

---

# **Specware Language Manual**

***Release 4.2***

**Kestrel Institute**

October 14, 2015



# CONTENTS

<b>1</b>	<b>Disclaimer</b>	<b>1</b>
<b>2</b>	<b>Introduction to Specware</b>	<b>3</b>
2.1	What is Specware? . . . . .	3
2.2	What is Specware for? . . . . .	3
2.3	The design process in Specware . . . . .	4
2.4	Stages of application building . . . . .	4
2.5	Reasoning about your code . . . . .	5
<b>3</b>	<b>Metaslang</b>	<b>7</b>
3.1	Preliminaries . . . . .	7
3.2	Lexical conventions . . . . .	10
3.3	Units . . . . .	12
3.4	Declarations . . . . .	22
3.5	Type-descriptors . . . . .	30
3.6	Expressions . . . . .	37
3.7	Matches and Patterns . . . . .	51
<b>A</b>	<b>Metaslang Grammar</b>	<b>57</b>
A.1	The Grammar Description Formalism . . . . .	57
A.2	The Grammar . . . . .	57
<b>B</b>	<b>Inbuilts</b>	<b>71</b>



# DISCLAIMER

As experience is gained with Specware 4.2, both the operation of the Specware system and the Metaslang language are bound to undergo changes, which may not always be fully “backwards compatible”.

For updates, news and bug reports, visit the Specware web site <http://www.specware.org>.



# INTRODUCTION TO SPECWARE

## 2.1 What is Specware?

Specware is a tool for building and manipulating a collection of related specifications. Specware can be considered:

- a design tool, because it can represent and manipulate designs for complex systems, software or otherwise
- a logic, because it can describe concepts in a formal language with rules of deduction
- a programming language, because it can express programs and their properties
- a database, because it can store and manipulate collections of concepts, facts, and relationships

Specifications are the primary units of information in Specware. A specification, or theory, describes a concept to some degree of detail. To add properties and extend definitions, you create new specifications that import or combine earlier specifications. Within a specification, you can reason about objects and their relationships. You declare types (data types) and operations (ops, functions), axioms that state properties of operations, and theorems that follow logically from axioms.

A morphism is a relationship between specifications that describes how the properties of one map relate to the properties of another. Morphisms describe both part-of and is-a relationships. You can propagate theorems from one specification to another using morphisms; for example, if the QEII is a ship, and ships cannot fly, then the QEII cannot fly.

## 2.2 What is Specware for?

Specware is a general-purpose tool that you can use to develop specifications for any system or realm of knowledge. You can do this as an abstract process, with no reference to computer programming; or you can produce a computer program that is provably a correct implementation of a specification; or you can use the process to redesign an existing program.

You can use Specware to:

- *Develop domain theories* You can use Specware to do “ontological engineering” – that is, to describe a real-world domain of knowledge in explicit or rigorous terms. You might wish to develop a domain theory in abstract terms that are not necessarily intended to become a computer program. You can use the inference engine to test the internal logic of your theory, derive conclusions, and propose theorems. You can use specifications and morphisms to represent abstract knowledge, with no refinement to any kind of concrete implementation. More commonly, you would use Specware to model expert knowledge of engineering design. In this case you would refine your theoretical specifications and morphisms to more concrete levels.
- *Develop code from specifications* You can use Specware to develop computer programs from specifications. One advantage of using Specware for this task is that you can prove that the generated code does implement the

specification correctly. Another advantage is that you can develop and compare different implementations of the same specification.

- *Develop specifications from code* You can use Specware for reverse engineering – that is, to help you derive a specification from existing code. To do this, you must examine the code to determine what problems are being solved by it, then use Specware’s language Metaslang to express the problems as specifications. In addition to providing a notation tool for this process, Specware allows you to operate on the derived specification. Once you have derived a specification from the original code, you can analyze the specification for correctness and completeness, and also generate different and correct implementations for it.

## 2.3 The design process in Specware

To solve real problems, programs typically combine domain theories about the physical world with problem solving theories about the computational world. Your domain theory is an abstract representation of a real-world problem domain. To implement it, you must transform the domain theory to a concrete computational model. The built-in specification libraries describe mathematical and computational concepts, which are building blocks for an implementation. Your specifications combine real-world knowledge with this built-in computational knowledge to generate program code that solves real- world problems in a rigorous and provable way.

