# Towards a Formal Semantics for Ada 9X
## Final Report
## NAS1-18972 Task 11

David Guaspari      John McHugh      Wolfgang Polak      Mark Saaltink

October 31, 1994

# Contents

# Chapter 1

# Introduction

The Ada 9X Language Precision Team (LPT) was formed in 1990 to study portions of the design of Ada 9X from a mathematical perspective. The first LPT project studied small parts of the language in isolation, formulating fairly simple models to explore the ramifications of the design. The idea was to avoid spending time studying the conventional parts of the language (where, we felt, little would be gained by the analysis) and to focus on the novel proposals such as the object-oriented features, overload resolution, and exception mechanisms. The results of this first project appear in two reports [9, 2].

The second LPT project had two separate goals. The first, similar in approach to the first project, was to study the rules of allowed optimizations. The second goal was rather different. Instead of defining many unrelated small models, and studying new features in depth, the plan was to formulate a broad model to cover a large part of the language. In this way, we hoped to find problems arising from the interactions between different features.

The level of effort of the project was clearly insufficient to define a complete model of the language, and our plan was not to make a complete model. Instead, we planned to define the framework for such a model, and to fill in the details of the framework only in certain areas. Furthermore, the framework was not intended to be complete; we did not expect to be able to describe concurrency or distributed programming. We did, however, hope for the framework to cover most of the sequential features.

Our expectation was not that the resulting incomplete model would necessarily be useful to anyone (although we hope that it could be extended to form the basis for analysis tools). Instead, we expected that the activity of making this model would allow us to influence the design of Ada 9X by identifying problems with specific language features or with the interactions between different features, or by suggesting improvements in the ways that parts of the language are described. As the design of Ada 9X was nearing completion when our project began, it was important to move as quickly as possible. So, the model is quite sketchy in areas. Moreover, the formal definition presented in this report omits several partial models that we built in the course of the project, as we did not have the time to integrate them with the overall framework. None the less, these models have played a useful role in helping us to understand and comment on various language features, and to influence (however slightly) the design of Ada 9X.

This report is organized as follows. The method used for defining the model is described in Chapter 2. A discussion of the model also appears there. The model itself appears in two parts. The "domains" (sets describing the values assumed by different entities in the language) are described in Chapter 3. The "judgements" describing possible executions of a program are described in Chapter 4. Our study of the optimization freedoms described in [11.6] does not fit into the main framework; it is described separately in Chapter 5. Conclusions are drawn in Chapter 6.

Two appendices give some additional information. Appendix A lists the official language com-

1

ments that were submitted by the LPT; most of these apply to Version 4.0 of the Draft Standard [3], and several have resulted in changes that appear in Version 5.0 [4]. Appendix B describes the intermediate syntax that results from overload resolution (and other static checks).

References to the Ada 83 Reference Manual [10] appear in the form [RM-83 $c.s(p)$], where $c$ is the chapter number, $s$ the section number, and $p$ the paragraph number. References to version 5.0 of the Annotated Draft Standard for Ada 9X [4] appear in the form [$c.s(p)$]; this standard as a whole is often referred to as "the Reference Manual".

# Chapter 2

# Method of Description

The "broad semantic framework" is defined using *Natural Semantics* [5]. The general idea of natural semantics is to define semantics as one or more relations between syntactic phrases and semantic values. These relations are defined using axioms and rules of inference. As a trivial example, a simple language of arithmetic expressions can be defined by the grammar

```
expression  ::=  numeral | <expression> "plus" <expression>
```

We can define the semantics of these expressions using a relation (between expressions and numbers) of "evaluates to", which we will write as $expression \Rightarrow value$, and a relation (between numerals and numbers) of "denotes", which we will write as $numeral \rightarrow value$.

Two rules suffice to define the semantics of expressions (although additional rules not shown here are needed to define the "denotes" relation). The first covers the base case of numerals:

$$\frac{n \rightarrow v}{n \Rightarrow v} \quad [\, n \in numeral \,]$$

The second gives the semantics of sums:

$$\frac{e1 \Rightarrow v1 \qquad e2 \Rightarrow v2}{e1 \text{ plus } e2 \Rightarrow v1 + v2}$$

The method is easily able to handle nondeterminism, where a phrase can have many possible results. If we extend the expression grammar above to include ranges, with the meaning that any number in the range is allowed, we have the grammar

```
expression  ::=  numeral
            |  <expression> "plus" <expression>
            |  <expression> ".." <expression>
```

Only one additional semantic rule is needed:

$$\frac{e1 \Rightarrow v1 \qquad e2 \Rightarrow v2}{e1 \,..\, e2 \Rightarrow v} \quad [\, v1 \leq v \leq v2 \,]$$

Using these rules, we can deduce

$$(0\,..\,2) \text{ plus } (10\,..\,20) \Rightarrow x$$

for any $x$ between 10 and 22 inclusive.

In practical applications of Natural Semantics, the judgements used are often more complex than in this simple example. Usually, there is a certain amount of contextual information (such as the definitions of functions or procedures); this is represented by an *environment*. Often a *store* is used to record the values of variables. Furthermore, the evaluation of a phrase may have an effect on the environment or store. So the judgements often have many components, and there are a number of auxiliary domains of semantic values. We write most judgements in a standardized form

$$S, E \vdash_{pt} p \Rightarrow v, \ldots,$$

where $S$ is a store, $E$ is an environment, $p$ is a phrase, the subscript $pt$ gives the kind of phrase (*e.g.*, whether $p$ is a declaration, statement, expression, or name), $v$ is a possible result of executing (or evaluating or elaborating) $p$, and the "..." are any other results that the execution may have. Usually, there is a final state that reflects any side-effects that the execution may have had.

We describe the domains of semantic values using the Z notation [8], which furnishes a standard toolkit of notations for sets, functions, relations, and "freely constructed" sets.

The Natural Semantics definitions have been written in a machine-readable form in Prolog. Judgements are represented directly as Prolog predicates, and semantic rules as Prolog rules. There is a slight difficulty in transcribing uses of functions, but a simple translation to relations is possible. The Prolog representation has two main advantages. Firstly, we were able to apply a type-checking package developed by Reddy and Lakshman [7] to the definition; this found a number of simple errors in the rules. Secondly, we are able to run the Prolog and determine what outcomes are predicted by the semantic definition. This allows the semantics definition to be tested on small examples.

Several aspects of Ada 9X are tricky to define properly. In the remainder of this chapter, some of the awkward parts of the language and some of the more intricate aspects of the Natural Semantics definition will be explained. Not everything described below has been implemented in the Natural Semantics; some of the discussion describes our plan for dealing with a feature even though we did not have time to include that feature in the semantics definitions.

## 2.1 External Effects and Nonterminating Programs

Ultimately, the meaning of an Ada program is defined in terms of its sequence of "external effects", as described in [1.1.3(8)]. We can readily define several types of external effects, such as operations on files using the standard I/O packages, propagation of an exception, or return from the main program. Other effects are not covered.

An outside observer can see these external effects during the execution of a program, and does not need to wait until (and if) the program terminates. Therefore, we use a small trick to allow the semantics to assert that a certain sequence of external effects can be viewed whether or not the program terminates. We use a special *incomplete* condition that is treated like an exception that cannot be handled. For any operation having an external effect, one possible result is to "raise" this condition. The semantic definition then propagates this condition out of the main call. Thus, we are able to infer judgements of the form

$$Library \vdash program\_name \Rightarrow e,$$

where $e$ is a sequence of external effects, for every sequence $e$ that might be observed during a run of the program.

## 2.2 Semantic Simplifications

Some language features appear to be very difficult to incorporate into this model. For these features, we have introduced a notion of an *unpredicted* result. When our definition allows the deduction that

*unpredicted* is a possible result of an execution, it means that the particular program includes a language feature, or encounters a situation, that we decided not to account for in our model. This is similar to erroneous executions, where the language standard does not predict the results of a program.

For example, Section [11.6] of the Ada 9X Reference Manuals allows implementations to produce results at variance with the language rules described elsewhere in the manual (in situations where a language-defined check would fail if those rules were followed). The freedoms allowed by Section [11.6] appear to be very difficult to incorporate into the model defined here. Therefore, we have kept the model simple by treating the failure of a language-defined check as an *unpredicted* execution.

There are some rules new to Ada 9X that constrain the result of an execution that Ada 83 classes as erroneous. These *bounded error* situations can be difficult to model. For example, reading the value of an uninitialized scalar variable is erroneous in Ada 83. In Ada 9X, it is a bounded error, which can result in an exception or an implementation-defined result. Version 4.0 of the proposed Standard introduced the concept of *invalid values* to describe these results. Unfortunately, the introduction of invalid values complicates the semantics of the language considerably, as it is necessary to provide rules for computing with these values. The draft standard does not always provide the complete details of these rules. For example, what is the result of a comparison involving invalid values? Are the ordering operators transitive, even when applied to invalid values? We decided to keep our model simple, and to avoid these questions, by refusing to predict the outcome of a program that reads an uninitialized scalar variable. Version 5.0 of the Standard has changed the description of this situation, but once again the exact rules are vague. Therefore, we are continuing to use the simple model that refuses to predict the outcome of a program in these situations.

## 2.3   Static Checks and Overload Resolution

It is conventional to process Ada in two (or more) steps; the first step checking syntax, applying all of the "legality" checks, and resolving any overloading. We planned to define the semantic model in a similar way, with two distinct definitions. The first *static semantics* takes Ada source text, and produces a program in *intermediate syntax*. The intermediate syntax differs from Ada source text in several significant ways:

- Intermediate syntax is in the form of a tree, rather than a linear string of characters. Therefore intermediate syntax does not need to be parsed.

- Overloading has been resolved. Identifiers, characters, and operator names have been replaced by *intermediate identifiers* (in the set *Id*) in such a way that no two distinct declarations declare the same intermediate identifier. Any use of an identifier, character literal, or operator name has been replaced by a use of the appropriate element of *Id*. (Some names using selection, e.g., package components, are also replaced by intermediate identifiers.)

- Many of the notational conveniences of Ada have been eliminated. For example, infix operators are replaced by function calls.

- Generics are eliminated. Generic instantiations are expanded to a sequence of declarations.

- Some additional information is included. For example, a *completing declaration* is explicitly marked as such.

The intermediate syntax is described in Appendix B.

We have not formally defined the static analysis, although we believe that a Natural Semantics formulation of the static rules is possible.

## 2.4 Environments, Entities, and Stores

The Natural Semantics definition is faithful to the Reference Manual in its treatment of entities. We use several different sorts of "entity locations", which serve as unique names or references for entities. When a declaration is elaborated, new names are generated for any of the entities that need to be "created", and the environment is updated to reflect the association of the declared *Id* with a view of one of these entities. The store is a collection of mappings indexed by these different entity locations, which associates a value or meaning with each entity.

This indirect representation, using references to entity locations rather than the meanings of entities, makes it fairly easy to handle situations where an entity has a declaration that is separate from its definition. Between the declaration and definition, any references to the entity cannot make use of the definition (because it is not yet known). The location associated with the entity *is* known, and can be used.

## 2.5 Ordering

The Ada Standard gives implementations considerable freedom to select the order in which actions are performed. For example, in evaluating a sum, either the left or the right operand might be evaluated first. It is easy to write a program that gives different results depending on which order is chosen.

In order to write a concise description of the possible effects of the evaluation of constructs allowing a choice of orders, we define a set of *actions*, and several ways of combining actions. One combination, written by encosing the actions in braces, allows the actions to be carried out in an arbitrary order; another, written by enclosing the actions in square brackets, requires the actions to be carried out in strict sequential order.

Actions are similar to judgements, except that the states do not appear explicitly. When actions are executed in some order, suitable states are added and the corresponding judgement is used. We write the actions in a notation that makes obvious the judgement for the corresponding execution. For example, corresponding to the judgement $S_1, E \vdash_{stm} Stm \Rightarrow S_2$ is an action written as $'E \vdash_{stm} Stm \Rightarrow'$; corresponding to the judgement $S_1, E \vdash_{exp} Exp \Rightarrow V, S_2$ is an action written as $'E \vdash_{exp} Exp \Rightarrow V'$.

We also use *states*, which are combinations of *stores* and control flow information (for example, whether an exception has been raised, whether a return command has been executed, whether execution is normal.) The rules defining the execution of a combined action check the control flow information to skip some actions if that is appropriate. For example, in executing "a followed by b", if the execution of "a" propagates an exception, the action "b" is not executed.

One advantage to this approach is that the actions themselves look simpler than the corresponding judgements, because the flow of control through them is described by the way they are combined. For example, in defining the possible results of a sum using explicit ordering, we would need several judgements, including

$$\frac{s, E \vdash_{exp} e1 \Rightarrow v1, s1 \\ s1, E \vdash_{exp} e2 \Rightarrow v2, s2}{s, E \vdash_{exp} e1 + e2 \Rightarrow v1 + v2, s2}$$

and

$$\frac{s, E \vdash_{exp} e2 \Rightarrow v2, s1 \\ s1, E \vdash_{exp} e1 \Rightarrow v1, s2}{s, E \vdash_{exp} e1 + e2 \Rightarrow v1 + v2, s2}$$

and others to account for exceptions. Instead, using actions, we can write

$$\frac{S_1 \vdash \left\{ \begin{array}{l} 'E \vdash_{exp} e1 \Rightarrow v1' \\ 'E \vdash_{exp} e2 \Rightarrow v2' \end{array} \right\} S_2}{S_1, E \vdash_{exp} e1 + e2 \Rightarrow v1 + v2, S_2}$$

which accounts for the different possible orders of evaluation and for the propagation of an exception from one of those evaluations. (We still need something extra to account for an overflow in the addition.)

## 2.6  Types

It is awkward to define a domain of "type values" that describe types, because the exact characteristics of a type can change through its scope. For example, a type may be limited in some parts of its scope, and nonlimited in other parts (such as the body of a package defining the type of a component); a type can be private in some places and not in others. Furthermore, an incompletely defined type can be used in various ways (such as a record component or designated type of an access type); the characteristics of the using type can change after the incompletely defined type's full definition.

In order to simplify the treatment of these situations, types are described by *descriptors* that refer to other types by their locations (see Section 2.4), rather than by their descriptors. This has the disadvantage that descriptors are not meaningful in isolation, but only with respect to the store that associates descriptors with type locations. However, it has several advantages:

- it gives a simple characterization of when types are the same; each type location represents a distinct type;

- when the characteristics of a type of a component change, that change can be reflected in just one descriptor; and

- circularities in type descriptors are easily handled (without needing any tricky domains allowing for infinite data structures).

An example illustrating these advantages is

```
type A;
type B is access A;
type A is access B;
```

## 2.7  Values

We expected it to be easy to describe the domain of values that objects might assume. It was surprising that this was not so. As mentioned above, the addition of *invalid* values to scalar types adds several complications, as the nature of such values is not completely specified. The latest version (5.0) of the proposed Standard no longer uses the term "invalid value"; instead, a variable may have an "invalid representation" [13.9.1].

We also argued whether "abnormal" values would be needed in order to model the concept of *abnormal* objects. We were able to avoid this, since the circumstances that can lead to abnormal objects are being treated as unpredictable executions.

There are a few situations where it is difficult to determine the set of values associated with a type. For example, given the declaration

```
subtype Void is Integer range 1 .. 0; -- an empty range
type R is record
  v: Void
  end R;
```

There are no values of subtype Void. However, there *are* values of type R. For example, a variable of type R can be declared, and it is not an error to "read" the value of such a variable, or to assign this value to a second variable of type R.

The problems with this type are related to those for uninitialized scalar variables, and we adopt a simple approach to solve them. We use a special indicator to denote an uninitialized scalar value. A scalar subcomponent of an object can have this value. If this "uninitialized" value is read, execution is unpredicted.

The set of values of an enumeration type is not obvious. Given the declarations

```
type E is (red, green);
for E use (red => 1; green => 100);
```

version 4.0 of the Draft Standard suggested that there were two "valid values" of type E, and (at least) 98 "invalid values" between them. The number of elements in an array indexed by E, then, is open to question. Are there elements corresponding to the invalid members of the base range?

Types declared with *per-object constraints* do not have obvious sets of values (since the constraint applied to a subcomponent might depend on the specific object of the type). Our model simply does not cover the kinds of per-object constraints that lead to this difficulty.

Our model for values uses integers to represent discrete values (even if the value is of an enumeration type). This means that the values of different types are not necessarily different. It would certainly be possible to mark values in such a way that no value belongs to more than one type, but there seems to be no benefit to doing so. An Ada program cannot directly compare values of different types, so there is no way for this detail to influence the outcome of a program.

## 2.8 Objects

It is normal in semantic definitions to use *location semantics* for variables, but different approaches can be used in accounting for structured (composite) variables and their components.

The approach that seems most convenient for us is to associate locations with *entire* variables (that is, variables that are not subcomponents of other variables). Every object is characterized by its location and a *selector* indicating which component of the entire variable it is.

### 2.8.1 Actual Subtypes

The *actual subtype* of an object is sometimes different from the *nominal subtype* in its declaration. This is an issue for assignments [5.2(11)] and formal parameters of mode **in out** or **out** that are passed by copy [6.4.1(17)]. So it is important only for variables.

The actual subtype of a variable differs from its nominal subtype in the following circumstances:

- the object is a declared object, and is constant, aliased, or has an indefinite nominal subtype [3.3.1(9)].

- the object is a formal parameter. [6.4.1(16)] states

    A formal parameter of mode **in out** or **out** with discriminants is constrained if either its nominal subtype or the actual parameter is constrained.

[6.4.1(12-15) gives additional rules for **out** parameters.

- the object is a generic formal object of mode **in out**. [12.4(8)] states that the nominal subtype is taken from the declaration of the formal, while the actual subtype is taken from the actual.

- the object is declared by an allocator, and the designated type of the result subtype of the allocator is indefinite or has discriminants ([3.3(23) and [3.10(9)]).

- the object is a view of another object, and the subtype of the view is indefinite [3.3(23)].

This leads to the question of how the actual subtype of an object is determined, and where, if needed, the actual subtype information is stored. There are two reasonable choices: the actual subtype might be associated with the object, or with each view of the object. However, two views of an object need not have the same type. Obviously, in such a case the actual subtypes must be different. Moreover, in a procedure call, the actual subtype of the view denoted by the formal can be different from the actual subtype of the actual parameter, even when the views have the same type. For example, the actual might be of an unconstrained discriminated type and the formal constrained. Therefore, we have decided to store the actual subtype as part of every view of an object.

## 2.8.2  Initialization

The calculation of the implicit initial value for an object is difficult to describe, as there is considerable freedom in the order of evaluation of default expressions used to initialize subcomponents. It is particularly awkward for subcomponents with discriminants; discriminants must be evaluated before any subcomponent that depends on them, but other subcomponents may have their initial values evaluated before then. So, given the declarations

```
type T(a: D := e0, b: D := e1) is record
  u: Integer := e2;
  v: U(a) := e3;
  w: U(b) := e4;
  x: S(a,b) := e5;
  end record;

y: T;
```

we must evaluate e0 before e3 and e5, and e1 before e4 and e5. The order of evaluation is otherwise unrestricted (unless references to a or b occur in e2, e3, or e4.)

In order to accommodate this flexibility, we use a variation on the "in some order" rules described in Section 2.5. We add an additional datum to the left and right of the turnstile; this datum records which discriminants have had their initializing expressions evaluated (and what the resulting value is). The individual actions record their prerequisites (that is, which discriminants must be evaluated before the action can be executed).

In the record of evaluated discriminants, we cannot simply use the name of the discriminant, as two subcomponents might have the same type, and thus have discriminants of the same name. Instead, for each discriminant subcomponent to be evaluated we generate a unique identifier. A "discriminant environment", associating discriminant identifiers with discriminant names, is therefore also used in the judgements for initialization.

Another difficulty in describing the initialization of objects concerns *per-object constraints*. Ada 9X allows the name of a type to be used in its own definition, in which case it stands for the "current instance" of the type. Thus, a constraint on a component can refer to the containing object. Describing this formally can be difficult: the object might not exist until its subtype can be determined (which involves elaborating per-object constraints), yet the elaboration of a per-object constraint may refer to the object. We decided not to consider per-object constraints that refer to the "current instance" (but we allow them to refer to discriminants).

## 2.9   Aliasing

Some rules concerning aliasing look difficult to model. [6.2(12)] states

> 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 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, 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
> while the first access path still exists. 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.

If we are to allow for accurate predictions of the effects of procedure calls (or to refuse to predict
the outcome of calls that might involve aliasing), we need to be able to recognize, at a minimum,
when the above rule might apply. It is not enough just to say that parameters of certain types may
be passed by copy or by reference at the whim of an implementation, because the above paragraph
allows for results that might not be produced under either of the two passing mechanisms. We might
refuse to predict the result of any call with aliasing, but that can be hard to recognize if access values
are used. Unfortunately, the notion of "access paths" is not well defined by the Reference Manual,
and the precise meaning of the aliasing rule is unclear.

We have submitted several official comments on the aliasing rules, and had some discussions
with the Mapping Team on possible interpretations of these rules. One model that may work can
be sketched as follows: we would define a function *access_path* on names, which gives an element
of *optional Id.* This "access path" gives the *Id* associated with the declaration of some variable
denoting the object denoted by the name. This might be the declaration that created the object, or
might be the name of a formal parameter. If the object was dynamically created, the access path is
null.

In most cases, the definition of *access_path* is simple, e.g.,

$access\_path(Id) = some(Id)$ if $Id$ is not declared by a renaming declaration
$access\_path(Nam.Id) = access\_path(Nam)$
$access\_path(Nam(exp, \ldots)) = access\_path(Nam)$
$access\_path(Nam.\texttt{all} = none$

For *Id*s declared by renaming declarations, we would want to use the access path of the renamed
object.

In order to state the rule of 6.2(12), we would associate a "last update path" with every object
(including subobjects). Whenever an object is updated by an assignment, the access path of the
name used in the assignment statement is recorded in the object (and every subobject and containing
object). In addition, formal parameter objects are updated in a call with the formal parameter *Id*
as the last update path, and after a call, any **in out** or **out** parameter objects are updated by
the access paths of the corresponding actual parameter names. It would be a bounded error to
evaluate a name denoting all or part of a formal parameter for which the parameter passing mode is
unspecified, if the access path differs from the last update path of the object it denotes. Similarly,
it would be a bounded error to evaluate a name if the last update path of the object it denotes is a
formal parameter for which the parameter passing mode is not specified.

These rules account for most of the situations described by 6.2(12), but probably need refinement
to deal properly with access values created by **Access** attributes.

# Chapter 3

# Semantic Domains

In this chapter, we define the domains of values used in the semantics. These sets describe the values assumed by the various entities of Ada 9X.

These definitions have been used as the basis for the Prolog representation of the Natural Semantics definitions presented in Chapter 4. However, some of the definitions defined here have not yet been incorporated into the Natural Semantics definition, and some small inconsistencies between the two definitions have not yet been eliminated.

## 3.1 Basic Notations

In this section, we define some basic notions that will be used in the model.

An *association* provides a finite function with an enumeration of its domain. It is convenient to represent such a function by enumerating (domain, range) pairs; the finite function is then the range of the sequence.

$$X \xrightarrow{a} Y == \{\ s : \operatorname{seq} X \times Y \mid \operatorname{ran} s \in X \nrightarrow Y \wedge \# \operatorname{ran} s = \# s\ \}$$

Functions *adom* and *aran* give the domain and range of an association. Function $\_ \cdot \_$ is used to apply an association to an argument (as though it were a finite function).

$$
\begin{array}{l}
\underline{[X, Y]} \\[4pt]
adom\_ : (X \xrightarrow{a} Y) \to \mathbb{P}\,X \\
aran\_ : (X \xrightarrow{a} Y) \to \mathbb{P}\,Y \\
\_ \cdot \_ : (X \xrightarrow{a} Y) \times X \nrightarrow Y \\[6pt]
\hline \\[-6pt]
\forall\, a : X \xrightarrow{a} Y \bullet adom\,a = \operatorname{dom}(\operatorname{ran} a) \\[6pt]
\forall\, a : X \xrightarrow{a} Y \bullet aran\,a = \operatorname{ran}(\operatorname{ran} a) \\[6pt]
(A, x) \in \operatorname{dom}\_ \cdot \_ \Leftrightarrow x \in adom\,A \\[6pt]
x \in adom\,A \Rightarrow A \cdot x = (\operatorname{ran} a)\,x
\end{array}
$$

We sometimes use optional values:

$$optional\ X ::= none \mid some \langle\!\langle X \rangle\!\rangle$$

Function *maximal* returns the set of maximal values of an arbitrary relation, where a maximal value of the relation $R : X \leftrightarrow X$ is defined as an element $z$ of $X$ such that no $y \neq z$ satisfies $zRy$.

$$\begin{array}{|l}
\hline [X] \rule{0pt}{0pt} \\
\hline
maximal : (X \leftrightarrow X) \to \mathbb{P}\, X \\
\hline
maximal(R) = X \setminus \mathrm{dom}(R \setminus \mathrm{id}\, X) \\
\hline
\end{array}$$

Function *restrict* restricts both the domain and the range of a relation to some given set.

$$\begin{array}{|l}
\hline [X] \rule{0pt}{0pt} \\
\hline
restrict : (\mathbb{P}\, X \times (X \leftrightarrow X)) \to (X \leftrightarrow X) \\
\hline
restrict(S, R) = (S \times S) \cap R \\
\hline
\end{array}$$

Equivalently,

$$restrict(S, R) = (S \lhd R) \rhd S$$

## 3.2  Entities and the Environment

After overload resolution, every occurrence of an identifier in an Ada program can be replaced by an *Id*, so that each *Id* has at most one declaration in the program.

The elaboration of a declaration creates an entity, and the *Id* of the declaration then denotes a *view* of this entity. A declaration might be elaborated many times (e.g., if it appears in a subprogram body), denoting a different entity each time.

$$Environment == Id \nrightarrow View$$

A *view* identifies an entity and provides some characteristics that affect the use of the entity. For example, there can be several views of the same subprogram, each having different parameter names and default expressions. Views refer to entities by using *locations* of various types.

$$[Type\_location, Subtype\_location, Object\_location, Subprogram\_location]$$

There are no views associated with packages or generic declarations. Packages are significant in their provision of information hiding and modularization, but those aspects concern the static semantics, not the dynamic semantics. Generic declarations are expanded by the static semantics, so that only ordinary (non-generic) declarations appear in the intermediate syntax.

Exceptions are unusual entities. No matter how often an exception declaration is elaborated, the same exception is denoted. This exception is represented by an *Exception_Id* that is determined by the static semantics. (The *Exception_Id* could be chosen to be the *Id* of the declaration, for example).

$$\begin{aligned}
View ::= {} & object\_view \langle\!\langle Object\_location \times Subtype \rangle\!\rangle \\
& \mid\ subtype\_view \langle\!\langle Subtype\_location \rangle\!\rangle \\
& \mid\ subprogram\_view \langle\!\langle Subprogram\_location \times Profile \rangle\!\rangle \\
& \mid\ exception \langle\!\langle Exception\_Id \rangle\!\rangle \\
& \mid\ constant \langle\!\langle Value \rangle\!\rangle
\end{aligned}$$

Most kinds of entity are held in a *store*. Assigning a *location* to refer to the entity, and placing an entity at that location in the store, corresponds to what the Reference Manual calls "creating" the entity. This activity happens when a declaration is elaborated.

Several kinds of entities are used in the semantics definition:

- objects, which have values;

- subtypes, with their associated type, constraint, and attributes;

- types, with descriptors and optional parents;

- subprograms, with formals and bodies; and

- operations (representing the "predefined operations" of the Reference Manual).

$$\begin{array}{|l}\hline \textit{Store} \\\hline \textit{types} : \textit{Type\_location} \nrightarrow \textit{Type} \\ \textit{subtypes} : \textit{Subtype\_location} \nrightarrow \textit{Subtype} \\ \textit{objects} : \textit{Object\_location} \nrightarrow \textit{Value} \\ \textit{subprograms} : \textit{Subprogram\_location} \nrightarrow \textit{SubprogramOrOp} \\\hline \end{array}$$

$$SubprogramOrOp ::= subprogram \langle\!\langle Environment \times (\text{seq } Id) \times Dcl \times Stm \rangle\!\rangle$$
$$| \quad operation \langle\!\langle \ldots \rangle\!\rangle$$

The different sorts of entities are described in the following sections.

Evaluation is defined in terms of a *state*, which (usually) includes a store, as well as certain control information. States are defined below in Section 3.6. Function *the_store*, giving the store associated with a state, is used in some of the definitions below.

## 3.3   Thunks

In several situations it is necessary to record an expression together with the environment in which it appears, so that the expression can be evaluated in some other context. The environment is retained so that any *Id*s appearing in the expression have their correct denotation. We call this combination of an expression and an environment a *thunk*.

$$Thunk == Exp \times Environment$$

Thunks appear in record type descriptors (where they describe the initializing values of any explicitly initialized components), and in parameter lists (where they describe any default values for parameters).

## 3.4   Values

There are several kinds of values of interest:

- discrete values (represented by integers)

- real values (represented by rationals)

- access values (represented by views of objects or of subprograms)

- record values (represented by partial functions)

- array values (represented by partial functions)

It is possible to use a model where the values of each type are distinct; however, the benefit of doing so is not completely clear. The rules of the language do not allow for comparisons of values of different types, so there is no way of telling whether these sets are disjoint.

### 3.4.1 Ranges

Ranges have two bounds, and determine a set of values of a scalar type.

$$Range ::= discrete\_range \langle\!\langle \mathbb{Z} \times \mathbb{Z} \rangle\!\rangle \mid real\_range \langle\!\langle Rational \times Rational \rangle\!\rangle$$

$$Discrete\_range == \operatorname{ran} discrete\_range$$

$$Real\_range == \operatorname{ran} real\_range$$

(The definition of the bounds functions contains a forward reference to functions *discrete_value* and *real_value*, defined in Section 3.4.5.)

$$low\_bound, high\_bound : Range \rightarrow Value$$

$$low\_bound(discrete\_range(l, h)) = discrete\_value(l)$$
$$high\_bound(discrete\_range(l, h)) = discrete\_value(h)$$

$$low\_bound(real\_range(l, h)) = real\_value(l)$$
$$high\_bound(real\_range(l, h)) = real\_value(h)$$

$$make\_range : Value \times Value \nrightarrow Range$$

$$make\_range(discrete\_value(v), discrete\_value(v')) = discrete\_range(v, v')$$

$$make\_range(real\_value(v), real\_value(v')) = real\_range(v, v')$$

$$\_ \; belongs\_to \; \_ : Value \leftrightarrow Range$$
$$values\_of\_range : Range \rightarrow \mathbb{P} \; Value$$
$$\_ \; is\_included\_in \; \_ : Range \leftrightarrow Range$$

$$v \; belongs\_to \; R \Leftrightarrow v \in values\_of\_range(R)$$

$$values\_of\_range(discrete\_range(l, h)) = discrete\_value(\![l \mathinner{\ldotp\ldotp} h]\!)$$

$$values\_of\_range(real\_range(l, h)) = real\_value(\![l \mathinner{\ldotp\ldotp} h]\!)$$

$$R \; is\_included\_in \; R' \Leftrightarrow values\_of\_range(R) \subseteq values\_of\_range(R')$$

### 3.4.2 Index Ranges

Arrays are indexed by sequences of discrete values. Index ranges are determined by a sequence of discrete ranges.

$$Array\_bounds == \operatorname{seq}_1(Discrete\_range)$$

Each sequence of bounds determines a set of indices:

$$indices : Array\_bounds \rightarrow \mathbb{P}(\operatorname{seq}_1 Value)$$

$$\forall B : Array\_bounds \bullet indices(B) = \{ \; s \in \operatorname{seq}_1 Value \mid$$
$$\#s = \#B \land \forall n \in \operatorname{dom} s \bullet s(n) \; belongs\_to \; B(i) \; \}$$

### 3.4.3 Tags

We use a set of *tags*. The precise nature of this set is immaterial.

$$[Tag]$$

### 3.4.4  Bindings

Bindings are simply partial mappings from *Id*s to values. Most often these *Id*s are the names of record fields or discriminants.

$$Binding == Id \nrightarrow Value$$

### 3.4.5  Values

Although it seems redundant, we include the bounds as part of an array value. This is because two arrays with no components (thus, with the same mapping function) can have different bounds.

Record values are furnished with optional tags, discriminants, and other components. This allows the descriptions of the various language rules concerning tagged records, discriminated records, and normal records to be combined.

A special value, *uninitialized_value*, is used for uninitialized scalar objects. This is used to detect when such an object is read (in which case the result of the execution is *unpredicted*).

$$
\begin{aligned}
Value ::= &\; uninitialized\_value \\
\mid &\; discrete\_value \langle\!\langle \mathbb{Z} \rangle\!\rangle \\
\mid &\; real\_value \langle\!\langle Float \rangle\!\rangle \\
\mid &\; access\_value \langle\!\langle optional\ View \times optional\ SubprogramLabel \rangle\!\rangle \\
\mid &\; record\_value \langle\!\langle (optional\ Tag) \times Binding \times Binding \rangle\!\rangle \\
\mid &\; array\_value \langle\!\langle \{\ B : Array\_bounds, v : (\text{seq}\ Value) \nrightarrow Value \mid \text{dom}\ v = indices(B)\ \} \rangle\!\rangle
\end{aligned}
$$

We can define various sets of values referred to in the language rules:

$$Discrete\_value == \text{ran}\ discrete\_value$$

$$Real\_value == \text{ran}\ real\_value$$

$$Access\_value == \text{ran}\ access\_value$$

$$Scalar\_value == Discrete\_values \cup Real\_values$$

$$Elementary\_value == Scalar\_values \cup Access\_values$$

$$Composite\_value == \text{ran}\ record\_value \cup \text{ran}\ array\_value$$

## 3.5  Types and Subtypes

Every type has an associated *type descriptor* giving the characteristics of the type (and possibly referring to other types via their type locations).

The descriptors are defined here, but described in the sections that follow.

$$
\begin{aligned}
Type\_Descriptor ::= &\; enumeration\_dsc \langle\!\langle \mathbb{N}_1 \rangle\!\rangle \\
\mid &\; signed\_integer\_dsc \langle\!\langle \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \rangle\!\rangle \\
\mid &\; modular\_integer\_dsc \langle\!\langle \mathbb{N}_1 \rangle\!\rangle \\
\mid &\; universal\_integer\_dsc \langle\!\langle \mathbb{Z} \times \mathbb{Z} \rangle\!\rangle \\
\mid &\; float\_dsc \langle\!\langle \mathbb{N}_1 \times Rational \times Rational \times Float\_Implementation \rangle\!\rangle \\
\mid &\; \ldots (\text{something for fixed-point types}) \\
\mid &\; array\_dsc \langle\!\langle (\text{seq}_1\ Subtype) \times Subtype \rangle\!\rangle \\
\mid &\; record\_dsc \langle\!\langle (optional\ Tag) \times Discriminant\_descriptor \times Component\_list\_descriptor \rangle\!\rangle \\
\mid &\; class\_dsc \langle\!\langle Type\_location \rangle\!\rangle \\
\mid &\; access\_dsc \langle\!\langle Subtype\_location \times Access\_Mode \rangle\!\rangle \\
\mid &\; \ldots
\end{aligned}
$$

A *type* is then a combination of an optional parent (in case the type was derived) plus a descriptor.

$$Type ::= (\mathit{optional\ Type\_location}) \times \mathit{Type\_Descriptor}$$

For each kind of type in Ada 9X, we define a type descriptor. Additionally, for each descriptor we define the set of values of the type:

$$descriptor\_values : Type\_Descriptor \times State \nrightarrow \mathbb{P}_1\ Value$$

Function *type_values* gives the set of values associated with a type location given a state:

$$type\_values : Type\_location \times State \rightarrow \mathbb{P}\ Value$$
$$\forall\, l : Type\_location;\ S : State \bullet type\_values(l, S) =$$
$$\quad descriptor\_values(snd(the\_store(S).types(u)), S)$$

Note that these sets of values might change over time as the information about a type is updated.

## 3.5.1  Subtypes and Constraints

A subtype is a combination of a type, a constraint, and certain attributes [3.2(8)]. There are in fact two sorts of subtypes; we will call them "partial" subtypes and "true" subtypes. Partial subtypes can contain unevaluated *per-object constraints*, for example, references to discriminants. These partial subtypes appear as the subtypes of components of a record with discriminants. When an object of a subtype is created, some of these per-object constraints are elaborated and the true subtype of the object and its components is determined.

There are several cases where a partial subtype cannot be elaborated: in a variant record, per-object constraints in initially unused components are not elaborated; in an initialized object, *none* of the per-object constraints are elaborated. The Reference Manual is not completely clear on this point, and for now we will only consider per-object constraints that are references to discriminants.

Partial subtypes appear only as the subtypes of components of types with discriminants; named subtypes, and the subtypes of objects, will always be "true" subtypes.

The Reference Manual identifies three kinds of constraints: range constraints, index constraints, and discriminant constraints. In fact, the last two can also be applied indirectly, to an access type having a designated subtype to which the constraint would apply directly. (Only one level of indirection is allowed; given

```
type A1 is access String;
type A2 is access A1;
```

an index constraint can be applied to A1, but not to A2.) We may find it useful to distinguish these indirect constraints from their direct counterparts.

$$
\begin{aligned}
Constraint ::=\ &no\_constraint \\
&|\ range\_constraint \langle\!\langle Range \rangle\!\rangle \\
&|\ index\_constraint \langle\!\langle \mathrm{seq}_1\ Discrete\_range \rangle\!\rangle \\
&|\ discriminant\_constraint \langle\!\langle Binding \rangle\!\rangle \\
&|\ indirect\_index\_constraint \langle\!\langle \mathrm{seq}_1\ Discrete\_range \rangle\!\rangle \\
&|\ indirect\_discriminant\_constraint \langle\!\langle Binding \rangle\!\rangle
\end{aligned}
$$

Some values *satisfy* a constraint:

$$\underline{\quad} \; satisfies \; \underline{\quad} : Value \leftrightarrow Constraint$$

$$\forall\, v : Value \bullet v \; satisfies \; no\_constraint$$

$$\forall\, v : Value \bullet v \; satisfies \; range\_constraint(R) \Leftrightarrow v \; belongs\_to \; R$$

$$array\_value(B, a) \; satisfies \; index\_constraint(S) \Leftrightarrow B = S$$

$$record\_value(t, d, r) \; satisfies \; discriminant\_constraint(d') \Leftrightarrow d = d'$$

Now we can define subtypes:

$$\boxed{\begin{array}{l} Subtype \\ \hline type : Type\_location \\ constraint : Constraint \\ attributes : Attributes \end{array}}$$

For every subtype, there is an associated set of values, namely the values of the associated type that satisfy the constraint.

$$subtype\_values : Subtype \to State \to \mathbb{P}\; Value$$

$$\forall\, S : State;\; s : Subtype \mid s.type \in \mathrm{dom}\; the\_store(S).types \bullet$$
$$subtype\_values(s, S) = \{\; v : Value \mid v \in type\_values(s.type, S) \wedge v \; satisfies \; s.constraint \;\}$$

We use function *subtype* to create subtype values:

$$subtype : Type\_location \times Constraint \times Attributes \to Subtype$$

$$subtype(t, c, a).type = t$$
$$subtype(t, c, a).constraint = c$$
$$subtype(t, c, a).attributes = a$$

### 3.5.2   Partial Subtypes

Partial constraints are similar to constraints, except they may contain references to discriminants in place of values.

$$Partial\_value \qquad\qquad ::= value \langle\!\langle Value \rangle\!\rangle \mid discriminant\_ref \langle\!\langle Id \rangle\!\rangle$$

$$Partial\_discrete\_range == Partial\_value \times Partial\_value$$

$$Partial\_constraint \qquad ::= no\_constraint$$
$$\mid range\_constraint \langle\!\langle Partial\_discrete\_range \rangle\!\rangle$$
$$\mid index\_constraint \langle\!\langle \mathrm{seq}_1\; Partial\_discrete\_range \rangle\!\rangle$$
$$\mid discriminant\_constraint \langle\!\langle Id \nrightarrow Partial\_value \rangle\!\rangle$$
$$\mid indirect\_index\_constraint \langle\!\langle \mathrm{seq}_1\; Partial\_discrete\_range \rangle\!\rangle$$
$$\mid indirect\_discriminant\_constraint \langle\!\langle Id \nrightarrow Partial\_value \rangle\!\rangle$$

A partial subtype combines a subtype and a partial constraint. (Using the subtype allows us to do a "dependent compatibility check" at the right time, and also gives us the needed attributes when we actualize.)

$$Partial\_subtype == Subtype \times Partial\_constraint$$

Given a mapping from discriminant names to values, a partial constraint can be turned into a true constraint.

$$actualize\_value : Binding \rightarrow Partial\_value \nrightarrow Value$$
$$actualize\_partial\_range : Binding \rightarrow Partial\_discrete\_range \nrightarrow Range$$
$$actualize\_constraint : Binding \rightarrow Partial\_constraint \nrightarrow Constraint$$
$$actualize\_subtype : Binding \rightarrow Partial\_subtype \nrightarrow Subtype$$

$$actualize\_value\ f\ (value\ v) = v$$
$$actualize\_value\ f\ (discriminant\_ref\ n) = f(n)$$

$$actualize\_partial\_range\ f\ (l, h) =$$
$$discrete\_range(actualize\_value\ f\ l, actualize\_value\ f\ h)$$

$$actualize\_constraint\ f\ no\_constraint = no\_constraint$$

$$actualize\_constraint\ f\ (range\_constraint(l, h)) =$$
$$range\_constraint(actualize\_partial\_range\ f\ (l, h))$$

$$actualize\_constraint\ f\ (index\_constraint\ s) =$$
$$index\_constraint((actualize\_partial\_range\ f) \circ s)$$

$$actualize\_constraint\ f\ (discriminant\_constraint\ d) =$$
$$discriminant\_constraint((actualize\_value\ f) \circ d)$$

$$actualize\_constraint\ f\ (indirect\_index\_constraint\ s) =$$
$$indirect\_index\_constraint((actualize\_partial\_range\ f) \circ s)$$

$$actualize\_constraint\ f\ (indirect\_discriminant\_constraint\ d) =$$
$$indirect\_discriminant\_constraint((actualize\_value\ f) \circ d)$$

$$actualize\_subtype\ f\ s =$$
$$\mu\ Subtype\ |\ type = s.type\ \wedge$$
$$constraint = actualize\_constraint\ f\ s.constraint\ \wedge$$
$$attributes = s.attributes$$

### 3.5.3  Derived Types and Classes

A derived type is a new entity, but it generally uses a copy of the parent descriptor. The set of values of the derived type is then the same as the set of values of the parent type. However, when a derived type definition furnishes new discriminants or defines a type extension, a new descriptor is needed.

