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine_Radix</td>
<td>Radix (2 or 10) that is used to represent a decimal fixed point type. See F.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max_Entry_Queue_Length</td>
<td>The maximum entry queue length for a task type, protected type, or entry. See D.4.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No_Controlled_Parts</td>
<td>A specification that a type and its descendants do not have controlled parts. See H.4.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No_Return</td>
<td>A subprogram/procedure will not return normally. See 6.5.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonblocking</td>
<td>Specifies that an associated subprogram does not block. See 9.5.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output</td>
<td>Procedure to write a value to a stream for a given type, including any bounds and discriminants. See 13.13.2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output'Class</td>
<td>Procedure to write a value to a stream for a the class-wide type associated with a given type, including any bounds and discriminants. See 13.13.2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pack</td>
<td>Minimize storage when laying out records and arrays. See 13.2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parallel_Calls</td>
<td>Specifies whether a given subprogram is expected to be called in parallel. See 9.10.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parallel_Iterator</td>
<td>An indication of whether a subprogram may use multiple threads of control to invoke a loop body procedure. See 5.5.3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post</td>
<td>Postcondition; a condition that will hold true after a call. See 6.1.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post'Class</td>
<td>Postcondition that applies to corresponding subprograms of descendant types, inherited on type derivation. See 6.1.1.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Precondition; a condition that is expected to hold true before a call. See 6.1.1.

Pre'Class Precondition that applies to corresponding subprograms of descendant types inherited on type derivation. See 6.1.1.

Predicate Failure Action to be performed when a predicate check fails. See 3.2.4.

Preelaborable_Initialization Declares that a type has preelaborable initialization. See 10.2.1.

Preelaborate Code execution during elaboration is avoided for a given package. See 10.2.1.

Priority Priority of a task object or type, or priority of a protected object or type; the priority is not in the interrupt range. See D.1.

Pure Side effects are avoided in the subprograms of a given package. See 10.2.1.

Put_Image Procedure to define the image of a given type. See 4.10.

Read Procedure to read a value from a stream for a given type. See 13.13.2.

Read'Class Procedure to read a value from a stream for the class-wide type associated with a given type. See 13.13.2.

Real_Literal Defines a function or functions to implement user-defined real literals. See 4.2.1.

Record layout See Layout. See 13.5.1.

Relative_Deadline Task or protected type parameter used in Earliest Deadline First Dispatching. See D.2.6.

Remote_Call_Interface Subprograms in a given package may be used in remote procedure calls. See E.2.3.

Remote_Types Types in a given package may be used in remote procedure calls. See E.2.2.

Shared_Passive A given package is used to represent shared memory in a distributed system. See E.2.1.

Size (object) Size in bits of an object. See 13.3.

Size (subtype) Size in bits of a subtype. See 13.3.

Small Scale factor for a fixed point type. See 3.5.10.

Stable_Properties A list of functions describing characteristics that usually are unchanged by primitive operations of the type or an individual primitive subprogram. See 7.3.4.

Stable_Properties'Class A list of functions describing characteristics that usually are unchanged by primitive operations of a class of types or a primitive subprogram for such a class. See 7.3.4.

Static Specifies that an associated expression function can be used in static expressions. See 6.8.
Static_Predicate
Condition that will hold true for objects of a given subtype; the subtype may be static. See 3.2.4.

Storage_Pool
Pool of memory from which new will allocate for a given access type. See 13.11.

Storage_Size (access)
Sets memory size for allocations for an access type. See 13.11.

Storage_Size (task)
Size in storage elements reserved for a task type or single task object. See 13.3.

Stream_Size
Size in bits used to represent elementary objects in a stream. See 13.13.2.

String_Literal
Defines a function to implement user-defined string literals. See 4.2.1.

Synchronization
Defines whether a given primitive operation of a synchronized interface will be implemented by an entry or protected procedure. See 9.5.

Type_Invariant
A condition that will hold true for all objects of a type. See 7.3.2.

Type_Invariant'Class
A condition that will hold true for all objects in a class of types. See 7.3.2.

Unchecked_Union
Type is used to interface to a C union type. See B.3.3.

Use_Formal
Generic formal parameters used in the implementation of an entity. See H.7.1.

Variable_Indexing
Defines function(s) to implement user-defined indexed_components. See 4.1.6.

Volatile
Declare that a type, object, or component is volatile. See C.6.

Volatile_Components
Declare that the components of an array type or object are volatile. See C.6.

Write
Procedure to write a value to a stream for a given type. See 13.13.2.

Write'Class
Procedure to write a value to a stream for the class-wide type associated with a given type. See 13.13.2.

Yield
Ensures that a callable entity includes a task dispatching point. See D.2.1.

K.2 Language-Defined Attributes

{A105-0229-1} {A105-0299-1} This subclause summarizes the definitions given elsewhere of the language-defined attributes. Attributes are properties of entities that can be queried by an Ada program.

P'Access
For a prefix P that denotes a subprogram:

P'Access yields an access value that designates the subprogram denoted by P. The type of P'Access is an access-to-subprogram type (S), as determined by the expected type. See 3.10.2.

X'Access
For a prefix X that denotes an aliased view of an object:
X'Access yields an access value that designates the object denoted by X. The type of
X'Access is an access-to-object type, as determined by the expected type. The expected type
shall be a general access type. See 3.10.2.

X'Address For a prefix X that denotes an object, program unit, or label:
Denotes the address of the first of the storage elements allocated to X. For a program unit or
label, this value refers to the machine code associated with the corresponding body or
statement. The value of this attribute is of type System.Address. See 13.3.

S'Adjacent For every subtype S of a floating point type T:
S'Adjacent denotes a function with the following specification:

function S'Adjacent (X, Towards : T)
return T

If Towards = X, the function yields X; otherwise, it yields the machine number of the type T
adjacent to X in the direction of Towards, if that machine number exists. If the result would
be outside the base range of S, Constraint_Error is raised. When T'Signed_Zeros is True, a
zero result has the sign of X. When Towards is zero, its sign has no bearing on the result. See
A.5.3.

S'Aft For every fixed point subtype S:
S'Aft yields the number of decimal digits needed after the decimal point to accommodate the
delta of the subtype S, unless the delta of the subtype S is greater than 0.1, in which case the
attribute yields the value one. (S'Aft is the smallest positive integer N for which
(10**N)*S'Delta is greater than or equal to one.) The value of this attribute is of the type
universal_integer. See 3.5.10.

S'Alignment For every subtype S:
The value of this attribute is of type universal_integer, and nonnegative.

For an object X of subtype S, if S'Alignment is not zero, then X'Alignment is a nonzero
integral multiple of S'Alignment unless specified otherwise by a representation item. See
13.3.

X'Alignment For a prefix X that denotes an object, program unit, or object:
The value of this attribute is of type universal_integer, and nonnegative; zero means that the
object is not necessarily aligned on a storage element boundary. If X'Alignment is not zero,
then X is aligned on a storage unit boundary and X'Address The Address of an object that is
allocated under control of the implementation is an integral multiple of X'Alignment the
Alignment of the object (that is, the Address modulo the Alignment is zero). The offset of a
record component is a multiple of the Alignment of the component. For an object that is not
allocated under control of the implementation (that is, one that is imported, that is allocated
by a user-defined allocator, whose Address has been specified, or is designated by an access
value returned by an instance of Unchecked_Conversion), the implementation may assume
that the Address is an integral multiple of its Alignment. The implementation shall not
assume a stricter alignment.

The value of this attribute is of type universal_integer, and nonnegative; zero means that the
object is not necessarily aligned on a storage element boundary. See 13.3.

S'Base For every scalar subtype S:
S'Base denotes an unconstrained subtype of the type of S. This unconstrained subtype is
called the base subtype of the type. See 3.5.
S'Bit_Order
For every specific record subtype S:
Denotes the bit ordering for the type of S. The value of this attribute is of type System.Bit_Order. See 13.5.3.

P'Body_Version
For a prefix P that statically denotes a program unit:
Yields a value of the predefined type String that identifies the version of the compilation unit that contains the body (but not any subunits) of the program unit. See E.3.

T'Callable
For a prefix T that is of a task type (after any implicit dereference):
Yields the value True when the task denoted by T is callable, and False otherwise; See 9.9.

E'Caller
For a prefix E that denotes an entry_declaration:
Yields a value of the type Task_Id that identifies the task whose call is now being serviced. Use of this attribute is allowed only inside an entry_body or accept_statement or entry_body after the entry_barrier, corresponding to the entry_declaration denoted by E. See C.7.1.

S'Ceiling
For every subtype S of a floating point type T:
S'Ceiling denotes a function with the following specification:

\[
\begin{align*}
  \text{function } & S'\text{Ceiling} \ (X : T) \\
  \text{return} & \ T
\end{align*}
\]

The function yields the value \( \lceil X \rceil \), that is, the smallest (most negative) integral value greater than or equal to \( X \). When \( X \) is zero, the result has the sign of \( X \); a zero result otherwise has a negative sign when S'Signed_Zeros is True. See A.5.3.

S'Class
For every subtype S of a tagged type T (specific or class-wide):
S'Class denotes a subtype of the class-wide type (called T'Class in this document) for the class rooted at T (or if S already denotes a class-wide subtype, then S'Class is the same as S).

S'Class is unconstrained. However, if S is constrained, then the values of S'Class are only those that when converted to the type T belong to S. See 3.9.

S'Class
For every subtype S of an untagged private type whose full view is tagged:
Denotes the class-wide subtype corresponding to the full view of S. This attribute is allowed only from the beginning of the private part in which the full view is declared, until the declaration of the full view. After the full view, the Class attribute of the full view can be used. See 7.3.1.

X'Component_Size
For a prefix X that denotes an array subtype or array object (after any implicit dereference):
Denotes the size in bits of components of the type of X. The value of this attribute is of type universal_integer. See 13.3.

S'Compose
For every subtype S of a floating point type T:
S'Compose denotes a function with the following specification:

\[
\begin{align*}
  \text{function } & S'\text{Compose} \ (\text{Fraction} : T; \\
  & \text{Exponent} : \text{universal_integer}) \\
  \text{return} & \ T
\end{align*}
\]

Let \( v \) be the value \( \text{Fraction} \cdot T'Machine_Radix^\text{Exponent-k} \), where \( k \) is the normalized exponent of \( \text{Fraction} \). If \( v \) is a machine number of the type \( T \), or if \( |v| \geq T'Model_Small \), the function yields \( v \); otherwise, it yields either one of the machine numbers of the type \( T \) adjacent to \( v \).
Constraint_Error is optionally raised if \( v \) is outside the base range of \( S \). A zero result has the sign of \( \text{Fraction} \) when \( S'\text{Signed_Zeros} \) is True. See A.5.3.

\[ \text{A'Constrained} \]

For a prefix \( A \) that is of a discriminated type (after any implicit dereference):

Yields the value True if \( A \) denotes a constant, a value, a tagged object, or a constrained variable, and False otherwise. The value of this attribute is of the predefined type Boolean. See 3.7.2.

\[ \text{S'Copy_Sign} \]

For every subtype \( S \) of a floating point type \( T \):

\( S'\text{Copy_Sign} \) denotes a function with the following specification:

\[
\text{function } S'\text{Copy_Sign} (\text{Value}, \text{Sign} : T) \text{ return } T
\]

If the value of \( \text{Value} \) is nonzero, the function yields a result whose magnitude is that of \( \text{Value} \) and whose sign is that of \( \text{Sign} \); otherwise, it yields the value zero. Constraint_Error is optionally raised if the result is outside the base range of \( S \). A zero result has the sign of \( \text{Sign} \) when \( S'\text{Signed_Zeros} \) is True. See A.5.3.

\[ \text{E'Count} \]

For a prefix \( E \) that denotes an entry of a task or protected unit:

Yields the number of calls presently queued on the entry \( E \) of the current instance of the unit. The value of this attribute is of the type \( \text{universal_integer} \). See 9.9.

\[ \text{S'Definite} \]

For a prefix \( S \) that denotes a formal indefinite subtype:

\( S'\text{Definite} \) yields True if the actual subtype corresponding to \( S \) is definite; otherwise, it yields False. The value of this attribute is of the predefined type Boolean. See 12.5.1.

\[ \text{S'Delta} \]

For every fixed point subtype \( S \):

\( S'\text{Delta} \) denotes the \( \text{delta} \) of the fixed point subtype \( S \). The value of this attribute is of the type \( \text{universal_real} \). See 3.5.10.

\[ \text{S'Denorm} \]

For every subtype \( S \) of a floating point type \( T \):

Yields the value True if every value expressible in the form

\[
\pm \text{mantissa} \cdot T'\text{Machine_Radix}^{T'\text{Machine_Emin}}
\]

where \( \text{mantissa} \) is a nonzero \( T'\text{Machine_Mantissa-digit fraction in the number base } T'\text{Machine_Radix} \), the first digit of which is zero, is a machine number (see 3.5.7) of the type \( T \); yields the value False otherwise. The value of this attribute is of the predefined type Boolean. See A.5.3.

\[ \text{S'Digits} \]

For every floating point subtype \( S \):

\( S'\text{Digits} \) denotes the requested decimal precision for the subtype \( S \). The value of this attribute is of the type \( \text{universal_integer} \). See 3.5.8.

\[ \text{S'Digits} \]

For every decimal fixed point subtype \( S \):

\( S'\text{Digits} \) denotes the \( \text{digits} \) of the decimal fixed point subtype \( S \), which corresponds to the number of decimal digits that are representable in objects of the subtype. The value of this attribute is of the type \( \text{universal_integer} \). See 3.5.10.

\[ \text{S'Enum_Rep} \]

For every discrete subtype \( S \):

\( S'\text{Enum_Rep} \) denotes a function with the following specification:

\[
\text{function } S'\text{Enum_Rep} (\text{Arg} : S'\text{Base}) \text{ return } \text{universal_integer}
\]
This function returns the representation value of the value of Arg, as a value of type
universal_integer. The representation value is the internal code specified in an enumeration
representation clause, if any, for the type corresponding to the value of Arg, and otherwise is
the position number of the value. See 13.4.

S'Enum_Val
For every discrete subtype S:

S'Enum_Val denotes a function with the following specification:

\[\text{function } S'\text{Enum_Val} (\text{Arg} : \text{universal_integer}) \text{ return } S'\text{Base}\]

This function returns a value of the type of S whose representation value equals the value of
Arg. For the evaluation of a call on S'Enum_Val, if there is no value in the base range of its
type with the given representation value, Constraint_Error is raised. See 13.4.

S'Exponent
For every subtype S of a floating point type T:

S'Exponent denotes a function with the following specification:

\[\text{function } S'\text{Exponent} (X : T) \text{ return } \text{universal_integer}\]

The function yields the normalized exponent of X. See A.5.3.

S'External_Tag
For every subtype S of a tagged type T (specific or class-wide):

S'External_Tag denotes an external string representation for S'Tag; it is of the predefined type
String. External_Tag may be specified for a specific tagged type via an
attribute_definition_clause; the expression of such a clause shall be static. The default
external tag representation is implementation defined. See 3.9.2 and 13.13.2. See 13.3.

A'First
For a prefix prefix A that is of an array type (after any implicit dereference), or denotes a
constrained array subtype:

A'First denotes the lower bound of the first index range; its type is the corresponding index
type. See 3.6.2.

S'First
For every scalar subtype S:

S'First denotes the lower bound of the range of S. The value of this attribute is of the type of
S. See 3.5.

A'First(N)
For a prefix prefix A that is of an array type (after any implicit dereference), or denotes a
constrained array subtype:

A'First(N) denotes the lower bound of the N-th index range; its type is the corresponding
index type. See 3.6.2.

R.C'First_Bit
For a component C of a composite, non-array object R:

If the nondefault bit ordering applies to the composite type, and if a component clause
specifies the placement of C, denotes the value given for the first bit of the
component clause, otherwise, denotes the offset, from the start of the first of the
storage elements occupied by C, of the first bit occupied by C. This offset is measured in bits.
The first bit of a storage element is numbered zero. The value of this attribute is of the type
universal_integer. See 13.5.2.

S'First_Valid
For every static discrete subtype S for which there exists at least one value belonging to S
that satisfies the predicates any predicate of S:
S'First_Valid denotes the smallest value that belongs to S and satisfies the predicate of S. The value of this attribute is of the type of S. See 3.5.5.

S'Floor For every subtype S of a floating point type T:

S'Floor denotes a function with the following specification:

function S'Floor (X : T)
return T

The function yields the value \( \lfloor X \rfloor \), that is, the largest (most positive) integral value less than or equal to X. When X is zero, the result has the sign of X; a zero result otherwise has a positive sign. See A.5.3.

S'Fore For every fixed point subtype S:

S'Fore yields the minimum number of characters needed before the decimal point for the decimal representation of any value of the subtype S, assuming that the representation does not include an exponent, but includes a one-character prefix that is either a minus sign or a space. (This minimum number does not include superfluous zeros or underlines, and is at least 2.) The value of this attribute is of the type universal_integer. See 3.5.10.

S'Fraction For every subtype S of a floating point type T:

S'Fraction denotes a function with the following specification:

function S'Fraction (X : T)
return T

The function yields the value \( X \cdot T'\text{Machine_Radix}^k \), where \( k \) is the normalized exponent of X. A zero result, which can only occur when X is zero, has the sign of X. See A.5.3.

X'Has_Same_Storage

For a prefix X that denotes an object:

X'Has_Same_Storage denotes a function with the following specification:

function X'Has_Same_Storage (Arg : any_type)
return Boolean

The actual parameter shall be a name that denotes an object. The object denoted by the actual parameter can be of any type. This function evaluates the names of the objects involved. It returns True if the representation of the object denoted by the actual parameter occupies exactly the same bits as the representation of the object denoted by X and the objects occupy at least one bit; otherwise, it returns False. See 13.3.

E'Identity For a prefix E that denotes an exception:

E'Identity returns the unique identity of the exception. The type of this attribute is Exception_Id. See 11.4.1.

T'Identity For a prefix T that is of a task type (after any implicit dereference):

Yields a value of the type Task_Id that identifies the task denoted by T. See C.7.1.

S'Image For every subtype S of a type T:

S'Image denotes a function with the following specification:

function S'Image(Arg : S'Base)
return String

S'Image calls S'Put Image passing Arg (which will typically store a sequence of character values in a text buffer) and then returns the result of retrieving the contents of that buffer with function Get. See 4.10.

X'Image For a prefix X of a type T other than universal_real or universal_fixed:
X'Image denotes the result of calling function S'Image with Arg being X, where S is the nominal subtype of X. See 4.10.

E'Index

For a prefix E that denotes an entry declaration of an entry family:

Within a precondition or postcondition expression for entry family E, denotes the value of the entry index for the call of E. The nominal subtype of this attribute is the entry index subtype. See 6.1.1.

S'Class'Input

For every subtype S'Class of a class-wide type T'Class:

S'Class'Input denotes a function with the following specification:

```ada
function S'Class'Input(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class) return T'Class
```

First reads the external tag from Stream and determines the corresponding internal tag (by calling Tags.Descendant_Tag_Internal_Tag(String'Input(Stream), S'Tag) which can raise Tag_Error — see 3.9) and then dispatches to the subprogram denoted by the Input attribute of the specific type identified by the internal tag; returns that result. If the specific type identified by the internal tag is not covered by T'Class or is abstract, Constraint_Error is raised. See 13.13.2.

S'Input

For every subtype S of a specific type T:

S'Input denotes a function with the following specification:

```ada
function S'Input(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class) return T
```

S'Input reads and returns one value from Stream, using any bounds or discriminants written by a corresponding S'Output to determine how much to read. See 13.13.2.

A'Last

For a prefix A that is of an array type (after any implicit dereference), or denotes a constrained array subtype:

A'Last denotes the upper bound of the first index range; its type is the corresponding index type. See 3.6.2.

S'Last

For every scalar subtype S:

S'Last denotes the upper bound of the range of S. The value of this attribute is of the type of S. See 3.5.

A'Last(N)

For a prefix A that is of an array type (after any implicit dereference), or denotes a constrained array subtype:

A'Last(N) denotes the upper bound of the N-th index range; its type is the corresponding index type. See 3.6.2.

R.C'Last_Bit

For a component C of a composite, non-array object R:

If the nondefault bit ordering applies to the composite type, and if a component clause specifies the placement of C, denotes the value given for the last bit of the component clause; otherwise, denotes the offset, from the start of the first of the storage elements occupied by C, of the last bit occupied by C. This offset is measured in bits. The value of this attribute is of the type universal_integer. See 13.5.2.
S'Last_Valid

For every static discrete subtype S for which there exists at least one value belonging to S that satisfies the predicate\( p \) of S:

S'Last_Valid denotes the largest value that belongs to S and satisfies the predicate\( p \) of S. The value of this attribute is of the type of S. See 3.5.5.

S'Leading_Part

For every subtype S of a floating point type T:

S'Leading_Part denotes a function with the following specification:

\[
\text{function } S'\text{Leading}\_\text{Part} (X : T; \text{Radix}\_\text{Digits} : \text{universal}\_\text{integer}) \text{ return } T
\]

Let \( v \) be the value \( T'\text{Machine}\_\text{Radix}^{k-\text{Radix}\_\text{Digits}} \), where \( k \) is the normalized exponent of \( X \). The function yields the value

- \( \lfloor X/v \rfloor \cdot v \), when \( X \) is nonnegative and \( \text{Radix}\_\text{Digits} \) is positive;
- \( \lceil X/v \rceil \cdot v \), when \( X \) is negative and \( \text{Radix}\_\text{Digits} \) is positive.

Constraint_Error is raised when \( \text{Radix}\_\text{Digits} \) is zero or negative. A zero result, which can only occur when \( X \) is zero, has the sign of \( X \). See A.5.3.

A'Length

For a prefix A that is of an array type (after any implicit dereference), or denotes a constrained array subtype:

A'Length denotes the number of values of the first index range (zero for a null range); its type is universal_integer. See 3.6.2.

A'Length(N)

For a prefix A that is of an array type (after any implicit dereference), or denotes a constrained array subtype:

A'Length(N) denotes the number of values of the N-th index range (zero for a null range); its type is universal_integer. See 3.6.2.

S'Machine

For every subtype S of a floating point type T:

S'Machine denotes a function with the following specification:

\[
\text{function } S'\text{Machine} (X : T) \text{ return } T
\]

If \( X \) is a machine number of the type \( T \), the function yields \( X \); otherwise, it yields the value obtained by rounding or truncating \( X \) to either one of the adjacent machine numbers of the type \( T \). Constraint_Error is raised if rounding or truncating \( X \) to the precision of the machine numbers results in a value outside the base range of S. A zero result has the sign of \( X \) when S'Signed_Zeros is True. See A.5.3.

S'Machine_Emax

Yields the largest (most positive) value of exponent such that every value expressible in the canonical form (for the type \( T \), having a mantissa of \( T'\text{Machine}\_\text{Mantissa} \) digits, is a machine number (see 3.5.7) of the type \( T \). This attribute yields a value of the type universal_integer. See A.5.3.

S'Machine_Emin

For every subtype S of a floating point type T:

Yields the smallest (most negative) value of exponent such that every value expressible in the canonical form (for the type \( T \), having a mantissa of \( T'\text{Machine}\_\text{Mantissa} \) digits, is a
machine number (see 3.5.7) of the type \( T \). This attribute yields a value of the type \( \text{universal_integer} \). See A.5.3.

**S'Machine_Mantissa**

For every subtype \( S \) of a floating point type \( T \):

Yields the largest value of \( p \) such that every value expressible in the canonical form (for the type \( T \), having a \( p \)-digit mantissa and an exponent between \( T'\text{Machine_Emin} \) and \( T'\text{Machine_Emax} \), is a machine number (see 3.5.7) of the type \( T \). This attribute yields a value of the type \( \text{universal_integer} \). See A.5.3.

**S'Machine_Machine_Mantissa**

For every subtype \( S \) of a floating point type \( T \):

Yields the value True if overflow and divide-by-zero are detected and reported by raising \( \text{Constraint_Error} \) for every predefined operation that yields a result of the type \( T \); yields the value False otherwise. The value of this attribute is of the predefined type Boolean. See A.5.3.

**S'Machine_Overflows**

For every subtype \( S \) of a fixed point type \( T \):

Yields the value False if rounding is performed on inexact results of every predefined operation that yields a result of the type \( T \); yields the value False otherwise. The value of this attribute is of the predefined type Boolean. See A.5.4.

**S'Machine_Radix**

For every subtype \( S \) of a floating point type \( T \):

Yields the radix of the hardware representation of the type \( T \). The value of this attribute is of the type \( \text{universal_integer} \). See A.5.3.

**S'Machine_Radix**

For every subtype \( S \) of a fixed point type \( T \):

Yields the radix of the hardware representation of the type \( T \). The value of this attribute is of the type \( \text{universal_integer} \). See A.5.4.

**S'Machine_Rounding**

For every subtype \( S \) of a floating point type \( T \):

S'Machine_Rounding denotes a function with the following specification:

\[
\text{function } \text{S'Machine_Rounding} \ (X : T) \ \text{return } T
\]

The function yields the integral value nearest to \( X \). If \( X \) lies exactly halfway between two integers, one of those integers is returned, but which of them is returned is unspecified. A zero result has the sign of \( X \) when \( S'\text{Signed_Zeros} \) is True. This function provides access to the rounding behavior which is most efficient on the target processor. See A.5.3.

**S'Machine_Rounds**

For every subtype \( S \) of a floating point type \( T \):

Yields the value True if rounding is performed on inexact results of every predefined operation that yields a result of the type \( T \); yields the value False otherwise. The value of this attribute is of the predefined type Boolean. See A.5.3.

**S'Machine_Rounds**

For every subtype \( S \) of a fixed point type \( T \):
Yields the value True if rounding is performed on inexact results of every predefined operation that yields a result of the type $T$; yields the value False otherwise. The value of this attribute is of the predefined type Boolean. See A.5.4.

For every scalar subtype $S$:

$\text{S'Max}$ denotes a function with the following specification:

\[
\begin{align*}
\text{function} & \quad \text{S'Max}(\text{Left}, \text{Right} : S'\text{Base}) \\
\text{return} & \quad \text{S'Base}
\end{align*}
\]

The function returns the greater of the values of the two parameters. See 3.5.

For every subtype $S$:

Denotes the maximum value for Alignment that can be requested by the implementation via Allocate for an access type whose designated subtype is $S$. The value of this attribute is of type $\text{universal_integer}$. See 13.11.1.

For every subtype $S$:

Denotes the maximum value for Size_In_Storage_Elements that can be requested by the implementation via Allocate for an access type whose designated subtype is $S$. For a type with access discriminants, if the implementation allocates space for a coextension in the same pool as that of the object having the access discriminant, then this accounts for any calls on Allocate that could be performed to provide space for such coextensions. The value of this attribute is of type $\text{universal_integer}$. See 13.11.1.

For every scalar subtype $S$:

$\text{S'Min}$ denotes a function with the following specification:

\[
\begin{align*}
\text{function} & \quad \text{S'Min}(\text{Left}, \text{Right} : S'\text{Base}) \\
\text{return} & \quad \text{S'Base}
\end{align*}
\]

The function returns the lesser of the values of the two parameters. See 3.5.

For every modular subtype $S$:

$\text{S'Mod}$ denotes a function with the following specification:

\[
\begin{align*}
\text{function} & \quad \text{S'Mod} (\text{Arg} : \text{universal_integer}) \\
\text{return} & \quad \text{S'Base}
\end{align*}
\]

This function returns $\text{Arg mod S'Modulus}$, as a value of the type of $S$. See 3.5.4.

For every subtype $S$ of a floating point type $T$:

$\text{S'Model}$ denotes a function with the following specification:

\[
\begin{align*}
\text{function} & \quad \text{S'Model} (X : T) \\
\text{return} & \quad T
\end{align*}
\]

If the Numerics Annex is not supported, the meaning of this attribute is implementation defined; see G.2.2 for the definition that applies to implementations supporting the Numerics Annex. See A.5.3.

For every subtype $S$ of a floating point type $T$:

If the Numerics Annex is not supported, this attribute yields an implementation defined value that is greater than or equal to the value of $T'Machine_Emin$. See G.2.2 for further requirements that apply to implementations supporting the Numerics Annex. The value of this attribute is of the type $\text{universal_integer}$. See A.5.3.
S'Model_Epsilon
For every subtype S of a floating point type T:
Yields the value $T'\text{Machine_Radix} \cdot T'\text{Model_Mantissa}$. The value of this attribute is of the type universal_real. See A.5.3.

S'Model_Mantissa
For every subtype S of a floating point type T:
If the Numerics Annex is not supported, this attribute yields an implementation defined value that is greater than or equal to $\lceil d \cdot \log(10) / \log(T'\text{Machine_Radix}) \rceil + 1$, where $d$ is the requested decimal precision of $T$, and less than or equal to the value of $T'\text{Machine_Mantissa}$. See G.2.2 for further requirements that apply to implementations supporting the Numerics Annex. The value of this attribute is of the type universal_integer. See A.5.3.

S'Model_Small
For every subtype S of a floating point type T:
Yields the value $T'\text{Machine_Radix} \cdot T'\text{Model_Emin}$. The value of this attribute is of the type universal_real. See A.5.3.

S'Modulus
For every modular subtype S:
S'Modulus yields the modulus of the type of S, as a value of the type universal_integer. See 3.5.4.

S'Object_Size
For every subtype S:
If S is definite, denotes the size (in bits) of a stand-alone aliased object, or a component of subtype S in the absence of an aspect specification or representation item that specifies the size of the object or component. If S is indefinite, the meaning is implementation-defined. The value of this attribute is of the type universal_integer. See 13.3.

X'Old
For a prefix X that denotes an object of a nonlimited type:
Each X'Old in a postcondition expression that is enabled, other than those that occur in subexpressions that are determined to be unevaluated, denotes a constant that is implicitly declared at the beginning of the subprogram body, or entry body, or accept statement. The constant is of the type of X and is initialized to the result of evaluating X (as an expression) at the point of the constant declaration. The value of X'Old in the postcondition expression is the value of this constant; the type of X'Old is the type of X. These implicit constant declarations occur in an arbitrary order. See 6.1.1.

S'Class'Output
For every subtype S'Class of a class-wide type T'Class:
S'Class'Output denotes a procedure with the following specification:

```ada
procedure S'Class'Output (Stream : not null access Ada.Streams.Root_Stream_Type'Class; Item : in T'Class)
```
First writes the external tag of Item to Stream (by calling String'Output(Stream, Tags.-External_Tag(Item'Tag)) — see 3.9) and then dispatches to the subprogram denoted by the Output attribute of the specific type identified by the tag. Tag_Error is raised if the tag of Item identifies a type declared at an accessibility level deeper than that of S. See 13.13.2.

S'Output
For every subtype S of a specific type T:
S'Output denotes a procedure with the following specification:
procedure S'Output(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class;
    Item : in T)

S'Output writes the value of Item to Stream, including any bounds or discriminants. See 13.13.2.

X'Overlaps_Storage

For a prefix X that denotes an object:

X'Overlaps_Storage denotes a function with the following specification:

function X'Overlaps_Storage (Arg : any_type)
return Boolean

The actual parameter shall be a name that denotes an object. The object denoted by the actual parameter can be of any type. This function evaluates the names of the objects involved and returns True if the representation of the object denoted by the actual parameter shares at least one bit with the representation of the object denoted by X; otherwise, it returns False. See 13.3.

X'Parallel_Reduce(Reducer, Initial_Value)

For a prefix X of an array type (after any implicit dereference), or that denotes an iterable container object (see 5.5.1):

X'Parallel_Reduce is a reduction expression that yields a result equivalent to replacing the attribute identifier with Reduce and the prefix of the attribute with the value_sequence:

[parallel for Item of X => Item]

See 4.5.10.

D'Partition_Id

For a prefix prefix D that denotes a library-level declaration, excepting a declaration of or within a declared-pure library unit:

Denotes a value of the type universal_integer that identifies the partition in which D was elaborated. If D denotes the declaration of a remote call interface library unit (see E.2.3) the given partition is the one where the body of D was elaborated. See E.1.

S'Pos

For every discrete subtype S:

S'Pos denotes a function with the following specification:

function S'Pos(Arg : S'Base)
return universal_integer

This function returns the position number of the value of Arg, as a value of type universal_integer. See 3.5.5.

R.Ct'Position

For a component C of a composite, non-array object R:

If the nondefault bit ordering applies to the composite type, and if a component_clause specifies the placement of C, denotes the value given for the position of the component_clause; otherwise, denotes denotes the same value as R.Ct'Address – R'Address.

The value of this attribute is of the type universal_integer. See 13.5.2.

S'Pred

For every scalar subtype S:

S'Pred denotes a function with the following specification:

function S'Pred(Arg : S'Base)
return S'Base

For an enumeration type, the function returns the value whose position number is one less than that of the value of Arg; Constraint_Error is raised if there is no such value of the type. For an integer type, the function returns the result of subtracting one from the value of Arg.
For a fixed point type, the function returns the result of subtracting *small* from the value of *Arg*. For a floating point type, the function returns the machine number (as defined in 3.5.7) immediately below the value of *Arg*; Constraint_Error is raised if there is no such machine number. See 3.5.

**S’Preelaborable Initialization**
For a nonformal composite subtype *S* declared within the visible part of a package or a generic package, or a generic formal private subtype or formal derived subtype:
This attribute is of Boolean type, and its value reflects whether the type of *S* has preelaborable initialization. See 10.2.1.

**P’Priority**
For a prefix *P* that denotes a protected object:
Denotes a non-aliased component of the protected object *P*. This component is of type System.Any_Priority and its value is the priority of *P*. P’Priority denotes a variable if and only if *P* denotes a variable. A reference to this attribute shall appear only within the body of *P*. See D.5.2.

**S’Put_ Image**
For every subtype *S* of a type *T* other than *universal_real* or *universal_fixed*:
S’Put_ Image denotes a procedure with the following specification:

```ada
procedure S’Put_ Image
    (Buffer : in out Ada.Strings.Text_Buffers.Root_Buffer_Type’Class;
     Arg : in T);
```

The default implementation of S’Put_ Image writes (using Wide_Wide_Put) an image of the value of *Arg*. See 4.10.

**A’Range**
For a prefix *A* that is of an array type (after any implicit dereference), or denotes a constrained array subtype:

A’Range is equivalent to the range *A’First* .. *A’Last*, except that the prefix *A* is only evaluated once. See 3.6.2.

**S’Range**
For every scalar subtype *S*:

S’Range is equivalent to the range *S’First* .. *S’Last*. See 3.5.

**A’Range(N)**
For a prefix *A* that is of an array type (after any implicit dereference), or denotes a constrained array subtype:

A’Range(N) is equivalent to the range *A’First(N)* .. *A’Last(N)*, except that the prefix *A* is only evaluated once. See 3.6.2.

**S’Class’Read**
For every subtype *S’Class* of a class-wide type *T’Class*:
S’Class’Read denotes a procedure with the following specification:

```ada
procedure S’Class’Read(
    Stream : not null access Ada.Streams.Root_Stream_Type’Class;
    Item : out T’Class)
```

Dispatches to the subprogram denoted by the Read attribute of the specific type identified by the tag of *Item*. See 13.13.2.

**S’Read**
For every subtype *S* of a specific type *T*:
S’Read denotes a procedure with the following specification:
procedure S'Read(
    Stream : not null access Ada.Streams.Root_Stream_Type'Class;
    Item  : out T)

S'Read reads the value of Item from Stream. See 13.13.2.

V'Reduce(Reducer, Initial_Value)
Featuring a value_sequence V:
This attribute represents a reduction expression, and is in the form of a
reduction_attribute_reference. See 4.5.10.

X'Reduce(Reducer, Initial_Value)
For a prefix X of an array type (after any implicit dereference), or that denotes an iterable
container object (see 5.5.1): 
X'Reduce is a reduction expression that yields a result equivalent to replacing the prefix of
the attribute with the value_sequence:
[for Item of X => Item]
See 4.5.10.

P'Relative_Deadline
For a prefix P that denotes a protected object:
Denotes a non-aliased component of the protected object P. This component is of type
Ada.Real_Time.Time_Span and its value is the relative deadline of P. P'Relative_Deadline
denotes a variable if and only if P denotes a variable. A reference to this attribute shall appear
only within the body of P. See D.5.2.

S'Remainder
For every subtype S of a floating point type T:
S'Remainder denotes a function with the following specification:
function S'Remainder (X, Y : T)
    return T
For nonzero Y, let v be the value \(X - n \cdot Y\), where n is the integer nearest to the exact value of
\(X/Y\); if \(|n - X/Y| = 1/2\), then n is chosen to be even. If v is a machine number of the type T, the
function yields v; otherwise, it yields zero. Constraint_Error is raised if Y is zero. A zero
result has the sign of X when S'Signed_Zeros is True. See A.5.3.

F'Result
For a prefix F that denotes a function declaration or an access-to-function type:
Within a postcondition expression for function F, denotes the return_result
object of the function call for which the postcondition expression is evaluated. The type of this attribute is
that of the result subtype of the function or access-to-function type_result except within a
Post'Class postcondition_expression for a function with a controlling result or with a
controlling access result; in those cases the type of the attribute is described above as part of the
Name Resolution Rules for Post'Class. For a controlling result, the type of the attribute is
T'Class, where T is the function result type. For a controlling access result, the type of the
attribute is an anonymous access_type whose designated type is T'Class, where T is the
designated type of the function result type. See 6.1.1.

S'Round
For every decimal fixed point subtype S:
function S'Round(X : universal_real)
    return S'Base
The function returns the value obtained by rounding X (away from 0, if X is midway between
two values of the type of S). See 3.5.10.
S'Rounding For every subtype S of a floating point type T:

S'Rounding denotes a function with the following specification:

\[
\begin{aligned}
\text{function } S'\text{Rounding} \ (X : T) \\
\text{return } T
\end{aligned}
\]

The function yields the integral value nearest to \( X \), rounding away from zero if \( X \) lies exactly halfway between two integers. A zero result has the sign of \( X \) when S'Signed_Zeros is True. See A.5.3.

S'Safe_First For every subtype S of a floating point type T:

Yields the lower bound of the safe range (see 3.5.7) of the type T. If the Numerics Annex is not supported, the value of this attribute is implementation defined; see G.2.2 for the definition that applies to implementations supporting the Numerics Annex. The value of this attribute is of the type \( \text{universal\_real} \). See A.5.3.

S'Safe_Last For every subtype S of a floating point type T:

Yields the upper bound of the safe range (see 3.5.7) of the type T. If the Numerics Annex is not supported, the value of this attribute is implementation defined; see G.2.2 for the definition that applies to implementations supporting the Numerics Annex. The value of this attribute is of the type \( \text{universal\_real} \). See A.5.3.

S'Scale For every decimal fixed point subtype S:

S'Scale denotes the scale of the subtype S, defined as the value N such that S'Delta = \( 10.0^{-(N)} \). The scale indicates the position of the point relative to the rightmost significant digits of values of subtype S. The value of this attribute is of the type \( \text{universal\_integer} \). See 3.5.10.

S'Scaling For every subtype S of a floating point type T:

S'Scaling denotes a function with the following specification:

\[
\begin{aligned}
\text{function } S'\text{Scaling} \ (X : T; \\
\text{Adjustment : universal\_integer}) \\
\text{return } T
\end{aligned}
\]

Let \( v \) be the value \( X \cdot T\text{Machine_Radix}^{\text{Adjustment}} \). If \( v \) is a machine number of the type T, or if \( |v| \geq T\text{Model\_Small} \), the function yields \( v \); otherwise, it yields either one of the machine numbers of the type T adjacent to \( v \). Constraint_Error is optionally raised if \( v \) is outside the base range of S. A zero result has the sign of \( X \) when S'Signed_Zeros is True. See A.5.3.

S'Signed_Zeros For every subtype S of a floating point type T:

Yields the value True if the hardware representation for the type T has the capability of representing both positively and negatively signed zeros, these being generated and used by the predefined operations of the type T as specified in IEC 559:1989; yields the value False otherwise. The value of this attribute is of the predefined type Boolean. See A.5.3.

S'Size For every subtype S:

If S is definite, denotes the size (in bits) that the implementation would choose for the following objects of subtype S:

- A record component of subtype S when the record type is packed.
- The formal parameter of an instance of Unchecked_Conversion that converts from subtype S to some other subtype.
If S is indefinite, the meaning is implementation defined. The value of this attribute is of the type `universal_integer`. See 13.3.

For a `prefix` X that denotes an object:

Denotes the size in bits of the representation of the object. The value of this attribute is of the type `universal_integer`. See 13.3.

For every fixed point subtype S:

S'Small denotes the `small` of the type of S. The value of this attribute is of the type `universal_real`. See 3.5.10.

For every access-to-object subtype S:

Denotes the storage pool of the type of S. The type of this attribute is `Root_Storage_Pool'Class`. See 13.11.

Yields the result of calling Storage_Size(S'Storage_Pool), which is intended to be a measure of the number of storage elements reserved for the pool. The type of this attribute is `universal_integer`. See 13.11.

For a `prefix` T that denotes a task object (after any implicit dereference):

Denotes the number of storage elements reserved for the task. The value of this attribute is of the type `universal_integer`. The Storage_Size includes the size of the task's stack, if any. The language does not specify whether or not it includes other storage associated with the task (such as the "task control block" used by some implementations.) See 13.3.

For every subtype S of an elementary type T:

Denotes the number of bits read from or written to a stream by the default implementations of S'Read and S'Write occupied in a stream by items of subtype S. Hence, the number of stream elements required per item of elementary type T is:

\[
\text{T'Stream_Size} / \text{Ada.Streams.Stream_Element'Size}
\]

The value of this attribute is of type `universal_integer` and is a multiple of `Stream_Element'Size`. See 13.13.2.

For every scalar subtype S:

S'Succ denotes a function with the following specification:

\[
\text{function } S'\text{Succ}(\text{Arg} : S'\text{Base}) \text{ return } S'\text{Base}
\]

For an enumeration type, the function returns the value whose position number is one more than that of the value of Arg; Constraint_Error is raised if there is no such value of the type. For an integer type, the function returns the result of adding one to the value of Arg. For a fixed point type, the function returns the result of adding small to the value of Arg. For a floating point type, the function returns the machine number (as defined in 3.5.7) immediately above the value of Arg; Constraint_Error is raised if there is no such machine number. See 3.5.

For every subtype S of a tagged type T (specific or class-wide):

S'Tag denotes the tag of the type T (or if T is class-wide, the tag of the root type of the corresponding class). The value of this attribute is of type Tag. See 3.9.
X'Tag
For a prefix X that is of a class-wide tagged type (after any implicit dereference):
X'Tag denotes the tag of X. The value of this attribute is of type Tag. See 3.9.

T'Terminated
For a prefix T that is of a task type (after any implicit dereference):
Yields the value True if the task denoted by T is terminated, and False otherwise. The value
of this attribute is of the predefined type Boolean. See 9.9.

S'Truncation
For every subtype S of a floating point type T:
S'Truncation denotes a function with the following specification:

\[
\text{function } S'\text{Truncation} (X : T) \text{ return } T
\]

The function yields the value \( \lceil X \rceil \) when \( X \) is negative, and \( \lfloor X \rfloor \) otherwise. A zero result has the
sign of \( X \) when \( S'Signed\_Zeros \) is True. See A.5.3.

S'Unbiased_Rounding
For every subtype S of a floating point type T:
S'Unbiased_Rounding denotes a function with the following specification:

\[
\text{function } S'\text{Unbiased\_Rounding} (X : T) \text{ return } T
\]

The function yields the integral value nearest to \( X \), rounding toward the even integer if \( X \) lies
exactly halfway between two integers. A zero result has the sign of \( X \) when \( S'Signed\_Zeros \) is True. See A.5.3.

X'Unchecked_Access
For a prefix X that denotes an aliased view of an object:
All rules and semantics that apply to X'Access (see 3.10.2) apply also to
X'Unchecked_Access, except that, for the purposes of accessibility rules and checks, it is as if
X were declared immediately within a library package. See 13.10.

S'Val
For every discrete subtype S:
S'Val denotes a function with the following specification:

\[
\text{function } S'\text{Val}(Arg : universal\_integer) \text{ return } S'\text{Base}
\]

This function returns a value of the type of S whose position number equals the value of \( Arg \).
See 3.5.5.

X'Valid
For a prefix X that denotes a scalar object (after any implicit dereference):
Yields True if and only if the object denoted by X is normal, and then, if the preceding conditions hold, the value of X also satisfies the predicate of the nominal subtype of X evaluates to True. The value of this attribute is of the
predefined type Boolean. See 13.9.2.

S'Value
For every scalar subtype S:
S'Value denotes a function with the following specification:

\[
\text{function } S'\text{Value}(Arg : String) \text{ return } S'\text{Base}
\]

This function returns a value given an image of the value as a String, ignoring any leading or
trailing spaces. See 3.5.

P'Version
For a prefix P that statically denotes a program unit:
Yields a value of the predefined type String that identifies the version of the compilation unit that contains the declaration of the program unit. See E.3.

S'Wide_Image

For every subtype S of a type T:

S'Wide_Image denotes a function with the following specification:

```ada
function S'Wide_Image(Arg : S'Base)
return Wide_String
```

S'Wide_Image calls S'Put_Image passing Arg (which will typically store a sequence of character values in a text buffer) and then returns the result of retrieving the contents of that buffer with function Wide_Get. See 4.10.

X'Wide_Image

For a prefix X of a type T other than universal real or universal fixed:

X'Wide_Image denotes the result of calling function S'Wide_Image with Arg being X, where S is the nominal subtype of X. See 4.10.

S'Wide_Value

For every scalar subtype S:

S'Wide_Value denotes a function with the following specification:

```ada
function S'Wide_Value(Arg : Wide_String)
return S'Base
```

This function returns a value given an image of the value as a Wide_String, ignoring any leading or trailing spaces. See 3.5.

S'Wide_Wide_Image

For every subtype S of a type T:

S'Wide_Wide_Image denotes a function with the following specification:

```ada
function S'Wide_Wide_Image(Arg : S'Base)
return Wide_Wide_String
```

S'Wide_Wide_Image calls S'Put_Image passing Arg (which will typically store a sequence of character values in a text buffer) and then returns the result of retrieving the contents of that buffer with function Wide_Wide_Get. See 4.10.

X'Wide_Wide_Image

For a prefix X of a type T other than universal real or universal fixed:

X'Wide_Wide_Image denotes the result of calling function S'Wide_Wide_Image with Arg being X, where S is the nominal subtype of X. See 4.10.

S'Wide_Wide_Value

For every scalar subtype S:

S'Wide_Wide_Value denotes a function with the following specification:

```ada
function S'Wide_Wide_Value(Arg : Wide_Wide_String)
return S'Base
```

This function returns a value given an image of the value as a Wide_Wide_String, ignoring any leading or trailing spaces. See 3.5.

S'Wide_Wide_Width

For every scalar subtype S:

S'Wide_Wide_Width denotes the maximum length of a Wide_Wide_String returned by S'Wide_Wide_Image over all values of the subtype S, assuming a default implementation of S'Put_Image. It denotes zero for a subtype that has a null range. Its type is universal integer. See 3.5.
**S'Wide_Width**

For every scalar subtype $S$:

\[ S'Wide_Width \]

$S'Wide_Width$ denotes the maximum length of a Wide_String returned by $S'Wide_Image$ over all values of the subtype $S$, assuming a default implementation of $S'Put_Image$. It denotes zero for a subtype that has a null range. Its type is $universal_integer$. See 3.5.

**S'Width**

For every scalar subtype $S$:

\[ S'Width \]

$S'Width$ denotes the maximum length of a String returned by $S'Image$ over all values of the subtype $S$, assuming a default implementation of $S'Put_Image$. It denotes zero for a subtype that has a null range. Its type is $universal_integer$. See 3.5.

**S'Class'Write**

For every subtype $S'Class$ of a class-wide type $T'Class$:

\[ S'Class'Write \]

$S'Class'Write$ denotes a procedure with the following specification:

\[ procedure \ S'Class'Write( \]
\[ \quad Stream \ : \ not \ null \ access \ Ada.Streams.Root_Stream_Type'Class; \]
\[ \quad Item \ : \ in \ T'Class) \]

Dispatches to the subprogram denoted by the Write attribute of the specific type identified by the tag of Item. See 13.13.2.