You interpret designs relative to an initial universe of models. In software design, for example, the models are programs, while in engineering design, they are circuits or pieces of metal. To design an object is to choose it from among the universe of possible models. You make this choice by beginning with an initial description and augmenting it until it uniquely describes the model you desire. In Specware, this process is called refinement.

Composition and refinement are the basic techniques of application building in Specware. You compose simpler specifications into more complex ones, and refine more abstract specifications into more concrete ones. When you refine a specification, you create a more specific case of it; that is, you reduce the number of possible models of it.

The process of refinement is also one of composition. To begin the refinement, you construct primitive refinements that show how to implement an abstract concept in terms of a concrete concept. You then compose refinements to deepen and widen the refinement.

For example, suppose you are designing a house. A wide but not deep view of the design specifies several rooms but gives no details. A deep but not wide view of the design specifies one room in complete detail. To complete the refinement, you must create a view that is both wide and deep; however, it makes no difference which view you create first.

The final refinement implements a complex, abstract specification from which code can be generated.

## 2.4 Stages of application building

Conceptually, there are two major stages in producing a Specware application. In the actual process, steps from these two stages may alternate.

1. Building a specification
2. Refining your specifications to constructive specifications

### 2.4.1 Building a specification

You must build a specification that describes your domain theory in rigorous terms. To do this, you first create small specifications for basic, abstract concepts, then specialize and combine these to make them more concrete and complex.



To relate concepts to each other in Specware, you use specification morphisms. A specification morphism shows how one concept is a specialization or part of another. For example, the concept “fast car” specializes both “car” and “fast thing”. The concept “room” is part of the concept “house”. You can specialize “room” in different ways, one for each room of the house.

You specialize in order to derive a more concrete specification from a more abstract specification. Because the specialization relation is transitive (if A specializes B and B specializes C, then A specializes C as well), you can combine a series of morphisms to achieve a step- wise refinement of abstract specifications into increasingly concrete ones.

You combine specifications in order to construct a more complex concept from a collection of simpler parts. In general, you increase the complexity of a specification by adding more structural detail.

Specware helps you to handle complexity and scale by providing composition operators that take small specifications and combine them in a rigorous way to produce a complex specification that retains the logic of its parts. Specware provides several techniques for combining specifications, that can be used in combination:

- The import operation allows you to include earlier specifications in a later one.
- The translate operation allows you to rename the parts of a specification.
- The colimit operation glues concepts together into a shared union along shared subconcepts.

A shared union specification combines specializations of a concept. For example, if you combine “red car” with “fast car” sharing the concept “car”, you obtain the shared union “fast, red car”. If you combine them sharing nothing, you obtain “red car and fast car”, which is two cars rather than one. Both choices are available.

## 2.4.2 Refining your specifications to constructive specifications

You combine specifications to extend the refinement iteratively. The goal is to create a refinement between the abstract specification of your problem domain and a concrete implementation of the problem solution in terms of types and operations that ultimately are defined in the Specware libraries of mathematical and computational theories.

For example, suppose you want to create a specification for a card game. An abstract specification of a card game would include concepts such as card, suit, and hand. A refinement for this specification might map cards to natural numbers and hands to lists containing natural numbers.

The Specware libraries contains constructive specifications for various types, including natural numbers and lists.

To refine your abstract specification, you build a refinement between the abstract Hand specification and the List-based specification. When all types and operations are refined to concrete library-defined types and operations, the Specware system can generate code from the specification.

## 2.5 Reasoning about your code

Writing software in Metaslang, the specification and programming language used in Specware, brings many advantages. Along with the previously-mentioned possibilities for incremental development, you have the option to perform rigorous verification of the design and implementation of your code, leading to the a high level of assurance in the correctness of the final application.

### 2.5.1 Abstractness in Specware

Specware allows you to work directly with abstract concepts independently of implementation decisions. You can put off making implementation decisions by describing the problem domain in general terms, specifying only those properties you need for the task at hand.

In most languages, you can declare either everything about a function or nothing about it. That is, you can declare only its type, or its complete definition. In Specware you must declare the signature of an operation, but after that you have almost complete freedom in stating properties of the operation. You can declare nothing or anything about it. Any properties you have stated can be used for program transformation.

For example, you can describe how squaring distributes over multiplication:

```
axiom square_distributes_over_times is
  fa(a, b) square(a * b) = square(a) * square(b)
```

This property is not a complete definition of the squaring operation, but it is true. The truth of this axiom must be preserved as you refine the operation. However, unless you are going to generate code for `square`, you do not need to supply a complete definition.