The store records some information about derivation, by recording the (optional) parent type [3.4(1)] of every known type.

$$parent : State \rightarrow (Type\_location \nrightarrow Type\_location)$$

$$parent(S) = \{\ t, t' : Type\_location\ |\ fst(the\_store(S).types(t)) = some(t')\ \}$$

Type extensions are considered in Section 3.5.8. Abstract types are considered in Section 3.5.8.1.

#### 3.5.3.1  Derivation Classes

The descriptor for a class_wide type has the form $class\_dsc(t)$, where $t$ is the $Type\_location$ of the root of the class. The values of this type are the values of all types derived (directly or indirectly) from $t$:

$$descriptor\_values(class\_dsc(t), S) =$$
$$\bigcup\{\ t' : Type\_location\ |\ (u', u) \in parent(S)^* \bullet descriptor\_values(t', S)\ \}$$

The notions of [3.4.1(10)] are easily defined:

18

$$descendant, ancestor : State \rightarrow (Type\_location \leftrightarrow Type\_location)$$

$$ultimate\_ancestor : State \times Type\_location \nrightarrow Type\_location$$

$$ancestor(S) = parent(S)^*$$

$$descendant(S) = ancestor(S)^{-1}$$

$$t \in \mathrm{dom}\ the\_store(S).types \Rightarrow$$
$$ultimate\_ancestor(S, t) = ((\mathrm{ran}\ parent(S)) \lhd ancestor(S))\ t$$

### 3.5.4   Scalar Types

Every scalar type records a base range, in addition to any other needed information.

$$base\_range : Type\_Descriptor \nrightarrow Range$$

Scalar types are either discrete types or real types. A value of discrete type is simply an integer; a value of a real type is a rational number.

Each scalar subtype determines a range, as specified in [3.5(6)]:

$$range\_of\_subtype : Subtype \times Store \nrightarrow Range$$

$$\sigma.constraint = range\_constraint(R) \Rightarrow range\_of\_subtype(\sigma, S) = R$$

$$\sigma.constraint = no\_constraint \Rightarrow$$
$$range\_of\_subtype(\sigma, S) = base\_range(snd(the\_store(S).types(\sigma.type)))$$

#### 3.5.4.1   Enumeration Types

The type descriptor for an enumeration type has the form $enumeration\_dsc(n)$, where $n : \mathbb{N}_1$ gives the number of enumerands

The base range of the enumeration is the set of discrete values with position numbers between $0$ and $n - 1$ (inclusive). The values of an enumeration type are the values in the base range.

$$base\_range(enumeration\_dsc(n)) = discrete\_range(0, n - 1)$$

$$descriptor\_values(enumeration\_dsc(n), S) = discrete\_value(\lvert 0 \mathinner{\ldotp\ldotp} n - 1 \rvert)$$

#### 3.5.4.2   Character Types

Character types are simply enumeration types.

#### 3.5.4.3   Boolean Types

Boolean types are simply enumeration types.

#### 3.5.4.4   Integer Types

There are three descriptors for integer types:

- $signed\_integer\_dsc(bf, bl, f, l)$, with $bf, bl, f, l : \mathbb{Z}$ satisfying (according to [3.5.4(7)]),

    1. $bf \leq 0 \leq bl$,
    2. $bf + bl \in \{-1, 0\}$, and
    3. $\{f, l\} \subseteq bf \mathinner{\ldotp\ldotp} bl$.

The base range of this type is $bf \mathinner{\ldotp\ldotp} bl$.

- $modular\_integer\_dsc(m)$, with $m : \mathbb{N}_1$. (The base range is $0 \mathinner{\ldotp\ldotp} (m - 1)$ [3.5.4(7)].

- $universal\_integer\_dsc(bf, bl)$ for $bf, bl : \mathbb{Z}$ (although the base range seems to be irrelevant here).

`root_integer` is just a particular signed integer type.

In every case, the set of valid values of the type consists of all discrete values [3.5.4(6)].

$$descriptor\_values(signed\_integer\_dsc(bf, bl, f, l), S) = discrete\_value(\!|\mathbb{Z}|\!) \cup Invalid\_value$$

$$descriptor\_values(modular\_integer\_dsc(m), S) = discrete\_value(\!|\mathbb{Z}|\!) \cup Invalid\_value$$

$$descriptor\_values(universal\_integer\_dsc(bf, bl), S) = discrete\_value(\!|\mathbb{Z}|\!) \cup Invalid\_value$$

$$base\_range(signed\_integer\_dsc(bf, bl, f, l)) = discrete\_range(bf, bl)$$

$$base\_range(modular\_integer\_dsc(m)) = discrete\_range(0, m - 1)$$

$$base\_range(universal\_integer\_dsc(bf, bl)) = discrete\_range(bf, bl)$$

### 3.5.4.5 Floating Point Types

As acknowledged in the Ada 9X Rationale, the core language leaves the semantics of floating point operations largely unspecified. By contrast, the floating point annex (Annex G) is quite precise—though some flaws in the annex will be noted below. Therefore our model has two parts, one for the core and the other for Annex G.

The semantics of the Reference Manual refers to the underlying machine values and operations, and makes features of them visible, for example, in the values of attributes. We have attempted to model this semantics directly, so that it will be clear how to tell whether an actual implementation satisfies the semantic rules. This provides a model from the point of view of the implementor. It would have been easier (and from some points of view, perhaps, preferable) to make a model from the user's point of view: e.g., take the values of the attributes as given and simply state axiomatically, in terms of the attributes, the resulting constraints on the values returned by the predefined operations. The user's model is, of course, a consequence of the implementor's model.

The descriptor for a floating point type has four components:

$$float\_dsc\langle\!\langle \mathbb{N}_1 \times Rational \times Rational \times Implementation \rangle\!\rangle$$

The first three components are provided directly by the type's definition: the requested precision and the bounds of its constraint. The fourth component characterizes the chosen implementation of the type. The descriptor for an integer type contains a component with analogous information, namely, the bounds of the underlying base type. We could represent the fourth component in a finitary way by listing the values of a large number of floating point attributes determined by the implementation. Instead, this component of the descriptor will consist of a model of the implementation itself, from which the attributes can be calculated.

$$descriptor\_values(float\_dsc(n, v, v', imp), S) = real\_value(\!|Float|\!)$$
$$base\_range(float\_dsc(n, v, v', imp)) = inf(imp.ma.numbers) \mathinner{\ldotp\ldotp} sup(imp.ma.numbers)$$

### 3.5.4.6 The core model of floating point

The values of a floating point type are rationals, with the possible addition of some extra things like signed zeroes or NaN's. For now these extra possibilities are ignored.

$$Float == Rational \cup \ldots$$

There is a problem in the Reference Manual: The possibility of signed zeroes or NaN's is incompatible with [RM-83 3.5.7(8)], which says that the set of values for a floating point type is the set of rational numbers.

**3.5.4.6.1  Machine arithmetics**  Elaboration of a floating point type declaration includes the choice of an appropriate *Implementation* (from some predefined non-empty finite set of them) to model the type. One component of an implementation is a *machine arithmetic*, which consists of a radix, a set of machine numbers, and relations modeling the predefined binary and unary floating point operations. Floating point operations will be modeled not as functions but as relations, in order to model their potential non-determinism. Some of the predefined binary floating point operations return floats and some return booleans; all unary operations return floats. It is convenient to add a special "return value," *overflow*, to represent the possibility of overflow:

$$FloatResult ::= overflow \mid result \langle\!\langle Float \rangle\!\rangle$$

$$BinOpFloat == Float^2 \leftrightarrow FloatResult$$

$$BinOpBool == Float^2 \leftrightarrow Boolean$$

$$UnOp == Float \leftrightarrow FloatResult$$

It will also be handy to have an operation that extracts the (non-overflow) *Float* values from a set of *FloatResult*s:

$$\begin{array}{|l}
\mathit{floats\_of} : \mathbb{P}\ FloatResult \rightarrow Float \\
\hline
\mathit{floats\_of}(X) = result^\sim (\!| X |\!)
\end{array}$$

In schema *MachineArithmetic*:

- *radix* is the radix of the machine representation

- *numbers* is the set of machine numbers—that is, the set of storable values that will "fit" in any variable of the type.

- *plus*, *equals*, ..., are relations modeling the predefined floating point operations; *convert* represents type conversion of an arbitrary real value to a machine number of this arithmetic.

$$\begin{array}{l}
\underline{MachineArithmetic}\\
\quad radix : \mathbb{N}_1\\
\quad numbers : \mathbb{F}_1\ Float\\
\quad plus : BinOpFloat\\
\quad \dots\\
\quad equals : BinOpBool\\
\quad \dots\\
\quad uminus : UnOp\\
\quad \dots\\
\quad convert : UnOp\\
\quad float\_outcomes : \mathbb{P}\ Float\\
\hline
\quad float\_outcomes =\\
\qquad numbers \cup floats\_of(\mathrm{ran}\ plus) \cup \dots \cup floats\_of(\mathrm{ran}\ convert)\\
\quad (float\_outcomes)^2 \subseteq \mathrm{dom}\ plus\\
\quad \dots\\
\quad (float\_outcomes)^2 \subseteq \mathrm{dom}\ equals\\
\quad \dots\\
\quad float\_outcomes \subseteq \mathrm{dom}\ uminus\\
\quad \dots\\
\quad Float \subseteq \mathrm{dom}\ convert\\
\quad \mathrm{ran}\ convert \subseteq ma.numbers\\
\quad sup(numbers) \le -inf(numbers)
\end{array}$$

Notice that operations like *plus* are not restricted to returning machine numbers of the type as values. The machine numbers represent the storable values of the type, but operations may return, e.g., extra-precision values that are not immediately rounded.

The axioms involving *float_outcomes* are technical conditions guaranteeing that the (non-overflow) results of any operation can legitimately be passed as arguments to any of the others.

The concluding inequality is all we can represent formally of paragraph 3.5.7(8):

> 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.

**Note:** It would probably be reasonable to suppose that the machine numbers are (roughly) symmetric in a stronger sense: the set of machine numbers between $-sup(numbers)$ and $sup(numbers)$ is closed under additive inverse. The Reference Manual does not require this.

**Note:** This definition could be shortened if we simply assumed that the relations modeling all the predefined operations were total. One reason for *not* making that assumption is the desire that there be an obvious relation between this definition and actual floating point implementations. In representing an actual implementation as a machine arithmetic two principles apply: First, the *plus* relation modeling an actual implementation of + should contain $((x, y), z)$ if $z$ is the actual result (presumably computed by the hardware in some register) of summing $x$ and $y$; and should also include $((x, y), z')$ for every possible "perturbation" $z'$ of $z$ obtained by moving $z$ to and from registers of other precisions or to and from storage. (Similar considerations apply to all other operations.) Second, it is sound to model an implementation by using relations that are supersets of this "minimal" model.

**3.5.4.6.2 Parameters of floating point implementations** We need two kinds of specifications for describing aspects of floating point implementations: A *MachineParam* is a specification requiring that certain floating point numbers actually be machine numbers of an implementation. It

does not constrain the semantics of the floating point operations. The "representation-oriented at-tributes" of a type will be defined to return, essentially, the "strongest" $MachineParam$ satisfied by the type's implementation. (Strictly speaking, we will define what it means for a machine arithmetic to satisfy a $MachineParam$, and a machine arithmetic is only one component of an implementation.) An $AccurParam$ does constrain the behavior of the floating point operations. Annex G will define the "model-oriented attributes" of a type to return, essentially, the strongest $AccurParam$ satisfied by the type's implementation. The core of the Reference Manual says very little about the relation between the implementation and these model attributes.

**3.5.4.6.3  Machine parameters**  A $MachineParam$ is a triple whose elements are interpreted as, respectively, a mantissa length, a minimum exponent, and a maximum exponent.

$$
\begin{array}{|l}
\underline{MachineParam} \underline{\phantom{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx}}\\
mantissa : \mathbb{N}_1 \\
emin : \{\ i : \mathbb{N} \mid i < 0\ \} \\
emax : \mathbb{N}_1
\end{array}
$$

A machine arithmetic satisfies a $MachineParam$ if all the canonical numbers defined in terms of these parameters (and of the machine arithmetic's radix) are machine numbers:

$$
\begin{array}{|l}
sat\_float\_param : MachineArithmetic \leftrightarrow MachineParam \\
\hline
(ma, fp) \in sat\_float\_param \Leftrightarrow \\
\quad BoundedCanonical(ma.radix, fp.mantissa, fp.emin, fp.emax) \subseteq ma.numbers
\end{array}
$$

The $BoundedCanonical$ numbers are defined in Section 3.5.4.6.4. Note that $sat\_float\_param$ does not constrain the operations of the machine arithmetic in any way.

A first $MachineParam$ is "improved by" a second if the second is at least as restrictive a specifi-cation as the first.

$$
\begin{array}{|l}
\_improved\_by\_ : MachineParam \leftrightarrow MachineParam \\
\hline
(p_1, emin_1, emax_1)\ improved\_by\ (p_2, emin_2, emax_2) \Leftrightarrow \\
\quad p_1 \leq p_2 \wedge emin_1 \geq emin_2 \wedge emax_1 \leq emax_2
\end{array}
$$

A $MachineParam$ $fp$ for $ma$ is maximal if $ma$ satisfies $fp$ but satisfies no strict improvement of $fp$. The function $max\_mach\_params(ma)$ returns the set of all maximal $MachineParam$s satisfied by $ma$.

$$
\begin{array}{|l}
max\_mach\_params : MachineArithmetic \rightarrow \mathbb{F}\ MachineParam \\
\hline
max\_mach\_params(ma) = \\
\quad maximal(restrict(\{\ mattr \mid sat\_float\_param(ma, mattr)\ \}, \\
\qquad \_improved\_by\_))
\end{array}
$$

The generic constant $maximal$ returns the set of maximal values of a relation. The generic constant $restrict$ returns the result of restricting both the domain and range of a relation to the same set. These constants are defined in Section 3.1.

There is a problem in the Reference Manual: [RM-83 A.5.3] defines the representation-oriented attributes of a floating point type. They are intended, collectively, to denote a "best" $MachineParam$ satisfied by the machine arithmetic of the type, but the definitions given there are not quite right. In particular, if $ma$ is the machine arithmetic chosen to implement type `T`, the rules of the Reference Manual do not guarantee that

$ma$ $sat\_float\_param$ (`T′machine_mantissa`, `T′machine_emin`, `T′machine_emax`)

although this is surely one intended consequence of the rules.

**3.5.4.6.4    Representations of floating point**    The canonical representions of floating point numbers are defined in the core semantics, Appendix A.

Our definitions will represent fractions with radix $r$ and mantissa length $m$ by length-$m$ sequences of the "digits" $0, \ldots, r-1$. A normal representation is a representation whose first element is non-zero, or which consists solely of zeroes.

$$reps : \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{P}\,seq(\mathbb{N})$$
$$normal\_reps : \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{P}\,seq(\mathbb{N})$$

$$reps(r, m) = 1 \mathinner{\ldotp\ldotp} m \to 0 \mathinner{\ldotp\ldotp} (r-1)$$
$$s \in normal\_reps(r, m) \Leftrightarrow s \in reps(r, m) \wedge$$
$$s(1) = 0 \Rightarrow \forall\, i : \mathrm{dom}(s) \bullet s(i) = 0$$

The operation *fraction_value* returns the fraction represented by the sequence $s$ in radix $r$—that is, the "decimal" $.s(1)s(2) \ldots s(m)$, understood as a literal in base $r$.

$$fraction\_value : \mathbb{N}_1 \times seq(\mathbb{N}_1) \to Rational$$
$$fractions : \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{P}\,Rational$$
$$normal\_fractions : \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{P}\,Rational$$

$$fraction\_value(r, s) = \Sigma_{i=1}^{\#s}\, s(i) * r^{-i}$$
$$fractions(r, m) = fraction\_value(\!|\,reps(r, m)\,|\!)$$
$$normal\_fractions(r, m) = fraction\_value(\!|\,normal\_reps(r, m)\,|\!)$$

The model floating point numbers are those suitably definable in scientific notation, i.e., as fractions times powers of the radix.

$$make\_floats : \mathbb{P}\,Rational \times \mathbb{Z} \times \mathbb{N}_1 \to \mathbb{P}\,Rational$$

$$make\_floats(fracs, exps, rad) =$$
$$\{\, f : Rational, e : \mathbb{N}_1 \mid f \in fracs \wedge e \in exps \bullet \pm f * rad^{\,e} \,\}$$

We are principally interested in two classes of "canonical" floating point numbers:

$$Canonical : \mathbb{N}_1 \times \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{P}\,Rational$$
$$BoundedCanonical : \mathbb{N}_1 \times \mathbb{N}_1 \times \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{P}\,Rational$$

$$Canonical(rad, mant, emin) =$$
$$make\_floats(normal\_fractions(rad, mant), \{\, i : \mathbb{Z} \mid emin \leq i \,\}, rad)$$
$$BoundedCanonical(rad, mant, emin, emax) =$$
$$make\_floats(normal\_fractions(rad, mant),$$
$$\{\, i : \mathbb{Z} \mid emin \leq i \leq emax \,\},$$
$$rad)$$

**3.5.4.6.5    Implementations**    An *Implementation* consists of a machine arithmetic, a *MachineParam* modeling the representation-oriented attributes of the arithmetic, and a boolean indicating the response to numeric overflow. The properties of the machine arithmetic do not uniquely determine the appropriate *MachineParam*.

----- *Implementation* -----------
$ma : MachineArithmetic$
$machine\_attr : MachineParam$
$overflows : Boolean$

$machine\_attr \in max\_mach\_params(ma)$

An *AccurParam* is a 6-tuple whose elements are interpreted as a radix, a mantissa length, a minimum exponent, the bounds for a safe interval, and an indication of whether overflows are to be reported. (The constraints defined by the other parameters are interpreted more strictly if the "overflows" flag is true.)

---
*AccurParam*
$radix, mantissa : \mathbb{N}_1$
$emin : \{\ i : \mathbb{N}\ |\ i < 0\ \}$
$sfirst, slast : Float$
$overflows : Boolean$

---

It is convenient to have an abbreviation for the set of safe numbers that an *AccurParam* defines.

---
$safe : AccurParam \rightarrow \mathbb{P}\ Float$

---
$safe(ap) = ap.sfirst \mathrel{..} ap.slast$

---

We will formalize an essential notion of Annex G with *_has_accuracy_*, which says what it means for an implementation to satisfy an *AccurParam*. From the core model, we can extract only some minimal properties of this relation, expressed in the weaker notion *_has_weak_acc_*:

---
$\_has\_weak\_acc\_ : Implementation \leftrightarrow AccurParam$
$\_has\_accuracy\_ : Implementation \leftrightarrow AccurParam$

---
$imp\ has\_weak\_acc\ ap \Leftrightarrow$
  $ap.radix = imp.ma.radix\ \wedge$
  $ap.mantissa \leq imp.machine\_attr.mantissa\ \wedge$
  $ap.emin \geq imp.machine\_attr.emin\ \wedge$
  $\{\ ap.sfirst, ap.slast\ \} \subseteq ma.numbers\ \wedge$
  $imp.overflows = ap.overflows$
$imp\ has\_accuracy\ ap \Rightarrow imp\ has\_weak\_acc\ ap$

---

For any implementation *imp*, in Annex defines *model_attr(imp)*, a unique "best" *AccurParam* satisfied by an implementation. All we can say in the core semantics is that *imp* satisfies the weak accuracy requirements imposed by *model_attr(imp)*.

---
$model\_attr : Implementation \rightarrow AccurParam$

---
$imp\ has\_weak\_acc\ model\_attr(imp)$

---

More precisely, Annex G defines *model_attr(imp)* to be a particular maximal *ap* such that *imp has_accuracy ap*.

The maximum number of decimal digits of accuracy is uniquely determined by the model-oriented attributes of the implementation.

---
$digits : Implementation \rightarrow \mathbb{N}_1$

---
$imp.radix = 10 \Rightarrow digits(imp) = model\_attr(imp).mantissa$
$imp.radix \neq 10 \Rightarrow$
  $digits(imp) = ceiling($
    $(model\_attr(imp).mantissa * log(10)/log(imp.ma.radix)) + 1$
  $)$

---

There is a problem in the Reference Manual: This definition of "digits" is not given anywhere in the Reference Manual. It is surely the intended one, but it does not seem to follow from anything in the Reference Manual.

There is a problem in the Reference Manual: Section A.5.3(67-68) defines the value of `S'Model_Mantissa` in incompatible ways, depending on whether or not the implementation "supports" Annex G. The same is true for `S'Model_Emin`. In consequence, an implementation can be valid for Core+G but not valid for the Core alone. (By contrast, the core semantics makes the semantics of the model-oriented attributes `'Safe_First` and `'Safe_Last` upward compatible by leaving them implementation-defined.)

The definitions of `S'Model_Mantissa` and `S'Model_Emin` given here are weaker than those of the core semantics. We require only that

$$\text{S}'\texttt{Model\_Mantissa} \quad \leq \quad \text{S}'\texttt{Machine\_Mantissa}$$
$$\text{S}'\texttt{Model\_Emin} \quad \geq \quad \text{S}'\texttt{Machine\_Emin}$$

(See the definition of $\_has\_weak\_acc\_$.)

These definitions make the core semantics compatible with Annex G. In addition, they capture the only information that the present version of the Reference Manual allows a user to rely on across all implementations.

**3.5.4.6.6   Satisfaction of a type definition**   A floating point declaration supplies a requested precision (a value of $\mathbb{N}$) and, optionally, a constraint (two *Rational*s). The accuracy of the type's implementation must be at least as great as the requested precision and the safe range of the implementation must include the interval defined by the constraint. This requirement is captured by the definition of *sat_float_def*.

The Reference Manual says that any such implementation may be chosen. We represent the particular strategy that the implementation uses for choosing the implementation (such as choosing the coarsest acceptable implementation type) by the relation *implements_float_def*. The judgement defining elaboration of a type definition selects an implementation satisfying *implements_float_def*. All the reference manual requires of this relation is that it be consistent with *sat_float_def*:

> $sat\_float\_def , implements\_float\_def :$
> $\quad Implementation \leftrightarrow (\mathbb{N} \times Rational \times Rational)$
> ───
> $(imp , (n , L , R)) \in sat\_float\_def \Rightarrow$
> $\quad L \mathbin{..} R \subseteq model\_attr(imp).sfirst \mathbin{..} model\_attr(imp).slast \land$
> $\quad m \leq digits(imp)$
> $implements\_float\_def \subseteq sat\_float\_def$

**3.5.4.6.7   Attributes**   If *imp* is the implementation chosen for type `T`, then the basic implementation-oriented attribute values of `T` are given as follows, where we let $imp.machine\_attr = (mant, emin, emax)$:

| | | |
|---|---|---|
| `T'Machine_Radix` | $=$ | $imp.ma.radix$ |
| `T'Machine_Mantissa` | $=$ | $mant$ |
| `T'Machine_Emin` | $=$ | $emin$ |
| `T'Machine_Emax` | $=$ | $emax$ |
| `T'Base'First` | $=$ | $min(imp.ma.numbers)$ |
| `T'Base'Last` | $=$ | $max(imp.ma.numbers)$ |

The limits of the base range are the least and greatest machine numbers. This follows from 3.5(6)

> 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

and from 3.5.7(8)

> 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 basic model-oriented attribute values of an implementation *imp* are given as follows (where we let $model\_attr(imp) = (Mant, Emin, sfirst, slast)$):

| | | |
|---|---|---|
| `T'Model_Mantissa` | $=$ | $Mant$ |
| `T'Model_Emin` | $=$ | $Emin$ |
| `T'Safe_First` | $=$ | $sfirst$ |
| `T'Safe_Last` | $=$ | $slast$ |
| `T'Base'Digits` | $=$ | $digits(imp)$ |

The definition of `T'Base'Digits` is something of a guess.

**Note:** The definitions of various attributes, such as `S'Model` (for floating point subtypes) and `S'Machine` (for fixed and floating point subtypes) say that the value returned is obtained "by rounding or truncating" the operand "to either one of the adjacent" model or machine numbers, as appropriate. It is not clear from this language whether these operations are non-deterministic.

### 3.5.4.7 Annex G

Annex G defines some more precise constraints on the floating point operations.

**3.5.4.7.1 Model numbers and accuracy** An accuracy parameter determines a set of model intervals (intervals bounded by the associated canonical real numbers) and associates a model interval with each bounded set (namely, the smallest model interval that contains it):

$$
\begin{array}{|l}
ModelIntervals : AccurParam \to \mathbb{P}\ Float \\
ModelIntOf\ : \mathbb{P}\ Float \times AccurParam \nrightarrow \mathbb{P}\ Float \\
\hline
u \in ModelIntervals(ap) \Leftrightarrow \\
\quad \exists\, lo, hi : Float \bullet \\
\qquad u = lo \mathinner{..} hi \land \\
\qquad \{\ lo, hi\ \} \subseteq Canonical(ap.radix, ap.mantissa, ap.emin) \\
ModelIntOf(X, ap) = \bigcap\{\ u \in ModelIntervals(ap) \mid X \subseteq u\ \}
\end{array}
$$

Given a "paradigm" operation $f$ and an accuracy specification $ap$, we define for each $x$ the set of results that approximate $f(x)$ to within the demands of $ap$—namely, the model interval of the set that results from applying $f$ to the model interval of $x$. (The same applies, *mutatis mutandis*, to the binary operations.) All definitions follow the same pattern, but the type restrictions of Z require us to provide separate definitions for unary operations, binary operations returning floats, and binary operations returning booleans.

$$
\begin{array}{|l}
ResultUnOp : (Float \to Float) \times AccurParam \to (Float \to \mathbb{P}\ Float) \\
ResultBinOpFloat : (Float^2 \to Float) \times AccurParam \to (Float^2 \to \mathbb{P}\ Float) \\
ResultBinOpBool : (Float^2 \to Bool) \times AccurParam \to (Float^2 \to \mathbb{P}\ Bool) \\
\hline
ResultUnOp(f, ap) = \\
\quad \lambda\, x : Float \bullet \\
\qquad ModelIntOf(f(\!|ModelIntOf(\{x\}, ap)|\!), ap) \\
ResultBinOpFloat(f, ap) = \\
\quad \lambda\, x, y : Float \bullet \\
\qquad ModelIntOf(f(\!|ModelIntOf(\{x\}, ap) \times ModelIntOf(\{y\}, ap)|\!), ap) \\
ResultBinOpBool(f, ap) = \\
\quad \lambda\, x, y : Float \bullet \\
\qquad ModelIntOf(f(\!|ModelIntOf(\{x\}, ap) \times ModelIntOf(\{y\}, ap)|\!), ap)
\end{array}
$$

Operands are "safe for" a paradigm operation if they and all their approximate results are safe.

$$SafeForUnOp : (Float \rightarrow Float) \times AccurParam \rightarrow \mathbb{P}\,Float$$
$$SafeForBinOpFloat : (Float^2 \rightarrow Float) \times AccurParam \rightarrow \mathbb{P}\,Float^2$$
$$SafeForBinOpBool : (Float^2 \rightarrow Bool) \times AccurParam \rightarrow \mathbb{P}\,Float^2$$

$$SafeForUnOp(f, ap) =$$
$$\{\ x \in safe(ap) \mid ResultUnOp(f, ap)(x) \subseteq safe(ap)\ \}$$
$$SafeForBinOpFloat(f, ap) =$$
$$\{\ (x, y) \in (safe(ap))^2 \mid ResultBinOpFloat(f, ap)(x, y) \subseteq safe(ap)\ \}$$
$$SafeForBinOpBool(f, ap) =$$
$$\{\ (x, y) \in (safe(ap))^2 \mid ResultBinOpFloat(f, ap)(x, y) \subseteq safe(ap)\ \}$$

A *UnOp* approximates a "paradigm" function to within some accuracy specification if it associates all operands with results that are acceptable approximations to that function. The same goes for *BinOpFloat*s and *BinOpBool*s. In particular, safe operands may not return an *overflow*; and if the "overflows" flag is true, unsafe operands must return either an approximately correct result or the *overflow* token.

$$\_Approx\,UnOp\_ : UnOp \leftrightarrow (Float \rightarrow Float) \times AccurParam$$
$$\_Approx\,BinOpFloat\_ : BinOpFloat \leftrightarrow (Float^2 \rightarrow Float) \times AccurParam$$
$$\_Approx\,BinOpBool\_ : BinOpBool \leftrightarrow (Float^2 \rightarrow Float) \times AccurParam$$

$$op\,Approx\,UnOp\,(f, ap) \Leftrightarrow$$
$$\quad \forall x \in \mathrm{dom}\,op \bullet$$
$$\qquad (x \in SafeForUnOp(f, ap) \Rightarrow$$
$$\qquad\quad overflow \notin op(\!|\{\ x\ \}|\!)$$
$$\qquad\quad \wedge$$
$$\qquad\quad floats\_of(op(\!|\{\ x\ \}|\!)) \subseteq ResultUnOp(f, ap)(x))$$
$$\qquad \wedge$$
$$\qquad (ap.overflows = true \Rightarrow$$
$$\qquad\quad floats\_of(op(\!|\{\ x\ \}|\!)) \subseteq ResultUnOp(f, ap)(x))$$
$$op\,Approx\,BinOpFloat\,(f, ap) \Leftrightarrow$$
$$\quad \forall (x, y) \in \mathrm{dom}\,op \bullet$$
$$\qquad ((x, y) \in SafeForBinOpFloat(f, ap) \Rightarrow$$
$$\qquad\quad overflow \notin op(\!|\{\ (x, y)\ \}|\!)$$
$$\qquad\quad \wedge$$
$$\qquad\quad floats\_of(op(\!|\{\ (x, y)\ \}|\!)) \subseteq ResultBinOpFloat(f, ap)(x, y))$$
$$\qquad \wedge$$
$$\qquad (ap.overflows = true \Rightarrow$$
$$\qquad\quad floats\_of(op(\!|\{\ (x, y)\ \}|\!)) \subseteq ResultBinOpFloat(f, ap)(x, y))$$
$$op\,Approx\,BinOpBool\,(f, ap) \Leftrightarrow$$
$$\quad \forall (x, y) \in \mathrm{dom}\,op \bullet$$
$$\qquad ((x, y) \in SafeForBinOpBool(f, ap) \Rightarrow$$
$$\qquad\quad overflow \notin op(\!|\{\ (x, y)\ \}|\!)$$
$$\qquad\quad \wedge$$
$$\qquad\quad floats\_of(op(\!|\{\ (x, y)\ \}|\!)) \subseteq ResultBinOpBool(f, ap)(x, y))$$
$$\qquad \wedge$$
$$\qquad (ap.overflows = true \Rightarrow$$
$$\qquad\quad floats\_of(op(\!|\{\ (x, y)\ \}|\!)) \subseteq ResultBinOpBool(f, ap)(x, y))$$

We can now define the property *_has_accuracy_* as the assertion that each machine operation approximates the appropriate paradigm function to within the given accuracy parameters:

$$imp\ has\_accuracy\ ap \Leftrightarrow$$
$$\quad imp\ has\_weak\_acc\ ap \wedge$$
$$\quad imp.ma.plus\ ApproxBinOpFloat\,(+, ap) \wedge$$
$$\quad \ldots$$
$$\quad imp.ma.equals\ ApproxBinOpBool\,(=, ap) \wedge$$
$$\quad \ldots$$
$$\quad imp.ma.convert\ ApproxUnOp\,(\mathrm{id}\ Float, ap)$$

**3.5.4.7.2 Model-oriented attributes** To define *model_attr* we choose a particular maximal *AccurParam* satisfied by an implementation. (Note: The definitions below do not follow the definition in version 5.0, which is incorrect, but Ken Dritz's subsequent reworking of version 5.0.)

$$best\_mant : \mathbb{P}\ AccurParam \to \mathbb{P}\ AccurParam$$
$$best\_emin : \mathbb{P}\ AccurParam \to \mathbb{P}\ AccurParam$$
$$best\_first : \mathbb{P}\ AccurParam \to \mathbb{P}\ AccurParam$$
$$best\_last : \mathbb{P}\ AccurParam \to \mathbb{P}\ AccurParam$$
$$best\_ap : \mathbb{P}\ AccurParam \to \mathbb{P}\ AccurParam$$

$$best\_ap(X) =$$
$$\quad best\_last(best\_first(best\_emin(best\_mant(X))))$$
$$model\_attr(imp) =$$
$$\quad \mu\ ap : AccurParam \bullet ap \in best_a p(ap' : AccurParam \mid imp\ has\_accuracy\ ap')ap \in best\_mant(X) \Leftrightarrow$$
$$\quad ap \in X \wedge \forall\, ap' : X \bullet ap.mantissa \geq ap'.mantissa$$
$$ap \in best\_emin(X) \Leftrightarrow$$
$$\quad ap \in X \wedge \forall\, ap' : X \bullet ap.emin \leq ap'.emin$$
$$ap \in best\_first(X) \Leftrightarrow$$
$$\quad ap \in X \wedge \forall\, ap' : X \bullet ap.sfirst \leq ap'.sfirst$$
$$ap \in best\_last(X) \Leftrightarrow$$
$$\quad ap \in X \wedge \forall\, ap' : X \bullet ap.slast \geq ap'.slast$$

There is, of course, exactly one *best_ap*:

$$\#best\_ap(\{\ ap : AccurParam \mid imp\ has\_accuracy\ ap\}) = 1$$

### 3.5.5 Array Types

The descriptor for an array type has the form $array\_dsc(i, c)$, where $i : \mathrm{seq}\ Subtype$ is a sequence of discrete subtypes (the *index subtypes*) , and $c : Subtype$ is the component subtype.

$$descriptor\_values(array\_dsc(i, c), S) =$$
$$\quad \{\ B : Index\_bounds, v : (\mathrm{seq}\ Value) \nrightarrow subtype\_values(c, S)$$
$$\qquad \mid Array(B, v) \in Value \wedge B = range\_of\_subtype \circ i$$
$$\qquad \bullet Array(B, v)\ \}$$

#### 3.5.5.1 String Types

String types are just particular array types.

### 3.5.6 Discriminants

Discriminants are specialized components of some composite types. We incorporate discriminants (which might be null) into the descriptor for every type that can have discriminants, in order to avoid a tedious duplication of definitions in similar cases.

This model does not account for access discriminants.

$$Discriminant\_descriptor == Id \xrightarrow{a} Subtype \times optional\ Thunk$$

---

$discriminant\_values : Discriminant\_descriptor \times State \to \mathbb{P}\ Binding$

---

$discriminant\_values(d, S) =$
  $\{\ f : adom\ d \to Values \mid \forall\ n \in adom\ d \bullet f(n) \in subtype\_values(first(d \cdot n), S)\ \}$

### 3.5.7   Record Types

It seems like a waste of effort to describe records with discriminants separately from records without discriminants, as there is a good deal of overlap in the two cases. Thus, we give every record type descriptor discriminants (which may be null).

Similarly, it seems like a big duplication of effort to describe tagged record types separately. Thus, we will give every record descriptor a tag (which may be null in the case of an untagged record).

$$Component\_list\_descriptor ==$$
$$(Id \xrightarrow{a} Partial\_subtype \times optional\ Thunk) \times optional\ Variant\_descriptor$$

A record type descriptor consists of a description of the discriminants (if any), and a component list description. The values of such a descriptor are records with fields for the discriminants, and fields for the other components. The subtypes of these latter fields (and even the exact fields present) may depend on a value of a discriminant.

$descriptor\_values(record\_dsc(t, DA, CL), S) =$
  $\{\ d, r : Binding \mid d \in discriminant\_values(DA, \rho) \land r \in CL\_values(CL, d, S)$
                $\bullet record(t, d, r)\ \}$

A binding giving the values of the discriminants is given to function $CL\_values$, so that the actual subtype of each component can be determined.

---

$CL\_values : Component\_list\_descriptor \times Binding \times State \to \mathbb{P}\ Binding$

---

$CL\_values((A, V), d, S) = \{f, v : Binding \mid \text{dom}\, f = adom\ A\ \land$
        $(\forall\, n \in \text{dom}\, f \bullet f(n) \in Subtype\_values(actualize\_subtype(first(A \cdot n), d), S))$
        $v \in Variant\_values(V, d, S)$
      $\bullet f \cup v\ \}$

#### 3.5.7.1   Variant Parts and Discrete Choices

A variant descriptor has the $Id$ of the discriminant of the variant part, and a mapping from the possible values of this discriminant to component list descriptors.

$$Variant\_descriptor == Id \times (Discrete\_value \nrightarrow Component\_list\_descriptor)$$

---

$Variant\_values : (optional\ Variant\_descriptor) \times Binding \times State \to \mathbb{P}\ Binding$

---

$Variant\_values(none, d, S) = \{\varnothing\}$

$d(n) \in \text{dom} f \Rightarrow Variant\_values(some(n, f), d, S) = CL\_values(f(d(n)), d, S)$

$d(n) \notin \text{dom} f \Rightarrow Variant\_values(some(n, f), d, S) = \{\varnothing\}$

### 3.5.8 Tagged Types and Type Extensions

The model for tagged types has not yet been developed.

#### 3.5.8.1 Abstract Types and Subprograms

[AARM 3.9.3(8.a)] asserts that there are no values of an abstract type. But it is possible to have subprograms for such subtypes, and for non-abstract descendents to inherit them. If we want to say something about the meanings of such subprograms, we probably need to talk about the values of the parameters. (In some sense, these are parameters of type T'Class.)

On the whole, it probably seems easiest to use a model of values as though the type were not abstract; we can also treat abstract subprograms as though their bodies raised `Program_Error`.

### 3.5.9 Access Types

The descriptor for an access type has the form $access\_dsc(s, m)$, where $s : Subtype\_location$ describes the designated subtype of the access type, and $m : Access\_mode$ describes the access mode.

$$Access\_Mode ::= constant\_access \mid all\_access \mid pool\_access$$

A value of an access-to-object type is either a null value, or a view of an object of the designated subtype:

$$descriptor\_values(access\_dsc(s, m), S) =$$
$$\{access\_value(none)\} \cup$$
$$\{ access\_value(some(object\_view(l, s'))) \mid$$
$$the\_store(S).objects(l) \in subtype\_values(the\_store(S).subtypes(s), S) \}$$

#### 3.5.9.1 Incomplete Type Declarations

The descriptor *incomplete* describes an incomplete type. When the full type definition for the type is elaborated, the type environment is updated to reflect the appropriate descriptor for the type.

Note that there is an issue about the first subtype of an incomplete type; it is constrained if there is no discriminant part. However, the first subtype corresponding to the full definition may be unconstrained. (See comment 94-3901.c.)

There are no values of an incomplete type.

## 3.6 States

A *state* combines a store, an external state, and control flow information (in the usual cases), or is *erroneous* or *unpredicted*. We use the state *unpredicted* in those cases where our semantic definition, in the interests of simplicity, makes no prediction about the effect of a program (even though the Standard defines the effect, or calls it *implementation-defined*).

$$State ::= normal \langle\!\langle Store \rangle\!\rangle$$
$$\mid \quad exception \langle\!\langle ExceptionId \times Store \rangle\!\rangle$$
$$\mid \quad exit \langle\!\langle Loop\_Id \times Store \rangle\!\rangle$$
$$\mid \quad proc\_return \langle\!\langle Store \rangle\!\rangle$$
$$\mid \quad func\_return \langle\!\langle Value \times Store \rangle\!\rangle$$
$$\mid \quad intermediate \langle\!\langle Store \rangle\!\rangle$$
$$\mid \quad erroneous$$
$$\mid \quad unpredicted$$

Function *the_store* gives the store associated with a state.

# Chapter 4

# Judgements

This section summarizes the domains and judgements used in the definition of Ada 9X semantics. The details of the domain definitions are given in Chapter 3. The formal definitions of these judgements are given in later sections.