**S'Write**

For every subtype $S$ of a specific type $T$:

\[ S'Write \]

$S'Write$ denotes a procedure with the following specification:

\[ procedure \ S'Write( \]
\[ \quad Stream \ : \ not \ null \ access \ Ada.Streams.Root_Stream_Type'Class; \]
\[ \quad Item \ : \ in \ T) \]

$S'Write$ writes the value of $Item$ to $Stream$. See 13.13.2.
Annex L
(informative)
Language-Defined Pragmas

This Annex summarizes the definitions given elsewhere of the language-defined pragmas.

**pragma** Admission_Policy (policy_identifier); — See D.4.1.
This paragraph was deleted. **pragma** All_Calls_Remote(library_unit_name); — See E.2.3.

**pragma** All_Calls_Remote(library_unit_name); — See J.15.15.

**pragma** Assert([Check =>] boolean_expression[, [Message =>] string_expression]); — See 11.4.2.
**pragma** Assertion_Policy(policy_identifier); — See 11.4.2.

**pragma** Assertion_Policy(assertion_aspect_mark => policy_identifier); — See 11.4.2.
This paragraph was deleted. **pragma** Asynchronous(local_name); — See E.4.1.

**pragma** Asynchronous (local_name); — See J.15.13.
This paragraph was deleted. **pragma** Atomic(local_name); — See C.6.

**pragma** Atomic (local_name); — See J.15.8.
This paragraph was deleted. **pragma** Atomic_Components(array_local_name); — See C.6.

**pragma** Atomic_Components (array_local_name); — See J.15.8.
This paragraph was deleted. **pragma** Attach_Handler(handler_name, expression); — See C.3.1.

**pragma** Attach_Handler (handler_name, expression); — See J.15.7.

**pragma** Conflict_Check_Policy (policy_identifier[, policy_identifier]); — See 9.10.1.
This paragraph was deleted. **pragma** Controlled(first_subtype_local_name); — See 13.11.3.
This paragraph was deleted. **pragma** Convention([Convention =>] convention_identifier[, Entity =>] local_name); — See B.1.

**pragma** Convention([Convention =>] convention_identifier[, Entity =>] local_name); — See J.15.5.
**pragma** CPU (expression); — See J.15.9.
**pragma** Default_Storage_Pool (storage_pool_indicator); — See 13.11.3.
**pragma** Detect_Blocking; — See H.5.

**pragma** Discard_Names([On => ] local_name); — See C.5.
**pragma** Dispatching_Domain (expression); — See J.15.10.
**pragma** Elaborate(library_unit_name[, library_unit_name]); — See 10.2.1.

**pragma** Elaborate_All(library_unit_name[, library_unit_name]); — See 10.2.1.
This paragraph was deleted. **pragma** Elaborate_Body(library_unit_name); — See 10.2.1.
**pragma** Elaborate_Body(library_unit_name); — See J.15.14.
This paragraph was deleted. **pragma Export(**
- [Convention =>] *convention_identifier*, [Entity =>] *local_name*
- [External_Name =>] *string_expression*[, [Link_Name =>] *string_expression*]); — See B.1.

**pragma Export(**
- [Convention =>] *convention_identifier*, [Entity =>] *local_name*
- [External_Name =>] *external_name_string_expression*
- [Link_Name =>] *link_name_string_expression*); — See J.15.5.

**pragma Generate_Deadlines;** — See D.2.6.

This paragraph was deleted. **pragma Import(**
- [Convention =>] *convention_identifier*, [Entity =>] *local_name*
- [External_Name =>] *string_expression*[, [Link_Name =>] *string_expression*]); — See B.1.

**pragma Import(**
- [Convention =>] *convention_identifier*, [Entity =>] *local_name*
- [External_Name =>] *external_name_string_expression*
- [Link_Name =>] *link_name_string_expression*); — See J.15.5.

**pragma Independent (component_local_name);** — See J.15.8.

**pragma Independent_Components (local_name);** — See J.15.8.

This paragraph was deleted. **pragma Inline(name {, name})**; — See 6.3.2.

**pragma Inline (name {, name});** — See J.15.1.

**pragma Inspection_Point[(object_name {, object_name})];** — See H.3.2.

This paragraph was deleted. **pragma Interrupt_Handler(handler_name);** — See C.3.1.

**pragma Interrupt_Handler (handler_name);** — See J.15.7.

This paragraph was deleted. **pragma Interrupt_Priority[(expression)];** — See D.1.

**pragma Interrupt_Priority [(expression)];** — See J.15.11.

**pragma Linker_Options(string_expression);** — See B.1.

**pragma List(identifier);** — See 2.8.

**pragma Locking_Policy(policy_identifier);** — See D.3.

This paragraph was deleted. **pragma No_Return(procedure_local_name{, procedure_local_name});** — See 6.5.1.

**pragma No_Return (subprogram_local_name, procedure_local_name{, subprogram_local_name, procedure_local_name});** — See J.15.2.

**pragma Normalize_Scalars;** — See H.1.

**pragma Optimize(identifier);** — See 2.8.

**pragma Pack(first_subtype_local_name);** — See 13.2.

**pragma Pack (first_subtype_local_name);** — See J.15.3.

**pragma Page;** — See 2.8.

**pragma Partition_Elaboration_Policy (policy_identifier);** — See H.6.

This paragraph was deleted. **pragma Prelaborable_Initialization(direct_name);** — See 10.2.1.
**pragma** Preelaborable_Initialization(\textit{direct	extunderscore name}); — See J.15.14.

This paragraph was deleted. **pragma** Preelaborate(\textit{library	extunderscore unit	extunderscore name}); — See J.15.14.

**pragma** Preelaborate(\textit{library	extunderscore unit	extunderscore name}); — See J.15.14.

This paragraph was deleted. **pragma** Priority(\textit{expression}); — See D.1.

**pragma** Priority(\textit{expression}); — See J.15.11.

**pragma** Priority\textunderscore Specific\textunderscore Dispatching(\textit{policy	extunderscore identifier, first	extunderscore priority	extunderscore expression, last	extunderscore priority	extunderscore expression}); — See D.2.2.

**pragma** Profile(\textit{profile	extunderscore identifier, profile	extunderscore pragma	extunderscore argument	extunderscore association}); — See D.13.

This paragraph was deleted. **pragma** Profile(\textit{profile	extunderscore identifier	extunderscore association}); — See D.13.

**pragma** Queuing\textunderscore Policy(\textit{policy	extunderscore identifier}); — See D.4.

This paragraph was deleted. **pragma** Relative\textunderscore Deadline(\textit{relative\textunderscore deadline\textunderscore expression}); — See D.2.6.

**pragma** Relative\textunderscore Deadline(\textit{relative\textunderscore deadline\textunderscore expression}); — See J.15.12.

This paragraph was deleted. **pragma** Remote\textunderscore Call\textunderscore Interface(\textit{library	extunderscore unit	extunderscore name}); — See E.2.3.

**pragma** Remote\textunderscore Call\textunderscore Interface(\textit{library	extunderscore unit	extunderscore name}); — See J.15.15.

This paragraph was deleted. **pragma** Remote\textunderscore Types(\textit{library	extunderscore unit	extunderscore name}); — See E.2.2.

**pragma** Remote\textunderscore Types(\textit{library	extunderscore unit	extunderscore name}); — See J.15.15.

**pragma** Restrictions(\textit{restriction, restriction}); — See 13.12.

**pragma** Reviewable; — See H.3.1.

This paragraph was deleted. **pragma** Shared\textunderscore Passive(\textit{library	extunderscore unit	extunderscore name}); — See E.2.1.

**pragma** Shared\textunderscore Passive(\textit{library	extunderscore unit	extunderscore name}); — See J.15.15.

This paragraph was deleted. **pragma** Storage\textunderscore Size(\textit{expression}); — See 13.3.

**pragma** Storage\textunderscore Size(\textit{expression}); — See J.15.4.

**pragma** Suppress(\textit{identifier, On => name}); — See 11.5.

**pragma** Task\textunderscore Dispatching\textunderscore Policy(\textit{policy	extunderscore identifier}); — See D.2.2.

This paragraph was deleted. **pragma** Unchecked\textunderscore Union(\textit{first\textunderscore subtype\textunderscore local\textunderscore name}); — See B.3.3.

**pragma** Unchecked\textunderscore Union(\textit{first\textunderscore subtype\textunderscore local\textunderscore name}); — See J.15.6.

**pragma** Unsuppress(\textit{identifier}); — See 11.5.

This paragraph was deleted. **pragma** Volatile(\textit{local\textunderscore name}); — See C.6.

**pragma** Volatile(\textit{local\textunderscore name}); — See J.15.8.

This paragraph was deleted. **pragma** Volatile\textunderscore Components(\textit{array\textunderscore local\textunderscore name}); — See C.6.

**pragma** Volatile\textunderscore Components(\textit{array\textunderscore local\textunderscore name}); — See J.15.8.
Wording Changes from Ada 83

39.a Pragmas List, Page, and Optimize are now officially defined in 2.8, “Pragmas”.
Annex M
(informative)

Summary of Documentation Requirements

The Ada language allows for certain target machine dependences in a controlled manner. Each Ada implementation is required to document many characteristics and properties of the target system. This Reference Manual contains specific documentation requirements. In addition, many characteristics that require documentation are identified throughout this Reference Manual as being implementation defined. Finally, this Reference Manual requires documentation of whether implementation advice is followed. The following subclauses provide summaries of these documentation requirements.

M.1 Specific Documentation Requirements

In addition to implementation-defined characteristics, each Ada implementation is required to document various properties of the implementation:

- The behavior of implementations in implementation-defined situations shall be documented — see M.2 for a listing. See 1.1.3(19).
- The set of values that a user-defined Allocate procedure needs to accept for the Alignment parameter. How the standard storage pool is chosen, and how storage is allocated by standard storage pools. See 13.11(22).
- The algorithm used for random number generation, including a description of its period. See A.5.2(44).
- The minimum time interval between calls to the time-dependent Reset procedure that is guaranteed to initiate different random number sequences. See A.5.2(45).
- The conditions under which Io_Exceptions.Name_Error, Io_Exceptions.Use_Error, and Io_Exceptions.Device_Error are propagated. See A.13(15).
- The behavior of package EnvironmentVariables when environment variables are changed by external mechanisms. See A.17(30/2).
- The overhead of calling machine-code or intrinsic subprograms. See C.1(6).
- The types and attributes used in machine code insertions. See C.1(7).
- The subprogram calling conventions for all supported convention identifiers. See C.1(8/3).
- The mapping between the Link_Name or Ada designator and the external link name. See C.1(9).
- The treatment of interrupts. See C.3(22).
- The metrics for interrupt handlers. See C.3.1(16).
- If the Ceiling_Locking policy is in effect, the default ceiling priority for a protected object that contains an interrupt handler aspect. See C.3.2(24/5).
- Any circumstances when the elaboration of a preelaborated package causes code to be executed. See C.4(12).
- Whether a partition can be restarted without reloading. See C.4(13).
• The effect of calling Current_Task from an entry body or interrupt handler. See C.7.1(19).

• For package Task_Attributes, limits on the number and size of task attributes, and how to configure any limits. See C.7.2(19).

• The metrics for the Task_Attributes package. See C.7.2(27).

• The details of the configuration used to generate the values of all metrics. See D(2).

• The maximum priority inversion a user task can experience from the implementation. See D.2.3(12/2).

• The amount of time that a task can be preempted for processing on behalf of lower-priority tasks. See D.2.3(13/2).

• The quantum values supported for round robin dispatching. See D.2.5(16/2).

• The accuracy of the detection of the exhaustion of the budget of a task for round robin dispatching. See D.2.5(17/2).

• Any conditions that cause the completion of the setting of the deadline of a task to be delayed for a multiprocessor. See D.2.6(32/2).

• Any conditions that cause the completion of the setting of the priority of a task to be delayed for a multiprocessor. See D.5.1(12/1/2).

• The metrics for Set_Priority. See D.5.1(14).

• The metrics for setting the priority of a protected object. See D.5.2(10).

• On a multiprocessor, any conditions that cause the completion of an aborted construct to be delayed later than what is specified for a single processor. See D.6(3).

• The metrics for aborts. See D.6(8).

• The values of Time_First, Time_Last, Time_Span_First, Time_Span_Last, Time_Span_Unit, and Tick for package Real_Time. See D.8(33).

• The properties of the underlying time base used in package Real_Time. See D.8(34).

• Any synchronization of package Real_Time with external time references. See D.8(35).

• Any aspects of the external environment that can interfere with package Real_Time. See D.8(36/5).

• The metrics for package Real_Time. See D.8(45).

• The minimum value of the delay expression of a delay_relative_statement that causes a task to actually be blocked. See D.9(7).

• The minimum difference between the value of the delay expression of a delay_until_statement and the value of Real_Time.Clock, that causes the task to actually be blocked. See D.9(8).

• The metrics for delay statements. See D.9(13).

• The upper bound on the duration of interrupt blocking caused by the implementation. See D.12(5).

• The metrics for entry-less protected objects. See D.12(12).

• The values of CPU_Time_First, CPU_Time_Last, CPU_Time_Unit, and CPU_Tick of package Execution_Time. See D.14(21/2).

• The properties of the mechanism used to implement package Execution_Time, including the values of the constants defined in the package. See D.14(22/2).

• The metrics for execution time. See D.14(27).
• The metrics for timing events. See D.15(24).
• The processor(s) on which the clock interrupt is handled; the processors on which each Interrupt_Id can be handled. See D.16.1(32).
• Whether the RPC-receiver is invoked from concurrent tasks, and if so, the number of such tasks. See E.5(25).
• Any techniques used to reduce cancellation errors in Numerics.Generic_Real_Arrays shall be documented. See G.3.1(86/2).
• Any techniques used to reduce cancellation errors in Numerics.Generic_Complex_Arrays shall be documented. See G.3.2(155/2).
• If a pragma Normalize_Scalars applies, the implicit initial values of scalar subtypes shall be documented. Such a value should be an invalid representation when possible; any cases when it not shall be documented. See H.1(5/2).
• The range of effects for each bounded error and each unspecified effect. If the effects of a given erroneous construct are constrained, the constraints shall be documented. See H.2(1).
• For each inspection point, a mapping between each inspectable object and the machine resources where the object's value can be obtained shall be provided. See H.3.2(8).
• If a pragma Restrictions(No Exceptions) is specified, the effects of all constructs where language-defined checks are still performed. See H.4(25).
• The interrupts to which a task entry may be attached. See J.7.1(12).
• The type of entry call invoked for an interrupt entry. See J.7.1(13).

M.2 Implementation-Defined Characteristics

{AI12-0442-1} The Ada language allows for certain machine dependences in a controlled manner. Each Ada implementation is required to document all implementation-defined characteristics:

**Ramification:** It need not document unspecified characteristics.

Some of the items in this list require documentation only for implementations that conform to Specialized Needs Annexes.

• Whether or not each recommendation given in Implementation Advice is followed — see M.3 for a listing. See 1.1.2(37).
• Capacity limitations of the implementation. See 1.1.3(3).
• Variations from the standard that are impractical to avoid given the implementation's execution environment. See 1.1.3(6).
• Which code_statements cause external interactions. See 1.1.3(10).
• The coded representation for the text of an Ada program. See 2.1(4/5).
• The semantics of an Ada program whose text is not in Normalization Form CKC. See 2.1(4.1/5).

This paragraph was deleted

The control functions allowed in comments. See 2.1(14/3).
• The representation for an end of line. See 2.2(2/3).
• Maximum supported line length and lexical element length. See 2.2(14).
• Implementation-defined pragmas. See 2.8(14).
• Effect of pragma Optimize. See 2.8(27).
• The message string associated with the Assertion_Error exception raised by the failure of a predicate check if there is no applicable Predicate_Failure aspect. See 3.2.4(31).
• The sequence of characters of the value returned by S’Image when some of the graphic characters of S’Wide_Wide_Image are not defined in Character. See 3.5(30).
• The sequence of characters of the value returned by S’Image when some of the graphic characters of S’Wide_Wide_Image are not defined in Character. See 3.5(37).
• The predefined integer types declared in Standard. See 3.5.4(25).
• Any nonstandard integer types and the operators defined for them. See 3.5.4(26/5).
• Any nonstandard real types and the operators defined for them. See 3.5.6(8/5).
• What combinations of requested decimal precision and range are supported for floating point types. See 3.5.7(7).
• The predefined floating point types declared in Standard. See 3.5.7(16/5).
• The small of an ordinary fixed point type. See 3.5.9(8/2).
• What combinations of small, range, and digits are supported for fixed point types. See 3.5.9(10).
• The result of Tags.Wide_Wide_Expanded_Name for types declared within an unnamed block_statement. See 3.9(10).
• The sequence of characters of the value returned by Tags.Expanded_Name (respectively, Tags.Wide_Wide_Expanded_Name) when some of the graphic characters of Tags.Wide_Wide_Expanded_Name are not defined in Character (respectively, Wide_Character). See 3.9(10.1/2).
• Implementation-defined attributes. See 4.1.4(12/5).
• The value of the parameter to Empty for some container_aggregates. See 4.3.5(40).
• The maximum number of chunks for a parallel_reduction_expression without a chunk_specification. See 4.5.10(21).
• Rounding of real static expressions which are exactly half-way between two machine numbers. See 4.9(38/2).
• The maximum number of chunks for a parallel_generalized_iterator without a chunk_specification. See 5.5.2(10).
• The number of chunks for an array component iterator. See 5.5.2(11).
• Any extensions of the Global aspect. See 6.1.2(43).
• The circumstances in which the implementation passes in the null value for a view conversion of an access type used as an out parameter. See 6.4.1(19/5).
• Any extensions of the Default Initial Condition aspect. See 7.3.3(11).
• Any implementation-defined time types. See 9.6(6/3).
• The time base associated with relative delays. See 9.6(20).
• The time base of the type Calendar.Time. See 9.6(23).
• The timezone used for package Calendar operations. See 9.6(24/2).
• Any limit on delay_until_statements of select_statements. See 9.6(29).
• The result of Calendar.Formatting.Image if its argument represents more than 100 hours. See 9.6.1(86/5).
• This paragraph was deleted. Whether or not two nonoverlapping parts of a composite object are independently addressable, in the case where packing, record layout, or Component_Size is specified for the object. See 9.10(1/5).
• **Implementation-defined conflict check policies.** See 9.10.1(5).

• The representation for a compilation. See 10.1(2).

• Any restrictions on compilations that contain multiple compilation_units. See 10.1(4).

• The mechanisms for creating an environment and for adding and replacing compilation units. See 10.1.4(3/2).

• **The mechanisms for adding a compilation unit mentioned in a limited with clause to an environment.** See 10.1.4(3).

• The manner of explicitly assigning library units to a partition. See 10.2(2).

• The implementation-defined means, if any, of specifying which compilation units are needed by a given compilation unit. See 10.2(2).

• The manner of designating the main subprogram of a partition. See 10.2(7).

• The order of elaboration of library_items. See 10.2(18).

• Parameter passing and function return for the main subprogram. See 10.2(21).

• The mechanisms for building and running partitions. See 10.2(24/5).

• The details of program execution, including program termination. See 10.2(25).

• The semantics of any nonactive partitions supported by the implementation. See 10.2(28/3).

• The information returned by Exception_Message. See 11.4.1(10.1/4).

• The result of `Exceptions.Wide_Wide_Exception_Name`. See 11.4.1(12).

• The sequence of characters of the value returned by `Exceptions.Exception_Name` (respectively, `Exceptions.Wide_Exceptio_Name`). See 11.4.1(12.1/2).

• The information returned by Exception_Information. See 11.4.1(13/2).

• **Implementation-defined policy identifiers and assertion aspect marks allowed in a pragma Assertion_Policy.** See 11.4.2(9/5).

• The default assertion policy. See 11.4.2(10).

• Implementation-defined check names. See 11.5(27).

• **Existence and meaning of second parameter of pragma Unspress.** See 11.5(27.1/2).

• **The cases that cause conflicts between the representation of the ancestors of a type declaration.** See 13.1(13.1/3).

• The interpretation of each `aspect of` representation aspect. See 13.1(20).

• Any restrictions placed upon the specification of representation aspects. See 13.1(20).

• Implementation-defined aspects, including the syntax for specifying such aspects and the legality rules for such aspects. See 13.1.1(38).

• The set of machine scalars. See 13.3(8.1/3).

• The meaning of Size for indefinite subtypes. See 13.3(48).

• **The meaning of Object_Size for indefinite subtypes.** See 13.3(58).

• The default external representation for a type tag. See 13.3(75/3).

• What determines whether a compilation unit is the same in two different partitions. See 13.3(76).
• Implementation-defined components. See 13.5.1(15).

• If Word_Size = Storage_Unit, the default bit ordering. See 13.5.3(5).

• The contents of the visible part of package System and its language-defined children. See 13.7(2).

• The range of Storage_Elements.Storage_Offset, the modulus of Storage_Elements.Storage_Element, and the declaration of Storage_Elements.Integer_Address. See 13.7.1(11).

• The contents of the visible part of package System.Machine_Code, and the meaning of code_statements. See 13.8(7).

• The result of unchecked conversion for instances with scalar result types whose result is not defined by the language. See 13.9(11).

• The effect of unchecked conversion for instances with nonscalar result types whose effect is not defined by the language. See 13.9(11).

• This paragraph was deleted. The manner of choosing a storage pool for an access type when Storage_Pool is not specified for the type. See 13.11(17).

• Whether or not the implementation provides user-accessible names for the standard pool type(s). See 13.11(17).

• The meaning of Storage_Size when neither the Storage_Size nor the Storage_Pool is specified for an access type. See 13.11(18).

• This paragraph was deleted. Implementation-defined aspects of storage pools. See 13.11(22/5).

• The effect of specifying aspect Default_Storage_Pool on an instance of a language-defined generic unit. See 13.11.3(5).

• This paragraph was deleted. The set of restrictions allowed in a pragma Restrictions. See 13.12(7/3).

• Implementation-defined restrictions allowed in a pragma Restrictions. See 13.12(8.7/3).

• The consequences of violating limitations on Restrictions pragmas. See 13.12(9).

• Implementation-defined usage profiles allowed in a pragma Profile. See 13.12(15).

• The contents of the stream elements read and written by the Read and Write attributes of elementary types in terms of stream elements. See 13.13.2(9).

• The names and characteristics of the numeric subtypes declared in the visible part of package Standard. See A.1(3).

• The values returned by Strings.Hash. See A.4.9(3/2).

• The value returned by a call to a Text_Buffer Get procedure if any character in the returned sequence is not defined in Character. See A.4.12(34).

• The value returned by a call to a Text_Buffer Wide_Get procedure if any character in the returned sequence is not defined in Wide_Character. See A.4.12(34).

• The accuracy actually achieved by the elementary functions. See A.5.1(1).

• The sign of a zero result from some of the operators or functions in Numerics.Generic_Elementary_Functions, when Float_Type'Signed_Zeros is True. See A.5.1(46).

• The value of Numerics.Float_Random.Max_Image_Width. See A.5.2(27).


• This paragraph was deleted. The algorithms for random number generation. See A.5.2(32/5).

• The string representation of a random number generator's state. See A.5.2(38).
• This paragraph was deleted. The minimum time interval between calls to the time dependent Reset
procedure that are guaranteed to initiate different random number sequences. See A.5.2(45).

• The values of the Model_Mantissa, Model_Emin, Model_Epsilon, Model, Safe_First, and
Safe_Last attributes, if the Numerics Annex is not supported. See A.5.3(72).

• This paragraph was deleted. Any implementation-defined characteristics of the input-output
packages. See A.7(14/5).

• The minimum time interval between calls to the time dependent Reset
procedure that are guaranteed to initiate different random number sequences. See A.5.2(45).

• The values of the Model_Mantissa, Model_Emin, Model_Epsilon, Model, Safe_First, and
Safe_Last attributes, if the Numerics Annex is not supported. See A.5.3(72).

• The interpretation of file names and directory names. See A.16(46/2).

• The maximum value for a file size in Directories. See A.16(87/2).

• The result for Directories.Size for a directory or special file. See A.16(93/2).

• The result for Directories.Modification_Time for a directory or special file. See A.16(95/2).

• The interpretation of a nonnull search pattern in Directories. See A.16(104/3).

• The results of a Directories search if the contents of the directory are altered while a search is in
progress. See A.16(110/3).

• The definition and meaning of an environment variable. See A.17(1/2).

• The circumstances where an environment variable cannot be defined. See A.17(16/2).

• Environment names for which Set has the effect of Clear. See A.17(17/2).

• The value of Containers.Hash_Type'Modulus. The value of Containers.Count_Type'Last. See
A.18.1(7/2).

• Implementation-defined convention names. See B.1(11/3).

• The meaning of link names. See B.1(36).

• The manner of choosing link names when neither the link name nor the address of an imported or
exported entity is specified. See B.1(36).

• The effect of pragma Linker_Options. See B.1(37).

• The contents of the visible part of package Interfaces and its language-defined descendants. See
B.2(1).

• Implementation-defined children of package Interfaces. The contents of the visible part of
package Interfaces. See B.2(11).

• The definitions of certain types and constants in Interfaces.C. See B.3(41).

• The types Floating, Long_Floating, Binary, Long_Binary, Decimal_Element, and
COBOL_Character; and the initializations of the variables Ada_To_COBOL and
COBOL_To_Ada, in Interfaces.COBOLO. See B.4(50).

• The types Fortran_Integer, Real, Double_Precision, and Character_Set in Interfaces.Fortran. See
B.5(17).
• **Implementation-defined intrinsic subprograms** Support for access to machine instructions. See C.1(1/3).

• **This paragraph was deleted** Implementation-defined aspects of access to machine operations. See C.1(9).

• **This paragraph was deleted** Implementation-defined aspects of interrupts. See C.3(2).

• Any restrictions on a protected procedure or its containing type when an aspect pragma Attach_handler or Interrupt_Handler is specified applies. See C.3.1(17).

• Any other forms of interrupt handler supported by the Attach_Handler and Interrupt_Handler aspects pragmas. See C.3.1(19).

• **This paragraph was deleted** Implementation-defined aspects of preelaboration. See C.4(13).

• The semantics of some attributes and functions of an entity for which aspect pragma Discard_Names is True. See C.5(7).

• The modulus and size of Test_and_Set_Flag. See C.6.3(8).

• The value used to represent the set value for Atomic_Test_and_Set. See C.6.3(10).

• The result of the Task_Identification.Image attribute. See C.7.1(7).

• The value of Current_Task when in a protected entry, or interrupt handler, or finalization of a task attribute. See C.7.1(17/3).

• **This paragraph was deleted** The effect of calling Current_Task from an entry body or interrupt handler. See C.7.1(19).

• Granularity of locking for Task_Attributes. See C.7.2(16/1).

• **This paragraph was deleted** Limits on the number and size of task attributes, and how to configure them. Implementation-defined aspects of Task_Attributes. See C.7.2(19).

• **This paragraph was deleted** Values of all Metrics. See D(2).

• The declarations of Any_Priority and Priority. See D.1(11).

• Implementation-defined execution resources. See D.1(15/5).

• Whether, on a multiprocessor, a task that is waiting for access to a protected object keeps its processor busy. See D.2.1(3).

• The effect of implementation-defined execution resources on task dispatching. See D.2.1(9/2).

• **This paragraph was deleted** Implementation-defined policy identifiers allowed in a pragma Task_Dispatching_Policy. See D.2.2(3/2).

• **This paragraph was deleted** Implementation-defined aspects of priority inversion. See D.2.2(16/2).

• Implementation defined task dispatching policies. See D.2.2(18).

• The value of Default_Quantum in Dispatching.Round_Robin. See D.2.5(4).

• Implementation-defined policy identifiers allowed in a pragma Locking_Policy. See D.3(4).

• The locking policy if no Locking_Policy pragma applies to any unit of a partition. See D.3(6).

• Default ceiling priorities. See D.3(10/4).

• The ceiling of any protected object used internally by the implementation. See D.3(16).

• Implementation-defined queuing policies. See D.4(1/5).

• **Implementation-defined admission policies. See D.4.1(1).**
• This paragraph was deleted. On a multiprocessor, any conditions that cause the completion of an aborted construct to be delayed later than what is specified for a single processor. See D.6(2).
• Any operations that implicitly require heap storage allocation. See D.7(8).
• When restriction No_Dynamic_CPU_Assignment applies to a partition, the processor on which a task with a CPU value of a Not_A_Specific_CPU will execute. See D.7(10).
• When restriction No_Task_Termination applies to a partition, what happens when a task terminates. See D.7(15.1/2).
• The behavior when restriction Max_Storage_At_Blocking is violated. See D.7(17/1).
• The behavior when restriction Max_Asynchronous_Select_Nesting is violated. See D.7(18/1).
• The behavior when restriction Max_Tasks is violated. See D.7(19).
• Whether the use of implementation-defined aspects of pragma Restrictions results in a reduction in program code or data size or execution time. See D.7(20).
• This paragraph was deleted. Implementation-defined aspects of package Real_Time. See D.8(17).
• This paragraph was deleted. Implementation-defined aspects of delay_statements. See D.9(8).
• The value of Barrier_Limit'Last in Synchronous_Barriers. See D.10.1(4/3).
• When an aborted task that is waiting on a Synchronous_Barrier is aborted. See D.10.1(13/3).
• The upper bound on the duration of interrupt blocking caused by the implementation. See D.12(5).
• The value of Min_Handler_Ceiling in Execution_Time.Group_Budgets. See D.14.2(7/2).
• The value of CPU_Range'Last in System.Multiprocessors. See D.16(4/3).
• The processor on which the environment task executes in the absence of a value for the aspect CPU. See D.16(13/3).

The means for creating and executing distributed programs. See E(5).
• Any events that can result in a partition becoming inaccessible. See E.1(7).
• The scheduling policies, treatment of priorities, and management of shared resources between partitions in certain cases. See E.1(11).
• This paragraph was deleted. Events that cause the version of a compilation unit to change. See E.3(5/4).
• Whether the execution of the remote subprogram is immediately aborted as a result of cancellation. See E.4(13).
• The range of type System.RPC.Partition_Id. See E.5(14).
• This paragraph was deleted. Implementation-defined aspects of the PCS. See E.5(25).
• Implementation-defined interfaces in the PCS. See E.5(26).
• The values of named numbers in the package Decimal. See F.2(7).
• The value of Max_Picture_Length in the package Text_IO.Editing See F.3.3(16).
• The value of Max_Picture_Length in the package Wide_Text_IO.Editing See F.3.4(5).
• The value of Max_Picture_Length in the package Wide_Wide_Text_IO.Editing See F.3.5(5).
• The accuracy actually achieved by the complex elementary functions and by other complex arithmetic operations. See G.1(1).
• The sign of a zero result (or a component thereof) from any operator or function in Numerics.Generic_Complex_Types, when Real'Signed_Zeros is True. See G.1.1(53).

• The sign of a zero result (or a component thereof) from any operator or function in Numerics.Generic_Complex_Elementary_Functions, when Complex_Types.Real'Signed_Zeros is True. See G.1.2(45).

• Whether the strict mode or the relaxed mode is the default. See G.2(2).

• The result interval in certain cases of fixed-to-float conversion. See G.2.1(10).

• The result of a floating point arithmetic operation in overflow situations, when the Machine_Overflows attribute of the result type is False. See G.2.1(13).

• The result interval for division (or exponentiation by a negative exponent), when the floating point hardware implements division as multiplication by a reciprocal. See G.2.1(16).

• The definition of close result set, which determines the accuracy of certain fixed point multiplications and divisions. See G.2.3(5).

• Conditions on a universal_real operand of a fixed point multiplication or division for which the result shall be in the perfect result set. See G.2.3(22).

• The result of a fixed point arithmetic operation in overflow situations, when the Machine_Overflows attribute of the result type is False. See G.2.3(27).

• The result of an elementary function reference in overflow situations, when the Machine_Overflows attribute of the result type is False. See G.2.4(4).

• The value of the angle threshold, within which certain elementary functions, complex arithmetic operations, and complex elementary functions yield results conforming to a maximum relative error bound. See G.2.4(10).

• The accuracy of certain elementary functions for parameters beyond the angle threshold. See G.2.4(10).

• The result of a complex arithmetic operation or complex elementary function reference in overflow situations, when the Machine_Overflows attribute of the corresponding real type is False. See G.2.6(5).

• The accuracy of certain complex arithmetic operations and certain complex elementary functions for parameters (or components thereof) beyond the angle threshold. See G.2.6(8).

• The accuracy requirements for the subprograms Solve, Inverse, Determinant, Eigenvalues and Eigensystem for type Real_Matrix. See G.3.1(81/2).

• The accuracy requirements for the subprograms Solve, Inverse, Determinant, Eigenvalues and Eigensystem for type Complex_Matrix. See G.3.2(149/2).

• This paragraph was deleted. Information regarding bounded errors and erroneous execution. See H.2(1/5).

• This paragraph was deleted. Implementation-defined aspects of pragma Inspection_Point. See H.2.2(8).

• The consequences of violating No_Hidden_IndirectGlobals. See H.4(23.9/5).

• This paragraph was deleted. Implementation-defined aspects of pragma Restrictions. See H.4(25).

• This paragraph was deleted. Any restrictions on pragma Restrictions. See H.4(27).

• Implementation-defined policy identifiers allowed in a pragma Partition_Elaboration_Policy. See H.6(4/2).
M.3 Implementation Advice

This Reference Manual sometimes gives advice about handling certain target machine dependences. Each Ada implementation is required to document whether that advice is followed:

- **Ramification:** Some of the items in this list require documentation only for implementations that conform to Specialized Needs Annexes.

- Program_Error should be raised when an unsupported Specialized Needs Annex feature is used at run time. See 1.1.3(20).

- Implementation-defined extensions to the functionality of a language-defined library unit should be provided by adding children to the library unit. See 1.1.3(21).

- If a bounded error or erroneous execution is detected, Program_Error should be raised. See 1.1.5(12).

- Implementation-defined pragmas should have no semantic effect for error-free programs. See 2.8(16/3).

- Implementation-defined pragmas should not make an illegal program legal, unless they complete a declaration or configure the library items in an environment. See 2.8(19).

- Long_Integer should be declared in Standard if the target supports 32-bit arithmetic. No other named integer subtypes should be declared in Standard. See 3.5.4(28).

- For a two's complement target, modular types with a binary modulus up to System.Max_Int*2+2 should be supported. A nonbinary modulus up to Integer'Last should be supported. See 3.5.4(29).

- Program_Error should be raised for the evaluation of S'Pos for an enumeration type, if the value of the operand does not correspond to the internal code for any enumeration literal of the type. See 3.5.5(8).

- Long_Float should be declared in Standard if the target supports 11 or more digits of precision. No other named float subtypes should be declared in Standard. See 3.5.7(17).

- Multidimensional arrays should be represented in row-major order, unless the array has convention Fortran. See 3.6.2(11/3).

- Tags.Internal_Tag should return the tag of a type, if one exists, whose innermost master is at the master of the point of the function call. See 3.9(26.1/3).

- A real static expression with a nonformal type that is not part of a larger static expression should be rounded the same as the target system. See 4.9(38.1/2).

- For each language-defined private type T, T'Image should generate an image that would be meaningful based only on the relevant public interfaces. See 4.10(56).

- The value of Duration'Small should be no greater than 100 microseconds. See 9.6(30).

- The time base for delay_relative_statements should be monotonic. See 9.6(31/5).

- Leap seconds should be supported if the target system supports them. Otherwise, operations in Calendar.Formatting should return results consistent with no leap seconds. See 9.6.1(89/2).

- This paragraph was deleted. When applied to a generic unit, a program unit pragma that is not a library unit pragma should apply to each instance of the generic unit for which there is not an overriding pragma applied directly to the instance. See 10.1.5(10/5).

- A type declared in a preelaborated package should have the same representation in every elaboration of a given version of the package. See 10.2.1(12).

- Exception_Information should provide information useful for debugging, and should include the Exception_Name and Exception_Message. See 11.4.1(19).
Exception Message by default should be short, provide information useful for debugging, and should not include the Exception Name. See 11.4.1(19).

Code executed for checks that have been suppressed should be minimized. See 11.5(28).

The recommended level of support for all representation items should be followed. See 13.1(28/5).

Storage allocated to objects of a packed type should be minimized. See 13.2(6).

The recommended level of support for the \texttt{pragma Pack} aspect should be followed. See 13.2(9).

For an array \texttt{X}, \texttt{X'Address} should point at the first component of the array rather than the array bounds. See 13.3(14).

The recommended level of support for the Address attribute should be followed. See 13.3(19).

For any tagged specific subtype \texttt{S}, \texttt{S'Class'Alignment} should equal \texttt{S'Alignment}. See 13.3(28).

The recommended level of support for the Alignment attribute should be followed. See 13.3(35).

The Size of an array object should not include its bounds. See 13.3(41.1/2).

If the Size of a subtype is nonconfirming and allows for efficient independent addressability, then the \texttt{Object Size} of the subtype (unless otherwise specified) should equal the Size of the subtype. See 13.3(52).

A Size clause on a composite subtype should not affect the internal layout of components. See 13.3(53).

The recommended level of support for the Size attribute should be followed. See 13.3(56).

An Object Size clause on a composite type should not affect the internal layout of components. See 13.3(58).

If \texttt{S} is a definite first subtype for which Object Size is not specified, \texttt{S'Object Size} should be the smallest multiple of the storage element size larger than or equal to \texttt{S'Size} that is consistent with the alignment of \texttt{S}. See 13.3(58).

The recommended level of support for the Object Size attribute should be followed. See 13.3(58).

The Size of most objects of a subtype should equal the Object Size of the subtype. See 13.3(58).

The recommended level of support for the Component Size attribute should be followed. See 13.3(73).

The recommended level of support for \texttt{enumeration representation clauses} should be followed. See 13.4(10).

The recommended level of support for \texttt{record representation clauses} should be followed. See 13.5.1(22).

If a component is represented using a pointer to the actual data of the component which is contiguous with the rest of the object, then the storage place attributes should reflect the place of the actual data. If a component is allocated discontiguously from the rest of the object, then a warning should be generated upon reference to one of its storage place attributes. See 13.5.2(5).

The recommended level of support for the nondefault bit ordering should be followed. See 13.5.3(8).

Type System Address should be a private type. See 13.7(37).

Operations in System and its children should reflect the target environment; operations that do not make sense should raise \texttt{Program Error}. See 13.7.1(16).

Type System Address should be a private type. See 13.7(37).
• Since the Size of an array object generally does not include its bounds, the bounds should not be part of the converted data in an instance of Unchecked Conversion. See 13.9(14/2).

• There should not be unnecessary runtime checks on the result of an Unchecked Conversion; the result should be returned by reference when possible. Restrictions on Unchecked Conversions should be avoided. See 13.9(15).

• The recommended level of support for Unchecked Conversion should be followed. See 13.9(17).

• Any cases in which heap storage is dynamically allocated other than as part of the evaluation of an allocator should be documented. See 13.11(23).

• A default storage pool for an access-to-constant type should not have overhead to support deallocation of individual objects. See 13.11(24).

• Usually, a storage pool for an access discriminant or access parameter should be created at the point of an allocator, and be reclaimed when the designated object becomes inaccessible. For other anonymous access types, the pool should be created at the point where the type is elaborated and may have no mechanism for the need not support deallocation of individual objects. See 13.11(25).

• For a standard storage pool, an instance of UncheckedDeallocation should actually reclaim the storage. See 13.11.2(17).

• A call on an instance of UncheckedDeallocation with a nonnull access value should raise Program Error if the actual access type of the instance is a type for which the Storage Size has been specified to be zero or is defined by the language to be zero. See 13.11.2(17.1/3).

• Streams.Storage.Bounded.Stream_Type objects should be implemented without implicit pointers or dynamic allocation. See 13.13.1(37).

• If not specified, the value of Stream Size for an elementary type should be the number of bits that corresponds to the minimum number of stream elements required by the first subtype of the type, rounded up to the nearest factor or multiple of the word size that is also a multiple of the stream element size. See 13.13.2(1.6/2).

• The recommended level of support for the Stream Size attribute should be followed. See 13.13.2(1.8/2).

• If an implementation provides additional named predefined integer types, then the names should end with “Integer”. If an implementation provides additional named predefined floating point types, then the names should end with “Float”. See A.1(52).

• Implementation-defined operations on Wide Character, Wide String, Wide Wide Character, and Wide Wide String should be child units of Wide Characters or Wide Wide Characters. See A.3.1(7/3).

• The string returned by Wide Characters.Handling.Character_Set_Version should include either “10646:” or “Unicode”. See A.3.5(62).

• Bounded string objects should not be implemented by implicit pointers and dynamic allocation. See A.4.4(106).

• Strings.Hash should be a good hash function, returning a wide spread of values for different string values, and similar strings should rarely return the same value. See A.4.9(12/2).

• If an implementation supports other string encoding schemes, a child of Ada.Strings similar to UTF_Encoding should be defined. See A.4.11(107/3).

• Bounded buffer objects should be implemented without dynamic allocation. See A.4.12(36).

• Any storage associated with an object of type Generator of the random number packages should be reclaimed on exit from the scope of the object. See A.5.2(46).
• Each value of Initiator passed to Reset for the random number packages should initiate a distinct sequence of random numbers, or, if that is not possible, be at least a rapidly varying function of the initiator value. See A.5.2(47).

• Get Immediate should be implemented with unbuffered input; input should be available immediately; line-editing should be disabled. See A.10.7(23).

• Package Directories.Information should be provided to retrieve other information about a file. See A.16(124/2).

• Directories.Start_Search and Directories.Search should raise Name_ErrorUse_Error for malformed patterns. See A.16(125).

• Directories.Rename should be supported at least when both New_Name and Old_Name are simple names and New_Name does not identify an existing external file. See A.16(126/2).

• Directories.Renaming should be provided for systems with hierarchical file naming, and should not be provided on other systems. See A.16.1(36/3).

• If the execution environment supports subprocesses, the current environment variables should be used to initialize the environment variables of a subprocess. See A.17(32/2).

• Changes to the environment variables made outside the control of Environment_Variables should be reflected immediately. See A.17(33/2).

• Containers.Hash_Type'Modulus should be at least 2**32. Containers.Count_Type'Last should be at least 2**31–1. See A.18.1(8/2).

• The worst-case time complexity of Element for Containers.Vector should be $O(\log N)$. See A.18.2(256/2).

• The worst-case time complexity of Append with Count = 1 when N is less than the capacity for Containers.Vector should be $O(\log N)$. See A.18.2(257/2).

• The worst-case time complexity of Prepend with Count = 1 and Delete First with Count=1 for Containers.Vectors should be $O(N \log N)$. See A.18.2(258/2).

• The worst-case time complexity of a call on procedure Sort of an instance of Containers.Generics.Sorting should be $O(N^2)$, and the average time complexity should be better than $O(N^2)$. See A.18.2(259/2).


• Containers.Vectors.Move should not copy elements, and should minimize copying of internal data structures. See A.18.2(261/2).

• If an exception is propagated from a vector operation, no storage should be lost, nor any elements removed from a vector unless specified by the operation. See A.18.2(262/2).

• The worst-case time complexity of Element, Insert with Count=1, and Delete with Count=1 for Containers.Doubly_Linked_Lists should be $O(\log N)$. See A.18.3(160/2).

• A call on procedure Sort of an instance of Containers.Doubly_Linked_Lists.Generic_Sorting should have an average time complexity better than $O(N^2)$ and worst case no worse than $O(N^2)$. See A.18.3(161/2).

• Containers.Doubly_Linked_Lists.Move should not copy elements, and should minimize copying of internal data structures. See A.18.3(162/2).

• If an exception is propagated from a list operation, no storage should be lost, nor any elements removed from a list unless specified by the operation. See A.18.3(163/2).
• Move for a map should not copy elements, and should minimize copying of internal data structures. See A.18.4(83/2).

• If an exception is propagated from a map operation, no storage should be lost, nor any elements removed from a map unless specified by the operation. See A.18.4(84/2).

• The average time complexity of Element, Insert, Include, Replace, Delete, Exclude, and Find operations that take a key parameter for Containers.Hashed_Maps should be $O(\log N)$. The average time complexity of the subprograms of Containers.Hashed_Maps that take a cursor parameter should be $O(1)$. The average time complexity of Containers.Hashed_Maps.Reserve_Capacity should be $O(N)$. See A.18.5(62/2).

• The worst-case time complexity of Element, Insert, Include, Replace, Delete, Exclude, and Find operations that take a key parameter for Containers.Ordered_Maps should be $O((\log N)^2)$ or better. The worst-case time complexity of the subprograms of Containers.Ordered_Maps that take a cursor parameter should be $O(1)$. See A.18.6(95/2).

• Move for sets should not copy elements, and should minimize copying of internal data structures. See A.18.7(104/2).

• If an exception is propagated from a set operation, no storage should be lost, nor any elements removed from a set unless specified by the operation. See A.18.7(105/2).

• The average time complexity of the Insert, Include, Replace, Delete, Exclude, and Find operations of Containers.Hashed_Sets that take an element parameter should be $O(\log N)$. The average time complexity of Containers.Hashed_Sets. Reserve_Capacity should be $O(N)$. See A.18.8(88/2).

• The worst-case time complexity of the Insert, Include, Replace, Delete, Exclude, and Find operations of Containers.Ordered_Sets that take an element parameter should be $O((\log N)^2)$. The worst-case time complexity of the subprograms of Containers.Ordered_Sets that take a cursor parameter should be $O(1)$. See A.18.9(116/2).

• The worst-case time complexity of the Element, Parent, First_Child, Last_Child, Next_Sibling, Previous_Sibling, Insert_Child with Count=1, and Delete operations of Containers.Multiway_Trees should be $O(\log N)$. See A.18.10(231/3).

• Containers.Multiway_Trees.Move should not copy elements, and should minimize copying of internal data structures. See A.18.10(232/3).

• If an exception is propagated from a tree operation, no storage should be lost, nor any elements removed from a tree unless specified by the operation. See A.18.10(233/3).

• Move and Swap in Containers.Indefinite_Holders.Move should not copy any elements, and should minimize copying of internal data structures. See A.18.18(73/5).

• If an exception is propagated from a holder operation, no storage should be lost, nor should the element be removed from a holder container unless specified by the operation. See A.18.18(74/3).

• Bounded vector objects should be implemented without implicit pointers or dynamic allocation. See A.18.19(16/3).

• The implementation advice for procedure Move to minimize copying does not apply to bounded vectors. See A.18.19(17/3).

• Bounded list objects should be implemented without implicit pointers or dynamic allocation. See A.18.20(19/3).

• The implementation advice for procedure Move to minimize copying does not apply to bounded lists. See A.18.20(20/3).
Bounded hashed map objects should be implemented without implicit pointers or dynamic allocation. See A.18.21(21/3).

The implementation advice for procedure Move to minimize copying does not apply to bounded hashed maps. See A.18.21(22/3).

Bounded ordered map objects should be implemented without implicit pointers or dynamic allocation. See A.18.22(18/3).

The implementation advice for procedure Move to minimize copying does not apply to bounded ordered maps. See A.18.22(19/3).

Bounded hashed set objects should be implemented without implicit pointers or dynamic allocation. See A.18.23(20/3).

The implementation advice for procedure Move to minimize copying does not apply to bounded hashed sets. See A.18.23(21/3).

Bounded ordered set objects should be implemented without implicit pointers or dynamic allocation. See A.18.24(17/3).

The implementation advice for procedure Move to minimize copying does not apply to bounded ordered sets. See A.18.24(18/3).

Bounded tree objects should be implemented without implicit pointers or dynamic allocation. See A.18.25(19/3).

The implementation advice for procedure Move to minimize copying does not apply to bounded trees. See A.18.25(20/3).

Containers.Generic_Array_Sort and Containers.Generic_Constrained_Array_Sort should have an average time complexity better than $O(N^2)$ and worst case no worse than $O(N^2)$. See A.18.26(10/2).

Containers.Generic_Array_Sort and Containers.Generic_Constrained_Array_Sort should minimize copying of elements. See A.18.26(11/2).

Containers.Generic_Sort should have an average time complexity better than $O(N^2)$ and worst case no worse than $O(N^2)$. See A.18.26(12/3).

Containers.Generic_Sort should minimize calls to the generic formal Swap. See A.18.26(13/3).