The completeness of your definitions determines the extent to which you can generate code. A complete refinement must completely define the operations of the source theory in terms of the target theory. This guarantees that, if the target is implementable, the source is also implementable.

### 2.5.2 Logical inference in Specware

Specware performs inference using external theorem provers; the distribution includes SRI's SNARK theorem prover. External provers are connected to Specware through logic morphisms, which relate logics to each other.

You can apply external reasoning agents to refinements in different ways (although only verification is fully implemented in the current release of Specware).

- Verification tests the correctness of a refinement. For example, you can prove that quicksort is a correct refinement of the sorting specification.
- Simplification is a complexity-reducing refinement. For example, given appropriate axioms, you can rewrite  $3*a+3*b$  to  $3*(a+b)$ .
- Synthesis derives a refinement for a given specification by combining the domain theory with computational theory. For example, you can derive quicksort semi-automatically from the sorting specification as a solution to a sorting problem, if you describe exactly how the problem is a sorting problem.

# METASLANG

This chapter introduces the Metaslang specification language.

The following sections give the grammar rules and meaning for each Metaslang language construct.

## 3.1 Preliminaries

### 3.1.1 The Grammar Description Formalism

The grammar rules used to describe the Metaslang language use the conventions of (extended) BNF. For example, a grammar rule like:

```
wiffle ::= waffle [ waffle_tail ] |  
         piffle { + piffle }*
```

defines a **wiffle** to be: either a **waffle** optionally followed by a **waffle\_tail**, or a sequence of one or more **piffles** separated by terminal symbols **+**. (Further rules would be needed for **waffle**, **waffle\_tail** and **piffle**.) In a grammar rule the left-hand side of **::=** shows the kind of construct being defined, and the right-hand side shows how it is defined in terms of other constructs. The sign **|** separates alternatives, the square brackets **[ ... ]** enclose optional parts, and the curly braces plus asterisk **{ ... }\*** enclose a part that may be repeated any number of times, including zero times. All other signs stand for themselves, like the symbol **+** in the example rule above.

In the grammar rules terminal symbols appear in a bold font. Some of the terminal symbols used, like **|** and **{**, are very similar to the grammar signs like **|** and **{** as described above. They can hopefully be distinguished by their bold appearance.

Grammar rules may be *recursive*: a construct may be defined in terms of itself, directly or indirectly. For example, given the rule:

```
piffle ::= 1 |  
         M { piffle }*
```

here are some possible **piffles**:

1            M            M1            M111            MMMM            M1M1

Note that the last two examples of **piffles** are ambiguous. For example, **M1M1** can be interpreted as: **M** followed by the two **piffles** **1** and **M1**, but also as: **M** followed by the three **piffles** **1**, **M**, and another **1**. Some of the actual grammar rules allow ambiguities; the accompanying text will indicate how they are to be resolved.

### 3.1.2 Models

`op ::= op_name`

In Metaslang, “`op`” is used as an abbreviation for “`op_name`”, where `op_names` are declared names representing values. (*Op* for *operator*, a term used for historical reasons, although including things normally not considered operators.)

`spec ::= spec_form`

The term `spec` is used as short for `spec_form`. The *semantics* of Metaslang `specs` is given in terms of classes of *models*. A model is an assignment of “types” to all the `type_names` and of “typed” values to all the `ops` declared – explicitly or implicitly – in the `spec`. The notion of *value* includes numbers, strings, arrays, functions, et cetera. Each type has a set of “inhabitants”, which are similar values. A typed value can be thought of as a pair  $(T, V)$ , in which  $T$  is a type and  $V$  is a value that is an inhabitant of  $T$ . For example, the expressions `0 : Nat` and `0 : Integer` correspond, semantically, to the typed values  $(N, 0)$  and  $(Z, 0)$ , respectively, in which  $N$  stands for the type of natural numbers  $\{0, 1, 2, \dots\}$ , and  $Z$  for the type of integers  $\{\dots, -2, -1, 0, 1, 2, \dots\}$ . For example, given this `spec`:

```
spec
  type Even
  op next : Even -> Even
  axiom nextEffect is
    fa(x : Even) ~ (next x = x)
end-spec
```

one possible model (out of many!) is the assignment of the even integers to `Even`, and of the function that increments an even number by 2 to `next`.