## 4.1 Domains

The definition is based on the concepts, domains and support functions, introduced in Chapter 3. Specifically, it uses the domains listed in Table 4.1

All of these domains are generated by term algebras (subject to the constraints defined in Chapter 3). Constructors for these domains are given below. In addition, the domains of component associations and environments are defined as follows:

$$
\begin{aligned}
CompAssoc &= \text{list}((Id \times (Subtype \times \text{optional}(Thunk)))) \\
Environment &= (Id \twoheadrightarrow View)
\end{aligned}
$$

Also the signatures for all functions (other than contructors) and predicates are given. Note that these signatures are those used in the Prolog representation of judgements and may differ from those given in Chapter 3.

### 4.1.1 Types

The structure of a type is given by a type descriptor of the form:

> **type**    $Type$
>         $enum\_type : integer \rightarrow Type$
>         $modular\_type : integer \rightarrow Type$
>         $signed\_integer\_type : integer \times integer \times integer \times integer \rightarrow Type$
>         $universal\_integer\_type : integer \times integer \rightarrow Type$
>         $array\_type : \text{list}(Subtype) \times Subtype \rightarrow Type$
>         $class\_type : Type\_location \rightarrow Type$
>         $access\_type : Subtype\_location \times Access\_modifier \rightarrow Type$
>         $func\_profile : (Id \xrightarrow{a} Parameter) \times Subtype \rightarrow Type$
>         $proc\_profile : (Id \xrightarrow{a} Parameter) \rightarrow Type$
>         $incomplete\_type : Discriminant \rightarrow Type$
>         $record\_type : \text{optional}(Type\_location) \times Discriminant \times Record\_fields \rightarrow Type$

| | |
|---|---|
| *Access_modifier* | access (type) modifier |
| *Action* | executable actions |
| *Attributes* | subtype attributes |
| *Bool* | truth values (non-Ada) |
| *Choice* | choices |
| *Constraint* | constraints |
| *Discriminant* | discriminants |
| *ExId* | internal names for exception identifiers |
| *Record_fields* | record fields including variants |
| *LValue* | L-values (addresses) |
| *LoopId* | internal names for loop identifiers |
| *Mode* | parameter modes |
| *Object_location* | addresses of top-level objects |
| *Object_mode* | indication of constancy and aliasing |
| *Partial_constraint* | partial constraints |
| *Partial_subtype* | partial subtypes |
| *Partial_value* | partial values |
| *Parameter* | formal parameters |
| *Range* | discrete and real ranges |
| *State* | state of a computation |
| *Store* | model of memory |
| *Subprogram* | subprogram values |
| *Subprogram_label* | unique tags for subprogram access values |
| *Subprogram_location* | addresses for subprogram values |
| *Subtype* | subtypes |
| *Subtype_location* | addresses for subtypes |
| *Thunk* | an expression with its declaration environment |
| *Type* | type descriptors |
| *Type_location* | address space for type information |
| *Value* | runtime values |
| *Variant* | variants |
| *View* | views |

Table 4.1: Domains used in the judgements

Descriptors of this form are stored in the state and are accessed by unique addresses of sort *Type_location*. A derived type is represented by a new name for an existing type descriptor. The use of type names has the advantage that it is easy to deal with cyclic types and type completion. It has the disadvantage that types can be understood only in the context of a state.

The domain *Type_location* contains constants that represent the predefined types of the language:

> **type**  *Type_location*
> *boolean_tn* : *Type_location*
> *character_tn* : *Type_location*
> *universal_integer_tn* : *Type_location*
> *universal_real_tn* : *Type_location*
> *root_integer_tn* : *Type_location*

In the case of tagged types, values of *Type_location* are used as unique tags. The optional *Type_location* component of a record type descriptor defines the tag of the parent type. Values of sort *Type_location* are related by the *ancestor* relation which represents both the derivation and class hierarchy:

> ancestor(*State, Type_location, Type_location*)
> descendant(*State, Type_location, Type_location*)
> ultimate_ancestor(*State, Type_location, Type_location*)

Access modifiers are used in the descriptors of access types with the obvious meaning.

> **type**  *Access_modifier*
> *constant_access* : *Access_modifier*
> *all_access* : *Access_modifier*
> *pool_access* : *Access_modifier*

Discriminants are represented as follows:

> **type**  *Discriminant*
> *discr* : $(Id \overset{a}{\to} (Subtype \times \text{optional}(Thunk))) \to Discriminant$
> $\langle\rangle$ : *Discriminant*

Two discriminants can be combined using:

> discriminant_union : $Discriminant \times Discriminant \to Discriminant$

A thunk represents an expression together with its declaration environment.

> **type**  *Thunk*
> *thunk* : $Environment \times Exp \to Thunk$

A component list represents *actualized* record fields, i.e., record fields that do not contain partial information that depends on discriminant values.

> **type**  $CompAssoc = \text{list}((Id \times (Subtype \times \text{optional}(Thunk))))$

The fields of a, possibly discriminated, record type are represented by the domain

**type**  *Record_fields*
   *fields* : $(Id \overset{a}{\to} (Partial\_subtype \times \text{optional}(Thunk))) \times \text{optional}((Id \times Variant)) \to Record\_fields$

which includes the proper fields (maybe partial) as well as any variant.

Component associations can be constructed from discriminant values and partial component lists or variants:

$actualized\_complist : (Id \nrightarrow Value) \times list((Id \times (Partial\_subtype \times optional(Thunk)))) \rightarrow CompAssoc$
$actualized\_components : (Id \nrightarrow Value) \times Record\_fields \rightarrow CompAssoc$
$actualized\_variants : (Id \nrightarrow Value) \times (Id \times Variant) \rightarrow CompAssoc)$
$append\_components : CompAssoc \times CompAssoc \rightarrow CompAssoc$

A variant part is represented by a pair $(Id \times Variant)$ where the identifier specifies the name of the discriminant and the second component represents the actual fields:

> **type**   *Variant*
>      $variant : list((Choice \times Record\_fields)) \rightarrow Variant$
>      $\langle\rangle : Variant$

Given a discriminant value, the actual record fields of a variant are defined by the predicate

$$the\_variant(\textit{Variant, Value, Record\_fields}).$$

$variant\_union : optional((Id \times Variant)) \times optional((Id \times Variant)) \rightarrow optional((Id \times Variant))$

The representation of subprogram access types uses parameter descriptors of the form:

> **type**   *Parameter*
>      $formal : Mode \times Subtype \times optional(Thunk) \rightarrow Parameter$

where modes are given by:

> **type**   *Mode*
>      $in\_mode : Mode$
>      $out\_mode : Mode$
>      $in\_out\_mode : Mode$

The following predicates define the set of values of a given type (descriptor):

$cl\_value(State, Record\_fields, (Id \nrightarrow Value), (Id \nrightarrow Value))$
$discriminant\_value(State, Discriminant, (Id \nrightarrow Value))$
$variant\_values(State, optional((Id \times Variant)), (Id \nrightarrow Value), (Id \nrightarrow Value))$
$descriptor\_value(State, Type, Value)$

### 4.1.2   Values

The representation of values is straightforward using the definition

> **type**   *Value*
>      $invalid\_val : Value$
>      $discrete\_val : integer \rightarrow Value$
>      $real\_val : real \rightarrow Value$
>      $access\_val : View \times optional(Subprogram\_label) \rightarrow Value$
>      $null : Value$
>      $record\_val : optional(Type\_location) \times (Id \nrightarrow Value) \times (Id \nrightarrow Value) \rightarrow Value$
>      $array\_val : list(Range) \times (list(Value) \nrightarrow Value) \rightarrow Value$

The term *access_val*(...) is used for access to object and access to subprogram values. In the latter case, each time a subprogram access is computed a new unique subprogram label

$$\textbf{type} \quad \textit{Subprogram\_label}$$

is generated. This label is needed to properly model equality of access to subprogram values.

Note that access values are views. This representation is used to determine the actual subtype of an access value.

Ranges are represented as pairs of values in the obvious way.

$$\textbf{type} \quad \textit{Range}$$
$$\textit{discrete\_rng} : \textit{integer} \times \textit{integer} \rightarrow \textit{Range}$$
$$\textit{real\_rng} : \textit{real} \times \textit{real} \rightarrow \textit{Range}$$

The following functions are defined for ranges.

$$\textit{low\_bound} : \textit{Range} \rightarrow \textit{Value}$$
$$\textit{high\_bound} : \textit{Range} \rightarrow \textit{Value}$$
$$\textit{make\_range} : \textit{Value} \times \textit{Value} \rightarrow \textit{Range}$$
$$\textit{base\_range} : \textit{State} \times \textit{Type} \rightarrow \textit{Range}$$
$$\textit{indices} : \text{list}(\textit{Range}) \rightarrow \textit{set}(\text{list}(\textit{Value}))$$

The latter function defines the set of all index vectors that fit a list of (index) ranges.

Sets of (scalar) values are represented using the domain

$$\textbf{type} \quad \textit{Choice}$$
$$\textit{choice\_range} : \textit{Range} \rightarrow \textit{Choice}$$
$$\textit{choice\_value} : \textit{Value} \rightarrow \textit{Choice}$$
$$\textit{choice\_lst} : \text{list}(\textit{Choice}) \rightarrow \textit{Choice}$$
$$\textit{choice\_default} : \textit{Choice}$$

The following are predicates on values

$$\textit{access\_value}(\textit{Value})$$
$$\textit{array\_value}(\textit{Value})$$
$$\textit{belongs\_to}(\textit{Value}, \textit{Range})$$
$$\textit{composite\_value}(\textit{Value})$$
$$\textit{covers}(\textit{Value}, \textit{Choice}, \textit{Bool})$$
$$\textit{discrete\_value}(\textit{Value})$$
$$\textit{elementary\_value}(\textit{Value})$$
$$\textit{real\_value}(\textit{Value})$$
$$\textit{satisfies}(\textit{Value}, \textit{Constraint})$$
$$\textit{scalar\_value}(\textit{Value})$$

### 4.1.3 Subtypes

The definition of subtypes follows the description provided by the Reference Manual:

$$\textbf{type} \quad \textit{Subtype}$$
$$\textit{subtype} : \textit{Type\_location} \times \textit{Constraint} \times \textit{Attributes} \rightarrow \textit{Subtype}$$

Access to the underlying type is indirect through a type location. The present version of the semantics does not use any subtype attributes.

$$\textbf{type} \quad \textit{Attributes}$$
$$\textit{not\_used} : \textit{Attributes}$$

Functions defined for subtypes are

$$range\_of\_subtype : State \times Subtype \rightarrow Range$$
$$ranges\_of\_subtypes : State \times \text{list}(Subtype) \rightarrow \text{list}(Range)$$
$$type\_struct : State \times Subtype \rightarrow Type$$

Constraints are

**type**  $Constraint$
$no\_constraint : Constraint$
$range\_constraint : Range \rightarrow Constraint$
$index\_constraint : \text{list}(Range) \rightarrow Constraint$
$discriminant\_constraint : (Id \nrightarrow Value) \rightarrow Constraint$
$indirect\_index\_constraint : \text{list}(Range) \rightarrow Constraint$
$indirect\_discriminant\_constraint : (Id \nrightarrow Value) \rightarrow Constraint$

In the case of discriminated record types, component subtypes can be *partial* if they depend on discriminant values. This leads to the following definitions of partial counterparts of values, constraints, and subtypes.

**type**  $Partial\_value$
$p\_value : Value \rightarrow Partial\_value$
$discriminant\_ref : Id \rightarrow Partial\_value$

**type**  $Partial\_constraint$
$p\_no\_constraint : Partial\_constraint$
$p\_range\_constraint : (Partial\_value \times Partial\_value) \rightarrow Partial\_constraint$
$p\_index\_constraint : \text{list}((Partial\_value \times Partial\_value)) \rightarrow Partial\_constraint$
$p\_discriminant\_constraint : (Id \nrightarrow Partial\_value) \rightarrow Partial\_constraint$
$p\_indirect\_index\_constraint : \text{list}((Partial\_value \times Partial\_value)) \rightarrow Partial\_constraint$
$p\_indirect\_discriminant\_constraint : (Id \nrightarrow Partial\_value) \rightarrow Partial\_constraint$

**type**  $Partial\_subtype$
$p\_subtype : Subtype \times Partial\_constraint \rightarrow Partial\_subtype$

Given a discriminant constraint, partial entities can be *actualized*. This process is defined by the functions:

$actualized\_partial\_range : (Id \nrightarrow Value) \times (Partial\_value \times Partial\_value) \rightarrow Range$
$actualized\_range\_list : (Id \nrightarrow Value) \times \text{list}((Partial\_value \times Partial\_value)) \rightarrow \text{list}(Range)$
$actualized\_value : (Id \nrightarrow Value) \times Partial\_value \rightarrow Value$
$actualized\_constraint : (Id \nrightarrow Value) \times Partial\_constraint \rightarrow Constraint$
$actualized\_binding\_list : binding(Id \nrightarrow Value) \times \text{list}((Id \times Partial\_value)) \rightarrow \text{list}((Id \times Value))$

The following predicates on subtypes define the taxonomy of RM 3.2:

$$is\_access\_to\_object\_type(State, Subtype)$$
$$is\_access\_to\_subprogram\_type(State, Subtype)$$
$$is\_access\_type(State, Subtype)$$
$$is\_array\_type(State, Subtype)$$
$$is\_boolean\_type(State, Subtype)$$
$$is\_by\_copy\_type(State, Subtype)$$
$$is\_by\_reference\_type(State, Subtype)$$
$$is\_character\_type(State, Subtype)$$
$$is\_composite\_type(State, Subtype)$$
$$is\_discrete\_type(State, Subtype)$$
$$is\_elementary\_type(State, Subtype)$$
$$is\_enumeration\_type(State, Subtype)$$
$$is\_integer\_type(State, Subtype)$$
$$is\_modular\_integer\_type(State, Subtype)$$
$$is\_protected\_type(State, Subtype)$$
$$is\_real\_type(State, Subtype)$$
$$is\_record\_type(State, Subtype)$$
$$is\_scalar\_type(State, Subtype)$$
$$is\_signed\_integer\_type(State, Subtype)$$
$$is\_string\_type(State, Subtype)$$
$$is\_tagged\_type(State, Subtype)$$
$$is\_task\_type(State, Subtype)$$

Other predicates used in the semantics are

$$component\_type((Id \twoheadrightarrow Value), Type, Id, Subtype)$$
$$convert\_return\_value(State, View, Subtype, View)$$
$$range\_constraints(State, \text{list}(Subtype), \text{list}(Range))$$
$$select\_component\_type((Id \twoheadrightarrow Value), Record\_fields, Id, Subtype)$$
$$subtype\_value(State, Subtype, Value)$$
$$test\_in(State, Value, Subtype)$$
$$type\_constraint(Environment, Subtype, Constraint, Type)$$
$$null\_range(Range)$$
$$included\_in(Range, Range)$$
$$values\_in\_range(Range, \text{set}(Value))$$
$$discrete\_range(Range)$$
$$real\_range(Range)$$

Finally, the following predicates describe state transformers related to various checks and conversions related to subtypes.

$$slice\_check(State, Range, Range, State)$$
$$view\_convert(State, Environment, Subtype, View, View, State)$$
$$subtype\_convert(State, Environment, Subtype, Value, Value, State)$$
$$index\_list(State, \text{list}(Range), \text{list}(Value), \text{list}(Value), State)$$
$$return\_check(State, Subtype, State)$$

### 4.1.4  Environments and Views

Environments map identifiers to views.

$$\textbf{type} \quad Environment = (Id \twoheadrightarrow View)$$

An environment is updated using the usual syntax for bindings.

$$\_[\_ \mapsto \_] : Environment \times Id \times View \rightarrow Environment$$

Note that identifiers are assumed to be unique and that all overloading and qualified names have been resolved to unique identifiers.

The lookup of an identifier $I$ in an environment $E$ is written as

$$E \vdash_{lookup} I \Rightarrow V$$

A view describes entities denoted by identifiers as follows:

**type**   *View*
     *object_view* : *LValue* $\times$ *Subtype* $\times$ *Object_mode* $\rightarrow$ *View*
     *loop_view* : *Id* $\rightarrow$ *View*
     *constant_view* : *Value* $\rightarrow$ *View*
     *subtype_view* : *Subtype_location* $\rightarrow$ *View*
     *subprogram_view* : *Subprogram_location* $\times$ (*Id* $\xrightarrow{a}$ *Parameter*) $\times$ optional(*Subtype*) $\rightarrow$ *View*
     *undefined_view* : *View*

Object views include a mode description of the form:

**type**   *Object_mode*
     *variable_object* : *Object_mode*
     *constant_object* : *Object_mode*
     *aliased_object* : *Object_mode*

Whether or not an object may be assigned to depends on its mode:

$$assignable(Object\_mode)$$

Loop views are used in defining exit from named and unnamed loops.

**type**   *LoopId*
     *unnamed* : *LoopId*
     *loop_id* : *Id* $\rightarrow$ *LoopId*

The following predicate defines how the bindings of a parameter association are added to an environment creating the environment in which a subprogram body is executed. Note that the names used in the given parameter association may differ from the names of the formal parameters (due to renaming). The names of the formals are provided by a separate argument.

$$bind\_actuals(Environment, (Id \xrightarrow{a} View), list(Id), Environment)$$

The following constants of sort *ExId* denote the language-defined exceptions (others may be added).

**type**   *ExId*
     *constraint_error* : *ExId*
     *program_error* : *ExId*
     *ex_id* : *Id* $\rightarrow$ *ExId*

New unique names for user-defined exceptions are introduced by static semantics.

### 4.1.5 Memory Model

Values of sort *Store* describe the current binding of addresses to Ada run-time values (of sort *Value*). In our model, there are four different types of addresses (locations). They include type location (see above) as well as locations for objects, subprograms and subtypes.

> **type** *Object_location*
> $loc : integer \rightarrow Object\_location$
>
> **type** *Subprogram_location*
>
> **type** *Subtype_location*

Object locations are associated only with objects that are not components of other objects. Components are specified by the address of the containing object together with a selector sequence. An address together with a selector sequence is a L-value (sort *LValue*).

> **type** *LValue*
> $location : Object\_location \rightarrow LValue$
> $array\_component : LValue \times list(Value) \rightarrow LValue$
> $array\_slice : LValue \times Range \rightarrow LValue$
> $record\_component : LValue \times Id \rightarrow LValue$

Thus, the domain of stores is defined as a 4-tuple as follows:

> **type** *Store*
> $\langle \_,\_,\_,\_ \rangle : (Object\_location \nrightarrow Value) \times$
> $\qquad (Subprogram\_location \nrightarrow Subprogram) \times$
> $\qquad (Type\_location \nrightarrow (\text{optional}(Type\_location) \times Type)) \times$
> $\qquad (Subtype\_location \nrightarrow Subtype) \rightarrow Store$

Individual components of a store can be updated using the following notation:

> $\_[\_ \mapsto_1 \_] : Store \times Object\_location \times Value \rightarrow Store$
> $\_[\_ \mapsto_2 \_] : Store \times Subprogram\_location \times Subprogram \rightarrow Store$
> $\_[\_ \mapsto_3 \_] : Store \times Type\_location \times (\text{optional}(Type\_location) \times Type) \rightarrow Store$
> $\_[\_ \mapsto_4 \_] : Store \times Subtype\_location \times Subtype \rightarrow Store$

Values of sort *State* describe a current store, together with the current status of program execution. A state may represent the propagation of an exception, exit from a subprogram, or exit from a loop.

> **type** *State*
> $exception : ExId \times Store \rightarrow State$
> $exit : LoopId \times Store \rightarrow State$
> $proc\_return : Store \rightarrow State$
> $func\_return : View \times Store \rightarrow State$
> $normal : Store \rightarrow State$

The following functions are defined to access and manipulate the store embedded in a state.

$$\_[\_ \mapsto_1 \_] : State \times Object\_location \times Value \to State$$
$$\_[\_ \mapsto_2 \_] : State \times Subprogram\_location \times Subprogram \to State$$
$$\_[\_ \mapsto_3 \_] : State \times Type\_location \times (\text{optional}(Type\_location) \times Type) \to State$$
$$\_[\_ \mapsto_4 \_] : State \times Subtype\_location \times Subtype \to State$$
$$\_^{obj}[\_] : State \times Object\_location \to Value$$
$$\_^{spg}[\_] : State \times Subprogram\_location \to Subprogram$$
$$\_^{typ}[\_] : State \times Type\_location \to (\text{optional}(Type\_location) \times Type)$$
$$\_^{stp}[\_] : State \times Subtype\_location \to Subtype$$
$$make\_state : State \times Store \to State$$
$$the\_store : State \to Store$$

The allocation of new location of the four different kinds is defined by the predicates:

$$new\_type(State, (\text{optional}(Type\_location) \times Type), Type\_location, State)$$
$$new\_subtype(State, Subtype, Subtype\_location, State)$$
$$new\_object(State, Value, Object\_location, State)$$
$$new\_subprogram(State, Subprogram, Subprogram\_location, State)$$

For a given state and L-value, the following predicate defines the current value. The definition of this predicate includes access of the appropriate subobjects denoted by an L-value.

$$content(State, LValue, Value)$$

States are classified as normal or abnormal. Abnormal states will, in general, alter the control flow.

$$abnormal\_state(State)$$
$$normal\_state(State)$$

The return from a subprogram may be indicated by an abnormal state. The following predicates deal with the cases of procedure and function returns, respectively.

$$proc\_exit(State, State)$$
$$return\_value(State, View, State)$$

Values stored in the subprogram component of a store are of the form:

**type** $Subprogram$
$subprogram : Environment \times \text{list}(Id) \times Dcl \times Stm \to Subprogram$
$operator : Operator \to Subprogram$
$unelaborated : Subprogram$

A user-declared subprogram is represented by the declaration environment, the names of the formal parameters and the declarations and statements that comprise the body. Predefined operators of the language are enumerated by a domain $Operator$. The definition of the semantics of the operators is not covered. An attempt to execute a subprogram of the form $unelaborated$ will raise program error.

### 4.1.6   Other Predicates

The following predicates deal with the selection of elements from parameter lists and record component associations.

$$the\_parameter(\text{list}(Pss), Id, Nam)$$
$$given\_parameter(\text{list}(Pss), Id, Exp)$$
$$find\_component(Id, \text{list}(Rca), Exp)$$

## 4.2  Judgements

Judgements for various syntactic domains define the effect of the elaboration or execution of language phrases of this domain. In most cases, the effect of a phrase depends on the current state and the current environment. The effect typically consists of a change in state and the possible return of a result. Depending on the kind of phrase, the result may be a value, a type, a new environment and so on. The meaning of some phrases depends on additional context beyond the state and the environment. For instance, the meaning of a type definition depends on the discriminant (which is part of the enclosing type declaration).

The general form of a judgement is

$$state, environment, context \vdash language\text{-}phrase \Rightarrow result, new\text{-}state$$

The following is a list of the judgements used in the definition. For each syntactic domain, the signature of the judgement is given together with an informal rationale.

If the evaluation of a construct raises an exception then the final state represents this information. The propagation of exceptions is described as part of the sequencing of actions described below.

The following conventions are used throughout the description of judgements:

| | | |
|---|---|---|
| $S_1 : State$ | – | The initial state. |
| $E : Environment$ | – | The environment. |
| $S_2 : State$ | – | The final state. |

### 4.2.1  Declarations

The effect of elaborating a (sequence of) declaration(s) is to add bindings corresponding to the newly introduced identifiers to the environment. The elaboration of a declaration may also affect the state.

$$S_1, E_1 \vdash_{dcl} \mathsf{Dcl} \Rightarrow E_2, S_2$$

| | | |
|---|---|---|
| $E_1 : Environment$ | – | The initial environment |
| $\mathsf{Dcl} : Dcl$ | – | A declaration. |
| $E_2 : Environment$ | – | A possibly modified environment. |

### 4.2.2  Parameter lists

Elaboration of subprogram declarations is defined in terms of the judgements

$$S_1, E, \vdash_{pas} \mathsf{Pas} \Rightarrow A, S_2$$

| | | |
|---|---|---|
| $\mathsf{Pas} : Pms^{*}$ | – | Formal parameter list. |
| $A : Id \xrightarrow{a} Parameter$ | – | Parameter signature. |

and

$$\vdash_{mod} \mathsf{Mod} \Rightarrow M$$

| | | |
|---|---|---|
| $\mathsf{Mod} : Mde$ | – | Parameter mode. |
| $M : Mode$ | – | Mode representation. |

The latter judgement uses neither states nor the environment.

### 4.2.3 Type Definitions

A type definition is elaborated in the context of a (possible) discriminant association. The result is the first-named subtype. Elaborating a type definition may affect the state and the environment because subexpressions may have side-effects and new internal type names may be bound in the environment.

$$S_1, E_1, D \vdash_{tdf} \mathsf{Tdf} \Rightarrow T, E_2, S_2$$

| | | |
|---|---|---|
| $D : Discriminant$ | – | The discriminant. |
| $\mathsf{Tdf} : Tdf$ | – | A type definition. |
| $T : Subtype$ | – | The resulting subtype. |
| $E_2 : Environment$ | – | The modified environment. |

### 4.2.4 Variant Parts

$$S_1, E, D \vdash_{vrn} \mathsf{Vrn} \Rightarrow V, S_2$$

| | | |
|---|---|---|
| $D : Discriminant$ | – | A discriminant. |
| $\mathsf{Vrn} : Vnt^*$ | – | A list of variant clauses. |
| $V : Variant$ | – | The resulting variant. |

The judgement always uses a discriminant that may be empty.

### 4.2.5 Discriminant Parts

The evaluation of a discriminant part results in an association that maps discriminant identifiers into their subtype and optional initialization. As with record component lists, the initialization is represented by a thunk.

$$S_1, E \vdash_{dsc} \mathsf{Dcp} \Rightarrow D, S_2$$

| | | |
|---|---|---|
| $\mathsf{Dcp} : Dcp$ | – | A discriminant part. |
| $D : Discriminant$ | – | The resulting association. |

### 4.2.6 Component Lists

The result of evaluating a record component list is an association that maps each component identifier into a pair consisting of the component's subtype and an optional initialization. The initialization is given by a *thunk* that represents the initialization expression, together with the environment in which this expression is to be evaluated.

$$S_1, E \vdash_{cmp} \mathsf{Cmp} \Rightarrow C, S_2$$

| | | |
|---|---|---|
| $\mathsf{Cmp} : Cmp$ | – | A component list. |
| $C : CompAssoc$ | – | The result. |

### 4.2.7 Subtype Indications

There are three flavors of judgements dealing with subtype indications. The normal case is covered by the declaration:

$$S_1, E \vdash_{sif} \mathsf{Sid} \Rightarrow T, S_2$$

$$\text{Sid} : \textit{Sid} \quad - \quad \text{A subtype indication.}$$
$$T : \textit{Subtype} \quad - \quad \text{The denoted subtype.}$$

A special case is needed for subtype indications that appear inside discriminated records because the result will be a partial subtype.

$$S_1, E_1, D \vdash_{psi} \text{Sid} \Rightarrow T, E_2, S_2$$

| | | |
|---|---|---|
| $D : \textit{Discriminant}$ | – | A discriminant. |
| $\text{Sid} : \textit{Sid}$ | – | A subtype indication. |
| $T : \textit{Partial\_subtype}$ | – | The denoted partial subtype. |

Finally, a third form of this judgement is needed to deal with access types to allow references to incomplete types. Instead of a subtype, this judgement returns a subtype location.

$$S_1, E \vdash_{sif_i} \text{Sid} \Rightarrow L, S_2$$

| | | |
|---|---|---|
| $\text{Sid} : \textit{Sid}$ | – | A subtype indication. |
| $L : \textit{Subtype}$ | – | A subtype location. |

A completing type declaration will initialize the subtype location.

### 4.2.8  Statements

The execution of a statement only affects the state and has no result.

$$S_1, E \vdash_{stm} \text{Stm} \Rightarrow S_2$$

$$\text{Stm} : \textit{Stm} \quad - \quad \text{A statement.}$$

### 4.2.9  Elsif Clauses

An elsif-clause consists of a condition and a sequence of statements. The judgement for this construct describes the evaluation of the condition followed by the conditional execution of the statements. There is a boolean result that indicates whether the condition was true. This result is used in the definition of cascaded elsif clauses.

$$S_1, E \vdash_{elf} \text{Eif} \Rightarrow B, S_2$$

| | | |
|---|---|---|
| $\text{Eif} : \textit{Eif}$ | – | An elsif clause. |
| $B : \textit{Bool}$ | – | The boolean result. |

### 4.2.10  Case Alternatives

The evaluation of a list of case alternatives depends on the value of the case selector:

$$S_1, E, V \vdash_{clt} \text{Alt} \Rightarrow B, S_2$$

| | | |
|---|---|---|
| $V : \textit{Value}$ | – | The value of the case selector. |
| $\text{Alt} : \textit{Alt}$ | – | A sequence of case alternatives. |
| $B : \textit{Bool}$ | – | True, if one of the alternatives has matched the case selector. |

The boolean result indicates whether one of the alternatives has been executed. The execution of the enclosing case statement will have to terminate in an exception if this result is false.

### 4.2.11 Discrete Choice Lists

Discrete choice lists are used in variant, array aggregates and case statements. The following judgement describes the evaluation of a list of choices. The result is a representation of the choices.

$$S_1, E \vdash_{chc} \mathsf{Dch} \Rightarrow C, S_2$$

$$
\begin{array}{lll}
\mathsf{Dch} : Dch^* & - & \text{A discrete choice list.} \\
C : Choice & - & \text{The representation of the choice list.}
\end{array}
$$

### 4.2.12 Expressions

The evaluation of an expression results in a value and possible side-effects. In certain cases the meaning of an expression depends on the expected type (e.g., the evaluation of aggregates and string literals). Rather than adding this type information to the judgement, the abstract syntax provides such information where necessary.

$$S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2$$

$$
\begin{array}{lll}
\mathsf{Exp} : Exp & - & \text{An expression.} \\
V : Value & - & \text{The resulting value.}
\end{array}
$$

The judgement for conditions differs from that for expressions by returning a truth value.

$$S_1, E \vdash_{cnd} \mathsf{Cnd} \Rightarrow V, S_2$$

$$
\begin{array}{lll}
\mathsf{Cnd} : Cnd & - & \text{A condition.} \\
B : Bool & - & \text{A truth value.}
\end{array}
$$

### 4.2.13 Names

The evaluation of a name results in a view of the named entity.

$$S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow W, S_2$$

$$
\begin{array}{lll}
\mathsf{N} : Nam & - & \text{A name.} \\
W : View & - & \text{The view denoted by the name.}
\end{array}
$$

The evaluation of certain kinds of names cannot have side-effects (e.g., subtype indications). Rather than defining a separate judgement for this case the definition will require that the initial and final states are identical in these cases.

### 4.2.14 Ranges

The following judgement defines the evaluation of ranges. In the abstract syntax ranges include discrete subtype definitions. The judgement also deals with the definition of the range attribute.

$$S_1, E \vdash_{rng} \mathsf{Rng} \Rightarrow R, S_2$$

$$
\begin{array}{lll}
\mathsf{Rng} : Rng & - & \text{A range or discrete subtype definition.} \\
R : Range & - & \text{The resulting range value.}
\end{array}
$$

### 4.2.15 Record Aggregates

The following judgement defines the value of a record or extension aggregate.

$$S_1, E, C \vdash_{agg_r} \mathsf{Agg} \Rightarrow V, S_2$$

$C : CompAssoc$ – The expected components of the aggregate.
$\mathsf{Agg} : Agg$ – The aggregate.
$V : Id \twoheadrightarrow Value$ – The resulting binding.

The expected type for the aggregate is provided in the abstract syntax by allowing only qualified aggregates. Qualification is added by static analysis where necessary.

### 4.2.16 Array Aggregates

A separate judgement is used for array aggregates. It has an additional sequence of index ranges as context.

$$S_1, E, R, T \vdash_{aag} \mathsf{Agg} \Rightarrow V, S_2$$

$R : \mathrm{list}(Range)$ – The index ranges of the aggregate.
$T : Subtype$ – The type of the elements.
$\mathsf{Agg} : Agg$ – An array aggregate.
$V : Value$ – The array value.

### 4.2.17 Attributes

The following judgement defines the values of (parameterless) attributes as defined in Appendix A of the Reference Manual.

$$S_1, E, W_1 \vdash_{att} \mathsf{Id} \Rightarrow W_2, S_2$$

$W_1 : View$ – A view.
$\mathsf{Id} : Id$ – The attribute name.
$W_2 : View$ – The view of the attribute.

All core language-defined attributes are free of side-effects. This means that the final state will always equal the initial state. Note that some attributes return a subprogram view which, when called, may have a side-effect or raise an exception. But the effect of such calls is not part of evaluating the attribute itself.

In the case of the range attribute, the signature differs as follows:

$$S_1, E, W_1 \vdash_{att_r} \mathsf{range} \Rightarrow R, S_2$$

$W : View$ – A view.
$R : Range$ – A range.

## 4.3 Actions

A sequence of statements is executed by sequentially executing each statement in the sequence. Execution is abandoned if one of the statements raises an exception or causes some other change in the flow of control. In the case of expressions, the language specifies that, in certain cases, several expressions are evaluated in arbitrary order.

In order to systematically define different kinds of order of execution of program parts, the notion of an action is introduced. An action can be viewed as a representation of a judgement without the state. Consider, for instance, the judgement for statements:

$$S_1, E \vdash_{stm} \mathsf{Stm} \Rightarrow S_2$$

The corresponding action is a term

$$statement\_fn(E, \mathsf{Stm})$$

that represents the environment and the statement. For convenience, we shall write actions just like judgements with the initial and final state omitted. In this case, the action is written as

$$E \vdash_{stm} \mathsf{Stm} \Rightarrow$$

Given an action $A$, it is meaningful to talk about the effect of executing the action in a given state $S_0$. This is expressed by the predicate $run$:

$$run(S_0, A, S_1)$$

holds if and only if the execution of action $A$ in state $S_0$ results in state $S_1$.

Using $run$ it is possible to define different orders of evaluation of sets and sequences of actions.

The notation

$$S_0 \left[ \begin{array}{c} A_1 \\ \dots \\ A_n \end{array} \right] S_1$$

means that the actions $A_1$ through $A_n$ are to be executed sequentially starting in state $S_0$ and leading to $S_1$. The definition of this notation needs to consider the propagation of exceptions by any of the actions.

Similarly, the notation

$$S_0 \left\{ \begin{array}{c} A_1 \\ \dots \\ A_n \end{array} \right\} S_1$$

means that the actions $A_1$ through $A_n$ are to be executed in arbitrary order.

The set of actions (sort $Action$) is given by the following terms. There is one action constructor for each judgement.

47

**type** $Action$

$then : \mathrm{list}(Action) \rightarrow Action$

$new\_object\_fn : Value \times Object\_location \rightarrow Action$

$attribute\_fn : Environment \times View \times Id \times View \rightarrow Action$

$param\_attribute\_fn : Environment \times View \times Id \times Value \times View \rightarrow Action$

$case\_alternative\_fn : Environment \times Value \times Alt \times Bool \rightarrow Action$

$choices\_fn : Environment \times Dch\_lst \times Choice \rightarrow Action$

$component\_list\_fn : \quad Environment\times$
$\qquad\qquad\qquad\quad Discriminant\times$
$\qquad\qquad\qquad\quad Cmp\_lst\times$
$\qquad\qquad\qquad\quad (Id \xrightarrow{a} (Partial\_subtype \times \mathrm{optional}(Thunk))) \rightarrow Action$

$constraint\_fn : Environment \times Subtype \times Cns \times Constraint \rightarrow Action$

$compatible\_fn : Environment \times Subtype \times Constraint \rightarrow Action$

$declaration\_fn : Environment \times Dcl \times Environment \rightarrow Action$

$default\_value\_fn : Environment \times Subtype \times Value \rightarrow Action$

$discr\_assoc\_fn : Environment \times Subtype \times Dca \times Constraint \rightarrow Action$

$discriminant\_part\_fn : Environment \times Dcp \times Discriminant \rightarrow Action$

$elsif\_clause\_fn : Environment \times Eif \times Bool \rightarrow Action$

$expression\_fn : Environment \times \mathrm{Exp} \times Value \rightarrow Action$

$name\_fn : Environment \times \mathrm{Nam} \times View \rightarrow Action$

$new\_type\_fn : (\mathrm{optional}(Type\_location) \times Type) \times Type\_location \rightarrow Action$

$range\_fn : Environment \times Rng \times Range \rightarrow Action$

$subtype\_indication\_fn : Environment \times Sid \times Subtype \rightarrow Action$

$p\_subtype\_indication\_fn : Environment \times Discriminant \times Sid \times Partial\_subtype \rightarrow Action$

$type\_definition\_fn : Environment \times Discriminant \times Tdf \times Subtype \times Environment \rightarrow Action$

$variant\_list\_fn : Environment \times Discriminant \times Vnt\_lst \times Variant \rightarrow Action$

$variant\_part\_fn : Environment \times Discriminant \times Vrp \times \mathrm{optional}((Id \times Variant)) \rightarrow Action$

$subtype\_convert\_fn : Environment \times Subtype \times Value \times Value \rightarrow Action$

$view\_convert\_fn : Environment \times Subtype \times View \times View \rightarrow Action$

$content\_fn : LValue \times Value \rightarrow Action$

$assign\_fn : Environment \times Subtype \times LValue \times Value \rightarrow Action$

$raw\_assign\_fn : LValue \times Value \rightarrow Action$

$finalize\_fn : Environment \times Subtype \times Value \rightarrow Action$

$value\_split\_fn : Environment \times Subtype \times Value \rightarrow Action$

$discrete\_type\_fn : Environment \times Subtype \times Bool \rightarrow Action$

$covers\_fn : Value \times Choice \times Bool \rightarrow Action$

$statement\_fn : Environment \times Stm \rightarrow Action$

$arb\_fn : \mathrm{list}(Action) \rightarrow Action$

$subprogram\_body\_fn : (Id \xrightarrow{a} View) \times View \rightarrow Action$

The following predicates define a sequence of actions for a variety of different syntactic constructs:

$component\_actions(Environment, CompAssoc, \mathrm{list}(Rca), \mathrm{list}((Id \times Value)), \mathrm{list}(Action))$

$expression\_list(Environment, \mathrm{list}(\mathrm{Exp}), \mathrm{list}(Value), \mathrm{list}(Action))$

$index\_actions(Environment, \mathrm{list}(Sid), (Subtype), \mathrm{list}(Action))$

$parameter\_action(Environment, \mathrm{list}(Pss), (Id \times Parameter), (Id \times View), Action)$

$parameter\_list(Environment, \mathrm{list}(Pss), (Id \xrightarrow{a} Parameter), (Id \xrightarrow{a} View), \mathrm{list}(Action))$

## 4.4 State

### 4.4.1 Classification of States

$$abnormal\_state(exception(I_e, N))$$

$$abnormal\_state(exit(I_s, N))$$

$$abnormal\_state(proc\_return(N))$$

$$abnormal\_state(func\_return(W, N))$$

$$normal\_state(normal(N))$$

### 4.4.2 Accessing the Store of a State

$$the\_store(exception(I_d, N)) = N$$

$$the\_store(exit(I_d, N)) = N$$

$$the\_store(proc\_return(N)) = N$$

$$the\_store(func\_return(W, N)) = N$$

$$the\_store(normal(N)) = N$$

$$make\_state(exception(I_d, N), N_1) = exception(I_d, N_1)$$

$$make\_state(exit(I_d, N), N_1) = exit(I_d, N_1)$$

$$make\_state(proc\_return(N), N_1) = proc\_return(N_1)$$

$$make\_state(func\_return(W, N), N_1) = func\_return(W, N_1)$$

$$make\_state(normal(N), N_1) = normal(N_1)$$

### 4.4.3   Reading and Writing the Store

$$\frac{the\_store(S) = \langle B, ?, ?, ?\rangle}{S^{obj}[I] = B[I]}$$

$$\frac{the\_store(S) = \langle ?, B, ?, ?\rangle}{S^{spg}[I] = B[I]}$$

$$\frac{the\_store(S) = \langle ?, ?, B, ?\rangle}{S^{typ}[I] = B[I]}$$

$$\frac{the\_store(S) = \langle ?, ?, ?, B\rangle}{S^{stp}[I] = B[I]}$$

$$S_1[I \mapsto_1 V] = make\_state(S_1, the\_store(S_1)[I \mapsto_1 V])$$

$$S_1[I \mapsto_2 V] = make\_state(S_1, the\_store(S_1)[I \mapsto_2 V])$$

$$S_1[I \mapsto_3 V] = make\_state(S_1, the\_store(S_1)[I \mapsto_3 V])$$

$$S_1[I \mapsto_4 V] = make\_state(S_1, the\_store(S_1)[I \mapsto_4 V])$$

$$\langle B_0, B_p, B_t, B_s\rangle[I \mapsto_1 V] = \langle B_0[I \mapsto V], B_p, B_t, B_s\rangle$$

$$\langle B_o, B_0, B_t, B_s\rangle[I \mapsto_2 V] = \langle B_o, B_0[I \mapsto V], B_t, B_s\rangle$$

$$\langle B_o, B_p, B_0, B_s\rangle[I \mapsto_3 V] = \langle B_o, B_p, B_0[I \mapsto V], B_s\rangle$$

$$\langle B_o, B_p, B_t, B_0\rangle[I \mapsto_4 V] = \langle B_o, B_p, B_t, B_0[I \mapsto V]\rangle$$