Bounded queue objects should be implemented without implicit pointers or dynamic allocation. See A.18.29(13/3).

Bounded priority queue objects should be implemented without implicit pointers or dynamic allocation. See A.18.31(14/3).

Bounded holder objects should be implemented without dynamic allocation. See A.18.32(15/5).

If pragma Export is supported for a language, the main program should be able to be written in that language. Subprograms named "adainit" and "adafinal" should be provided for elaboration and finalization of the environment task. See B.1(39/3).

Automatic elaboration of preelaborated packages should be provided when specifying the pragma Export aspect as True is supported. See B.1(40/3).

For each supported convention L other than Intrinsic, specifying the aspects pragma Import and Export should be supported for objects of L-compatible types and for subprograms, and aspect pragma Convention should be supported for L-eligible types and for subprograms. See B.1(41/5).

If an interface to C, COBOL, or Fortran is provided, the corresponding package or packages described in Annex B, “Interface to Other Languages” should also be provided. See B.2(13/3).
• The constants nul, wide_nul, char16_nul, and char32_nul in package Interfaces.C should have a representation of zero. See B.3(62.5/3).

• If C interfacing is supported, the interface correspondences between Ada and C should be supported. See B.3(71).

• If the C implementation supports unsigned long long and long long, unsigned_long_long and long_long should be supported. See B.3(71).

• If COBOL interfacing is supported, the interface correspondences between Ada and COBOL should be supported. See B.4(98).

• If Fortran interfacing is supported, the interface correspondences between Ada and Fortran should be supported. See B.5(26).

• The machine code or intrinsics support should allow access to all operations normally available to assembly language programmers for the target environment. See C.1(3).

• Interface to assembler should be supported; the default assembler should be associated with the convention identifier Assembler. See C.1(4/3).

• If an entity is exported to assembly language, then the implementation should allocate it at an addressable location even if not otherwise referenced from the Ada code. A call to a machine code or assembler subprogram should be treated as if it can only read or update every object that is specified as exported. See C.1(5).

• Little or no overhead should be associated with calling intrinsic and machine-code subprograms. See C.1(10).

• Intrinsic subprograms should be provided to access any machine operations that provide special capabilities or efficiency not normally available. See C.1(16).

• If the Ceiling Locking policy is not in effect and the target system allows for finer-grained control of interrupt blocking, a means for the application to specify which interrupts are to be blocked during protected actions should be provided. See C.3(28/2).

• Interrupt handlers should be called directly by the hardware. See C.3.1(20).

• Violations of any implementation-defined restrictions on interrupt handlers should be detected before run time. See C.3.1(21).

• If implementation-defined forms of interrupt handler procedures are supported, then for each such form of a handler, a type analogous to Parameterless_Handler should be specified in a child package of Interrupts, with the same operations as in the predefined package Interrupts. See C.3.2(25).

• Prelaborated packages should be implemented such that little or no code is executed at run time for the elaboration of entities. See C.4(14).

• If aspect pragma Discard_Names is True for an entity, then the amount of storage used for storing names associated with that entity should be reduced. See C.5(8/4).

• A load or store of a volatile object whose size is a multiple of System.Storage_Unit and whose alignment is nonzero, should be implemented by accessing exactly the bits of the object and no others. See C.6(22/5).

• A load or store of an atomic object should be implemented by a single load or store instruction. See C.6(23/2).

• If the target domain requires deterministic memory use at run time, storage for task attributes should be pre-allocated statically and the number of attributes pre-allocated should be documented. See C.7.2(30).
• Finalization of task attributes and reclamation of associated storage should be performed as soon as possible after task termination. See C.7.2(30.1/2).

• Names that end with “Locking” should be used for implementation-defined locking policies. See D.3(17).

• Names that end with “Queuing” should be used for implementation-defined queuing policies. See D.4(16).

• The `abort_statement` should not require the task executing the statement to block. See D.6(9).

• On a multi-processor, the delay associated with aborting a task on another processor should be bounded. See D.6(10).

• When feasible, specified restrictions should be used to produce a more efficient implementation. See D.7(21).

• When appropriate, mechanisms to change the value of Tick should be provided. See D.8(47).

• Calendar.Clock and Real.Time.Clock should be transformations of the same time base. See D.8(48).

• The “best” time base which exists in the underlying system should be available to the application through Real.Time.Clock. See D.8(49).

• On a multiprocessor system, each processor should have a separate and disjoint ready queue. See D.13(9).

• When appropriate, implementations should provide configuration mechanisms to change the value of Execution.Time.CPU_Tick. See D.14(29/2).

• For a timing event, the handler should be executed directly by the real-time clock interrupt mechanism. See D.15(25).

• Starting a protected action on a protected object statically assigned to a processor should not use busy-waiting. See D.16(16).

• Each dispatching domain should have separate and disjoint ready queues. See D.16.1(31).

• The PCS should allow for multiple tasks to call the RPC-receiver. See E.5(28).

• The `System.RPC.Write` operation should raise Storage_Error if it runs out of space when writing an item. See E.5(29).

• If COBOL (respectively, C) is supported in the target environment, then interfacing to COBOL (respectively, C) should be supported as specified in Annex B. See F(7/3).

• Packed decimal should be used as the internal representation for objects of subtype `S` when `S'Machine_Radix = 10`. See F.1(2).

• If Fortran (respectively, C) is supported in the target environment, then interfacing to Fortran (respectively, C) should be supported as specified in Annex B. See G(7/3).

• Mixed real and complex operations (as well as pure-imaginary and complex operations) should not be performed by converting the real (resp. pure-imaginary) operand to complex. See G.1.1(56/5).

• If Real'Signed_Zeros is True for Numerics.Generic_Complex_Types, a rational treatment of the signs of zero results and result components should be provided. See G.1.1(58).

• If Complex_Types.Real'Signed_Zeros is True for Numerics.Generic_Complex_Elementary_Functions, a rational treatment of the signs of zero results and result components should be provided. See G.1.2(49).
• For elementary functions, the forward trigonometric functions without a Cycle parameter should not be implemented by calling the corresponding version with a Cycle parameter. Log without a Base parameter should not be implemented by calling Log with a Base parameter. See G.2.4(19).

• For complex arithmetic, the Compose From Polar function without a Cycle parameter should not be implemented by calling Compose From Polar with a Cycle parameter. See G.2.6(15).

• Solve and Inverse for Numerics.Generic_Real_Arrays should be implemented using established techniques such as LU decomposition and the result should be refined by an iteration on the residuals. See G.3.1(88/3).

• The equality operator should be used to test that a matrix in Numerics.Generic_Real_Arrays is symmetric. See G.3.1(90/2).

• An implementation should minimize the circumstances under which the algorithm used for Numerics.Generic_Real_Arrays.Eigenvalues and Numerics.Generic_Real_Arrays.Eigensystem fails to converge. See G.3.1(91/3).

• Solve and Inverse for Numerics.Generic_Complex_Arrays should be implemented using established techniques and the result should be refined by an iteration on the residuals. See G.3.2(158/3).

• The equality and negation operators should be used to test that a matrix is Hermitian. See G.3.2(160/2).

• An implementation should minimize the circumstances under which the algorithm used for Numerics.Generic_Complex_Arrays.Eigenvalues and Numerics.Generic_Complex_Arrays.Eigensystem fails to converge. See G.3.2(160.1/3).

• Mixed real and complex operations should not be performed by converting the real operand to complex. See G.3.2(161/2).

• The information produced by pragma Reviewable should be provided in both a human-readable and machine-readable form, and the latter form should be documented. See H.3.1(19).

• Object code listings should be provided both in a symbolic format and in a numeric format. See H.3.1(20).

• If the partition elaboration policy is Sequential and the Environment task becomes permanently blocked during elaboration, then the partition should be immediately terminated. See H.6(15/3).

• When applied to a generic unit, a program unit pragma that is not a library unit pragma should apply to each instance of the generic unit for which there is not an overriding pragma applied directly to the instance. See J.15(9/5).
This Annex contains informal descriptions of some of the terms used in this Reference Manual. The index provides references to more formal definitions of all of the terms used in this Reference Manual. To find more formal definitions, look up the term in the index.

Informal definitions of various terms are now found in 1.3.
This Annex summarizes the complete syntax of the language.

P.1 Syntax Rules

This subclause lists the complete syntax of the language in the order it appears in this Reference Manual. See 1.1.4 for a description of the notation used.

2.1: character ::= graphic_character | format_effector | other_control_function

2.1: graphic_charater ::= identifier_letter | digit | space_character | special_character

2.3: identifier ::= identifier_start {identifier_start | identifier_extend} identifier_letter {underline} letter_or_digit

2.3: identifier_start ::= letter_or_digit ::= letter_uppercase | letter_lowercase | letter_titlecase | letter_modifier | letter_other | number_letter

2.3: identifier_extend ::= mark_non_spacing | mark_spacing_combining | number_decimal | punctuation_connector | other_format

2.4: numeric_literal ::= decimal_literal | based_literal

2.4.1: decimal_literal ::= numeral [.numeral] [exponent]

2.4.1: numeral ::= digit {[underline] digit}

2.4.1: exponent ::= E [+] numeral | E – numeral

2.4.1: digit ::= 0 1 2 3 4 5 6 7 8 9

2.4.2: based_literal ::= base # based_numeral [.based_numeral] # [exponent]

2.4.2: base ::= numeral

2.4.2: based_numeral ::= extended_digit {[underline] extended_digit}
2.5:  
character_literal ::= 'graphic_character'

2.6:  
string_literal ::= "{string_element}"  
string_element ::= "" | non_quotation_mark_graphic_character

2.7:  
comment ::= -->{non_end_of_line_character}

2.8:  
pragma ::= 
  pragma identifier [(pragma_argument_association {}, pragma_argument_association{})];

2.8:  
pragma_argument_association ::= 
  [pragma_argument_identifier =>] name
  | [pragma_argument_identifier =>] expression
  | pragma_argument aspect_mark => name
  | pragma_argument aspect_mark => expression

3.1:  
basic_declaration ::= 
  type_declaration       | subtype_declaration
  | object_declaration    | number_declaration
  | subprogram_declaration| abstract_subprogram_declaration
  | null_procedure_declaration | expression_function_declaration
  | package_declaration
  | renaming_declaration  | exception_declaration
  | generic_declaration   | generic_instantiation

3.1:  
defining_identifier ::= identifier

3.2.1:  
type_declaration ::= full_type_declaration
  | incomplete_type_declaration
  | private_type_declaration
  | private_extension_declaration

3.2.1:  
full_type_declaration ::= 
  type defining_identifier [known_discriminant_part] is type_definition
  | [aspect_specification];
  | task_type_declaration
  | protected_type_declaration

3.2.1:  
type_definition ::= 
  enumeration_type_definition | integer_type_definition
  | real_type_definition       | array_type_definition
  | record_type_definition     | access_type_definition
  | derived_type_definition    | interface_type_definition

3.2.2:  
subtype_declaration ::= 
  subtype defining_identifier is subtype_indication
  | [aspect_specification];

3.2.2:  
subtype_indication ::= [null_exclusion] subtype_mark [constraint]

3.2.2:  
subtype_mark ::= subtype_name
constraint ::= scalar_constraint | composite_constraint

3.2.2:
scalar_constraint ::= range_constraint | digits_constraint | delta_constraint

3.2.2:
composite_constraint ::= index_constraint | discriminant_constraint

3.3.1:
object_declaration ::= defining_identifier_list : [aliased] [constant] subtype_indication [:= expression]
| defining_identifier_list : [aliased] [constant] access_definition [:= expression]
| defining_identifier_list : [aliased] [constant] array_type_definition [:= expression]
| single_task_declaration
| single_protected_declaration

3.3.1:
defining_identifier_list ::= defining_identifier {, defining_identifier}

3.3.2:
number_declaration ::= defining_identifier_list : constant := static_expression;

3.4:
derived_type_definition ::= [abstract] [limited] new parent subtype_indication [and interface_list] record_extension_part

3.5:
range_constraint ::= range range

3.5:
rngae ::= range_attribute_reference
| simple_expression .. simple_expression

3.5.1:
enumeration_type_definition ::= (enumeration_literal_specification {, enumeration_literal_specification})

3.5.1:
enumeration_literal_specification ::= defining_identifier | defining_character_literal

3.5.1:
defining_character_literal ::= character_literal

3.5.4:
integer_type_definition ::= signed_integer_type_definition | modular_type_definition

3.5.4:
signed_integer_type_definition ::= range static_simple_expression .. static_simple_expression

3.5.4:
modular_type_definition ::= mod static_expression

3.5.6:
real_type_definition ::= floating_point_definition | fixed_point_definition

3.5.7:
floating_point_definition ::= digits static_expression [real_range_specification]

3.5.7:
real_range speculation ::= range static_simple_expression .. static_simple_expression
3.5.9:
fixed_point_definition ::= 
  ordinary_fixed_point_definition | decimal_fixed_point_definition

3.5.9:
ordinary_fixed_point_definition ::= 
  delta static_expression real_range_specification

3.5.9:
decimal_fixed_point_definition ::= 
  delta static_expression digits static_expression [real_range_specification]

3.5.9:
digits_constraint ::= 
  digits static simple_expression expression [range_constraint]

3.6:
array_type_definition ::= 
  unconstrained_array_definition | constrained_array_definition

3.6:
unconstrained_array_definition ::= 
  array (index_subtype_definition {, index_subtype_definition}) of component_definition

3.6:
index_subtype_definition ::= subtype_mark range <=

3.6:
constrained_array_definition ::= 
  array (discrete_subtype_definition {, discrete_subtype_definition}) of component_definition

3.6:
discrete_subtype_definition ::= discrete_subtype_indication | range

3.6:
component_definition ::= 
  [aliased] subtype_indication 
  [aliased] access_definition

3.6.1:
index_constraint ::= (discrete_range {, discrete_range})

3.6.1:
discrete_range ::= discrete_subtype_indication | range

3.7:
discriminant_part ::= unknown_discriminant_part | known_discriminant_part

3.7:
unknown_discriminant_part ::= (<>)

3.7:
known_discriminant_part ::= 
  (discriminant_specification {, discriminant_specification})

3.7:
discriminant_specification ::= 
  defining_identifier_list : null_exclusion subtype_mark ::= default_expression 
  [aspect_specification]
  defining_identifier_list : access_definition ::= default_expression 
  [aspect_specification]

3.7:
default_expression ::= expression

3.7.1:
discriminant_constraint ::= 
  (discriminant_association {, discriminant_association})

3.7.1:
discriminant_association ::= 
  [discriminant_selector_name {, discriminated_selector_name} =>] expression

3.8:
record_type_definition ::= [[abstract tagged] [limited] record_definition
3.8:
record_definition ::= 
   record
   component_list
end record [record_identifier] 
| null record 

3.8:
component_list ::= 
   component_item {component_item}
   | {component_item} variant_part 
   | null; 

3.8:
component_item ::= component_declaration | aspectClause | representationClause 

3.8:
component_declaration ::= 
   defining_identifier_list : component_definition [:= default_expression]
   [aspectSpecification]; 

3.8.1:
variant_part ::= 
   case discriminant_direct_name is
   variant
   | variant
end case; 

3.8.1:
variant ::= 
   when discrete_choice_list =>
   component_list 

3.8.1:
discrete_choice_list ::= discrete_choice {\| discrete_choice} 

3.8.1:
discrete_choice ::= 
   choice_expression expression | discrete_subtype_indication | ranged_discrete_range | others 

3.9.1:
record_extension_part ::= with record_definition 

3.9.3:
abstract_subprogram_declaration ::= 
   [overriding_indicator]
   subprogram_specification is abstract 
   [aspectSpecification]; 

3.9.4:
interface_type_definition ::= 
   [limited | task | protected | synchronized] interface [and interface_list] 

3.9.4:
interface_list ::= interface_subtype_mark [and interface_subtype_mark] 

3.10:
access_type_definition ::= 
   [null_exclusion] access_to_object_definition 
   [null_exclusion] access_to_subprogram_definition 

3.10:
access_to_object_definition ::= 
   access [general_access_modifier] subtype_indication 

3.10:
general_access_modifier ::= all | constant 

3.10:
access_to_subprogram_definition ::= 
   access [protected] procedure parameter_profile 
   | access [protected] function parameter_and_result_profile
null_exclusion ::= not null

access_definition ::= [null_exclusion] access [constant] subtype_mark
[null_exclusion] access [protected] procedure parameter_profile
[null_exclusion] access [protected] function parameter_and_result_profile

incomplete_type_declaration ::= type defining_identifier [discriminant_part] [is tagged];

declarative_part ::= {declarative_item}

declarative_item ::= basic_declarative_item | body

basic_declarative_item ::= basic_declaration | aspect_clause | representation_clause | use_clause

body ::= proper_body | body_stub

proper_body ::= subprogram_body | package_body | task_body | protected_body

name ::= direct_name | explicit_dereference
indexed_component | slice
selected_component | attribute_reference
| type_conversion | function_call
character_literal | qualified_expression
| generalized_reference | generalized_indexing
| target_name

direct_name ::= identifier | operator_symbol

prefix ::= name | implicit_dereference

explicit_dereference ::= name.all

implicit_dereference ::= name

indexed_component ::= prefix(expression {, expression})

slice ::= prefix(discrete_range)

selected_component ::= prefix.selector_name

selector_name ::= identifier | character_literal | operator_symbol

attribute_reference ::= __prefix.attribute_designator
| reduction_attribute_reference

attribute_designator ::= identifier[(static expression)]
| Access | Delta | Digits | Mod
4.1.4:
range_attribute_reference ::= prefix'range_attribute_designator

4.1.4:
range_attribute_designator ::= Range(static_expression)

4.1.5:
generalized_reference ::= reference_object_name

4.1.6:
generalized_indexing ::= indexable_container_object_prefix actual_parameter_part

4.3:
aggregate ::= record_aggregate | extension_aggregate | array_aggregate
| delta_aggregate | container_aggregate

4.3.1:
record_aggregate ::= (record_component_association_list)

4.3.1:
record_component_association_list ::= record_component_association , record_component_association
| null_record

4.3.1:
record_component_association ::= [component_choice_list => ] expression
| [component_choice_list => <>]

4.3.1:
component_choice_list ::= component_selector_name ["" component_selector_name]
| others

4.3.2:
extension_aggregate ::= (ancestor_part with record_component_association_list)

4.3.2:
ancestor_part ::= expression | subtype_mark

4.3.3:
array_aggregate ::= positional_array_aggregate | null_array_aggregate | named_array_aggregate

4.3.3:
positional_array_aggregate ::= (expression, expression , expression)
| (expression , expression , others => expression)
| (expression , expression , others => <>)
| "[" expression , expression ]; others => expression ]"
| "[" expression , expression ]; others => <> ""

4.3.3:
null_array_aggregate ::= "[]"

4.3.3:
named_array_aggregate ::= (array_component_association_list)
| "["array_component_association_list ""]array_component_association {, array_component_association}"

4.3.3:
array_component_association_list ::= array_component_association {, array_component_association}

4.3.3:
array_component_association ::= discrete_choice_list => expression
| discrete_choice_list => <>
| iterated_component_association

4.3.3:
iterated_component_association ::=
for defining_identifier in discrete_choice_list => expression
for iterator_specification => expression

4.3.4:
delta_aggregate ::= record_delta_aggregate | array_delta_aggregate

4.3.4:
record_delta_aggregate ::= (base_expression with delta record_component_association_list)

4.3.4:
array_delta_aggregate ::= (base_expression with delta array_component_association_list)

4.3.5:
container_aggregate ::= null_container_aggregate | positional_container_aggregate | named_container_aggregate

4.3.5:
null_container_aggregate ::= [ ]

4.3.5:
positional_container_aggregate ::= [ expression , expression ]

4.3.5:
named_container_aggregate ::= [ ' ' container_element_association_list ' ' ]

4.3.5:
container_element_association_list ::= container_element_association |

4.3.5:
container_element_association ::= key_choice_list => expression |
key_choice_list => <> |
iterated_element_association

4.3.5:
key_choice_list ::= key_choice | key_choice_list | '

4.3.5:
key_choice ::= key_expression | discrete_range

4.3.5:
iterated_element_association ::= for loop_parameter_specification[ use key_expression ] => expression |
for iterator_specification[ use key_expression ] => expression

4.4:
expression ::= relation { and relation } | relation { and then relation }
| relation { or relation } | relation { or else relation }
| relation { xor relation }

4.4:
choice_expression ::= choice_relation { and choice_relation }
| choice_relation { or choice_relation }
| choice_relation { xor choice_relation }
| choice_relation { and then choice_relation }
| choice_relation { or else choice_relation }

4.4:
choice_relation ::= simple_expression [ relational_operator simple_expression ]

4.4:
relation ::= simple_expression [ relational_operator simple_expression ]
| tested simple_expression simple_expression [ not ] in membership_choice_list
raise_expression :=
| simple_expression {not} in subtype_mark

membership_choice_list ::= membership_choice {"|" membership_choice}

membership_choice ::= choice simple_expression choice_expression | range | subtype_mark

simple_expression ::= [unary_adding_operator] term {binary_adding_operator term}
term ::= factor {multiplying_operator factor}
factor ::= primary [** primary] | abs primary | not primary

primary ::= numeric_literal | null | string_literal | aggregate | name | qualified_expression | allocator | (expression) | (conditional_expression) | (quantified_expression) | (declare_expression)

logical_operator ::= and | or | xor

relational_operator ::= = | /= | < | <= | > | >=

binary_adding_operator ::= + | – | &

unary_adding_operator ::= + | –

multiplying_operator ::= * | / | mod | rem

highest_precedence_operator ::= ** | abs | not

conditional_expression ::= if_expression | case_expression

if_expression ::= if condition then dependent_expression {elsif condition then dependent_expression} [else dependent_expression]

condition ::= boolean_expression

case_expression ::= for quantifier loop_parameter_specification => predicate | for quantifier iterator_specification => predicate

quantifier ::= all | some
4.5.8: 
   predicate ::= boolean_expression

4.5.9: 
   declare_expression ::= 
       declare (declare_item) 
       begin body_expression

4.5.9: 
   declare_item ::= object_declaration | object_renaming_declaration

4.5.10: 
   reduction_attribute_reference ::= 
       value_sequence/reduction_attribute_designator 
       | prefix/reduction_attribute_designator

4.5.10: 
   value_sequence ::= 
       '[' [parallel] [chunk_specification] [aspect_specification] 
       iterated_element_association ']

4.5.10: 
   reduction_attribute_designator ::= 
       reduction_identifier(reduction_specification)

4.5.10: 
   reduction_specification ::= reducer_name, initial_value_expression

4.6: 
   type_conversion ::= 
       subtype_mark(expression) 
       | subtype_mark(name)

4.7: 
   qualified_expression ::= 
       subtype_mark'(expression) | subtype_mark'aggregate

4.8: 
   allocator ::= 
       new [subpool_specification] subtype_indication 
       | new [subpool_specification] qualified_expression

4.8: 
   subpool_specification ::= (subpool_handle_name)

5.1: 
   sequence_of_statements ::= statement {statement} [label]

5.1: 
   statement ::= 
       {label} simple_statement | {label} compound_statement

5.1: 
   simple_statement ::= null_statement 
       | assignment_statement 
       | goto_statement 
       | simple_return_statement 
       | return_statement 
       | requeue_statement 
       | abort_statement 
       | code_statement 

5.1: 
   compound_statement ::= 
       if_statement 
       | loop_statement 
       | extended_return_statement 
       | parallel block_statement 
       | accept_statement 
       | case_statement 
       | block_statement 

5.1: 
   null_statement ::= null;
label ::= "<label_statement_identifier>"

5.1:
statement_identifier ::= direct_name

5.2:
assignment_statement ::= 
    variable_name := expression;

5.2.1:
target_name ::= @

5.3:
if_statement ::= 
    if condition then
    sequence_of_statements
    {elsif condition then
    sequence_of_statements}
    [else
    sequence_of_statements]
end if;

5.3:
condition ::= boolean_expression

5.4:
case_statement ::= 
    case selecting_expression is
    case_statement_alternative
    {case_statement_alternative}
    end case;

5.4:
case_statement_alternative ::= 
    when discrete_choice_list =>
    sequence_of_statements

5.5:
loop_statement ::= 
    [loop_statement_identifier:] 
    [iteration_scheme] loop
    sequence_of_statements
    end loop [loop_identifier];

5.5:
iteration_scheme ::= while condition
    | for loop_parameter_specification
    | for iterator_specification
    | [parallel [aspect_specification]]
    | for procedural_iterator
    | [parallel [chunk_specification]] [aspect_specification]
    | for loop_parameter_specification
    | [parallel [chunk_specification]] [aspect_specification]
    | for iterator_specification

5.5:
chunk_specification ::= 
    integer_simple_expression
    | defining_identifier in discrete_subtype_definition

5.5:
loop_parameter_specification ::= 
    defining_identifier in [reverse] discrete_subtype_definition
    | [iterator_filter]

5.5:
iterator_filter ::= when condition

5.5.2:
iterator_specification ::= 
    defining_identifier [loop_parameter_subtype_indication] in [reverse] iterator_name
5.5.2:  
loop_parameter_subtype_indication ::= subtype_indication | access_definition

5.5.3:  
procedural_iterator ::=  
  iterator_parameter_specification of iterator_procedure_call
  [iterator_filter]

5.5.3:  
iterator_parameter_specification ::=  
  formal_part
  | (defining_identifier, defining_identifier)

5.5.3:  
iterator_procedure_call ::=  
  procedure_name
  | procedure_prefix iterator_actual_parameter_part

5.5.3:  
iterator_actual_parameter_part ::=  
  (iterator_parameter_association, iterator_parameter_association)

5.5.3:  
iterator_parameter_association ::=  
  parameter_association
  | parameter_association_with_box

5.5.3:  
parameter_association_with_box ::=  
  [formal_parameter_selector_name => ] <>

5.6:  
block_statement ::=  
  [block_statement_identifier:]  
  [declare  
    declarative_part]  
  begin  
    handled_sequence_of_statements  
  end [block_identifier];

5.6.1:  
parallel_block_statement ::=  
  parallel [(chunk_specification)] [aspect_specification] do  
  sequence_of_statements
  and
  sequence_of_statements
  [and
  sequence_of_statements]
  end do;

5.7:  
exit_statement ::=  
  exit [loop_name] [when condition];

5.8:  
goto_statement ::= goto label_name;

6.1:  
subprogram_declaration ::=  
  [overriding_indicator]
  subprogram_specification
  [aspect_specification];

6.1:  
abstract_subprogram_declaration ::= subprogram_specification is abstract;

6.1:  
subprogram_specification ::=
procedure_specification | function_specification

procedure defining_program_unit_name parameter_profile

function defining_designator parameter_and_result_profile

6.1:
procedure_specification ::= 
    procedure defining_program_unit_name parameter_profile

6.1:
function_specification ::= 
    function defining_designator parameter_and_result_profile

6.1:
designator ::= [parent_unit_name . ]identifier | operator_symbol

6.1:
defining_designator ::= 
    defining_program_unit_name | defining_operator_symbol

6.1:
defining_program_unit_name ::= [parent_unit_name . ]defining_identifier

6.1:
operator_symbol ::= string_literal

6.1:
defining_operator_symbol ::= operator_symbol

6.1:
parameter_profile ::= [formal_part]

6.1:
parameter_and_result_profile ::= 
    [formal_part] return [null_exclusion] subtype_mark
    [formal_part] return access_definition

6.1:
formal_part ::= 
    (parameter_specification {; parameter_specification})

6.1:
parameter_specification ::= 
    defining_identifier_list: [aliased] mode [null_exclusion] subtype_mark [:= default_expression]

7 aspect specification

| defining_identifier_list: access_definition [:= default_expression]

6.1:
mode ::= [in] | in out | out

6.1.2:
    global_aspect_definition ::= 
        null
        Unspecified
        global_mode global_designator
        (global_aspect_element {; global_aspect_element})

6.1.2:
global_aspect_element ::= 
    global_mode global_set
    global_mode all
    global_mode synchronized

6.1.2:
global_mode ::= 
    basic_global_mode
    extended_global_mode

6.1.2:
basic_global_mode ::= in | in out | out

6.1.2:
global_set ::= global_name {, global_name}
6.1.2:
  global_designator ::= all | synchronized | global_name

6.1.2:
  global_name ::= object_name | package_name

6.3:
  subprogram_body ::= 
    [overriding_indicator] 
    subprogram_specification 
    [aspect_specification] is 
    declarative_part 
    begin 
    handled_sequence_of_statements 
    end [designator];

6.4:
  procedure_call_statement ::= 
    procedure_name; 
    | procedure_prefix actual_parameter_part;

6.4:
  function_call ::= 
    function_name 
    | function_prefix actual_parameter_part

6.4:
  actual_parameter_part ::= 
    (parameter_association {, parameter_association})

6.4:
  parameter_association ::= 
    [formal_parameter_selector_name =>] explicit_actual_parameter

6.4:
  explicit_actual_parameter ::= expression | variable_name

6.5:
  simple_return_statement ::= return [expression];

6.5:
  extended_return_object_declaration ::= 
    defining_identifier : [aliased] [constant] return_subtype_indication [:= expression] 
    [aspect_specification]

6.5:
  extended_return_statement ::= 
    return extended_return_object_declaration defining_identifier : [constant aliased] return_subtype_indication [:= expression] do 
    handled_sequence_of_statements 
    end return;

6.5:
  return_subtype_indication ::= subtype_indication | access_definition

6.7:
  null_procedure_declaration ::= 
    [overriding_indicator] 
    procedure_specification is null 
    [aspect_specification];

6.8:
  expression_function_declaration ::= 
    [overriding_indicator] 
    function_specification is 
    (expression) 
    [aspect_specification]; 
    | [overriding_indicator] 
    function_specification is 
    aggregate 
    [aspect_specification];
7.1:
    package_declaration ::= package_specification;

7.1:
    package_specification ::= 
        package defining_program_unit_name 
        [aspect_specification] is 
        {basic_declarative_item} 
        [private 
        {basic_declarative_item}] 
        end [parent_unit_name.]identifier]

7.2:
    package_body ::= 
        package body defining_program_unit_name 
        [aspect_specification] is 
        declarative_part 
        [begin 
        handled_sequence_of_statements] 
        end [parent_unit_name.]identifier];

7.3:
    private_type_declaration ::= 
        type defining_identifier [discriminant_part] is [[abstract] tagged] [limited] private 
        [aspect_specification];

7.3:
    private_extension_declaration ::= 
        type defining_identifier [discriminant_part] is 
        [abstract] [limited | synchronized] new ancestor_subtype_indication 
        [and interface_list] with private 
        [aspect_specification];

8.3.1:
    overriding_indicator ::= [not] overriding

8.4:
    use_clause ::= use_package_clause | use_type_clause

8.4:
    use_package_clause ::= use package_name {, package_name};

8.4:
    use_type_clause ::= use [all] type subtype_mark {, subtype_mark};

8.5:
    renaming_declaration ::= 
        object_renaming_declaration 
        | exception_renaming_declaration 
        | package_renaming_declaration 
        | subprogram_renaming_declaration 
        | generic_renaming_declaration

8.5.1:
    object_renaming_declaration ::= 
        defining_identifier [: [null_exclusion] subtype_mark] renames object_name 
        [aspect_specification];
        | defining_identifier : access_definition renames object_name 
        [aspect_specification];

8.5.2:
    exception_renaming_declaration ::= 
        defining_identifier : exception renames exception_name 
        [aspect_specification];

8.5.3:
    package_renaming_declaration ::= 
        package defining_program_unit_name renames package_name 
        [aspect_specification];

8.5.4:
subprogram_renaming_declaration ::=  
  [overriding_indicator]  
  subprogram_specification renames callable_entity_name  
  [aspect_specification];

8.5.5:  
generic_renaming_declaration ::=  
  generic package defining_program_unit_name renames generic_package_name  
  [aspect_specification];  
  |  
  generic procedure defining_program_unit_name renames generic_procedure_name  
  [aspect_specification];  
  |  
  generic function defining_program_unit_name renames generic_function_name  
  [aspect_specification];

9.1:  
task_type_declaration ::=  
  task type defining_identifier [known_discriminant_part]  
  [aspect_specification] [is  
  [new interface_list with]  
  task_definition];

9.1:  
single_task_declaration ::=  
  task defining_identifier  
  [aspect_specification] [is  
  [new interface_list with]  
  task_definition];

9.1:  
task_definition ::=  
  {task_item}  
  [private  
  {task_item}]  
  end [task_identifier]

9.1:  
task_item ::= entry_declaration | aspect_clause representation_clause

9.1:  
task_body ::=  
  task body defining_identifier  
  [aspect_specification] is  
  declarative_part  
  begin  
  handled_sequence_of_statements  
  end [task_identifier];

9.4:  
protected_type_declaration ::=  
  protected type defining_identifier [known_discriminant_part]  
  [aspect_specification] is  
  [new interface_list with]  
  protected_definition;

9.4:  
single_protected_declaration ::=  
  protected defining_identifier  
  [aspect_specification] is  
  [new interface_list with]  
  protected_definition;

9.4:  
protected_definition ::=  
  { protected_operation_declaration }  
  [private  
  { protected_element_declaration } ]  
  end [protected_identifier]

9.4:  
protected_operation_declaration ::= subprogram_declaration
| entry_declaration
| aspect_clause representation_clause

9.4:
protected_element_declaration ::= protected_operation_declaration
| component_declaration

9.4:
protected_body ::= protected body defining_identifier
| [aspect_specification] is
| { protected_operation_item }
| end [protected_identifier];

9.4:
protected_operation_item ::= subprogram_declaration
| subprogram_body
| null_procedure_declaration
| expression_function_declaration
| entry_body
| aspect_clause representation_clause

9.5:
synchronization_kind ::= By_Entry | By_Protected_Procedure | Optional

9.5.2:
entry_declaration ::= [overriding_indicator]
| entry defining_identifier [(discrete_subtype_definition)] parameter_profile
| [aspect_specification];

9.5.2:
accept_statement ::= accept entry_direct_name [(entry_index)] parameter_profile [do
| handled_sequence_of_statements
| end [entry_identifier]];

9.5.2:
entry_index ::= expression

9.5.2:
entry_body ::= entry defining_identifier entry_body_formal_part
| [aspect_specification]
| entry_barrier is
| declarative_part
| begin
| handled_sequence_of_statements
| end [entry_identifier];

9.5.2:
entry_body_formal_part ::= [(entry_index_specification)] parameter_profile

9.5.2:
entry_barrier ::= when condition

9.5.2:
entry_index_specification ::= for defining_identifier in discrete_subtype_definition [aspect_specification]

9.5.3:
entry_call_statement ::= entry_name [actual_parameter_part];

9.5.4:
requeue_statement ::= requeue procedure_or_entry_entry_name [with abort];

9.6:
delay_statement ::= delay_until_statement | delay_relative_statement

9.6:
delay_until_statement ::= delay until delay_expression;
delay_relative_statement ::= delay delay_expression;

9.7:
select_statement ::= selective_accept
| timed_entry_call
| conditional_entry_call
| asynchronous_select

9.7.1:
selective_accept ::= select
[guard]
select_alternative
{ or
 [guard]
 select_alternative }
[ else
 sequence_of_statements ]
end select;

9.7.1:
guard ::= when condition =>

9.7.1:
select_alternative ::= accept_alternative
| delay_alternative
| terminate_alternative

9.7.1:
accept_alternative ::= accept_statement [sequence_of_statements]

9.7.1:
delay_alternative ::= delay_statement [sequence_of_statements]

9.7.1:
terminate_alternative ::= terminate;

9.7.2:
timed_entry_call ::= select
 entry_call_alternative
or
delay_alternative
end select;

9.7.2:
entry_call_alternative ::= procedure_or_entry_call entry_call_statement [sequence_of_statements]

9.7.2:
procedure_or_entry_call ::= procedure_call_statement | entry_call_statement

9.7.3:
conditional_entry_call ::= select
 entry_call_alternative
else
 sequence_of_statements
end select;

9.7.4:
asynchronous_select ::= select
 triggering_alternative
 then abort
 abortable_part
end select;
9.7.4: triggering_alternative ::= triggering_statement [sequence_of_statements]
9.7.4: triggering_statement ::= procedure_or_entry_callentry_call_statement | delay_statement
9.7.4: abortable_part ::= sequence_of_statements
9.8: abort_statement ::= abort task_name {, task_name};
10.1.1: compilation ::= {compilation_unit}
10.1.1: compilation_unit ::= context_clause library_item | context_clause subunit
10.1.1: library_item ::= [private] library_unit_declaration | library_unit_body | [private] library_unit_renaming_declaration
10.1.1: library_unit_declaration ::= subprogram_declaration | package_declaration | generic_declaration | generic_instantiation
10.1.1: library_unit_renaming_declaration ::= package_renaming_declaration | generic_renaming_declaration | subprogram_renaming_declaration
10.1.1: library_unit_body ::= subprogram_body | package_body
10.1.1: parent_unit_name ::= name
10.1.2: context_clause ::= {context_item}
10.1.2: context_item ::= with_clause | use_clause
10.1.2: with_clause ::= limited_with_clause | nonlimited_with_clause with library_unit_name {, library_unit_name};
10.1.2: limited_with_clause ::= limited [private] with library_unit_name {, library_unit_name};
10.1.2: nonlimited_with_clause ::= [private] with library_unit_name {, library_unit_name};
10.1.3: body_stub ::= subprogram_body_stub | package_body_stub | task_body_stub | protected_body_stub
10.1.3: subprogram_body_stub ::= [overriding_indicator]
10.1.3: package_body_stub ::= package_body defining_identifier is separate
10.1.3: aspect_specification;
10.1.3: task_body_stub ::= task body defining_identifier is separate [aspect_specification];

10.1.3: protected_body_stub ::= protected body defining_identifier is separate [aspect_specification];

10.1.3: subunit ::= separate (parent_unit_name) proper_body

11.1: exception_declaration ::= defining_identifier_list : exception [aspect_specification];

11.2: handled_sequence_of_statements ::= sequence_of_statements {exception exception_handler {exception_handler}}

11.2: exception_handler ::= when [choice_parameter_specification:] exception_choice ['|' exception_choice] => sequence_of_statements

11.2: choice_parameter_specification ::= defining_identifier

11.2: exception_choice ::= exception_name | others

11.3: raise_statement ::= raise:

11.3: raise_expression ::= raise exception_name [with string_expression]; raise [exception_name];

12.1: generic_declaration ::= generic_subprogram_declaration | generic_package_declaration

12.1: generic_subprogram_declaration ::= generic_formal_part subprogram_specification [aspect_specification];

12.1: generic_package_declaration ::= generic_formal_part package_specification;

12.1: generic_formal_part ::= generic {generic_formal_parameter_declaration | use_clause}

12.1: generic_formal_parameter_declaration ::= formal_object_declaration | formal_type_declaration | formal_subprogram_declaration | formal_package_declaration

12.3: genericInstantiation ::= package defining_program_unit_name is new generic_package_name [generic_actual_part] [aspect_specification]; [overriding_indicator]
procedure defining_program_unit_name is
  new generic_procedure_name [generic_actual_part]
  [aspect_specification];
  [overriding_indicator]
function defining_designator is
  new generic_function_name [generic_actual_part]
  [aspect_specification];
12.3: generic_actual_part ::= (generic_association {. generic_association})
12.3: explicit_generic_actual_parameter ::= expression | variable_name
  | subprogram_name | entry_name | subtype_mark
  | package_instance_name
12.4: formal_object_declaration ::= defining_identifier_list : mode [null_exclusion] subtype_mark [:= default_expression]
  [aspect_specification];
  |- defining_identifier_list : mode access_definition [:= default_expression]
  [aspect_specification];
12.5: formal_type_declaration ::= formal_complete_type_declaration
  | formal_incomplete_type_declaration
12.5: formal_complete_type_declaration ::= type defining_identifier [discriminant_part] is formal_type_definition
  | [or use default subtype_mark] [aspect_specification];
12.5: formal_incomplete_type_declaration ::= type defining_identifier [discriminant_part] [is tagged]
  | [or use default subtype_mark];
12.5: formal_type_definition ::= formal_private_type_definition
  | formal_derived_type_definition
  | formal_discrete_type_definition
  | formal_signed_integer_type_definition
  | formal_modular_type_definition
  | formal_floating_point_definition
  | formal_ordinary_fixed_point_definition
  | formal_decimal_fixed_point_definition
  | formal_array_type_definition
  | formal_access_type_definition
  | formal_interface_type_definition
12.5.1: formal_private_type_definition ::= [[abstract] tagged] [limited] private
12.5.1: formal_derived_type_definition ::= [abstract] [limited] synchronized new subtype_mark [and interface_list with private]
12.5.2: formal_discrete_type_definition ::= (<>)
12.5.2: formal_signed_integer_type_definition ::= range <>
formal_modular_type_definition ::= mod <>
12.5.2:
formal_floating_point_definition ::= digits <>
12.5.2:
formal_ordinary_fixed_point_definition ::= delta <>
12.5.2:
formal_decimal_fixed_point_definition ::= delta <> digits <>
12.5.3:
formal_array_type_definition ::= array_type_definition
12.5.4:
formal_access_type_definition ::= access_type_definition
12.5.5:
formal_interface_type_definition ::= interface_type_definition
12.6:
formal_subprogram_declaration ::= formal_concrete_subprogram_declaration
    | formal_abstract_subprogram_declaration with subprogram_specification [is subprogram_default];
12.6:
formal_concrete_subprogram_declaration ::=__with subprogram_specification [is subprogram_default]
    __[aspect_specification];
12.6:
formal_abstract_subprogram_declaration ::=__with subprogram_specification is abstract [subprogram_default]
    __[aspect_specification];
12.6:
subprogram_default ::= default_name | <> | null
12.6:
default_name ::= name
12.7:
formal_package_declaration ::=__with package defining_identifier is new generic_package_name formal_package_actual_part
    __[aspect_specification];
12.7:
formal_package_actual_part ::=__[(others =>) <>]
    __[generic_actual_part]
    __((formal_package_association ), formal_package_association ) [ others =>]<>|[generic_actual_part]
12.7:
formal_package_association ::=__generic_association
    __generic_formal_parameter_selector_name => <>
13.1:
aspect_clauserepresentation_clause ::= attribute_definition_clause
    | enumeration_representation_clause
    | record_representation_clause
    | at_clause
13.1:
local_name ::= direct_name
    | direct_name'attribute_designator
    | library_unit_name
13.1.1:
aspect_specification ::=__with aspect_mark [=> aspect_definition] [,
    __] aspect_mark [=> aspect_definition]
13.1.1:
aspect_marker ::= aspect_identifier[Class]
13.1.1:
aspect_definition ::= 
  name | expression | identifier 
  | aggregate | global_aspect_definition

13.3:
attribute_definition_clause ::= 
  for local_name attribute_designator use expression; 
  | for local_name attribute_designator use name;

13.4:
enumeration_representation_clause ::= 
  for first_subtype_local_name use enumeration_aggregate;

13.4:
enumeration_aggregate ::= array_aggregate

13.5.1:
record_representation_clause ::= 
  for first_subtype_local_name use 
    record [mod_clause] 
    {component_clause} 
  end record [local_name];

13.5.1:
component_clause ::= 
  component_local_name at position range first_bit .. last_bit;

13.5.1:
position ::= static_expression

13.5.1:
first_bit ::= static_simple_expression

13.5.1:
last_bit ::= static_simple_expression

13.8:
code_statement ::= qualified_expression;

13.11.3:
storage_pool_indicator ::= storage_pool_name | null | Standard

13.12:
restriction ::= restriction_identifier 
  | restriction_parameter_identifier => restriction_parameter_argument

13.12:
restriction_parameter_argument ::= name | expression

H.7:
extended_global_mode ::= 
  overriding basic_global_mode

H.7.1:
formal_parameter_set ::= 
  formal_group_designator 
  | formal_subprogram_name 
  | ((formal_parameter_name | formal_parameter_name))

H.7.1:
formal_group_designator ::= null | all

H.7.1:
formal_parameter_name ::= 
  formal_subtype_mark 
  | formal_subprogram_name 
  | formal_access_to_subprogram_object_name

H.7.1:
dispatching_operation_set ::= 
  dispatching_operation_specifier 
  | (dispatching_operation_specifier | dispatching_operation_specifier)
### P.2 Syntax Cross Reference

**{AI05-0299-1}** In the following syntax cross reference, each syntactic category is followed by the subclause number where it is defined. In addition, each syntactic category $S$ is followed by a list of the categories that use $S$ in their definitions. For example, the first listing below shows that `abort_statement` appears in the definition of `simple_statement`.