Each model has to *respect typing*; for example, given the above assignment to `Even`, the function that increments a number by 1 does not map all even numbers to even numbers, and therefore can not – in the same model – be assigned to `next`. Additionally, the `claims` (axioms, theorems and conjectures) of the `spec` have to be satisfied in the model. The axiom labeled `nextEffect` above states that the function assigned to `op next` maps any value of the type assigned to `type_name` `Even` to a different value. So the squaring function, although type-respecting, could not be assigned to `next` since it maps 0 to itself.

If all type-respecting combinations of assignments of types to `type_names` and values to `ops` fail the one or more `claims`, the `spec` has no models and is called *inconsistent*. Although usually undesirable, an inconsistent `spec` is not by itself considered ill formed. The Specware system does not attempt to detect inconsistencies, but associated provers can sometimes be used to find them. Not always; in general it is undecidable whether a `spec` is consistent or not.

In general, the meaning of a construct in a model depends on the assignments of that model, and more generally on an *environment*: a model possibly extended with assignments to `local_variables`. For example, the meaning of the `claim` `fa(x : Even) ~ (next x = x)` in axiom `nextEffect` depends on the meanings of `Even` and `next`, while the sub-expression `next x`, for example, also depends on an assignment (of an “even” value) to `x`. To avoid laborious phrasings, the semantic descriptions use language like “the function `next` applied to `x`” as shorthand for this lengthy phrase: “the function assigned in the environment to `next` applied to the value assigned in the environment to `x`”.

When an environment is extended with an assignment to a `local_variable`, any assignments to synonymous `ops` or other `local_variables` are superseded by the new assignment in the new environment. In terms of Metaslang text, within the scope of the binding of `local_variables`, synonymous `ops` and earlier introduced `local_variables` (that is, having the same `simple_name`) are “hidden”; any use of the `simple_name` in that scope refers to the textually most recently introduced `local_variable`. For example, given:

```

op x : String = "op-x"
op y : String = let v = "let-v" in x
op z : String = let x = "let-x" in x

```

the value of `y` is "op-x" (`op x` is not hidden by the `local_variable` `v` of the `let_binding`), whereas the value of `z` is "let-x" (`op x` is hidden by the `local_variable` `x` of the `let_binding`).

### 3.1.3 Type-correctness

Next to the general requirement that each model respects typing, there are specific restrictions for various constructs that constrain the possible types for the components. For example, in an `application` `f(x)`, the type of the `actual_parameter` `x` has to match the domain type of function `f`. These requirements are stated in the relevant sections of this language manual. If no type-respecting combinations of assignments meeting all these requirements exist for a given `spec`, it is considered *type-incorrect* and therefore *ill formed*. This is determined by Specware while elaborating the `spec`, and signaled as an error. Type-incorrectness differs from inconsistency in that the meaning of the `claims` does not come into play, and the question whether an ill-formed `spec` is consistent is moot.

To be precise, there are subtle and less subtle differences between type-incorrectness of a `spec` and its having no type-respecting combinations of assignments. For example, the following `spec` is type-correct but has no models:

```

spec
  type Empty = | Just Empty
  op IdoNotExist : Empty
end-spec

```

The explanation is that the `type_definition` for `Empty` generates an *implicit* axiom that all inhabitants of the type `Empty` must satisfy, and for this recursive definition the axiom effectively states that such creatures can't exist: the type `Empty` is uninhabited. That by itself is no problem, but precludes a type-respecting assignment of an inhabitant of `Empty` to `op IdoNotExist`. So the `spec`, while type-correct, is actually inconsistent. See further under *Type-definitions*.

Here is a type-incorrect `spec` that has type-respecting combinations of assignments:

```

spec
  type Outcome = | O.Positive | O.Negative
  type Sign = | S.Positive | S.Zero | S.Negative
  def whatAmI = Positive
end-spec

```

Here there are two constructors `O.Positive` and `S.Positive` of different types, the type `Outcome` and the type `Sign` respectively. That by itself is fine, but when such “overloaded” constructors are used without a `qualifier`, the context must give sufficient information which is meant. Here, the use of `Positive` in the `definition` for `op whatAmI` may refer to either `O.Positive` or `S.Positive`; as used it is *type-ambiguous*. Metaslang allows omitting type information provided that, given a type assignment to all `local_type_variables` in scope, unique types for all typed constructs, such as expressions and patterns, can be inferred from the context. If no complete and unambiguous type-assignment can be made, the `spec` is not accepted by the Specware system. Type-ambiguous expressions can be disambiguated either by using the full qualified name or by using a `type_annotation`, as described under *Annotated-expressions*. In the example, the `definition` of `whatAmI` can be disambiguated in any of the following ways:

```

def whatAmI : Sign = Positive
def whatAmI = Positive : Sign
def whatAmI = S.Positive