### 4.4.4 The Content of a Location

This function differs from *stored_value* because it works on a state rather than a store and because it allows L-values rather than just locations. In the case of a structured L-value, the appropriate component of a compound object will be returned.

$$S \vdash content(location(I)) \Rightarrow S^{obj}[I]$$

$$\frac{S \vdash content(L_v) \Rightarrow array\_val(R_s, B)}{S \vdash content(array\_component(L_v, V_s)) \Rightarrow B[V_s]}$$

$$\frac{S \vdash content(L_v) \Rightarrow array\_val([R_1], B)}{S \vdash content(array\_slice(L_v, R)) \Rightarrow array\_val([R], B)}$$

$$\frac{S \vdash content(L_v) \Rightarrow record\_val(T_g, D_v, C_l)}{S \vdash content(record\_component(L_v, I_d)) \Rightarrow C_l[I_d]}$$

$$\frac{the\_store(S_1) = \langle B, ?, ?, ? \rangle \quad \neg I \in dom(B)}{new\_object(S_1, V, I, S_1[I \mapsto_1 V])}$$

$$\frac{the\_store(S_1) = \langle ?, B, ?, ? \rangle \quad \neg I \in dom(B)}{new\_subprogram(S_1, V, I, S_1[I \mapsto_2 V])}$$

$$\frac{the\_store(S_0[I \mapsto_3 T_e]) = \langle ?, ?, B, ? \rangle \quad \neg I \in dom(B)}{new\_type(S_0, T_e, U, S_0[I \mapsto_3 T_e])}$$

$$\frac{the\_store(S_0[I \mapsto_4 T_e]) = \langle ?, ?, ?, B \rangle \quad \neg I \in dom(B)}{new\_subtype(S_0, T_e, U, S_0[I \mapsto_4 T_e])}$$

## 4.5 Order of Execution

### 4.5.1 Sequential Execution

$$S [] S$$

$$\frac{\text{run}(normal(N), A_0, S_2) \quad S_2 \begin{bmatrix} A_1 \\ \dots \\ A_n \end{bmatrix} S_3}{normal(N) \begin{bmatrix} A_0 \\ A_1 \\ \dots \\ A_n \end{bmatrix} S_3}$$

$$\frac{abnormal\_state(S)}{S \begin{bmatrix} A_1 \\ \dots \\ A_n \end{bmatrix} S}$$

## 4.5.2 Arbitrary Order Execution

$$S \, \{\} \, S$$

$$\frac{abnormal\_state(S)}{S \left\{ \begin{array}{c} A_1 \\ \dots \\ A_n \end{array} \right\} S}$$

$$\frac{pick(A, A_j, A_t) \quad \text{run}(normal(N), A_j, S_1) \quad S_1 \left\{ \begin{array}{c} A_{t\,1} \\ \dots \\ A_{t\,n} \end{array} \right\} S_2}{normal(N) \left\{ \begin{array}{c} A_1 \\ \dots \\ A_n \end{array} \right\} S_2}$$

$$pick(A \cdot A_s, A, A_s)$$

$$\frac{pick(A_s, A_x, A_t)}{pick(A \cdot A_s, A_x, A \cdot A_t)}$$

## 4.5.3 Executing Individual Actions

Note that there are predicates that do not involve state. They are included as a matter of convenience. It is possible to include the appropriate terms in a sequential or arbitrary order execution where this makes the definition more readable.

$$\frac{S_1 \begin{bmatrix} A_1 \\ \dots \\ A_n \end{bmatrix} S_2}{\mathsf{run}(S_1, \mathit{then}(A), S_2)}$$

$$\frac{\mathit{new\_object}(S_1, V, L, S_2)}{\mathsf{run}(S_1, \mathit{new\_object\_fn}(V, L), S_2)}$$

$$\frac{S_1, E, V \vdash_{clt} \mathsf{Clt} \Rightarrow B, S_2}{\mathsf{run}(S_1, E, V \vdash_{clt} \mathsf{Clt} \Rightarrow B, S_2)}$$

$$\frac{S_1, E \vdash_{chc} \mathsf{Chc} \Rightarrow C, S_2}{\mathsf{run}(S_1, E \vdash_{chc} \mathsf{Chc} \Rightarrow C, S_2)}$$

$$\frac{S_1, E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Cmp}, A}{\mathsf{run}(S_1, E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Cmp}, S_2)}$$

$$\frac{S_1, E_1 \vdash_{dcl} \mathsf{Dcl} \Rightarrow E_2, S_2}{\mathsf{run}(S_1, E_1 \vdash_{dcl} \mathsf{Dcl} \Rightarrow E_2, S_2)}$$

$$\frac{S_1, E \vdash_{elf} \mathsf{Elf} \Rightarrow R, S_2}{\mathsf{run}(S_1, E \vdash_{elf} \mathsf{Elf} \Rightarrow R, S_2)}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2}{\mathsf{run}(S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2)}$$

$$\frac{S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow D, S_2}{\mathsf{run}(S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow D, S_2)}$$

$$\frac{S_1, E \vdash_{rng} \mathsf{Rng} \Rightarrow R, S_2}{\mathsf{run}(S_1, E \vdash_{rng} \mathsf{Rng} \Rightarrow R, S_2)}$$

$$\frac{S_1, E \vdash_{stm} \mathsf{Stm} \Rightarrow S_2}{\mathsf{run}(S_1, E \vdash_{stm} \mathsf{Stm} \Rightarrow, S_2)}$$

$$\frac{S_1, E_1, D \vdash_{tdf} \mathsf{Tdf} \Rightarrow S_t, E_2, S_2}{\mathsf{run}(S_1, E_1, D \vdash_{tdf} \mathsf{Tdf} \Rightarrow S_t, E_2, S_2)}$$

$$\frac{S_1, E, S_t \vdash \mathit{subtype\_convert}(V_1) \Rightarrow V_2, S_2}{\mathsf{run}(S_1, E, S_t \vdash \mathit{subtype\_convert}(V_1) \Rightarrow V_2, S_2)}$$

$$\frac{S_1, E, S_t \vdash \mathit{subtype\_convert}(W_1) \Rightarrow W_2, S_2}{\mathsf{run}(S_1, E, S_t \vdash \mathit{subtype\_convert}(W_1) \Rightarrow W_2, S_2)}$$

$$\frac{S \vdash \mathit{content}(L_v) \Rightarrow V}{\mathsf{run}(S, \vdash \mathit{content}(L_v) \Rightarrow V, S)}$$

$$\frac{S_1 \left\{ \begin{array}{c} A_1 \\ \dots \\ A_n \end{array} \right\} S_2}{\mathsf{run}\left(S_1, \left\{ \begin{array}{c} A_1 \\ \dots \\ A_n \end{array} \right\}, S_2\right)}$$

$$\frac{subprogram\_body(S_1, A, W, S_2)}{\mathsf{run}(S_1, subprogram\_body\_fn(A, W), S_2)}$$

## 4.6  Values

### 4.6.1  Ranges

$$discrete\_range(discrete\_rng(I_1, I_2))$$

$$real\_range(real\_rng(R_1, R_2))$$

$$low\_bound(discrete\_rng(I, ?)) = discrete\_val(I)$$

$$low\_bound(real\_rng(R, ?)) = real\_val(R)$$

$$high\_bound(discrete\_rng(?, I)) = discrete\_val(I)$$

$$high\_bound(real\_rng(?, R)) = real\_val(R)$$

$$make\_range(discrete\_val(I_1), discrete\_val(I_2)) = discrete\_rng(I_1, I_2)$$

$$make\_range(real\_val(R_1), real\_val(R_2)) = real\_rng(R_1, R_2)$$

$$\frac{\begin{array}{c} R_1 \leq R \\ R \leq R_2 \end{array}}{belongs\_to(real\_val(R), real\_rng(R_1, R_2))}$$

$$\frac{\begin{array}{c} I_1 \leq I \\ I \leq I_2 \end{array}}{belongs\_to(discrete\_val(I), discrete\_rng(I_1, I_2))}$$

$$\frac{\begin{array}{c} I_1 \geq I_3 \\ I_4 \geq I_2 \end{array}}{included\_in(discrete\_rng(I_1, I_2), discrete\_rng(I_3, I_4))}$$

$$\frac{I_1 > I_2}{null\_range(discrete\_rng(I_1, I_2))}$$

$$\frac{R_1 > R_2}{null\_range(real\_rng(R_1, R_2))}$$

$$values\_in\_range(discrete\_rng(I, I), set\_of([\,discrete\_val(I)\,]))$$

$$\frac{I_1 > I_2}{values\_in\_range(discrete\_rng(I_1, I_2), set\_of([\,]))}$$

$$\frac{values\_in\_range(discrete\_rng(I_1 + 1, I_2), set\_of(V_s))}{values\_in\_range(discrete\_rng(I_1, I_2), set\_of(discrete\_val(I_1) \cdot V_s))}$$

### 4.6.2   Index Ranges

$$indices([\,]) = set\_of([\,])$$

$$\frac{values\_in\_range(R, V_r)}{index\_pairing(V_r, indices(R_s), V)}{indices(R \cdot R_s) = V}$$

$$index\_pairing(set\_of([\,]), V_1, set\_of([[\,]]))$$

$$\frac{index\_pairing(set\_of(V_r), V_1, V_x)}{prefix\_set\_with\_element(V, V_1, V_y)}{index\_pairing(set\_of(V \cdot V_r), V_1, V_x \cup V_y)}$$

$$prefix\_set\_with\_element(V, set\_of([\,]), set\_of([\,]))$$

$$\frac{prefix\_set\_with\_element(V, set\_of(E_r), set\_of(E_p))}{prefix\_set\_with\_element(V, set\_of(E_1 \cdot E_r), set\_of(V \cdot E_1 \cdot E_p))}$$

### 4.6.3 Predicates of Values

$$discrete\_value(discrete\_val(X))$$

$$real\_value(real\_val(X))$$

$$access\_value(access\_val(X,?))$$

$$\frac{discrete\_value(V)}{scalar\_value(V)}$$

$$\frac{real\_value(V)}{scalar\_value(V)}$$

$$\frac{scalar\_value(V)}{elementary\_value(V)}$$

$$\frac{access\_value(V)}{elementary\_value(V)}$$

$$composite\_value(record\_val(X,Y,Z))$$

$$composite\_value(array\_val(X,Y))$$

$$\frac{dom(V) = indices(B)}{array\_value(array\_val(B,V))}$$

## 4.7 Types

### 4.7.1 Type Descriptors

$$\frac{S^{typ}[U] = (? \times T_y)}{type\_struct(S, subtype(U,?,?)) = T_y}$$

### 4.7.2 Ancestry Relation

$$ancestor(S, U, U)$$

$$\frac{\begin{array}{c} S^{typ}[U] = (some(U_2)\times?) \\ ancestor(S, U_2, U_1) \end{array}}{ancestor(S, U, U_1)}$$

$$\frac{ancestor(S, U_2, U_1)}{descendant(S, U_1, U_2)}$$

$$\frac{S^{typ}[U] = (none\times?)}{ultimate\_ancestor(S, U, U)}$$

$$\frac{\begin{array}{c} S^{typ}[U] = (some(U_2)\times?) \\ ultimate\_ancestor(S, U_1, U_2) \end{array}}{ultimate\_ancestor(S, U, U_2)}$$

### 4.7.3 Ranges of Scalar Types

$$base\_range(S, enum\_type(N)) = discrete\_rng(0, N)$$

$$base\_range(S, modular\_type(N)) = discrete\_rng(0, N, -, 1)$$

$$base\_range(S, signed\_integer\_type(B_f, B_l, ?, ?)) = discrete\_rng(B_f, B_l)$$

$$base\_range(S, universal\_integer\_type(B_f, B_l)) = discrete\_rng(B_f, B_l)$$

$$\frac{S_t = subtype(U, no\_constraint, A)}{range\_of\_subtype(S, S_t) = base\_range(S, type\_struct(S, S_t))}$$

$$range\_of\_subtype(S, subtype(U, range\_constraint(R), A)) = R$$

$$ranges\_of\_subtypes(S, [\,]) = [\,]$$

$$ranges\_of\_subtypes(S, S_1 \cdot S_r) = range\_of\_subtype(S, S_1) \cdot ranges\_of\_subtypes(S, S_r)$$

### 4.7.4 Values of a Type

$$\frac{\begin{array}{c} ancestor(S, U, U_p) \\ S^{typ}[U_p] = (? \times T_y) \\ descriptor\_value(S, T_y, V) \end{array}}{descriptor\_value(S, class\_type(U), V)}$$

$$\frac{belongs\_to(V, base\_range(S, enum\_type(N)))}{descriptor\_value(S, enum\_type(N), V)}$$

$$descriptor\_value(S, enum\_type(N), invalid\_val)$$

$$\frac{belongs\_to(V, base\_range(S, modular\_type(N)))}{descriptor\_value(S, modular\_type(N), V)}$$

$$descriptor\_value(S, modular\_type(N), invalid\_val)$$

$$descriptor\_value(S, signed\_integer\_type(B_f, B_l, F, L), discrete\_val(N))$$

$$descriptor\_value(S, signed\_integer\_type(B_f, B_l, F, L), invalid\_val)$$

$$descriptor\_value(S, universal\_integer\_type(B_f, B_l), discrete\_val(N))$$

$$descriptor\_value(S, universal\_integer\_type(B_f, B_l), invalid\_val)$$

$$\frac{array\_value(array\_val(ranges\_of\_subtypes(S, I), B))}{descriptor\_value(S, array\_type(I, C), array\_val(ranges\_of\_subtypes(S, I), B))}$$

$$\frac{\begin{array}{c} N \in set\_of(adom(D)) \\ D[N] = (S_t \times T_h) \\ subtype\_value(S, S_t, B[N]) \end{array}}{discriminant\_value(S, discr(D), B)}$$

$$\frac{\begin{array}{c} discriminant\_value(S, D_a, D_v) \\ cl\_value(S, C_l, D_v, C_v) \end{array}}{descriptor\_value(S, record\_type(T_g, D_a, C_l), record\_val(T_g, D_v, C_v))}$$

$$dom(F) = set\_of(adom(A))$$
$$A[I_d] = (P_s \times T_h)$$
$$subtype\_value(S, actualize(D_v, P_s), F[I_d])$$
$$\frac{variant\_values(S, V_r, D_v, F_v)}{cl\_value(S, fields(A, V_r), D_v, F \oplus F_v)}$$

$$variant\_values(S, none, D_v, [\,])$$

$$the\_variant(F, D_v[I_d], C_l)$$
$$\frac{cl\_value(S, C_l, D_c, V_v)}{variant\_values(S, some((I_d \times F)), D_v, V_v)}$$

## 4.7.5 Record Fields

The following definitions are useful to deal with the types of record fields. Binding $B$ represented the values of the discriminants.

$$\frac{D_a[I_d] = (S_t \times T_k)}{component\_type(B, record\_type(T_g, discr(D_a), C_l), I_d, S_t)}$$

$$\frac{select\_component\_type(B, C_l, I_d, S_t)}{component\_type(B, record\_type(T_g, D_a, C_l), I_d, S_t)}$$

$$\frac{C_a[I_d] = (P_s \times T_k)}{select\_component\_type(B, fields(C_a, ?), I_d, actualize(B, P_s))}$$

Since component names have to be unique, we can quantify over values $V$ in the following rule.

$$the\_variant(V_b, V, C_l)$$
$$\frac{select\_component\_type(B, C_l, I_d, S_t)}{select\_component\_type(B, fields(C_a, some((I_v \times V_b))), I_d, S_t)}$$

$$\frac{covers(X, C, true)}{the\_variant(variant((C \times C_l) \cdot L), X, C_l)}$$

$$covers(X, C, false)$$
$$\frac{the\_variant(variant(L), X, C_l)}{the\_variant(variant((C \times C_l) \cdot L), X, C_l)}$$

### 4.7.6  Classification of Types

$$\frac{is\_scalar\_type(S, T_y)}{is\_elementary\_type(S, T_y)}$$

$$\frac{is\_access\_type(S, T_y)}{is\_elementary\_type(S, T_y)}$$

$$\frac{is\_array\_type(S, T_y)}{is\_composite\_type(S, T_y)}$$

$$\frac{is\_record\_type(S, T_y)}{is\_composite\_type(S, T_y)}$$

$$\frac{is\_tagged\_type(S, T_y)}{is\_composite\_type(S, T_y)}$$

$$\frac{is\_protected\_type(S, T_y)}{is\_composite\_type(S, T_y)}$$

$$\frac{is\_discrete\_type(S, T_y)}{is\_scalar\_type(S, T_y)}$$

$$\frac{is\_real\_type(S, T_y)}{is\_scalar\_type(S, T_y)}$$

$$\frac{is\_access\_to\_object\_type(S, T_y)}{is\_access\_type(S, T_y)}$$

$$\frac{is\_access\_to\_subprogram\_type(S, T_y)}{is\_access\_type(S, T_y)}$$

$$\frac{is\_enumeration\_type(S, T_y)}{is\_discrete\_type(S, T_y)}$$

$$\frac{is\_integer\_type(S, T_y)}{is\_discrete\_type(S, T_y)}$$

$$\frac{type\_struct(S, T_y) = enum\_type(N)}{is\_enumeration\_type(S, T_y)}$$

$$is\_boolean\_type(S, subtype(boolean\_tn, ?, ?))$$

$$is\_character\_type(S, subtype(character\_tn, ?, ?))$$

$$\frac{is\_signed\_integer\_type(S, T_y)}{is\_integer\_type(S, T_y)}$$

$$\frac{is\_modular\_integer\_type(S, T_y)}{is\_integer\_type(S, T_y)}$$

$$is\_signed\_integer\_type(S, subtype(root\_integer\_tn, ?, ?))$$

$$\frac{type\_struct(S, T_y) = modular\_type(?)}{is\_modular\_integer\_type(S, T_y)}$$

$$\frac{not\ yet\ defined}{is\_real\_type(S, T_y)}$$

$$\frac{type\_struct(S, T_y) = access\_type(S_t, A_m)}{is\_access\_to\_object\_type(S, T_y)}$$

$$\frac{type\_struct(S, T_y) = func\_profile(P_a, S_t)}{is\_access\_to\_subprogram\_type(S, T_y)}$$

$$\frac{type\_struct(S, T_y) = proc\_profile(P_a)}{is\_access\_to\_subprogram\_type(S, T_y)}$$

$$\frac{type\_struct(S, T_y) = array\_type(C, B)}{is\_array\_type(S, T_y)}$$

$$\frac{not\ yet\ defined}{is\_string\_type(S, T_y)}$$

$$\frac{type\_struct(S, T_y) = record\_type(T_g, D, C)}{is\_record\_type(S, T_y)}$$

$$\frac{type\_struct(S, T_y) = record\_type(some(I_t), D, C)}{is\_tagged\_type(S, T_y)}$$

$$\frac{not\ yet\ defined}{is\_task\_type(S, T_y)}$$

$$\frac{not\ yet\ defined}{is\_protected\_type(S, T_y)}$$

$$\frac{is\_elementary\_type(S, T_y)}{is\_by\_copy\_type(S, T_y)}$$

$$\frac{is\_tagged\_type(S, T_y)}{is\_by\_reference\_type(S, T_y)}$$

$$\frac{is\_task\_type(S, T_y)}{is\_by\_reference\_type(S, T_y)}$$

$$\frac{is\_protected\_type(S, T_y)}{is\_by\_reference\_type(S, T_y)}$$

## 4.8   Subtypes

### 4.8.1   Constraint Satisfaction

$$satisfies(V, no\_constraint)$$

$$\frac{belongs\_to(V, R)}{satisfies(V, range\_constraint(R))}$$

$$satisfies(array\_val(B, A), index\_constraint(B))$$

$$satisfies(record\_val(T_g, D, R), discriminant\_constraint(D))$$

### 4.8.2   Values of a Subtype

$$\frac{\begin{array}{c} S^{typ}[U] = (P \times T_y) \\ descriptor\_value(S, T_y, V) \\ satisfies(V, C) \end{array}}{subtype\_value(S, subtype(U, C, A), V)}$$

### 4.8.3 Actualization

#### 4.8.3.1 Values

$$actualized\_value(B, p\_value(V)) = V$$

$$actualized\_value(B, discriminant\_ref(I)) = B[I]$$

#### 4.8.3.2 Ranges

$$\frac{actualized\_value(B, L) = discrete\_val(L_a)}{actualized\_value(B, H) = discrete\_val(H_a)}{actualized\_partial\_range(B, (L \times H)) = discrete\_rng(L_a, H_a)}$$

$$actualized\_range\_list(B, [\,]) = [\,]$$

$$actualized\_range\_list(B, R \cdot R_s) = actualized\_partial\_range(B, R) \cdot actualized\_range\_list(B, R_s)$$

#### 4.8.3.3 Binding Lists

$$actualized\_binding\_list(B, [\,]) = [\,]$$

$$actualized\_binding\_list(B, (I \times V) \cdot R) = (I \times actualized\_value(B, V)) \cdot actualized\_binding\_list(B, R)$$

#### 4.8.3.4 Constraints

$$actualized\_constraint(B, p\_no\_constraint) = no\_constraint$$

$$actualized\_constraint(B, p\_range\_constraint(R)) = range\_constraint(actualized\_partial\_range(B, R))$$

$$actualized\_constraint(B, p\_index\_constraint(S)) = index\_constraint(actualized\_range\_list(B, S))$$

$$\frac{C = discriminant\_constraint(actualized\_binding\_list(B, S))}{actualized\_constraint(B, p\_discriminant\_constraint(S)) = C}$$

$$\frac{C = indirect\_index\_constraint(actualized\_range\_list(B, S))}{actualized\_constraint(B, p\_indirect\_index\_constraint(S)) = C}$$

$$\frac{C = indirect\_discriminant\_constraint(actualized\_binding\_list(B, S))}{actualized\_constraint(B, p\_indirect\_discriminant\_constraint(S)) = C}$$

### 4.8.3.5  Subtypes

$$actualize(B, p\_subtype(subtype(U, C, A), P_c)) = subtype(U, actualized\_constraint(B, P_c), A)$$

### 4.8.3.6  Components

$$A_1 + A_2 = A_1 + A_2$$

$$actualized\_components(B, fields(C_a, some(V_p))) = actualized\_complist(B, C_a) + actualized\_variants(B, V_p)$$

$$actualized\_components(B, fields(C_a, none)) = actualized\_complist(B, C_a)$$

### 4.8.3.7  Component Lists

$$actualized\_complist(B, [\,]) = [\,]$$

$$\frac{actualized\_complist(B, A) = A_a}{actualized\_complist(B, (I \times P_s) \cdot A) = (I \times actualize(B, P_s)) \cdot A_a}$$

$$\frac{the\_variant(V_a, B[I], C_l)}{actualized\_variants(B, (I \times V_a)) = actualized\_components(B, C_l)}$$

## 4.9   Declarations

### 4.9.1   Declarations

### 4.9.2   Types and Subtypes

### 4.9.2.1   Type Declarations

The semantics of a type definition are determined in the context of a discriminant association. For types without discriminant, this association is empty

$$\frac{S_1, E_1, \langle\rangle \vdash_{tdf} \mathsf{Tdf} \Rightarrow S_t, E_2, S_2 \qquad new\_subtype(S_2, S_t, L_s, S_3)}{S_1, E_1 \vdash_{dcl} \mathsf{type}\ \mathsf{I_d}\ \mathsf{is}\ \mathsf{Tdf};\ \Rightarrow E_2[I_d \mapsto subtype\_view(L_s)], S_3}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{dsc} \mathsf{Dcp} \Rightarrow D \\ E, D \vdash_{tdf} \mathsf{Tdf} \Rightarrow S_t, E_2 \end{array} \right] S_2$$
$$\frac{new\_subtype(S_2, S_t, L_s, S_3)}{S_1, E \vdash_{dcl} \mathbf{type}\ \mathsf{I_d}\ \mathsf{Dcp}\ \mathbf{is}\ \mathsf{Tdf};\ \Rightarrow E_2[I_d \mapsto subtype\_view(L_s)], S_3}$$

For a given type descriptor, the following rule creates a new unique type name and constructs a *first subtype*.

### 4.9.2.2 Subtype Declarations

A subtype indication may be a named subtype or a subtype with a constraint. In the former case, evaluation of the subtype indication cannot have side-effects.

$$\frac{S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1}{S_1, E \vdash_{sid} \mathsf{Nam} \Rightarrow S_1^{stp}[L_s], S_1}$$

$$\frac{\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ S_1, E, S_1^{stp}[L_s] \vdash_{cns} \mathsf{Csn} \Rightarrow C, S_2 \\ compatible(E, S_1^{stp}[L_s], C) \\ S_1^{stp}[L_s] = subtype(U, C_1, A) \end{array}}{S_1, E \vdash_{sid} \mathsf{Nam}\ \mathsf{Cns} \Rightarrow subtype(U, C, A), S_2}$$

$$\frac{S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1}{S_1, E, D \vdash_{psi} \mathsf{Nam} \Rightarrow p\_subtype(S_1^{stp}[L_s], p\_no\_constraint), S_1}$$

$$\frac{\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ p\_constraint(S_1, E, D, S_1^{stp}[L_s], \mathsf{Csn}, P, S_2) \\ compatible(E, S_1^{stp}[L_s], C) \\ S_1^{stp}[L_s] = subtype(U, C_1, A) \end{array}}{S_1, E, D \vdash_{psi} \mathsf{Nam}\ \mathsf{Cns} \Rightarrow p\_subtype(subtype(U, no\_constraint, A), P), S_2}$$

The following syntax represents ranges in a discrete subtype definition. It applies only to constrained array type definitions.

$$\frac{not\ yet\ defined}{S_1, E \vdash_{sid} \mathsf{Rng} \Rightarrow subtype(U, C, A), S_2}$$

$$\frac{\begin{array}{c} S_1, E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t, S_2 \\ new\_subtype(S_2, S_t, L_s, S_3) \end{array}}{S_1, E_1 \vdash_{dcl} \mathbf{subtype}\ \mathsf{I_d}\ \mathbf{is}\ \mathsf{Sid};\ \Rightarrow E_1[I_d \mapsto subtype\_view(L_s)], S_3}$$

### 4.9.3 Objects and Named Numbers

#### 4.9.3.1 Object Declarations

$$\frac{S_1 \left[ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ new\_object\_fn(invalid\_val, L) \\ default\_value\_fn(E_1, S_t, V) \\ assign\_fn(E_1, S_t, location(L), V) \end{array} \right] S_2}{S_1, E_1 \vdash_{dcl} \mathsf{Id} : \mathsf{Sid}; \ \Rightarrow E_1[I_d \mapsto object\_view(location(L), S_t, variable)], S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ new\_object\_fn(invalid\_val, L) \\ default\_value\_fn(E_1, S_t, V) \\ assign\_fn(E_1, S_t, location(L), V) \end{array} \right] S_2}{S_1, E_1 \vdash_{dcl} \mathsf{Id} : \textbf{constant } \mathsf{Sid}; \ \Rightarrow E_1[I_d \mapsto object\_view(location(L), S_t, constant)], S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ new\_object\_fn(invalid\_val, L) \\ E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow V \\ assign\_fn(E_1, S_t, location(L), V) \end{array} \right] S_2}{S_1, E_1 \vdash_{dcl} \mathsf{Id} : \mathsf{Sid} := \mathsf{Exp}; \ \Rightarrow E_1[I_d \mapsto object\_view(location(L), S_t, variable)], S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ new\_object\_fn(invalid\_val, L) \\ E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow V \\ assign\_fn(E_1, S_t, location(L), V) \end{array} \right] S_2}{S_1, E_1 \vdash_{dcl} \mathsf{Id} : \textbf{constant } \mathsf{Sid} := \mathsf{Exp}; \ \Rightarrow E_1[I_d \mapsto object\_view(location(L), S_t, constant)], S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ new\_object\_fn(invalid\_val, L) \\ default\_value\_fn(E_1, S_t, V) \\ assign\_fn(E_1, S_t, location(L), V) \end{array} \right] S_2}{S_1, E_1 \vdash_{dcl} \mathsf{Id} : \textbf{aliased } \mathsf{Sid}; \ \Rightarrow E_1[I_d \mapsto object\_view(location(L), S_t, aliased)], S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ new\_object\_fn(invalid\_val, L) \\ default\_value\_fn(E_1, S_t, V) \\ assign\_fn(E_1, S_t, location(L), V) \end{array} \right] S_2}{S_1, E_1 \vdash_{dcl} \mathsf{Id} : \textbf{aliased constant } \mathsf{Sid}; \ \Rightarrow E_1[I_d \mapsto object\_view(location(L), S_t, constant)], S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ new\_object\_fn(invalid\_val, L) \\ E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow V \\ assign\_fn(E_1, S_t, location(L), V) \end{array} \right] S_2}{S_1, E_1 \vdash_{dcl} \mathsf{Id} : \textbf{aliased } \mathsf{Sid} := \mathsf{Exp}; \ \Rightarrow E_1[I_d \mapsto object\_view(location(L), S_t, aliased)], S_2}$$

$$S_1 \left[ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ new\_object\_fn(invalid\_val, L) \\ E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow V \\ assign\_fn(E_1, S_t, location(L), V) \end{array} \right] S_2$$
$$\overline{S_1, E_1 \vdash_{dcl} \mathsf{I_d} : \textbf{aliased constant } \mathsf{Sid} := \mathsf{Exp}; \; \Rightarrow E_1[I_d \mapsto object\_view(location(L), S_t, constant)], S_2}$$

#### 4.9.3.2  Number Declarations

$$S_1, E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2$$
$$new\_object(S_1, V, L, S_2)$$
$$\frac{E_3 = E_1[I_d \mapsto object\_view(location(L), subtype(universal\_real\_tn, no\_constraint, not\_used), constant)]}{S_1, E_1 \vdash_{dcl} \mathsf{I_d} : \textbf{constant} := \mathsf{Exp}; \; \Rightarrow E_3, S_2}$$

$$S_1, E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2$$
$$new\_object(S_1, V, L, S_2)$$
$$\frac{E_3 = E_1[I_d \mapsto object\_view(location(L), subtype(universal\_integer\_tn, no\_constraint, not\_used), constant)]}{S_1, E_1 \vdash_{dcl} \mathsf{I_d} : \textbf{constant} := \mathsf{Exp}; \; \Rightarrow E_3, S_2}$$

### 4.9.4  Derived Types and Classes

$$S_0, E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow subtype(P, C, A), S_1$$
$$S_1^{typ}[P] = (P_p \times T_y)$$
$$\frac{new\_type(S_1, (some(P) \times T_y), U, S_2)}{S_0, E_1, D_0 \vdash_{tdf} \textbf{new } \mathsf{Sid} \Rightarrow subtype(U, C, A), E_2, S_2}$$

### 4.9.5  Scalar Types

$$S_1 \left\{ \begin{array}{c} E \vdash_{exp} \mathsf{Exp_1} \Rightarrow V_1 \\ E \vdash_{exp} \mathsf{Exp_2} \Rightarrow V_2 \end{array} \right\} S_2$$
$$\overline{S_1, E \vdash_{rng} \mathsf{Exp_1..Exp_2} \Rightarrow make\_range(V_1, V_2), S_2}$$

$$S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow W, S_2$$
$$\frac{abnormal\_state(S_2)}{S_1, E \vdash_{rng} \mathsf{Nam'range} \Rightarrow R, S_2}$$

$$S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow W, S_2$$
$$normal\_state(S_2)$$
$$\frac{S_2, E, W \vdash_{attr} \mathsf{range} \Rightarrow R, S_3}{S_1, E \vdash_{rng} \mathsf{Nam'range} \Rightarrow R, S_3}$$

$$\frac{not\ yet\ defined}{S_1, E \vdash_{rng} \mathsf{Nam'range(Exp)} \Rightarrow R, S_2}$$

#### 4.9.5.1 Enumeration Types

#### 4.9.5.2 Character Types

#### 4.9.5.3 Boolean Types

#### 4.9.5.4 Integer Types

$$\frac{\begin{array}{c} S_1, E_1 \vdash_{exp} \mathsf{Exp_1} \Rightarrow discrete\_val(V_1), S_1 \\ S_1, E_1 \vdash_{exp} \mathsf{Exp_2} \Rightarrow discrete\_val(V_2), S_1 \\ new\_type(S_1, (some(root\_integer\_tn) \times signed\_integer\_type(V_1, V_2, V_1, V_2)), U, S_2) \end{array}}{S_1, E_1, \langle\rangle \vdash_{tdf} \mathbf{range}\ \mathsf{Exp_1}..\mathsf{Exp_2} \Rightarrow subtype(U, no\_constraint, not\_used), E_1, S_2}$$

$$\frac{\begin{array}{c} S_1, E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow discrete\_val(V), S_1 \\ new\_type(S_1, (some(root\_integer\_tn) \times modular\_type(V)), U, S_2) \end{array}}{S_1, E_1, \langle\rangle \vdash_{tdf} \mathbf{mod}\ \mathsf{Exp} \Rightarrow subtype(U, no\_constraint, not\_used), E_1, S_2}$$

#### 4.9.5.5 Operations of Discrete Types

#### 4.9.5.6 Real Types

#### 4.9.5.7 Floating Point Types

$$\frac{not\ yet\ defined}{S_1, E_1, D \vdash_{tdf} \mathbf{digits}\ \mathsf{Exp}\ \mathsf{Cns} \Rightarrow S_t, E_2, S_2}$$

$$\frac{not\ yet\ defined}{S_1, E_1, D \vdash_{tdf} \mathbf{digits}\ \mathsf{Exp} \Rightarrow S_t, E_2, S_2}$$

#### 4.9.5.8 Operations of Floating Point Types

#### 4.9.5.9 Fixed Point Types

$$\frac{not\ yet\ defined}{S_1, E_1, D \vdash_{tdf} \mathbf{delta}\ \mathsf{Exp}\ \mathbf{digits}\ \mathsf{Exp}\ \mathsf{Cns} \Rightarrow S_t, E_2, S_2}$$

$$\frac{not\ yet\ defined}{S_1, E_1, D \vdash_{tdf} \mathbf{delta}\ \mathsf{Exp}\ \mathbf{digits}\ \mathsf{Exp} \Rightarrow S_t, E_2, S_2}$$

$$\frac{not\ yet\ defined}{S_1, E_1, D \vdash_{tdf} \mathbf{delta}\ \mathsf{Exp}\ \mathsf{Rng} \Rightarrow S_t, E_2, S_2}$$

#### 4.9.5.10 Operations of Fixed Point Types

### 4.9.6 Array Types

The evaluation of a subtype mark has no side-effect. Therefore, the evaluation of lists of subtype marks is defined sequentially.

$$S, E \vdash_{Stl} () \Rightarrow [\,]$$

$$\frac{\begin{array}{c} S, E \vdash_{nam} \mathsf{Nam_0} \Rightarrow subtype\_view(L_s), S \\ S, E \vdash_{Stl} (\mathsf{Nam}, \ldots) \Rightarrow S_t \end{array}}{S, E \vdash_{Stl} (\mathsf{Nam_0}, \mathsf{Nam}, \ldots) \Rightarrow S^{stp}[L_s] \cdot S_t}$$

$$index\_actions(E, (\ ), [\ ], [\ ])$$

$$\frac{index\_actions(E, (\mathsf{Sid}, \ldots), S_t, A_c)}{index\_actions(E, (\mathsf{Sid}_0, \mathsf{Sid}, \ldots), St_0 \cdot S_t, E \vdash_{sid} \mathsf{Sid}_0 \Rightarrow St_0 \cdot A_c)}$$

$$range\_constraints(S, [\ ], [\ ])$$

$$\frac{type\_constraints(S, S_t, R)}{range\_constraints(S, subtype(?, range\_constraint(R_0), ?) \cdot S_t, R_0 \cdot R)}$$

$$\frac{not\ yet\ defined}{S_1, E_1, D \vdash_{tdf} \mathbf{array}(\mathsf{Rng\_lst})\mathbf{of\ aliased}\ \mathsf{Sid} \Rightarrow S_t, E_2, S_2}$$

$$\frac{not\ yet\ defined}{S_1, E_1, D \vdash_{tdf} \mathbf{array}(\mathsf{Nam}_0, \mathsf{Nam}, \ldots)\mathbf{of\ aliased}\ \mathsf{Sid} \Rightarrow S_t, E_2, S_2}$$

$$\frac{\begin{array}{c} index\_actions(E, \mathsf{Idx}, S_i, A_c) \\ S_1 \left\{ \begin{array}{c} E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t \\ A_{c1} \\ \ldots \\ A_{cn} \end{array} \right\} S_2 \\ range\_constraints(S_2, S_i, R) \\ new\_type(S_2, (none \times array\_type(S_i, S_t)), U, S_3) \end{array}}{S_1, E_1, \langle\rangle \vdash_{tdf} \mathbf{array}(\mathsf{Idx})\mathbf{of}\ \mathsf{Sid} \Rightarrow subtype(U, index\_constraint(R), not\_used), E_2, S_3}$$

$$\frac{\begin{array}{c} S_1, E_1 \vdash_{Stl} \mathsf{Idx} \Rightarrow S_i \\ S_1, E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow S_t, S_2 \\ new\_type(S_2, (none \times array\_type(S_i, S_t)), U, S_3) \end{array}}{S_1, E_1, \langle\rangle \vdash_{tdf} \mathbf{array}(\mathsf{Idx})\mathbf{of}\ \mathsf{Sid} \Rightarrow subtype(U, no\_constraint, not\_used), E_1, S_3}$$

### 4.9.7   Discriminants

### 4.9.8   Record Types

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Cmp} \\ E, D \vdash_{vrn} \mathsf{Vrp} \Rightarrow V \\ new\_type\_fn((none \times record\_type(none, D, fields(C, V))), U) \end{array} \right] S_2}{S_1, E, D \vdash_{tdf} \mathsf{Cmp} \Rightarrow subtype(U, no\_constraint, not\_used), E, S_2}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Cmp} \\ E, D \vdash_{vrn} \mathsf{Vrp} \Rightarrow V \\ new\_type\_fn((none \times record\_type(some(U), D, fields(C, V))), U) \end{array} \right] S_2$$
$$\overline{S_1, E, D \vdash_{tdf} \mathbf{tagged}\ \mathsf{Cmp} \Rightarrow subtype(U, no\_constraint, not\_used), E, S_2}$$

$$S, E \vdash_{cmp} \mathsf{D} \Rightarrow \langle \rangle, [\,]$$

$$\frac{not\ yet\ defined}{S_1, E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Idn} : \mathbf{aliased}\ \mathsf{Sid};\ \mathsf{Cmp}\ \ldots, A}$$

$$\frac{S_1 \left[ \begin{array}{c} E, D \vdash_{psi} \mathsf{Sid} \Rightarrow P_s \\ E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Cmp}\ \ldots \end{array} \right] S_2}{S_1, E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Idn} : \mathsf{Sid};\ \mathsf{Cmp}\ \ldots, A_1[\mathsf{Idn} \mapsto (P_s \times none)]}$$

$$\frac{not\ yet\ defined}{S_1, E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Idn} : \mathbf{aliased}\ \mathsf{Sid} := \mathsf{Exp};\ \mathsf{Cmp}\ \ldots, A}$$

$$\frac{S_1 \left[ \begin{array}{c} E, D \vdash_{psi} \mathsf{Sid} \Rightarrow P_s \\ E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Cmp}\ \ldots \end{array} \right] S_2}{S_1, E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Idn} : \mathsf{Sid} := \mathsf{Exp};\ \mathsf{Cmp}\ \ldots, A}$$

### 4.9.8.1   Variant Parts and Discrete Choices

$$S, E, D \vdash_{vrn}\ \Rightarrow none, S$$

$$\frac{S_1, E, D \vdash_{vrn} \mathsf{Vnt} \Rightarrow B, S_2}{S_1, E, D \vdash_{vrn} \mathbf{case}\ \mathsf{Idn}\ \mathbf{is}\ \mathsf{Vnt}\ \mathbf{end\ case};\ \Rightarrow some((\mathsf{Idn} \times B)), S_2}$$

$$\langle \rangle = variant([\,])$$

$$S, E, D \vdash_{vrn} \langle \rangle \Rightarrow \langle \rangle, S$$

$$\frac{S_1 \left[ \begin{array}{c} S_1, E \vdash_{chc} \mathsf{Dch} \Rightarrow C_v, S_1 \\ E \vdash_{cmp} \mathsf{D} \Rightarrow \mathsf{Cmp} \\ E, D \vdash_{vrn} \mathsf{Vrp} \Rightarrow V \\ E, D \vdash_{vrn} \mathsf{Vnt};\ \ldots \Rightarrow variant(B_1) \end{array} \right] S_2}{S_1, E, D \vdash_{vrn} \mathbf{when}\ \mathsf{Dch} => \mathsf{CmpVrp};\ \mathsf{Vnt};\ \ldots \Rightarrow variant(((C_v \times fields(C, V)) \cdot B_2), S_2}$$