<table>
<thead>
<tr>
<th>Syntactic Category</th>
<th>Subclause</th>
<th>Used by Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>abort_statement</code></td>
<td>9.8</td>
<td><code>qualified_expression</code></td>
</tr>
<tr>
<td><code>simple_statement</code></td>
<td>5.1</td>
<td><code>qualified_expression</code>, <code>allocator</code>, <code>primary</code></td>
</tr>
<tr>
<td><code>abortable_part</code></td>
<td>9.7.4</td>
<td><code>protocol_part</code>, <code>asynchronous_select</code></td>
</tr>
<tr>
<td><code>asynchronous_select</code></td>
<td>9.7.4</td>
<td><code>protocol_part</code>, <code>asynchronous_select</code></td>
</tr>
<tr>
<td><code>abstract_subprogram_declaration</code></td>
<td>3.9.3</td>
<td><code>basic_declaration</code>, <code>select_alternative</code>, <code>select_alternative</code></td>
</tr>
<tr>
<td><code>basic_declaration</code></td>
<td>3.1</td>
<td><code>select_alternative</code>, <code>select_alternative</code></td>
</tr>
<tr>
<td><code>accept_alternative</code></td>
<td>9.7.1</td>
<td><code>select_alternative</code></td>
</tr>
<tr>
<td><code>select_alternative</code></td>
<td>9.7.1</td>
<td><code>select_alternative</code></td>
</tr>
<tr>
<td><code>accept_statement</code></td>
<td>9.5.2</td>
<td><code>array_component_association</code>, <code>array_component_association_list</code>, <code>named_array_aggregate</code>, <code>qualified_expression</code></td>
</tr>
<tr>
<td><code>accept_alternative</code></td>
<td>9.7.1</td>
<td><code>array_component_association</code>, <code>array_component_association_list</code>, <code>named_array_aggregate</code>, <code>qualified_expression</code></td>
</tr>
<tr>
<td><code>compound_statement</code></td>
<td>5.1</td>
<td><code>compound_statement</code>, <code>compound_statement</code>, <code>compound_statement</code></td>
</tr>
<tr>
<td><code>access_definition</code></td>
<td>3.10</td>
<td><code>array_component_association_list</code>, <code>array_delta_aggregate</code>, <code>named_array_aggregate</code>, <code>type_definition</code>, <code>type_definition</code>, <code>type_definition</code></td>
</tr>
<tr>
<td><code>component_definition</code></td>
<td>3.6</td>
<td><code>array_component_association_list</code>, <code>array_delta_aggregate</code>, <code>named_array_aggregate</code>, <code>type_definition</code>, <code>type_definition</code>, <code>type_definition</code></td>
</tr>
<tr>
<td><code>discriminant_specification</code></td>
<td>3.7</td>
<td><code>array_component_association_list</code>, <code>array_delta_aggregate</code>, <code>named_array_aggregate</code>, <code>type_definition</code>, <code>type_definition</code>, <code>type_definition</code></td>
</tr>
<tr>
<td><code>formal_object_declaration</code></td>
<td>12.4</td>
<td><code>extension_aggregate</code>, <code>implementation_aggregate</code></td>
</tr>
<tr>
<td><code>loop_parameter_subtype_indication</code></td>
<td>5.5.2</td>
<td><code>array_delta_aggregate</code>, <code>array_type_definition</code>, <code>delta_aggregate</code></td>
</tr>
<tr>
<td><code>object_declaration</code></td>
<td>3.3.1</td>
<td><code>array_delta_aggregate</code>, <code>array_type_definition</code>, <code>delta_aggregate</code></td>
</tr>
<tr>
<td><code>object_renaming_declaration</code></td>
<td>8.5.1</td>
<td><code>array_delta_aggregate</code>, <code>array_type_definition</code>, <code>delta_aggregate</code></td>
</tr>
<tr>
<td><code>parameter_and_result_profile</code></td>
<td>6.1</td>
<td><code>array_delta_aggregate</code>, <code>array_type_definition</code>, <code>delta_aggregate</code></td>
</tr>
<tr>
<td><code>parameter_specification</code></td>
<td>6.1</td>
<td><code>array_delta_aggregate</code>, <code>array_type_definition</code>, <code>delta_aggregate</code></td>
</tr>
<tr>
<td><code>return_subtype_indication</code></td>
<td>6.5</td>
<td><code>array_delta_aggregate</code>, <code>array_type_definition</code>, <code>delta_aggregate</code></td>
</tr>
<tr>
<td><code>access_to_object_definition</code></td>
<td>3.10</td>
<td><code>component_definition</code>, <code>discriminant_specification</code>, <code>loop_parameter_subtype_indication</code></td>
</tr>
<tr>
<td><code>access_to_type_definition</code></td>
<td>3.10</td>
<td><code>component_definition</code>, <code>discriminant_specification</code>, <code>loop_parameter_subtype_indication</code></td>
</tr>
<tr>
<td><code>access_to_subprogram_definition</code></td>
<td>3.10</td>
<td><code>access_to_type_definition</code>, <code>access_to_type_definition</code>, <code>access_to_type_definition</code></td>
</tr>
<tr>
<td><code>access_type_definition</code></td>
<td>3.10</td>
<td><code>access_to_type_definition</code>, <code>access_to_type_definition</code>, <code>access_to_type_definition</code></td>
</tr>
<tr>
<td><code>access_type_definition</code></td>
<td>3.10</td>
<td><code>access_to_type_definition</code>, <code>access_to_type_definition</code>, <code>access_to_type_definition</code></td>
</tr>
<tr>
<td><code>access_type_definition</code></td>
<td>3.10</td>
<td><code>access_to_type_definition</code>, <code>access_to_type_definition</code>, <code>access_to_type_definition</code></td>
</tr>
<tr>
<td><code>access_type_definition</code></td>
<td>3.10</td>
<td><code>access_to_type_definition</code>, <code>access_to_type_definition</code>, <code>access_to_type_definition</code></td>
</tr>
<tr>
<td><code>access_type_definition</code></td>
<td>3.10</td>
<td><code>access_to_type_definition</code>, <code>access_to_type_definition</code>, <code>access_to_type_definition</code></td>
</tr>
<tr>
<td><code>access_type_definition</code></td>
<td>3.10</td>
<td><code>access_to_type_definition</code>, <code>access_to_type_definition</code>, <code>access_to_type_definition</code></td>
</tr>
<tr>
<td><code>actual_parameter_part</code></td>
<td>6.4</td>
<td><code>entry_call_statement</code>, <code>function_call</code>, <code>generalized_indexing</code>, <code>procedure_call_statement</code></td>
</tr>
<tr>
<td><code>entry_call_statement</code></td>
<td>9.5.3</td>
<td><code>expression_function_declaration</code>, <code>primary</code>, <code>primary</code></td>
</tr>
<tr>
<td><code>function_call</code></td>
<td>6.4</td>
<td><code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code></td>
</tr>
<tr>
<td><code>generalized_indexing</code></td>
<td>4.1.6</td>
<td><code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code>, <code>primary</code></td>
</tr>
</tbody>
</table>
| `procedure_call_statement` | 6.4       | `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `primary`, `prim
<table>
<thead>
<tr>
<th>Syntax Cross Reference</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>entry_index_specification</td>
<td>9.5.2</td>
</tr>
<tr>
<td>exception_declaration</td>
<td>11.1</td>
</tr>
<tr>
<td>exception_renaming_declaration</td>
<td>8.5.2</td>
</tr>
<tr>
<td>expression_function_declaration</td>
<td>6.8</td>
</tr>
<tr>
<td>extended_return_object_declaration</td>
<td>6.5</td>
</tr>
<tr>
<td>formal_abstract_subprogram_declaration</td>
<td>12.6</td>
</tr>
<tr>
<td>formal_complete_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_concrete_subprogram_declaration</td>
<td>12.6</td>
</tr>
<tr>
<td>formal_object_declaration</td>
<td>12.4</td>
</tr>
<tr>
<td>formal_package_declaration</td>
<td>12.7</td>
</tr>
<tr>
<td>full_type_declaration</td>
<td>3.2.1</td>
</tr>
<tr>
<td>generic_instantiation</td>
<td>12.3</td>
</tr>
<tr>
<td>generic_renaming_declaration</td>
<td>8.5.5</td>
</tr>
<tr>
<td>generic_subprogram_declaration</td>
<td>12.1</td>
</tr>
<tr>
<td>iteration_scheme</td>
<td>5.5</td>
</tr>
<tr>
<td>null_procedure_declaration</td>
<td>6.7</td>
</tr>
<tr>
<td>object_declaration</td>
<td>3.3.1</td>
</tr>
<tr>
<td>object_renaming_declaration</td>
<td>8.5.1</td>
</tr>
<tr>
<td>package_body</td>
<td>7.2</td>
</tr>
<tr>
<td>package_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>package_renaming_declaration</td>
<td>8.5.3</td>
</tr>
<tr>
<td>package_specification</td>
<td>7.1</td>
</tr>
<tr>
<td>parallel_block_statement</td>
<td>5.6</td>
</tr>
<tr>
<td>parameter_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>private_extension_declaration</td>
<td>7.3</td>
</tr>
<tr>
<td>private_type_declaration</td>
<td>7.3</td>
</tr>
<tr>
<td>protected_body</td>
<td>9.4</td>
</tr>
<tr>
<td>protected_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>protected_type_declaration</td>
<td>9.4</td>
</tr>
<tr>
<td>single_protected_declaration</td>
<td>9.4</td>
</tr>
<tr>
<td>single_task_declaration</td>
<td>9.1</td>
</tr>
<tr>
<td>subprogram_body</td>
<td>6.3</td>
</tr>
<tr>
<td>subprogram_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>subprogram_declaration</td>
<td>6.1</td>
</tr>
<tr>
<td>subprogram_renaming_declaration</td>
<td>8.5.4</td>
</tr>
<tr>
<td>subtype_declaration</td>
<td>3.2.2</td>
</tr>
<tr>
<td>task_body</td>
<td>9.1</td>
</tr>
<tr>
<td>task_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>task_type_declaration</td>
<td>9.1</td>
</tr>
<tr>
<td>value_sequence</td>
<td>4.5.10</td>
</tr>
<tr>
<td>assignment_statement</td>
<td>5.2</td>
</tr>
<tr>
<td>simple_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>asynchronous_select</td>
<td>9.7.4</td>
</tr>
<tr>
<td>select_statement</td>
<td>9.7</td>
</tr>
<tr>
<td>at_clause</td>
<td>1.7</td>
</tr>
<tr>
<td>aspect_clause</td>
<td>13.1</td>
</tr>
<tr>
<td>attribute_definition_clause</td>
<td>13.3</td>
</tr>
<tr>
<td>aspect_clause</td>
<td>13.1</td>
</tr>
<tr>
<td>attribute_designator</td>
<td>4.1.4</td>
</tr>
<tr>
<td>attribute_definition_clause</td>
<td>13.3</td>
</tr>
<tr>
<td>attribute_reference</td>
<td>4.1.4</td>
</tr>
<tr>
<td>local_name</td>
<td>13.1</td>
</tr>
<tr>
<td>attribute_reference</td>
<td>4.1.4</td>
</tr>
<tr>
<td>name</td>
<td>4.1</td>
</tr>
<tr>
<td>base</td>
<td>2.4.2</td>
</tr>
<tr>
<td>based_literal</td>
<td>2.4.2</td>
</tr>
<tr>
<td>based_literal</td>
<td>2.4.2</td>
</tr>
<tr>
<td>numeric_literal</td>
<td>2.4</td>
</tr>
<tr>
<td>based_numeral</td>
<td>2.4.2</td>
</tr>
<tr>
<td>based_literal</td>
<td>2.4.2</td>
</tr>
<tr>
<td>basic_declaration</td>
<td>3.1</td>
</tr>
<tr>
<td>basic_declarative_item</td>
<td>3.11</td>
</tr>
<tr>
<td>basic_declarative_item</td>
<td>3.11</td>
</tr>
<tr>
<td>declarative_item</td>
<td>3.11</td>
</tr>
<tr>
<td>package_specification</td>
<td>7.1</td>
</tr>
<tr>
<td>basic_global_mode</td>
<td>6.1.2</td>
</tr>
<tr>
<td>extended_global_mode</td>
<td>H.7</td>
</tr>
<tr>
<td>global_mode</td>
<td>6.1.2</td>
</tr>
<tr>
<td>binary_adding_operator</td>
<td>4.5</td>
</tr>
<tr>
<td>simple_expression</td>
<td>4.4</td>
</tr>
<tr>
<td>block_statement</td>
<td>5.6</td>
</tr>
<tr>
<td>compound_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>body</td>
<td>3.11</td>
</tr>
<tr>
<td>declarative_item</td>
<td>3.11</td>
</tr>
<tr>
<td>body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>body</td>
<td>3.11</td>
</tr>
<tr>
<td>case_expression</td>
<td>4.5.7</td>
</tr>
<tr>
<td>conditional_expression</td>
<td>4.5.7</td>
</tr>
<tr>
<td>case_expression_alternative</td>
<td>4.5.7</td>
</tr>
<tr>
<td>case_expression</td>
<td>4.5.7</td>
</tr>
<tr>
<td>case_statement</td>
<td>5.4</td>
</tr>
<tr>
<td>compound_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>case_statement_alternative</td>
<td>5.4</td>
</tr>
<tr>
<td>case_statement</td>
<td>5.4</td>
</tr>
<tr>
<td>character</td>
<td>2.1</td>
</tr>
<tr>
<td>comment</td>
<td>2.7</td>
</tr>
<tr>
<td>character_literal</td>
<td>2.5</td>
</tr>
<tr>
<td>defining_character_literal</td>
<td>3.5.1</td>
</tr>
<tr>
<td>name</td>
<td>4.1</td>
</tr>
<tr>
<td>selector_name</td>
<td>4.1.3</td>
</tr>
<tr>
<td>choice_expression</td>
<td>4.4</td>
</tr>
<tr>
<td>discrete_choice</td>
<td>3.8.1</td>
</tr>
<tr>
<td>membership_choice</td>
<td>4.4</td>
</tr>
<tr>
<td>choice_parameter_specification</td>
<td>11.2</td>
</tr>
<tr>
<td>exception_handler</td>
<td>11.2</td>
</tr>
<tr>
<td>choice_relation</td>
<td>4.4</td>
</tr>
<tr>
<td>choice_expression</td>
<td>4.4</td>
</tr>
<tr>
<td>chunk_specification</td>
<td>5.5</td>
</tr>
<tr>
<td>iteration_scheme</td>
<td>5.5</td>
</tr>
<tr>
<td>parallel_block_statement</td>
<td>5.6.1</td>
</tr>
<tr>
<td>value_sequence</td>
<td>4.5.10</td>
</tr>
<tr>
<td>code_statement</td>
<td>13.8</td>
</tr>
<tr>
<td>simple_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>compilation_unit</td>
<td>10.1.1</td>
</tr>
<tr>
<td>compilation</td>
<td>10.1.1</td>
</tr>
<tr>
<td>component_choice_list</td>
<td>4.3.1</td>
</tr>
<tr>
<td>record_component_association</td>
<td>4.3.1</td>
</tr>
<tr>
<td>component_clause</td>
<td>13.5.1</td>
</tr>
<tr>
<td>Syntax Cross Reference</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>record_representation_clause</td>
<td>13.5.1</td>
</tr>
<tr>
<td>component_declaration</td>
<td>3.8</td>
</tr>
<tr>
<td>component_item</td>
<td>3.8</td>
</tr>
<tr>
<td>protected_element_declaration</td>
<td>9.4</td>
</tr>
<tr>
<td>component_definition</td>
<td>3.6</td>
</tr>
<tr>
<td>component_declaration</td>
<td>3.8</td>
</tr>
<tr>
<td>constrained_array_definition</td>
<td>3.6</td>
</tr>
<tr>
<td>unconstrained_array_definition</td>
<td>3.6</td>
</tr>
<tr>
<td>component_item</td>
<td>3.8</td>
</tr>
<tr>
<td>component_list</td>
<td>3.8</td>
</tr>
<tr>
<td>variant</td>
<td>3.8.1</td>
</tr>
<tr>
<td>composite_constraint</td>
<td>3.2.2</td>
</tr>
<tr>
<td>constraint</td>
<td>3.2.2</td>
</tr>
<tr>
<td>compound_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>statement</td>
<td>5.1</td>
</tr>
<tr>
<td>condition</td>
<td>4.5.7</td>
</tr>
<tr>
<td>entry_barrier</td>
<td>9.5.2</td>
</tr>
<tr>
<td>exit_statement</td>
<td>5.7</td>
</tr>
<tr>
<td>guard</td>
<td>9.7.1</td>
</tr>
<tr>
<td>if_expression</td>
<td>4.5.7</td>
</tr>
<tr>
<td>if_statement</td>
<td>5.3</td>
</tr>
<tr>
<td>iteration_scheme</td>
<td>5.5</td>
</tr>
<tr>
<td>iterator_filter</td>
<td>5.5</td>
</tr>
<tr>
<td>conditional_entry_call</td>
<td>9.7.3</td>
</tr>
<tr>
<td>select_statement</td>
<td>9.7</td>
</tr>
<tr>
<td>conditional_expression</td>
<td>4.5.7</td>
</tr>
<tr>
<td>primary</td>
<td>4.4</td>
</tr>
<tr>
<td>constrained_array_definition</td>
<td>3.6</td>
</tr>
<tr>
<td>array_type_definition</td>
<td>3.6</td>
</tr>
<tr>
<td>constraint</td>
<td>3.2.2</td>
</tr>
<tr>
<td>subtype_indication</td>
<td>3.2.2</td>
</tr>
<tr>
<td>container_aggregate</td>
<td>4.3.5</td>
</tr>
<tr>
<td>aggregate</td>
<td>4.3</td>
</tr>
<tr>
<td>container_element_association</td>
<td>4.3.5</td>
</tr>
<tr>
<td>container_element_association_list</td>
<td>4.3.5</td>
</tr>
<tr>
<td>container_element_association_list</td>
<td>4.3.5</td>
</tr>
<tr>
<td>named_container_aggregate</td>
<td>4.3.5</td>
</tr>
<tr>
<td>context_clause</td>
<td>10.1.2</td>
</tr>
<tr>
<td>compilation_unit</td>
<td>10.1.1</td>
</tr>
<tr>
<td>context_item</td>
<td>10.1.2</td>
</tr>
<tr>
<td>context_clause</td>
<td>10.1.2</td>
</tr>
<tr>
<td>decimal_fixed_point_definition</td>
<td>3.5.9</td>
</tr>
<tr>
<td>fixed_point_definition</td>
<td>3.5.9</td>
</tr>
<tr>
<td>decimal_literal</td>
<td>2.4.1</td>
</tr>
<tr>
<td>numeric_literal</td>
<td>2.4</td>
</tr>
<tr>
<td>declarative_item</td>
<td>3.11</td>
</tr>
<tr>
<td>declarative_part</td>
<td>3.11</td>
</tr>
<tr>
<td>block_statement</td>
<td>5.6</td>
</tr>
<tr>
<td>entry_body</td>
<td>9.5.2</td>
</tr>
<tr>
<td>package_body</td>
<td>7.2</td>
</tr>
<tr>
<td>subprogram_body</td>
<td>6.3</td>
</tr>
<tr>
<td>task_body</td>
<td>9.1</td>
</tr>
<tr>
<td>declare_expression</td>
<td>4.5.9</td>
</tr>
<tr>
<td>primary</td>
<td>4.4</td>
</tr>
<tr>
<td>declare_item</td>
<td>4.5.9</td>
</tr>
<tr>
<td>declare_expression</td>
<td>4.5.9</td>
</tr>
<tr>
<td>default_expression</td>
<td>3.7</td>
</tr>
<tr>
<td>component_declaration</td>
<td>3.8</td>
</tr>
<tr>
<td>discriminant_specification</td>
<td>3.7</td>
</tr>
<tr>
<td>formal_object_declaration</td>
<td>12.4</td>
</tr>
<tr>
<td>parameter_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>default_name</td>
<td>12.6</td>
</tr>
<tr>
<td>subprogram_default</td>
<td>12.6</td>
</tr>
<tr>
<td>defining_character_literal</td>
<td>3.5.1</td>
</tr>
<tr>
<td>enumeration_literal_specification</td>
<td>3.5.1</td>
</tr>
<tr>
<td>defining_designator</td>
<td>6.1</td>
</tr>
<tr>
<td>function_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>generic_instantiation</td>
<td>12.3</td>
</tr>
<tr>
<td>subprogram_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>defining_identifier</td>
<td>3.1</td>
</tr>
<tr>
<td>choice_parameter_specification</td>
<td>11.2</td>
</tr>
<tr>
<td>chunk_specification</td>
<td>5.5</td>
</tr>
<tr>
<td>defining_identifier_list</td>
<td>3.3.1</td>
</tr>
<tr>
<td>defining_program_unit_name</td>
<td>6.1</td>
</tr>
<tr>
<td>entry_body</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_declaration</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_index_specification</td>
<td>9.5.2</td>
</tr>
<tr>
<td>enumeration_literal_specification</td>
<td>3.5.1</td>
</tr>
<tr>
<td>exception_renaming_declaration</td>
<td>8.5.2</td>
</tr>
<tr>
<td>extended_return_object_declaration</td>
<td>6.5</td>
</tr>
<tr>
<td>extended_return_statement</td>
<td>6.5</td>
</tr>
<tr>
<td>formal_complete_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_incomplete_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_package_declaration</td>
<td>12.7</td>
</tr>
<tr>
<td>formal_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>full_type_declaration</td>
<td>3.2.1</td>
</tr>
<tr>
<td>incomplete_type_declaration</td>
<td>3.10.1</td>
</tr>
<tr>
<td>iterated_component_association</td>
<td>4.3.3</td>
</tr>
<tr>
<td>iterator_parameter_specification</td>
<td>5.5.3</td>
</tr>
<tr>
<td>iterator_specification</td>
<td>5.5.2</td>
</tr>
<tr>
<td>loop_parameter_specification</td>
<td>5.5</td>
</tr>
<tr>
<td>object_renaming_declaration</td>
<td>8.5.1</td>
</tr>
<tr>
<td>package_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>private_extension_declaration</td>
<td>7.3</td>
</tr>
<tr>
<td>private_type_declaration</td>
<td>7.3</td>
</tr>
<tr>
<td>protected_body</td>
<td>9.4</td>
</tr>
<tr>
<td>protected_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>protected_type_declaration</td>
<td>9.4</td>
</tr>
<tr>
<td>single_protected_declaration</td>
<td>9.4</td>
</tr>
<tr>
<td>single_task_declaration</td>
<td>9.1</td>
</tr>
<tr>
<td>subtype_declaration</td>
<td>3.2.2</td>
</tr>
<tr>
<td>task_body</td>
<td>9.1</td>
</tr>
<tr>
<td>task_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>task_type_declaration</td>
<td>9.1</td>
</tr>
<tr>
<td>defining_identifier_list</td>
<td>3.3.1</td>
</tr>
<tr>
<td>component_declaration</td>
<td>3.8</td>
</tr>
<tr>
<td>discriminant_specification</td>
<td>3.7</td>
</tr>
<tr>
<td>Syntax</td>
<td>Cross Reference</td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>exception_declaration</td>
<td>11.1</td>
</tr>
<tr>
<td>formal_object_declaration</td>
<td>12.4</td>
</tr>
<tr>
<td>number_declaration</td>
<td>3.3.2</td>
</tr>
<tr>
<td>object_declaration</td>
<td>3.3.1</td>
</tr>
<tr>
<td>parameter_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>defining_operator_symbol</td>
<td>6.1</td>
</tr>
<tr>
<td>defining_designator</td>
<td>6.1</td>
</tr>
<tr>
<td>defining_program_unit_name</td>
<td>6.1</td>
</tr>
<tr>
<td>defining_designator</td>
<td>6.1</td>
</tr>
<tr>
<td>generic_instantiation</td>
<td>12.3</td>
</tr>
<tr>
<td>generic_renaming_declaration</td>
<td>8.5.5</td>
</tr>
<tr>
<td>package_body</td>
<td>7.2</td>
</tr>
<tr>
<td>package_renaming_declaration</td>
<td>8.5.3</td>
</tr>
<tr>
<td>package_specification</td>
<td>7.1</td>
</tr>
<tr>
<td>procedure_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>subprogram_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>delay_alternative</td>
<td>9.7.1</td>
</tr>
<tr>
<td>select_alternative</td>
<td>9.7.1</td>
</tr>
<tr>
<td>timed_entry_call</td>
<td>9.7.2</td>
</tr>
<tr>
<td>delay_relative_statement</td>
<td>9.6</td>
</tr>
<tr>
<td>delay_statement</td>
<td>9.6</td>
</tr>
<tr>
<td>delay_statement</td>
<td>9.6</td>
</tr>
<tr>
<td>delay_alternative</td>
<td>9.7.1</td>
</tr>
<tr>
<td>simple_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>triggering_statement</td>
<td>9.7.4</td>
</tr>
<tr>
<td>delay_until_statement</td>
<td>9.6</td>
</tr>
<tr>
<td>delay_statement</td>
<td>9.6</td>
</tr>
<tr>
<td>delta_aggregate</td>
<td>4.3.4</td>
</tr>
<tr>
<td>aggregate</td>
<td>4.3</td>
</tr>
<tr>
<td>delta_constraint</td>
<td>J.3</td>
</tr>
<tr>
<td>scalar_constraint</td>
<td>3.2.2</td>
</tr>
<tr>
<td>derived_type_definition</td>
<td>3.4</td>
</tr>
<tr>
<td>type_definition</td>
<td>3.2.1</td>
</tr>
<tr>
<td>designator</td>
<td>6.1</td>
</tr>
<tr>
<td>subprogram_body</td>
<td>6.3</td>
</tr>
<tr>
<td>digit 2.4.1</td>
<td>2.4.2</td>
</tr>
<tr>
<td>extended_digit</td>
<td>2.3</td>
</tr>
<tr>
<td>identifier_start</td>
<td>2.4.1</td>
</tr>
<tr>
<td>numeral</td>
<td>2.4.1</td>
</tr>
<tr>
<td>digits_constraint</td>
<td>3.5.9</td>
</tr>
<tr>
<td>scalar_constraint</td>
<td>3.2.2</td>
</tr>
<tr>
<td>direct_name</td>
<td>4.1</td>
</tr>
<tr>
<td>accept_statement</td>
<td>9.5.2</td>
</tr>
<tr>
<td>at_clause</td>
<td>J.7</td>
</tr>
<tr>
<td>local_name</td>
<td>13.1</td>
</tr>
<tr>
<td>name</td>
<td>4.1</td>
</tr>
<tr>
<td>statement_identifier</td>
<td>5.1</td>
</tr>
<tr>
<td>variant_part</td>
<td>3.8.1</td>
</tr>
<tr>
<td>discrete_choice</td>
<td>3.8.1</td>
</tr>
<tr>
<td>discrete_choice_list</td>
<td>3.8.1</td>
</tr>
<tr>
<td>discrete_choice_list</td>
<td>3.8.1</td>
</tr>
<tr>
<td>array_component_association</td>
<td>4.3.3</td>
</tr>
<tr>
<td>case_expression_alternative</td>
<td>4.5.7</td>
</tr>
<tr>
<td>case_statement_alternative</td>
<td>5.4</td>
</tr>
<tr>
<td>iterated_component_association</td>
<td>4.3.3</td>
</tr>
<tr>
<td>variant</td>
<td>3.8.1</td>
</tr>
<tr>
<td>discrete_range</td>
<td>3.6.1</td>
</tr>
<tr>
<td>discrete_choice</td>
<td>3.8.1</td>
</tr>
<tr>
<td>index_constraint</td>
<td>3.6.1</td>
</tr>
<tr>
<td>key_choice</td>
<td>4.3.5</td>
</tr>
<tr>
<td>slice</td>
<td>4.1.2</td>
</tr>
<tr>
<td>discrete_subtype_definition</td>
<td>3.6</td>
</tr>
<tr>
<td>chunk_specification</td>
<td>5.5</td>
</tr>
<tr>
<td>constrained_array_definition</td>
<td>3.6</td>
</tr>
<tr>
<td>entry_declaration</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_index_specification</td>
<td>9.5.2</td>
</tr>
<tr>
<td>loop_parameter_specification</td>
<td>5.5</td>
</tr>
<tr>
<td>discriminant_association</td>
<td>3.7.1</td>
</tr>
<tr>
<td>discriminant_constraint</td>
<td>3.7.1</td>
</tr>
<tr>
<td>discriminant_constraint</td>
<td>3.7.1</td>
</tr>
<tr>
<td>composite_constraint</td>
<td>3.2.2</td>
</tr>
<tr>
<td>discriminant_part</td>
<td>3.7</td>
</tr>
<tr>
<td>formal_complete_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_incomplete_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>incomplete_type_declaration</td>
<td>3.10.1</td>
</tr>
<tr>
<td>private_extension_declaration</td>
<td>7.3</td>
</tr>
<tr>
<td>private_type_declaration</td>
<td>7.3</td>
</tr>
<tr>
<td>dispatching_specification</td>
<td>3.7</td>
</tr>
<tr>
<td>known_discriminant_part</td>
<td>3.7</td>
</tr>
<tr>
<td>dispatching_operation_specifier</td>
<td>H.7.1</td>
</tr>
<tr>
<td>dispatching_operation_set</td>
<td>H.7.1</td>
</tr>
<tr>
<td>entry_barrier</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_body</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_body</td>
<td>9.5.2</td>
</tr>
<tr>
<td>protected_operation_item</td>
<td>9.4</td>
</tr>
<tr>
<td>entry_body_formal_part</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_body</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_call_alternative</td>
<td>9.7.2</td>
</tr>
<tr>
<td>conditional_entry_call</td>
<td>9.7.3</td>
</tr>
<tr>
<td>timed_entry_call</td>
<td>9.7.2</td>
</tr>
<tr>
<td>entry_call_statement</td>
<td>9.5.3</td>
</tr>
<tr>
<td>entry_call_alternative</td>
<td>9.7.2</td>
</tr>
<tr>
<td>procedure_or_entry_call</td>
<td>9.7.2</td>
</tr>
<tr>
<td>simple_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>triggering_statement</td>
<td>9.7.4</td>
</tr>
<tr>
<td>entry_declaration</td>
<td>9.5.2</td>
</tr>
<tr>
<td>protected_operation_declaration</td>
<td>9.4</td>
</tr>
<tr>
<td>task_item</td>
<td>9.1</td>
</tr>
<tr>
<td>entry_index</td>
<td>9.5.2</td>
</tr>
<tr>
<td>accept_statement</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_index_specification</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_body_formal_part</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_body_formal_part</td>
<td>9.5.2</td>
</tr>
<tr>
<td>enumeration_aggregate</td>
<td>13.4</td>
</tr>
<tr>
<td>enumeration_representation_clause</td>
<td>13.4</td>
</tr>
<tr>
<td>enumeration_literal_specification</td>
<td>3.5.1</td>
</tr>
<tr>
<td>enumeration_type_definition</td>
<td>3.5.1</td>
</tr>
<tr>
<td>Formal Diection</td>
<td>Clause</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>formal_decimal_fixed_point_definition</td>
<td>12.5.2</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_derived_type_definition</td>
<td>12.5.1</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_discrete_type_definition</td>
<td>12.5.2</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_floating_point_definition</td>
<td>12.5.2</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_group_designator</td>
<td>H.7.1</td>
</tr>
<tr>
<td>formal_incomplete_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_interface_type_definition</td>
<td>12.5.5</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_modular_type_definition</td>
<td>12.5.2</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_object_declaration</td>
<td>12.4</td>
</tr>
<tr>
<td>generic_formal_type_declaration</td>
<td>12.1</td>
</tr>
<tr>
<td>formal_ordinary_fixed_point_definition</td>
<td>12.5.2</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_package_actual_part</td>
<td>12.7</td>
</tr>
<tr>
<td>formal_package_declaration</td>
<td>12.7</td>
</tr>
<tr>
<td>formal_package_association</td>
<td>12.7</td>
</tr>
<tr>
<td>formal_package_actual_part</td>
<td>12.7</td>
</tr>
<tr>
<td>generic_formal_package_actual_part</td>
<td>12.1</td>
</tr>
<tr>
<td>generic_formal_type_declaration</td>
<td>12.1</td>
</tr>
<tr>
<td>formal_parameter_name</td>
<td>H.7.1</td>
</tr>
<tr>
<td>formal_parameter_set</td>
<td>H.7.1</td>
</tr>
<tr>
<td>formal_part</td>
<td>6.1</td>
</tr>
<tr>
<td>iterator_parameter_specification</td>
<td>5.5.3</td>
</tr>
<tr>
<td>parameter_and_result_profile</td>
<td>6.1</td>
</tr>
<tr>
<td>parameter_profile</td>
<td>6.1</td>
</tr>
<tr>
<td>formal_private_type_definition</td>
<td>12.5.1</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_signed_integer_type_definition</td>
<td>12.5.2</td>
</tr>
<tr>
<td>formal_type_definition</td>
<td>12.5</td>
</tr>
<tr>
<td>formal_subprogram_declaration</td>
<td>12.6</td>
</tr>
<tr>
<td>generic_formal_parameter_declaration</td>
<td>12.1</td>
</tr>
<tr>
<td>formal_type_declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>generic_formal_parameter_declaration</td>
<td>12.1</td>
</tr>
<tr>
<td>global_aspect_definition</td>
<td>6.1.2</td>
</tr>
<tr>
<td>aspect_definition</td>
<td>13.1.1</td>
</tr>
<tr>
<td>global_aspect_element</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_aspect_definition</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_designator</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_aspect_definition</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_mode</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_aspect_definition</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_name</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_designator</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_set</td>
<td>6.1.2</td>
</tr>
<tr>
<td>global_aspect_element</td>
<td>6.1.2</td>
</tr>
<tr>
<td>goto_statement</td>
<td>5.8</td>
</tr>
<tr>
<td>simple_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>graphic_character</td>
<td>2.1</td>
</tr>
<tr>
<td>character_literal</td>
<td>2.5</td>
</tr>
<tr>
<td>string_element</td>
<td>2.6</td>
</tr>
<tr>
<td>function_call</td>
<td>6.4</td>
</tr>
<tr>
<td>name</td>
<td>4.1</td>
</tr>
<tr>
<td>function_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>expression_function_declaration</td>
<td>6.8</td>
</tr>
<tr>
<td>Syntax Cross Reference</td>
<td>Page 9.7.1</td>
</tr>
<tr>
<td>Syntax Cross Reference</td>
<td>16 October 2023</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>discriminant_specification</td>
<td>3.7</td>
</tr>
<tr>
<td>formal_object_declaration</td>
<td>12.4</td>
</tr>
<tr>
<td>object_renaming_declaration</td>
<td>8.5.1</td>
</tr>
<tr>
<td>parameter_and_result_profile</td>
<td>6.1</td>
</tr>
<tr>
<td>parameter_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>subtype_indication</td>
<td>3.2.2</td>
</tr>
<tr>
<td>null_procedure_declaration</td>
<td>6.7</td>
</tr>
<tr>
<td>basic_declaration</td>
<td>3.1</td>
</tr>
<tr>
<td>protected_operation_item</td>
<td>9.4</td>
</tr>
<tr>
<td>null_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>simple_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>number_decimal</td>
<td>...</td>
</tr>
<tr>
<td>identifier_extend</td>
<td>2.3</td>
</tr>
<tr>
<td>number_declaration</td>
<td>3.3.2</td>
</tr>
<tr>
<td>basic_declaration</td>
<td>3.1</td>
</tr>
<tr>
<td>number_letter</td>
<td>...</td>
</tr>
<tr>
<td>identifier_start</td>
<td>2.3</td>
</tr>
<tr>
<td>numeral</td>
<td>2.4.1</td>
</tr>
<tr>
<td>base</td>
<td>2.4.2</td>
</tr>
<tr>
<td>decimal_literal</td>
<td>2.4.1</td>
</tr>
<tr>
<td>exponent</td>
<td>2.4.1</td>
</tr>
<tr>
<td>numeric_literal</td>
<td>2.4</td>
</tr>
<tr>
<td>primary</td>
<td>4.4</td>
</tr>
<tr>
<td>object_declaration</td>
<td>3.3.1</td>
</tr>
<tr>
<td>basic_declaration</td>
<td>3.1</td>
</tr>
<tr>
<td>declare_item</td>
<td>4.5.9</td>
</tr>
<tr>
<td>object_renaming_declaration</td>
<td>8.5.1</td>
</tr>
<tr>
<td>declare_item</td>
<td>4.5.9</td>
</tr>
<tr>
<td>renaming_declaration</td>
<td>8.5</td>
</tr>
<tr>
<td>operator_symbol</td>
<td>6.1</td>
</tr>
<tr>
<td>defining_operator_symbol</td>
<td>6.1</td>
</tr>
<tr>
<td>designator</td>
<td>6.1</td>
</tr>
<tr>
<td>direct_name</td>
<td>4.1</td>
</tr>
<tr>
<td>selector_name</td>
<td>4.1.3</td>
</tr>
<tr>
<td>ordinary_fixed_point_definition</td>
<td>3.5.9</td>
</tr>
<tr>
<td>fixed_point_definition</td>
<td>3.5.9</td>
</tr>
<tr>
<td>other_format</td>
<td>...</td>
</tr>
<tr>
<td>identifier_extend</td>
<td>2.3</td>
</tr>
<tr>
<td>overriding_indicator</td>
<td>8.3.1</td>
</tr>
<tr>
<td>abstract_subprogram_declaration</td>
<td>3.9.3</td>
</tr>
<tr>
<td>entry_declaration</td>
<td>9.5.2</td>
</tr>
<tr>
<td>expression_function_declaration</td>
<td>6.8</td>
</tr>
<tr>
<td>generic_instantiation</td>
<td>12.3</td>
</tr>
<tr>
<td>null_procedure_declaration</td>
<td>6.7</td>
</tr>
<tr>
<td>subprogram_body</td>
<td>6.3</td>
</tr>
<tr>
<td>subprogram_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>subprogram_declaration</td>
<td>6.1</td>
</tr>
<tr>
<td>subprogram_renaming_declaration</td>
<td>8.5.4</td>
</tr>
<tr>
<td>package_body</td>
<td>7.2</td>
</tr>
<tr>
<td>library_unit_body</td>
<td>10.1.1</td>
</tr>
<tr>
<td>proper_body</td>
<td>3.11</td>
</tr>
<tr>
<td>package_body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>body_stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>package_declaration</td>
<td>7.1</td>
</tr>
<tr>
<td>basic_declaration</td>
<td>3.1</td>
</tr>
<tr>
<td>library_unit_declaration</td>
<td>10.1.1</td>
</tr>
<tr>
<td>package_renaming_declaration</td>
<td>8.5.3</td>
</tr>
<tr>
<td>library_unit_renaming_declaration</td>
<td>10.1.1</td>
</tr>
<tr>
<td>renaming_declaration</td>
<td>8.5</td>
</tr>
<tr>
<td>package_specification</td>
<td>7.1</td>
</tr>
<tr>
<td>generic_package_declaration</td>
<td>12.1</td>
</tr>
<tr>
<td>package_declaration</td>
<td>7.1</td>
</tr>
<tr>
<td>parallel_block_statement</td>
<td>5.6.1</td>
</tr>
<tr>
<td>compound_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>parameter_and_result_profile</td>
<td>6.1</td>
</tr>
<tr>
<td>access_definition</td>
<td>3.10</td>
</tr>
<tr>
<td>access_to_subprogram_definition</td>
<td>3.10</td>
</tr>
<tr>
<td>function_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>subprogram_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>parameterassociation</td>
<td>6.4</td>
</tr>
<tr>
<td>actual_parameter_part</td>
<td>6.4</td>
</tr>
<tr>
<td>iterator_parameter_association</td>
<td>5.5.3</td>
</tr>
<tr>
<td>parameterassociationwithbox</td>
<td>5.5.3</td>
</tr>
<tr>
<td>iterator_parameterassociation</td>
<td>5.5.3</td>
</tr>
<tr>
<td>parameter_profile</td>
<td>6.1</td>
</tr>
<tr>
<td>accept_statement</td>
<td>9.5.2</td>
</tr>
<tr>
<td>access_definition</td>
<td>3.10</td>
</tr>
<tr>
<td>entry_body_formal_part</td>
<td>9.5.2</td>
</tr>
<tr>
<td>entry_declaration</td>
<td>9.5.2</td>
</tr>
<tr>
<td>procedure_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>subprogram_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>parameter_specification</td>
<td>6.1</td>
</tr>
<tr>
<td>formal_part</td>
<td>6.1</td>
</tr>
<tr>
<td>parent_unit_name</td>
<td>10.1.1</td>
</tr>
<tr>
<td>defining_program_unit_name</td>
<td>6.1</td>
</tr>
<tr>
<td>designator</td>
<td>6.1</td>
</tr>
<tr>
<td>package_body</td>
<td>7.2</td>
</tr>
<tr>
<td>package_specification</td>
<td>7.1</td>
</tr>
<tr>
<td>subunit</td>
<td>10.1.3</td>
</tr>
<tr>
<td>position</td>
<td>13.5.1</td>
</tr>
<tr>
<td>component_clause</td>
<td>13.5.1</td>
</tr>
<tr>
<td>positional_array_aggregate</td>
<td>4.3.3</td>
</tr>
<tr>
<td>array_aggregate</td>
<td>4.3.3</td>
</tr>
<tr>
<td>positional_container_aggregate</td>
<td>4.3.5</td>
</tr>
<tr>
<td>container_aggregate</td>
<td>4.3.5</td>
</tr>
<tr>
<td>pragma_argument_association</td>
<td>2.8</td>
</tr>
<tr>
<td>pragma</td>
<td>2.8</td>
</tr>
<tr>
<td>predicate</td>
<td>4.5.8</td>
</tr>
<tr>
<td>quantified_expression</td>
<td>4.5.8</td>
</tr>
<tr>
<td>prefix</td>
<td>4.1</td>
</tr>
<tr>
<td>attribute_reference</td>
<td>4.1.4</td>
</tr>
<tr>
<td>function_call</td>
<td>6.4</td>
</tr>
<tr>
<td>generalized_indexing</td>
<td>4.1.6</td>
</tr>
<tr>
<td>indexed_component</td>
<td>4.1.1</td>
</tr>
<tr>
<td>iterator_procedure_call</td>
<td>5.5.3</td>
</tr>
<tr>
<td>procedure_call_statement</td>
<td>6.4</td>
</tr>
<tr>
<td>expression</td>
<td>4.4</td>
</tr>
<tr>
<td>relational_operator</td>
<td>4.5</td>
</tr>
<tr>
<td>choice_relation</td>
<td>4.4</td>
</tr>
<tr>
<td>relation</td>
<td>4.4</td>
</tr>
<tr>
<td>renaming_declaration</td>
<td>8.5</td>
</tr>
<tr>
<td>basic_declaration</td>
<td>3.1</td>
</tr>
<tr>
<td>representation_clause</td>
<td>13.1</td>
</tr>
<tr>
<td>basic_declarative_item</td>
<td>3.11</td>
</tr>
<tr>
<td>component_item</td>
<td>3.8</td>
</tr>
<tr>
<td>protected_operation_declaration</td>
<td>9.4</td>
</tr>
<tr>
<td>protected_operation_item</td>
<td>9.4</td>
</tr>
<tr>
<td>task_item</td>
<td>9.1</td>
</tr>
<tr>
<td>requeue_statement</td>
<td>9.5.4</td>
</tr>
<tr>
<td>simple_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>restriction_parameter_argument</td>
<td>13.12</td>
</tr>
<tr>
<td>restriction</td>
<td>13.12</td>
</tr>
<tr>
<td>return_statement</td>
<td>6.5</td>
</tr>
<tr>
<td>simple_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>return_subtype_indication</td>
<td>6.5</td>
</tr>
<tr>
<td>extended_return_object_declaration</td>
<td>6.5</td>
</tr>
<tr>
<td>extended_return_statement</td>
<td>6.5</td>
</tr>
<tr>
<td>scalar_constraint</td>
<td>3.2.2</td>
</tr>
<tr>
<td>constraint</td>
<td>3.2.2</td>
</tr>
<tr>
<td>select_alternative</td>
<td>9.7.1</td>
</tr>
<tr>
<td>selective_accept</td>
<td>9.7.1</td>
</tr>
<tr>
<td>select_statement</td>
<td>9.7</td>
</tr>
<tr>
<td>compound_statement</td>
<td>5.1</td>
</tr>
<tr>
<td>selected_component</td>
<td>4.1.3</td>
</tr>
<tr>
<td>name</td>
<td>4.1</td>
</tr>
<tr>
<td>selective_accept</td>
<td>9.7.1</td>
</tr>
<tr>
<td>select_statement</td>
<td>9.7</td>
</tr>
<tr>
<td>selector_name</td>
<td>4.1.3</td>
</tr>
<tr>
<td>component_choice_list</td>
<td>4.3.1</td>
</tr>
<tr>
<td>discriminant_association</td>
<td>3.7.1</td>
</tr>
<tr>
<td>formal_package_association</td>
<td>12.7</td>
</tr>
<tr>
<td>generic_association</td>
<td>12.3</td>
</tr>
<tr>
<td>parameter_association</td>
<td>6.4</td>
</tr>
<tr>
<td>parameter_association_with_box</td>
<td>5.5.3</td>
</tr>
<tr>
<td>selected_component</td>
<td>4.1.3</td>
</tr>
<tr>
<td>sequence_of_statements</td>
<td>5.1</td>
</tr>
<tr>
<td>abortable_part</td>
<td>9.7.4</td>
</tr>
<tr>
<td>accept_alternative</td>
<td>9.7.1</td>
</tr>
<tr>
<td>case_statement_alternative</td>
<td>5.4</td>
</tr>
<tr>
<td>conditional_entry_call</td>
<td>9.7.3</td>
</tr>
<tr>
<td>delay_alternative</td>
<td>9.7.1</td>
</tr>
<tr>
<td>entry_call_alternative</td>
<td>9.7.2</td>
</tr>
<tr>
<td>exception_handler</td>
<td>11.2</td>
</tr>
<tr>
<td>handled_sequence_of_statements</td>
<td>11.2</td>
</tr>
<tr>
<td>if_statement</td>
<td>5.3</td>
</tr>
<tr>
<td>loop_statement</td>
<td>5.5</td>
</tr>
<tr>
<td>parallel_block_statement</td>
<td>5.6.1</td>
</tr>
<tr>
<td>selective_accept</td>
<td>9.7.1</td>
</tr>
<tr>
<td>signed_integer_type_definition</td>
<td>3.5.4</td>
</tr>
<tr>
<td>Library Unit Renaming Declaration</td>
<td>10.1.1</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Renaming Declaration</td>
<td>8.5</td>
</tr>
<tr>
<td><strong>Subprogram Specification</strong></td>
<td></td>
</tr>
<tr>
<td>Abstract Subprogram Declaration</td>
<td>3.9.3</td>
</tr>
<tr>
<td>Formal Abstract Subprogram Declaration</td>
<td>12.6</td>
</tr>
<tr>
<td>Formal Concrete Subprogram Declaration</td>
<td>12.6</td>
</tr>
<tr>
<td>Formal Subprogram Declaration</td>
<td>12.6</td>
</tr>
<tr>
<td>Generic Subprogram Declaration</td>
<td>12.1</td>
</tr>
<tr>
<td>Subprogram Body</td>
<td>6.3</td>
</tr>
<tr>
<td>Subprogram Body Stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td>Subprogram Declaration</td>
<td>6.1</td>
</tr>
<tr>
<td>Subprogram Renaming Declaration</td>
<td>8.5.4</td>
</tr>
<tr>
<td><strong>Subtype Declaration</strong></td>
<td></td>
</tr>
<tr>
<td>Basic Declaration</td>
<td>3.1</td>
</tr>
<tr>
<td>Subtype Indication</td>
<td>3.2.2</td>
</tr>
<tr>
<td>Access to Object Definition</td>
<td>3.10</td>
</tr>
<tr>
<td>Allocator</td>
<td>4.8</td>
</tr>
<tr>
<td>Component Definition</td>
<td>3.6</td>
</tr>
<tr>
<td>Derived Type Definition</td>
<td>3.4</td>
</tr>
<tr>
<td>Discrete Choice</td>
<td>3.8.1</td>
</tr>
<tr>
<td>Discrete Range</td>
<td>3.6.1</td>
</tr>
<tr>
<td>Discrete Subtype Definition</td>
<td>3.6</td>
</tr>
<tr>
<td>Iterator Specification</td>
<td>5.5.2</td>
</tr>
<tr>
<td>Loop Parameter Subtype Indication</td>
<td>5.5.2</td>
</tr>
<tr>
<td>Object Declaration</td>
<td>3.3.1</td>
</tr>
<tr>
<td>Private Extension Declaration</td>
<td>7.3</td>
</tr>
<tr>
<td>Return Subtype Indication</td>
<td>6.5</td>
</tr>
<tr>
<td>Subtype Declaration</td>
<td>3.2.2</td>
</tr>
<tr>
<td><strong>Subtype Mark</strong></td>
<td></td>
</tr>
<tr>
<td>Access Definition</td>
<td>3.10</td>
</tr>
<tr>
<td>Ancestor Part</td>
<td>4.3.2</td>
</tr>
<tr>
<td>Discriminant Specification</td>
<td>3.7</td>
</tr>
<tr>
<td>Explicit Generic Actual Parameter</td>
<td>12.3</td>
</tr>
<tr>
<td>Formal Complete Type Declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>Formal Derived Type Definition</td>
<td>12.5.1</td>
</tr>
<tr>
<td>Formal Incomplete Type Declaration</td>
<td>12.5</td>
</tr>
<tr>
<td>Formal Object Declaration</td>
<td>12.4</td>
</tr>
<tr>
<td>Formal Parameter Name</td>
<td>H.7.1</td>
</tr>
<tr>
<td>Index Subtype Definition</td>
<td>3.6</td>
</tr>
<tr>
<td>Interface List</td>
<td>3.9.4</td>
</tr>
<tr>
<td>Membership Choice</td>
<td>4.4</td>
</tr>
<tr>
<td>Object Renaming Declaration</td>
<td>8.5.1</td>
</tr>
<tr>
<td>Parameter and Result Profile</td>
<td>6.1</td>
</tr>
<tr>
<td>Parameter Specification</td>
<td>6.1</td>
</tr>
<tr>
<td>Qualified Expression</td>
<td>4.7</td>
</tr>
<tr>
<td>Relation</td>
<td>4.4</td>
</tr>
<tr>
<td>Subtype Indication</td>
<td>3.2.2</td>
</tr>
<tr>
<td>Type Conversion</td>
<td>4.6</td>
</tr>
<tr>
<td>Type Conversion</td>
<td>4.6</td>
</tr>
<tr>
<td>Use Type Clause</td>
<td>8.4</td>
</tr>
<tr>
<td><strong>Subunit</strong></td>
<td></td>
</tr>
<tr>
<td>Compilation Unit</td>
<td>10.1.3</td>
</tr>
<tr>
<td>Target Name</td>
<td>10.1.1</td>
</tr>
<tr>
<td>Name</td>
<td>5.2.1</td>
</tr>
<tr>
<td>Task Body</td>
<td>4.1</td>
</tr>
<tr>
<td>Proper Body</td>
<td>9.1</td>
</tr>
<tr>
<td>Task Body Stub</td>
<td>3.11</td>
</tr>
<tr>
<td>Body Stub</td>
<td>10.1.3</td>
</tr>
<tr>
<td><strong>Task Item</strong></td>
<td></td>
</tr>
<tr>
<td>Single Task Declaration</td>
<td>9.1</td>
</tr>
<tr>
<td>Task Type Declaration</td>
<td>9.1</td>
</tr>
<tr>
<td>Task Item</td>
<td>9.1</td>
</tr>
<tr>
<td>Task Definition</td>
<td>9.1</td>
</tr>
<tr>
<td>Task Type Declaration</td>
<td>9.1</td>
</tr>
<tr>
<td>Full Type Declaration</td>
<td>3.2.1</td>
</tr>
<tr>
<td>Term 4.4</td>
<td>4.4</td>
</tr>
<tr>
<td>Simple Expression</td>
<td>4.4</td>
</tr>
<tr>
<td>Terminate Alternative</td>
<td>9.7.1</td>
</tr>
<tr>
<td>Select Alternative</td>
<td>9.7.1</td>
</tr>
<tr>
<td>Timed Entry Call</td>
<td>9.7.2</td>
</tr>
<tr>
<td>Select Statement</td>
<td>9.7</td>
</tr>
<tr>
<td>Triggering Alternative</td>
<td>9.7.4</td>
</tr>
<tr>
<td>Asynchronous Select</td>
<td>9.7.4</td>
</tr>
<tr>
<td>Triggering Statement</td>
<td>9.7.4</td>
</tr>
<tr>
<td>Triggering Alternative</td>
<td>9.7.4</td>
</tr>
<tr>
<td>Type Conversion</td>
<td>4.6</td>
</tr>
<tr>
<td>Name</td>
<td>4.1</td>
</tr>
<tr>
<td><strong>Type Declaration</strong></td>
<td></td>
</tr>
<tr>
<td>Basic Declaration</td>
<td>3.1</td>
</tr>
<tr>
<td>Type Declaration</td>
<td>3.2.1</td>
</tr>
<tr>
<td>Full Type Declaration</td>
<td>3.2.1</td>
</tr>
<tr>
<td><strong>Unary Adding Operator</strong></td>
<td></td>
</tr>
<tr>
<td>Simple Expression</td>
<td>4.4</td>
</tr>
<tr>
<td><strong>Unconstrained Array Definition</strong></td>
<td>3.6</td>
</tr>
<tr>
<td>Array Type Definition</td>
<td>3.6</td>
</tr>
<tr>
<td><strong>Underline</strong></td>
<td></td>
</tr>
<tr>
<td>Based Numeral</td>
<td>2.4.2</td>
</tr>
<tr>
<td>Identifier</td>
<td>2.3</td>
</tr>
<tr>
<td>Numeral</td>
<td>2.4.1</td>
</tr>
<tr>
<td>Unknown Discriminant Part</td>
<td>3.7</td>
</tr>
<tr>
<td>Discriminant Part</td>
<td>3.7</td>
</tr>
<tr>
<td><strong>Use Clause</strong></td>
<td></td>
</tr>
<tr>
<td>Basic Declarative Item</td>
<td>8.4</td>
</tr>
<tr>
<td>Context Item</td>
<td>3.11</td>
</tr>
<tr>
<td><strong>Variant</strong></td>
<td></td>
</tr>
<tr>
<td>Variant Part</td>
<td>3.8.1</td>
</tr>
<tr>
<td>Variant Part</td>
<td>3.8.1</td>
</tr>
<tr>
<td>Component List</td>
<td>3.8</td>
</tr>
<tr>
<td><strong>With Clause</strong></td>
<td></td>
</tr>
<tr>
<td>Context Item</td>
<td>10.1.2</td>
</tr>
<tr>
<td><strong>Value Sequence</strong></td>
<td></td>
</tr>
<tr>
<td>Reduction Attribute Reference</td>
<td>4.5.10</td>
</tr>
<tr>
<td><strong>Variant Part</strong></td>
<td></td>
</tr>
<tr>
<td>Variant Part</td>
<td>3.8.1</td>
</tr>
<tr>
<td>Component List</td>
<td>3.8</td>
</tr>
</tbody>
</table>
Annex Q
(informative)
Language-Defined Entities

This annex lists the language-defined entities of the language. A list of language-defined library units can be found in Annex A, “Predefined Language Environment”.