```

Also, if the `spec` elsewhere contains something along the lines of:

```
op signToNat : Sign -> Nat
def sw = signToNat whatAmI
```

that is sufficient to establish that `whatAmI` has type `Sign` and thereby disambiguate the use of `Positive`. See further under *Op-definitions* and *Structors*.

### 3.1.4 Constructive

When code is generated for a *spec*, complete “self-contained” code is only generated for `type_definitions` and `op_definitions` that are fully *constructive*. Non-constructiveness is “contagious”: a *definition* is only constructive if all components of the definition are. The type of a *type\_name* without *definition* is not constructive. A type is only constructive if all component types are. An *op* without *definition* is non-constructive, and so is an *op* whose type is non-constructive. A *quantification* is non-constructive. The polymorphic *inbuilt\_op* `=` for testing equality and its inequality counterpart `~=` are only constructive for *discrete types* (see below).

A type is called discrete if the equality predicate `=` for that type is constructive. The inbuilt and base-library types `Bool`, `Integer`, `NonZeroInteger`, `Nat`, `PosNat`, `Char`, `String` and `Compare` are all discrete. Types `List T` and `Option T` are discrete when `T` is. All function types are non-discrete (even when the domain type is the unit type). Sum types, product types and record types are discrete whenever all component types are. Subtype  $(T|P)$  is discrete when supertype `T` is. (Predicate `P` need not be constructive: the equality test is that of the supertype.) Quotient type  $T/Q$  is discrete when predicate `Q` is constructive. (Type `T` need not be discrete: the equality test on the quotient type is just the predicate `Q` applied to pairs of members of the `Q`-equivalence classes.)

## 3.2 Lexical conventions

A Metaslang text consists of a sequence of *symbols*, possibly interspersed with whitespace. The term *whitespace* refers to any non-empty sequence of spaces, tabs, newlines, and *comments* (described below). A *symbol* is presented in the text as a sequence of one or more “marks” (ASCII characters). Within a composite (multi-mark) *symbol*, as well as within a *unit\_identifier*, no whitespace is allowed, but whitespace may be needed between two *symbols* if the first mark of the second *symbol* could be taken to be the continuation of the first *symbol*. More precisely, letting `X`, `Y` and `Z` stand for arbitrary (possibly empty) sequences of marks, and `m` for a single mark, then whitespace is required between two adjacent *symbols*, the first being `X` and the second `mY`, when for some `Z` the sequence `XmZ` is also a *symbol*. So, for example, whitespace is required where shown in `succ 0` and `op! : Nat->Nat`, since `succ0` and `! :` are valid *symbols*, but none is required in the *expression* `n+1`.

Inside *literals* (constant-denotations) whitespace is also disallowed, except for “*significant\_whitespace*” as described under *String-literals*.

Other than that, whitespace – or the lack of it – has no significance. Whitespace can be used to lay-out the text for readability, but as far as only the meaning is concerned, the following two presentations of the same *spec* are entirely equivalent:

```
spec
  type Even
  op next : Even -> Even
  axiom nextEffect is
    fa(x : Even) ~(next x = x)
end-spec

spec type Even op next : Even -> Even axiom nextEffect
is fa(x : Even) ~(next x = x) end-spec
```

### 3.2.1 Symbols and Names

```

symbol          ::=  simple_name |
                    literal |
                    special_symbol

simple_name      ::=  first_syllable { _ next_syllable }*
first_syllable  ::=  first_word_syllable |
                    non_word_syllable
next_syllable   ::=  next_word_syllable |
                    non_word_syllable
first_word_syllable ::= word_start_mark { word_continue_mark }*
next_word_syllable ::= word_continue_mark { word_continue_mark }*
word_start_mark ::= letter
word_continue_mark ::= letter | decimal_digit | ` | ?
letter          ::=  A | B | C | D | E | F |
                    G | H | I | J | K | L |
                    M | N | O | P | Q | R |
                    S | T | U | V | W | X |
                    Y | Z | a | b | c | d |
                    e | f | g | h | i | j |
                    k | l | m | n | o | p |
                    q | r | s | t | u | v |
                    w | x | y | z
decimal_digit   ::=  0 | 1 | 2 | 3 | 4 | 5 |
                    6 | 7 | 8 | 9
non_word_syllable ::= non_word_mark { non_word_mark }*
non_word_mark   ::=  ` | ~ | ! | @ | $ | ^ |
                    & | * | - | = | + | \ |
                    " | " | : | < | > | / | ` |
                    ?
special_symbol   ::=  _ | ( | ) | "[" | "]" |
                    "{" | "}" | ; | , | .