70

### 4.9.9 Tagged Types and Type Extensions

#### 4.9.9.1 Type Extensions

$$S_1 \left[ \begin{array}{c} S_0, E_1 \vdash_{sid} \mathsf{Sid} \Rightarrow subtype(P, C, A), S_1 \\ S_1^{typ}[P] = (P_p \times record\_type(some(U_p), D_1, fields(C_1, V_1))) \\ E_1 \vdash_{cmp} \mathsf{D_0} \Rightarrow \mathsf{Cmp} \\ E_1, D_0 \vdash_{vrn} \mathsf{Vrp} \Rightarrow V_2 \\ new\_type\_fn((some(U_p) \times record\_type(some(U), discriminant\_union(D_0, D_1), fields(C_1 \oplus C_2, V_1 \oplus V_2))), U) \end{array} \right] S_2$$
$$\overline{S_0, E_1, D_0 \vdash_{tdf} \mathbf{new}\ \mathsf{Sid}\ \mathbf{with}\ \mathsf{Cmp} \Rightarrow subtype(U, no\_constraint, not\_used), E_2, S_2}$$

$$none \oplus V = V$$

$$V \oplus none = V$$

$$discriminant\_union(discr(A_1), discr(A_2)) = discr(A_1 \oplus A_2)$$

### 4.9.10 Access Types

$$\frac{\begin{array}{c} S_1, E_1 \vdash_{Sid_i} \mathsf{Sid} \Rightarrow L_s, S_2 \\ new\_type(S_2, (none \times access\_type(L_s, pool\_access)), U, S_3) \end{array}}{S_1, E_1, D \vdash_{tdf} \mathbf{access}\ \mathsf{Sid} \Rightarrow subtype(U, no\_constraint, not\_used), E_1, S_3}$$

$$\frac{\begin{array}{c} S_1, E_1 \vdash_{Sid_i} \mathsf{Sid} \Rightarrow L_s, S_2 \\ new\_type(S_2, (none \times access\_type(L_s, all\_access)), U, S_3) \end{array}}{S_1, E_1, D \vdash_{tdf} \mathbf{access\ all}\ \mathsf{Sid} \Rightarrow subtype(U, no\_constraint, not\_used), E_1, S_3}$$

$$\frac{\begin{array}{c} S_1, E_1 \vdash_{Sid_i} \mathsf{Sid} \Rightarrow L_s, S_2 \\ new\_type(S_2, (none \times access\_type(L_s, constant\_access)), U, S_3) \end{array}}{S_1, E_1, D \vdash_{tdf} \mathbf{access\ constant}\ \mathsf{Sid} \Rightarrow subtype(U, no\_constraint, not\_used), E_1, S_3}$$

$$\frac{S_1, E \vdash_{pas} \mathsf{Pms} \Rightarrow A, S_2}{S_1, E, \langle\rangle \vdash_{tdf} \mathbf{access\ procedure}\ \mathsf{Pms} \Rightarrow subtype(U, no\_constraint, not\_used), E, S_2[proc\_profile(A) \mapsto_3 U]}$$

$$\frac{\begin{array}{c} S_1, E \vdash_{pas} \mathsf{Pms} \Rightarrow A, S_2 \\ S_2, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(S_l), S_2 \end{array}}{S_1, E_1, \langle\rangle \vdash_{tdf} \mathbf{access\ function}\ \mathsf{Pms} \Rightarrow subtype(U, no\_constraint, not\_used), E_2, S_2[func\_profile(A, S_2^{stp}[S_l]) \mapsto_3 U]}$$

#### 4.9.10.1 Incomplete Type Declarations

In the case of access type definitions, a subtype indication may denote an incomplete type.

$$\frac{S_1, E \vdash_{nam} \textsf{Nam} \Rightarrow subtype\_view(L_s), S_1}{S_1, E \vdash_{Sid_i} \textsf{Nam} \Rightarrow L_s, S_1}$$

$$\frac{\begin{array}{c} S_1, E \vdash_{nam} \textsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ S_1, E, S_1^{stp}[L_s] \vdash_{cns} \textsf{Csn} \Rightarrow C, S_2 \\ compatible(E, S_1^{stp}[L_s], C) \\ S_1^{stp}[L_s] = subtype(U, C_1, A) \\ new\_subtype(S_2, subtype(U, C, A), L_t, S_3) \end{array}}{S_1, E \vdash_{Sid_i} \textsf{Nam Cns} \Rightarrow L_t, S_3}$$

$$\langle\rangle = discr([\,])$$

For incomplete type declarations, a new incomplete type descriptor carries the discriminant information.

$$\frac{\begin{array}{c} new\_type(S_0, (none \times incomplete\_type(\langle\rangle)), U, S_1) \\ new\_subtype(S_1, subtype(U, no\_constraint, not\_used), L_s, S_2) \end{array}}{S_0, E_1 \vdash_{dcl} \textbf{type } \textsf{I}_\textsf{d}; \ \Rightarrow E_1[I_d \mapsto subtype\_view(L_s)], S_2}$$

$$\frac{\begin{array}{c} S_1, E_1 \vdash_{dsc} \textsf{Dcp} \Rightarrow D, S_2 \\ new\_type(S_2, (none \times incomplete\_type(D)), U, S_3) \\ new\_subtype(S_3, subtype(U, no\_constraint, not\_used), L_s, S_4) \end{array}}{S_1, E_1 \vdash_{dcl} \textbf{type } \textsf{I}_\textsf{d} \ \textsf{Dcp}; \ \Rightarrow E_1[I_d \mapsto subtype\_view(L_s)], S_3}$$

Completing type declarations have their own abstract syntax.

$$\frac{\begin{array}{c} E_1 \vdash_{lookup} \textsf{I}_\textsf{d} \Rightarrow subtype\_view(L_s) \\ S_1, E_1, \langle\rangle \vdash_{tdf} \textsf{Tdf} \Rightarrow S_t, E_2, S_2 \end{array}}{S_1, E_1 \vdash_{dcl} \textbf{completetype } \textsf{I}_\textsf{d} \ \textbf{is } \textsf{Tdf}; \ \Rightarrow E_2, S_2[L_s \mapsto_4 S_t]}$$

$$\frac{\begin{array}{c} E_1 \vdash_{lookup} \textsf{I}_\textsf{d} \Rightarrow subtype\_view(L_s) \\ S_1 \left[ \begin{array}{c} E \vdash_{dsc} \textsf{Dcp} \Rightarrow D \\ E, D \vdash_{tdf} \textsf{Tdf} \Rightarrow S_t, E_2 \end{array} \right] S_2 \end{array}}{S_1, E_1 \vdash_{dcl} \textbf{completetype } \textsf{I}_\textsf{d} \ \textsf{Dcp is } \textsf{Tdf}; \ \Rightarrow E_2, S_2[L_s \mapsto_4 S_t]}$$

## 4.10 Expressions

### 4.10.1 Names

$$\frac{E \vdash_{lookup} \textsf{Idn} \Rightarrow W}{S, E \vdash_{nam} \textsf{Idn} \Rightarrow W, S}$$

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{nam} \textsf{Nam} \Rightarrow object\_view(L_1, S_t, ?) \\ \vdash content(L_1) \Rightarrow access\_val(W, ?) \end{array} \right] S_2}{S_1, E \vdash_{nam} \textsf{Nam.all} \Rightarrow W, S_2}$$

#### 4.10.1.1   Indexed Components

The function *expression_list* computes a sequence of actions that corresponds to the evaluation of a sequence of expressions.

$$expression\_list(E, [\,], [\,], [\,])$$

$$\frac{\begin{array}{c} expression\_list(E, \mathsf{Exs}, V_s, A_s) \\ A = E \vdash_{exp} \mathsf{Exp} \Rightarrow V \end{array}}{expression\_list(E, \mathsf{Exp} \cdot \mathsf{Exs}, V \cdot V_s, A \cdot A_s)}$$

$$index\_list(S, [\,], [\,], [\,], S)$$

$$\frac{\begin{array}{c} belongs\_to(V, R) \\ index\_list(S_1, R_s, V_s, I_s, S_2) \end{array}}{index\_list(S_1, R \cdot R_s, V \cdot V_s, V \cdot I_s, S_2)}$$

$$\frac{\neg belongs\_to(V, R)}{index\_list(normal(N), R \cdot R_s, V \cdot V_s, I \cdot I_s, exception(constraint\_error, N))}$$

$$\frac{S_1 \left\{ \begin{array}{c} expression\_list(E, \mathsf{Exs}, V_i, A_s) \\ E \vdash_{nam} \mathsf{Prefix} \Rightarrow object\_view(L_1, S_t, ?) \\ A_{s\,1} \\ \ldots \\ A_{s\,n} \end{array} \right\} S_2}{S_1, E \vdash_{nam} \mathsf{Prefix}(\mathsf{Exs}, \ldots) \Rightarrow undefined\_view, S_2} \quad abnormal\_state(S_2)$$

$$\frac{\begin{array}{c} S_1 \left\{ \begin{array}{c} expression\_list(E, \mathsf{Exs}, V_i, A_s) \\ E \vdash_{nam} \mathsf{Prefix} \Rightarrow object\_view(L_1, S_t, C) \\ A_{s\,1} \\ \ldots \\ A_{s\,n} \end{array} \right\} S_2 \\ normal\_state(S_2) \\ type\_struct(S_2, S_t) = array\_type(?, B) \\ S_2 \vdash content(L_1) \Rightarrow array\_val(R, A_v) \\ index\_list(S_2, R, V_i, I_x, S_3) \end{array}}{S_1, E \vdash_{nam} \mathsf{Prefix}(\mathsf{Exs}, \ldots) \Rightarrow object\_view(array\_component(L_1, I_x), B, C), S_3}$$

#### 4.10.1.2   Slices

$$\frac{null\_range(R_s)}{slice\_check(S, R_s, R_a, S)}$$

$$\frac{included\_in(R_s, R_a)}{slice\_check(S, R_s, R_a, S)}$$

$$\frac{\neg null\_range(R_s) \qquad \neg included\_in(R_s, R_a)}{slice\_check(normal(N), R_s, R_a, exception(constraint\_error, N))}$$

$$\frac{S_1 \left\{ \begin{array}{l} E \vdash_{nam} \mathsf{Prefix} \Rightarrow W \\ E \vdash_{rng} \mathsf{Rng} \Rightarrow R_s \end{array} \right\} S_2 \qquad abnormal\_state(S_2)}{S_1, E \vdash_{nam} \mathsf{Prefix(Rng)} \Rightarrow undefined\_view, S_2}$$

$$\frac{\begin{array}{c} S_1 \left\{ \begin{array}{l} E \vdash_{nam} \mathsf{Prefix} \Rightarrow object\_view(L_v, S_t, C) \\ E \vdash_{rng} \mathsf{Rng} \Rightarrow R_s \end{array} \right\} S_2 \\ normal\_state(S_2) \\ S_2 \vdash content(L_v) \Rightarrow array\_val([\,R_a\,], A_v) \\ constrain(S_t, range\_constraint(R_s), S_q) \\ slice\_check(S_2, R_s, R_a, S_3) \end{array}}{S_1, E \vdash_{nam} \mathsf{Prefix(Rng)} \Rightarrow object\_view(array\_slice(L_v, R_s), S_q, C), S_3}$$

### 4.10.1.3 Selected Components

$$\frac{S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow W, S_2 \qquad abnormal\_state(S_2)}{S_1, E \vdash_{nam} \mathsf{Nam.Idn} \Rightarrow undefined\_view, S_2}$$

$$\frac{\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow object\_view(L_v, S_t, ?), S_2 \\ component\_type(D_v, type\_struct(S_2, S_t), \mathsf{Idn}, S_q) \\ S_2 \vdash content(L_v) \Rightarrow record\_val(T_g, D_v, C_v) \\ new\_object(S_2, D_v[\mathsf{Idn}], L, S_3) \end{array}}{S_1, E \vdash_{nam} \mathsf{Nam.Idn} \Rightarrow object\_view(location(L), S_q, constant), S_3}$$

$$\frac{\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow object\_view(L_v, S_t, C), S_2 \\ S_2 \vdash content(L_v) \Rightarrow record\_val(T_g, D_v, C_v) \\ component\_type(D_v, type\_struct(S_2, S_t), \mathsf{Idn}, S_q) \end{array}}{S_1, E \vdash_{nam} \mathsf{Nam.Idn} \Rightarrow object\_view(record\_component(L_v, \mathsf{Idn}), S_q, C), S_2}$$

$$\frac{S, E \vdash_{nam} \mathsf{Nam} \Rightarrow object\_view(L_v, S_t, ?), normal(N) \qquad \neg component\_type(B, type\_struct(normal(N), S_t), \mathsf{Idn}, S_q)}{S, E \vdash_{nam} \mathsf{Nam.Idn} \Rightarrow undefined\_view, exception(constraint\_error, N)}$$

#### 4.10.1.4 Expanded Names

#### 4.10.1.5 Attributes

$$S_1 \left[ \begin{array}{c} E \vdash_{nam} \mathsf{Nam} \Rightarrow W_1 \\ E,\, W_1 \vdash_{att} \mathsf{Idn} \Rightarrow W \end{array} \right] S_2$$
$$\overline{S_1,\, E \vdash_{nam} \mathsf{Nam'Idn} \Rightarrow W,\, S_2}$$

$$S_1,\, E \vdash_{exp} \mathsf{Exp} \Rightarrow V,\, S_1$$
$$S_1 \left[ \begin{array}{c} E \vdash_{nam} \mathsf{Nam} \Rightarrow W_1 \\ E,\, W_1,\, V \vdash_{att_p} \mathsf{Idn} \Rightarrow W \end{array} \right] S_2$$
$$\overline{S,\, E \vdash_{nam} \mathsf{Nam'Idn(Exp)} \Rightarrow W,\, S}$$

Note that the abstract syntax distinguishes N'I(E) for static expression E from N'I(E) where N'I is a function-valued attribute.

### 4.10.2 Literals

$$S,\, E \vdash_{exp} \mathbf{null} \Rightarrow null,\, S$$

In the abstract syntax, the representation of character literals is given by the numeric value of the position of the character.

$$S,\, E \vdash_{exp} \mathsf{'C'} \Rightarrow discrete\_val(C),\, S$$

$$S,\, E \vdash_{exp} \mathsf{R} \Rightarrow real\_val(R),\, S$$

$$S,\, E \vdash_{exp} \mathsf{N} \Rightarrow discrete\_val(N),\, S$$

### 4.10.3 Aggregates

Only explicitly qualified aggregates are defined. Static semantics adds qualification where needed.

We assume a normalized representation using named associations. This is possible because of [4.3.1(14)].

$$S_1,\, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s),\, S_1$$
$$type\_struct(S_1,\, S_1^{stp}[L_s]) = record\_type(T_g,\, discr(L),\, C_l)$$
$$S_1^{stp}[L_s] = subtype(?,\, no\_constraint,\, ?)$$
$$S_1,\, E,\, L \vdash_{agg} \mathsf{Agg} \Rightarrow B_d,\, S_2$$
$$\underline{S_2,\, E,\, actualized\_components(B_d,\, C_l) \vdash_{agg} \mathsf{Agg} \Rightarrow B_c,\, S_3}$$
$$S_1,\, E \vdash_{exp} \mathsf{Nam'Agg} \Rightarrow record\_val(T_g,\, B_d,\, B_c),\, S_3$$

$$S_1,\, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s),\, S_1$$
$$type\_struct(S_1,\, S_1^{stp}[L_s]) = record\_type(T_g,\, D_a,\, C_l)$$
$$S_1^{stp}[L_s] = subtype(?,\, discriminant\_constraint(B_d),\, ?)$$
$$\underline{S_1,\, E,\, actualized\_components(B_d,\, C_l) \vdash_{agg} \mathsf{Agg} \Rightarrow B_c,\, S_2}$$
$$S_1,\, E \vdash_{exp} \mathsf{Nam'Agg} \Rightarrow record\_val(T_g,\, B_d,\, B_c),\, S_2$$

$$find\_component(I_d, \mathbf{others} => \mathsf{Exp} \cdot \mathsf{Rca}, \mathsf{Exp})$$

$$\frac{member(I_d, \mathsf{Lst})}{find\_component(I_d, \mathsf{Lst}, \ldots => \mathsf{Exp} \cdot \mathsf{Rca}, \mathsf{Exp})}$$

$$component\_actions(E, [\,], \mathsf{Rca}, [\,], [\,])$$

$$\frac{find\_component(I_d, \mathsf{Rca}, \mathsf{Exp})}{component\_actions(E, B, \mathsf{Rca}, B_c, A_s)}$$
$$\frac{}{component\_actions(E, (I_d \times ?) \cdot B, \mathsf{Rca}, (I_d \times V) \cdot B_c, E \vdash_{exp} \mathsf{Exp} \Rightarrow V \cdot A_s)}$$

$$\frac{\neg find\_component(I_d, \mathsf{Rca}, ?)}{component\_actions(E, B, \mathsf{Rca}, B_c, A_s)}$$
$$\frac{}{component\_actions(E, (I_d \times ?) \cdot B, \mathsf{Rca}, (I_d \times V) \cdot B_c, E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow V \cdot A_s)}$$

$$\frac{component\_actions(E, A, \mathsf{Rca}, B, A_s)}{S_1 \left\{ \begin{array}{c} A_{s\,1} \\ \ldots \\ A_{s\,n} \end{array} \right\} S_2}$$
$$\frac{}{S_1, E, A \vdash_{agg} (\mathsf{Rca}, \ldots) \Rightarrow B, S_2}$$

$$S, E, [\,] \vdash_{agg} (\mathbf{null\ record}) \Rightarrow [\,], S$$

$$\frac{not\ yet\ defined}{S_1, E, R_s, C_s \vdash_{agg} (\mathsf{Exp}_1, \mathsf{Exp}_2, \ldots) \Rightarrow V, S_2}$$

$$\frac{not\ yet\ defined}{S_1, E, R_s, C_s \vdash_{agg} (\mathsf{Exp}_1, \mathsf{Exp}_2, \ldots, \mathbf{others} => \mathsf{Exp}) \Rightarrow V, S_2}$$

$$\frac{not\ yet\ defined}{S_1, E, R_s, C_s \vdash_{agg} (\mathsf{Aca}_1, \mathsf{Aca}_2, \ldots) \Rightarrow V, S_2}$$

$$\frac{not\ yet\ defined}{S_1, E, R_s, C_s \vdash_{agg} (\mathsf{Exp}_1, \mathsf{Exp}_2, \ldots, \mathbf{others} => \mathsf{Exp}) \Rightarrow V, S_2}$$

### 4.10.4   Operators and Expression Evaluation

It is assumed that static semantics has resolved all operators into function calls as defined in [4.5] with the following exceptions:

- short-circuit operators

- **in** and **not in** operators

#### 4.10.4.1 Logical Operators and Short-circuit Control Forms

$$S_1 \left[ \begin{array}{c} E \vdash_{exp} \mathsf{Exp_1} \Rightarrow discrete\_val(1) \\ E \vdash_{exp} \mathsf{Exp_2} \Rightarrow V \end{array} \right] S_2$$
$$\overline{S_1, E \vdash_{exp} \mathsf{Exp_1} \textbf{ and then } \mathsf{Exp_2} \Rightarrow V, S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp_1} \Rightarrow discrete\_val(0), S_2}{S_1, E \vdash_{exp} \mathsf{Exp_1} \textbf{ and then } \mathsf{Exp_2} \Rightarrow discrete\_val(0), S_2}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{exp} \mathsf{Exp_1} \Rightarrow discrete\_val(0) \\ E \vdash_{exp} \mathsf{Exp_2} \Rightarrow V \end{array} \right] S_2$$
$$\overline{S_1, E \vdash_{exp} \mathsf{Exp_1} \textbf{ or else } \mathsf{Exp_2} \Rightarrow V, S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp_1} \Rightarrow discrete\_val(1), S_2}{S_1, E \vdash_{exp} \mathsf{Exp_1} \textbf{ or else } \mathsf{Exp_2} \Rightarrow discrete\_val(1), S_2}$$

#### 4.10.4.2 Relational Operators and Membership Tests

$$\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2 \\ belongs\_to(V, range\_of\_subtype(S_1, S_1^{stp}[L_s])) \\ \hline S_1, E \vdash_{exp} \mathsf{Exp} \textbf{ in } \mathsf{Nam} \Rightarrow discrete\_val(1), S_2 \end{array}$$

$$\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2 \\ \neg belongs\_to(V, range\_of\_subtype(S_2, S_1^{stp}[L_s])) \\ \hline S_1, E \vdash_{exp} \mathsf{Exp} \textbf{ in } \mathsf{Nam} \Rightarrow discrete\_val(0), S_2 \end{array}$$

$$S_1 \left\{ \begin{array}{c} E \vdash_{rng} \mathsf{Rng} \Rightarrow R \\ E \vdash_{exp} \mathsf{Exp} \Rightarrow V \end{array} \right\} S_2$$
$$\begin{array}{c} belongs\_to(V, R) \\ \hline S_1, E \vdash_{exp} \mathsf{Exp} \textbf{ in } \mathsf{Rng} \Rightarrow discrete\_val(1), S_2 \end{array}$$

$$S_1 \left\{ \begin{array}{c} E \vdash_{rng} \mathsf{Rng} \Rightarrow R \\ E \vdash_{exp} \mathsf{Exp} \Rightarrow V \end{array} \right\} S_2$$
$$\begin{array}{c} \neg belongs\_to(V, R) \\ \hline S_1, E \vdash_{exp} \mathsf{Exp} \textbf{ in } \mathsf{Rng} \Rightarrow discrete\_val(0), S_2 \end{array}$$

$$\frac{\begin{array}{c} \neg is\_tagged\_type(S, S_t) \\ S_t = subtype(U, C, ?) \\ satisfies(V, C) \end{array}}{test\_in(S, V, S_1)}$$

$$S_t = subtype(U, C, ?)$$
$$satisfies(V, C)$$
$$V = record\_val(some(T_g), ?, ?)$$
$$\frac{ancestor(S, U, T_g)}{test\_in(S, V, S_t)}$$

$$\frac{S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \quad S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2 \quad test\_in(S_2, V, S_1^{stp}[L_s])}{S_1, E \vdash_{exp} \mathsf{Exp\ in\ Nam} \Rightarrow discrete\_val(1), S_2}$$

$$\frac{S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \quad S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2 \quad \neg test\_in(S_2, V, S_1^{stp}[L_s])}{S_1, E \vdash_{exp} \mathsf{Exp\ in\ Nam} \Rightarrow discrete\_val(0), S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp\ in\ Nam} \Rightarrow discrete\_val(1), S_2}{S_1, E \vdash_{exp} \mathsf{Exp\ not\ in\ Nam} \Rightarrow discrete\_val(0), S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp\ in\ Nam} \Rightarrow discrete\_val(0), S_2}{S_1, E \vdash_{exp} \mathsf{Exp\ not\ in\ Nam} \Rightarrow discrete\_val(1), S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp\ in\ Rng} \Rightarrow discrete\_val(1), S_2}{S_1, E \vdash_{exp} \mathsf{Exp\ not\ in\ Rng} \Rightarrow discrete\_val(0), S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp\ in\ Rng} \Rightarrow discrete\_val(0), S_2}{S_1, E \vdash_{exp} \mathsf{Exp\ not\ in\ Rng} \Rightarrow discrete\_val(1), S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp\ in\ Nam} \Rightarrow discrete\_val(1), S_2}{S_1, E \vdash_{exp} \mathsf{Exp\ not\ in\ Nam} \Rightarrow discrete\_val(0), S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp\ in\ Nam} \Rightarrow discrete\_val(0), S_2}{S_1, E \vdash_{exp} \mathsf{Exp\ not\ in\ Nam} \Rightarrow discrete\_val(1), S_2}$$

### 4.10.5 Type Conversions

$$\frac{S_1 \left[ \begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ E \vdash_{exp} \mathsf{Exp} \Rightarrow V_1 \\ E, S_1^{stp}[L_s] \vdash subtype\_convert(V_1) \Rightarrow V_2 \end{array} \right] S_2}{S_1, E \vdash_{exp} \mathsf{Nam(Exp)} \Rightarrow V_2, S_2}$$

$$S_1 \left[ \begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam}_1 \Rightarrow subtype\_view(L_s), S_1 \\ E \vdash_{nam} \mathsf{Nam}_2 \Rightarrow W_1 \\ E, S_1^{stp}[L_s] \vdash subtype\_convert(W_1) \Rightarrow W_2 \end{array} \right] S_2$$
$$\frac{}{S_1, E \vdash_{nam} \mathsf{Nam}_1(\mathsf{Nam}_2) \Rightarrow W_2, S_2}$$

### 4.10.6  Qualified Expressions

$$\frac{\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2 \\ abnormal\_state(S_2) \end{array}}{S_1, E \vdash_{exp} \mathsf{Nam}'(\mathsf{Exp}) \Rightarrow V, S_2}$$

$$\frac{\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ S_1^{stp}[L_s] = subtype(?, C, ?) \\ S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2 \\ normal\_state(S_2) \\ satisfies(V, C) \end{array}}{S_1, E \vdash_{exp} \mathsf{Nam}'(\mathsf{Exp}) \Rightarrow V, S_2}$$

$$\frac{\begin{array}{c} S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(L_s), S_1 \\ S_1^{stp}[L_s] = subtype(?, C, ?) \\ S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, normal(N) \\ \neg satisfies(V, C) \end{array}}{S_1, E \vdash_{exp} \mathsf{Nam}'(\mathsf{Exp}) \Rightarrow V, exception(constraint\_error, N)}$$

### 4.10.7  Allocators

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{exp} \mathsf{Exp} \Rightarrow V \\ new\_object\_fn(invalid\_val, L) \end{array} \right] S_2}{S_1, E \vdash_{exp} \mathbf{new}\ \mathsf{Exp} \Rightarrow access\_val(object\_view(location(L), ?, aliased), none), S_2}$$

$$\frac{not\ yet\ defined}{S, E \vdash_{exp} \mathbf{new}\ \mathsf{Sid} \Rightarrow V, S}$$

## 4.11  Statements

### 4.11.1  Statement Sequences

$$\frac{S_0 \left[ \begin{array}{c} E \vdash_{stm} \mathsf{Stm}_1 \Rightarrow \\ E \vdash_{stm} \mathsf{Stm}_2 \ldots \Rightarrow \end{array} \right] S_1}{S_0, E \vdash_{stm} \mathsf{Stm}_1\ \mathsf{Stm}_2\ \ldots \Rightarrow S_1}$$

$$S, E \vdash_{stm} \langle\rangle \Rightarrow S$$

$$\frac{S, E \vdash_{stm} \textsf{Stm} \Rightarrow S}{S, E \vdash_{stm} \textsf{<< Nam >> Stm} \Rightarrow S}$$

$$S, E \vdash_{stm} \textbf{null}; \; \Rightarrow S$$

## 4.11.2 Assignment Statements

$$assignable(variable)$$

$$assignable(aliased)$$

$$\frac{S_0 \left\{ \begin{array}{c} E \vdash_{nam} \textsf{Nam} \Rightarrow object\_view(L, S_t, M) \\ E \vdash_{exp} \textsf{Exp} \Rightarrow V \end{array} \right\} S_1 \\ assignable(M) \\ S_1 \left[ \begin{array}{c} E, S_t \vdash subtype\_convert(V) \Rightarrow V_1 \\ \vdash content(L) \Rightarrow V_0 \\ finalize\_fn(E, S_t, V_0) \\ assign\_fn(E, S_t, L, V_1) \\ value\_split\_fn(E, S_t, V_1) \end{array} \right] S_2}{S_0, E \vdash_{stm} \textsf{Nam := Exp} \Rightarrow S_2}$$

$$\frac{S_0 \left\{ \begin{array}{c} E \vdash_{nam} \textsf{Nam} \Rightarrow object\_view(L, S_t, variable) \\ E \vdash_{exp} \textsf{Exp} \Rightarrow V \end{array} \right\} S_1 \\ not \; yet \; defined}{S_0, E \vdash_{stm} \textsf{Nam := Exp} \Rightarrow S_1}$$

## 4.11.3 If Statements

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{exp} \textsf{Exp} \Rightarrow discrete\_val(1) \\ E \vdash_{stm} \textsf{Stm}_1 \Rightarrow \end{array} \right] S_2}{S_1, E \vdash_{stm} \textbf{if } \textsf{Exp} \textbf{ then } \textsf{Stm}_1 \textbf{ Eif else } \textsf{Stm}_2 \textbf{ end if}; \; \Rightarrow S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{exp} \textsf{Exp} \Rightarrow discrete\_val(0) \\ E \vdash_{elf} \textsf{Eif} \Rightarrow true \end{array} \right] S_2}{S_1, E \vdash_{stm} \textbf{if } \textsf{Exp} \textbf{ then } \textsf{Stm}_1 \textbf{ Eif else } \textsf{Stm}_2 \textbf{ end if}; \; \Rightarrow S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{exp} \textsf{Exp} \Rightarrow discrete\_val(0) \\ E \vdash_{elf} \textsf{Eif} \Rightarrow false \\ E \vdash_{stm} \textsf{Stm}_2 \Rightarrow \end{array} \right] S_2}{S_1, E \vdash_{stm} \textbf{if } \textsf{Exp} \textbf{ then } \textsf{Stm}_1 \textbf{ Eif else } \textsf{Stm}_2 \textbf{ end if}; \; \Rightarrow S_2}$$

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{exp} \textsf{Exp} \Rightarrow discrete\_val(1) \\ E \vdash_{stm} \textsf{Stm}_1 \Rightarrow \end{array} \right] S_2}{S_1, E \vdash_{stm} \textbf{if } \textsf{Exp} \textbf{ then } \textsf{Stm}_1 \textbf{ Eif end if}; \; \Rightarrow S_2}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{exp} \mathsf{Exp} \Rightarrow discrete\_val(0) \\ E \vdash_{elf} \mathsf{Eif} \Rightarrow true \end{array} \right] S_2$$
$$\overline{S_1, E \vdash_{stm} \textbf{if } \mathsf{Exp} \textbf{ then } \mathsf{Stm}_1 \textbf{ Eif end if}; \Rightarrow S_2}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{exp} \mathsf{Exp} \Rightarrow discrete\_val(0) \\ E \vdash_{elf} \mathsf{Eif} \Rightarrow false \end{array} \right] S_2$$
$$\overline{S_1, E \vdash_{stm} \textbf{if } \mathsf{Exp} \textbf{ then } \mathsf{Stm}_1 \textbf{ Eif end if}; \Rightarrow S_2}$$

$$S, E \vdash_{elf} \langle\rangle \Rightarrow false, S$$

$$\frac{S_1, E \vdash_{elf} \mathsf{Eif}_1 \Rightarrow true, S_2}{S_1, E \vdash_{elf} \mathsf{Eif}_1 \mathsf{Eif}_2 \ldots \Rightarrow true, S_2}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{elf} \mathsf{Eif}_1 \Rightarrow false \\ E \vdash_{elf} \mathsf{Eif}_2 \ldots \Rightarrow R \end{array} \right] S_2$$
$$\overline{S_1, E \vdash_{elf} \mathsf{Eif}_1 \mathsf{Eif}_2 \ldots \Rightarrow R, S_2}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{exp} \mathsf{Exp} \Rightarrow discrete\_val(1) \\ E \vdash_{stm} \mathsf{Stm} \Rightarrow \end{array} \right] S_2$$
$$\overline{S_1, E \vdash_{elf} \textbf{elsif } \mathsf{Exp} \textbf{ then } \mathsf{Stm} \Rightarrow true, S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow discrete\_val(0), S_2}{S_1, E \vdash_{elf} \textbf{elsif } \mathsf{Exp} \textbf{ then } \mathsf{Stm} \Rightarrow false, S_2}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{exp} \mathsf{Exp} \Rightarrow V \\ E, V \vdash_{clt} \mathsf{Alt} \Rightarrow true \end{array} \right] S_2$$
$$\overline{S_1, E \vdash_{stm} \textbf{case } \mathsf{Exp} \textbf{ is } \mathsf{Alt} \textbf{ end case}; \Rightarrow S_2}$$

### 4.11.4 Case Statements

$$normal(N), E, V \vdash_{clt} \langle\rangle \Rightarrow R, exception(constraint\_error, N)$$

$$\frac{S_1, E, V \vdash_{clt} \mathsf{Alt}_1 \Rightarrow true, S_2}{S_1, E, V \vdash_{clt} \mathsf{Alt}_1 \mathsf{Alt}_2 \ldots \Rightarrow true, S_2}$$

$$S_1 \left[ \begin{array}{c} E, V \vdash_{clt} \mathsf{Alt}_1 \Rightarrow false \\ E, V \vdash_{clt} \mathsf{Alt}_2 \ldots \Rightarrow R \end{array} \right] S_2$$
$$\overline{S_1, E, V \vdash_{clt} \mathsf{Alt}_1 \mathsf{Alt}_2 \ldots \Rightarrow R, S_2}$$

$$S_1 \left[ \begin{array}{c} E \vdash_{chc} \mathsf{Dch} \Rightarrow C \\ covers\_fn(V, C, true) \\ E \vdash_{stm} \mathsf{Stm} \Rightarrow \end{array} \right] S_2$$
$$\overline{S_1, E, V \vdash_{clt} \textbf{when } \mathsf{Dch} => \mathsf{Stm} \Rightarrow true, S_2}$$

$$S_1 \begin{bmatrix} E \vdash_{chc} \mathsf{Dch} \Rightarrow C \\ covers\_fn(V, C, false) \end{bmatrix} S_2$$
$$\overline{S_1, E, V \vdash_{clt} \mathbf{when} \ \mathsf{Dch} => \mathsf{Stm} \Rightarrow false, S_2}$$

$$\frac{S, E \vdash_{stm} \mathsf{Stm} \Rightarrow exit(unnamed, N)}{S, E \vdash_{stm} \mathbf{loop} \ \mathsf{Stm} \ \mathbf{end} \ \mathbf{loop}; \ \Rightarrow normal(N)}$$

### 4.11.4.1 Choices

$$\frac{S_1, E \vdash_{rng} \mathsf{Rng} \Rightarrow R, S_2}{S, E \vdash_{chc} \mathsf{Rng} \Rightarrow choice\_range(R), S_2}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, S_2}{S_1, E \vdash_{chc} \mathsf{Exp} \Rightarrow choice\_value(V), S_2}$$

$$S, E \vdash_{chc} \mathbf{others} \Rightarrow choice\_default, S$$

$$S, E \vdash_{chc} \langle\rangle \Rightarrow choice\_lst([\,]), S$$

$$S_1, E \vdash_{chc} \mathsf{Dch}_1 \Rightarrow C_1, S_2$$
$$\frac{S_2, E \vdash_{chc} \mathsf{Dch}_2 \mid \ldots \Rightarrow choice\_lst(C_2), S_3}{S_1, E \vdash_{chc} \mathsf{Dch}_1 \mid \mathsf{Dch}_2 \mid \ldots \Rightarrow choice\_lst(C_1 \cdot C_2), S_3}$$

$$covers(V, choice\_value(V), true)$$

$$\frac{N_1 \neq N_2}{covers(discrete\_val(N_1), choice\_value(discrete\_val(N_2)), false)}$$

$$\frac{belongs\_to(V, R)}{covers(V, choice\_range(R), true)}$$

$$\frac{\neg belongs\_to(V, R)}{covers(V, choice\_range(R), false)}$$

$$covers(V, choice\_default, true)$$

$$covers(V, choice\_lst([\,]), false)$$

$$\frac{covers(V, C_1, true)}{covers(V, choice\_lst(C_1 \cdot C_2), true)}$$

$$\frac{covers(V, C_1, false) \quad covers(V, choice\_lst(C_2), R)}{covers(V, choice\_lst(C_1 \cdot C_2), R)}$$

### 4.11.5 Loop Statements

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{stm} \text{Stm} \Rightarrow \\ E \vdash_{stm} \textbf{loop Stm end loop;} \Rightarrow \end{array} \right] S_2}{S_1, E \vdash_{stm} \textbf{loop Stm end loop;} \Rightarrow S_2}$$

$$\frac{unique(X) \quad S_1, E_1[\text{Idn} \mapsto loop\_view(X)] \vdash_{stm} \textbf{loop Stm end loop;} \Rightarrow normal(N)}{S_1, E_1 \vdash_{stm} \text{Idn} : \textbf{loop Stm end loop;} \Rightarrow normal(N)}$$

$$\frac{unique(X) \quad S_1, E_1[\text{Idn} \mapsto loop\_view(X)] \vdash_{stm} \textbf{loop Stm end loop;} \Rightarrow exit(loop\_id(X), N)}{S_1, E_1 \vdash_{stm} \text{Idn} : \textbf{loop Stm end loop;} \Rightarrow normal(N)}$$

$$\frac{S \left[ \begin{array}{c} E \vdash_{exp} \text{Exp} \Rightarrow discrete\_val(1) \\ E \vdash_{stm} \text{Stm} \Rightarrow \end{array} \right] exit(unnamed, N)}{S, E \vdash_{stm} \textbf{while Exp loop Stm end loop;} \Rightarrow normal(N)}$$

$$\frac{S_1 \left[ \begin{array}{c} E \vdash_{exp} \text{Exp} \Rightarrow discrete\_val(1) \\ E \vdash_{stm} \text{Stm} \Rightarrow \\ E \vdash_{stm} \textbf{while Exp loop Stm end loop;} \Rightarrow \end{array} \right] S_2}{S_1, E \vdash_{stm} \textbf{while Exp loop Stm end loop;} \Rightarrow S_2}$$

$$\frac{S_1, E \vdash_{exp} \text{Exp} \Rightarrow discrete\_val(0), S_2}{S_1, E \vdash_{stm} \textbf{while Exp loop Stm end loop;} \Rightarrow S_2}$$

$$\frac{unique(X) \quad S_1, E_1[\text{Idn} \mapsto loop\_view(X)] \vdash_{stm} \textbf{while Exp loop Stm end loop;} \Rightarrow normal(N)}{S_1, E_1 \vdash_{stm} \text{Idn} : \textbf{while Exp loop Stm end loop;} \Rightarrow normal(N)}$$

$$\frac{unique(X) \quad S_1, E_1[\text{Idn} \mapsto loop\_view(X)] \vdash_{stm} \textbf{while Exp loop Stm end loop;} \Rightarrow exit(loop\_id(X), N)}{S_1, E_1 \vdash_{stm} \text{Idn} : \textbf{while Exp loop Stm end loop;} \Rightarrow normal(N)}$$

### 4.11.6 Block Statements

$$\frac{S_1, E \vdash_{stm} \mathsf{Hsm} \Rightarrow S_2}{S_1, E \vdash_{stm} \mathbf{begin}\ \mathsf{Hsm}\ \mathbf{end};\ \Rightarrow S_2}$$

$$\frac{S_1, E \vdash_{stm} \mathsf{Hsm} \Rightarrow S_2}{S_1, E \vdash_{stm} \mathsf{Nam} : \mathbf{begin}\ \mathsf{Hsm}\ \mathbf{end};\ \Rightarrow S_2}$$

$$\frac{S_1 \left[\begin{array}{c} E_1 \vdash_{dcl} \mathsf{Dcl} \Rightarrow E_2 \\ E_2 \vdash_{stm} \mathsf{Hsm} \Rightarrow \end{array}\right] S_2 \\ S_2, E_2 \vdash \mathit{finalize}(B) \Rightarrow S_3}{S_1, E_1 \vdash_{stm} \mathbf{declare}\ \mathsf{Dcl}\ \mathbf{begin}\ \mathsf{Hsm}\ \mathbf{end};\ \Rightarrow S_3}$$

$$\frac{S_1 \left[\begin{array}{c} E_1 \vdash_{dcl} \mathsf{Dcl} \Rightarrow E_2 \\ E_2 \vdash_{stm} \mathsf{Hsm} \Rightarrow \end{array}\right] S_2 \\ S_2, E_2 \vdash \mathit{finalize}(B) \Rightarrow S_3}{S_1, E_1 \vdash_{stm} \mathsf{Nam} : \mathbf{declare}\ \mathsf{Dcl}\ \mathbf{begin}\ \mathsf{Hsm}\ \mathbf{end};\ \Rightarrow S_3}$$

### 4.11.7 Exit Statements

$$\mathit{normal}(N), E \vdash_{stm} \mathbf{exit};\ \Rightarrow \mathit{exit}(\mathit{unnamed}, N)$$

$$\frac{S, E \vdash_{nam} \mathsf{Nam} \Rightarrow \mathit{loop\_view}(X), \mathit{normal}(N)}{S, E \vdash_{stm} \mathbf{exit}\ \mathsf{Nam};\ \Rightarrow \mathit{exit}(\mathit{loop\_id}(X), N)}$$

$$\frac{S, E \vdash_{exp} \mathsf{Exp} \Rightarrow \mathit{discrete\_val}(1), \mathit{normal}(N)}{S, E \vdash_{stm} \mathbf{exit\ when}\ \mathsf{Exp};\ \Rightarrow \mathit{exit}(\mathit{unnamed}, N)}$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow B, S_2}{S_1, E \vdash_{stm} \mathbf{exit\ when}\ \mathsf{Exp};\ \Rightarrow S_2}$$

$$\frac{S \left[\begin{array}{c} E \vdash_{nam} \mathsf{Nam} \Rightarrow \mathit{loop\_view}(X) \\ E \vdash_{exp} \mathsf{Exp} \Rightarrow \mathit{discrete\_val}(1) \end{array}\right] \mathit{normal}(N)}{S, E \vdash_{stm} \mathbf{exit}\ \mathsf{Nam}\ \mathbf{when}\ \mathsf{Exp};\ \Rightarrow \mathit{exit}(\mathit{loop\_id}(X), N)}$$

$$\frac{S_1 \left[\begin{array}{c} E \vdash_{nam} \mathsf{Nam} \Rightarrow \mathit{loop\_view}(X) \\ E \vdash_{exp} \mathsf{Exp} \Rightarrow \mathit{discrete\_val}(0) \end{array}\right] S_2}{S_1, E \vdash_{stm} \mathbf{exit}\ \mathsf{Nam}\ \mathbf{when}\ \mathsf{Exp};\ \Rightarrow S_2}$$

## 4.12 Subprograms

### 4.12.1 Subprogram Declarations

$$\frac{S_1, E_1 \vdash_{pas} \mathsf{Pms} \Rightarrow A, S_2 \\ \mathit{new\_subprogram}(S_2, \mathit{unelaborated}, U, S_3)}{S_1, E_1 \vdash_{dcl} \mathbf{procedure}\ \mathsf{Idn}\ \mathsf{Pms};\ \Rightarrow E_1[\mathsf{Idn} \mapsto \mathit{subprogram\_view}(U, A, \mathit{none})], S_3}$$

$$S_1, E_1 \vdash_{pas} \mathsf{Pms} \Rightarrow A, S_2$$
$$S_2, E_1 \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(S_l), S_2$$
$$new\_subprogram(S_2, unelaborated, U, S_3)$$
$$\overline{S_1, E_1 \vdash_{dcl} \textbf{function } \mathsf{Idn} \; \mathsf{Pms}; \; \Rightarrow E_1[\mathsf{Idn} \mapsto subprogram\_view(U, A, some(S_2^{stp}[S_l]))], S_3}$$


$$S_1, E \vdash_{pas} \mathsf{Pms} \Rightarrow A, S_2$$
$$E \vdash_{lookup} \mathsf{Idn} \Rightarrow subprogram\_view(U, A, none)$$
$$\overline{S_1, E \vdash_{dcl} \textbf{procedure } \mathsf{Idn} \; \mathsf{Pms} \textbf{ is } \mathsf{Dcl} \textbf{ begin } \mathsf{Stm} \textbf{ end}; \; \Rightarrow E, S_2[U \mapsto_2 subprogram(E, adom(A), \mathsf{Dcl}, \mathsf{Stm})]}$$


$$S_1, E \vdash_{pas} \mathsf{Pms} \Rightarrow A, S_2$$
$$S_2, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(S_l), S_2$$
$$E \vdash_{lookup} \mathsf{Idn} \Rightarrow subprogram\_view(U, A, some(S_2^{stp}[S_l]))$$
$$\overline{S_1, E \vdash_{dcl} \textbf{function } \mathsf{Idn} \; \mathsf{Pms} \textbf{ is } \mathsf{Dcl} \textbf{ begin } \mathsf{Stm} \textbf{ end}; \; \Rightarrow E, S_2}$$


$$S, E \vdash_{pas} \langle\rangle \Rightarrow [\,], S$$


$$not \; yet \; defined$$
$$\overline{S, E \vdash_{pas} \mathsf{Idn} : \textbf{access } \mathsf{Nam}; \; \mathsf{Pms}; \; \ldots \Rightarrow A, S}$$


$$not \; yet \; defined$$
$$\overline{S, E \vdash_{pas} \mathsf{Idn} : \textbf{access } \mathsf{Nam} := \mathsf{Exp}; \; \mathsf{Pms}; \; \ldots \Rightarrow A, S}$$


$$\vdash_{mod} \mathsf{Mde} \Rightarrow M$$
$$S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(S_l), S_1$$
$$S_1, E \vdash_{pas} \mathsf{Pms}; \; \ldots \Rightarrow A_1, S_2$$
$$\overline{S_1, E \vdash_{pas} \mathsf{Idn} : \mathsf{Mde} \; \mathsf{Nam} := \mathsf{Exp}; \; \mathsf{Pms}; \; \ldots \Rightarrow A_1[\mathsf{Idn} \mapsto formal(M, S_1^{stp}[S_l], some(thunk(E, \mathsf{Exp})))], S_2}$$


$$\vdash_{mod} \mathsf{Mde} \Rightarrow M$$
$$S_1, E \vdash_{nam} \mathsf{Nam} \Rightarrow subtype\_view(S_l), S_1$$
$$S_1, E \vdash_{pas} \mathsf{Pms}; \; \ldots \Rightarrow A_1, S_2$$
$$\overline{S, E \vdash_{pas} \mathsf{Idn} : \mathsf{Mde} \; \mathsf{Nam}; \; \mathsf{Pms}; \; \ldots \Rightarrow A, S}$$


### 4.12.2  Formal Parameter Modes

$$\vdash_{mod} \textbf{in} \Rightarrow in\_mode$$


$$\vdash_{mod} \textbf{in out} \Rightarrow in\_out\_mode$$


$$\vdash_{mod} \Rightarrow in\_mode$$

$$\vdash_{mod} \textbf{out} \Rightarrow out\_mode$$

### 4.12.3 Subprogram Bodies

There are no semantics associated with subprogram bodies. The declarations and the statement part of a subprogram body, together with the declaration environment, are stored as a subprogram value. The rules given below define the effect of executing a subprogram value.