Q.1 Language-Defined Packages

This subclause lists all language-defined packages.

Ada A.2(2/5)
Address_To_Access_Conversions
  child of System 13.7.2(2/5)
Arithmetic
  child of Ada.Calendar 9.6.1(8/5)
ASCII
  in Standard A.1(36.3/2)
Assertions
  child of Ada 11.4.2(12/5)
Asynchronous_Task_Control
  child of Ada D.11(3/5)
Atomic_Operations
  child of System C.6.1(3/5)
Big_Integers
  child of Ada.Numerics.Big_Numbers A.5.5(3/5), A.5.6(2/5)
Big_Reals
  child of Ada.Numerics.Big_Numbers A.5.7(2/5)
Bounded
  child of Ada.Strings.Text_Buffers A.4.12(26/5)
Bounded_Doubly_Linked_Lists
  child of Ada.Containers A.18.20(1/3)
Bounded_Hashed_Maps
  child of Ada.Containers A.18.21(1/3)
Bounded_Hashed_Sets
  child of Ada.Containers A.18.23(1/3)
Bounded_Indefinite_Holders
  child of Ada.Containers A.18.32(1/5)
Bounded_IO
  child of Ada.Text_IO A.10.11(3/5)
Bounded_Multiway_Trees
  child of Ada.Containers A.18.25(1/3)
Bounded_Ordered_Maps
  child of Ada.Containers A.18.22(1/3)
Bounded_Ordered_Sets
  child of Ada.Containers A.18.24(1/3)
Bounded_Priority_Queues
  child of Ada.Containers A.18.31(2/5)
Bounded_Synchronized_Queue
  child of Ada.Containers A.18.29(2/5)
Bounded_Vectors
  child of Ada.Containers A.18.19(1/3)
C
  child of Interfaces B.3(4/5)
Calendar
  child of Ada 9.6(10/5)
Characters
  child of Ada A.3.1(2/5)
COBOL
  child of Interfaces B.4(7/5)
Command_Line
  child of Ada A.15(3/5)
Complex_Arrays
  child of Ada.Numerics G.3.2(53/2)
Complex_Elementary_Functions
  child of Ada.Numerics G.1.2(9/1)
Complex_Text_IO
  child of Ada G.1.3(9/2)
Complex_Types
  child of Ada.Numerics G.1.1(25/1)
Complex_IO
  child of Ada.Text_IO G.1.3(3/5)
  child of Ada.Wide_Text_IO G.1.4(1)
  child of Ada.Wide_Wide_Text_IO G.1.5(1/2)
Constants
  child of Ada.Strings.Maps A.4.6(3/5)
Containers
  child of Ada A.18.1(3/5)
Conversions
  child of Ada.Characters A.3.4(2/5)
  child of Ada.Strings.UTF_Encoding A.4.11(15/5)
Decimal
  child of Ada F.2(2/5)
Decimal_Conversions
  in Interfaces.COBOL B.4(31)
Decimal_IO
  in Ada.Text_IO A.10.1(73)
Decimal_Output
  in Ada.Text_IO.Editing F.3.3(11)
Direct_IO
  child of Ada A.8.4(2/5)
Directories
  child of Ada A.16(3/5)
Discrete_Random
  child of Ada.Numerics A.5.2(17/5)
Dispatching
  child of Ada D.2.1(2/5)
Dispatching_Domains
  child of System.Multiprocessors D.16.1(3/5)
Double_Precision_Complex_Types
  in Interfaces.Fortran B.5(10.1/5)

Doubly_Linked_Lists
  child of Ada.Containers A.18.3(5/5)

Dynamic_Priorities
  child of Ada D.5.1(3/5)

EDF
  child of Ada.Dispatching D.2.6(9/5)
  child of Ada.Synchronous_Task_Control D.10(5.2/5)

Editing
  child of Ada.Text_IO F.3.3(3/5)
  child of Ada.Wide_Text_IO F.3.4(1)

Elementary_Functions
  child of Ada.Numerics A.5.1(9/1)

Enumeration_IO
  in Ada.Text_IO A.10.1(79)

Environment_Variables
  child of Ada A.17(3/5)

Exceptions
  child of Ada 11.4.1(2/5)

Exchange

Execution_Time
  child of Ada D.14(3/5)

Finalization
  child of Ada 7.6(4/5)

Fixed
  child of Ada.Strings A.4.3(5/5)
  Fixed_Conversions
    in Ada.Numerics.Big_Numbers.Big_Reals A.5.7(14/5)
  Fixed_IO
    in Ada.Text_IO A.10.1(68)

Float_Random
  child of Ada.Numerics A.5.2(5/5)

Float_Text_IO
  child of Ada A.10.9(33)
  child of Ada A.11(2/2), A.11(3/2)
  Float_Wide_Text_IO
  child of Ada A.11(3/2)
  Float_Conversions
    in Ada.Numerics.Big_Numbers.Big_Reals A.5.7(13/5)
  Float_IO
    in Ada.Text_IO A.10.1(63)

Formatting
  child of Ada.Calendar 9.6.1(15/5)

Fortran
  child of Interfaces B.5(4/5)

Generic_Complex_Arrays
  child of Ada.Numerics G.3.2(2/5)

Generic_Complex_Elementary_Functions
  child of Ada.Numerics G.1.2(2/5)

Generic_Complex_Types
  child of Ada.Numerics G.1.1(2/5)

Generic_Dispatching_Constructor
  child of Ada.Tags 3.9(18.2/5)

Generic_Elementary_Functions
  child of Ada.Numerics A.5.1(3/5)

Generic_Bounded_Length

Generic_Keys
  in Ada.Containers.Hashed_Sets A.18.8(50/5)
  in Ada.Containers.Ordered_Sets A.18.9(62/5)

Generic_Real_Arrays
  child of Ada.Numerics G.3.1(2/5)

Generic_Sorting
  in Ada.Containers.Doubly_Linked_Lists A.18.3(47/5)
  in Ada.Containers.Vectors A.18.2(75/5)

Group_Budgets
  child of Ada.Execution_Time D.14.2(3/5)

Handling
  child of Ada.Characters A.3.2(2/5)
  child of Ada.Wide_Characters A.3.5(3/5)
  child of Ada.Wide_Wide_Characters A.3.6(1/3)

Hashed_Maps
  child of Ada.Containers A.18.5(2/5)

Hashed_Sets
  child of Ada.Containers A.18.8(2/5)

Hierarchical_File_Names
  child of Ada.Directories A.16.1(3/5)
  child of Ada.Wide_Directories A.16.2(3/5)
  child of Ada.Wide_Wide_Directories A.16.2(3/5)

Indefinite_Doubly_Linked_Lists
  child of Ada.Containers A.18.12(2/3)

Indefinite_Hashed_Maps
  child of Ada.Containers A.18.13(2/3)

Indefinite_Hashed_Sets
  child of Ada.Containers A.18.15(2/3)

Indefinite_Holders
  child of Ada.Containers A.18.18(5/5)

Indefinite_Multiway_Trees
  child of Ada.Containers A.18.17(2/3)

Indefinite_Ordered_Maps

Indefinite_Ordered_Sets
  child of Ada.Containers A.18.16(2/3)

Indefinite_Vectors
  child of Ada.Containers A.18.11(2/3)

Information
  child of Ada.Directories A.16.12(4/2)
  child of Ada.Wide_Directories A.16.2(2/5)
  child of Ada.Wide_Wide_Directories A.16.2(3/5)

Integer_Text_IO
  child of Ada A.10.8(21)

Integer_Wide_Text_IO
  child of Ada A.11(2/2), A.11(3/2)

Integer_Wide_Wide_Text_IO
  child of Ada A.11(3/2)

Integer_Arithmetic

Integer_IO
  in Ada.Text_IO A.10.1(52)

Interfaces B.2(3/5)

Interrupts
  child of Ada C.3.2(2/5)
  child of Ada.Execution_Time D.14.3(3/5)

IO_Exceptions
  child of Ada A.13(3/5)

Iterator_Interfaces
  child of Ada 5.5.1(2/5)

Latin_1
  child of Ada A.3.3(3/5)

ListIterator_Interfaces
  in Ada.Containers.Doubly_Linked_Lists A.18.3(9.3/3), A.18.3(51.7/5)

Locales
  child of Ada A.19(3/5)
Machine_Code
  child of System 13.8(7)
Map_Iterator_Interfaces
  in Ada.Containers.Hashed_Maps A.18.5(6.3/5), A.18.5(37.8/5)
  in Ada.Containers.Ordered_Maps A.18.6(7.3/5), A.18.6(51.9/5)
Maps
  child of Ada.Strings A.4.2(3/5)
Modular_Arithmetic
Modular_IO
  in Ada.Text_IO A.10.1(57)
Multiprocessors
  child of System D.16(3/5)
Multiway_Trees
  child of Ada.Containers A.18.10(7/5)
Names
  child of Ada.Interrupts C.3.2(12/5)
Non_Preemptive
  child of Ada.Dispatching D.2.4(2.2/5)
Numerics
  child of Ada A.5(3/5)
Ordered_Maps
  child of Ada.Containers A.18.6(2/5)
Ordered_Sets
  child of Ada.Containers A.18.9(2/5)
Pointers
  child of Interfaces.C B.3.2(4/5)
Real_Arrays
  child of Ada.Numerics G.3.1(31/2)
Real_Time
  child of Ada D.8(3/5)
Round_Robin
  child of Ada.Dispatching D.2.5(4/5)
RPC
  child of System E.5(3/5)
Sequential_IO
  child of Ada A.8.1(2/5)
Set_Iterator_Interfaces
  in Ada.Containers.Ordered_Sets A.18.9(7.3/3), A.18.9(74.7/5)
Signed_Conversions
  in Ada.Numerics.Big_Numbers.Big_Integers A.5.6(13/5)
Single_Precision_Complex_Types
  in Interfaces.Fortran B.5(8)
Stable
  in Ada.Containers.Doubly_Linked_Lists A.18.3(51.1/5)
  in Ada.Containers.Hashed_Maps A.18.5(37.2/5)
  in Ada.Containers.Hashed_Sets A.18.8(59.1/5)
  in Ada.Containers.Multiway_Trees A.18.10(70.1/5)
  in Ada.Containers.Ordered_Maps A.18.6(51.3/5)
  in Ada.Containers.Ordered_Sets A.18.9(74.1/5)
  in Ada.Containers.Vectors A.18.2(79.1/5)
Standard
  A.1(4/5)
Storage
  child of Ada.Streams 13.13.1(12/5)
Storage_Elements
  child of System 13.7.1(2/5)
Storage_IO
  child of Ada A.9(3/5)
Storage_Pools
  child of System 13.11(5/5)
Stream_IO
  child of Ada.Streams A.12.1(3/5)
Streams
  child of Ada 13.13.1(2/5)
Strings
  child of Ada A.4.1(3/5)
  child of Ada.Strings.UTF_Encoding A.4.11(22/5)
  child of Interfaces.C B.3.1(3/5)
Subpools
  child of System.Storage_Pools 13.11.4(3/5)
Synchronized_Queue_Interfaces
  child of Ada.Containers A.18.27(3/5)
Synchronous_Bars
  child of Ada D.10.1(3/5)
Synchronous_Task_Control
  child of Ada D.10(3/5)
System
  13.7(3/5)
Tags
  child of Ada 3.9(6/5)
Task_Attributes
  child of Ada C.7.2(2/5)
Task_Identification
  child of Ada C.7.1(2/5)
Task_Termination
  child of Ada C.7.3(2/5)
Test_And_Set
  child of System.Atomic_Operations C.6.3(3/5)
Text_Streams
  child of Ada.Text_IO A.12.2(3/5)
  child of Ada.Wide_Text_IO A.12.3(3/5)
  child of Ada.Wide_Wide_Text_IO A.12.4(3/5)
Text_Buffers
  child of Ada.Strings A.4.12(3/5)
Text_IO
  child of Ada A.10.1(2/5)
Time_Zones
  child of Ada.Calendar 9.6.1(2/5)
Timers
Timing_Events
  child of Ada.Real_Time D.15(3/5)
Tree_Iterator_Interfaces
  in Ada.Containers.Multiway_Trees A.18.10(13/3), A.18.10(70.7/5)
Unbounded
  child of Ada Streams.Storage 13.13.1(18/5)
  child of Ada.Strings A.4.5(3/5)
  child of Ada.Strings.Text_Buffers A.4.12(18/5)
Unbounded_IO
  child of Ada.Text_IO A.10.12(3/5)
Unbounded_Priority_Queues
  child of Ada.Containers A.18.30(2/5)
Unbounded_Synchronized_Quanties
  child of Ada.Containers A.18.28(2/5)
Unsigned_Conversions
  in Ada.Numerics.Big_Numbers.Big_Integers A.5.6(13/5)
UTF_Encoding
  child of Ada.Strings A.4.11(3/5)
Vector_Iterator_Interfaces
  in Ada.Containers.Vectors A.18.2(11.3/5), A.18.2(79.7/5)
Vectors
  child of Ada.Containers A.18.2(6/5)
Q.1 Language-Defined Packages

Q.2 Language-Defined Types and Subtypes

This subclause lists all language-defined types and subtypes.
Byte_Array
  in Interfaces.COBOL   B.4(29/3)
C_bool
  in Interfaces.C   B.3(13.1/5)
C_float
  in Interfaces.C   B.3(15)
Cause_Of_Termination
  in Ada.Task_Termination   C.7.3(3/2)
char
  in Interfaces.C   B.3(19)
char16_array
  in Interfaces.C   B.3(23/3)
char16_t
  in Interfaces.C   B.3(39.14/3)
char32_array
  in Interfaces.C   B.3(39.11/2)
char_array
  in Interfaces.C   B.3(19)
chars_ptr
  in Interfaces.C.Strings   B.3.1(5/5)
chars_ptr_array
  in Interfaces.C.Strings   B.3.1(6/2)
Character
  in Standard   A.1(35/3)
Character_Mapping
  in Ada.Strings.Maps   A.4.2(20/5)
Character_Mapping_Function
Character_Range
  in Ada.Strings.Maps   A.4.2(6)
Character_Ranges
  in Ada.Strings.Maps   A.4.2(7)
Character_Sequence subtype of String
  in Ada.Strings.Maps   A.4.2(16)
Character_Set
  in Ada.Strings.Maps   A.4.2(4/5)
chars_ptr
  in Interfaces.C.Strings   B.3.1(5/5)
chars_ptr_array
  in Interfaces.C.Strings   B.3.1(6/2)
Chunk_Index subtype of Positive
  in Ada.Iterator_Interfaces   5.5.1(4/2)
COBOL_Character
  in Interfaces.COBOL   B.4(13)
Complex
  in Ada.Numerics.Generic_Complex_Types   G.1.1(3)
in Interfaces.Fortran   B.5(9)
Complex_Matrix
  in Ada.Numerics.Generic_Complex_Arrays   G.3.2(4/2)
Complex_Vector
  in Ada.Numerics.Generic_Complex_Arrays   G.3.2(4/2)
Constant_Reference_Type
  in Ada.Containers.Doubly_Linked_Lists   A.18.3(7/5)
in Interfaces.Fortran   B.5(11)
Controlled
  in Ada.Finalization   7.6(5/5)
Count
  in Ada.Direct_IO   A.8.4(4)
in Ada.Streams.Stream_IO   A.12.1(7)
in Ada.Text_IO   A.10.1(5)
Count_Type
  in Ada.Containers   A.18.1(5/2)
Country_Code
  in Ada.Locales   A.19(4/4)
CPU subtype of CPU_Range
  in System.Multiprocessors   D.16(4/3)
CPU_Range
  in System.Multiprocessors   D.16(4/3)
CPU_Set
CPU_Time
  in Ada.Execution_Time   D.14(4/2)
Cursor
  in Ada.Containers.Doubly_Linked_Lists   A.18.3(7/5)
in Ada.Containers.Hashed_Sets   A.18.8(4/5)
in Ada.Containers.Multiway_Trees   A.18.10(9/5)
in Ada.Containers.Ordered_Maps   A.18.6(5/5)
in Ada.Containers.Ordered_Sets   A.18.9(5/5)
in Ada.Containers.Vectors   A.18.2(9/5)
Day_Count
  in Ada.Calendar.Arithmetic   9.6.1(10/2)
Day_Duration subtype of Duration
  in Ada.Calendar   9.6(11/2)
Day_Name
  in Ada.Calendar.Formatting   9.6.1(17/2)
Day_Number subtype of Integer
  in Ada.Calendar   9.6(11/2)
Deadline subtype of Time
  in Ada.Dispatching.EDF   D.2.6(9/5)
Decimal_Element
  in Interfaces.COBOL   B.4(12/3)
Direction
  in Ada.Strings   A.4.1(6)
Directory_Entry_Type
  in Ada.Directories   A.16(29/2)
Dispatching_Domain
Display_Format
  in Interfaces.COBOL   B.4(22)
double
  in Interfaces.C   B.3(16)
Double_Complex
  in Interfaces.Fortran   B.5(10.2/5)
Double_Imaginary subtype of Imaginary
  in Interfaces.Fortran   B.5(10.3/5)
Double_Precision
  in Interfaces.Fortran   B.5(6)
Duration
  in Standard   A.1(43)
Encoding_Scheme
  in Ada.Strings.UTF_Encoding   A.4.11(4/3)
Exception_Id
  in Ada.Exceptions   11.4.1(2/5)
Exception_Occurrence
  in Ada.Exceptions 11.4.1(3/5)
Exception_Occurrence_Access
  in Ada.Exceptions 11.4.1(3/5)
Exit_Status
  in Ada.Command_Line A.15(7)
Extended_Index subtypes of Index_Type/Base
  in Ada.Containers.Vectors A.18.2(7/2)
Field subtype of Integer
  in Ada.Numerics.Big_Numbers.Big_Integers A.5.5(3/5)
in Ada.Text_IO A.10.1(6)
Field_Access
  in Ada.Text_IO A.10.1(18)
Field_Kind
  in Ada.Directories A.16(22/2)
File_Mode
  in Ada.Direct_IO A.8.4(4)
in Ada.Sequential_IO A.12.1(6)
in Ada.Text_IO A.10.1(4)
Filter_Type
  in Ada.Directories A.16(23/2)
Float
  in Ada.Directories A.16(30/2)
Floating
  in Interfaces.COBOL B.4(9)
Fortran_Character
  in Interfaces.Fortran B.5(12/3)
Fortran_Integer
  in Interfaces.Fortran B.5(5)
Forward_Iterator
  in Ada.Iterator_Interfaces 5.5.1(3/3)
Generator
in Ada.Numerics.Float_Random A.5.2(7)
Group_Budget
Group_Budget_Handler
  in Ada.Execution_Time.Group_Budgets D.14.2(5/5)
Hash_Type
  in Ada.Containers A.18.1(4/2)
Holder
  in Ada.Containers.Indefinite_Holders A.18.18(6/5)
Hour_Number subtype of Natural
  in Ada.Calendar.Formatting 9.6.1(20/2)
Imaginary
Imaginary subtype of Imaginary
  in Interfaces.Fortran B.5(10)
int
  in Interfaces.C B.3(7)
Integer
  in Standard A.1(12)
Integer_Address
  in System.Storage_Element 13.7.1(10/3)
Interrupt_Id
  in Ada.Interrupts C.3.2(2/5)
Interrupt_Priority subtype of Any_Priority
  in System 13.7(16)
ISO_646 subtype of Character
  in Ada.Characters.Handling A.3.2(9)
Language_Code
  in Ada.Locales A.19(4/4)
Leap_Seconds_Count subtype of Integer
  in Ada.Calendar.Arithmetic 9.6.1(11/2)
Length_Range subtype of Natural
Limited_Controlled
  in Ada.Execution_Time.Group_Budgets D.14.2(5/5)
List
  in Ada.Containers.Doubly_Linked_Lists A.18.3(6/5),
    A.18.3(51.2/5)
Logical
  in Interfaces.Fortran B.5(7)
long
  in Interfaces.C B.3(7)
Long_Binary
  in Interfaces.COBOL B.4(10)
long_double
  in Interfaces.C B.3(17)
Long_Floating
  in Interfaces.COBOL B.4(9)
Map
in Ada.Containers.Ordered_Maps A.18.6(4/5),
  A.18.6(51.4/5)
Membership
  in Ada.Strings A.4.1(6)
Minute_Number subtype of Natural
  in Ada.Calendar.Formatting 9.6.1(20/2)
Month_Number subtype of Integer
  in Ada.Calendar 9.6(11/2)
Name
  in System 13.7(4)
Name_Case_Kind
  in AdaDirectories A.16(20.1/3)
Natural subtype of Integer
  in Standard A.1(13)
Number_Base subtype of Integer
in Ada.Text_IO A.10.1(6)
Numeric
  in Interfaces.COBOL B.4(20/3)
Packed_Decimal
  in Interfaces.COBOL B.4(12/3)
Packed_Format
  in Interfaces.COBOL B.4(26)
Parallel_Iterator
  in Ada.Iterator_Interfaces 5.5.1(4.1/5)
Parallel_Reversible_Iterator
  in Ada.Iterator_Interfaces 5.5.1(4.8/5)
Parameterless_Handler
  in Ada.Interrupts C.3.2(2/5)
Params_Stream_Type
  in System.RPC E.5(6)
Partition_Id
  in System.RPC E.5(4)
Picture
  in Ada.Text_IO.Editing F.3.3(4)
plain_char
  in Interfaces.C B.3(11)
Set
  in Ada.Containers.Hashed_Sets A.18.8(3/5), A.18.8(59.2/5)
  in Ada.Containers.Ordered_Sets A.18.9(4/5), A.18.9(74.2/5)
short
  in Interfaces.C B.3(7)
signed_char
  in Interfaces.C B.3(8)
size_t
  in Interfaces.C B.3(13)
State
  in Ada.Numerics.Discrete_Random A.5.2(23)
  in Ada.Numerics.Float_Random A.5.2(11)
Storage_Array
  in System.Storage_Elements 13.7.1(5)
Storage_Count subtype of Storage_Offset
  in System.Storage_Elements 13.7.1(4)
Storage_Element
  in System.Storage_Elements 13.7.1(5)
Stream_Element
  in Ada.Streams.Storage 13.13.1(13/5)
Stream_Access
  in Ada.Streams.Storage_IO A.12.1(4)
  in Ada.Text_IO.Text_Stremes A.12.2(3/5)
  in Ada.Wide_Text_IO.Text_Streams A.12.3(3/5)
  in Ada.Wide_Wide_Text_IO.Text_Streams A.12.4(3/5)
Stream_Element
  in Ada.Streams 13.13.1(4/1)
Stream_Element_Array
  in Ada.Streams 13.13.1(4/1)
Stream_Element_Count subtype of Stream_Element_Offset
  in Ada.Streams 13.13.1(4/1)
Stream_Element_Offset
  in Ada.Streams 13.13.1(4/1)
Stream_Type
String
  in Standard A.1(37/3)
String_Access
  in Ada.Strings.Unbounded A.4.5(7)
Subpool_Handle
Suspension_Object
  in Ada.Synchronous_Task_Control D.10(4/5)
Synchronous_Barrier
  in Ada.Synchronous_Barriers D.10.1(5/3)
Tag
  in Ada.Tags 3.9(6/5)
Tag_Array
  in Ada.Tags 3.9(7.3/2)
Task_Array
  in Ada.Tag_Termination C.7.3(4/2)
Task_Id
  in Ada.Task_Identification C.7.1(2/5)
Termination_Handler
  in Ada.Task_Termination C.7.3(4/2)
Test_And_Set_Flag
  in System.Atomic_Operations.Test_And_Set C.6.3(4/5)
Text_Buffer_Count
  in Ada.Strings.Text_Buffers A.4.12(4/5)
Time
  in Ada.Calendar  9.6(10/5)
  in Ada.Real_Time D.8(4)
Time_Offset
  in Ada.Calendar.Time_Zones  9.6.1(4/2)
Time_Span
  in Ada.Real_Time D.8(5)
Timer
Timer_Handler
Timing_Event
Timing_Event_Handler
Tree
  in Ada.Containers.Multiway_Trees A.18.10(8/5), A.18.10(70.2/5)
Trim_End
  in Ada.Strings A.4.1(6)
Truncation
  in Ada.Strings A.4.1(6)
Type_Set
  in Ada.Text_IO A.10.1(7)
Unbounded_String
  in Ada.Strings.Unbounded A.4.5(4/5)
Uniformly_Distributedsubtype of Float
  in Ada.Numerics.Float_Random A.5.2(8/5)
unsigned
  in Interfaces.C B.3(9)
unsigned_char
  in Interfaces.C B.3(10)
unsigned_long
  in Interfaces.C B.3(9)
unsigned_short
  in Interfaces.C B.3(9)
UTF_16.Wide_String subtype of Wide_String
  in Ada.Strings.UTF_Encoding A.4.11(7/3)
UTF_8.String subtype of String
  in Ada.Strings.UTF_Encoding A.4.11(6/3)
UTF.String subtype of String
  in Ada.Strings.UTF_Encoding A.4.11(5/3)
Valid_Big_Integer subtype of Big_Integer
  in Ada.Numerics.Big_Numbers.Big_Integers A.5.6(5/5)
Valid_Big_Real subtype of Big_Real
  in Ada.Numerics.Big_Numbers.Big_Reals A.5.7(5/5)
Vector
  in Ada.Containers.Vectors A.18.2(8/5), A.18.2(79.2/5)
wchar_array
  in Interfaces.C B.3(33/3)
wchar_t
  in Interfaces.C B.3(30/1)
Wide_Character
  in Standard A.1(36.1/5)
Wide_Character_Mapping
  in Ada.Strings.Wide_Maps A.4.7(20/5)
Wide_Character_Mapping_Function
  in Ada.Strings.Wide_Maps A.4.7(26)
Wide_Character_Range
  in Ada.Strings.Wide_Maps A.4.7(6)
Wide_Character_Ranges
  in Ada.Strings.Wide_Maps A.4.7(7)
Wide_Character_Sequence subtype of Wide_String
  in Ada.Strings.Wide_Maps A.4.7(16)
Wide_Character_Set
  in Ada.Strings.Wide_Maps A.4.7(4/5)
Wide_String
  in Standard A.1(41/3)
Wide_Character
  in Standard A.1(36.2/5)
Wide_Character_Mapping
  in Ada.Strings.Wide_Wide_Maps A.4.8(20/5)
Wide_Character_Mapping_Function
  in Ada.Strings.Wide_Wide_Maps A.4.8(26/2)
Wide_Character_Range
  in Ada.Strings.Wide_Wide_Maps A.4.8(6/2)
Wide_Character_Ranges
  in Ada.Strings.Wide_Wide_Maps A.4.8(7/2)
Wide_Character_Sequence subtype of Wide_Wide_String
  in Ada.Strings.Wide_Wide_Maps A.4.8(16/2)
Wide_Character_Set
  in Ada.Strings.Wide_Wide_Maps A.4.8(4/5)
Wide_Wide_String
  in Standard A.1(42.1/3)
Year_Number subtype of Integer
  in Ada.Calendar  9.6(11/2)

Q.3 Language-Defined Subprograms

This subclause lists all language-defined subprograms.
Append
  in Ada.Containers.Doubly_Linked_Lists A.18.3(23.1/5), A.18.3(23/5)
in Ada.Containers.Vectors A.18.2(46/5), A.18.2(47.1/5), A.18.2(47/5)
Append_Child
  in Ada.Containers.Multiway_Trees A.18.10(52/5)
Append_Vector
  in Ada.Containers.Vectors A.18.2(46/5)
Arcos
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arcosinh
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arcot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccoth
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccosh
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccos
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccosech
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccoth
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccos
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccosech
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccoth
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccosinh
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccoth
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccoth
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccosinh
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccoth
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccosinh
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccoth
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccosinh
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccoth
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Arccosh
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(7)
Arccot
  in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(5)
Argmlin
  in Ada.Command_Line A.15(5)
in Ada.Numerics.Generic_Complex_Arrays G.3.2(10/2), G.3.2(31/2)
in Ada.Numerics.Generic_Complex_Types G.1.1(10)
Assert in Ada.Assertions 11.4.2(14/2)
Assign
  in Ada.Containers.Doubly_Linked_Lists A.18.3(17.5/5), A.18.3(51.8/5)
in Ada.Containers.Hashed_Maps A.18.5(17.7/5), A.18.5(37.9/5)
in Ada.Containers.Hashed_Sets A.18.8(17.4/5), A.18.8(59.8/5)
in Ada.Containers.Indefinite_Holders A.18.18(20/5)
in Ada.Containers.Multiway_Trees A.18.10(32/5), A.18.10(70.8/5)
in Ada.Containers.Ordered_Maps A.18.6(16.7/5), A.18.6(51.10/5)
in Ada.Containers.Ordered_Sets A.18.9(16.4/5), A.18.9(74.8/5)
in Ada.Containers.Vectors A.18.2(34.7/5), A.18.2(79.8/5)
Assign_Task
Atomic_Add
Atomic_Clear
  in System.Atomic_Operations.Test_And_Set C.6.3(6/5)
Atomic_Compare_And_Exchange
Atomic.Exchange
Atomic_Fetch_And_Add
Atomic_Fetch_And_Subtract
in System.Atomic_Operations.Modular_Arithmetic C.6.5(7/5)
Atomic_Subtract
Atomic_Test_And_Set
  in System.Atomic_Operations.Test_And_Set C.6.3(5/5)
Attach_Handler in Ada.Interrupts C.3.2(7)
Base_Name in Ada.Directories A.16(19/5)
Blank_When_Zero in Ada.Text_IO.Editing F.3.3(7)
Budget_Has_Expired
  in Ada.Execution_Time.Group_Budgets D.14.2(9/2)
Budget_Remaining
  in Ada.Execution_Time.Group_Budgets D.14.2(9/2)
Cancel_Handler
  in Ada.Execution_Time.Group_Budgets D.14.2(10/2)
in Ada.Real_Time.Timing_Events D.15(5/2)
Capacity
  in Ada.Containers.Hashed_Maps A.18.5(8/5)
in Ada.Containers.Hashed_Sets A.18.8(10/5)
in Ada.Containers.Vectors A.18.2(19/5)
Ceiling
  in Ada.Containers.Ordered_Maps A.18.6(41/5)
in Ada.Containers.Ordered_Sets A.18.9(51.2/5), A.18.9(71/5)
Character_Set_Version
  in Ada.Wide_Characters.Handling A.3.5(4/3)
Child_Count
  in Ada.Containers.Multiway_Trees A.18.10(46.1/5), A.18.10(46/5)
Child_Depth
  in Ada.Containers.Multiway_Trees A.18.10(47.1/5), A.18.10(47/5)
Chunk_Count
  in Ada.Iterator_Interaces 5.5.1(4/5)
Clear
  in Ada.Containers.Doubly_Linked_Lists A.18.3(13/5)
in Ada.Containers.Hashed_Maps A.18.5(12/5)
Contains
in Ada.Containers.Hashing_Ordered_Maps A.18.8(58.3/5)
in Ada.Containers.Ordered_Maps A.18.6(16.8/5)
in Ada.Containers.Bounded_Ordered_Maps A.18.22(13/5)
in Ada.Containers.Bounded_Hashed_Maps A.18.21(13/5)
in Ada.Containers.Bounded_Doubly_Linked_Lists A.18.3(17.6/5), A.18.3(51.9/5)
in Ada.Containers.Hashed_Maps A.18.5(17.8/5), A.18.5(37.10/5)
in Ada.Containers.Hashed_Sets A.18.8(17.5/5), A.18.8(59.9/5)
in Ada.Containers.Indefinite_Holders A.18.18(11/5)
in Ada.Containers.Maps A.18.6(16.8/5)
in Ada.Containers.Sets A.18.5(17.8/5)
in Ada.Containers.Vectors A.18.2(34.8/5), A.18.2(79.9/5)
Copy_Array in Interfaces.C.Pointers B.3.2(15)
Copy_File in Ada.Directories A.16(13/2)
Copy_Local_Subtree
in Ada.Containers.Multiway_Trees A.18.10(54.1/5), A.18.10(54.2/5), A.18.10(54.3/5)
Copy_Terminated_Array
in Interfaces.C.Pointers B.3.2(14)
Cos
in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(4)
Cosh
in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(6)
Cot
in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(4)
Coth
in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(6)
Count
in Ada.Strings.Fixed A.4.3(13), A.4.3(14), A.4.3(15)
in Ada.Strings.Unbounded A.4.5(43), A.4.5(44), A.4.5(45)
Country in Ada.Locales A.19(63)
Create
in Ada.Direct_IO A.8.4(6), A.8.4(18.10/5), A.8.4(18.3/5)
in Ada.Sequential_IO A.8.1(6), A.8.1(15.10/5), A.8.1(15.3/5)
in Ada.Text_IO A.10.1(9), A.10.1(85.10/5), A.10.1(85.3/5)
Current_Directory in Ada.Directories A.16(5/2)
Current_Error in Ada.Text_IO A.10.1(17), A.10.1(20)
Current_Handler
  in Ada.Execution_Time.Group_Budgets D.14.2(10/2)
  in Ada.Interrupts C.3.2(6)
in Ada.Real_Time.Timing_Events D.15(5/2)
Current_Indent
  in Ada.Strings.Text_Buffers A.4.12(14/5)
Current_Input in Ada.Text_IO A.10.1(17), A.10.1(20)
Current_Output in Ada.Text_IO A.10.1(17), A.10.1(20)
Current_State
  in Ada.Synchronous_Task_Control D.10(4/5)
Current_Task
  in Ada.Task_Identification C.7.1(3/5)
  in Ada.Task_Fallback_Handler
  in Ada.Task_Termination C.7.3(5/2)
Current_Use
  in Ada.Containers.Bounded_Priority_Queue_Header A.18.31(7/5)
in Ada.Containers.Bounded_Synchronized_Queue A.18.29(6/5)
in Ada.Containers.Synchronized_Queue B.18.27(7/5)
in Ada.Containers.Unbounded_Priority_Queue A.18.30(7/5)
in Ada.Containers.Unbounded_Synchronized_Queue A.18.28(6/5)
Day
  in Ada.Calendar 9.6(13)
  in Ada.Calendar.Formatting 9.6.1(23/2)
Day_of_Week
  in Ada.Calendar.Formatting 9.6.1(18/2)
Dealocate
  in System.Storage_Pools 13.11(8)
in System.Storage_Pools.Subpools 13.11.4(15/3)
Dealocate_Subpool
Decode
  in Ada.Strings.UTF_Encoding.Wide_Strings A.4.11(34/3), A.4.11(35/3), A.4.11(36/3)
  in Ada.Strings.UTF_Encoding.Wide_Wide_Strings A.4.11(42/3), A.4.11(43/3), A.4.11(44/3)
Decrease_Indent
  in Ada.Strings.Text_Buffers A.4.12(16/5)
Decrement in Interfaces.C.Pointers B.3.2(11/3)
Default_Modulus
  in Ada.Containers.Bounded_Hashed_Maps A.18.21(10/3)
in Ada.Containers.Bounded_Hashed_Sets A.18.23(10/3)
Default_Subpool_for_Pool
  in System.Storage_Pools.Subpools 13.11.4(13/3)
Delay_Until_And_Set_CPU
Delay_Until_And_Set_Deadline
  in Ada.Dispatching.EDF D.2.6(9/5)
Delete
  in Ada.Containers.Doubly_Linked_Lists A.18.3(24/5)
in Ada.Containers.Hashed_Maps A.18.5(25/5), A.18.5(26/5)
in Ada.Containers.Hashed_Sets A.18.8(24/5), A.18.8(25/5), A.18.8(55/5)
in Ada.Containers.Ordered_Maps A.18.6(24/5), A.18.6(25/5)
in Ada.Containers.Ordered_Sets A.18.9(23/5), A.18.9(24/5), A.18.9(68/5)
in Ada.Containers.Vectors A.18.2(50/5), A.18.2(51/5)
in Ada.Direct_IO A.8.4(8)
in Ada.Sequential_IO A.8.1(8)
in Ada.Streams.Stream_IO A.12.1(10)
in Ada.Strings.Bounded A.4.4(64), A.4.4(65)
in Ada.Strings.Fixed A.4.3(29), A.4.3(30)
in Ada.Strings.Unbounded A.4.5(59), A.4.5(60)
in Ada.Text_IO A.10.1(11)
Delete_Children
  in Ada.Containers.Multiway_Trees A.18.10(53/5)
Delete_Directory in Ada.Directories A.16(8/2)
Delete_File in Ada.Directories A.16(11/2)
Delete_First
  in Ada.Containers.Doubly_Linked_Lists A.18.3(25/5)
in Ada.Containers.Ordered_Maps A.18.6(26/5)
in Ada.Containers.Ordered_Sets A.18.9(25/5)
in Ada.Containers.Vectors A.18.2(52/5)
Delete_Last
  in Ada.Containers.Doubly_Linked_Lists A.18.3(26/5)
in Ada.Containers.Ordered_Maps A.18.6(27/5)
in Ada.Containers.Ordered_Sets A.18.9(26/5)
in Ada.Containers.Vectors A.18.2(53/5)
Delete_Leaf
  in Ada.Containers.Multiway_Trees A.18.10(35/5)
Delete_Subtree
  in Ada.Containers.Multiway_Trees A.18.10(36/5)
Delete_Tree in Ada.Directories A.16(10/2)
Denominator
  in Ada.Numerics.Big_Numbers.Big_Reals A.5.7(8/5)
Depth
  in Ada.Containers.Multiway_Trees A.18.10(19.1/5), A.18.10(19/5)
Dequeue
in Ada.Containers.Bounded_Synchronized_Queue A.18.29(5/3)
in Ada.Containers.Synchronized_Queue B.18.27(6/5)
in Ada.Containers.Unbounded_Priority_Queue B.18.30(5/3)
in Ada.Containers.Unbounded_Synchronized_Queue A.18.28(5/3)
Dequeue_Every_High_Priority
Dequeue_Every_Low_Priority
  in Interfaces.C.Strings B.3.1(12)
Descendant_Tag in Ada.Tags 3.9(7.1/2)
Detach_Handler in Ada.Interrupts C.3.2(9)
Dereference_Error
  in Interfaces.C.Pointers C.3.2(11/3)
Default_Modulus
  in Ada.Containers.Bounded_Hashed_Maps A.18.21(10/3)
in Ada.Containers.Bounded_Hashed_Sets A.18.23(10/3)
Default_Subpool_for_Pool
  in System.Storage_Pools.Subpools 13.11.4(13/3)
Delay_Until_And_Set_CPU
Delay_Until_And_Set_Deadline
  in Ada.Dispatching.EDF D.2.6(9/5)

Q.3
Do_RPC in System.RPC  E.5(10)
Do_RPC in System.RPC  E.5(9)

Eigenvalues
  in Ada.Numerics.Generic_Complex_Arrays  G.3.2(49/2)
in Ada.Numerics.Generic_Real_Arrays  G.3.1(27/2)

Eigenvalues
  in Ada.Numerics.Generic_Complex_Arrays  G.3.2(48/2)
in Ada.Numerics.Generic_Real_Arrays  G.3.1(26/2)

Element_Count
  in Ada.Containers.Doubly_Linked_Lists  A.18.3(14.1/5),
A.18.3(14/5)
A.18.5(14/5), A.18.5(31/2)
in Ada.Containers.Hashed_Sets  A.18.8(15.1/5),
A.18.8(15/5), A.18.8(52/2)
in Ada.Containers.Infinite_Holders  A.18.18(12/5)
in Ada.Containers.Multiway_Trees  A.18.10(24/1/5),
A.18.10(24/5)
in Ada.Containers.Ordered_Maps  A.18.6(13.1/5),
A.18.6(13/5), A.18.6(39/2)
in Ada.Containers.Ordered_Sets  A.18.9(14.1/5),
A.18.9(14/5), A.18.9(65/2)
A.18.2(28/5)
in Ada.Strings.Unbounded  A.4.5(20)

Environment_Task
  in Ada.Task_Identification  C.7.1(3/5)

Equal_Cancel
  in Ada.Task_Identification  C.7.1(3/5)

Equal_Element
  in Ada.Containers.Infinite_Holders  A.18.18(7.1/5)
in Ada.Containers.Multiway_Trees  A.18.10(11.1/5)

Equal_Subtree
  in Ada.Containers.Multiway_Trees  A.18.10(14/3)

Equivalent_Elements
  in Ada.Containers.Hashed_Sets  A.18.8(46/5), A.18.8(47/5),
A.18.8(48/5)
in Ada.Containers.Ordered_Sets  A.18.9(3/2)

Equivalent_Keys
  in Ada.Containers.Hashed_Sets  A.18.5(34/5), A.18.5(35/5),
A.18.5(36/5)
in Ada.Containers.Ordered_Maps  A.18.6(3/5)
in Ada.Containers.Ordered_Sets  A.18.9(63/2)

Equivalent_Sets
  in Ada.Containers.Hashed_Sets  A.18.8(9/2)
in Ada.Containers.Ordered_Sets  A.18.9(9/2)

Establish_RPC_Receiver in System.RPC  E.5(12)

Exception_Identity in Ada.Exceptions  11.4.1(5/2)

Exception_Information
  in Ada.Exceptions  11.4.1(5/2)

Exception_Message in Ada.Exceptions  11.4.1(4/3)

Exception_Name in Ada.Exceptions  11.4.1(2/5), 11.4.1(5/2)

Exchange_Handler in Ada.Interrupts  C.3.2(8)

Exclude
  in Ada.Containers.Hashed_Maps  A.18.5(24/5)
in Ada.Containers.Hashed_Sets  A.18.8(23/5), A.18.8(54/5)
in Ada.Containers.Ordered_Maps  A.18.6(23/5)
in Ada.Containers.Ordered_Sets  A.18.9(22/5), A.18.9(67/5)

Exists
  in Ada.Directories  A.16(24/2)
in Ada.Environment_Variables  A.17(5/2)

Exp
  in Ada.Numerics.Generic_Complex_Elementary_Functions  G.1.2(3)

Expanded_Name in Ada.Tags  3.9(7/2)

Extension in Ada.Directories  A.16(18/5)

External_Tag in Ada.Tags  3.9(7/2)

Finalize in Ada.Finalization  7.6(6/2), 7.6(8/2)

Find
  in Ada.Containers.Doubly_Linked_Lists  A.18.3(41/5)
in Ada.Containers.Hashed_Maps  A.18.5(30/5)
in Ada.Containers.Hashed_Sets  A.18.8(43/5), A.18.8(56/5)
in Ada.Containers.Multiway_Trees  A.18.10(38/5)
in Ada.Containers.Ordered_Maps  A.18.6(38/5)
in Ada.Containers.Ordered_Sets  A.18.9(49/5), A.18.9(69/5)
in Ada.Containers.Vectors  A.18.2(68/5)

Find_In_Subtree
  in Ada.Containers.Multiway_Trees  A.18.10(39.1/5),
A.18.10(39/5)

Find_Index in Ada.Containers.Vectors  A.18.2(67/2)

in Ada.Strings.Fixed  A.4.3(15.1/3), A.4.3(16)
First
  in Ada.Containers.Doubly_Linked_Lists A.18.3(33/5)
in Ada.Containers.HashMap A.18.4(27/5)
in Ada.Containers.HashMap_Access A.18.9(40/5)
in Ada.Containers.HashMap_Access_Sets A.18.9(41/5)
in Ada.Containers.HashMap_Access_Vectors A.18.2(58/5)
in Ada.Iterator_Interfaces 5.5.1(3/3), 5.5.1(4.6/5)
First_Child
  in Ada.Containers.Multiway_Trees A.18.10(60.1/5), A.18.10(60.5)
First_Child_Element
  in Ada.Containers.Multiway_Trees A.18.10(61.1/5), A.18.10(61.5)
First_Element
  in Ada.Containers.Doubly_Linked_Lists A.18.3(34/5)
in Ada.Containers.Ordered_Maps A.18.6(29/5)
in Ada.Containers.Ordered_Sets A.18.9(42/5)
in Ada.Containers.Vectors A.18.2(57/5)
First_Index
  in Ada.Containers.Vectors A.18.2(57/5)
Floor
  in Ada.Containers.Ordered_Maps A.18.6(30/5)
in Ada.Containers.Ordered_Sets A.18.6(40/5)
in Ada.Containers.Ordered_Sets A.18.9(50/2), A.18.9(70/5)
Flush
  in Ada.Direct_IO A.8.4(10.1/5)
in Ada.Sequential_IO A.8.1(10.1/5)
in Ada.Text_IO A.10.1(21/5)
Form
  in Ada.Direct_IO A.8.4(9), A.8.4(18.13/5), A.8.4(18.6/5)
in Ada.Sequential_IO A.8.1(9), A.8.1(15.13/5), A.8.1(15.6/5)
in Ada.Text_IO A.10.1(12), A.10.1(85.13/5), A.10.1(85.6/5)
Free
  in Ada.Strings.Unbounded A.4.5(7)
in Interfaces.C.Strings B.3.1(11)
From_BigInteger
  in Ada.Numerics.Bignum A.5.6(12/5), A.5.6(13/5)
From_BigReal
  in Ada.Numerics.Bignum A.5.7(13/5)
From_Choice
  in Ada.Numerics.Bignum A.5.7(14/5)
From_Polynomial
  in Ada.Numerics.Bignum A.5.7(15/5)
From_Rational
  in Ada.Numerics.Bignum A.5.7(16/5)
From_Real
  in Ada.Numerics.Bignum A.5.7(17/5), A.5.7(18/5)
Full_Name
  in Ada.Directories A.16(15/5), A.16(39/2)
Generic_Array_Sort
  child of Ada.Containers A.18.26(3/5)
Generic_Constrained_Array_Sort
  child of Ada.Containers A.18.26(7/5)
Generic_Sort
  child of Ada.Containers A.18.26(9.2/5)
Q.3 Language-Defined Subprograms
Language-Defined Subprograms 16 October 2023
Sort
in Ada.Containers.Doubly_Linked_Lists A.18.3(49/5)
in Ada.Containers.Vectors A.18.2(77/5)
Specific_Handler
in Ada.Task_Termination C.7.3(6/2)
Splice
in Ada.Containers.Doubly_Linked_Lists A.18.3(30/5), A.18.3(31/5), A.18.3(32/2)
Splice_Children
in Ada.Containers.Multiway_Trees A.18.10(57/5), A.18.10(58/5)
Splice_Subtree
in Ada.Containers.Multiway_Trees A.18.10(55/5), A.18.10(56/5)
Split
in Ada.Calendar 9.6(14)
in Ada.Execution_Time D.14(8/2)
in Ada.Real_Time D.8(16)
Split_Into_Chunks
in Ada.Iterator_Interfaces 5.5.1(4/5)
Sqrt
in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(3)
Standard_Error
in Ada.Text_IO A.10.1(16), A.10.1(19)
Standard_Output
in Ada.Text_IO A.10.1(16), A.10.1(19)
Standard_Output
in Ada.Text_IO A.10.1(16), A.10.1(19)
Start_Search
in Ada.Directories A.16(32/2)
Storage_Size
in System.Storage_Pools 13.11(9)
in System.Storage_Pools.Subpools 13.11.4(16/3)
Stream
in Ada.Streams.Stream_IO A.12.1(13)
in Ada.Text_IO.Text_Streams A.12.2(4)
in Ada.Wide_Text_IO.Text_Streams A.12.3(4)
in Ada.Wide_Text_IO.Text_Streams A.12.4(4/2)
Strlen
in Interfaces.C.Strings B.3.1(17)
Sub_Second
in Ada.Calendar.Formatting 9.6.1(27/2)
Subtree_Node_Count
in Ada.Containers.Multiway_Trees A.18.10(18/1/5), A.18.10(18/5)
Supported
in Ada.Execution_TimeInterrupts D.14.3(3/5)
Suspend_Until_True
in Ada.Synchronous_Task_Control.D.10(4/5)
Suspend_Until_True_And_Set_Deadline
in Ada.Synchronous_Task_Control.EDF D.10(5/2/5)
Swap
in Ada.Containers.Doubly_Linked_Lists A.18.3(28/5)
in Ada.Containers.Indefinite_Holders A.18.18(22.1/5)
in Ada.Containers.Multiway_Trees A.18.10(37/5)
in Ada.Containers.Vectors A.18.2(77/5)
Swap_Links
in Ada.Containers.Doubly_Linked_Lists A.18.3(29/5)
Symmetric_Difference
in Ada.Containers.Hashed_Sets A.18.8(35/5), A.18.8(36/5)
in Ada.Containers.Ordered_Sets A.18.9(36/5), A.18.9(37/5)
Tail
in Ada.Strings.Fixed A.4.3(37), A.4.3(38)
in Ada.Strings.Unbounded A.4.5(67), A.4.5(68)
Tampering_With.Cursors_Prohibited
in Ada.Containers.Doubly_Linked_Lists A.18.3(10.1/5)
in Ada.Containers.Hashed_Sets A.18.5(7.1/5)
in Ada.Containers.Hashed_Sets A.18.8(8.1/5)
in Ada.Containers.Multiway_Trees A.18.10(15.1/5)
in Ada.Containers.Ordered_Maps A.18.6(8.1/5)
in Ada.Containers.Ordered_Sets A.18.9(9.1/5)
in Ada.Containers.Vectors A.18.2(12.1/5)
Tampering_With.Elements_Prohibited
in Ada.Containers.Doubly_Linked_Lists A.18.3(10.2/5)
in Ada.Containers.Hashed_Sets A.18.5(7.2/5)
in Ada.Containers.Multiway_Trees A.18.10(15.2/5)
in Ada.Containers.Ordered_Maps A.18.6(8.2/5)
in Ada.Containers.Vectors A.18.2(12.2/5)
Tampering_With.The_Element_Prohibited
in Ada.Containers.Indefinite_Holders A.18.18(8.1/5)
Tan
in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(4)
Tanpi
in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(6)
Text_Truncated
Time_Of
in Ada.Calendar 9.6(15)
in Ada.Calendar.Formatting 9.6.1(30/2), 9.6.1(31/2)
in Ada.Execution_Time D.14(9/2)
in Ada.Real_Time D.8(16)
Time_Of_Event
in Ada.Real_Time.Timing_Events D.15(6/2)
Time_Remaining
To_Ada
in Interfaces.C.39.4/2), B.3(39.7/2), B.3(39.9/2)
in Interfaces.C.39), B.3(39.13/2), B.3(39.17/2), B.3(39.19/2), B.3(39.4/2), B.3(39.8/2)
in Interfaces.COBOL B.4(17), B.4(19)
in Interfaces.Fortran B.5(13), B.5(14), B.5(16)
To_Address
in System.Address_To_Access_Conversions 13.7.2(3/3)
in System.Storage_Elements 13.7.1(10/3)
To_Basic
in Ada.Characters.Handling A.3.2(6), A.3.2(7)
To_Big_Integer
in Ada.Numerics.Big_Numbers.Big_Integers A.5.6(7/5), A.5.6(12/5), A.5.6(13/5)
To_Big_Real
in Ada.Numerics.Big_Numbers.Big_Rals A.5.7(9/5), A.5.7(13/5), A.5.7(14/5)
To_Binary
in Interfaces.COBOL B.4(45), B.4(48)
To_Bounded_String
To_C
in Interfaces.C B.3(21), B.3(25), B.3(27), B.3(32), B.3(36), B.3(38), B.3(39.13/2), B.3(39.16/2), B.3(39.18/2), B.3(39.4/2), B.3(39.7/2), B.3(39.9/2)
To_Character
in Ada.Characters.Conversions A.3.4(5/2)
in Ada.Characters.Handling A.3.2(15/2)
To_CHARS_Ptr
in Interfaces.C.Strings B.3.1(8)
Q.3 Language-Defined Subprograms
Q.4 Language-Defined Exceptions

{AI95-00440-01} {AI05-0299-1} This subclause lists all language-defined exceptions.