```

Sample simple\_names:

```

Date          **$*          ?!
yymmdd2date   <*>          :=:
well_ordered? ~==          x'
c_<+>         /_47a

```

For convenience, here are the 13 printing ASCII marks that, next to letters and decimal\_digits, can *not* occur as a non\_word\_mark:

```

#    %    "    _    ;    ,    .
(    )    [    ]    {    }

```

**Restriction.** As mentioned before, no whitespace is allowed in symbols: while anode is a single simple\_name, both a node and an ode consist of two simple\_names. Further, the case (lower or upper) of letters in simple\_names is significant: grandparent, grandParent and grandpaRent are three different simple\_names.

**Restriction.** In general, simple\_names can be chosen freely. However, the following *reserved symbols* have a special meaning and must not be used for simple\_names:

```

as      embed      from      let      quotient
axiom   embed?     generate  morphism  spec

```

by	endspec	if	obligations	the
case	ex	import	of	then
choose	ex1	in	op	theorem
conjecture	fa	infixl	project	true
def	false	infixr	prove	type
else	fn	is	qualifying	where

  

:			=	<=>	<-	<<
::	&&	~=	=>	->	+>	

They each count as a single `symbol`, and no whitespace is allowed inside any reserved symbol.

`Non_word_syllables` can be used to choose convenient `simple_names` for ops that, conventionally, are written with non-alphabetic marks.

Some Metaslang users follow the convention of using `simple_names` that start with a capital letter for `unit_identifiers` and `type_names` and for constructor ops, while `simple_names` chosen for non-constructor ops and `field_names` start with a lower-case `letter`. Both plain `local_variables` and `local_type_variables` are often chosen to be single lower-case letters: x, y, z, a, b, c, with the start of the alphabet preferred for `local_type_variables`. Op\_names of predicates (that is, having some type  $T \rightarrow \text{Bool}$ ) often end with the mark `?`. These are just conventions that users are free to follow or ignore.

### 3.2.2 Comments

```
comment           ::=  line_end_comment |
                        block_comment
line_end_comment  ::=  % line_end_comment_body
line_end_comment_body ::=  any_text_up_to_end_of_line
block_comment     ::=  (* block_comment_body *)
block_comment_body ::=  any_text_including_newlines_and_nested_block_comments
```

Sample comments:

```
% keys must be unique
(* op yymmdd2Date : String -> Date *)
```

Metaslang allows two styles of `comments`. The `%`-style is light-weight, for adding comment on a line *after* the formal text (or taking a line on its own, but always confined to a single line). The `(*...*)`-style can be used for blocks of text, spanning several lines, or stay within a line. Any text remaining on the line after the closing `*)` is processed as formal text. `Block_comments` may be nested, so the pairs of brackets `(*` and `*)` must be balanced.

A `block_comment` can not contain a `line_end_comment` and vice versa: whichever starts first has “the right of way”. For example, `(* 100 % or more! *)` is a `block_comment` with `block_comment_body` `100 % or more! .` The `%` here is a mark like any other; it does not introduce a `line_end_comment`. Conversely, in the `line_end_comment` `% op <*>` stands for `(*)` the `(*` is part of the `line_end_comment_body`; it does not introduce a `block_comment`. Note also that `%` and `(*` have no special significance in literals (which must not contain whitespace, including comments): `"100 % or more!"` is a well-formed `string_literal`.

## 3.3 Units

A “unit” is an identifiable `unit_term`, where “identifiable” means that the `unit_term` can be referred to by a `unit_identifier`. `Unit_terms` can be “elaborated”, resulting in `specs`, `morphisms`, `diagrams` or other enti-



ties. The effect of elaborating a `unit_definition` is that its `unit_term` is elaborated and becomes associated with its `unit_identifier`.