The following definition creates an environment for the execution of a procedure body by binding the formal parameter names to the views of the actual parameters. The actual parameters are given as an association but, due to renaming, the names in the association may differ from those of the formal parameters.

$$bind\_actuals(E, [\,], [\,], E)$$

$$\frac{bind\_actuals(E_1[I_1 \mapsto W_1], P, \textsf{Ids}, E_3)}{bind\_actuals(E_1, (P_1 \times W_1) \cdot P, I_1 \cdot \textsf{Ids}, E_3)}$$

$$proc\_exit(exception(X, N), exception(X, N))$$

$$\frac{not \ yet \ defined}{proc\_exit(exit(?, N), ?)}$$

$$\frac{not \ yet \ defined}{proc\_exit(func\_return(?, N), ?)}$$

$$proc\_exit(proc\_return(N), normal(N))$$

$$proc\_exit(normal(N), normal(N))$$

$$\frac{\begin{array}{c} S_1^{spg}[L] = subprogram(E_1, \textsf{Ids}, \textsf{Dcl}, \textsf{Stm}) \\ bind\_actuals(E_1, A, \textsf{Ids}, E_2) \\ S_1 \left[ \begin{array}{c} E_2 \vdash_{dcl} \textsf{Dcl} \Rightarrow E_3 \\ E_3 \vdash_{stm} \textsf{Stm} \Rightarrow \end{array} \right] S_2 \\ proc\_exit(S_2, S_3) \end{array}}{subprogram\_body(S_1, A, subprogram\_view(L, A_f, none), S_3)}$$

$$return\_check(exception(X, N), S_t, exception(X, N))$$

$$\frac{not\ yet\ defined}{return\_check(exit(?, N), S_t, S)}$$

$$\frac{not\ yet\ defined}{return\_check(proc\_return(N), S_t, S)}$$

$$\frac{convert\_return\_value(normal(N), W_1, S_t, W_2)}{return\_check(func\_return(W_1, N), S_t, func\_return(W_2, N))}$$

$$return\_check(normal(N), S_t, exception(program\_error, N))$$

$$\frac{\begin{array}{c} S_1^{spg}[L] = subprogram(E_1, \mathsf{Ids}, \mathsf{Dcl}, \mathsf{Stm}) \\ bind\_actuals(E_1, A, \mathsf{Ids}, E_2) \\ S_1 \left[ \begin{array}{c} E_2 \vdash_{dcl} \mathsf{Dcl} \Rightarrow E_3 \\ E_3 \vdash_{stm} \mathsf{Stm} \Rightarrow \end{array} \right] S_2 \\ return\_check(S_2, S_t, S_3) \end{array}}{subprogram\_body(S_1, A, subprogram\_view(L, A_f, some(S_t)), S_3)}$$

Appropriate rules need to be defined for all predefined operators.

$$\frac{\begin{array}{c} S_1^{spg}[L] = operator(\mathsf{Opn}) \\ not\ yet\ defined \end{array}}{subprogram\_body(S_1, A, subprogram\_view(L, A_f, ?), S_2)}$$

A call to an unelaborated subprogram raises program error.

$$\frac{normal(N)^{spg}[L] = unelaborated}{subprogram\_body(normal(N), A, subprogram\_view(L, A_f, ?), exception(program\_error, N))}$$

### 4.12.4  Subprogram Calls

The rules given here are incomplete and do not describe subtype and view conversions that are part of a call.

$$return\_value(func\_return(W, N), W, normal(N))$$

$$return\_value(exception(X, N), ?, exception(X, N))$$

87

$$parameter\_list(E, \mathsf{Pss}, A_f, A_a, P)$$
$$W = subprogram\_view(?, A_f, ?)$$
$$S_1 \left[ \left\{ \begin{array}{c} E \vdash_{nam} \mathsf{Nam} \Rightarrow W \\ P_1 \\ \ldots \\ P_n \end{array} \right\} \\ subprogram\_body\_fn(A_a, W) \right] S_2$$
$$\dfrac{return\_value(S_2, W_r, S_3)}{S_1, E \vdash_{nam} \mathsf{Nam}(\mathsf{Pss}, \ldots) \Rightarrow W_r, S_3}$$


$$parameter\_list(E, \mathsf{Pss}, A_f, A_a, P)$$
$$W = subprogram\_view(?, A_f, ?)$$
$$S_1 \left[ \left\{ \begin{array}{c} E \vdash_{nam} \mathsf{Nam} \Rightarrow W \\ P_1 \\ \ldots \\ P_n \end{array} \right\} \\ subprogram\_body\_fn(A_a, W) \right] S_2$$
$$\dfrac{}{S_1, E \vdash_{stm} \mathsf{Nam}(\mathsf{Pss}, \ldots); \ \Rightarrow S_2}$$


### 4.12.4.1   Parameter Associations

$$parameter\_list(E, \mathsf{Pss}, [\,], [\,], [\,])$$


$$\dfrac{parameter\_list(E, \mathsf{Pss}, F, R, A)}{parameter\_action(E, \mathsf{Pss}, F_1, R_1, A_1)}$$
$$parameter\_list(E, \mathsf{Pss}, F_1 \cdot F, R_1 \cdot R, A_1 \cdot A)$$


$$\dfrac{\neg given\_parameter(\mathsf{Pss}, \mathsf{Idn}, ?)}{parameter\_action(E, \mathsf{Pss}, (\mathsf{Idn} \times formal(in\_mode, S_t, some(thunk(E_1, \mathsf{Exp})))), (\mathsf{Idn} \times constant\_view(V)), E_1 \vdash_{exp} \mathsf{Exp} \Rightarrow}$$


$$\dfrac{given\_parameter(\mathsf{Pss}, \mathsf{Idn}, \mathsf{Exp})}{parameter\_action(E, \mathsf{Pss}, (\mathsf{Idn} \times formal(in\_mode, S_t, ?)), (\mathsf{Idn} \times constant\_view(V)), E \vdash_{exp} \mathsf{Exp} \Rightarrow V)}$$


$$\dfrac{the\_parameter(\mathsf{Pss}, \mathsf{Idn}, \mathsf{Nam})}{parameter\_action(E, \mathsf{Pss}, (\mathsf{Idn} \times formal(out\_mode, S_t, ?)), (\mathsf{Idn} \times W), E \vdash_{nam} \mathsf{Nam} \Rightarrow W)}$$


$$\dfrac{the\_parameter(\mathsf{Pss}, \mathsf{Idn}, \mathsf{Nam})}{parameter\_action(E, \mathsf{Pss}, (\mathsf{Idn} \times formal(in\_out\_mode, S_t, ?)), (\mathsf{Idn} \times W), E \vdash_{nam} \mathsf{Nam} \Rightarrow W)}$$


$$given\_parameter(\mathsf{Idn} => \mathsf{Exp} \cdot \mathsf{Pss}, \mathsf{Idn}, \mathsf{Exp})$$

$$\frac{\begin{array}{c} \mathsf{Idn}_1 \neq \mathsf{Idn}_2 \\ given\_parameter(\mathsf{Pss}, \mathsf{Idn}_2, \mathsf{Exp}) \end{array}}{given\_parameter(\mathsf{Idn}_1 => ? \cdot \mathsf{Pss}, \mathsf{Idn}_2, \mathsf{Exp})}$$

$$the\_parameter(\mathsf{Idn} => \mathsf{Nam} \cdot \mathsf{Pss}, \mathsf{Idn}, \mathsf{Nam})$$

$$\frac{\begin{array}{c} \mathsf{Idn}_1 \neq \mathsf{Idn}_2 \\ the\_parameter(\mathsf{Pss}, \mathsf{Idn}_2, \mathsf{Nam}) \end{array}}{the\_parameter(\mathsf{Idn}_1 => ? \cdot \mathsf{Pss}, \mathsf{Idn}_2, \mathsf{Nam})}$$

### 4.12.5 Return Statements

$$normal(N), E \vdash_{stm} \textbf{return}; \; \Rightarrow proc\_return(N)$$

$$\frac{S_1, E \vdash_{exp} \mathsf{Exp} \Rightarrow V, normal(N)}{S_1, E \vdash_{stm} \textbf{return } \mathsf{Exp}; \; \Rightarrow func\_return(constant\_view(V), N)}$$

The following needs to be defined to describe the rules of [6.5(6)] through [6.5(21)].

$$\frac{not \; yet \; defined}{convert\_return\_value(S, W_1, S_t, W_2)}$$

## 4.13 Attributes

$$\frac{\begin{array}{c} is\_scalar\_type(S_1, S_1^{stp}[L_s]) \\ low\_bound(range\_of\_subtype(S_1, S_1^{stp}[L_s])) = V \\ new\_object(S_1, V, L, S_2) \end{array}}{S_1, E, subtype\_view(L_s) \vdash_{att} \mathsf{first} \Rightarrow object\_view(L, S_1^{stp}[L_s], constant), S_2}$$

$$\frac{\begin{array}{c} is\_scalar\_type(S_1, S_1^{stp}[L_s]) \\ high\_bound(range\_of\_subtype(S_1, S_1^{stp}[L_s])) = V \\ new\_object(S_1, V, L, S_2) \end{array}}{S_1, E, subtype\_view(L_s) \vdash_{att} \mathsf{last} \Rightarrow object\_view(L, S_1^{stp}[L_s], constant), S_2}$$

$$\frac{\begin{array}{c} S_1^{stp}[L_s] = subtype(U, C, A) \\ is\_scalar\_type(S_1, subtype(U, C, A)) \\ new\_subtype(S_1, subtype(U, no\_constraint, A), L_a, S_2) \end{array}}{S_1, E, subtype\_view(L_s) \vdash_{att} \mathsf{base} \Rightarrow subtype\_view(L_a), S_2}$$

$$\frac{\begin{array}{c} S_1^{stp}[L_s] = subtype(?, index\_constraint(R \cdot R_s), ?) \\ new\_object(S_1, low\_bound(R), L, S_2) \end{array}}{S_1, E, subtype\_view(L_s) \vdash_{att} \mathsf{first} \Rightarrow object\_view(L, S_t, constant), S_2}$$

$$\frac{\begin{array}{c} S_1^{stp}[L_s] = subtype(?, index\_constraint(R \cdot R_s), ?) \\ new\_object(S_1, high\_bound(R), L, S_2) \end{array}}{S_1, E, subtype\_view(L_s) \vdash_{att} \mathsf{last} \Rightarrow object\_view(L, S_t, constant), S_2}$$

$$\frac{\begin{array}{c} S_1^{stp}[L_s] = subtype(?, index\_constraint(R \cdot R_s), ?) \\ low\_bound(R) = discrete\_val(N_l) \\ S_t = subtype(universal\_integer\_tn, no\_constraint, ?) \\ high\_bound(R) = discrete\_val(N_h) \\ new\_object(S_1, discrete\_val(Nh - Nl + 1), L, S_2) \end{array}}{S_1, E, subtype\_view(L_s) \vdash_{att} \mathsf{length} \Rightarrow object\_view(L, S_t, constant), S_2}$$

$$\frac{\begin{array}{c} S_1, E, W \vdash_{att} \mathsf{first} \Rightarrow object\_view(L_1, ?, ?), S_2 \\ S_2, E, W \vdash_{att} \mathsf{last} \Rightarrow object\_view(L_2, ?, ?), S_3 \\ S_3 \vdash content(L_1) \Rightarrow V_1 \\ S_3 \vdash content(L_2) \Rightarrow V_2 \end{array}}{S_1, E, W \vdash_{att_r} \mathsf{range} \Rightarrow make\_range(V_1, V_2), S_3}$$

# Chapter 5

# Exceptions and Optimization

## 5.1 Introduction

Version 5.0 of the Annotated Draft Ada 9X reference manual [4] contains language that obviates many of the problems associated with section 11.6 of the Ada 83 reference manual [10]. The purpose of this chapter is twofold. The first is to examine the Ada revision as represented by Version 5.0 in light of the earlier Language Precision Team work in this area as published in the LPT Task 1 report [9]. The second is to discuss the consequences of the remaining problems that the semantics of Ada 9X present in the areas of predictability and to offer suggestions for accommodating them in practice. The report concludes with a brief commentary on the Annotated Draft used to support this research.

## 5.2 The Ada 9X revision of 11.6

Section 11.6 of the Ada 83 reference manual contained explicit permissions to reorder operations or to omit some checks that might propagate predefined exceptions. In Ada 83 the notion of the "effect" of a program or of an operation was not as clearly defined as it is in Ada 9X and the language of the section gave rise to endless discussions such as those captured in AI-315.

As revised, [11.6] contains two substantive paragraphs, (5) and (7). The first gives permission to avoid raising exceptions under some circumstances. The second permits more extensive reordering of operations than was generally considered permissible in Ada 83 by relaxing the requirements for state predictability when an exception handler is entered.

### 5.2.1 [11.6(5)]

This paragraph allows the implementation to avoid raising exceptions in the face of failures of predefined language exceptions under some circumstances. In the context of a clearer notion of "effect," it is somewhat of an improvement over the language of Ada 83. Even so, the language used in [11.6] is less clear than it might be. Consider the language of [RM-83 11.6(7)]:

> A predefined operation need not be invoked at all, if its only possible effect is to propagate a predefined exception. Similarly, a predefined operation need not be invoked if the removal of subsequent operations by the above rule renders this invocation ineffective. 7

In Ada 83 the term *effect* is not defined[1] and the meaning of the term is the subject of considerable discussion in AI-315 and elsewhere. The gist of many of the discussions concerns the case in which the

---

[1] The index entry for "effect" in [RM-83 Appendix I] is "[see: elaboration has no other effect]."

programmer has apparently written an operation that is sure to raise an exception as a "shorthand" for a **raise** statement. While this should be considered to be poor programming style, suppressing the operation leads to surprising effects.

We note that Chapter 14 of the Ada 83 rationale[2] which deals with exceptions does not discuss the material contained in [RM-83 11.6] and a search through the text of the rationale for the root string "optimiz" does not provide any appropriate insight.

From the discussions contained in AI-315 it appears that the primary need that the language of [RM-83 11.6(7)] is attempting to capture is the desire to remove code that is dead along its normal execution path even if executing it may (or is certain to) raise an exception due to the failure of a language-defined check. According to [11.6(7.f)], the language of [RM-83 11.6(7)] is now reflected in paragraph [11.6(5)] which reads:

> An implementation need not always raise an exception when a language-defined check   5
> fails. Instead, the operation that failed the check can simply yield an *undefined result*.
> The exception need 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.]

### 5.2.1.1   **Defining** *undefined*

Unfortunately, the index for Version 5.0 contains exactly one entry for *undefined result*, i.e., [11.6(5)]. Although this reference purports to define *undefined result*, we are given no useful semantics to associate with the term. Thus we are left to attempt to define exactly what is meant by the phrase through other means. A search of the source text for Version 5.0 yields several additional uses of the word *undefined*. The ones that appear to be related to its use in [11.6(5)] are:

### 13.9.1  NOTES

> 19 Objects can become abnormal due to other kinds of actions that directly update the   14
> object's representation; such actions are generally considered directly erroneous, however.

*Wording Changes From Ada 83*

> In order to reduce the amount of erroneousness, we separate the concept of an   14.a
> 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   14.b
> 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.

### 3.8.1    • The discrete_choice **others** covers all values of its expected type that are not covered by   12
> previous discrete_choice_lists of the same construct.

> > **Ramification:** For case_statements, this includes values outside the range of   12.a
> > 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.

### 7.4                                           *Extensions to Ada 83*

---

[2] This document may be obtained by anonymous ftp from `ajpo.sei.cmu.edu` in the directory `public/rationale`.

The rules for too-early uses of deferred constants are modified in Ada 9X 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 9X, they cannot be touched until they become constant.

The first item seems to be the key. The remaining two items use the word *undefined* in ways that seem to confirm the impressions given by [13.9.1] as a whole. Thus, we see that *undefined* either applies to a scalar object with an invalid representation or to an abnormal object. Abnormal objects can either be produced by disrupted assignments (with a reference from [13.9.1(5)] back to [11.6], presumably to [11.6(6)]) or (for non-scalars) by a return from a call to either a language defined input procedure or to an imported procedure. It is, perhaps, stretching things to call the latter an *operation* in the sense of the discussion of [3.2].

**Discussion:** An *operation* is a program entity that operates on zero or more operands to produce an effect, or yield a result, or both.

It seems more likely that the operations referred to are akin to the *primitive operations* partially defined in 3.2.

A *type* is characterized by a set of values, and a set of *primitive operations* which implement the fundamental aspects of its semantics.

This leads us to consider the invalid values that can be associated with scalar objects and the predefined operations on scalar types. These are discussed in general in [4.5] where the relevant language appears in [4.5(9)–4.5(12)].

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. 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.

*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.

Unfortunately, there is a reading of this language that would make it impossible for a predefined operation on integer types to produce an invalid value. Paragraph (10) requires the operation to either yield the mathematically correct result or to raise Constraint_error. Paragraph (11) states that the implementation of the predefined operation may raise Constraint_error only if the result is outside the base range of the result type. Now, if we assume that "result" in paragraph (11) is the value produced by the implementation, it is almost certainly the case that this result will be within the range of the base type; it just will not be mathematically correct. It is likely that what is intended is

The implementation of a predefined operator that delivers a result of an integer or fixed point type may raise Constraint_Error only if the [mathematically correct] result [of the operation] is outside the base range of the result type.

As the language is currently defined, there is a direct contradiction between the language of [4.5(10-11)] and that of [11.6(5)]

If we assume the revised interpretation, then we have a class of operations that can produce results that are not mathematically correct though they will typically be precisely defined by the implementation. If 11.6(5) is to have any reasonable meaning, it must be the case that results of this kind are the *undefined* results referred to. If this is the case, we have extended the notion of invalid to include representations of scalar objects that do represent values of the object's subtype but are not the mathematically correct values that would be produced without the violated constraint.[3] **This is a fairly serious extension and deserves more consideration.** We will return to this shortly.

### 5.2.1.2    Use of *undefined* results

The implementation note associated with [11.6(5)] seems to raise two distinct points. One, allowing the removal of dead code, is fairly obvious and seems to be the only clear-cut case. The other discusses implementation assumptions and seems to involve the extension noted above.

**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:

```
if X * Y > Integer'Last then
    Put_Line("X * Y overflowed");
end if;
```

---

[3]Addition in a 2's complement $n$ bit machine produces a result that is either a mathematically correct integer result or the mathematically correct integer result minus $2^n$. Consider a 2 bit, 2's complement machine. Its value set is given as

| $i_2$ | $i_{10}$ | | + | 00 ( 0) | 01 ( 1) | 10 (-2) | 11 (-1) | |
|-------|----------|---|---|---------|---------|---------|---------|---|
| 00 | 0 | | 00 ( 0) | 00 ( 0) | 01 ( 1) | 10 (-2) | 11 (-1) | |
| 01 | 1 | and + defined as | 01 ( 1) | 01 ( 1) | *10 (-2)* | 11 (-1) | 00 ( 0) | where the values in *italics* are not |
| 10 | -2 | | 10 (-2) | 10 (-2) | 11 (-1) | *00 ( 0)* | *01 ( 1)* | |
| 11 | -1 | | 11 (-1) | 11 (-1) | 00 ( 0) | *01 ( 1)* | 10 (-2) | |

mathematically correct integer results but are both well-defined and have a valid integer representation.

```
   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:                                5.f

```
   subtype Str10 is String(1..10);                                                     5.g
   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."

The first point is that if the result of an operation is not subsequently used, then we can ignore the
possibility that execution of an operation might have raised an exception. Examples that illustrate
this situation are somewhat contrived since programmers generally do not try to write code that is
not useful. For example, we might illustrate the permission by writing something like:

```
  subtype Str10 is String(1..10);
  X : Str10 := " ";
begin
  X := "2 01";
    Put_line(X);
  X := "8 01234567";
    Put_line(X);
  X := "10 0123456789";
exception
  when others =>
      Put_Line("OOPS");
end;
```

Since the scope of X does not extend beyond the end of the block, the value produced by the last
assignment has no effect along the normal path of execution. [11.6(5)] gives permission to ignore the
possibility (in this case, a certainty) that the assignment will raise Constraint_Error. This, in turn,
allows the elision of the entire assignment statement using conventional, "dead code" elimination
techniques.

Note that without the extra permission of [11.6(5)], the code for the last assignment is not dead
since there is a a well-defined "effect" along the exceptional[4] path. The extra permission allows
the implementation to restrict its analysis to the normal path. This is important since exception
handlers are dynamically bound and an analysis that shows that an operation is dead along its
exceptional path is generally intractable, while one that shows that the operation is dead along its
normal path may require only local analysis.

While the example is contrived, the situation that it presents appears fairly frequently as the
result of other transformations during code generation and optimization. For example, unrolling

---

[4]See the definitions of *exceptional* and *normal* paths below.

a loop may well leave dead code in the final iteration, e.g., the code intended to initialize the next iteration. Value propagation and common subexpression elimination also serve to create dead variables and dead code to manipulate them.

The language of [11.6(5)] does not ensure that the obviously intended meanings of some realistic examples will be preserved. For example, in AI-315, Robert Dewar presents the following example:

```
function Add_overflows(A, B: Integer) return Boolean is
  T: Integer
begin
  T := A + B;
  return False;
exception
  when Constraint_Error => return True;
end Add_Overflows;
```

The writer of code like this might hope to detect a potential overflow situation and, perhaps, use the knowledge to invoke an alternate more robust computation, however, it appears that the permissions of [11.5] would allow the constraint_error to be ignored, rendering the assignment dead and allowing its elimination permitting the function to always return False. This could cascade, if for example, the function were to be in lined, eliminating the code for the alternate computation which would also appear dead.

Note that both Dewar's example and the example of [11.6(5.e)] have the same intent, the detection of overflow. They differ in minor details with respect to the way the overflow is detected. It is probably unreasonable to expect a casual (or even experienced) user of the language to detect the subtleties. Indeed, the casual observer ought to come to the conclusion that the example of [11.6(5.e)] cannot work because the implementation result (as opposed to the mathematically correct result) of X * Y cannot possibly be larger than Integer'Last so that the first Put_Line cannot appear. This would lead the user towards an example similar to Dewar's which apparently will not work. It is not clear that there is any easy fix. The approach offered with respect to code motion in [11.6(6)], a compromise that allows local code motion with local analysis, but does not insist on global analysis to ensure that the permitted code motion does not disrupt the canonical semantics might also apply here. This would require that analysis proceed along both the normal and exceptional paths following from an operation if there were an exception handler for the exception potentially raised by the operation associated with the innermost sequence of statements containing the operation.

The examples given in (5.e) and (5.g) raise more subtle points. In the absence of [11.6(5)], Ada's exception model is similar to that of Gypsy. If we use a Gypsy-like model to specify the Ada operations, we get a possibility of two execution paths from each operation [6]. We will call these paths the *normal* and *exceptional* paths. If none of the language-defined checks fail during the performance of the operation, execution proceeds along the normal path. If performance of the operation causes a language-defined check to fail, execution proceeds along the exceptional path. Associated with each operation is an entry specification which is assumed[5] to be true when the operation is invoked. Associated with each exit path is an exit specification which is guaranteed to hold if the path is followed.

For example, the implementation of the integer multiplication operation on a given machine might be specified as follows:

```
function Machine_Mul(X, Y : Machine_Integer)
          return Machine_Integer
  entry
```

---

[5] "Assumed" is with respect to the operator definition. The implementation is required to "prove" that the assumption holds every time the operation is invoked. In the case of operations such as Machine_Mul and Machine_CMP all possible bit patterns represent valid values of Machine_Integer and the entry condition is trivially satisfied.

```
  X, Y in (Machine_Integer'First .. Machine_Integer'Last);
normal exit
  Machine_Mul(X, Y) = Integer_Mul(X, Y) and
  Machine_Mul(X, Y) in
    (Machine_Integer'First .. Machine_Integer'Last);
exceptional exit
  Machine_Mul(X, Y) != Integer_Mul(X, Y) and
  Machine_Mul(X, Y) in
    (Machine_Integer'First .. Machine_Integer'Last) and
  Integer_Mul(X, Y) not in
    (Machine_Integer'First .. Machine_Integer'Last);
```

This says that for some (possibly empty) set of input values, machine multiplication is equivalent to abstract integer multiplication and that execution will proceed along the normal path when this is the case. When machine and integer multiplication do not produce the same result, we are told that the true result is not representable as a **Machine_Integer** but that some result[6] representable as a machine integer is produced.[7] Now, if we look at a possible specification for the comparison operator, $>$, we see a potential problem with the language of the note.

```
function Machine_CMP(X, Y : Machine_Integer)
          return Machine_CC
  entry
    X, Y in (Machine_Integer'First .. Machine_Integer'Last);
  normal exit
    Machine_CMP(X, Y) = GT implies Integer_GT(X, Y) and
    ... -- Specifications for other return values
  exceptional exit
    false;
```

In this case, we assume a comparison instruction at the machine level that sets some condition codes to indicate the results of the comparison. GT is a condition code value that indicates the first operand, interpreted as an abstract integer, was greater than the second operand, also interpreted as an abstract integer. Note that the only entry condition assumes that the inputs are machine integers. This condition is satisfied by the exit condition of the multiply operation under either its normal or exceptional execution. Note also that this operation is defined to always exit normally.

We note that, in program verification, an operational semantics that allows exceptions to be raised when a language-defined check fails is, in a sense a dual of an operational semantics that produces an *undefined* result under the same circumstances. In the absence of a way to effect a meaningful recovery from failed checks,[8] we must show that the exceptional path is not taken. The proofs involved are exactly those that are required to show that operations do not produce *undefined* results. Languages such as Euclid and Verdi (and C for that matter) use an *undefined* semantics while Ada (in the absence of [11.6]) and Gypsy use an exception-based semantics.

For formal reasoning, the differences are largely matters of style. From an implementation standpoint, unless it can be shown that a given program will not have effects based on *undefined* results, the choice is between being able to detect a departure from normal execution and not. [11.6(5)] requires that exceptions not be suppressed if suppressing them would lead to a visible

---

[6] For most machines, we could specify exactly what this result is, i.e., how to compute it as a function of **X** and **Y**. It is not *undefined* in the sense that we know nothing about it.

[7] The first conjunct is redundant since it could be deduced from the other two.

[8] By a meaningful recovery, we mean undoing or overcoming the failed operation in such a way that computation can resume execution along the normal path, satisfying all the implicit and explicit assumptions of that path. In practice, this is extremely difficult unless the specification of the normal computation is extremely weak.

effect due to the subsequent use of an *undefined* result. We will examine the process of substituting operator definitions that produce "undefined" results for those that raise exceptions.

The stated assumptions associated with the example of [11.6(5.e)] are not sufficiently strong. In most machines, the result of an integer operation that fails an Ada implementation-defined check will be a valid value of the base type of the operation's result and, in many cases, it will be a valid value of the appropriate subtype as well. Thus, the values supplied to the comparison operation will always be "in–range integer value"s. The *value* is not the issue. If we allow the operation to omit its exception check, we must consider the result to be more than a value for the purposes of analysis. In the abstract, the result of an operation that yields an undefined result must be seen as a object having two attributes, **'value** and **'defined**. **'value** is of the base type of the result of the operation while **'defined** is boolean.

Under this view, multiply and compare might be defined as follows:

```
function Machine_Mul(X, Y : Machine_Integer)
           return Machine_Integer
```
  **entry**
  X**'value**, Y**'value**
    **in (Machine_Integer'First .. Machine_Integer'Last) and**
  X**'defined and** Y**'defined;**
  **exit**
    **if** Machine_MUL**'defined then**
      Machine_Mul**'value(X, Y) =** Integer_Mul(X, Y) **and**
      Machine_Mul**'value(X, Y) in**
        **(Machine_Integer'First .. Machine_Integer'Last) and**
    **else**
      Machine_Mul**'value(X, Y) !=** Integer_Mul(X, Y) **and**
      Machine_Mul**'value(X, Y) in**
        **(Machine_Integer'First .. Machine_Integer'Last) and**
      Integer_Mul(X, Y) **not in**
        **(Machine_Integer'First .. Machine_Integer'Last);**
    **end if**

```
function Machine_CMP(X, Y : Machine_Integer)
           return Machine_CC
```
  **entry**
    X, Y **in (Machine_Integer'First .. Machine_Integer'Last) and**
    X**'defined and** Y**'defined;**
  **exit**
     Machine_CMP**'defined(X, Y) and**
    **(**Machine_CMP**'value(X, Y) = GT implies** Integer_GT(X, Y) **and**
    ... -- Specifications for other return values)

Under this view of operational semantics, the obligation to take appropriate action in the case of exceptional operations has shifted from the operation making the check to the operation using the result. The substitution of "undefined" semantics for "exception" semantics might be done as follows:

1. Tentatively replace an operation using "exception" semantics with the equivalent operation using "undefined" semantics. Note that this substitution is dependent on being able to prove the stronger **entry** specification of the latter.[9]

---

[9] In the implementation of a language using the "undefined" semantics, we note that there is, in general, no way to determine by inspection that a given bit string represents an "undefined" value. A two's complement machine

2. If it is possible to prove that the **'defined** attribute of the operation's result is always **true** then the substitution is permitted (see the ramification [11.6(5.a)]) and no further analysis is required.

3. Locate all uses of the result of the replaced operation. If there are none, the substitution is permitted. If there are any, substitute the corresponding "undefined" semantics operation, if necessary, and check the entry specification for references to the **'defined** attribute of the result in question. If any using operation assumes that the **'defined** attribute of the result is **true**, the substitution cannot be made.

If the substitution can be made, the net effect is to remove from further consideration the execution path arising from the exception exit of the replaced operator definition. This, in turn, should enable additional program transformations, including removal of the replaced operation since it is known to be without an externally visible effect. The removal of the exception path may permit additional removals since dependencies along the path no longer require consideration. Removal of the operation may permit additional operations to be removed since its inputs are now referenced at fewer places.

Note that this is an analytical approach, not an implementation. Typically, there is no practical way to tag values with an indication that they represent an "undefined" result. When this is the case there is no way for subsequent operations in an implementation to check explicitly for the undefined property. In addition, the amount of analysis required to detect all uses of a result may require extensive reasoning about the values of index expressions, etc., when the values are components of arrays or other composite structures.

Implicit in the assumption of the last paragraph of [11.6(5.e)] appears to be an additional assumption that the values being compared are also the mathematically correct results of the operations that produced them, i.e., that they are not undefined.

It is probably the case that the only permission actually granted by [11.6(5)] is the removal of code that is "dead" along its normal exit path regardless of any effects along its exceptional exit path.

### 5.2.1.3   Bounded errors and erroneous executions

The Ada 9X revision has made a serious attempt to reduce the number and types of circumstances under which a program's execution can become erroneous. Since an erroneous execution can exhibit arbitrary behavior, this change is highly desirable. Recognizing that most implementations do reasonable things in the face of program errors that violate language semantics, the notion of a bounded error has been introduced. The bounded errors associated with invalid representations are discussed in [13.9.1]

*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 read 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:

- If the representation of the object represents a value of the object's type, the value of the type is used.

---

addition, for example, operating on two n bit long bit strings interpreted as integers produces an n bit long bit string that can be interpreted as an integer congruent to the mathematically correct integer result modulo $2^n$. Because of this, the entry specifications cannot be executed but must be reasoned about.

- 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. 11

*Erroneous Execution*

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. 12

> **Ramification:** In a typical implementation, every bit pattern that fits in an object of an integer subtype will represent a value of the type, if not of the subtype. However, for an enumeration or floating point type, 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. 12.a

> If a stand-alone scalar object is initialized to a an [**sic**] in-range value, then the implementation can take advantage of the fact that any out-of-range value has to be abnormal. Such an out-of-range value can be produced only by things like unchecked conversion, input, and disruption of an assignment due to abort or to failure of a language-defined check. 12.b

> This depends on out-of-range values being checked before assignment (that is, checks are not optimized away unless they are proven redundant).

The language of the **Ramification** sounds reasonable, but it flies in the face of the conventions used in many of the logics used to reason about program behavior. Typically, *undefined* is a loaded term in these logics. *Undefined* is used to represent a distinguished value about which nothing can be proven. Thus $\nvdash undefined = undefined$. This is too strong for implementation semantics in most cases. In any implementation in which evaluating $x$ is free of side effects that could change its value, $x = x$ is **true** even if x has an invalid representation or is *undefined* so long as the implementation of $=$ simply involves comparing bit patterns. In the absence of a requirement to actually evaluate $x$, it should be unconditionally ok to substitute **true** for the equality.

On the other hand, this language seems to have the potential for conflicts with semantics of "undefined" results discussed above in connection with [11.6(5)]. The relationship between undefined as used in [13.9.1] and [11.6(5)] should be further clarified.

## 5.2.2  [11.6(7)]

This paragraph allows fairly arbitrary reordering of actions within the scope of an exception handler by reducing the expectations that the programmer may have concerning the state of the computation at the time that the handler is entered. This is essentially the "Undefined" execution order of [9, section 2.6.5]. We note that the only effective actions that a programmer can take when an exception handler is entered in the face of this kind of reordering is to assign normal values to all variables that might have become abnormal due to operations disrupted by the exception.

The first sentence of this paragraph is complex and convoluted and calls out to be simplified or clarified. The following discussion may aid in finding more suitable language. An exception_handler is optionally associated with a handled_sequence_of_statements which contains a sequence_of_statements

and is, among other things, the operational portion of a `task_body`. When an exception is raised, it will either be handled or cause the containing `task_body` to terminate. In either case, all that the user can expect to know is that the exception was raised somewhere in the code of the `sequence_of_statements` component of the `handled_sequence_of_statements` that contains the `exception_handler` just entered or that constitutes the operational part of the task being terminated. The reordering that can be done is limited in two respects.

1. The operation that raises the exception due to a failed language–defined check cannot have been moved into the code of an independent subprogram, and

2. The operation that raises the exception due to a failed language–defined check cannot have been moved into the code of some abort-deferred operation.

Just breaking up the sentence may help. Instead of

- 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 need reflect only that the exception was 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.  6

perhaps language similar to the following would be more understandable.

- 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 containing task, if no handler is present), the external interactions that have occurred need reflect only that the exception was raised somewhere within the execution of the `sequence_of_statements` associated with the handler (or the `task_body`). It may appear that the exception was raised earlier than defined by the canonical semantics (or later if the interactions are independent of the result of the checked operation). It may not appear as if the exception were raised within the execution of some abort-deferred operation or within the execution of an *independent* subprogram that does not dynamically enclose the execution of the construct whose check failed.  6

## 5.3 Living with the "Canonical Semantics"

The canonical semantics define a potentially very large family of valid executions. This is due to the numerous places in which the language definition allows operations to be performed in an arbitrary order. An implementation is free to select any order under these circumstances. In the absence of order dependencies and tasking considerations, all canonical executions should produce the same externally visible effect. Order-dependent side effects, including exceptions raised due to the failure of language-defined checks, can affect the effect of the program. The problem is twofold:

1. Reducing the potential effect space of the program, and

2. Determining which execution the implementation has selected.

First of all, it is worth noting that this kind of problem is not unique to Ada (both Ada 83 and Ada 9X). Most programming languages, including C and C++, admit similar behaviors, either implicitly or explicitly. Ada is more explicit about them. In general, the failure of languages to define or enforce restrictive canonical executions is attributed to a need for flexibility in order to achieve run-time efficiency. There is tension between this need and the requirements for predictable

program behavior, which are imposed by small segments of the user community, typically those users associated with safety and security critical applications. Predictable behavior is usually defined as having a rigorous semantic definition that allows the formal verification of programs written in the language, preferably using mechanical aids.

In theory, one could reason about Ada programs by enumerating the set of possible executions and reasoning individually about each one. A program could then be said to shown to exhibit a given property if each of its possible executions could be shown to exhibit the property. In practice, the combinatorics of potential execution choices are likely to render this approach infeasible for any non-trivial program. If we assume that a compiler conforming to the language standard produces code that follows one of the set of canonical executions of a given program, it seems a waste of time to prove properties of the set as a whole unless there is a need to guarantee the behavior of the program under all possible conforming implementations. This is seldom the case. Further complications arise when it is possible to show that some, but not all, members of the canonical execution set exhibit the desired property. In this case, it is essential to determine whether the implementation being considered exhibits the property.

There are several possibilities. The first is to attempt to reduce the size of the set of canonical executions to a tractable size and possibly to a single member. The second is to discover the member of the canonical execution set that has been chosen by a particular implementation and to reason about that execution alone.