Argument_Error
in Ada.Numerics A.5(3/5)

Assertion_Error
in Ada.Assertions 11.4.2(13/2)

Capacity_Error
in Ada.Containers A.18.1(5.1/3)

Communication_Error
in System.RPC E.5(5)

Constraint_Error
in Standard A.1(46)

Conversion_Error
in Interfaces.COBOL B.4(30)

Data_Error
in Ada.Direct_IO A.8.4(18)

End_Error
in Ada.Streams.Stream_IO A.12.1(26)

Value
in Ada.Calendar.Formatting 9.6.1(36/2), 9.6.1(38/2)

in Ada.Environment_Variables A.17(4.1/3), A.17(4/2)


in Ada.Numerics.Float_Random A.5.2(14)

in Ada.Strings.Maps A.4.2(21)

in Ada.Strings.Wide_Maps A.4.7(21)

in Ada.Strings.Wide_Wide_Maps A.4.8(21/2)

in Ada.Task_Attributes C.7.2(4)

in Interfaces.C.Pointers B.3.2(6), B.3.2(7)

in Interfaces.C.Strings B.3.1(13), B.3.1(14), B.3.1(15), B.3.1(16)

Virtual_Length
in Interfaces.C.Pointers B.3.2(13)

Wait_For_Release
in Ada.Demanding_Barriers D.10.1(6/5)

Write
in Ada.Direct_IO A.8.4(13/5)

in Ada.Sequential_IO A.8.1(12/5)

in Ada.Storage_IO A.9(7)

in Ada.Streams Stream_IO A.12.1(18/5), A.12.1(19/5)

in System.RPC E.5(8)

Year
in Ada.Calendar 9.6(13)

in Ada.Calendar.Formatting 9.6.1(21/2)

Yield
in Ada.Dispatching D.2.1(1.3/5)

Yield_To_Higher
in Ada.Dispatching.Non_Preemptive D.2.4(2.2/5)

Yield_To_Same_Or_Higher
in Ada.Dispatching.Non_Preemptive D.2.4(2.2/5)
Q.4 Language-Defined Exceptions

Q.5 Language-Defined Objects

Q.5 Language-Defined Objects

This subclause lists all language-defined constants, variables, named numbers, and enumeration literals.

To be honest: Formally, named numbers and enumeration literals aren’t objects, but it was thought to be too weird to say “Language-Defined Objects and Values”.

ACK in Ada.Characters.Latin_1 A.3.3(5)
Acute in Ada.Characters.Latin_1 A.3.3(22)
Ada_TO_COBOL in Interfaces.COBOL B.4(14)
Alphanumeric_Set
    in Ada.Strings.Maps.Constants A.4.6(4)
Ampersand in Ada.Characters.Latin_1 A.3.3(8)
APC in Ada.Characters.Latin_1 A.3.3(19)
Apostrophe in Ada.Characters.Latin_1 A.3.3(8)
Asterisk in Ada.Characters.Latin_1 A.3.3(8)
Basic_Map
    in Ada.Strings.Maps.Constants A.4.6(5)
Basic_Set
    in Ada.Strings.Maps.Constants A.4.6(4)
BEL in Ada.Characters.Latin_1 A.3.3(5)
BOM_16 in Ada.Strings.UTF_Encoding A.4.11(12/3)
BOM_16BE in Ada.Strings.UTF_Encoding A.4.11(10/3)
BOM_16LE in Ada.Strings.UTF_Encoding A.4.11(11/3)
BOM_8 in Ada.Strings.UTF_Encoding A.4.11(9/3)
BPH in Ada.Characters.Latin_1 A.3.3(17)
Broken_Bar in Ada.Characters.Latin_1 A.3.3(21/3)
BS in Ada.Characters.Latin_1 A.3.3(5)
Buffer_Size in Ada.Storage_IO A.9(4)
CAN in Ada.Characters.Latin_1 A.3.3(6)
CCH in Ada.Characters.Latin_1 A.3.3(18)
Cedilla in Ada.Characters.Latin_1 A.3.3(22)
Cent_Sign in Ada.Characters.Latin_1 A.3.3(21/3)
char16_nul in Interfaces.C.B.3(39/3)
char32_nul in Interfaces.C.B.3(39/12/3)
CHAR_BIT in Interfaces.C.B.3(6)
Character_Set
    in Ada.Strings.Wide_Maps A.4.7(46/2)
    in Ada.Strings.Wide_Maps.Wide_Constants A.4.8(48/2)
Circumflex in Ada.Characters.Latin_1 A.3.3(12)
COBOL_TO_Ada in Interfaces.COBOL B.4(15)
Colon in Ada.Characters.Latin_1 A.3.3(10)
Comma in Ada.Characters.Latin_1 A.3.3(8)
Commercial_At
    in Ada.Characters.Latin_1 A.3.3(10)
Control_Set
    in Ada.Strings.Maps.Constants A.4.6(4)
ISO_646_Set
  in Ada.Strings.Maps.Constants A.4.6(4)
j
  in Ada.Numerics.Generic_Complex_Types G.1.1(5)
in Interfaces.Fortran B.5(10)
Language_Unknown in Ada.Locales A.19(5/3)
LC_A in Ada.Characters.Latin_1 A.3.3(13)
LC_A_Acute in Ada.Characters.Latin_1 A.3.3(25)
LC_A_Circumflex in Ada.Characters.Latin_1 A.3.3(25)
LC_A_Diaeresis in Ada.Characters.Latin_1 A.3.3(25)
LC_A_Diagonal_Stroke in Ada.Characters.Latin_1 A.3.3(26)
LC_A_Grave in Ada.Characters.Latin_1 A.3.3(26)
LC_A_Hook in Ada.Characters.Latin_1 A.3.3(26)
LC_A_I overbar in Ada.Characters.Latin_1 A.3.3(26)
LC_A_O overline in Ada.Characters.Latin_1 A.3.3(26)
LC_A_Circling in Ada.Characters.Latin_1 A.3.3(26)
LC_A double overbar in Ada.Characters.Latin_1 A.3.3(26)
LC_A_Angle in Ada.Characters.Latin_1 A.3.3(26)
LC_A_Double_Angle in Ada.Characters.Latin_1 A.3.3(26)
LC_B in Ada.Characters.Latin_1 A.3.3(13)
LC_C in Ada.Characters.Latin_1 A.3.3(13)
LC_C_Cedilla in Ada.Characters.Latin_1 A.3.3(25)
LC_D in Ada.Characters.Latin_1 A.3.3(25)
LC_E in Ada.Characters.Latin_1 A.3.3(25)
LC_E_Acute in Ada.Characters.Latin_1 A.3.3(25)
LC_E_Circumflex in Ada.Characters.Latin_1 A.3.3(25)
LC_E_Diaeresis in Ada.Characters.Latin_1 A.3.3(25)
LC_E_GRAVE in Ada.Characters.Latin_1 A.3.3(25)
LC_E_MARK in Ada.Characters.Latin_1 A.3.3(25)
LC_F in Ada.Characters.Latin_1 A.3.3(25)
LC_G in Ada.Characters.Latin_1 A.3.3(13)
LC_H in Ada.Characters.Latin_1 A.3.3(24)
LC_I in Ada.Characters.Latin_1 A.3.3(13)
LC_I_Acute in Ada.Characters.Latin_1 A.3.3(25)
LC_I_Circumflex in Ada.Characters.Latin_1 A.3.3(25)
LC_I_Diaeresis in Ada.Characters.Latin_1 A.3.3(25)
LC_ISO_A_2202 in Ada.Characters.Latin_1 A.3.3(25)
LC_ISO_A_2100 in Ada.Characters.Latin_1 A.3.3(25)
LC_K in Ada.Characters.Latin_1 A.3.3(13)
LC_L in Ada.Characters.Latin_1 A.3.3(13)
LC_L_Acute in Ada.Characters.Latin_1 A.3.3(26)
LC_L_Circumflex in Ada.Characters.Latin_1 A.3.3(26)
LC_L_Diaeresis in Ada.Characters.Latin_1 A.3.3(26)
LC_L_MARK in Ada.Characters.Latin_1 A.3.3(25)
LC_M in Ada.Characters.Latin_1 A.3.3(13)
LC_N in Ada.Characters.Latin_1 A.3.3(13)
LC_N_Acute in Ada.Characters.Latin_1 A.3.3(26)
LC_N_Circumflex in Ada.Characters.Latin_1 A.3.3(26)
LC_N_Diaeresis in Ada.Characters.Latin_1 A.3.3(26)
LC_N_Tilde in Ada.Characters.Latin_1 A.3.3(26)
LC_O in Ada.Characters.Latin_1 A.3.3(14)
LC_O_Acute in Ada.Characters.Latin_1 A.3.3(26)
LC_O_Circumflex in Ada.Characters.Latin_1 A.3.3(26)
LC_O_Diaeresis in Ada.Characters.Latin_1 A.3.3(26)
LC_O_GRAVE in Ada.Characters.Latin_1 A.3.3(26)
LC_O_MARK in Ada.Characters.Latin_1 A.3.3(26)
LC_O_O overline in Ada.Characters.Latin_1 A.3.3(26)
LC_O_Underline in Ada.Characters.Latin_1 A.3.3(26)
LC_O_VAbove in Ada.Characters.Latin_1 A.3.3(26)
LC_O_VBelow in Ada.Characters.Latin_1 A.3.3(26)
LC_O_Wedge in Ada.Characters.Latin_1 A.3.3(26)
LC_O_XOverbar in Ada.Characters.Latin_1 A.3.3(26)
LC_O_double_underline in Ada.Characters.Latin_1 A.3.3(26)
LC_P in Ada.Characters.Latin_1 A.3.3(14)
LC_Q in Ada.Characters.Latin_1 A.3.3(14)
LC_R in Ada.Characters.Latin_1 A.3.3(14)
Success in Ada.Command_Line A.15(8)
Sunday in Ada.Calendar.Formatting 9.6.1(17/2)
Superscript One
  in Ada.Characters.Latin_1 A.3.3(22)
Superscript Three
  in Ada.Characters.Latin_1 A.3.3(22)
Superscript Two
  in Ada.Characters.Latin_1 A.3.3(22)
SYN in Ada.Characters.Latin_1 A.3.3(6)
System_Dispatching_Domain
System_Name in System 13.7(4)
Thursday in Ada.Calendar.Formatting 9.6.1(17/2)
Tick
  in Ada.Real_Time D.8(6)
  in System 13.7(10)
Tilde in Ada.Characters.Latin_1 A.3.3(14)
Time_First in Ada.Real_Time D.8(4)
Time_Last in Ada.Real_Time D.8(4)
Time_Span_First in Ada.Real_Time D.8(5)
Time_Span_Last in Ada.Real_Time D.8(5)
Time_Span_Unit in Ada.Real_Time D.8(5)
Time_Span_Zero in Ada.Real_Time D.8(5)
Time_Unit in Ada.Real_Time D.8(4)
Trailing_Nonseparate
  in Interfaces.COBOL B.4(23)
Trailing_Separate in Interfaces.COBOL B.4(23)
Tuesday in Ada.Calendar.Formatting 9.6.1(17/2)
UC_A_Acute in Ada.Characters.Latin_1 A.3.3(23)
UC_A_Circumflex
  in Ada.Characters.Latin_1 A.3.3(23)
UC_A_Diaeresis
  in Ada.Characters.Latin_1 A.3.3(23)
UC_A_Grave
  in Ada.Characters.Latin_1 A.3.3(23)
UC_A_Icelandic_Eth
  in Ada.Characters.Latin_1 A.3.3(23)
UC_A_Icelandic_Thorn
  in Ada.Characters.Latin_1 A.3.3(23)
UC_A_Oblique_Stroke
  in Ada.Characters.Latin_1 A.3.3(23)
UC_A_Tilde
  in Ada.Characters.Latin_1 A.3.3(23)
UC_AE_Diphthong
  in Ada.Characters.Latin_1 A.3.3(23)
UC_C_Cedilla
  in Ada.Characters.Latin_1 A.3.3(23)
UC_E_Acute in Ada.Characters.Latin_1 A.3.3(23)
UC_E_Circumflex
  in Ada.Characters.Latin_1 A.3.3(23)
UC_E_Diaeresis
  in Ada.Characters.Latin_1 A.3.3(23)
UC_E_Grave
  in Ada.Characters.Latin_1 A.3.3(23)
UC_E_Oblique_Stroke
  in Ada.Characters.Latin_1 A.3.3(23)
UC_E_Tilde
  in Ada.Characters.Latin_1 A.3.3(23)
UC_I_Acute
  in Ada.Characters.Latin_1 A.3.3(23)
UC_I_Circumflex
  in Ada.Characters.Latin_1 A.3.3(23)
UC_I_Diaeresis
  in Ada.Characters.Latin_1 A.3.3(23)
UC_I_Grave
  in Ada.Characters.Latin_1 A.3.3(23)
UC_Icelandic_Eth
  in Ada.Characters.Latin_1 A.3.3(23)
UC_Icelandic_Thorn
  in Ada.Characters.Latin_1 A.3.3(23)
UC_O_Acute
  in Ada.Characters.Latin_1 A.3.3(23)
UC_O_Circumflex
  in Ada.Characters.Latin_1 A.3.3(23)
UC_O_Diaeresis
  in Ada.Characters.Latin_1 A.3.3(23)
UC_O_Grave
  in Ada.Characters.Latin_1 A.3.3(23)
UC_O_Oblique_Stroke
  in Ada.Characters.Latin_1 A.3.3(23)
UC_O_Tilde
  in Ada.Characters.Latin_1 A.3.3(23)
UC_U_Acute
  in Ada.Characters.Latin_1 A.3.3(23)
UC_U_Circumflex
  in Ada.Characters.Latin_1 A.3.3(23)
UC_U_Diaeresis
  in Ada.Characters.Latin_1 A.3.3(23)
UC_U_Grave
  in Ada.Characters.Latin_1 A.3.3(23)
UC_Y_Acute
  in Ada.Characters.Latin_1 A.3.3(23)
Index

Index entries are given by paragraph number. A list of all language-defined library units may be found under Language-Defined Library Units. A list of all language-defined types may be found under Language-Defined Types. A list of all language-defined subprograms may be found under Language-Defined Subprograms.

<table>
<thead>
<tr>
<th>Paragraph Numbers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1(2/2), 2.1(3/2), 5.3(3/3), 6.1(3/2)</td>
<td>&lt; operator 4.5(1), 4.5.2(1)</td>
</tr>
<tr>
<td>&amp; operator 4.5(1), 4.5.3(3)</td>
<td>&lt;= operator 4.5(1), 4.5.2(1)</td>
</tr>
<tr>
<td>* operator 4.5(1), 4.5.5(1)</td>
<td>= operator 4.5(1), 4.5.2(1)</td>
</tr>
<tr>
<td>** operator 4.5(1), 4.5.6(7)</td>
<td>&gt; operator 4.5(1), 4.5.2(1)</td>
</tr>
<tr>
<td>+ operator 4.5(1), 4.5.3(1), 4.5.4(1)</td>
<td>&gt;= operator 4.5(1), 4.5.2(1)</td>
</tr>
<tr>
<td>- operator 4.5(1), 4.5.3(1), 4.5.4(1)</td>
<td>&gt; operator 4.5(1), 4.5.2(1)</td>
</tr>
<tr>
<td>/ operator 4.5(1), 4.5.5(1)</td>
<td>&gt;= operator 4.5(1), 4.5.2(1)</td>
</tr>
<tr>
<td>/= operator 4.5(1), 4.5.2(1), 6.6(6/3)</td>
<td>&gt; operator 4.5(1), 4.5.2(1)</td>
</tr>
</tbody>
</table>

---

2.1(2/2), 2.1(3/2), 5.3(3/3), 6.1(3/2)  | < operator 4.5(1), 4.5.2(1) |
& operator 4.5(1), 4.5.3(3)  | <= operator 4.5(1), 4.5.2(1) |
* operator 4.5(1), 4.5.5(1)  | = operator 4.5(1), 4.5.2(1) |
** operator 4.5(1), 4.5.6(7)  | > operator 4.5(1), 4.5.2(1) |
+ operator 4.5(1), 4.5.3(1), 4.5.4(1)  | >= operator 4.5(1), 4.5.2(1) |
- operator 4.5(1), 4.5.3(1), 4.5.4(1)  | > operator 4.5(1), 4.5.2(1) |
/ operator 4.5(1), 4.5.5(1)  | >= operator 4.5(1), 4.5.2(1) |
/= operator 4.5(1), 4.5.2(1), 6.6(6/3)  | > operator 4.5(1), 4.5.2(1) |
ARG 1.3(1.f/5)

Argument
in Ada.Command_Line A.15(5)
in Ada.Numerics.Generic_Complex - Arrays G.3.2(10/2), G.3.2(31/2)
in Ada.Numerics.Generic_Complex - Types G.1.1(10)

argument of a pragma 2.8(9)
Argument_Count
in Ada.Command_Line A.15(4)
assertion raised by failure of runtime check
3.2.4(31.1/4), 3.2.4(31/5), 4.6(57/5),
6.1.1(32/3), 6.1.1(33/3), 6.1.1(35/3),
6.5(22/5), 7.3.2(22/3), 7.3.3(9/5),
11.5(23.3/5)
in Ada.Assertions
associated discriminants
of a named discriminant association
3.7.1(5)
of a positional discriminant association
3.7.1(5)
associated entity
of an aspect specification
13.1.1(5/5)
associated object
of a value of a by-reference type
6.2(10/5)
of a value of a limited type
6.2(10.f)
asterisk
2.1(15/5)
in Ada.Characters.Latin_1
A.3.3(8)
asynchronous
remote procedure call
E.4.1(9/3)
Asynchronous aspect
E.4.1(8.1/3)
Asynchronous pragma
E.4.1(3/3),
J.15.13(2/3), L(3.1/3), L(3/3)
asynchronous remote procedure call
E.4.1(5/5)
asynchronous select
9.7.4(2)
used
9.7(2), P.1
Asynchronous_Task_Control
child of Ada_D1.1(3/5)
at sign
2.1(15/5)
at-most-once execution
E.4(11)
at clause
J.1(1)
used
13.1(2/1), P.1
atomic
C.6(7/3)
Atomic aspect
C.6(2/3)
Atomic pragma
C.6(3/3), J.15.8(2/3),
L(4.1/3), L(4/3)
Atomic_Add
in
System.Atomic_Operations.Integer_Arithmetic
C.6.4(4/5)
in
System.Atomic_Operations.Modular_Arithmetic
C.6.5(4/5)
Atomic_Clear
in
System.Atomic_Operations.Test_And_Set
C.6.3(6/5)
Atomic_Compare_And_Exchange
in
C.6.2(7/5)
Atomic_Components aspect
C.6(6.7/3)
Atomic_Components pragma
C.6(5/3),
J.15.8(5/3), L(5.1/3), L(5/3)
Atomic_Exchange
in
C.6.2(6/5)
Atomic_Fetch_And_Add
in
System.Atomic_Operations.Integer_Arithmetic
C.6.4(6/5)
in
System.Atomic_Operations.Modular_Arithmetic
C.6.5(6/5)
Bounded_Slice
  in Ada.Strings.Bounded A.4.4(28/1.2), C A.4.4(28/2.2)
Bounded_String
Bounded_Synchronized_Queues
  child of Ada.Containers A.18.29(2/5)
Bounded_Vectors
  child of Ada.Containers A.18.19(1/3)
BPH
  in Ada.Characters.Latin_1 A.3.3(17)
  broadcast signal
    See protected object 9.4(1)
    See requeue 9.5.4(1)
Broken_Bar
  in Ada.Characters.Latin_1 A.3.3(21/3)
BS
  in Ada.Characters.Latin_1 A.3.3(5)
  budget D.14.2(14/2)
Budget_Has_Expired
  in Ada.Execution_Time.Group_Budgets D.14.2(9/2)
Budget_Remaining
  in Ada.Execution_Time.Group_Budgets D.14.2(9/2)
Buffer_Size
  in Ada.Storage_IO A.9(4)
Buffer_Type
in
  in Ada.Strings.Text_Buffers.Unbounded A.4.12(19/5)
Buffer_Type subtype of Storage_Array
  in Ada.Storage_IO A.9(4)
build-in-place
  [partial] 7.5(8.2/3), 7.6(17.1.v.1/3)
  See built in place
built in place 7.6(17.1/5)
by copy parameter passing 6.2(2)
by reference parameter passing 6.2(2)
by-copy type 6.2(3/3)
by-reference primitive 13.1(10/5)
by-reference type 6.2(4)
atomic or volatile C.6(18)
Byte
  in Interfaces.COBOL B.4(29/3)
  See storage element 13.3(8)
byte sex
  See ordering of storage elements in a word 13.5.3(5)
Byte_Array
  in Interfaces.COBOL B.4(29/3)
C
  child of Interfaces B.3(4/5)
  C interface B.3(1/4)
  C standard 1.2(7.5), 1.2.1(8/5)
++ standard 1.2(9/5), 1.2.1(9/5)
  C_bool
    in Interfaces.C B.3(13.1/5)
  C_float
    in Interfaces.C B.3(15)
  C_Variadic
    in Interfaces.C B.3(60.16/4)
Calendar
  child of Ada 9.6(10/5)
  Calendar_Assertion_Check 11.5(23.4/5)
call 6(2/3)
  master of 3.10.2(10.1/3)
call on a dispatching operation 3.9.2(2/3)
callable 9.9(2)
  Callable attribute 9.9(2)
  Callable construct 6(2/3)
  callable entity 6(2/3)
called partial 9.4(1)
called partition E.4(1/5)
caller attribute C.7.1(14/3)
calling convention 6.3(12/1), B.1(11/3)
Ada 6.3(13/3)
  associated with a designated profile 3.10(11)
  entry 6.3.1(13/4)
  Intrinsic 6.3.1(4)
  protected 6.3.1(12/4)
calling partition E.4(1/5)
calling stub E.4(10)
CAN
  in Ada.Characters.Latin_1 A.3.3(6)
can cancel 13.1(28/5)
cancel a logical thread 5.1(16/5)
a parallel construct 5.1(16/5)
Cancel_Handler
  in Ada.Execution_Time.Group_Budgets D.14.2(10/2)
in
in
  in Ada.Real_Time.Timing_Events D.15(5/2)
cancellation
  of a delay_statement 9.6(22/3)
of an entry call 9.5.3(20)
cancellation of a remote subprogram call E.4(13)
canonical form A.5.3(3)
canonical order of array components 5.5.2(11/5)
canonical semantics 11.6(2/3)
canonical-form representation A.5.3(10)
capacity
  of a hashed map A.18.5(41/2)
of a hashed set A.18.8(63/2)
of a queue A.18.27(10/3)
of a vector A.18.2(2/2)
in
  in Ada.Containers.Hashed_Maps A.18.5(8/5)
in
  in Ada.Containers.Hashed_Sets A.18.8(10/5)
in
  in Ada.Containers.Vectors A.18.2(9/5)
Capacity_Error
  in Ada.Containers A.18.1(5.1/3)
case expression 4.5.7(1/3)
case insensitive 2.3(5.2/3), 2.3(5/5)
case_expression 4.5.7(5/3)
  used 4.5.7(2/3), P.1
case_expression_alternative 4.5.7(6/3)
  used 4.5.7(5/3), P.1
case_statement 5.4(2/3)
  used 5.1(5/3), P.1
case_statement_alternative 5.4(3)
  used 5.4(2/3), P.1
cast
  See type conversion 4.6(1/3)
  See unchecked type conversion 13.9(1)
catch (an exception)
  See handle 11(1/3)
categorization aspect E.2(2/3)
categorization pragma E.2(2/3), J.15.15(8/5)
Pure J.15.15(9/5)
Remote_Call_Interface E.2.3(2/5), J.15.15(9/5)
Remote_Types E.2.2(2/5), J.15.15(9/5)
Shared.Passive E.2.1(2/5), J.15.15(9/5)
categorized library unit E.2(2/3)
category
  of types 3.2(2/5), 3.4(1/2)
category determined for a formal type 12.5(6/3)
category of types 1.3.1(13/5)
catenation operator
  See concatenation operator 4.5(1)
  See concatenation operator 4.5.3(3)
Cause_Of_Termination
  in Ada.Task_Termination C.7.3(3/2)
CCH
  in Ada.Characters.Latin_1 A.3.3(18)
  cease to exist
    object 7.6.1(11/3), 13.11.2(10/4)
type 7.6.1(11/3)
Cedilla
  in Ada.Characters.Latin_1 A.3.3(22)
Ceiling
  in Ada.Containers.Ordered_Maps A.18.6(41/5)
in
  in Ada.Containers.Ordered_Sets A.18.9(51/2), A.18.9(71/5)
Ceiling attribute A.5.3(33)
  ceiling priority
    of a protected object D.3(8/3)
Ceiling_Check
Ceiling_Locking locking policy D.3(7)
Cent_Sign
  in Ada.Characters.Latin_1 A.3.3(21/3)
change of representation 13.6(1/5)
char
  in Interfaces.C B.3(19)
container_element_association_list

used A.3.5(17/5)
Containers
child of Ada A.18.1(3/5)
Containers_Assertion_Check
A.11.5(23/6.5)
Containing_Directory
in Ada.Directories A.16(17/5)
Contains
in Ada.Containers.Doubly_Linked_Lists A.18.3(43/2)
in Ada.Containers.Hashed_Maps A.18.5(32/2)
in Ada.Containers.Hashed_Sets A.18.8(44/2), A.18.8(57/2)
in Ada.Containers.Multway_Trees A.18.10(41/3)
in Ada.Containers.Ordered_Maps A.18.6(42/2)
in Ada.Containers.Ordered_Sets A.18.9(52/2), A.18.9(72/2)
in Ada.Containers.Vectors A.18.2(71/2)
context free grammar
complete listing P.1(1/5)
cross reference P.2(1/3)
notation 1.1.4(3)
derunder Syntax heading 1.1.2(25)
context_clause 10.1.2(2)
context_item 10.1.2(3)
used 10.1.2(2), P.1
contiguous representation [partial] 13.1(7.a/2), 13.5.2(5),
13.7.1(12), 13.9(9), 13.9(17/3),
13.11(16/3), 13.11(17.d),
13.11(21.6/5)
Continue
in Ada.Asynchronous_Task_Control D.11(3/5)
contract model of generics 12.3.1(3.5)
control character
a category of Character A.3.2(22)
a category of Character A.3.3(4),
A.3.3(15)
See also format_effector 2.1(13/3)
See also other_control_function 2.1(14/3)
Control_Set
in Ada.Strings,Maps,Constants A.4.6(4)
controlled
aspect of representation 13.11.3(5/4)
in Ada.Finalization 7.6(5/5)
Controlled pragma 13.11.3(3.3), L(7/3)
controlled type 1.3.1(19/5), 7.6(2),
7.6(9/2)
controlling access result 3.9.2(2/3)
controlling formal parameter 3.9.2(2/3)
controlling operand 3.9.2(2/3)
controlling result 3.9.2(2/3)
controlling tag
for a call on a dispatching operation
3.9.2(1/5)
controlling tag_value 3.9.2(14)
for the expression in an
assignment_statement 5.2(9)
controlling type
of a
formal_abstract_subprogram_declaration
12.6(8/5)
convention 6.3.1(2/1), B.1(11/3)
aspect of representation B.1(28/3)
Convention aspect B.1(2/3)
Convention pragma B.1(7/3), J.15.5(4/3),
L.8(1/3), L(8/3)
conversion 4.6(1/3), 4.6(28)
access 4.6(13/2), 4.6(18/2),
4.6(24.11/2), 4.6(24.18/2),
4.6(24.19/2), 4.6(47)
arbitrary order 1.1.4(18)
array 4.6(9/2), 4.6(24.2/2), 4.6(36)
composite (non-array) 4.6(21/3),
4.6(40)
enumeration 4.6(21.1/2), 4.6(21/3),
4.6(34)
numeric 4.6(8/2), 4.6(24.1/2), 4.6(29)
unchecked 13.9(1)
value 4.6(5/5)
view 4.6(5/5)
Conversion_Error
in Interfaces.COBOL B.4(30)
Conversions
child of Ada.Characters A.3.4(2/5)
child of Ada.Strings.UTF_Encoding
A.4.11(15/5)
Convert
in Ada.Strings.UTF_Encoding.Conversions
A.4.11(16/3), A.4.11(17/3),
A.4.11(18/3), A.4.11(19/3),
A.4.11(20/3)
convertible 4.6(4/3)
required 3.7(16/3), 3.7(1/9/3),
4.6(11/2), 4.6(15/2), 4.6(24.13/2),
4.6(24.2/2), 4.6.6(1/3), 8.6(27.1/4)
Copy
in Ada.Containers.Bounded_Hashed_Maps A.18.21(13/5)
in Ada.Containers.Bounded_Hashed_Sets A.18.23(13/5)
in Ada.Containers.Bounded_Ordered_Ma
ps A.18.22(10/5)
in Ada.Containers.Doubly_Linked_Lists A.18.3(17.6/5), A.18.3(51.9/5)
in Ada.Containers.Hashed_Maps A.18.5(17.8/5), A.18.5(37.10/5)
in Ada.Containers.Hashed_Sets A.18.8(17.5/5), A.18.8(59.9/5)
in Ada.Containers.Indefinite_Holders A.18.18(21/5)
in Ada.Containers.Multway_Trees A.18.10(33/5), A.18.10(70.9/5)
in Ada.Containers.Ordered_Maps A.18.6(16.8/5), A.18.6(51.11/5)
in Ada.Containers.Ordered_Sets A.18.9(16.5/5), A.18.9(74.9/5)
in Ada.Containers.Vectors A.18.2(48.5/5), A.18.2(79.9/5)
Copy_Array
in Interfaces.C.Pointers B.3.2(15)
Copy_File
in Ada.Directories A.16(13/2)
Copy_Local_Subtree
in Ada.Containers.Multway_Trees A.18.10(54.1/5)
Copy_Sign_attribute A.5.3(51)
Copy_Subtree
in Ada.Containers.Multway_Trees A.18.10(54.2/5), A.18.10(54/5)
Copy_Terminated_Array
in Interfaces.C.Pointers B.3.2(14)
Copyright_Sign
in Ada.Characters.Latin_1 A.3.3(21/3)
core language 1.1.2(2), 1.3.8(5)
Correction 1.1.2(40.aa/3), 1.1.2(40.nn/5),
1.1.2(40.qq/5)
corresponding constraint 3.4(6)
corresponding discriminants 3.7(18)
corresponding expression
class-wide type invariant 7.3(8/5)
corresponding expression
class-wide postcondition 6.1.1(18/5)
class-wide precondition 6.1.1(18/5)
corresponding index
for an array_aggregate 4.3.3(8)
corresponding subtype 3.4(18/3)
corresponding value
of the target type of a conversion
4.6(28)
Corrigeendum 1.1.2(40.aaa/6),
1.1.2(40.dd/6), 1.1.2(40.ggg/6),
1.1.2(40.jjj/6), 1.1.2(40.nn/3),
1.1.2(40.nn/5), 1.1.2(40.qq/5),
1.1.2(40.tt/5), 1.1.2(40.ww/5)
Cos
in Ada.Numerics.Generic_Complex_Elementary_Functions G.1.2(4)
defining_identifier_list  3.3.1(3)
  used  3.3.1(2/3), 3.3.2(2), 3.7(5/5), 3.8(6/3), 6.1(15/5), 11.1(2/3), 12.4(2/3), P.1
defining_operator_symbol  6.1(11)
  used  6.1(6), P.1
defining_program_unit_name  6.1(7)
  used  6.1(4/1), 6.1(4/2), 6.1(6), 7.1(3/3), 7.2(2/3), 8.5.3(2/3), 8.5.5(2/3), 12.3(2/3), P.1
Definite attribute  12.5.1(23/5)
definition  3.1(7)
definite subtype  3.3(23/5)
Definite attribute  12.5.1(23/3)
definition  3.1(7)
Degree_Sign  8.6(16)
denominator  4.3.4(2/5)
Delta attribute  3.5.10(3)
delta aggregate  4.3.4(1/5)
Delta attribute  3.5.10(3)
delta aggregate  4.3.4(2/5)
  used  4.3(2/5), P.1
delta_constraint  J.3(2/4)
  used  3.2(2/6), P.1
Denominator  3.5.7(8/5)
Denorm attribute  A.5.3(9)
denormalized number  A.5.3(10)
denote  8.6(16)
informal definition  3.1(8)
name used as a pragma argument  8.6(32)
depend on a discriminant
  for a component  3.7(20)
  for a constraint or
  component_definition  3.7(19)
dependence
  elaboration  10.2(9/5)
of a task on a master  9.3(1)
of a task on another task  9.3(4)
semantic  10.1.1(26/2)
deep
accessibility level  3.10.2(3/5)
of a task on a master  9.3(1)
of a task on another task  9.3(4)
semantic  10.1.1(26/2)
depth
first-order  A.18.10(5/3)
Delete  A.18.10(35/5)
Delete_Tree  A.18.10(36/5)
Delete_Tree  in Ada.Directories A.16(10/2)
delimiter  2.2(8/2)
delivery  of an interrupt  C.3(2)
delta
of a fixed point type  3.5.9(1)
delta aggregate  4.3.4(1/5)
Delta attribute  3.5.10(3)
delta aggregate  4.3.4(2/5)
  used  4.3(2/5), P.1
delta_constraint  J.3(2/4)
  used  3.2(2/6), P.1
Denominator
in
  Ada.Numerics.Big_Numbers.Big_Real A.5.7(8/5)
Denorm attribute  A.5.3(9)
denormalized number  A.5.3(10)
denote  8.6(16)
informal definition  3.1(8)
name used as a pragma argument  8.6(32)
depend on a discriminant
  for a component  3.7(20)
  for a constraint or
  component_definition  3.7(19)
dependence
  elaboration  10.2(9/5)
of a task on a master  9.3(1)
of a task on another task  9.3(4)
semantic  10.1.1(26/2)
deep
accessibility level  3.10.2(3/5)
of a task on a master  9.3(1)
of a task on another task  9.3(4)
semantic  10.1.1(26/2)
depth
first-order  A.18.10(5/3)
Dequeue
in
in
  Ada.Containers.Bounded_Synchronized_Interfaces A.18.27(6/5)
in
in
  Ada.Containers.Unbounded_Synchronized_Queue A.18.28(6/5)
Dequeue_Only_High_Priority
in
in
dereference  4.1(8)
Dereference_Error
in
  Interfaces.C.Strings B.3.1(12)
derivation class
for a type  3.4.1(2/2)
derived from
directly or indirectly  3.4.1(2/2)
derived type  1.3.1(22/5), 3.4(1/2)
[partial]  3.4(24)
derived_type_definition  3.4(2/2)
  used  3.2(14/2), P.1
descendant  10.1.1(11)
  at run time  3.9(12/3/3)
of a tree node  A.18.10(4/3)
of a type  3.4.1(10/2)
of an incomplete view  7.3.1(5/3)
of the full view of a type  7.3.1(5/2)
relationship with scope  8.2(4)
descendant of a type  1.3.1(25/5)
Descendant_Tag
in
  Ada.Tags  3.9(7/1/2)
designate  3.10(1)
designated profile
of an access-to-subprogram type  3.10(11)
of an anonymous access type  3.10(12/3)
designated subtype
of a named access type  3.10(10)
of an anonymous access type  3.10(12/3)
designated type
of a named access type  3.10(10)
of an anonymous access type  3.10(12/3)
designator  6.1(5)
  used  6.3(2/3), P.1
destructor
See finalization  7.6(1)
See finalization  7.6.1(1)
Detach_Handler
in Ada.Interrupts C.3.2(9)

Detect_Blocking pragma H.5(3/2), L(8.4/2)

Determinant
in Ada.Numerics.Generic_Complex_Arrays G.3.2(4/6)
in Ada.Numerics.Generic_Real_Arrays G.3.1(24/2)
determined category for a formal type 12.5(6/3)
determined class for a formal type 12.5(6/3)
determined to be unevaluated 6.1.1(24/1/5)
determines a type by a subtype_mark 3.2.2(8)
determining expression 6.1.1(22.16/5)
Device_Error
in Ada.Direct_IO A.8.4(18)
in Ada.Directories A.16(43/2)
in Ada.IO_Exceptions A.13(4)
in Ada.Sequential_IO A.8.1(15)
in Ada.Streams.Stream_IO A.12.1(26)
in Ada.Text_IO A.10.1(85/5)

Diaeresis
in Ada.Characters.Latin_1 A.3.3(21/3)

Difference
in Ada.Calendar.Arithmetic 9.6.1(12/2)
in Ada.Containers.Hashed_Sets A.18.8(32/5), A.18.8(33/5)
in Ada.Containers.Ordered_Sets A.18.9(33/5), A.18.9(34/5)
digit 2.1(10/2), 2.4.1(4/1/2)
used 2.1(3/2), 2.3(3/2), 2.4.1(3), 2.4.2(5), P.1
digits of a decimal fixed point subtype 3.5.9(6), 3.5.10(7)
Digits attribute 3.5.8(2/1), 3.5.10(7)
digits_constraint 3.5.9(5/4)
used 3.2(6), P.1
dimensionality of an array 3.6(12)
direct access A.8(3)
direct file A.8(1/2)

Direct_IO
child of Ada A.8.4(2/5)
direct_name 4.1(3)
used 3.8(1/2), 4.1(2/5), 5.1(8), 9.5.2(3), 10.2(24/2), 13.1(3), 1.7(1), J.15.14(4/2), L.25(2/5), L.25(3/5), P.1
Direction
in Ada.Strings A.4.1(6)
directly specified of a representation aspect of an entity 13.1(8/5)
of an aspect of representation of an entity 13.1(8/5)
of an operational aspect of an entity 13.1(8/5)
directly visible 8.3(2), 8.3(21)
within a pragma in a context_clause 10.1.6(3)
within a pragma that appears at the place of a compilation unit 10.1.6(5)
within a use_clause in a context_clause 10.1.6(3)
within a with_clause 10.1.6(2/2)
within the parent_unit_name of a library_unit 10.1.6(2/2)
within the parent_unit_name of a subunit 10.1.6(4)

Directories
child of Ada A.16(3/5)
directory A.16(45/2)
directory entry A.16(49/2)
directory name A.16(46/2)
Directory_Type
in Ada.Directories A.16(29/2)
disabled predicate checks 3.2.4(7/3)
Discard_Names aspect C.5(1.3/4)
Discard_Names pragma C.5(3), L(9)
discrete array type 4.5.2(1)
discrete type 13.1(27/5), 3.2(3), 3.5(1)
discrete_choice 3.8.1(5/3)
used 3.8.1(4/5), P.1
discrete_choice_list 3.8.1(4/5)
used 3.8.1(3), 4.3.6(5/3), 4.3.3(5/5), 4.5.7(6/3), 5.4(3), P.1
Discrete_Random
child of Ada.Numerics A.5.2(17/5)
discrete_range 3.6.1(3)
used 3.6.1(2), 3.8.1(5/3), 4.1.2(2), 4.3.5(20/5), P.1
discrete_subtype_definition 3.6(6)
used 3.6(5), 5.5(3/1/5), 5.5(4/5), 9.5.2(2/3), 9.5.2(8/5), P.1
discriminant 1.3.1(28/5), 3.2(5/2), 3.7(1/2)
of a variant_part 3.8.1(6)
used in a record definition 3.8(12/3)
discriminant_association 3.7(1/3/5)
used 3.7(1/2), P.1

Discriminant
in Ada.Dispatching D.2.1(1.2/5), D.2.1(4/3)

Dispatching_Domain
child of System.MultithreadedDispatching.Domains D.16(1.4/3)

Disrupting_Domain
child of System.MultithreadedDispatching.Domains D.16(1.5/3)

Dispatching_Policy_Error
in Ada.Dispatching D.2.1(1.2/5), D.2.1(4/3)

Display_Format
in Interfaces.COBOL B.4(22)
displayed magnitude (of a decimal value) F.3.2(14)
disruption of an assignment 9.8(21), 13.9(1/5)
distinct access paths 6.2(12/3)
distinguished receiver notation 4.1.3(19/2/2)
distributed accessibility 3.10.2(32/1/3)
distributed program E(3)
dispatching aspect H.7.1(8/5)
dispatching call on a dispatching_operation D.9.2(1/5)
dispatching domain D.16.1(16/4)
dispatching operation 3.9.2(1/5), 3.9.2(2/3)
[partial] 3.9(1)
dispatching operation set H.7.1(14/5)
dispatching point D.2.1(4/5)
[partial] D.2.1(8/5), D.2.2(12/2), D.2.3(8/2), D.2.4(9/3)
dispatching policy for tasks 9.10.a(3)
[partial] D.2.1(5/2)
dispatching, task D.2.1(4/5)

Dispatching_Domain

Display_Name
displaying_operation D.16.1(18/3)
displaying_operation_specifier H.7.1(10/5)
used H.7.1(9/5), P.1

Dispatch_Policy_Error
in Ada.Dispatching D.2.1(1.2/5), D.2.1(4/3)

Display_Name
displaying_operation D.16.1(18/3)
displaying_operation_specifier H.7.1(10/5)
used H.7.1(9/5), P.1

Dispatching_Policy_Error
in Ada.Dispatching D.2.1(1.2/5), D.2.1(4/3)