For the elaboration of a `unit_term` to be meaningful, it has to be well formed and result in a well-formed – and therefore type- correct – entity. Well-formedness is a stricter requirement than type-correctness. If a `unit_term` or one of its constituent parts does not meet any of the restrictions stated in this language manual, it is ill formed. This holds throughout, also if it is not mentioned explicitly for some syntactic construct. Well-formedness is more than a syntactic property; in general, to establish well- formedness it may be necessary to “discharge” (prove) proof obligations engendered by the `unit_term`.

A Specware project consists of a collection of Metaslang `unit_definitions`. They can be recorded in one or more Specware files. There are basically two styles for recording `unit_definitions` using Specware files. In the single-unit style, the file, when processed by Specware, contributes a single `unit_definition` to the project. In the multiple-unit style, the file may contribute several `unit_definitions`. The two styles may be freely mixed in a project (but not in the same Specware file). This is explained in more detail in what follows.

```

unit_definition      ::=  unit_identifier = unit_term
unit_term            ::=  spec_term |
                           morphism_term |
                           diagram_term |
                           target_code_term |
                           proof_term
specware_file_contents ::=  unit_term |
                           infile_unit_definition { infile_unit_definition }*
infile_unit_definition ::=  fragment_identifier = unit_term
fragment_identifier  ::=  simple_name

```

`Unit_definitions` may use other `unit_definitions`, including standard libraries, which in Specware 4.2 are supposed to be part of each project. However, the dependencies between units must not form a cycle; it must always be possible to arrange the `unit_definitions` in an order in which later `unit_definitions` only depend on earlier ones. How `unit_definitions` are processed by Specware is further dealt with in the Specware User Manual.

As mentioned above, `unit_definitions` are collected in Specware files, which in Specware 4.2 must have an `.sw` extension. The Specware files do not directly contain the `unit_definitions` that form the project. In fact, a user never writes `unit_definition` explicitly. These are instead determined from the contents of the Specware files using the following rules. There are two possibilities here. The first is that the `specware_file_contents` consists of a single `unit_term`. If `*P*.sw` is the path for the Specware file, the unit being defined has as its `unit_identifier` `P`. For example, if file `C:/units/Layout/Fixture.sw` contains a single `unit_term` `U`, the `unit_identifier` is `/units/Layout/Fixture`, and the `unit_definition` it contributes to the project is

```
/units/Layout/Fixture = *U*
```

(Note that this is not allowed as an `infile_unit_definition` in a `specware_file_contents`, since the `unit_identifier` is not a `fragment_identifier`.)

The second possibility is that the Specware file contains one or more `infile_unit_definitions`. If `I` is the `fragment_identifier` of such an `infile_unit_definition`, and `*P*.sw` is the path for the Specware file, the unit being defined has as its `unit_identifier` `P##I`. For example, if file `C:/units/Layout/Cart.sw` contains an `infile_unit_definition` `Pos =U`, the `unit_identifier` is `/units/Layout/Cart#Pos`, and the `unit_definition` it contributes to the project is

```
/units/Layout/Cart#Pos = *U*
```

### 3.3.1 Unit Identifiers

```
unit_identifier ::= swpath_based_path |
                  relative_path
swpath_based_path ::= / relative_path
relative_path ::= { path_element / } * path_element [ # fragment_identifier ]
path_element ::= path_mark { path_mark } *
path_mark ::= letter | decimal_digit |
             ! | * | & | " | + |
             - | = |
             @ | ^ | ` | ~ | .
```

Unit\_identifiers are used to identify unit\_terms, by identifying files in a file store that contain unit\_terms or infile\_unit\_definitions. Which path\_marks can actually be used in forming a path\_element may depend on restrictions of the operating system. The path\_elements .. and . have special meanings: “parent folder” and “this folder”. Under than this use, the mark . should not be used as the first or last path\_mark of a path\_element.

Typically, only a final part of the full unit\_identifier is used. When Specware is started with environment variable SWPATH set to a semicolon-separated list of pathnames for directories, the Specware files are searched for relative to these pathnames; for example, if SWPATH is set to C:/units/Layout;C:/units/Layout/Cart, then C:/units/Layout/Fixture.sw may be shortened to /Fixture, and C:/units/Layout/Cart.sw to /Cart. How unit\_definitions are processed by Specware is further dealt with in the Specware User Manual.