### 5.3.1 Restricting the execution set size

The size of the canonical execution set about which one must reason can be reduced by one of two methods; reducing the choices available to the implementation or finding equivalence classes within the set, or by some combination of the two. Ada 9X provides some means for imposing order. For example, the order of the association of operands with a sequence of operators of the same precedence can be controlled by the explicit use of parentheses. The introduction of explicit intermediate variables and assignments should have a similar effect. For example, suppose that side effects exist such that the value resulting from the evaluation of `<exp1>` depends on whether it is evaluated before or after `<exp2>`, but that there are no other order dependencies between the expressions. Further assume that the evaluations produce results of some integer subtype.

```
A := <exp1> + <exp2>;
```

Either of the possible results is a member of the canonical execution set for this fragment. If we want to ensure that `<exp1>` is evaluated first, we might write:

```
A1 := <exp1>;
A2 := <exp2>;
A := A1 + A2;
```

It is not clear that the additional freedoms to reorder operations granted by [11.6(6)] allow an implementation to ignore structuring of this kind, but aggressive optimizations in compilers for other languages are known to do so in some cases. Presumably, the dependency between the two expressions either becomes explicit or the implementation will be forced to recognize that it cannot assume independence because the expressions invoke separately compiled routines and it will be forced to produce the intended result[10].

Note that the explicitly ordered code may still exhibit a family of canonical executions. In the expression `A1 + A2`, the language allows `A1` or `A2` to be "evaluated" first. We claim that given

---

[10] If the expressions are sufficiently complex and the dependencies between them limited, it may be possible to interleave their evaluations. This would be permitted under the general freedoms noted in [11.6(3)]

appropriate type declarations (and barring some pathological implementation of +) that both orders will be equivalent and trivial.

By a combination of these two techniques, forcing orders where order makes a difference and creating situations where it is easy to show that, at least locally, all canonical executions are equivalent, it should be possible to reduce the number of canonical executions associated with a program to a tractable number. In most cases, the analysis of the remaining canonical executions should show that language-defined checks will not fail, rendering moot the freedoms of [11.6]. The utility of this approach depends on the implementation or implementations of interest ensuring that the canonical semantics are honored.

If the notion of a subset of Ada 9X for High Integrity systems, as recently proposed by Brian Wichmann, is accepted, the subset definition could restrict the ordering freedoms permitted by the primary language definition. This approach would necessitate subset compilers to enforce the restrictions, but would offer a higher degree of assurance than the use of general purpose compilers. If a subset is adopted with the notion of supporting mechanical verification, it is not unreasonable to expect that integrated environments will be developed in which both the verification and implementation tools are based on the same semantic assumptions.

### 5.3.2 Discovering the execution

Another approach to the problem of a canonical execution set is the determination of the actual execution produced for a given program by a given implementation. This requires that the compiler output its object code in a form that allows the user to determine the actual execution that will occur when the program is executed. Implementations conforming to the Safety and Security Annex, in particular to section [H.3], will provide this kind of information. With an appropriate transformation of the object code back into an appropriate Ada or Ada-like source form, it should be possible to perform source level analysis or verification on the program while maintaining confidence that the results are, in fact, applicable to the compiled program.

It is clear that this approach requires facilities that are not present in many, if not all, existing compilers, but the Annex should encourage development of this facility.

## 5.4 Observations on the Reference Manual

In the course of using the Reference Manual in the preparation of this chapter, a number of general shortcomings have been observed. These have more to do with presentation than with substance and can be fixed prior to the release of the final document.

First of all, we wish to compliment the Mapping/Revision Team on the content and style of the manual. Not only is the wording a substantial improvement over the Ada 83 Reference Manual, but the inclusions of the annotations provide useful and substantive insight into the workings of the language. It is to be hoped that the annotated version will be maintained along with its "official" subcomponents and that it will see widespread use by serious students of Ada 9X.

This said, there are ways in which the the Reference Manual could be further improved.

1. The index is not sufficiently comprehensive. On a number of occasions, an attempt to trace the consequences of a definition found that the defining occurrence was the only reference in the index. Fortunately, the source files are available and can be searched as necessary; however, any term important enough to be marked as a definition is important enough to have the consequences of that definition tracked. A presentation similar to that used in the index for syntactic constructs should be adapted for defined terms, i.e., a defining reference followed by using references.

2. The index does not appear to cover the annotations. Extending it to this level would greatly aid in the use of the annotated manual.

3. The Syntax Cross-Reference would be much more useful if references for the defining occurrence as well as the using occurrences were given. For example, we find from the cross-reference that a `task_body` is used in the definition of a `proper_body` in [3.11], but we must go to the main index to discover that a `task_body` is defined in [9.1(6)]. Extending the indexing to the numbered paragraph level as is done in the index would also be useful.

4. The marginal paragraph numbering is incomplete and inconsistent. For example, the paragraphs following the example codes of [11.6(5.e)] and [11.6(5.g)] are not numbered while similar paragraphs elsewhere, e.g., [8.3(29.o)] are. There is a similar problem in [13.9.1(12.b)] as well. This is probably the result of the mechanical approach taken to inserting the annotating scribe commands. In preparing the LaTeX source for the Annotated version of the Ada 83 reference manual, I found it necessary to insert this material manually.

5. In some cases, precision seems to have been sacrificed for readability. This occurs when it is difficult to determine the antecedents for pronouns or where the same noun appears in an ambiguous context. An example is [4.5(11)] discussed in Section 5.2.1.1 on page 94 above. More liberal use of the @Redundant (or a similar) construct might alleviate this problem in the annotated version.

# Chapter 6

# Conclusions

We did not expect to formulate a complete semantic definition (even for the sequential part of Ada) in this project; there were simply not enough resources to do so. What we did expect was to gain some insights into the structure of the language, and to identify some problems either with the description in the Reference Manual or in the design of the language itself, and to contribute to the development of Ada 9X by suggesting improvements to the description or design. Those expectations were met to some degree; for example, we identified some flaws (that have now been fixed) in the design in the area of per-object constraints; we identified some conceptual and some wording problems in the area of floating point and developed a model that was used in the development of new wording for the Reference Manual; and we identified some incompleteness in the description of actual subtypes.

However, we did not make as much progress in the natural semantics definition as we had originally hoped. It was more difficult to understand the supposedly trivial parts of the language than we had imagined. Large-scale languages like Ada do not have neat, independent parts; rather, each feature is affected in some measure by the others. For example, the type system is affected by the concurrency mechanism (e.g., task types), by the packaging mechanism (e.g., private types), and in several ways by the object-oriented features (e.g., access discriminants, per-object expressions, class-wide types). So, indeed, there are no really trivial aspects of the language. In the original LPT project, we had felt that it would be a waste of effort to develop a formal model for things that "everyone understands". Our recent efforts, however, have shown us that there are interesting problems lurking at the fringes of even these areas.

Even though there are serious gaps in the definition, a considerable amount of groundwork has been done. We have identified most of the basic semantic domains that must be used in a full definition, we developed structuring mechanisms for the definition that allow us to describe many of the implementation freedoms, and we have several tools (such as the type checker for the Prolog representation of the definition, and the tool that derives LaTeX source from the Prolog representation) that help in the production and documentation of the definition. So, we feel that we have made a good start in the direction of a complete description of the sequential part of the language.

We are not sure how easily our framework could be adapted to deal with concurrency. The influence of tasking in DDC's formal definition of Ada 83 [1] is pervasive, and we suspect that incorporating concurrency into our definition would similarly affect every part of the model.

## 6.1  Implementation Freedoms

One impediment to writing a formal definition like ours is the high degree of underspecification in the Reference Manual. This allows implementations considerable freedom to choose orders of actions, accuracy of results, base ranges of types, and so on. These freedoms can be difficult to

model; where an implementation need only produce one acceptable result, our semantics tries to describe *all* acceptable results.

Modeling these freedoms sometimes forces our formal model to differ in significant ways from an implementation (and to use representations that no implementation is likely to use). For a simple example, consider the following rule about access-to-subprogram values:

> 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.

In order to model this, we are forced to use a representation of access-to-subprogram values that consists of both a reference to the designated subprogram and an "instance" value that tells which evaluation of an Access attribute gave the access value. Each evaluation of an Access attribute increments this instance value, so that we can determine whether two access values derive from the same evaluation or not. Our definition of the equality function checks both the subprogram reference and the instance number, and can give a result of equal, unequal, or unknown. Such a representation is unlikely to be used in any implementation of Ada 9X.

An implementor of the language need not be concerned with all these freedoms; just one particular implementation choice needs to be made and the existence of other possible choices is irrelevant. A programmer does not necessarily need to be concerned about all the alternative orders; it is usually possible to write programs in such a way that the specific choice made by an implementation does not matter (for example, by avoiding side effects in functions, restricting the statements in a `package_body` to affect only variables local to the package, and so on). On the other hand, anyone trying to read an Ada program may indeed be concerned about the different possible outcomes of an execution (especially if the writer has not been careful to avoid situations where the different orders matter). So, our model, while unnatural if compared to an implementation, is quite natural as a description of the complexities that careful readers must deal with.

## 6.2   Notation and Tools

The natural semantics framework seems to have worked fairly well, although there were a few awkward aspects to our formalization of the language semantics. In particular, our need to introduce explicit sequencing and arbitrary-order combinations of actions (in two slightly different variations) seems somewhat artificial. However, this mechanism of actions allows us to present reasonably concise descriptions of many language features.

The use of Prolog to make the definition executable (and type-checkable) was a great help. We have been able to execute parts of the definition to confirm that it expresses what we intended. The type checker was able to find a number of trivial errors in our semantics. There is some price to be paid, hovever; it is sometimes inconvenient to express a rule in a manner acceptable to Prolog. This is particularly evident in the descriptions of the various semantic domains and the primitive functions acting over those domains. Prolog does not support defined functions (instead, relations must be used). We used a program to convert the Prolog code into the LaTeX source used for this report. This program is able to introduce functional notation in places where we have instructed it to, so at least our published form of the rules can use a more expressive notation than Prolog. But this is still rather unsatisfactory. It is possible that other tools might be able to provide better mechanical support.

## 6.3  Bounded Errors

A number of rules and concepts were added to Ada 83 in order to make programs more predictable. For example, many situations leading to erroneous executions in Ada 83 have been made into *bounded errors*. For these errors, a range of possible outcomes is described. This seems like a beneficial change. However, there is a price to be paid for this benefit: the model for a feature using bounded errors can be substantially more complex than a model using erroneous executions. For example, in order to change the evaluation of an uninitialized scalar variable from erroneous to a bounded error, it was necessary to introduce the notion of "invalid representations" of scalar objects. The addition of this notion has an influence on a number of other areas of the language (e.g., relational operators, membership tests, and type conversions). So, the formal model is more complex, which means that *formal* predictions about programs are harder to derive. On the other hand, the execution of programs is more predictable in the sense that these executions are more constrained (the old rules allowed any behavior, whereas the new rules are more specific).

## 6.4  Structure of Models

It does not seem possible, using our methods, to formulate a model for Ada 9X that is simultaneously concise, comprehensible, broad, and accurate. Accounting for all the special cases of features adds so much detail to the model that it becomes unusable.

Textbook writers face a similar dilemma; if too much detail is presented, readers will find the text impenetrable. Therefore, authors present simplified descriptions of parts of the language. These simplified descriptions, even when they lead the reader to draw incorrect conclusions about the behavior of some programs, are nevertheless useful to readers who are first learning the language. In a later part of a book, an author may elaborate on some of these missing details, and may need to contradict some of his earlier oversimplified assertions.

We do not know exactly how to make layered formal models using a similar structure. In most formal notations, it is not possible to override an earlier assertion with a more detailed assertion. Even if this were allowed, it is unclear how a user of such a layered formal model would know when the simpler part of model was applicable.

In the model developed in this report, we have tried to approach this ideal of structured models in a very modest way through our use of the "unpredicted" outcomes to simplify the formal model; we can certainly imagine a more complex version of this model that would, in fact, make predictions where this simpler model refuses to. However, we have not had the resources to develop the more complex model.

# Bibliography

[1] *The Draft Formal Definition of Ada.* Denmark, 1987.

[2] David Guaspari. Formal methods in the design of Ada 9X. In *Proceedings of the Ninth Annual Conference on Computer Assurance*, 1994.

[3] Intermetrics, Inc. *Annotated Ada 9X Reference Manual, Version 4.0*, September 1993.

[4] Intermetrics, Inc. *Annotated Ada 9X Reference Manual, Version 5.0*, June 1994.

[5] G. Kahn. Natural semantics. In *Fourth Annual Symposium of Theoretical Aspects of Computer Science*, pages 22–39, 1987. LNCS 247.

[6] John McHugh. *Towards Efficient Code from Verified Programs.* PhD thesis, The University of Texas at Austin, 1983.

[7] U.S. Reddy and T.K. Lakshman. Typed Prolog: A Semantic Reconstruction of the Mycroft-O'Keefe Type System. Submitted to the '91 Intl. Logic Programming Symp., San Deigo, California, February 1991.

[8] J. M. Spivey. *The Z Notation: A Reference Manual.* Prentice Hall, 1992.

[9] Language Precision Team. Formal studies of Ada 9X, final report. Technical report, Odyssey Research Associates, December 1992.

[10] United States Department of Defense, New York. *Reference Manual for the Ada Programming Language*, February 1983. ANSI/MIL-STD-1815A-1983.

# Appendix A

# Official comments submitted

This appendix lists the official comments submitted by the LPT. For each comment, we give its official "key" number, its title, and a short description of the comment or its effect on the Standard.

Comment 93-3209.a: *Too much extra permission to remove checks.* The conceptual framework of section 11.6 has been changed.

Comment 93-3398.a: *per-object constraints and the "current instance".* A new rule [3.8(13)] has been added to avoid the problem described.

Comment 93-3511.a: *What is the base range of an enumeration type?.*

Comment 93.3547.a: *constants that aren't.* The problem described has been identified as an erroneous execution in [13.9.1(13)]

Comment 93-3547.b: *subcomponents that are constrained by their initial value.* A new legality rule [3.6(11)] was added.

Comment 93-3547.c: *conversion to a type with aliased components.* A new legality rule [3.6(11)] was added.

Comment 93-3574.a: *interleaving evaluation and conversion.* Several paragraphs have been modified to clarify the rules.

Comment 93-03574.b: *reassociation of sequences of predefined operators.* A note [4.5(13.b)] has been added to the Annotated Reference Manual. It is unclear, however, that the note clarifies the issue raised in this comment.

Comment 93-3575.a: *aliased subcomponents with per-object constraints.* A new legality rule [3.6(11)] was added.

Comment 94-3621.a: *Initialize a discriminant before any subcomponents that depend on it.* This clause has been added to the rules of [3.3.1(20)].

Comment 94-3760.a: *Phraseology.* An inaccurate statement has been reworded in [M(1)].

Comment 94-3761.a: *Phraseology.* Some wording in [3.3] has been improved.

Comment 94-3762.a: *Phraseology.*

Comment 94-3763.a: *Phraseology.* The wording of [3.2.3] has been clarified.

Comment 94-3764.a: *Phraseology.* A clarifying cross-reference was added.

Comment 94-3765.a: *Phraseology.*

Comment 94-3901.a: *Are first subtypes of enumeration types constrained?.* A clause has been added to [3.5.1(10)] to answer this question.

Comment 94-3901.b: *First subtypes of discriminated types are unconstrained.* This clause has been added to [3.7(26)].

Comment 94.3901.c: *First subtypes of incomplete types.* A new note in the [3.10.1(10.a)] Annotated Reference Manual argues that this issue is unimportant.

Comment 94.3901.d: *Predefined operators and invalid scalar components.* The entire discussion of "invalid" scalars has been modified in version 5.0 of the Reference Manual. This comment and

the following two are cited in the changes.

Comment 94-4045.a: *Model for valid and invalid values.* See above.

Comment 94-4054.a: *Model for valid and invalid values.* See above.

Comment 94-4064.a: *What is the actual subtype of a formal object?.* The question has been answered in [6.4.1(15)].

Comment 94-4065.a: *Normalizing composite objects.* An explicit statement about restoring objects to normal state appears in [13.9.1(7)].

Comment 94-4149.a: *Incomplete definition of 'expected profile' and 'corresponding parameter'.* Some rules have been clarified

Comment 94-4171.a: *Actual subtypes and aliased views.* The rules in [3.10(9)] have been reworded.

The remaining comments were sent too late to affect version 5.0 of the Reference Manual. Some of them are addressed in the electronically-distributed version 5.3, as noted below. Furthermore, the floating-point annex is under revision to address some of the comments on the floating-point model.

Comment 94-4448.a: *Signed zeroes not permitted as floating point values.*

Comment 94-4454.a: *Model-oriented floating point attributes.*

Comment 94-4455.a: *Relation between requested precision and model numbers.*

Comment 94-4481.a: *Inappropriate references to Annex G.*

Comment 94-4482.a: *Are S'Model, S'Machine deterministic?.*

Comment 94-4486.a: *Symmetry of floating point types.*

Comment 94-4489.a: *Derivation from a floating point type.*

Comment 94-4535.a: *Derived types with new discriminants are extensions.* A sentence has been added.

Comment 94-4535.b: *Discriminants used in constraints in derived type definitions.*

Comment 94-4535.c: *Incorrect rules for uses of new discriminants in constraint on parent.* A new rule has been added.

Comment 94-4535.d: *Current instance of a derived type.* A note has been added in a "to be honest" section of the AARM.

Comment 94-4572.a: *An object that is not {a part of} a formal parameter.*

Comment 94-4572.b: *For aliasing, the type of the formal, not the part, matters.*

Comment 94-4572.c: *When does an access path exist?.*

Comment 94-4587.a: *Incompatibility between semantics of the core and annex G?.*

Comment 94-4796.a: *reading a composite with an uninitialized scalar component.* The wording of this rule has been changed.

# Appendix B

# Intermediate Syntax

This appendix describes the decorated abstract syntax representation of Ada 9X programs. This representation includes all static semantic information needed for defining the dynamic semantics.

One approach, not taken here, is to define a representation of semantic information such as types, subtypes, and overload information and defining necessary tree attributes. Instead of using semantic attributes we chose to give a purely syntactic representation of necessary information by introducing new kinds of tree nodes and new synthetic names.

For instance, the results of overload resolution are captured by the introduction of new unique names and suitable renaming of overloaded entities and their use. Crucial type information is represented using existing syntax for qualified expressions. Thus the result of static semantic analysis is a normalized abstract syntax tree. The details of this normalization are described below.

Declarations that introduce multiple names are replaced by static analysis with multiple declarations introducing single names where this is legal.

Constructs for which no abstract syntax is provided are either not treated in this definition (e.g., tasking) or have not significance for the dynamic semantics (e.g., generics).

## B.1 Syntactic Domains

The following is a complete listing of the term algebra used to represent abstract syntax trees. The constructors are grouped by sorts and are arranged alphabetically.

### B.1.1 Component Associations ($Aca$)

$$\text{array\_comp\$assoc}: \quad Dch^*, Exp \rightarrow Aca$$

### B.1.2 Aggregates ($Agg$)

$$
\begin{array}{ll}
\text{ext\$agg}: & Exp, Rca^* \rightarrow Agg \\
\text{named\_array\$agg}: & Aca^* \rightarrow Agg \\
\text{null\_ext\$agg}: & Exp \rightarrow Agg \\
\text{null\_record\$agg}: & \rightarrow Agg \\
\text{other\_array\$agg}: & Exp^*, Exp \rightarrow Agg \\
\text{pos\_array\$agg}: & Exp^* \rightarrow Agg \\
\text{record\$agg}: & Rca^* \rightarrow Agg
\end{array}
$$

### B.1.3 Case Alternatives ($Alt$)

$$Alt\$lst : \quad list(Alt) \rightarrow Alt$$
$$case\$Alt : \quad Dch^*, Stm \rightarrow Alt$$

### B.1.4 Choice Lists ($Ccl$)

$$list\$choice : \quad id^* \rightarrow Ccl$$
$$others\$choice : \quad \rightarrow Ccl$$

### B.1.5 Context Items ($Cit$)

$$with\$context : \quad Nam^* \rightarrow Cit$$

### B.1.6 Component Declarations ($Cmp$)

$$aliased\_comp\$decl : \quad Id, Sid \rightarrow Cmp$$
$$comp\$decl : \quad Id, Sid \rightarrow Cmp$$
$$init\_aliased\_comp\$decl : \quad Id, Sid, Exp \rightarrow Cmp$$
$$init\_comp\$decl : \quad Id, Sid, Exp \rightarrow Cmp$$

### B.1.7 Compilation Units ($Cmp$)

$$lib\$unit : \quad Cit^*, Dcl \rightarrow cmu$$
$$private\$unit : \quad Cit^*, Dcl \rightarrow cmu$$
$$sub\$unit : \quad Cit^*, Nam, Dcl \rightarrow cmu$$

### B.1.8 Conditions ($Cnd$)

$$Exp\$condition : \quad Exp \rightarrow Cnd$$

### B.1.9 Constraints ($Cns$)

$$constr\_delta\$constr : \quad Exp, Cns \rightarrow Cns$$
$$constr\_digits\$constr : \quad Exp, Cns \rightarrow Cns$$
$$delta\$constr : \quad Exp \rightarrow Cns$$
$$digits\$constr : \quad Exp \rightarrow Cns$$
$$discr\$constr : \quad Dca^* \rightarrow Cns$$
$$index\$constr : \quad Rng^* \rightarrow Cns$$
$$range\$constr : \quad Rng \rightarrow Cns$$

### B.1.10 Discriminant Associations ($Dca$)

$$named\$assoc : \quad Id, Exp \rightarrow Dca$$

### B.1.11 Discrete Choices ($Dch$)

$$discr\_other\$choice : \quad \rightarrow Dch$$
$$exp\$choice : \quad Exp \rightarrow Dch$$
$$range\$choice : \quad Rng \rightarrow Dch$$

## B.1.12 Declarations ($Dcl$)

$$
\begin{array}{ll}
\text{dcl\$lst :} & \text{list}(Dcl) \rightarrow Dcl \\
\text{a\_c\_i\_obj\$decl :} & Id,\ Sid,\ Exp \rightarrow Dcl \\
\text{a\_c\_obj\$decl :} & Id,\ Sid \rightarrow Dcl \\
\text{a\_i\_obj\$decl :} & Id,\ Sid,\ Exp \rightarrow Dcl \\
\text{a\_obj\$decl :} & Id,\ Sid \rightarrow Dcl \\
\text{c\_i\_obj\$decl :} & Id,\ Sid,\ Exp \rightarrow Dcl \\
\text{c\_obj\$decl :} & Id,\ Sid \rightarrow Dcl \\
\\
\text{real\_const\$decl :} & Id,\ Exp \rightarrow Dcl \\
\text{int\_const\$decl :} & Id,\ Exp \rightarrow Dcl \\
\text{d\_ext\$decl :} & Id,\ Dcp,\ Sid \rightarrow Dcl \\
\text{d\_i\_type\$decl :} & Id,\ Dcp \rightarrow Dcl \\
\\
\text{d\_type\$decl :} & Id,\ Dcp,\ Tdf \rightarrow Dcl \\
\text{exception\$renaming :} & Id,\ Nam \rightarrow Dcl \\
\text{excpt\$decl :} & Id \rightarrow Dcl \\
\text{ext\$decl :} & Id,\ Sid \rightarrow Dcl \\
\\
\text{i\_obj\$decl :} & Id,\ Sid,\ Exp \rightarrow Dcl \\
\text{i\_type\$decl :} & Id \rightarrow Dcl \\
\text{obj\$decl :} & Id,\ Sid \rightarrow Dcl \\
\text{object\$renaming :} & Id,\ Nam,\ Nam \rightarrow Dcl \\
\\
\text{s\_subp\$spec :} & Sps \rightarrow Dcl \\
\text{subp\$body :} & Sps,\ Dcl,\ Stm \rightarrow Dcl \\
\text{subp\$renaming :} & Sps,\ Nam \rightarrow Dcl \\
\text{subp\$spec :} & Sps \rightarrow Dcl \\
\text{subtype\$decl :} & Id,\ Sid \rightarrow Dcl \\
\text{type\$decl :} & Id,\ Tdf \rightarrow Dcl \\
\text{c\_type\$decl :} & Id,\ Tdf \rightarrow Dcl \\
\text{c\_d\_type\$decl :} & Id,\ Tdf,\ Dcp \rightarrow Dcl
\end{array}
$$

## B.1.13 Discriminant Parts ($Dcp$)

$$
\begin{array}{ll}
\text{box\$discr :} & \rightarrow Dcp \\
\text{list\$discr :} & Dcs^{*} \rightarrow Dcp
\end{array}
$$

## B.1.14 Discriminant Specifications ($Dcs$)

$$
\begin{array}{ll}
\text{acc\$discr :} & Id,\ Nam \rightarrow Dcs \\
\text{acc\_init\$discr :} & Id,\ Nam,\ Exp \rightarrow Dcs \\
\text{init\$discr :} & Id,\ Nam,\ Exp \rightarrow Dcs \\
\text{simple\$discr :} & Id,\ Nam \rightarrow Dcs
\end{array}
$$

## B.1.15 Exception Choices ($Ech$)

$$
\begin{array}{ll}
\text{named\$excpt :} & Nam \rightarrow Ech \\
\text{others\$excpt :} & \rightarrow Ech
\end{array}
$$

113

### B.1.16 Else-If Clauses (*Eif*)

$$
\begin{array}{ll}
\text{eif\$lst :} & \textit{Eif}^* \rightarrow \textit{Eif} \\
\text{elsif\$clause :} & \textit{Cnd, Stm} \rightarrow \textit{Eif}
\end{array}
$$

### B.1.17 Expressions (*Exp*)

$$
\begin{array}{ll}
\text{and\_then\$}\textit{Exp} : & \textit{Exp, Exp} \rightarrow \textit{Exp} \\
\text{exp\$alloc :} & \textit{Exp} \rightarrow \textit{Exp} \\
\text{in\_name\$exp :} & \textit{Exp, Nam} \rightarrow \textit{Exp} \\
\text{in\_range\$exp :} & \textit{Exp, Rng} \rightarrow \textit{Exp} \\
\text{in\_type\$exp :} & \textit{Exp, Nam} \rightarrow \textit{Exp} \\
\text{name\$exp :} & \textit{Nam} \rightarrow \textit{Exp} \\
\text{not\_in\_name\$exp :} & \textit{Exp, Nam} \rightarrow \textit{Exp} \\
\text{not\_in\_range\$exp :} & \textit{Exp, Rng} \rightarrow \textit{Exp} \\
\text{not\_in\_type\$exp :} & \textit{Exp, Nam} \rightarrow \textit{Exp} \\
\\
\text{null\$exp :} & \rightarrow \textit{Exp} \\
\text{integer\$exp :} & \text{integer} \rightarrow \textit{Exp} \\
\text{real\$exp :} & \text{real} \rightarrow \textit{Exp} \\
\text{char\$exp :} & \text{integer} \rightarrow \textit{Exp} \\
\text{or\_else\$exp :} & \textit{Exp, Exp} \rightarrow \textit{Exp} \\
\text{paren\$exp :} & \textit{Exp} \rightarrow \textit{Exp} \\
\text{qual\$aggregate :} & \textit{Nam, Agg} \rightarrow \textit{Exp} \\
\text{qual\$exp :} & \textit{Nam, Exp} \rightarrow \textit{Exp} \\
\text{type\$alloc :} & \textit{Sid} \rightarrow \textit{Exp} \\
\text{type\$conversion :} & \textit{Nam, Exp} \rightarrow \textit{Exp}
\end{array}
$$

### B.1.18 Modes (*Mde*)

$$
\begin{array}{ll}
\text{in\$mode :} & \rightarrow \textit{Mde} \\
\text{in\_out\$mode :} & \rightarrow \textit{Mde} \\
\text{no\$mode :} & \rightarrow \textit{Mde} \\
\text{out\$mode :} & \rightarrow \textit{Mde}
\end{array}
$$

### B.1.19 Names (*Nam*)

$$
\begin{array}{ll}
\text{access\$attr :} & \textit{Nam} \rightarrow \textit{Nam} \\
\text{delta\$attr :} & \textit{Nam} \rightarrow \textit{Nam} \\
\text{digits\$attr :} & \textit{Nam} \rightarrow \textit{Nam} \\
\text{deref\$name :} & \textit{Nam} \rightarrow \textit{Nam} \\
\text{direct\$name :} & \textit{Id} \rightarrow \textit{Nam} \\
\text{func\$call :} & \textit{Nam, Pss}^* \rightarrow \textit{Nam} \\
\textit{Id}\text{\$attr :} & \textit{Nam, Id} \rightarrow \textit{Nam} \\
\text{indexed\$comp :} & \textit{Nam, Exp}^* \rightarrow \textit{Nam} \\
\\
\text{name\_type\$conversion :} & \textit{Nam, Nam} \rightarrow \textit{Nam} \\
\text{param\$attr :} & \textit{Nam, Id, Exp} \rightarrow \textit{Nam} \\
\text{selected\$comp :} & \textit{Nam, Id} \rightarrow \textit{Nam} \\
\text{slice\$op :} & \textit{Nam, Rng} \rightarrow \textit{Nam}
\end{array}
$$

### B.1.20    Parameter Specifications ($Pms$)

$$
\begin{array}{ll}
\text{access\$param :} & Id,\, Nam \rightarrow Pms \\
\text{access\_default\$param :} & Id,\, Nam,\, Exp \rightarrow Pms \\
\text{default\$param :} & Id,\, Mde,\, Nam,\, Exp \rightarrow Pms \\
\text{normal\$param :} & Id,\, Mde,\, Nam \rightarrow Pms \\
\end{array}
$$

### B.1.21    Pragmas ($Prg$)

$$
\begin{array}{ll}
\text{param\$pragma :} & Id,\, Pss^{*} \rightarrow Prg \\
\text{simple\$pragma :} & Id \rightarrow Prg \\
\end{array}
$$

### B.1.22    Parameter Associations ($Pss$)

$$
\begin{array}{ll}
\text{named\_exp\$arg :} & Id,\, Exp \rightarrow Pss \\
\text{named\_name\$arg :} & Id,\, Nam \rightarrow Pss \\
\end{array}
$$

### B.1.23    Record Component Associations ($Rca$)

$$
\begin{array}{ll}
\text{choice\$assoc :} & Ccl,\, Exp \rightarrow Rca \\
\end{array}
$$

### B.1.24    Ranges ($Rng$)

$$
\begin{array}{ll}
\text{attr\$range :} & Nam \rightarrow Rng \\
\text{explicit\$range :} & Exp,\, Exp \rightarrow Rng \\
\text{parm\_attr\$range :} & Nam,\, Exp \rightarrow Rng \\
\end{array}
$$

### B.1.25    Subtype Indications ($Sid$)

$$
\begin{array}{ll}
\text{constrained\$subtype :} & Nam,\, Cns \rightarrow Sid \\
\text{named\$subtype :} & Nam \rightarrow Sid \\
\text{subtype\$range :} & Rng \rightarrow Sid \\
\end{array}
$$

### B.1.26    Subprogram Specifications ($Sps$)

$$
\begin{array}{ll}
\text{function\$spec :} & Id,\, Pms^{*},\, Nam \rightarrow Sps \\
\text{procedure\$spec :} & Id,\, Pms^{*} \rightarrow Sps \\
\end{array}
$$

### B.1.27    Statements ($Stm$)

$$
\begin{array}{ll}
\text{stm\$lst :} & \text{list}(Stm) \rightarrow Stm \\
\text{agg\_code\$stm :} & Nam,\, Agg \rightarrow Stm \\
\text{assign\$stm :} & Nam,\, Exp \rightarrow Stm \\
\text{call\$stm :} & Nam,\, Pss^{*} \rightarrow Stm \\
\text{case\$stm :} & Exp,\, Alt \rightarrow Stm \\
\text{cond\$exit :} & Cnd \rightarrow Stm \\
\text{declare\$block :} & Dcl,\, Stm \rightarrow Stm \\
\text{exp\_code\$stm :} & Nam,\, Exp \rightarrow Stm \\
\text{for\$loop :} & Id,\, Rng,\, Stm \rightarrow Stm \\
\text{func\_return\$stm :} & Exp \rightarrow Stm \\
\end{array}
$$

$$goto\$stm : \qquad Nam \rightarrow Stm$$
$$if\$stm : \qquad Cnd, Stm, Eif \rightarrow Stm$$
$$if\_else\$stm : \qquad Cnd, Stm, Eif, Stm \rightarrow Stm$$
$$labled\$stm : \qquad Id, Stm \rightarrow Stm$$
$$name\$exit : \qquad Nam \rightarrow Stm$$
$$name\_cond\$exit : \qquad Nam, Cnd \rightarrow Stm$$
$$named\$block : \qquad Id, Stm \rightarrow Stm$$
$$named\$loop : \qquad Id, Stm \rightarrow Stm$$
$$named\_declare\$block : \qquad Id, Dcl, Stm \rightarrow Stm$$
$$named\_for\$loop : \qquad Id, Id, Rng, Stm \rightarrow Stm$$

$$named\_reverse\$loop : \qquad Id, Id, Rng, Stm \rightarrow Stm$$
$$named\_while\$loop : \qquad Id, Cnd, Stm \rightarrow Stm$$
$$null\$stm : \qquad \rightarrow Stm$$
$$plain\$exit : \qquad \rightarrow Stm$$
$$plain\$loop : \qquad Stm \rightarrow Stm$$
$$raise\$stm : \qquad Nam \rightarrow Stm$$
$$reraise\$stm : \qquad \rightarrow Stm$$
$$return\$stm : \qquad \rightarrow Stm$$
$$reverse\$loop : \qquad Id, Rng, Stm \rightarrow Stm$$
$$simple\$block : \qquad Stm \rightarrow Stm$$
$$while\$loop : \qquad Cnd, Stm \rightarrow Stm$$
$$handled\$statement : \qquad Stm, Xhd^* \rightarrow Stm$$
$$unhandled\$statement : \qquad Stm \rightarrow Stm$$

## B.1.28 Type Definitions ($Tdf$)

$$access\$type : \qquad Sid \rightarrow Tdf$$
$$aliased\_array\$type : \qquad Rng^*, Sid \rightarrow Tdf$$
$$aliased\_uc\_array\$type : \qquad Nam^*, Sid \rightarrow Tdf$$
$$all\_access\$type : \qquad Sid \rightarrow Tdf$$
$$array\$type : \qquad Rng^*, Sid \rightarrow Tdf$$
$$const\_access\$type : \qquad Sid \rightarrow Tdf$$

$$const\_dec\_fixed\$type : \qquad Exp, Exp, Cns \rightarrow Tdf$$
$$const\_float\$type : \qquad Exp, Cns \rightarrow Tdf$$
$$dec\_fixed\$type : \qquad Exp, Exp \rightarrow Tdf$$
$$der\$type : \qquad Sid \rightarrow Tdf$$
$$enum\$type : \qquad Id^* \rightarrow Tdf$$
$$ext\$type : \qquad Sid, rcd \rightarrow Tdf$$
$$float\$type : \qquad Exp \rightarrow Tdf$$
$$func\$type : \qquad Pms^*, Nam \rightarrow Tdf$$
$$int\$type : \qquad Exp, Exp \rightarrow Tdf$$

$$mod\$type : \qquad Exp \rightarrow Tdf$$
$$named\$type : \qquad Sid \rightarrow Tdf$$
$$ord\_fixed\$type : \qquad Exp, Rng \rightarrow Tdf$$
$$proc\$type : \qquad Pms^* \rightarrow Tdf$$
$$record\$type : \qquad Cmp^*, Vrp \rightarrow Tdf$$
$$t\_record\$type : \qquad Cmp^*, Vrp \rightarrow Tdf$$
$$uc\_array\$type : \qquad Nam^*, Sid \rightarrow Tdf$$

116

### B.1.29   Variants ($Vnt$)

$$\text{variant\$clause} : \quad Dch^*, Cmp^*, Vrp \rightarrow Vnt$$

### B.1.30   Variant Parts ($Vrp$)

$$\text{no\$variant} : Vrp$$
$$\text{variant\$part} : \quad Nam, Vnt^* \rightarrow Vrp$$

### B.1.31   Exception Choices ($Xhd$)

$$\text{choice\$handler} : \quad Id, Ech^*, Stm \rightarrow Xhd$$
$$\text{expt\$handler} : \quad Ech^*, Stm \rightarrow Xhd$$

## B.2   Lexical Elements

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

$$\boxed{\begin{array}{ll}\text{param\$pragma} : & Id, Pss^* \rightarrow Prg \\ \text{simple\$pragma} : & pragma, Id \rightarrow Prg\end{array}}$$

pragma_argument_association ::=
        [ identifier => ] name
    |  [ identifier => ] expression

$$\boxed{\begin{array}{ll}\text{named\_exp\$arg} : & Id, Exp \rightarrow Pss \\ \text{named\_name\$arg} : & Id, Nam \rightarrow Pss\end{array}}$$

## B.3   Declarations and Types

### B.3.1   Declarations

basic_declaration ::=
        type_declaration
    |  subtype_declaration
    |  object_declaration
    |  number_declaration
    |  subprogram_declaration
    |  abstract_subprogram_declaration
    |  package_declaration
    |  renaming_declaration
    |  exception_declaration
    |  generic_declaration
    |  generic_instantiation

It is convenient to treat sequences of declarations as a single declaration.

$$Dcl\$lst : \quad Dcl^* \rightarrow Dcl$$

defining_identifier ::=
        identifier

## B.3.2   Types and Subtypes

### B.3.2.1   Type Declarations

type_declaration ::=
        full_type_declaration
    |  incomplete_type_declaration
    |  private_type_declaration
    |  private_extension_declaration

full_type_declaration ::=
        **type** defining_identifier [ known_discriminant_part ] **is** type_definition ;
    |  task_type_declaration
    |  protected_type_declaration

$$
\begin{array}{ll}
\text{d\_type\$decl :} & Id,\ Dcp,\ Tdf \rightarrow Dcl \\
\text{type\$decl :} & Id,\ Tdf \rightarrow Dcl
\end{array}
$$

type_definition ::=
        enumeration_type_definition
    |  integer_type_definition
    |  real_type_definition
    |  array_type_definition
    |  record_type_definition
    |  access_type_definition
    |  derived_type_definition

### B.3.2.2   Subtype Declarations

subtype_declaration ::=
        **subtype** defining_identifier **is** subtype_indication ;

$$\text{subtype\$decl :} \quad Id,\ Sid \rightarrow Dcl$$

subtype_indication ::=
        subtype_mark [ constraint ]

subtype_mark ::=
        name

$$\begin{array}{ll}
\text{constrained\$subtype :} & \textit{Nam, Cns} \rightarrow \textit{Sid} \\
\text{named\$subtype :} & \textit{Nam} \rightarrow \textit{Sid} \\
\text{subtype\$range :} & \textit{Rng} \rightarrow \textit{Sid}
\end{array}$$

The form subtype\$range applies only to discrete subtype definitions.

constraint ::=
        scalar_constraint
    |   composite_constraint


scalar_constraint ::=
        range_constraint
    |   digits_constraint
    |   delta_constraint


composite_constraint ::=
        index_constraint
    |   discriminant_constraint


### B.3.2.3  Classification of Operations

## B.3.3  Objects and Named Numbers

### B.3.3.1  Object Declarations

object_declaration ::=
        defining_identifier_list : [ **aliased** ] [ **constant** ] subtype_indication [ := expression ] ;
    |   defining_identifier_list : [ **aliased** ] [ **constant** ] array_type_definition [ := expression ] ;
    |   single_task_declaration
    |   single_protected_declaration

$$\begin{array}{ll}
\text{a\_c\_i\_obj\$decl :} & \textit{Id, Sid, Exp} \rightarrow \textit{Dcl} \\
\text{a\_c\_obj\$decl :} & \textit{Id, Sid} \rightarrow \textit{Dcl} \\
\text{a\_i\_obj\$decl :} & \textit{Id, Sid, Exp} \rightarrow \textit{Dcl} \\
\text{a\_obj\$decl :} & \textit{Id, Sid} \rightarrow \textit{Dcl} \\
\text{c\_i\_obj\$decl :} & \textit{Id, Sid, Exp} \rightarrow \textit{Dcl} \\
\text{c\_obj\$decl :} & \textit{Id, Sid} \rightarrow \textit{Dcl} \\
\text{i\_obj\$decl :} & \textit{Id, Sid, Exp} \rightarrow \textit{Dcl} \\
\text{obj\$decl :} & \textit{Id, Sid} \rightarrow \textit{Dcl}
\end{array}$$

All forms of object declarations are normalized such that each declaration defines exactly one name. This is always possible by [3.3.1].

defining_identifier_list ::=
        defining_identifier { , defining_identifier }

### B.3.3.2 Number Declarations

number_declaration ::=
          defining_identifier_list : **constant** := expression

$$
\begin{array}{ll}
\text{real\_const\$decl}: & Id,\, Exp \rightarrow Dcl \\
\text{int\_const\$decl}: & Id,\, Exp \rightarrow Dcl
\end{array}
$$

Number declarations are disambiguated by static analysis into real and integer number declarations.