Display_Name
displaying_operation D.16.1(18/3)
displaying_operation_specifier H.7.1(10/5)
used H.7.1(9/5), P.1

Dispatching_Policy_Error
in Ada.Dispatching D.2.1(1.2/5), D.2.1(4/3)

Display_Name
displaying_operation D.16.1(18/3)
displaying_operation_specifier H.7.1(10/5)
used H.7.1(9/5), P.1

Dispatching_Policy_Error
in Ada.Dispatching D.2.1(1.2/5), D.2.1(4/3)
documentation (required of an implementation) 1.1.3(18), M.1(1/5), M.2(1/5), M.3(1/5)
documentation requirements 1.1.2(34), M.1(1/5)
summary of requirements M.1(1/5)

Dollar_Sign
  in Ada.Characters.Latin_1 A.3.3(8)
dope 13.5.1(15.d)
dot 2.1(15/5)
dot selection
  See selected_component 4.1.3(1)
double
  in Interfaces.C B.3(16)
  in Interfaces.Fortran B.5(10.2/5)
  in Interfaces.Imaginary subtype of Imaginary
    in Interfaces.Fortran B.5(10.3/5)
Double_Precision
  in Interfaces.Fortran B.5(6)
  in Interfaces.Complex_Types
    in Interfaces.Fortran B.5(10.1/5)
Double_Linked_Lists
  child of Ada.Containers A.18.3(5/5)
downward closure 3.10.2(13.3/2), 3.10.2(37/5)
drift rate D.8(41)
Duration
  in Standard A.1(43)
dynamic binding
  See dispatching operation 3.9(1)
dynamic semantics 1.1.2(30)
Dynamic_Predicate aspect 3.2.4(1/5)
Dynamic_Priorities
  child of Ada D.5.1(3/5)
dynamically determined tag 3.9.2(1/5)
dynamically enclosing
  of one execution by another 11.4(2)
dynamically tagged 3.9.2(5/2)

E
e
  in Ada.Numerics A.5(3/5)
EDF
  child of Ada.Dispatching D.2.6(9/5)
child of
    Ada.Synchronous_Task_Control D.10(5.2/5)
EDF_Across_Priorities task dispatching policy D.2.6(7/5)
EDF_Within_Priorities task dispatching policy D.2.6(7/5)
edited output F.3(1/2)

Editing
  child of Ada.Text_IO F.3.3(3/5)
  child of Ada.Wide_Text_IO F.3.4(1)
child of Ada.Wide_Wide_Text_IO F.3.5(1/2)
effect
  external 1.1.3(8)
efficiency 11.5(29/5), 11.6(1/3)

Eigensystem
  in Ada.Numerics.Generic_Complex_Arrays G.3.2(49/2)
in Ada.Numerics.Generic_Real_Arrays G.3.1(27/2)

Eigenvalues
  in Ada.Numerics.Generic_Complex_Arrays G.3.2(48/2)
in Ada.Numerics.Generic_Real_Arrays G.3.1(26/2)
elementary
  3.1(11)
Elaborate pragma 10.2.1(20), L(10)
Elaborate_All pragma 10.2.1(21), L(11)
Elaborate_Body aspect 10.2.1(26.1/5)
Elaborate_Body pragma 10.2.1(22/5), J.15.14(6/5), L(12/5)
elementarily
  3.1(11)
elaboration
  1.3.4(3/5), 3.1(11)
abstract_subprogram_declaration
  3.9.3(11.1/2), 6.1(31/2)
access_declaration 3.10(17/2)
access_type_definition 3.10(16)
array_type_definition 3.6(21)
aspect_clause 13.1(19/1)
choice_parameter_specification 11.4(7)
chunk_specification 5.5(8.1/5)
component_declaration 3.8(17)
component_definition 3.6(22/2), 3.8(18/2)
component_list 3.8(17)
declaration named by a pragma Import B.1(38/3)
declaration with a True Import aspect B.1(38/3)
declarative_part 3.11(7)
defered constant declaration 7.4(10/3)
delta_constraint 3.1(11)
derived_type_definition 3.4(26)
digits_constraint 3.5(9/19/4)
discrete_subtype_definition 3.6(22/2)
discriminant_constraint 3.7(12.1/5)
entry_declaration 9.5.2(22/1)
enumeration_type_definition 3.5.1(10)
exception_declaration 11.1(5)
expression_function_declaration 6.8(8/3)
fixed_point_definition 3.5.9(17)
floating_point_definition 3.5.7(13)
full_type_definition 3.2.1(11)
full_type declaración 3.2.1(11)
generic body 12.2(2)
generic_declaration 12.1(10)
generic_instantiation 12.3(20)
incomplete_type_declaration 3.10.1(12)
index_constraint 3.6.1(8)
integer_type_declaration 5.5(9/5)
nongeneric package_body 7.2(6)
nongeneric_subprogram_body 6.3(6)
null_procedure_declaration 6.7(5/3)
number_declaration 3.3.2(7)
object_declaration 3.3.1(15), 7.6(10/2)

of library units for a foreign language main

package_body of Standard A.1(50)
package_declaration 7.1(8)
partition E.1(6)
partition E.5(21)
per-object constraint 3.8(18/1)
pragma 2.8(12)
private_extension_declaration 7.3(17)
private_type_declaration 7.3(17)
protected_declaration 9.4(12)
protected_body 9.4(15)
protected_definition 9.4(13)
range_constraint 3.5(9)
real_type_definition 3.5.6(5)
record_definition 3.8(16)
record_extension_part 3.9(1/5)
record_type_definition 3.8(16)
renaming_declaration 8.5(3)
representation_clause 13.1(19/1)
single_protected_declaration 9.4(12)
single_task_declaration 9.1(10)
Storage_Size pragma A.13.66(3)
subprogram_declaration 6.1(31.2)
su subtype_declaration 3.2.2(9)
su subtype_indication 3.2.2(9)
task_declaration 9.1(10)
task_body 9.1(13)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
task_definition 9.1(11)
use_clause 8.4(12)
variant_part 3.8.1(22)
elaboration control 10.2.1(1/5)
elaboration dependence
library_item on another 10.2(9/5)

Elaboration_Check 11.5(20)

[partial] 3.11(9)
element
of a storage pool 13.11(11)
in Ada.Containers.Doubly_Linked_Lists A.18.3(4/1.5), A.18.3(14/5)
in Ada.Containers.Hashed_Maps A.18.5(14/5), A.18.5(31/2)
in Ada.Containers.Hashed_Sets A.18.8(15/5), A.18.8(52/2)
in Ada.Containers.Indefinite_Holders A.18.18(12/5)
in Ada.Containers.Multiway_Trees A.18.10(24/1.5), A.18.10(24/5)
in Ada.Containers.Ordered_Maps A.18.6(13.5/5), A.18.6(39/2)
in Ada.Containers.Ordered_Sets A.18.9(14/5), A.18.9(14/5), A.18.9(65/2)
in Ada.Containers.Vectors A.18.2(27/5), A.18.2(28/1.5), A.18.2(28/5)
in Ada.Strings.Unbounded A.4.5(20)
element type
container aggregate 4.3.5(7/6), 4.3.5(9/6)
EPA
  in Ada.Characters.Latin_1   A.3.3(18)
epoch   D.8(19)
equal operator   4.5(1), 4.5.2(1)
Equal Case Insensitive
  child of Ada.Strings   A.4.10(2/5)
child of Ada.Strings.Bounded
  A.4.10(7/5)
child of Ada.Strings.Fixed   A.4.10(5/3)
child of Ada.Strings.Unbounded
  A.4.10(10/5)
Equivalent_Sets
  Equivalent_Keys
  Equivalent_Elements
  of an ordered map   A.18.6(55/2)
of a hashed map   A.18.5(42/2)
equivalent key
  of an ordered set   A.18.9(78/2)
of a hashed set   A.18.8(64/2)
equivalent element
  of a hashed map   A.18.10(14/3)
equality operator   4.5.2(1)
special inheritance rule for tagged types
  3.4(17/2), 4.5.2(14/3)
equals sign
  2.1(15/5)
Equals_Sign
  in Ada.Characters.Latin_1   A.3.3(10)
equivalence of use clauses and
  selected_components   8.4(1.a)
equivalent element
  of a hashed set   A.18.8(64/2)
of an ordered set   A.18.9(78/2)
equivalent key
  of a hashed map   A.18.5(42/2)
of an ordered map   A.18.6(55/2)
Equivalent_Elements
  in Ada.Containers.Indefinite_Holders
  A.18.18(7.1/5)
in Ada.Containers.Multiway_Trees
  A.18.10(11.1/5)
Equal_Subtree
  in Ada.Containers.Multiway_Trees
  A.18.10(14/3)
equality operator   4.5.2(1)
special inheritance rule for tagged types
  3.4(17/2), 4.5.2(14/3)
equals sign
  2.1(15/5)
error
  compile-time   1.1.2(27), 1.1.5(4)
link-time   1.1.2(29), 1.1.5(4)
run-time   1.1.2(30), 1.1.5(6), 11.5(2/3), 11.6(1/3)
See also bounded error, erroneous execution
  ESA
  in Ada.Characters.Latin_1   A.3.3(17)
ESC
  in Ada.Characters.Latin_1   A.3.3(6)
Establish_RPC_Receiver
  in System.RPC   E.5(12)
ETB
  in Ada.Characters.Latin_1   A.3.3(6)
ETX
  in Ada.Characters.Latin_1   A.3.3(5)
evaluable   3.1(11.f)
evaluated operative constituent
  evaluation   1.3.4(5/5), 3.1(11)
aggregate   4.3(5)
allocor   4.8(7/2)
array_aggregate   4.3.3(21/5)
attribute_reference   4.1.4(11/5)
case_expression   4.5.7(21/3)
concatenation   4.5.3(5)
dereference   4.1(13)
discrete_range   3.6.1(8)
extension_aggregate   4.3.2(7)
generalized_reference   4.1.5(8/3)
generic_association   12.3(21)
generic_association for a formal object
  of mode in   12.4(11)
if_expression   4.5.7(20/3)
indexed_component   4.1.1(7)
initialized allocator   4.8(7/2)
membership test   4.5.2(27/4)
name   4.1(11/2)
name that has a prefix   4.1(12)
null literal   4.2(9/5)
numeric literal   4.2(9/5)
parameter_association   6.4.1(7)
primary that is a name   4.4(10)
qualifier   4.7(5/4)
quantified_expression   4.5.8(6/5)
range   3.5(9)
range_attribute_reference   4.1.4(11/5)
record_aggregate   4.3.1(18)
record_component_association_list
  4.3.1(19/5)
reduction_attribute_reference   4.5.10(24/5)
selected_component   4.1.3(14)
short-circuit control form   4.5.1(7)
slice   4.1(2/7)
string_literal   4.2(10/5)
uninitialized allocator   4.8(8)
Val
  3.5.7(5), K.2(261)
Value
  3.5(55/5)
value conversion   4.6(28)
value_sequence   4.5.10(20/5)
view_conversion   4.6(52)
Wide_Value
  3.5(43/5)
Wide_Wide_Value
  3.5(39.4/3)
exception
  1.3.5(2/5), 11.1(1)
exception occurrence   13.5(3/5), 11.1(3)
exception choice
  11.1(5)
used
  11.2(3/5), P.1
exception_declaration
  11.1(2/3)
used
  3.1(3/3), P.1
exception_handler
  11.2(3/5)
used
  11.2(2), P.1
Exception_Id
  in Ada.Exceptions
  11.4.1(2/5)
Exception_Identity
  in Ada.Exceptions
  11.4.1(5/2)
Exception_Information
  in Ada.Exceptions
  11.4.1(5/2)
Exception_Message
  in Ada.Exceptions
  11.4.1(4/3)
Exception_Name
  in Ada.Exceptions
  11.4.1(2/5), 11.4.1(5/2)
Exception_Occurrence
  in Ada.Exceptions
  11.4.1(3/5)
Exception_Occurrence_Access
  in Ada.Exceptions
  11.4.1(3/5)
exception_renaming_declaration
  8.5.2(2/3)
used
  8.5(2), P.1
Exceptions
  child of Ada
  11.4.1(2/5)
Exchange
  child of System.Atomic_Operations
  C.6.2(5/5)
Exchange_Handler
  in Ada.Interrupts
  C.3.2(8)
Exclamation
  in Ada.Characters.Latin_1   A.3.3(8)
exclamation point
  2.1(15/5)
Exclude
  in Ada.Containers.Hashed_Maps
  A.18.5(24/5)
in Ada.Containers.Hashed_Sets
  A.18.8(23/5), A.18.8(54/5)
asynchronous_select with a procedure
assignment_statement   5.2(7), 7.6(17),
whether 3.10(13.1/2)
exclusive
protected operation 9.5.1(2.4/4)
Exclusive_Functions aspect   9.5.1(2.2/4)
protected subprogram call   9.5.1(3)
program   10.2(25)
partition   10.2(25)
null_statement   5.1(13)
loop_statement   5.5(7/5)
loop_statement with a for
iteration_scheme   5.5(9/5)
loop_statement with a while
iteration_scheme   5.5(9/5)
null_statement   5.1(13)
partition 10.2(25)
pragma 2.8(12)
program 10.2(25)
protected subprogram call   9.5.1(3)
raise_statement with an
exception_name   11.3(4/4)
re-raise statement 11.3(4/4)
remote subprogram call E.4(9)
array delta aggregate 4.3.4(6/5)
array_aggregate 4.3.3(7/2)
array_aggregate component expression
4.3.3(7/2)
array_aggregate discrete_choice
4.3.8(3)
assignment_statement expression
5.2(4/2)
assignment_statement_variable_name
5.2(4/2)
Attach_Handler pragma second
argument J.15.7(6/3)
attribute_definition_clause expression or
name 13.3(4)
attribute_designator expression 4.1.4(7)
base expression of a delta aggregate
4.3.4(7/5)
case expression 5.4(4/3)
case_expression_selecting_expression
4.5.7(15/3)
case_expression_alternative
discrete_choice 4.5.7(15/3)
case_statement_selecting_expression
5.4(4/3)
case_statement_alternative
discrete_choice 4.5.4(3)
character_literal 4.2(3)
code_statement 13.8(4)
component_clause expressions
13.5.1(7)
component_declaration
default_expression 3.8(7)
condition 4.5.7(14/3), 5.3(4/3)
CPU pragma argument J.15.9(3/3)
decimal fixed point type digits 3.5.9(6)
delay_relative_statement expression
9.6(5)
delay_until_statement expression
9.6(5)
delta aggregate base expression
4.3.4(7/5)
delta_constraint_expression J.3(3/4)
dependent_expression 4.5.7(8/3)
dereference_name 4.1(8)
discrete_subtype_definition_range
3.6(8)
discriminant_default_expression 3.7(7)
discriminant_association_expression
3.7.1(6)
Dispatching_Domains pragma argument J.15.10(3/3)
entry_index 9.5.2(11)
enumeration_representation_clause
expressions 13.4(4)
expression in an aspect_specification
13.1.1(7/3).expression of a
Default_Component_Value aspect
3.6(22.4/3)
expression of a Default_Value aspect
3.5(56.5/3)
expression of a predicate aspect
3.2.4(2/3)
extensions to Ada 95 1.1.2(40.s/2),
2.1(19.f/2), 2.3(8.e/2), 3.2.2(15.d/2),
3.3.1(33.g/2), 3.3.1(33.h/2),
3.4(38.j/2), 3.5(63.j/2), 3.5.2(11.2),
3.5.4(36.k/2), 3.6(30.g/2), 3.6.3(8.h/2),
3.8(31.e/2), 3.8(31.f/2), 3.9(33.e/2),
3.9.1(17.b/2), 3.9.2(24.a/2),
3.9.3(17.d/2), 3.9.4(36.a/2),
3.10(26.b/2), 3.10.1(23.j/2),
3.10.2(41.g/2), 4.1(13.e/2),
4.2(14.d/2), 4.3(61.2), 4.3.1(31.c/2),
4.3(49.f/2), 4.2(39.f/2), 4.6(71.l/2),
4.8(20.h/2), 5.1(22.d/2), 6.1(42.f/2),
6.3(2.7e), 6.4(31.d/2), 6.5(28.a/2),
6.5.1(11.a/2), 6.7(7.a/2), 7.3(25.d/2),
7.4(14.j/2), 7.5(26.c/2), 7.6(27.c/2),
8.3.1(16.b/2), 8.5.1(10.d/2),
8.5.4(21.a/2), 8.6(34.q/2), 9.1(32.e/2),
9.4(35.b/2), 9.6.1(91.b/2),
9.7.4(14.b/2), 10.1.1(35.r/2),
10.1.2(32.g/2), 10.1.2(32.i/3),
10.13(24.b/2), 10.2.1(28.g/2),
11.3(8.b/2), 11.4.1(20.f/2),
11.4.2(28.a/2), 11.5(31.g/2),
12.3(29.i/2), 12.4(12.e/2),
12.5.1(28.c/2), 12.5.5(8.a/2),
12.6(24.a/2), 12.7(25.b/2),
13.1(29.i/2), 13.5.1(32.e/2),
13.7(38.e/2), 13.7.1(16.d/2),
13.11(43.e/2), 13.12(7.c/3),
13.13.2(60.i/2), 1.6(56.h/2),
A.3.1(7.b/2), A.3.2(60.c/2),
A.3.4(35.a/2), A.4.2(68.a/2),
A.4.5(88.d/2), A.4.6(88.b/2),
A.4.7(49.b/2), A.4.8(51.a/2),
A.4.9(12.c/2), A.5(5.c/2),
A.5.3(72.i/2), A.10.7(26.b/2),
A.10.11(29.a/2), A.10.12(29.a/2),
A.11.5(b/2), A.12.4(5.a/2),
A.16.131.c/2), A.17(33.b/2),
A.18.12(3.d/3), A.18.1(8.c/2),
A.18.2(264.b/2), A.18.3(164.a/2),
A.18.5(62.c/2), A.18.6(95.d/2),
A.18.8(82.c/2), A.18.9(116.c/2),
A.18.11(13.a/2), A.18.12(12.a/2),
A.18.13(13.a/2), A.18.14(13.a/2),
A.18.15(5.d/2), A.18.16(5.d/2),
A.18.26(13.a/2), B.3(84.b/2),
B.3.1(60.b/2), B.3.3(32.a/2),
C.7.3(17.a/2), D.2.2(21.a/2),
D.2.4(11.a/2), D.2.5(19.a/2),
D.2.6(34.b/2), D.2.3(23.a/2),
D.5(19.a/2), D.5.2(11.a/2),
D.7(22.b/2), D.10(12.a/2),
D.11(19.a/2), D.13(13.a/3),
D.14(29.b/2), D.14.1(29.a/2),
D.14.2(38.a/2), D.15(27.a/2),
E.2.2(20.c/3), F.3.5(6.a/2),
G.1.1(58.g/2), G.1.3(35.a/2),
G.1.5(1.a/2), G.3(13.2.c), G.3.1(91.b/2),
G.3.2(16.b/2), H.4(28.c/2),
H.5(7.a/2), H.6(17.a/2), J.15.1(6.c/3),
external call 9.5(4.3)}
first element
  of a hashed set A.18.8(68/2)
  of a set A.18.7(6/2)
  of an ordered set A.18.9(81/3)
first node
  of a hashed map A.18.5(46/2)
  of a map A.18.4(6/2)
  of an ordered map A.18.6(58/3)
first subtype 3.2.1(6/5), 3.4.1(5)
First(N) attribute 3.6.2(4)
First_Bit attribute 13.5.2(3/2)
First_Child
  in Ada.Containers.Multiway_Trees A.18.10(60.1/5), A.18.10(60/5)
First_Element
  in Ada.Containers.Multiway_Trees A.18.10(61.5), A.18.10(61/5)
First_Element
  in Ada.Containers.Doubly_Linked_Lists A.18.3(34/5)
First_Invalid attribute 3.5.6(2), P.1
Fixed
  child of Ada.Strings A.4.3(5/5)
fixed point type 3.5.9(1)
Fixed_Conversions
  in Ada.Numerics.Big_Numbers.Big_Real A.5.7(14/5)
Fixed_IO
  in Ada.Text_IO A.10.1(68)
fixed_point_definition 3.5.9(2)
used 3.5.6(2), P.1
Float 3.5.7(12), 3.5.7(14)
in Standard A.1(21)
Float_Conversions
  in Ada.Numerics.Big_Numbers.Big_Real A.5.7(13/5)
Float_IO
  in Ada.Text_IO A.10.1(63)
Float_Random
  child of Ada.Numerics A.5.2(5/5)
Float_Text IO
  child of Ada A.10.9(33)
Float_Wide_Text IO
  child of Ada A.11(2/2), A.11(3/2)
Floating
  in Interfaces.COBOL B.4(9)
floating point type 3.5.7(1)
floating_point_definition 3.5.7(2)
used 3.5.6(2), P.1
Floor
  in Ada.Containers.Ordered_Maps A.18.6(40/5)
in Ada.Containers.Ordered_Sets A.18.9(50/2), A.18.9(70/5)
Floor attribute 3.5.3(30)
Flush
  in Ada.Direct_IO A.8.4(10.1/5)
in Ada.Sequential_IO A.8.1(10.1/5)
in Ada.Streams.Stream_IO A.12.1(25/1)
in Ada.Text_IO A.10.1(21/5)
Fore attribute 3.5.10(4)
form
  of an external file A.7(1)
in Ada.Direct_IO A.8.4(9), A.8.4(18.13/5), A.8.4(18.6/5)
in Ada.Sequential_IO A.8.1(9), A.8.1(15.13/5), A.8.1(15.6/5)
in Ada.Streams.Stream_IO A.12.1(11), A.12.1(25/6), A.12.1(26/5)
in Ada.Text_IO A.10.1(12), A.10.1(85.13/5), A.10.1(85/6)
fixed object, generic 12.4(1)
fixed package, generic 12.7(1)
formal parameter
  of a subprogram 6.1(17)
formal parameter set H.7.1(13/5)
formal subprogram, generic 12.6(1)
formal subtype 12.5(5)
formal type 12.5(5)
formal_abstract_subprogram_declaration 12.6(2.3/3)
used 12.6(2/2), P.1
formal_access_type_definition 12.5.4(2)
used 12.5(3/2), P.1
formal_array_type_definition 12.5.3(2)
used 12.5(3/2), P.1
formal_complete_type_declaration 12.5(2.1/5)
used 12.5(2/3), P.1
formal_concrete_subprogram_declaration 12.6(2.1/3)
used 12.6(2/2), P.1
formal_decimal_fixed_point_definition 12.5.2(7)
used 12.5(3/2), P.1
formal_interface_type_definition 12.5.5(2/2)
used 12.5(3/2), P.1
formal_modular_type_definition 12.5.2(4)
used 12.5(3/2), P.1
formal_object_declaration 12.4(2/3)
used 12.1(6), P.1
formal_ordinary_fixed_point_definition 12.5.2(6)
used 12.5(3/2), P.1
formal_package_actual_part 12.7(3/2)
used 12.7(3/2), P.1
formal_package_association 12.7(3/1)
used 12.7(3/2), P.1
formal_package_declaration 12.7(2/3)
used 12.1(6), P.1
formal_parameter_name H.7.1(6/5)
used H.7.1(4/5), P.1
formal_parameter_set H.7.1(4/5)
formal_part 6.1(14)
used 5.5.3(5), 6.1(11/2), 6.1(13/2), P.1
formal_private_type_definition 12.5.1(2)
used 12.5(3/2), P.1
formal_signed_integer_type_definition 12.5.2(3)
used 12.5(3/2), P.1
formal_subprogram_declaration 12.6(2/2)
used 12.1(6), P.1
formal_type_declaration 12.5(2/3)
used 12.1(6), P.1
formal_type_definition 12.5(3/2)
used 12.5(2/3), 12.5(2/3), P.1
format_effector 2.1(13/3)
used 2.1(2/2), P.1
Formatting
  child of Ada.Calendar 9.6.1(15/5)
Fortran
  child of Interfaces B.5(4/5)
Fortran_interface B.5(1/3)
Fortran_standard 1.2(3/5), 1.2.1(3/5)
Fortran_character
  in Interfaces.Fortran B.5(12/3)
Fortran_Integer
  in Interfaces.Fortran B.5(5)
forward iterator 5.5.2(4/5)
Forward_Iterator
  in Ada.Iterator.Interfaces 5.5.1(3/3)
Fraction attribute A.5.3(21)
Fraction_Bounds
  in Ada.Characters.Latin_1 A.3.3(22)
Fraction_Bounds
  in Ada.Characters.Latin_1 A.3.3(22)
Fraction_Three_Quarters
  in Ada.Characters.Latin_1 A.3.3(22)
Fraction_Value
  in Ada.Characters.Latin_1 A.3.3(22)
Free
  in Ada.Strings.Unbounded A.4.5(7)
in Interfaces.C.Strings B.3.1(11)
freed
See nonexistent 13.11.2(10/4)
freening storage 13.11.2(1)
freezing
by a constituent of a construct 13.14(4/1)
by an expression 13.14(8/4)
by an implicit call 13.14(8.1/3)
by an object name 13.14(8/4)
class-wide type caused by the freezing of the specific type 13.14(15/5)
constituents of a full type definition 13.14(15/5)
designated subtype caused by an allocator 13.14(13)
entity 13.14(2)
entity caused by a body 13.14(3/5)
entity caused by a construct 13.14(4/1)
entity caused by a name 13.14(11)
entity caused by the end of an enclosing construct 13.14(3/5)
expression of an expression function by a call 13.14(10.1/4)
expression of an expression function by Access attribute 13.14(10.3/4)
extension of an expression function by an instantiation 13.14(10.2/4)
first subtype caused by the freezing of the type 13.14(15/5)
function call 13.14(14/3)
generic instantiation 13.14(5/3)
nominal subtype caused by a name 13.14(11)
object_declaration 13.14(6)
profile 13.14(2.1/3)
profile of a callable entity by an instantiation 13.14(10.2/4)
profile of a function call 13.14(10.1/4)
specific type caused by the freezing of the class-wide type 13.14(15/5)
subtype caused by a record extension 13.14(7)
subtype caused by an implicit conversion 13.14(8.2/1)
subtype caused by an implicit dereference 13.14(11.1/1)
subtypes of the profile of a callable entity 13.14(14/3)
type caused by a range 13.14(12)
type caused by an expression 13.14(10/5)
type caused by the freezing of a subtype 13.14(15/5)
freezing points
entity 13.14(2)
Friday
in Ada.Calendar.Formatting 9.6.1(17/2)
From_Big_Integer
in Ada.Numerics.Big_Numbers.Big_Integer 13.5.6(12/5), A.5.6(13/5)
From_Big_Real
in Ada.Numerics.Big_Numbers.Big_Real 13.5.7(13/5), A.5.7(14/5)
From_Entity
in Ada.Numerics.Big_Numbers.Big_Real 13.5.7(19/5)
From_String
in Ada.Numerics.Big_Numbers.Big_Real 13.5.6(15/5)
From_Universal_Image
in Ada.Numerics.Big_Numbers.Big_Real 13.5.7(16/5)
function_specification
used 4.1(2/5), P.1
function_definition
used 6.1(4/2), 6.8(2/4), P.1
G
function_specification
in Ada.Characters.Latin_1 13.7(19.8/6)
full access
object 6.8(2/5)
type 6.8(2/5)
full_conformance
for discrete subtype definitions 6.3.1(12/4)
for expressions 6.3.1(19)
for known_discriminant_parts 6.3.1(23)
for profiles 6.3.1(18/3)
required 3.10.1(4/3), 3.6(4/5), 6.7(2/1), 6.8(4/3), 7.8(9/5), 8.3(12.3/5), 8.5(5/3), 9.5(2/14), 9.5.2(16), 9.5.1(17), 10.1.3(11/5), 10.1.3(12)
full constant declaration 3.3.1(6/5)
corresponding to a formal object of mode in 12.4(10/2)
dereference 4.1.5(4/3)
function 1.3.2(1/5), 6.1(3.1/2)
generic instantiation 12.5(4)
generic actual type 12.5(4)
generic actual subtype 12.5(4)
generic contract/private type contract
achievement 12.3(11.5)
partial 3.2(49/3), 3.4(5.1/3), 3.7(10/3), 3.7(17/3), 3.9(1.3/2), 3.9.3(7/5), 3.9.4(17/2), 3.10(28.1/3), 3.10.2(283), 3.10.2(322/5), 4.1.6(9/5), 4.2.1(16/5), 4.3.5(13.6/5), 4.5.2(8/5), 4.6(17/2), 4.6(26/2), 4.6(24.17/4), 4.6(24.21/4), 4.6(26.24/5), 4.8(5.4/3), 4.8(5.6/3), 4.9(37/2), 6.1.1(17/2.4), 6.3.1(17.a), 6.4.1(5.4/4), 6.4.1(6.3/4), 6.5(20/2), 6.5.1(6/5), 7.8(8), 8.3(26/2), 8.3.1(7/2), 8.5.1(4.6/5), 8.5.1(5.1/5), 8.5.1(6/5), 8.5.4(3.2/3), 9.1(9.9/2), 9.4(11.13/2), 9.4(11.18/2), 9.5(17/3), 9.5.1(7/5), 9.5.2(13.4/2), 10.2(11.8/5), 10.2.1(11/5), 10.2.1(17/5), 12.4(8/5), 12.4(8/5), 12.6(8/3), 13.1(11.8/6), 13.1.2(3.1/3), 13.1.4(23/3), 13.1.2(49/4), B.3.3(10.3), C.3.1(7/3), D.2.1(12.5), E.2.3(15.1), F.4.1(5/4), 1.15(7.3/3), 1.15(14/12)
generic contract model 12.3(1.a/5)
generic contract/private type contract
analogy 7.3(19.a)
generic formal 12.1(9)
generic formal object 12.4(1)
generic formal package 12.7(1)
generic formal subprogram 12.6(1)
generic formal subtype 12.5(5)
generic formal type 12.5(5)
generic function 12.1(8/2)
generic instance 1.3.3(12/5)
generic package 12.1(8/2)
generic procedure 12.1(8/2)
generic subprogram 12.1(8/2)
generic unit 1.3.3(13/5), 12(1)
See also dispatching operation 3.9(1)
generic_actual_part 12.3(3)
used 12.3(2/3), 12.7(3/2), P.1
Generic_Array_Sort
child of Ada.Containers A.18.26(3/5)
generic association 12.3(4)
used 12.3(3), 12.7(3.1/2), P.1
Generic_Bounded_Length
Generic_Complex_Arrays
child of Ada.Numerics G.3.2(2/5)
Generic_Complex_Elementary_Functions
child of Ada.Numerics G.1.2(2/5)
Generic_Complex_Types
child of Ada.Numerics G.1.1(2/5)
Generic_Constrained_Array_Sort
child of Ada.Containers A.18.26(7/5)
generic declaration 12.1(2)
used 3.1(3/3), 10.1.1(5), P.1
Generic_Dispatching_Constructor
child of Ada.Tags 3.9(18.2/5)
Generic_Elementary_Functions
child of Ada.Numerics A.5.1(3/5)
generic_formal_declaration 12.1(6)
used 12.1(5), P.1
generic_formal_part 12.1(5)
used 12.1(3/3), 12.1(4), P.1
generic_instantiation 12.3(2/3)
used 3.1(3/3), 10.1.1(5), P.1
Generic_Graphic_Character
in Ada.Text_IO.A.3.2(23)
generic_formal_part 12.1(4)
used 12.1(2), P.1
Generic_Graphic_Character
child of Ada.Numerics G.3.1(2/5)
generic_renaming_declaration 8.5.5(2/3)
used 8.5(2), 10.1.1(6), P.1
Generic_Graphic_Character
in Ada.Containers.Doubly_Linked_Lists A.18.3(47/5)
in Ada.Containers.Vectors A.18.2(75/5)
generic_subprogram_declaration 12.1(3/3)
used 12.1(2), P.1
Get
in Ada.Strings.Text_Buffers.Unbounded A.4.12(20/5)
in Ada.Text_IO.Complex_IO G.1.3(6), G.1.3(8/5)
Get_CPU
in Ada.Interrupts C.3.2(10.1/3)
Get_CPU_Set
Get_Deadline
in Ada.Dispatching.EDF D.2.6(9/5)
Get_Dispatching_Domain
Get_First_CPU
Get_Immediate
in Ada.Text_IO A.10.1(44/5), A.10.1(45/5)
Get_Last_CPU
Get_Last_Release_Time
in Ada.Dispatching.EDF D.2.6(9/5)
Get_Line
in Ada.Text_IO A.10.1(49.1/5), A.10.1(49/5)
in Ada.Text_IO.Bounded_IO A.10.11(8/2), A.10.11(9/2), A.10.11(10/2), A.10.11(11/2)
Get_Next_Entry
in Ada.Directories A.16(35/2)
Get_Priority
in Ada.Dynamic_Priorities D.5.1(5)
Get_Relative_Deadline
in Ada.Dispatching.EDF D.2.6(9/5)
Get_UTF8
Global aspect 6.1.2(11/5), 6.1.2(16/5)
global to 8.1(15)
global variable set 6.1.2(24/5)
Global'Class aspect 6.1.2(15/5)
global_aspect_definition 6.1.2(2/5)
used 13.1.1(4/5), P.1
global_aspect_element 6.1.2(3/5)
used 6.1.2(2/5), P.1
global_designator 6.1.2(7/5)
used 6.1.2(2/5), P.1
global_mode 6.1.2(4/5)
used 6.1.2(2/5), 6.1.2(3/5), P.1
global_name 6.1.2(8/5)
used 6.1.2(6/5), 6.1.2(7/5), P.1
global_set 6.1.2(6/5)
used 6.1.2(3/5), P.1
Glossary N(1/5)
glyphs 2.1(15/a/5)
goto statement 5.8(2)
used 5.1(4/2), P.1
govern a variant 3.8.1(20)
govern a variant_part 3.8.1(20)
grand
ambiguous 1.1(4/1/5)
complete listing P.1(1/5)
cross reference P.2(1/3)
notation 1.1(4)3
resolution of ambiguity 1.1.4(14.a), 8.6(3)
under Syntax_heading 1.1.2(25)
graphic character
a category of Character A.3.2(23)
graphic symbols 2.1(15/a/5)
grahic_character 2.1(14/3)
used 2.1(2/2), 2.5(2), 2.6(3), P.1
Graphic_Set
in Ada.Strings.Maps.Consts A.4.6(4)
Grave
in Ada.Characters.Latin_1 A.3.3(13)
greater than operator 4.5(1), 4.5.2(1)
greater than or equal operator 4.5(1), 4.5.2(1)
greater-than_sign 2.1(15/5)
Greater Than_Sign
in Ada.Characters.Latin_1 A.3.3(10)
Greatest_Common_Divisor
in Ada.Numerics.Big_Numbers.Big_Integers A.5.6(19/5)
Group_Budget
Group_Budget_Error
in Ada.Execution_Time.Group_Budgets D.14.2(11/2)
Group_Budget_Handler
in Ada.Execution_Time.Group_Budgets D.14.2(5/2)
Group_Budgets
child of Ada.Execution_Time D.14.2(3/5)
GS
in Ada.Characters.Latin_1 A.3.3(6)
illegal
construct 1.1.2(27)
partition 1.1.2(29)

in Ada.Numerics.Generic_Complex_ -
Arrays  G.3.2(7/2), G.3.2(27/2)
in Ada.Numerics.Generic_Complex_ -
Types  G.1.1(6)

image
of a value  3.5(27.3/5), 3.5(30/5),
  4.10(1/5)
in Ada.Calendar.Formating
  9.6.1(35/2), 9.6.1(37/2)
in Ada.Numerics.Discrete_Random
  A.5.2(26)
in Ada.Numerics.Float_Random
  A.5.2(14)
in Ada.Task_Identification
C.7.1(3/5)
in Ada.Text_IO.Editing
 F.3.3(13)
in Ada.Numerics.Discrete_Random
  A.5.2(14)
in Ada.Numerics.Generic_Complex_ -
Types  G.1.1(4/5)

Imaginary subtype of Imaginary
in Interfaces.Fortran  B.5(10)
immediate scope
of (a view of) an entity  8.2(11)
of a declaration  8.2(2)
of a pragma  8.2(12/4)

Immediate_Reclamation restriction
H.4(10)
immediately enclosing  8.1(13)
immediately visible  8.3(4), 8.3(21)
immediately within  8.1(13)
immutably limited  7.5(8.1/3)
implementation  1.1.3(1a)
implementation advice  1.1.2(37)
summary of advice  M.3(1/5)
implementation defined  1.1.3(18)
summary of characteristics  M.2(1/5)
implementation permissions  1.1.2(36)
implementation requirements  1.1.2(33)
implementation-dependent
  See unspecific 1.1.3(18)
implemented
by a protected entry  9.4(11/3)
by a protected subprogram  9.4(11/3)
by a task entry  9.1(9/2)

implicit conversion
  legality 8.6(27.1/4)
implicit declaration  3.1.5
implicit initial values
for a subtype  3.3.1(10)
implicit subtype conversion  4.6(59),
  4.6(60)
Access attribute
  3.10.2(30/5)
access discriminant  3.7(27/2)
array bounds  4.6(38)
array index  4.1.1(7)
assignment to view conversion
  4.6(55/5)
assignment_statement  5.2(11/5)

in Ada.Containers.Ordered_Maps
  A.18.6(21/5)
in Ada.Containers.Hashed_Sets
  A.18.8(21/5)
in Ada.Containers.Hashed_Maps
  A.18.5(22/5)
in Ada.Containers.Ordered_Maps
  A.18.9(20/5)
in Ada.Containers.Discrete_Maps
  A.18.9(20/5)
in Ada.Containers.Discrete_Sets
  A.18.9(20/5)
in Ada.Vectors
  A.18.9(20/5)
in Ada.Collections
  A.18.9(20/5)
in Ada.Numerics.Generic_Complex_ -
Arrays  G.3.2(7/2), G.3.2(27/2)
in Ada.Numerics.Generic_Complex_ -
Types  G.1.1(6)

bounds of a decimal fixed point type
  3.5.9(16)
bounds of a fixed point type  3.5.9(14)
bounds of a range  3.5(9), 3.6(18)
choices of aggregate  4.3.3(22)
component defaults  3.3.1(13/5)
container_aggregate  4.3.5(54/6)
default value of a scalar
  3.3.1(11/5)
delay expression  9.6(20)
derived type discriminants  3.4(21)
discriminant values  3.7.1(12/5)
entry index  9.5.2(24/5)
expressions in aggregate  4.3.1(19/5)
expressions of aggregate  4.3.2(23)
function return  6.5(12/5), 6.5(6/2)
generic formal object of mode
  in 12.4(11)

inherited enumeration literal
  3.4(29)
initialization expression
  3.3.1(17/5)
initialization expression of allocator
  4.8(7/2)

Interrupt_Priority aspect
D.1(17/4),
D.3(6/1/3)

named number value
  3.3.2(6)
operand of concatenation  4.5.3(9)
parameter passing  6.4.1(10), 6.4.1(11),
  6.4.1(17)
pragma Interrupt_Priority
D.1(17/4),
D.3(6/1/3), D.3(9/2)
pragma Priority
D.1(17/4), D.3(6/1/3), D.3(9/2)

Priority aspect
D.1(17/4), D.3(6/1/3)
expression
  4.7(4/5)
result of inherited function
  3.4(27/2)
implicit Dereference aspect
  4.1(6)

used  4.1(4), P.1

Implicit_Dereference aspect
  4.1.5(2/3)
impliedly composed
aspect  13.1.1(18.3/5)
Import aspect
B.1(13/5)
Import pragma
B.1(5/3), J.15.5(2/3),
B.1(13/5)
imported
aspect
B.1(23/3)
imported entity
B.1(23/3)
in (membership test)
  4.5(1), 4.5(2/3)

In_Range
in Ada.Numerics.Big_Numbers.Big_Inte-
gers  A.5.6(10/5)
in Ada.Numerics.Big_Numbers.Big_Real
  A.5.7(12/5)
in Ada.Numerics.Big_Numbers.Big_Inte-
gers  A.5.6(10/5)
in Ada.Numerics.Big_Numbers.Big_Real
  A.5.7(12/5)
in Ada.Numerics.Generic_Complex_ -
Arrays  G.3.2(7/2), G.3.2(27/2)
in Ada.Numerics.Generic_Complex_ -
Types  G.1.1(6)
in Ada.Num.