## B.3.4 Derived Types and Classes

derived_type_definition ::=
          [ abstract ] **new** subtype_indication [ record_extension_part ]

$$
\begin{array}{ll}
\text{der\$type}: & Sid \rightarrow Tdf \\
\text{ext\$type}: & Sid,\, \text{rcd} \rightarrow Tdf
\end{array}
$$

### B.3.4.1 Derivation Classes

## B.3.5 Scalar Types

range_constraint ::=
          **range** range

$$
\text{range\$constr}: \quad Rng \rightarrow Cns
$$

range ::=
          range_attribute_reference
      |   simple_expression .. simple_expression

$$
\begin{array}{ll}
\text{attr\$range}: & Nam \rightarrow Rng \\
\text{explicit\$range}: & Exp,\, Exp \rightarrow Rng \\
\text{parm\_attr\$range}: & Nam,\, Exp \rightarrow Rng
\end{array}
$$

### B.3.5.1 Enumeration Types

enumeration_type_definition ::=
          ( enumeration_literal_specification { , enumeration_literal_specification } )

$$
\text{enum\$type}: \quad Id^{*} \rightarrow Tdf
$$

enumeration_literal_specification ::=
          defining_identifier
      |   defining_character_literal

defining_character_literal ::=
        character_literal

| char$enum : | char → *Id* |
|---|---|
| id$enum : | *Id* → *Id* |

## B.3.5.2  Character Types

## B.3.5.3  Boolean Types

## B.3.5.4  Integer Types

integer_type_definition ::=
        signed_integer_type_definition
    |   modular_type_definition


signed_integer_type_definition ::=
        **range** simple_expression .. simple_expression

| int$type : | *Exp, Exp → Tdf* |
|---|---|

modular_type_definition ::=
        **mod** expression

| mod$type : | *Exp → Tdf* |
|---|---|

## B.3.5.5  Operations of Discrete Types

## B.3.5.6  Real Types

real_type_definition ::=
        floating_point_definition
    |   fixed_point_definition


## B.3.5.7  Floating Point Types

floating_point_definition ::=
        **digits** expression [ real_range_specification ]

| float$type : | *Exp → Tdf* |
|---|---|
| const_float$type : | *Exp, Cns → Tdf* |

real_range_specification ::=
        **range** simple_expression .. simple_expression


See scalar types (3.5).

**B.3.5.8   Operations of Floating Point Types**

**B.3.5.9   Fixed Point Types**

fixed_point_definition ::=
        ordinary_fixed_point_definition
    |   decimal_fixed_pointq_definition


ordinary_fixed_point_definition ::=
        **delta** expression real_range_specification

$$\boxed{\text{ord\_fixed\$type} : \quad Exp,\ Rng \rightarrow Tdf}$$

decimal_fixed_point_definition ::=
        **delta** expression **digits** expression [ real_range_specification ]

$$\boxed{\begin{array}{ll} \text{const\_dec\_fixed\$type} : & Exp,\ Exp,\ Cns \rightarrow Tdf \\ \text{dec\_fixed\$type} : & Exp,\ Exp \rightarrow Tdf \end{array}}$$

decimal_digits_constraint ::=
        **digits** expression [ range_constraint ]

$$\boxed{\begin{array}{ll} \text{constr\_digits\$constr} : & Exp,\ Cns \rightarrow Cns \\ \text{digits\$constr} : & Exp \rightarrow Cns \end{array}}$$

**B.3.5.10   Operations of Fixed Point Types**

# B.3.6   Array Types

array_type_definition ::=
        unconstrained_array_definition
    |   constrained_array_definition


unconstrained_array_definition ::=
        **array** ( index_subtype_definition { , index_subtype_definition } ) **of** component_definition

$$\boxed{\begin{array}{ll} \text{aliased\_uc\_array\$type} : & Nam^{*},\ Sid \rightarrow Tdf \\ \text{uc\_array\$type} : & Nam^{*},\ Sid \rightarrow Tdf \end{array}}$$

index_subtype_definition ::=
        subtype_mark **range** <>


constrained_array_definition ::=
        **array** ( discrete_subtype_definition { , discrete_subtype_definition } ) **of** component_definition

$$
\begin{array}{ll}
\text{aliased\_array\$type}: & \mathit{Rng}^*, \mathit{Sid} \to \mathit{Tdf} \\
\text{array\$type}: & \mathit{Rng}^*, \mathit{Sid} \to \mathit{Tdf}
\end{array}
$$

discrete_subtype_definition ::=
      subtype_indication
   |  range


Discrete subtype definitions are subsumed under subtype indications (*Sid*).

component_definition ::=
      [ **aliased** ] subtype_indication


### B.3.6.1   Index Constraints and Discrete Ranges

index_constraint ::=
      ( discrete_range { , discrete_range } )

$$
\text{index\$constr}: \quad \mathit{Rng}^* \to \mathit{Cns}
$$

discrete_range ::=
      subtype_indication
   |  range


### B.3.6.2   Operations of Array Types

### B.3.6.3   String Types

## B.3.7   Discriminants

discriminant_part ::=
      unknown_discriminant_part
   |  known_discriminant_part


unknown_discriminant_part ::=
      ( <> )


known_discriminant_part ::=
      ( discriminant_specification { ; discriminant_specification } )

$$
\begin{array}{ll}
\text{box\$discr}: & \to \mathit{Dcp} \\
\text{list\$discr}: & \mathit{Dcs}^* \to \mathit{Dcp}
\end{array}
$$

discriminant_specification ::=
      defining_identifier_list : subtype_mark [ := default_expression ]
   |  defining_identifier_list : access_definition [ := default_expression ]

default_expression ::=
        expression

$$
\begin{array}{ll}
\text{acc\$discr} : & Id,\, Nam \rightarrow Dcs \\
\text{acc\_init\$discr} : & Id,\, Nam,\, Exp \rightarrow Dcs \\
\text{init\$discr} : & Id,\, Nam,\, Exp \rightarrow Dcs \\
\text{simple\$discr} : & Id,\, Nam \rightarrow Dcs
\end{array}
$$

### B.3.7.1  Discriminant Constraints

discriminant_constraint ::=
        ( discriminant_association { , discriminant_association } )

$$
\text{discr\$constr} : \quad Dca^{*} \rightarrow Cns
$$

discriminant_association ::=
        [ selector_name { | selector_name } => ] expression

$$
\text{named\$assoc} : \quad Id,\, Exp \rightarrow Dca
$$

### B.3.7.2  Operations of Discriminated Types

## B.3.8  Record Types

record_type_definition ::=
        [ [ abstract ] **tagged** ] [ limited ] record_definition

$$
\begin{array}{ll}
\text{record\$type} : & Cmp^{*},\, Vrp \rightarrow Tdf \\
\text{t\_record\$type} : & Cmp^{*},\, Vrp \rightarrow Tdf
\end{array}
$$

record_definition ::=
        record
        component_list
        **end record**
    | **null record**


component_list ::=
        component_declaration { component_declaration }
    | { component_declaration } variant_part
    | **null** ;


component_declaration ::=
        defining_identifier_list : component_definition [ := default_expression ] ;

$$\begin{array}{ll}
\text{aliased\_comp\$decl :} & Id,\ Sid \rightarrow Cmp \\
\text{comp\$decl :} & Id,\ Sid \rightarrow Cmp \\
\text{init\_aliased\_comp\$decl :} & Id,\ Sid,\ Exp \rightarrow Cmp \\
\text{init\_comp\$decl :} & Id,\ Sid,\ Exp \rightarrow Cmp
\end{array}$$

Component declarations with multiple identifiers are replaced by multiple component declarations.

### B.3.8.1   Variant Parts and Discrete Choices

variant_part ::=
       **case** direct_name **is**
       variant
       { variant }
       **end case** ;

$$\begin{array}{ll}
\text{no\$variant:} & Vrp \\
\text{variant\$part :} & Nam,\ Vnt^* \rightarrow Vrp
\end{array}$$

variant ::=
       **when** discrete_choice_list =>
       component_list

$$\text{variant\$clause :} \quad Dch^*,\ Cmp^*,\ Vrp \rightarrow Vnt$$

discrete_choice_list ::=
       discrete_choice {
    |  discrete_choice }

discrete_choice ::=
       expression
    |  discrete_range
    |  others

$$\begin{array}{ll}
\text{discr\_other\$choice :} & \rightarrow Dch \\
Exp\text{\$choice :} & Exp \rightarrow Dch \\
\text{range\$choice :} & Rng \rightarrow Dch
\end{array}$$

## B.3.9   Tagged Types and Type Extensions

### B.3.9.1   Type Extensions

record_extension_part ::=
       **with** record_definition

**B.3.9.2  Dispatching Operations of Tagged Types**

**B.3.9.3  Abstract Types and Subprograms**

# B.3.10  Access Types

access_type_definition ::=
       access_to_object_definition
    | access_to_subprogram_definition


access_to_object_definition ::=
       **access** [ general_access_modifier ] subtype_indication


general_access_modifier ::=
       all
    | constant

| | |
|---|---|
| access\$type : | $Sid \rightarrow Tdf$ |
| all_access\$type : | $Sid \rightarrow Tdf$ |
| const_access\$type : | $Sid \rightarrow Tdf$ |

access_to_subprogram_definition ::=
       **access** [ **protected** ] **procedure** parameter_profile
       **access** [ **protected** ] **function** parameter_and_result_profile

| | |
|---|---|
| func\$type : | $Pms^{*}, Nam \rightarrow Tdf$ |
| proc\$type : | $Pms^{*} \rightarrow Tdf$ |

access_definition ::=
       **access** subtype_mark


**B.3.10.1  Incomplete Type Declarations**

incomplete_type_declaration ::=
       **type** defining_identifier [ discriminant_part ] ;

| | |
|---|---|
| d_i_type\$decl : | $Id, Dcp \rightarrow Dcl$ |
| i_type\$decl : | $Id \rightarrow Dcl$ |

**B.3.10.2  Operations of Access Types**

# B.3.11  Declarative Parts

declarative_part ::=
       { declarative_item}

```
declarative_item ::=
        basic_declarative_item
    |   body


basic_declarative_item ::=
        basic_declaration
    |   representation_clause
    |   use_clause


body ::=
        proper_body
    |   body_stub


proper_body ::=
        subprogram_body
    |   package_body
    |   task_body
    |   protected_body
```

### B.3.11.1   Completions of Declarations

# B.4   Names and Expressions

## B.4.1   Names

```
name ::=
        direct_name
    |   explicit_dereference
    |   indexed_component
    |   slice
    |   selected_component
    |   attribute_reference
    |   type_conversion
    |   function_call
    |   character_literal
```

String and character literals that denote operators are included as direct names. String literals that denote string values are represented as aggregates.

$$\boxed{\mathrm{char}\$Exp : \quad integer \rightarrow Exp}$$

```
direct_name ::=
        identifier
    |   operator_symbol
```

$$\boxed{\mathrm{direct}\$\mathrm{name} : \quad Id \rightarrow Nam}$$

127

Names that are represented as strings, character literals, and identifiers are all treated uniformly as elements of type *Id*

prefix ::=
      name
   | implicit_dereference


explicit_dereference ::=
      name . all

$$\boxed{\text{deref\$name} : \quad Nam \rightarrow Nam}$$

The abstract syntax for dereferencing includes explicit as well as implicit dereferencing.

implicit_dereference ::=
      name


### B.4.1.1   Indexed Components

indexed_component ::=
      prefix ( expression { , expression } )

$$\boxed{\text{indexed\$comp} : \quad Nam, Exp^{*} \rightarrow Nam}$$

### B.4.1.2   Slices

slice ::=
      prefix ( discrete_range )

$$\boxed{\text{slice\$op} : \quad Nam, Rng \rightarrow Nam}$$

### B.4.1.3   Selected Components

selected_component ::=
      prefix . selector_name

$$\boxed{\text{selected\$comp} : \quad Nam, Id \rightarrow Nam}$$

Static semantics separates expanded names from selected components.

selector_name ::=
      identifier
   | character_literal
   | operator_symbol

### B.4.1.4 Attributes

attribute_reference ::=
      prefix ' attribute_designator


attribute_designator ::=
      identifier [ ( expression ) ]
    |  access
    |  delta
    |  digits


range_attribute_reference ::=
      prefix ' range_attribute_designator


range_attribute_designator ::=
      **range** [ ( expression ) ]

$$
\begin{array}{ll}
Id\$attr: & Nam,\ Id \rightarrow Nam \\
param\$attr: & Nam,\ Id,\ Exp \rightarrow Nam
\end{array}
$$

There is special abstract syntax needed for attributes that are reserved words.

## B.4.2 Literals

## B.4.3 Aggregates

aggregate ::=
      record_aggregate
    |  extension_aggregate
    |  array_aggregate


### B.4.3.1 Record Aggregates

record_aggregate ::=
      ( record_component_association_list )


record_component_association_list ::=
      record_component_association { , record_component_association}
    |  **null** record

$$
\begin{array}{ll}
null\_record\$Agg: & \rightarrow Agg \\
record\$Agg: & Rca^{*} \rightarrow Agg
\end{array}
$$

record_component_association ::=
      [ component_choice_list => ] expression

$$\boxed{\text{choice\$assoc}: \quad Ccl, Exp \rightarrow Rca}$$

Positional parameter associations have been eliminated by static analysis and are represented with an explicit choice list. This normalization is possible since, by [4.3.1], discriminant values that determine variants are required to be static.

component_choice_list ::=
        selector_name { | selector_name }
    | others

$$\boxed{\begin{array}{ll} \text{list\$choice}: & Id^* \rightarrow Ccl \\ \text{others\$choice}: & \rightarrow Ccl \end{array}}$$

## B.4.3.2 Extension Aggregates

extension_aggregate ::=
        ( expression **with** record_component_association_list )

$$\boxed{\begin{array}{ll} \text{ext\$}Agg: & Exp, Rca^* \rightarrow Agg \\ \text{null\_ext\$}Agg: & Exp \rightarrow Agg \end{array}}$$

## B.4.3.3 Array Aggregates

array_aggregate ::=
        positional_array_aggregate
    | named_array_aggregate

positional_array_aggregate ::=
        ( expression , expression { , expression} )
    | ( expression { , expression} , **others** => expression )

named_array_aggregate ::=
        ( array_component_association { , array_component_association} )

$$\boxed{\begin{array}{ll} \text{named\_array\$}Agg: & Aca^* \rightarrow Agg \\ \text{other\_array\$}Agg: & Exp^*, Exp \rightarrow Agg \\ \text{pos\_array\$}Agg: & Exp^* \rightarrow Agg \end{array}}$$

array_component_association ::=
        discrete_choice_list => expression

$$\boxed{\text{array\_comp\$assoc}: \quad Dch^*, Exp \rightarrow Aca}$$

## B.4.4 Expressions

expression ::=
        relation { **and** relation }
    |  relation { **and then** relation }
    |  relation { **or** relation }
    |  relation { **or else** relation }
    |  relation { **xor** relation }

$$
\begin{array}{ll}
\text{and\_then\$}Exp : & Exp,\, Exp \rightarrow Exp \\
\text{or\_else\$}Exp : & Exp,\, Exp \rightarrow Exp
\end{array}
$$

Short-circuit operators are non-strict and require explicit representation.

relation ::=
        simple_expression [ relational_operator simple_expression ]
    |  simple_expression [ **not** ] **in** range
    |  simple_expression [ **not** ] **in** subtype_mark

$$
\begin{array}{ll}
\text{in\_name\$}Exp : & Exp,\, Nam \rightarrow Exp \\
\text{in\_range\$}Exp : & Exp,\, Rng \rightarrow Exp \\
\text{in\_type\$}Exp : & Exp,\, Nam \rightarrow Exp \\
\text{not\_in\_name\$}Exp : & Exp,\, Nam \rightarrow Exp \\
\text{not\_in\_range\$}Exp : & Exp,\, Rng \rightarrow Exp \\
\text{not\_in\_type\$}Exp : & Exp,\, Nam \rightarrow Exp
\end{array}
$$

Static semantics distinguishes between membership tests where the name denotes an object and those where the name denotes a subtype.

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 )

$$
\begin{array}{ll}
\text{paren\$}Exp : & Exp \rightarrow Exp \\
\text{qual\$aggregate} : & Nam,\ Agg \rightarrow Exp \\
\text{name\$}Exp : & Nam \rightarrow Exp \\
\text{null\$}Exp : & \rightarrow Exp \\
\text{integer\$}Exp : & \text{integer} \rightarrow Exp \\
\text{real\$}Exp : & \text{real} \rightarrow Exp
\end{array}
$$

All aggregates are assumed to be qualified by static analysis. String literals are represented as qualified aggregates. It may be necessary for static analysis to introduce new type names for aggregates of anonymous array types.

Numeric literals are separated into integer and real literals.

### B.4.5  Operators and Expression Evaluation

All strict operators on ordinary values are represented in the abstract syntax as function calls. As with other function calls, the function designators specify the unique overload that applies. Non-strict operators or operators that take subtypes as arguments (e.g., **in**) have an explicit representation given below.

```
logical_operator ::=
        and
    |   or
    |   xor


relational_operator ::=
        =
    |   / =
    |   <
    |   <=
    |   >
    |   >=


binary_adding_operator ::=
        +
    |   -
    |   &


unary_adding_operator ::=
        -
    |   +


multiplying_operator ::=
        *
    |   /
    |   mod
    |   rem
```

```
highest_precedence_operator ::=
        **
      |  abs
      |  not
```

### B.4.5.1   Logical Operations and Short-Circuit Control Forms

### B.4.5.2   Relational Operators and Membership Tests

### B.4.5.3   Binary Adding Operators

### B.4.5.4   Multiplying Operators

### B.4.5.5   Highest Precedence Operators

## B.4.6   Type Conversions

```
type_conversion ::=
        subtype_mark ( expression )
      |  subtype_mark ( name )
```

$$
\begin{array}{ll}
\text{type\$conversion :} & Nam, Exp \rightarrow Exp \\
\text{name\_type\$conversion :} & Nam, Nam \rightarrow Nam
\end{array}
$$

## B.4.7   Qualified Expressions

```
qualified_expression ::=
        subtype_mark' ( expression )
      |  subtype_mark ' aggregate
```

$$
\text{qual\$}Exp : \quad Nam, Exp \rightarrow Exp
$$

The abstract syntax for qualified aggregates is covered under aggregates.

## B.4.8   Allocators

```
allocator ::=
        new subtype_indication
      |  new qualified_expression
```

$$
\begin{array}{ll}
Exp\text{\$alloc :} & Exp \rightarrow Exp \\
\text{type\$alloc :} & Sid \rightarrow Exp
\end{array}
$$

### B.4.9 Static Expressions and Static Subtypes

#### B.4.9.1 Statically Matching Constraints and Subtypes

# B.5 Statements

## B.5.1 Simple and Compound Statements – Sequences of Statements

sequence_of_statements ::=
      statement { statement }


Sequences of statements can be treated as single statements.

$$Stm\$lst : \quad Stm^* \rightarrow Stm$$

statement ::=
      { label } simple_statement
    |  { label } compound_statement


$$labeld\$stm : \quad Id, Stm \rightarrow Stm$$

simple_statement ::=
      null_statement
    |  assignment_statement
    |  exit_statement
    |  goto_statement
    |  procedure_call_statement
    |  return_statement
    |  entry_call_statement
    |  requeue_statement
    |  delay_statement
    |  abort_statement
    |  raise_statement
    |  code_statement


compound_statement ::=
      if_statement
    |  case_statement
    |  loop_statement
    |  block_statement
    |  accept_statement
    |  select_statement


null_statement ::=
      **null** ;


$$null\$stm : \quad \rightarrow Stm$$

label ::=
      << statement_identifier >>


statement_identifier ::=
      direct_name


## B.5.2 Assignment Statement

assignment_statement ::=
      name := expression

$$\boxed{\text{assign\$stm}: \quad Nam,\ Exp \rightarrow Stm}$$

## B.5.3 If Statements

if_statement ::=
      **if** condition **then**
          sequence_of_statements
      { **elsif** condition **then**
          sequence_of_statements}
      [ **else**
          sequence_of_statements ]
      **end if** ;

$$\boxed{\begin{array}{ll} \text{if\$stm}: & Cnd,\ Stm,\ Eif \rightarrow Stm \\ \text{if\_else\$stm}: & Cnd,\ Stm,\ Eif,\ Stm \rightarrow Stm \\ Eif\text{\$lst}: & Eif^{*} \rightarrow Eif \\ \text{elsif\$clause}: & Cnd,\ Stm \rightarrow Eif \end{array}}$$

condition ::=
      expression

$$\boxed{Exp\text{\$condition}: \quad Exp \rightarrow Cnd}$$

## B.5.4 Case Statements

case_statement ::=
      **case** expression **is**
          case_statement_alternative
          { case_statement_alternative }
      **end case** ;

$$\boxed{\text{case\$stm}: \quad Exp,\ Alt \rightarrow Stm}$$

case_statement_alternative ::=
        **when** discrete_choice_list =>
        sequence_of_statements

$$
\begin{array}{ll}
Alt\$\mathrm{lst} : & Alt^* \rightarrow Alt \\
\mathrm{case}\$Alt : & Dch^*, Stm \rightarrow Alt
\end{array}
$$

## B.5.5   Loop Statements

loop_statement ::=
        [ statement_identifier : ]
        [ iteration_scheme ] loop
        sequence_of_statements
        **end loop** [ identifier ] ;


iteration_scheme ::=
        **while** condition
    |   **for** loop_parameter_specification


loop_parameter_specification ::=
        defining_identifier **in** [ **reverse** ] discrete_subtype_definition

$$
\begin{array}{ll}
\mathrm{named\_for}\$\mathrm{loop} : & Id, Id, Rng, Stm \rightarrow Stm \\
\mathrm{named\_reverse}\$\mathrm{loop} : & Id, Id, Rng, Stm \rightarrow Stm \\
\mathrm{named\_while}\$\mathrm{loop} : & Id, Cnd, Stm \rightarrow Stm \\
\mathrm{named}\$\mathrm{loop} : & Id, Stm \rightarrow Stm \\
\mathrm{for}\$\mathrm{loop} : & Id, Rng, Stm \rightarrow Stm \\
\mathrm{reverse}\$\mathrm{loop} : & Id, Rng, Stm \rightarrow Stm \\
\mathrm{while}\$\mathrm{loop} : & Cnd, Stm \rightarrow Stm \\
\mathrm{plain}\$\mathrm{loop} : & Stm \rightarrow Stm
\end{array}
$$

## B.5.6   Block Statements

block_statement ::=
        [ statement_identifier : ]
            [ **declare**
                declarative_part ]
            **begin**
                handled_sequence_of_statements
        **end** [ identifier ] ;

$$
\begin{array}{ll}
\mathrm{simple}\$\mathrm{block} : & Stm \rightarrow Stm \\
\mathrm{declare}\$\mathrm{block} : & Dcl, Stm \rightarrow Stm \\
\mathrm{named}\$\mathrm{block} : & Id, Stm \rightarrow Stm \\
\mathrm{named\_declare}\$\mathrm{block} : & Id, Dcl, Stm \rightarrow Stm
\end{array}
$$

### B.5.7 Exit Statements

exit_statement ::=
       **exit** [ name ] [ **when** condition ] ;

| | |
|---|---|
| name$exit : | $Nam \rightarrow Stm$ |
| name_cond$exit : | $Nam,\ Cnd \rightarrow Stm$ |
| plain$exit : | $\rightarrow Stm$ |
| cond$exit : | $Cnd \rightarrow Stm$ |

### B.5.8 Goto Statements

goto_statement ::=
       **goto** name ;

| | |
|---|---|
| goto$stm : | $Nam \rightarrow Stm$ |

## B.6 Subprograms

### B.6.1 Subprogram Declarations

subprogram_declaration ::=
       subprogram_specification ;

| | |
|---|---|
| subp$spec : | $Sps \rightarrow Dcl$ |

abstract_subprogram_declaration ::=
       subprogram_specification **is abstract** ;

| | |
|---|---|
| subp$spec : | $Sps \rightarrow Dcl$ |

subprogram_specification ::=
       **procedure** defining_program_unit_name parameter_profile
     | **function** defining_designator parameter_and_result_profile

| | |
|---|---|
| function$spec : | $Id,\ Pms^{*},\ Nam \rightarrow Sps$ |
| procedure$spec : | $Id,\ Pms^{*} \rightarrow Sps$ |

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


operator_symbol ::=
       string_literal


defining_operator_symbol ::=
       operator_symbol


parameter_profile ::=
       [ formal_part ]

$$
\begin{array}{ll}
\text{no\$params}: & \rightarrow Psig \\
\text{param\$list}: & Pms^{*} \rightarrow Psig
\end{array}
$$

parameter_and_result_profile ::=
       [ formal_part ] **return** subtype_mark


formal_part ::=
       ( parameter_specification { ; parameter_specification } )


parameter_specification ::=
       defining_identifier_list : mode subtype_mark [ := default_expression ]
    |  defining_identifier_list : access_definition [ := default_expression ]

$$
\begin{array}{ll}
\text{access\$param}: & Id, Nam \rightarrow Pms \\
\text{access\_default\$param}: & Id, Nam, Exp \rightarrow Pms \\
\text{default\$param}: & Id, Mde, Nam, Exp \rightarrow Pms \\
\text{normal\$param}: & Id, Mde, Nam \rightarrow Pms
\end{array}
$$

mode ::=
       [ **in** ]
    |  **in** out
    |  out

$$
\begin{array}{ll}
\text{in\$mode}: & \rightarrow Mde \\
\text{in\_out\$mode}: & \rightarrow Mde \\
\text{no\$mode}: & \rightarrow Mde \\
\text{out\$mode}: & \rightarrow Mde
\end{array}
$$

## B.6.2  Formal Parameter Modes

## B.6.3  Subprogram Bodies

subprogram_body ::=
      subprogram_specification is
          declarative_part
      **begin**
          handled_sequence_of_statements
      **end** [ designator ] ;

$$\text{subp\$body}: \quad Sps,\, Dcl,\, Stm \rightarrow Dcl$$

### B.6.3.1  Conformance Rules

### B.6.3.2  Inline Expansion of Subprograms

## B.6.4  Subprogram Calls

procedure_call_statement ::=
      name
  | prefix actual_parameter_part ;

$$\text{call\$stm}: \quad Nam,\, Pss^{*} \rightarrow Stm$$

function_call ::=
      name
  | prefix actual_parameter_part

$$\text{func\$call}: \quad Nam,\, Pss^{*} \rightarrow Nam$$

actual_parameter_part ::=
      ( parameter_association { , parameter_association } )

parameter_association ::=
      [ selector_name => ] explicit_actual_parameter

explicit_actual_parameter ::=
      expression
  | name

$$\begin{array}{ll}\text{named\_exp\$arg}: & Id,\, Exp \rightarrow Pss \\ \text{named\_name\$arg}: & Id,\, Nam \rightarrow Pss\end{array}$$

**B.6.4.1  Parameter Associations**

**B.6.5  Return Statements**

return_statement ::=
      **return** [ expression ] ;

$$
\begin{array}{ll}
\text{func\_return\$stm :} & Exp \rightarrow Stm \\
\text{return\$stm :} & \rightarrow Stm
\end{array}
$$

**B.6.6  Overloading of Operators**

# B.7  Packages

**B.7.1  Package Specifications and Declarations**

package_declaration ::=
      package_specification ;

package_specification ::=
      **package** defining_program_unit_name **is**
          {basic_declarative_item}
      [ private
          {basic_declarative_item} ]
      **end** [ [ parent_unit_name . ] identifier ]

**B.7.2  Package Bodies**

package_body ::=
      **package body** defining_program_unit_name **is**
          declarative_part
      [ begin
          handled_sequence_of_statements
      **end** [ [ parent_unit_name . ] identifier ] ;

**B.7.3  Private Type and Private Extensions**

private_type_declaration ::=
      **type** defining_identifier [ discriminant_part ] **is** [ [ abstract ] **tagged** ] [ **limited** ] **private** ;

private_extension_declaration ::=
      **type** defining_identifier [ discriminant_part ] **is**
      [ abstract ] **new** subtype_indication **with private** ;

$$
\begin{array}{ll}
\text{d\_ext\$decl :} & Id,\, Dcp,\, Sid \rightarrow Dcl \\
\text{ext\$decl :} & Id,\, Sid \rightarrow Dcl
\end{array}
$$

# B.8   Visibility Rules

## B.8.1   Declarative Region

## B.8.2   Scope of Declarations

## B.8.3   Visibility

## B.8.4   Use Clauses

use_clause ::=
        use_package_clause
      | use_type_clause


use_package_clause ::=
        **use** name { , name } ;

$$\boxed{\text{use\$clause} : \quad Nam^{*} \rightarrow Dcl}$$

use_type_clause ::=
        **use type** subtype_mark { , subtype_mark } ;

$$\boxed{\text{use\_type\$clause} : \quad Nam^{*} \rightarrow Dcl}$$

## B.8.5   Renaming Declarations

renaming_declaration ::=
        object_renaming_declaration
      | exception_renaming_declaration
      | package_renaming_declaration
      | subprogram_renaming_declaration
      | generic_renaming_declaration


### B.8.5.1   Object Renaming Declarations

object_renaming_declaration ::=
        defining_identifier : subtype_mark **renames** name ;

$$\boxed{\text{object\$renaming} : \quad Id,\ Nam,\ Nam \rightarrow Dcl}$$

### B.8.5.2   Exception Renaming Declarations

exception_renaming_declaration ::=
        defining_identifier : **exception renames** name ;

$$\boxed{\text{exception\$renaming}: \quad Id,\ Nam \rightarrow Dcl}$$

### B.8.5.3   Package Renaming Declarations

package_renaming_declaration ::=
        **package** defining_program_unit_name **renames** name ;

### B.8.5.4   Subprogram Renaming Declarations

subprogram_renaming_declaration ::=
        subprogram_specification **renames** name ;

$$\boxed{\text{subp\$renaming}: \quad Sps,\ Nam \rightarrow Dcl}$$

### B.8.5.5   Generic Renaming Declarations

generic_renaming_declaration ::=
        **generic package** defining_program_unit_name **renames** name ;
    |   **generic procedure** defining_program_unit_name **renames** name ;
    |   **generic function** defining_program_unit_name **renames** name ;

## B.8.6   The Context of Overload Resolution

# B.9   Tasks and Synchronization

## B.9.1   Task Units and Task Objects

task_type_declaration ::=
        **task type** defining_identifier [ known_discriminant_part ] [ **is task** definition ] ;

single_task_declaration ::=
        **task** defining_identifier [ **is task** definition ] ;

task_definition ::=
        { task_item }
        [ private
        {task_item} ]
        **end** [ identifier ]

task_item ::=
        entry_declaration
    | representation_clause


task_body ::=
        **task body** defining_identifier **is**
        declarative_part
        **begin**
        handled_ sequence_of_statements
        **end** [ identifier ] ;


## B.9.2  Task Execution – Task Activation

## B.9.3  Task Dependence – Termination of Tasks

## B.9.4  Protected Units and Protected Objects

protected_type_declaration ::=
        **protected type** defining_identifier [ known_discriminant_part ] **is** protected_definition ;


single_protected_declaration ::=
        **protected** defining_identifier **is** protected_definition ;


protected_definition ::=
        { protected_operation_declaration }
        [ private
        {protected_element_declaration} ]
        **end** [ identifier ]


protected_operation_declaration ::=
        subprogram_declaration
    | entry_declaration


protected_element_declaration ::=
        protected_operation_declaration
    | component_declaration


protected_body ::=
        **protected body** defining_identifier **is**
        {protected_operation_item}
        **end** [ identifier ] ;


protected_operation_item ::=
        subprogram_declaration
    | subprogram_body
    | entry_body

## B.9.5  Intertask Communication

entry_declaration ::=
      **entry** defining_identifier [ ( discrete_subtype_definition ) ] parameter_profile ;


accept_statement ::=
      **accept** direct_name [ ( entry_index ) ] parameter_profile [ **do**
         handled_sequence_of_statements
      **end** [ identifier ] ] ;


entry_index ::=
      expression


entry_body ::=
      **entry** defining_identifier entry_body_formal_part entry_barrier **is**
      declarative_part
      begin
      handled_sequence_of_statements
      **end** [ identifier ] ;


entry_body_formal_part ::=
      [ ( entry_index_specification ) ]parameter_profile


entry_barrier ::=
      **when** condition


entry_index_specification ::=
      **for** defining_identifier **in** discrete_subtype_definition


entry_call_statement ::=
      name [ actual_parameter_part ] ;


requeue_statement ::=
      requeue name [ **with abort** ] ;


## B.9.6  Delay Statements, Duration, and Time

delay_statement ::=
      delay_until_statement
    | delay_relative_statement


delay_until_statement ::=
      **delay** until expression ;

delay_relative_statement ::=
      **delay** expression ;

## B.9.7   Select Statements

select_statement ::=
      selective_accept
    |   timed_entry_call
    |   conditional_entry_call
    |   asynchronous_select

## B.9.8   Selective Accept

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** ;

## B.9.9   Timed Entry Calls

timed_entry_call ::=
      select
          entry_call_alternative

```
        or
            delay_alternative
        end select ;
```

```
entry_call_alternative ::=
        entry_call_statement [ sequence_of_statements ]
```

## B.9.10   Conditional Entry Calls

```
conditional_entry_call ::=
        select
            entry_call_alternative
        else
            sequence_of_statements
        end select ;
```

## B.9.11   Asynchronous Transfer of Control

```
asynchronous_select ::=
        select
        triggering_alternative
        then abort
        abortable_part
        end select ;
```

```
triggering_alternative ::=
        triggering_statement [ sequence_of_statements ]
```

```
triggering_statement ::=
        entry_call_statement
    |   delay_statement
```

```
abortable_part ::=
        sequence_of_statements
```

## B.9.12   Abort of a Task − Abort of a Sequence of Statements

```
abort_statement ::=
        abort name { , name} ;
```

# B.10    Program Structure and Compilation Issues

## B.10.1    Separate Compilation

### B.10.1.1    Compilation Units – Library Units

```
compilation ::=
        {compilation_unit}


compilation_unit ::=
        context_clause library_item
    |   context_clause subunit


library_item ::=
        [ private ] library_unit_declaration
    |   library_unit_body


library_unit_declaration ::=
        subprogram_declaration
    |   package_declaration
    |   generic_declaration
    |   generic_instantiation
    |   library_unit_renaming_declaration


library_unit_renaming_declaration ::=
        package_renaming_declaration
    |   generic_renaming_declaration
    |   subprogram_renaming_declaration


library_unit_body ::=
        subprogram_body
    |   package_body


parent_unit_name ::=
        name
```

$$
\begin{array}{ll}
\text{lib\$unit :} & Cit^{*},\, Dcl \rightarrow \text{cmu} \\
\text{private\$unit :} & Cit^{*},\, Dcl \rightarrow \text{cmu} \\
\text{sub\$unit :} & Cit^{*},\, Nam,\, Dcl \rightarrow \text{cmu}
\end{array}
$$

Renaming of library units is dealt with in static semantics.

**B.10.1.2   Context Clauses – With Clauses**

context_clause ::=
          { context_item}


context_item ::=
          with_clause
      |   use_clause


with_clause ::=
          **with** name { , name } ;


$$\text{with\$context}: \quad Nam^* \rightarrow Cit$$


**B.10.1.3   Subunits of Compilation Units**

body_stub ::=
          subprogram_body_stub
      |   package_body_stub
      |   task_body_stub
      |   protected_body_stub


subprogram_body_stub ::=
          subprogram_specification **is separate** ;


$$\text{s\_subp\$spec}: \quad Sps \rightarrow Dcl$$

package_body_stub ::=
          **package body** defining_identifier **is separate** ;


task_body_stub ::=
          **task body** defining_identifier **is separate** ;


protected_body_stub ::=
          **protected body** defining_identifier **is separate** ;


subunit ::=
          **separate** ( parent_unit_name ) proper_body

# B.11   Exceptions

## B.11.1   Exception Declarations

exception_declaration ::=
        defining_identifier_list : **exception** ;

$$\text{excpt\$decl} : \quad Id \rightarrow Dcl$$

As with object declarations, only a single name is defined by each exception declaration.

## B.11.2   Exception Handlers

handled_sequence_of_statements ::=
        sequence_of_statements
        [ exception
        exception_handler
        { exception_handler } ]

$$
\begin{array}{ll}
\text{handled\$statement} : & Stm, Xhd^* \rightarrow Stm \\
\text{unhandled\$statement} : & Stm \rightarrow Stm
\end{array}
$$

exception_handler ::=
        **when** [ choice_parameter_specification : ] exception_choice { | exception_choice } =>
            sequence_of_statements

$$
\begin{array}{ll}
\text{choice\$handler} : & Id, Ech^*, Stm \rightarrow Xhd \\
\text{expt\$handler} : & Ech^*, Stm \rightarrow Xhd
\end{array}
$$

choice_parameter_specification ::=
        defining_identifier

exception_choice ::=
        name
     |  others

$$
\begin{array}{ll}
\text{named\$excpt} : & Nam \rightarrow Ech \\
\text{others\$excpt} : & \rightarrow Ech
\end{array}
$$

### B.11.3   Raise Statements

raise_statement ::=
      **raise** [ name ] ;

$$
\begin{array}{ll}
\text{raise\$stm :} & Nam \rightarrow Stm \\
\text{reraise\$stm :} & \rightarrow Stm
\end{array}
$$

### B.11.4   Exception Handling

### B.11.5   Suppressing Checks

### B.11.6   Exceptions and Optimization

# B.12   Generic Units

### B.12.1   Generic Declarations

generic_declaration ::=
      generic_subprogram_declaration
    |  generic_package_declaration


generic_subprogram_declaration ::=
      generic_formal_part subprogram_specification ;


generic_package_declaration ::=
      generic_formal_part package_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


### B.12.2   Generic Bodies

### B.12.3   Generic Instantiation

generic_instantiation ::=
      **package** defining_program_unit_name **is**
        **new** name [ generic_actual_part ] ;
    |  **procedure** defining_program_unit_name **is**
        **new** name [ generic_actual_part ] ;

| **function** defining_designator is
new name [ generic_actual_part ] ;


generic_actual_part ::=
( generic_association { , generic_association } )


generic_association ::=
[ selector_name => ] explicit_generic_actual_parameter


explicit_generic_actual_parameter ::=
expression
| name
| subtype_mark


## B.12.4   Formal Objects

formal_object_declaration ::=
defining_identifier_list : mode subtype_mark [ := default_expression ] ;

$$
\begin{array}{ll}
\text{init\_formal\$obj}: & Id^{*}, \, Mde, \, Nam, \, Exp \rightarrow Gpd \\
\text{formal\$obj}: & Id^{*}, \, Mde, \, Nam \rightarrow Gpd
\end{array}
$$

## B.12.5   Formal Types

formal_type_declaration ::=
**type** defining_identifier [ discriminant_part ] **is** formal_type_definition ;


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


### B.12.5.1   Formal Private and Derived Types

formal_private_type_definition ::=
[ [ abstract ] tagged ] [ limited ] private

formal_derived_type_definition ::=
        [ abstract ] **new** subtype_mark [ with private ]


### B.12.5.2    Formal Scalar Types

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 ::=
        **digits** <> **delta** <>


### B.12.5.3    Formal Array Types

formal_array_type_definition ::=
        array_type_definition


### B.12.5.4    Formal Access Types

formal_access_type_definition ::=
        access_type_definition


## B.12.6    Formal Subprograms

formal_subprogram_declaration ::=
        **with** subprogram_specification [ **is** subprogram_default ] ;


subprogram_default ::=
        default_name
    |   <>


default_name ::=
        name

### B.12.7  Formal Packages

formal_package_declaration ::=
      **with package** defining_identifier **is new** name formal_package_actual_part ;


formal_package_actual_part ::=
      ( <> )
  |  [ generic_actual_part ]


### B.12.8  Example of a Generic Package

## B.13  Representation Clauses and Implementation−Dependent Features

representation_clause ::=
      attribute_definition_clause
  |  enumeration_representation_clause
  |  record_representation_clause
  |  at_clause


attribute_definition_clause ::=

      **for** direct_name ' attribute_designator **use** expression ;
  |  **for** direct_name ' attribute_designator **use** name ;


enumeration_representation_clause ::=
      **for** direct_name **use** enumeration_aggregate ;


enumeration_aggregate ::=
      array_aggregate


record_representation_clause ::=
      **for** direct_name **use**
      **record** [ mod_clause ]
      {component_clause}
      **end record** ;


component_clause ::=
      component_clause_component_name **at position range** first_bit .. last_bit ;


component_clause_component_name ::=
      direct_name
  |  direct_name ' attribute_designator

```
position ::=
        expression


first_bit ::=
        simple_expression


last_bit ::=
        simple_expression


code_statement ::=
        qualified_expression ;
```

$$
\begin{array}{ll}
\text{agg\_code\$stm :} & Nam,\ Agg \rightarrow Stm \\
\text{exp\_code\$stm :} & Nam,\ Exp \rightarrow Stm
\end{array}
$$

```
restriction ::=
        identifier
    |   identifier => expression


delta_constraint ::=
        delta expression [ range_constraint ]
```

$$
\begin{array}{ll}
\text{constr\_delta\$constr :} & Exp,\ Cns \rightarrow Cns \\
\text{delta\$constr :} & Exp \rightarrow Cns
\end{array}
$$

```
at_clause ::=
        for directed_name use at expression ;


mod_clause ::=
        at mod expression ;
```

## B.14   Ada 9X Input–Output