immutably limited
  7.5(8.1/3)
immediately within
  8.1(13)
immediately visible
  8.3(4), 8.3(21)
immuntable limited
  7.5(8.1/3)
implementation
  1.1.3(1a)
implementation advice
  1.1.2(37)
summary of advice
  M.3(1/5)
implementation defined
  1.1.3(18)
summary of characteristics
  M.2(1/5)
implementation permissions
  1.1.2(36)
implementation requirements
  1.1.2(33)
implementation-dependant
  See unspecific 1.1.3(18)
implemented
  by a protected entry
  9.4(11/3)
  by a protected subprogram
  9.4(11/3)
  by a task entry
  9.1(9/2)
implied conversion
  legality
  8.6(27.1/4)
implied declaration
  3.1.5
implicit initial values
  for a subtype
  3.3.1(10)
implied subtype conversion
  4.6(59),
  4.6(60)
Access attribute
  3.10.2(30/5)
access discriminant
  3.7(27/2)
array bounds
  4.6(38)
array index
  4.1.1(7)
assignment to view conversion
  4.6(55/5)
assignment_statement
  5.2(11/5)
incompatibilities with Ada 2022
1.1.2(40.c/6), 4.3.5(92.c/6),
4.5(12.b/6), 5.5.2(17.j/6),
13.11(39.t/6)
incompatibilities with Ada 83 1.1.2(40.e),
2.9(19.e), 2.9(3.a), 3.2(2.15.a),
3.2(38.a), 3.4(38.b), 3.5(63.a/1),
3.5(211.b), 3.6(8.b), 4.2(14.a),
4.3(34.9.a/1), 4.5(35.1/2),
4.6(71.a), 4.8(20.a/1), 4.9(44.m),
5.4(18.a.1/1), 6.3(7.a.3), 6.5(28.a/2),
7.1(17.a.5), 8.6(34.a), 12.3(29.b),
12.5(1.28.a), 12.5(3.16.a),
12.5(4.13.a), 13.1(29.a), 13.1(42.a),
A.5(3.72.d), A.5(4.4.a), A.8(17.a),
A.10(1.86.a), C.6(26.b), J.15(1.6.a/3)
incompatibilities with Ada 95
1.1.2(40.p/2), 2.9(3.c/2), 3.7(15.c/2),
3.9(33.d/3), 3.9(234.b/2), 3.10(26.e/2),
3.10(1.23.h/2), 3.10.2(11.b/2),
4.3(86.f/2), 4.3(23.13.b/2), 4.5(35.2.d/2),
4.6(71.2/2), 4.8(20.2/2), 5.2(92.d/2),
6.5(28.g/2), 8.3(29.s/2), 8.5(10.b/2),
8.6(34.n/2), 9.7(2.7.b/3),
10.1(2.23.2/2), 10.2(28.2/2),
11.4(1.2.e/3), 13.5(3.32.d/2),
13.5.2(25.c/2), 13.11(43.d/2),
13.11.9(3.b/3), 13.14(20.p/2),
13.14(20.t/3), A.4(1.6.a/3),
A.4(3.109.a), A.4(4.106.f/3),
A.5(88.b/2), A.5(479.a/2),
A.5(2.62.a/2), A.8(17.2/b),
A.8(4.20.a/2), A.10(1.86.c/2),
A.10(26.a/3), A.12(1.36.b/2),
B.3(34.a/3), C.3(25.a/2), D.7(22.a/2),
D.8(31.a/3), E.2(20.b/3),
E.2(320.b/3), E.5(30.a/2)
incompatibilities with Ada 2012
7.3.2(41.h/5), D.2.6(34.c/5)
incomplete type 1.3.1(35/5), 3.2(4.1/2),
3.10.1(1.2/4), 3.10.1(1.1/2)
incomplete view 1.3.1(37/5),
3.10.1(2.1/4)
tagged 3.10.1(2.1/4)
used 3.2.1(2), P.1
inconsistencies with Ada 2005
1.1.2(40.z/3), 2.1(19.g/3), 3.5(63.l/3),
3.9(33.i/3), 4.3.2(13.d/3), 4.3.3(49.l/3),
4.5(239.i/3), 4.6(71.u/3),
4.6(19.d/3), 6.5(28.n/3),
7.6(24.c/3), 8.5(421.f/1.3),
9.6(191.c/3), 13.3(66.l/3),
A.10(5.52.a/3), A.10.8(27.a/3),
A.16(131.d/3), A.18.3(164.b/3), D.14.2(38.b/3)
inconsistencies with Ada 2012
1.1.2(40.mm/5), 3.2.4(52.c/5),
3.3.1(33.n/5), 3.10.2(41.a/5),
4.5(49.k/4), 4.4(15.f/4),
4.5.3(39.p/4), 4.7(10.b/5),
6.1(144.b/4), 6.4.1(19.k/5),
6.5(28.s/5), 7.3.2(41.b/4), 8.6(34.y/4),
9.5(72.d/5), 9.5(420.c/4),
9.6.1(91.c/5), 12.5(16.j/5),
13.11.2(19.e/4), A.18.2(264.1/5),
A.18.3(164.m/5), A.18.4(84.k/5),
A.18.7(105.k/5), A.18.10(233.d/5),
A.18.15(5.4/4), A.18.16(5.e/4),
A.18.17(12.b/4), A.18.18(74.c/4),
A.18.19(17.b/5), A.18.20(20.b/5),
A.18.21(22.b/5), A.18.22(19.b/5),
A.18.25(20.b/5), A.19(12.c/4),
C.3(1.25.f/5), C.6(26.j/5),
D.2(1.17.d/5), D.16.1(34.c/4)
inconsistencies with Ada 2012
1.1.2(40.22/6), 4.3.3(49.r/6),
4.4(92.b/6)
inconsistencies with Ada 83 11.2(40.b/6),
3.4(38.a), 3.5.2(11.a), 3.5.7(22.a),
3.5.9(28.a), 3.6.3(8.a), 3.7.1(15.a),
4.3(14.a), 4.5.6(13.1.a/1), 9.6(40.a),
11.1(8.a), 12.3(29.a), 13.8(51.a/2),
A.6(1.a), G.2(1.16.c), G.2(27.b)
inconsistencies with Ada 95
1.1.2(40.m/2), 3.3.1(33.f/2),
3.5.2(11.h/2), 3.6.3(8.g/2), 3.9(33.b/2),
3.10(26.c/3), A.12.3(36.b/2),
B.3(34.a/3), C.3(25.a/2), D.7(22.a/2),
D.8(31.a/3), E.2(20.b/3),
E.2(320.b/3), E.5(30.a/2)
Index
Index attribute 6.1.1(30.2/5)
index parameter
of an array aggregate 4.3.3(6.5/1),
range 3.6(13)
index subtype 3.6(9)
index type 3.6(9)
container aggregate 4.3.5(25/5),
indexed aggregate 4.3.5(25/5)
Index_Check 11.5(14)
[partial] 4.1(17), 4.1.2(7),
4.3.3(20.4/6), 4.3.3(29.3), 4.3.3(30),
4.3.4(20.5), 4.5.3(8), 4.6(51.5),
4.7(4/5), 4.8(10/2)
index_constraint 3.6(1.2)
used 3.2.2(7), P.1
Index_Error
in Ada.Strings.A.4.(1/5)
Index_Non Blank
in Ada.Strings.Bounded A.4.4(46.1/2),
A.4.4(47)
in Ada.Strings.Fixed A.4.3(11.2/2),
A.4.3(12)
in Ada.Strings.Unbounded
A.4.5(41.1/2), A.4.5(42)
index_subtype_definition 3.6(4)
used 3.6(3), P.1
indexable container object 4.1.6(5/3),
indexable container type 1.3.1(39/5),
4.1.6(5/3)
indexed aggregate 4.3.5(25/5)
indexed_component 4.1.1(2)
used 4.1(2.5), P.1
indexing
constant 4.1.6(12/3)
variable 4.1.6(16/3)
individual membership test 4.5.2(26.1/3)
divisible 4.6(10/4)
inferable discriminants 14.3.3(20.2)
Information
child_of 16.12(4/2)
child_of 16.12(2/5)
child of Ada.Wide_Wide_Directories
A.16.2(3/5)
information hiding
See package 7(1)
See private types and private extensions
7.3(1)
information systems  C(1), F(1)
informative 1.1.2(18)
inhertibly mutable object  3.3(13/3)
inheritance
See derived types and classes  3.4(1/2)
See also tagged types and type
extension 3.9(1)
inherted
from an ancestor type  3.4.1(11)
inherted component  3.4(11), 3.4(12)
inherted discriminant  3.4(11)
inherted entry 3.4(12)
inherted protected subprogram  3.4(12)
inherited subprogram 3.4(17/2)
initailized by default  3.3.1(18/2)
initialize
of an object  3.3.1(18/2), 3.3.1(19/2)
of a task object  9.1(12/1), J.7.1(7)
of a protected object  C.3.1(10/3),
of a protected object  9.4(14)
initialization
Initial_Directory
in
Ada.Directories.Hierarchical_File_Na
mes A.16.1(12/3)
initialization
of a protected object  9.4(14)
of a protected object  C.3.1(10/3),
C.3.1(11/3)
of a task object  9.1(12/1), J.7.1(7)
of an object  3.3.1(18/2), 3.3.1(19/2)
initialization expression 3.3.1(1/3),
3.3.1(4)
Initilize 7.6(2)
in Ada.Finalization 7.6(6/2), 7.6(8/2)
initialized allocator 4.8(4)
initialized by default 3.3.1(18/2)
Inline aspect 6.3.2(5.1/3)
Inline pragma 6.3.2(3/3), J.15.1(2/3),
L(15.1/3), L(15/3)
innermost dynamically enclosing 11.4(2)
input A.6(1/5)
Input aspect 13.13.2(38/5)
Input attribute 13.13.2(22), 13.13.2(32)
Input clause 13.3(7/2), 13.13.2(38/5)
InputClass aspect 13.13.2(38/5)
input-output
specified for access types A.7(6)
Insert
in Ada.Containers.Doubly_Linked_-
Lists A.18.3(19/5), A.18.3(20/5),
A.18.3(21/5)
in Ada.Containers.Hashed_Maps
A.18.5(19/5), A.18.5(20/5),
A.18.5(21/5)
in Ada.Containers.Hashed_Sets
A.18.8(19/5), A.18.8(20/5)
in Ada.Containers.Ordered_Maps
A.18.6(18/5), A.18.6(19/5),
A.18.6(20/5)
in Ada.Containers.Ordered_Sets
A.18.9(18/5), A.18.9(19/5)
in Ada.Containers.Vectors
A.18.2(36/5), A.18.2(37/5),
A.18.2(38/5), A.18.2(39/5),
A.18.2(40/5), A.18.2(41/5),
A.18.2(42/5), A.18.2(43/5)
in Ada.Strings.Bounded
A.4.4(60), A.4.4(61)
in Ada.Strings.Fixed
A.4.3(25), A.4.3(26)
in Ada.Strings.Unbounded
A.4.5(55), A.4.5(56)
Insert.Child
in Ada.Containers.Multiway_Trees
A.18.10(48/5), A.18.10(49/5),
A.18.10(50/5)
Insert.Space
in Ada.Containers.Vectors
A.18.2(48/5), A.18.2(49/5)
Insert.Vector
in Ada.Containers.Vectors
A.18.2(36/5), A.18.2(37/5),
A.18.2(38/5)
sanctifiable object H.3.2(5/2)
inspecion point H.3.2(5/2)
Inspection_Point pragma
H.3.2(3), L(16)
instance
of a generic function 12.3(13)
of a generic package 12.3(13)
of a generic procedure 12.3(13)
of a generic subprogram 12.3(13)
of a generic unit 12.3(1)
instructions for comment submission
0.2(57.22/5), 0.2(58/5)
int
in Interfaces.C  B.3(7)
Integer 3.5.4(11), 3.5.4(21)
in Standard A.1(12)
teger literal 2.4(1)
teger literals 3.5.4(14), 3.5.4(30)
teger type 1.3.1(40/5), 3.5.4(1)
teger Address
in System.Storage_Elements
13.7.1(10/3)
Integer.Arithmetic
child of System.Atomic_Operations
C.6.4(3/5)
Integer.IO
in Ada.Text.IO
A.10.1(52)
Integer.Literal_aspect
4.2.1(3/5)
Integer.N  B.2(8)
Integer.Text.IO
child of Ada.A.10.8(21)
teger_type_definition 3.5.4(2)
userd 3.2.1(42), P.1
Integer.Wide_Text.IO
child of Ada.A.11(2/2), A.11(3/2)
Integer.Wide_Text.IO
child of Ada.A.11(3/2)
interaction
between tasks 9.1(5)
interface 3.9.4(2)
limited 3.9.4(5/2)
nonlimited 3.9.4(5/2)
protected 3.9.4(5/2)
synchronized 3.9.4(5/2)
task 3.9.4(5/2)
type 3.9.4(4/2)
terface to assembly language C.1(4/3)
terface to C B.3(1/4)
terface to COBOL B.4(1/3)
terface to Fortran B.5(1/3)
terface to other languages B(1)
terface type 1.3.1(42/5)
terface Ancestor Tags
in Ada.Tags 3.9(7.4/2)
terface_list 3.9.4(3/2)
used 3.4(2/2), 3.9.4(2/2), 7.3(3/3),
12.5.1(3/5), P.1
interfacer_type_definition 3.9.4(2/2)
used 3.2.1(42), 12.5.5(2/2), P.1
Interfacer 2.3(5/5)
Interfacer.C  B.3(4/5)
Interfacer.C.Pointers  B.3.2(4/5)
Interfacer.C.Strings  B.3(1/3)
Interfacer.COBOl  B.4(7/5)
Interfacer.Fortran  B.5(4/5)
Interfacer_Assertion_Check
11.5(23.7/5)
terfacing aspect B.1(0.1/3)
terfacing pragma B.1(4/3), J.15.5(1/3)
Convention B.1(4/3), J.15.5(1/3)
Export B.1(4/3), J.15.5(1/3)
Import B.1(4/3), J.15.5(1/3)
internal call 9.5(3/3)
internal code 13.4(7)
internal node
of a tree A.18.10(2/4)
internal requeuf 9.5(7)
Internal_Tag
in Ada.Tags 3.9(7/2)
terpretation
of a complete context 8.6(10)
of a constituent of a complete context
8.6(15)
overload resolution 8.6(14)
terrupt C.3(2)
example using asynchronous select
9.7.4(10), 9.7.4(12)
terrupt entry J.7.1(5)
terrupt handler C.3(2)
terrupt.Clocks_Supported
in Ada.Execution_Time
D.14(9.1/3)
terrupt_Handler aspect
C.3.1(6.2/3)
terrupt_Handler pragma
C.3.1(2/3),
J.15.7(2/3), L(17.1/3), L(17/3)
terrupt_Id
in Ada.Interrupts C.3.2(2/5)
terrupt.Priority aspect
D.1(6.3/3)
terrupt.Priority pragma
D.1(5/3),
J.15.11(4/3), L(18.3/3), L(18/3)
terrupt.Priority.subtype of Any_Priority
in System 13.7(16)
terrupts
child of Ada C.3.2(2/5)
child of Ada.Execution_Time
D.14.3(3/5)
lifetime 3.10.2(3/5)
limited interface 3.9.4(5/2)
limited type 1.3.1(46/5), 7.5(3/3)
becoming nonlimited 7.3.1(5/1), 7.5(16)
immutably 7.5(8.1/3)
limited view 10.1.1(12.1/2)
Limited_Controlled
in Ada.Finalization 7.6(7/5)
limited with clause 10.1.2(4/1)
used 10.1.2(4/2), P.1
line 2.2(2/3)
in Ada.Text_IO A.10.1(38/5)
line terminator A.10.7
Line_Length
in Ada.Text_IO A.10.1(25/5)
link name B.1(35)
link-time error
See post-compilation error 1.1.2(29)
See post-compilation error 1.1.5(4)
Link_Name aspect B.1(1/3)
Linker_Options pragma B.1(8), L(19)
linking
See partition building 10.2(2/5)
List
in Ada.Containers.Doubly_Linked - Lists A.18.3(6/5), A.18.3(51.2/5)
list container A.18.3(1/2)
List pragma 2.8(21), L(20)
List_Iterator Interfaces
in Ada.Containers.Doubly_Linked - Lists A.18.3(9.3/3), A.18.3(51.7/5)
literal 4.2(1)
  based 2.4.2(1)
  decimal 2.4.1(1)
  numeric 2.4(1)
  See also aggregate 4.3(1)
  See also_bit 4.3(1)
  See also_handle 4.3(1)
  See also_identifier_letter 2.1(9/2)
  See also_ordinal 4.3(1)
  See also_ordinal_indicator 4.3(1)
  See also_partition 10.2(2/5)
  See also_partition subprogram 10.2(2/5)
  See also_partition type 10.2(2/5)
  See also_partition_type 10.2(2/5)
  See also_partition_var 10.2(2/5)
  See also_partitioning 10.2(2/5)
load time C.4(1)
local to 8.1(14)
Local_Image
in Ada.Calendar.Formating 9.6.1(35.1/5)
local_name 13.1(3)
Local_Time_Offset
  in Ada.Calendar.Time_Zones 9.6.1(6/5)
  locale A.19(1/3)
  active A.19(8/3)
Locales
child_of Ada A.19(3/5)
localization 3.5.2(6/2), 3.5.2(7/2)
lock-free C.6.1(5/5)
locking policy D.3(6/2)
Ceiling_Locking D.3(7)
Locking_Policy pragma D.3(3), L(21)
Log
Logical
in Interfaces.Fortran B.5(7)
logical operator 4.5.1(2)
See also not operator 4.5.6(3)
logical thread of control 1.3.4(9/5), 9(1/5)
logical_operator 4.5(2)
long
in Interfaces.C B.3(7)
Long_Binary
in Interfaces.COBOL B.4(10)
long_double
in Interfaces.C B.3(17)
Long_Float
3.5.7(15), 3.5.7(16/5), 3.5.7(17)
Long_Floating
in Interfaces.COBOL B.4(9)
Long_Integer
3.5.4(22), 3.5.4(25), 3.5.4(28)
Look_Ahead
in Ada.Text_IO A.10.1(43/5)
loop
parallel 5.5(8/5)
sequential 5.5(9/5)
loop_body procedure 5.5.3(15/5)
loop_curisor 5.5.2(12/5)
loop_iterator 5.5.2(10/5)
container_element_iterator 5.5.2(12/5)
loop_parameter 5.6(6/5), 5.5.2(7/5)
loop_parameter_specification 5.4(5)
used 4.3.5(21/5), 4.5.8(3/1), 5.5.3(5), P.1
loop_parameter_subtype_indication 5.5.2(2.1/5)
used 5.5.2(2/5), P.1
loop_statement 5.5.2
used 5.1(5/5), P.1
low line 2.1(15/5)
low-level_programming C(1)
Low_Line
in Ada.Characters.Latin_1 A.3.3(12)
Low_Order_First 13.5.3(2)
in Interfaces.COBOL B.4(25)
in System 13.7(15/2)
lower bound
of a range 3.5(4)
lower-case letter
a category of Character A.3.2(25)
lower_case_identifier_letter 2.1(9/2)
Lower_Case_Map
in Ada.Strings.Maps.Constants A.4.6(5)
Lower_Set
in Ada.Strings.Maps.Constants A.4.6(4)
LR(1) 1.1.4(14.a)
M
Machine attribute A.5.3(60)
machine code insertion 13.8(1), C.1(2/5)
machine numbers
of a fixed point type 3.5.9(8/2)
of a floating point type 3.5.7(8)
machine scalar 13.8(1/3)
Machine_Code
See child of System 13.8(7)
Machine_Emax attribute A.5.3(8)
Machine_Emin attribute A.5.3(7)
Machine_Mantissa attribute A.5.3(6)
Machine_Overflows attribute A.5.3(12), A.5.4(4)
Machine_Radix aspect F.1(1/5)
Machine_Radix attribute A.5.3(2), A.5.4(2)
Machine_Radix clause 13.7(2/2), F.1(1/5)
Machine_Rounding attribute A.5.3(41.1/2)
Machine_Rounds attribute A.5.3(11), A.5.4(3)
macro
See generic unit 12(1)
Macron
in Ada.Characters.Latin_1 A.3.3(21/3)
main subprogram
for a partition 10.2(7)
malloc
See allocator 4.8(1)
Map
in Ada.Containers.Ordered_Maps A.18.6(4/5), A.18.6(51.4/5)
map container A.18.4(1/2)
Map_Iterator Interfaces
in Ada.Containers.Ordered_Maps A.18.6(7.3/5), A.18.6(51.9/5)
Maps
child of Ada.Strings A.4.2(3/5)
mark_non_spacing 2.1(9.4/2), 2.1(9.5/2)
used 2.3(1.3/3), P.1
mark_spacing_combining
used 2.3(1.3/3), P.1
marshalling E.4(9)
Masculine_Ordinal_Indicator
in Ada.Characters.Latin_1 A.3.3(22)
master 1.3.4(10/5), 7.6.1(3/5)
Multiplying_operator   4.5(6)
multiplying operator   4.5.5(1)
multiply operator   4.5(1), 4.5.5(1)
multiply   2.1(15/5)
Notwithstanding 3.10(21.1/5),
nonstandard mode 1.1.5(11),
normal completion 7.6.1(2/2),
normal library unit E.2(4/3),
nonoverridable aspect 13.1.1(18,3/5),
not equal operator 4.5(1), 4.5.2(1),
null pointer .See null access value 4.2(9/5),
null procedure 6.7(3/5),
normally becoming nonlimited 7.3.1(5/1), 7.5(16),
nonstandard type 1.3.1(50/5), 7.5(7),
null array 3.6.1(7),
null exception 3.9.1(4/1/2),
null range 3.5(4),
normative 1.1.2(14),
normal state of an object 11.6(6/5), 11.7(1/4),
null access value 4.3.3(3/1/5),
null_record 3.8(1/5),
normal library unit E.2(4/3),
normal completion 7.6.1(2/2),
null procedure declaration 6.7(2/3),
null_range 3.5(4),
normal completion 7.6.1(2/2),
normal library unit E.2(4/3),
normal state of an object 11.6(6/5), 13.9(1/4),
null_char 4.5(1), 4.5.2(3),
null_char 4.5(1), 4.5.2(3),
null_char 4.5(1), 4.5.2(3),
noretical item 13.1(18,2/5),
representation aspect 13.1(18,2/5),
representation item 13.1(18,2/5),
representation value 13.1(18,2/5),
nonoverridable aspect 13.1.1(18,3/5),
nonoverridable aspect 13.1.1(18,3/5),

Index
precondition check
  class-wide 6.1.1(33/3)
specific 6.1.1(32/3)
precondition expression
  class-wide 6.1.1(3/5)
specific 6.1.1(2/5)
Pred attribute 3.5(25)
predecessor element
  of an ordered set A.18.9(81/3)
  of an ordered map A.18.6(58/3)
predefined environment A(1)
prefixed view profile A.18.10(67.1/5)
prefixed view A.18.9(47.1/5)
predicate-static 3.2.4(15/3)
predicate specification 3.2.4(1/5)
object_declaration 3.2.4(31/5)
in out parameters 3.2.4(31/5)
enabled 3.2.4(7/3)
procedure instance 12.3(13)
null 6.7(3/5)
procedure instance 12.3(13)
procedure_call_statement 6.4(2)
used 5.1(4/2), 9.7(3.1/2), P.1
procedure_or_entry_call 9.7(3.1/2)
used 9.7(3/2), 9.7(4/2), P.1
procedure_specification 6.1(4/2)
used 6.1(4/2), 6.7(2/3), P.1
processing node Et(2)
profile 6.1(22)
associated with a dereference 4.1(10)
fully conformant 6.3(18/3)
mode conformant 6.3(116/3)
No_Implementation_Extensions 13.12(10/3)
subtype conformant 6.3(17/3)
type conformant 6.3(15/2)
preempted task D.2.1(7/5)
preemptible resource D.2.1(7/5)
preference
  for root numeric operators and ranges 8.6(29)
  for universal access equality operators 8.6(29/1/3)
preference control See requeue 9.5.4(1)
prefix 4.1(4)
of a prefixed view 4.1.3(9.2/3)
used 4.1.1(2), 4.1.2(2), 4.1.3(2),
  4.1.4(2), 4.1.4(4), 4.1.6(10/3),
  4.5.10(2/5), 5.5.3(4/5), 6.4(2), 6.4(3), P.1
prefix view 4.1.3(9.2/3)
prefix view profile 6.3.1(24.1/2)
Prepend
  in Ada.Containers.Doubly_Linked_Lists A.18.3(22/5)
in Ada.Containers.Vectors A.18.2(44/5)
Prepend_Child
  in Ada.Containers.Multiway_Trees A.18.10(51/5)
Prepend_Vector
  in Ada.Containers.Vectors A.18.2(44/5)
prescribed result
  for the evaluation of a complex arithmetic operation G.1.1(42)
  for the evaluation of a complex elementary function G.1.2(35)
  for the evaluation of an elementary function A.5.1(37)
Previous
  in Ada.Containers.Doubly_Linked_Lists A.18.3(38.1/5), A.18.3(38/5),
  A.18.3(40.1/5), A.18.3(40/5)
in Ada.Containers.Ordered_Maps A.18.6(36.1/5), A.18.6(36/5),
  A.18.6(37.1/5), A.18.6(37/5)
in Ada.Containers.Ordered_Sets A.18.9(47.1/5), A.18.9(47/5),
  A.18.9(48.1/5), A.18.9(48/5)
in Ada.Containers.Vectors A.18.2(65.1/5), A.18.2(65/5),
  A.18.2(66.1/5), A.18.2(66/5)
in Ada.Iterator_Interfaces 5.5.1(4/3)
Precedent_Sibling
  in Ada.Containers.Multiway_Trees A.18.10(66.1/5), A.18.10(66/5),
  A.18.10(67.1/5), A.18.10(67/5)
  primary 4.4(7/5)
  used 4.4(6), P.1
primitive
  by-reference 13.10(5)
  for root numeric operators and ranges 8.6(9)
  for universal access equality operators 8.6(9/1/3)
priority aspect D.1(15/5)
priority attribute D.5.2(3/2)
priority inheritance D.1(15/5)
priority inversion D.2.2(14/2), D.2.3(11/2)
priority of an entry call D.4(9)
priority pragma D.1(3/3), J.15.11(2/3),
  L(27/3), L(27/3)
Priority subtype Any_Priority
  in System 13.7(16)
Priority_Queueing queueing policy D.4(8)
Priority_Specific_Dispatching pragma
  D.2.2(2/2), L(27/2)
private declaration of a library unit
  10.1.1(2)
private descendant
  of a library unit 10.1.1(12)
private extension
  1.3.1(60/5), 3.2.4(1/2),
  3.2(4/2), 3.9(2.1/2), 3.9(2/2), 3.9.1(1/2)
  [partial] 7.3(14), 12.5.1(5/3)
private library unit 10.1.1(12)
private operations 7.3.1(1)
private part 8.2(5)
  of a package 7.1(6/2), 12.3(12b)
  of a protected unit 9.4(11/2)
  of a task unit 9.1(9)
private type
  1.3.1(61/5), 3.2(4.1/2), 3.2(4/2)
  [partial] 7.3(14)
private types and private extensions
  7.3(1)
private with_clause 10.1.2(4.b/2)
predicate
  membership 4.5.2(29/4)
  of a subtype 3.2.4(6/4)
  used 4.5.8(1/3), P.1
  predicate aspect 3.2.4(1/5)
predicate check
  allocator 3.2.4(31/5)
  enabled 3.2.4(7/3)
in out parameters 3.2.4(31/5)
object_declaration 3.2.4(31/5)
subtypes conversion 4.6(5/1)
predicate evaluated
  membership 4.5.2(29/4)
  Valid attribute 13.9.2(3/4), K.2(263/4)
  predicate specification 3.2.4(1/5)
predicate-static 3.2.4(15/3)
Predicate_Failure aspect 3.2.4(14.2/4)
predicates satisfied 3.2.4(29/2/4)
predicates satisfied required
  membership 4.5.2(29/4)
  Valid attribute 13.9.2(3/4), K.2(263/4)
preelaborable
  of an elaborable construct 10.2.1(5)
  preelaborable initialization 10.2.1(11.1/5)
Preelaborable_Initialization attribute 10.2.1(11.7/5)
Preelaborable_Initialization pragma
  10.2.1(4.2/5), J.15.14(4/5), L(25.2/5), L(25/3/5)
Preelaborate aspect 10.2.1(11/5)
Preelaborate pragma
  10.2.1(3/5), J.15.14(3/5), L(26.1/5), L(26/5)
preelaborated 10.2.1(11/5)
  [partial] 10.2.1(11/5), E.2.1(9)
implementation requirements C.4(2)
Profile pragma 13.12(11/3), D.13(3/3),
  L(27/3), L(27/4/3)
profile resolution rule
name with a given expected profile
8.6(26)
progenitor 1.3.1(63/5)
progenitor subtype 3.9.4(9/2)
program 1.3.3(31/5), 10.2(1)
program execution 10.2(1)
program library
See library 10(2)
See library 10.1.4(9/5)
program unit 1.3.3(32/5), 10.1(1)
program unit pragma 10.1.5(2/5), 10.1.5(2/5)
Convention B.1(29/3)
Export B.1(29/3)
Import B.1(29/3)
In line 6.3.2(2/3), 15.1(1/3)
library unit pragma 10.1.5(7/5), 10.1.5(7/5)
program-counter-counter approach to finalization 7.6.1(24.s)
Program Error
raised by a nonreturning procedure 6.5.1(9/2)
raised by Address of an intrinsic subprogram 13.3(11.1/3)
raised by barrier failure 9.5.3(7/3)
raised by closed alternatives 9.7.1(21)
raised by detection of a bounded error
raised by detection of a bounded error
9.5.5(5/5)
raised by failed finalization 7.6.1(15), 7.6.1(16/5), 7.6.1(17), 7.6.1(17.1/3), 7.6.1(17.2/1), 7.6.1(18/2)
raised by failure of runtime check
3.2.4(29).1/4, 3.2.4(33/4), 3.10.2(29), 3.11(14), 4.6(57.5), 4.8(10.1/3), 4.8(10.2/2), 4.8(10.3/2), 4.8(10.4/3), 5.5.8(1.5), 5.6.1(4.5), 6.4.1(13.4/5), 6.5(8/5), 6.5(20/2), 6.5(21/3), 7.6.1(20/8), 9.5.4(7.2/5), 11.1(4), 11.5(8.4a), 11.5(19/5), 12.5.1(23.3/2), 13.3(75.1/3), 13.11.4(27.3), 13.11.4(30.3), B.3.3(22/2), C.3.1(10/3), C.3.1(11/3), C.3.1(13.1/5), C.3.2(20), D.3(13), D.3(13.5/5), D.4(22/5), D.4(23/5), D.5.2(6/3), D.7(7.1/3), D.7(10.5/3), D.7(19.1/2), E.4(18.1), H.4(23.11.5), J.17(7)
raised by finalization of a protected object
9.4(20)
raised for missing return statement
6.4(11/2)
in Standard A.1(46)
Program_Error
raised by program unit pragma 10.1.5(7/5), 10.1.5(7/5)
raised by program pragma 1.3.3(31/5), 10.2(1)
raised by property of runtime check
11.4(1)
protected unit 9.4.1(1)
protected_body 9.4.7(3)
used 3.11(6), P.1
protected_body_stub 10.1.3(6/3)
used 10.1.3(2), P.1
protected definition 9.4(4)
used 9.4(2/3), 9.4(3/3), P.1
protected element declaration 9.4(6)
used 9.4(4), P.1
protected operation declaration 9.4(5/1)
used 9.4(4), 9.4(6), P.1
protected_operation_item 9.4(8/4)
used 9.4(7/3), P.1
protected_type declaration 9.4(2/3)
used 3.2(1.3/3), P.1
protect_t
in Interfaces.C B.3(12)
PJU
in Ada.Characters.Latin_1 A.3.3(18)
PJU2
in Ada.Characters.Latin_1 A.3.3(18)
public declaration of a library unit 10.1.1(12)
public descendant of a library unit 10.1.1(12)
public library unit 10.1.1(12)
punctuation connector 2.1(10.2/2)
used 2.3(3/1), P.1
pure 10.2.1(15.1/5), 10.2.1(16/2)
Pure aspect 10.2.1(17/5)
Pure pragma 10.2.1(14/5), J.15.14(5/5), L(28.1/5), L(28/5)
pure-barrier-barrier D.7(1.1/5)
Pure_Bars restriction D.7(10.11/5)
Put
in Ada.Strings.Text_Buffers A.4.12(7/5)
in Ada.Text_IO.Bounded_IO A.10.11(4/2), A.10.11(5/2)
in Ada.Text_IO.Complex_IO G.1.3(7), G.1.3(8/5)
in Ada.Text_IO.Editing F.3.3(14/5), F.3.3(15/5), F.3.3(16)
in Ada.Text_IO.Unbounded_IO A.10.12(4/2), A.10.12(5/2)
Put_Image
in Ada.Numerics.Big_Numbers.Big_Integers A.5.6(17/5)
in Ada.Numerics.Big_Numbers.Big_Real s A.5.7(20/5)
Put_Image_aspect 4.10(4/5)
Put_Image_attribute 4.10(3/5)
Simple_Bars   D.7(10.12/5)
Restrictions pragma   13.12(3), L(32)
Result attribute   6.1.1(29/5)
result interval   for a component of the result of evaluating a complex function
G.2.6(3/5)
for the evaluation of a predefined arithmetic operation
G.2.1(8)
for the evaluation of an elementary function
G.2.4(2)
result
of a Random function A.5.2(40.2/5)
result subtype   of a function 6.5(3/5)
return expression   6.5(3.5/5)
of expression function   6.8(3.1/5), 6.8(6/5)
return object
extended_return_statement   6.5(11/5)
simple_return_statement   6.5(6/2)
return_statement   6.5(1/2)
return-by-reference type   6.5(11/2)
return
used   5.1(4/2), P.1
return subtype indication   6.5(2.3/2)
used   6.5(2.1/5), 6.5(2.2/3), P.1
returns a readable reference   H.4(23.7/5)
returns a writable reference   H.4(23.7/5)
reverse iterator   5.5.2(4/5)
returns a writable reference   H.4(23.7/5)
returns a readable reference   H.4(23.7/5)
Reverse_Element
in Ada.Containers.Doubly_Linked_Lists   A.18.3(27/5)
in Ada.Containers.Vectors   A.18.2(54/5)
Reverse_Find
in Ada.Containers.Doubly_Linked_Lists   A.18.3(42/5)
in Ada.Containers.Vectors   A.18.2(70/5)
Reverse_Find_Index
in Ada.Containers.Vectors   A.18.2(69/2)
Reverse_Iterate
in Ada.Containers.Doubly_Linked_Lists   A.18.3(46/5)
in Ada.Containers.Ordered_Maps   A.18.6(51/5)
in Ada.Containers.Ordered_Sets   A.18.9(61/5)
in Ada.Containers.Vectors   A.18.2(74/5)
Reverse_Iterate_Children
in Ada.Containers.Multiway_Trees   A.18.10(69.1/5), A.18.10(69/5)
Reverse_Solidus
in Ada.Characters.Latin_1   A.3.3(12)
reversible iterable container object   5.5.1(11/5)
reversible iterable container type   5.5.1(11/5)
reversible iterator object   5.5.1(6/5)
reversible iterator type   5.5.1(6/5)
reversible iterator type   5.5.1(6/5)
Reversible_Iterator
in Ada.Iterator_Interfaces   5.5.1(4/3)
Reviewable pragma   H.3.1(3), L(33)
Reverse in Ada.Characters.Latin_1   A.3.3(17)
right curly bracket   2.1(15/5)
right parenthesis   2.1(15/5)
right square bracket   2.1(15/5)
Right_Angle_Quotation
in Ada.Characters.Latin_1   A.3.3(22)
Right_Curly_Bracket
in Ada.Characters.Latin_1   A.3.3(14)
Right_Parenthesis
in Ada.Characters.Latin_1   A.3.3(8)
Right_Square_Bracket
in Ada.Characters.Latin_1   A.3.3(12)
Ring_Above
in Ada.Characters.Latin_1   A.3.3(22)
ripple effect   10.1.2(1.b/2)
root of a tree   A.18.10(2.4), A.18.10(3/4)
in Ada.Containers.Multiway_Trees   A.18.10(2.2/5)
root directory A.16(47.1/5)
root library unit 10.1.1.10
root node of a tree   A.18.10(2.4), A.18.10(3/4)
root type of a class   3.4.1(2/2)
Root_Buffer_Type
in Ada.Strings.Text_Buffers   A.4.12(6/5)
root_integer   3.5.4(14)
[partial]   3.4.1(8)
root_real   3.5.6(3)
[partial]   3.4.1(8)
Root_Storage_Pool
in System.Storage_Pools   13.11(6/5)
Root_Storage_Pool_With_Subpools
Root_StreamReader
in Ada.Strings.Text_Streams   13.13.1(3/2)
Root_Subpool
rooted at a type   3.4.1(2/2)
roots the subtree A.18.10(3/4)
Rosen trick 13.9(14.e/3)
rotate B.2(9)
Rotate_Left B.2(6)
Rotate_Right B.2(6)
Round attribue   3.5.10(12)
Round_Robin_child_of_Aدا.Đ派遣_D.2.5(4/5)
Round_Robin_Within_Priorities_task dispatching policy   D.2.5(2/2)
Rounding attribute   A.5.3(36)
RPC
child of System   E.5(3/5)
RPC-receiver   E.5(21)
RPC_Receiver
in System.RPC   E.5(11)
RS
in Ada.Characters.Latin_1   A.3.3(6)
run-time error   1.1.2(30), 1.1.5(6), 11.5(2/3), 11.6(1/3)
run-time polymorphism   3.9.2(1/5)
run-time semantics   1.1.2(30)
run-time type
See tag 3.9(3)
running a program
See program execution   10.2(1)
running task D.2.1(6/2)
runtime check
See language-defined check   11.5(2/3)
runtime name text
entity with C.5(1.1/4)
S
safe range
of a floating point type 3.5.7(9)
of a floating point type 3.5.7(10/5)
safe separate compilation 10(3.b)
Safe_First_attribute A.5.3(71), G.2.2(5)
Safe_Last_attribute A.5.3(72), G.2.2(6)
safety-critical systems H(1/2)
same value
for a limited type 6.2(10.f)
satisfied
filter 5.6.2(5)
satisfies
a discriminant constraint 3.7.1(11)
a range constraint 3.5(4)
a subtype predicate 3.4.3(32/4)
an index constraint 3.6.1(7)
for an access value 3.10(15/2)
satisfies the predicates
of a subtype 3.2.4(29.2/4)
Saturday
in Ada.Calendar.Formatting   9.6.1(17/2)
Save
in Ada.Numerics.Discrete_Random   A.5.2(24/5)
in Ada.Numerics.Float_Random   A.5.2(12/5)
Save_Occurrence
in Ada.Exceptions   11.4.1(6/2)
scalar type 1.3.1(72/5), 3.2(3), 3.5(1)
scalar_constraint   3.2.2(6)
used   3.2.2(5), P.1
scale
of a decimal fixed point subtype 3.5.10(11), K.2(216)
Scale attribute 3.5.10(11)
Scaling attribute A.5.3(27)
SCHAR_MAX
in Interfaces.C   B.3(6)
SCHAR_MIN
in Interfaces.C   B.3(6)
SCI
in Ada.Characters.Latin_1   A.3.3(19)
scope
informal definition   3.1(8)
of (a view of) an entity   8.2(11)
of a declaration   8.2(10)
signal (an exception)
  See raise 11(1/3)
signal handling
  example 9.7.4(10)
signed integer type 3.5.4(1)
signed_char
  in Interfaces.C B.3(8)
Signed_Conversions
  in
    Ada.Numerics.Big_Numbers.Big_Inte-
gers A.5.6(12/5)
signed_integer_type_definition 3.5.4(3)
used 3.5.4(2), P.1
Signed_Zeros attribute A.5.3(13)
simple entry call 9.5.3(1)
simple name
of a file A.16(47/2)
Simple_Barriers restriction D.7(10.12/5)
simple_expression 4.4(4)
Simple_Name
  in Ada.Directories A.16(16/5), A.16(38/2)
in
    Ada.Directories.Hierarchical_File_Name-
es A.16(1.10/3)
simple_return_statement 6.5(2/2)
  used 5.1(4/2), P.1
simple_statement 5.1(4/2)
  used 5.1(3), P.1
Sin
  in Ada.Numerics.Generic_Complex_-Elementary_Functions G.1.2(4)
in Ada.Numerics.Generic_Elementary_-Functions A.5.1(5)
single
  class expected type 8.6(27/2)
single entry 9.5.2(20)
Single_Precision_Complex_Types
  in Interfaces.Fortran B.5(8)
single_protected_declaration 9.4(3/3)
  used 3.3.1(2/3), P.1
single_task_declaration 9.1(3/5)
  used 3.3.1(2/3), P.1
Sinh
  in Ada.Numerics.Generic_Complex_-Elementary_Functions G.1.2(6)
in Ada.Numerics.Generic_Elementary_-Functions A.5.1(7)
size
  of an object 13.1(7/5)
in Ada.Direct_IO A.8.4(15)
in Ada.Directories A.16(26/2), A.16(41/2)
in Ada.Strings.Stream_IO A.12.1(23)
Size (object) aspect 13.3(41)
Size (subtype) aspect 13.3(48)
Size attribute 13.3(40), 13.3(45)
Size clause 13.3(7/2), 13.3(41), 13.3(48)
size_t
  in Interfaces.C B.3(13)
Skip_Line
  in Ada.Text.IO A.10.1(29/5)
Skip_Page
  in Ada.Text.IO A.10.1(32/5)
slice 4.1.2(2)
  used 4.1.2(5), P.1
in Ada.Strings.Unbounded A.4.5(22)
small
  of a fixed point type 3.5.9(8/2)
Small aspect 3.5.10(2/5)
Small attribute 3.5.10(2/5)
Small clause 3.5.10(2/5), 13.3(7/2)
smallest first order A.18(5/5)
SO
  in Ada.Characters.Latin_1 A.3.3(5)
Soft_Hyphen
  in Ada.Characters.Latin_1 A.3.3(21/3)
SOH
  in Ada.Characters.Latin_1 A.3.3(5)
solidus
  in
    Ada.Strings.Maps.Constants A.4.6(4)
Space
  in Ada.Characters.Latin_1 A.3.3(19)
SOS
  in Ada.Characters.Latin_1 A.3.3(18)
Specifiable (of an attribute and for an
entity) 13.3(53)
specific_handler C.7.3(9/2)
specific_postcondition_expression 6.1.1(4/5)
specific_precondition_expression 6.1.1(2/5)
specific_stable_property_function 7.3.4(5/5)
specification 3.4.1(3/5)
Specific_Handler
  in Ada.Task_Termination C.7.3(6/2)
specified
  of an aspect of representation of an
dependency 13.1(17)
of an operational aspect of an
dependency 13.1(18/5)
specified (not!) 1.13(18), M.2(1.a)
specified as independently addressable
C.6(8.1/4)
specified discriminant 3.7(18)
Slice
  in Ada.Containers.Doubly_Linked_-Lists A.18.3(49/5)
in Ada.Containers.Vectors A.18.2(77/5)
SOS
  in Ada.Characters.Latin_1 A.3.3(19)
Splice
  in Ada.Containers.Doubly_Linked_-Lists A.18.3(30/5), A.18.3(31/5),
A.18.3(32/2)
Splice_Children
  in Ada.Containers.Multiway_Trees A.18.10(57/5), A.18.10(58/5)
Splice_Subtree
  in Ada.Containers.Multiway_Trees A.18.10(55/5), A.18.10(56/5)
Split
  in Ada.Calendar 9.6(14)
in Ada.Execution_Time D.14(8/2)
in Ada.Real_Time D.8(16)
Split_Into_Chunks
  in Ada.Iterator_Interfaces 5.5.1(4/4/5)
Index 16 October 2023 1628
Synchronization aspect 9.5(12/3)
synchronization_kind 9.5(10/3)
synchronized 1.3.1(78/5)
synchronized interface 3.9.4(5/2)
synchronized object 9.10(18/5)
synchronized tagged type 3.9.4(6/2)
Synced_Barrier 9.5(12/3)
Synced_Barriers D.10.1(5/3)
Synched_Barriers D.10.1(5/3)
Synched_Barriers D.10.1(5/3)
"child of Ada.Containers.A.18.27(3/5)
"child of Ada.Containers.A.18.27(3/5)
System 13.7(3/5)
System.Address_To_Access - Conversions 13.7.2(2/5)
System.Atomic_Operations.Test_And_Set C.6.3(3/5)
System.Multiprocessors.D16.3(5/5)
System.RPC E.5(3/5)
System.Storage_Track.Elements 13.7.1(2/5)
System.Storage_Track.Pools 13.11(5/5)
System.Storage_Track.Subpools 13.11.4(3/5)
System.Assertion_Check 11.5(23.11/5)
System_Name "in System 13.7(4)
systems programming C(1)

T
italicized 4.5.1(3.2/3)
Tag 3.9(6/5)
Tag attribute 3.9(16), 3.9(18)
tag indeterminate 3.9(26/2)
tag of an object 3.9(3)
class-wide object 3.9(22)
object created by an allocator 3.9(21/5)
preserved by type conversion and parameter passing 3.9(25)
returning from a procedure 3.9(23), 3.9(24/2)
stand-alone object, component, or aggregate 3.9(20)
Tag_Array in Ada.Tags 3.9(7.3/2)
Tag_Check 11.5(18)
[partial] 3.9.2(16), 4.6(42), 4.6(52), 5.2(10), 6.5(8.2/5), 6.5(9/2)
Tags child of Ada 3.9(6/5)
Tail in Ada.Strings.Bounded A.4.4(72), A.4.4(73)
in Ada.Strings.Fixed A.4.3(37), A.4.3(38)
in Ada.Strings.Unbounded A.4.5(67), A.4.5(68)
tail of a queue D.2.1(5/2)
tamper with cursors [partial] A.18.2(1.5/2)
of a list A.18.3(61.5), A.18.3(62/5)
of a map A.18.4(7/5), A.18.4(8/5)
of a set A.18.7(7/5), A.18.7(8/5)
of a tree A.18.10(80/5), A.18.10(81/5)
of a vector A.18.2(90/5), A.18.2(91/5)
tamper with elements [partial] A.18.2(1.5/2)
of a holder A.18.18(29/5), A.18.18(30/5)
of a list A.18.3(61/5), A.18.3(67/5), A.18.4(13/5), A.18.7(13/5)
of a map A.18.4(7/5)
of a set A.18.7(7/5)
of a tree A.18.10(80/5), A.18.10(87/5)
of a vector A.18.2(90/5), A.18.2(95/5)
tampering prohibited for a holder A.18.18(29/5), A.18.18(35/5)
prohibited for a list A.18.3(61/5), A.18.3(69.1/5)
prohibited for a map A.18.4(7/5), A.18.4(15.1/5)
prohibited for a set A.18.7(7/5), A.18.7(14.1/5)
prohibited for a tree A.18.10(80/5), A.18.10(90/5)
prohibited for a vector A.18.2(90/5), A.18.2(97.1/5)
Tampering_With_Cursors_Prohibited in Ada.Containers.Doublely_Linked - Lists A.18.3(10.1/5)
in Ada.Containers.Hashed_Maps A.18.5(7.1/5)
in Ada.Containers.Hashed_Sets A.18.8(8.1/5)
Index 16 October 2023 1632

Time-Out

Example 9.7.4(12)
See asynchronous_select 9.7.4(12)
See selective_accept 9.7.1(1)
See timed_entry_call 9.7.2(1/5)

Time_Error

In Ada.Calendar 9.6(18)

Time_First

In Ada.Real_Time D.8(4)

Time_Last

In Ada.Real_Time D.8(4)

Time_Of

In Ada.Calendar 9.6(15)
In Ada.Calendar.Formatting 9.6.1(30/2), 9.6.1(31/2)
In Ada.Execution_Time D.14(9/2)
In Ada.Real_Time D.8(16)

Time_Of_Event

In Ada.Real_Time.Timing_Events D.15(6/2)

Time_Of_Frequency

In Ada.Calendar.Time_Zones 9.6(4/2)

Time_Remaining

In Ada.Execution_Time.Timers D.14.1(8/2)

Time_Span

In Ada.Real_Time D.8(5)

Time_Span_First

In Ada.Real_Time D.8(5)

Time_Span_Last

In Ada.Real_Time D.8(5)

Time_Span_Unit

In Ada.Real_Time D.8(5)

Time_Span_Zero

In Ada.Real_Time D.8(5)

Time_Unit

In Ada.Real_Time D.8(4)

Time_Zones

Child of Ada.Calendar 9.6.1(2/5)
Timed entry call 9.7.2(2)
Used 9.7(2), P.1

Timer


Timer_Error

Example 9.7.4(12)

Timer_Handler


Timer_Resource_Error

In Ada.Execution_Time.Timers D.14.1(9/2)

Timers


Times operator 4.5(1), 4.5.5(1)

Timing

See delay_statement 9.6(1)

Timing_Event

In Ada.Real_Time.Timing_Events D.15(4/5)

Timing_Event_Handler

In Ada.Real_Time.Timing_Events D.15(4/5)

Timing_Events

Child of Ada.Real_Time D.15(3/5)

To_Ada

In Interfaces.C B.3(22), B.3(26), B.3(28), B.3(31), B.3(37), B.3(39), B.3(39.10/2), B.3(39.13/2), B.3(39.17/2), B.3(39.19/2), B.3(39.4/2), B.3(39.8/2)

In Interfaces.COBOL B.4(17), B.4(19)

In Interfaces.Fortran B.5(13), B.5(14), B.5(16)

To_Address

In System.Address_To_Access._Conversions 13.7.2(3/3)
In System.Storage_Elements 13.7.1(10/3)

To_Basic

In Ada.Characters.Handling A.3.2(6), A.3.2(7)
In Ada.Wide_Characters.Handling A.3.5(20.15/5), A.3.5(21.1/5)

To_Big_Real

In Ada.Numerics.Big_Numbers.Big_Integers A.5.6(7/5), A.5.6(12/5), A.5.6(13/5)

To_Big_Real

In Ada.Numerics.Big_Numbers.Big_Real s A.5.7(9/5), A.5.7(13/5), A.5.7(14/5)

To_Binary

In Interfaces.COBOL B.4(45), B.4(48)

To_Bounded_String


To_C

In Interfaces.C B.3(21), B.3(25), B.3(27), B.3(32), B.3(36), B.3(38), B.3(39.13/2), B.3(39.16/2), B.3(39.18/2), B.3(39.4/2), B.3(39.7/2), B.3(39.9/2)

To_Character

In Ada.Characters.Conversions A.3.4(5/2)

In Ada.Characters.Handling A.3.2(15/2)

To_Chars_Ptr

In Interfaces.C.Strings B.3.1(8)

To_COBOL

In Interfaces.COBOL B.4(17), B.4(18)

To_Cursor

In Ada.Containers.Vectors A.18.2(25/5)

To_Decimal

In Interfaces.COBOL B.4(35), B.4(40), B.4(44), B.4(47)

To_Display

In Interfaces.COBOL B.4(36)

To_Domain

In Ada.Strings.Maps A.4.2(24)
In Ada.Strings.Wide_Maps A.4.7(24)

In Ada.Strings.Wide_Maps A.4.8(24/2)

To_Duration

In Ada.Real_Time D.8(13)

To_Fortran

In Interfaces.Fortran B.5(13), B.5(14), B.5(15)

To_Holder

In Ada.Containers.Indefinite_Holders A.18.18(9/5)

To_Index


To_Integer

In Ada.Numerics.Big_Numbers.Big_Integers A.5.6(11/5)
In System.Storage_Elements 13.7.1(10/3)

To_ISO_646

In Ada.Characters.Handling A.3.2(11), A.3.2(12)

To_Long_Binary

In Interfaces.COBOL B.4(48)

To_Lower

In Ada.Characters.Handling A.3.2(6), A.3.2(7)
In Ada.Wide_Characters.Handling A.3.5(20/3), A.3.5(21/3)

To_Mapping

In Ada.Strings.Maps A.4.2(23)
In Ada.Strings.Wide_Maps A.4.7(23)
In Ada.Strings.Wide_Maps A.4.8(23/2)

To_Packed

In Interfaces.COBOL B.4(41)

To_Picture

In Ada.Text_IO.Editing F.3.3(6)

To_Pointer

In System.Address_To_Access._Conversions 13.7.2(3/3)

To_Quotient_String

In Ada.Numerics.Big_Numbers.Big_Real s A.5.7(19/5)

To_Range

In Ada.Strings.Maps A.4.2(24)
In Ada.Strings.Wide_Maps A.4.7(25)
In Ada.Strings.Wide_Maps A.4.8(25/2)

To_Ranges

In Ada.Strings.Maps A.4.2(10)
In Ada.Strings.Wide_Maps A.4.7(10)
In Ada.Strings.Wide_Maps A.4.8(10/2)

To_Real

In Ada.Numerics.Big_Numbers.Big_Real s A.5.7(10/5)

To_Sequenc

In Ada.Strings.Maps A.4.2(19)
In Ada.Strings.Wide_Maps A.4.7(19)
In Ada.Strings.Wide_Maps A.4.8(19/2)
Wide_Wide_Character_Sequencetype
ofWide_Wide_String
inAda.Strings.Wide_Wide_Maps
A.4.8(16/2)
Wide_Wide_Character_Set
inAda.Strings.Wide_Wide_Maps
A.4.8(4/5)
Wide_Wide_Characters
child ofAda A.3.1(6/5)
Wide_Wide_Command_Line
child ofAda A.15.1(3/5)
Wide_Wide_Constants
Wide_Wide_Characters child ofAda A.3.1(6/5)
Wide_Wide_Directories
Wide_Wide_Characters child ofAda A.16.2(3/5)
Wide_Wide_Exception_Name
inAda.Exceptions 11.4.1(2/5), 11.4.1(5/2)
Wide_Wide_Expanded_Name
inAda.Tags 3.9(7/2)
Wide_Wide_Fixed
child ofAda Strings A.4.8(1/3)
Wide_Wide_Get
inAda.Strings.Text_Buffers
A.4.12(22/5)
Wide_Wide_Hash
child ofAda Strings A.4.8(1/3)
Wide_Wide_Hash_CaseInsensitive
child ofAda Strings A.4.8(1/3)
Wide_Wide_Images
attribute
3.5(27.1/5), 3.5(55.2/5), 4.10(38.5)
Wide_Wide_Strings
inStandard A.1(42.1/3)
Wide_Wide(Strings)
child ofAda A.4.1(4/2)
Wide_Wide_Space
inAda.Strings A.4.1(4/2)
Wide_Wide_Text_IO
child ofAda A.1(11.3/2)
Wide_Wide_Unbounded
child ofAda Strings A.4.8(1/3)
Wide_Wide_Unbounded_IO
child ofAda.Strings.A.4.8(1/3)
Wide_Wide_Width
attribute 3.5(37.1/5)
Width
attribute 3.5(39.1/5)
Write
inAda.Direct_IO A.8.4(18.8/5)
inAda.Sequential_IO A.8.1(15.8/5)
inAda.Strings.Stream_IO
A.12.1(26.8/5)
inAda.Text_IO A.10.1(85.8/5)
Year
inAda.Calendar 9.6(13)
inAda.Calendar.Formatting 9.6.1(21.2)
Year_Number subtype of Integer
inAda.Calendar 9.6(11/2)
Yen_Sign
inAda.Characters.Latin_1 A.3.3(21.3)
 Yield
inAda.Dispatching D.2.1(1.3/5)
Yield_aspect
D.2.1(1.7/5)
Yield_To_Higher
inAda.Dispatching.Non_Preemptive
D.2.4(2.2/5)
Yield_To_Same_Or_Higher
inAda.Dispatching.Non_Preemptive
D.2.4(2.2/5)
X
xor operator 4.5.1, 4.5.1(2)
Y
xoperator 4.5.1, 4.5.1(2)