Further, unit\_identifiers can be relative to the directory containing the Specware file in which they occur. So, for example, both in file C:/units/Layout/Fixture.sw and in file C:/units/Layout/Cart.sw, unit\_identifier Tools/Pivot refers to the unit\_term contained in file C:/units/Layout/Tools/Pivot.sw, while Props#SDF refers to the unit\_term of infile\_unit\_definition SDF = ... contained in file C:/units/Layout/Props.sw. As a special case, a unit\_term with the same name as the file may be referenced without a fragment\_identifier. For example, in the current case, if the file C:/units/Layout/Props.sw contains the unit\_term of infile\_unit\_definition Props = ..., then this unit\_term can be referred to either by Props#Props or Props.

The unit\_identifier must identify a unit\_definition as described above; the elaboration of the unit\_identifier is then the result of elaborating the corresponding unit\_term, yielding a spec, morphism, diagram, or other entity.

### 3.3.2 Specs

```
spec_term ::= unit_identifier |
              spec_form |
              spec_qualification |
              spec_translation |
              spec_substitution |
              diagram_colimit |
              obligator
```

Restriction. When used as a spec\_term, the elaboration of a unit\_identifier must yield a spec.

The elaboration of a spec\_term, if defined, yields an “expanded” spec\_form as defined in the next subsection.

## Spec Forms

```
spec_form ::= spec { declaration }* end-spec
```

Sample spec\_forms:

```
spec import Measures, Value end-spec
```

An *expanded spec\_form* is a `spec_form` containing no `import_declarations`.

The elaboration of a `spec_form` yields the Metaslang text which is that `spec` itself, after expanding any `import_declarations`. The *meaning* of that text is the class of models of the `spec`, as described throughout this Chapter.

## Qualifications

Names of types and ops may be *simple* or *qualified*. The difference is that `simple_names` are “unqualified”: they do not contain a dot sign “.”, while `qualified_names` are prefixed with a “*qualifier*” followed by a dot. Examples of `simple_names` are `Date`, `today` and `<*>`. Examples of `qualified_names` are `Calendar.Date`, `Calendar.today` and `Monoid.<*>`.

Qualifiers can be used to disambiguate. For example, there may be reason to use two different ops called `union` in the same context: one for set union, and one for bag (multiset) union. They could then more fully be called `Set.union` and `Bag.union`, respectively. Unlike in earlier versions of Specware, there is no rigid relationship between `qualifiers` and the `unit_identifiers` identifying specs. The author of a collection of specs may use the `qualifier` deemed most appropriate for any `type_name` or `op_name`. For example, there could be a single `spec` dubbed `SetsAndBags` that introduces two new ops, one called `Set.union` and one called `Bag.union`. Generally, types and ops that “belong together” should receive the same `qualifier`. It is up to the author of the specs to determine what belongs together.

`Type_names` and `op_names` are *introduced* in a `declaration` or `definition`, and may then be *employed* elsewhere in the same `spec`. Thus, all occurrences of a `type_name` or `op_name` can be divided into “introductions” and “employs”. The `name` as introduced in an introduction is the *full name* of the type or op. If that `name` is a `simple_name`, the full name is a `simple_name`. If the `name` as introduced is a `qualified_name`, then so is the full `name`.

For employs the rules are slightly different. First, if the `name` employed occurs just like that in an introduction, then it is the full `name`. Also, if the `name` employed is qualified, it is the full `name`. Otherwise, the `name` as employed may be unqualified shorthand for a qualified full `name`. For example, given an employ of the unqualified `type_name` `Date`, possible qualified full names for it are `Calendar.Date`, `DateAndTime.Date`, `Diary.Date`, and so on. But, of course, the full `name` must be one that is introduced in the `spec`. If there is precisely one `qualified_name` introduced whose last part is the same as the `simple_name` employed, then that `name` is the full `name`. Otherwise, type information may be employed to disambiguate (“resolve overloading”).

Here is an illustration of the various possibilities:

```
spec
  type Apple
  type Fruit.Apple
  type Fruit.Pear
  type Fruit.Date
  type Calendar.Date
  type Fruit.Basket = Apple * Pear * Date
end-spec
```

In the definition of `type Fruit.Basket` we have three unqualified employs of `type_names`, viz. `Apple`, `Pear` and `Date`. The `name` `Apple` is introduced like that, so the employ `Apple` already uses the full `name`; it does not

refer to `Fruit.Apple`. The `name` `Pear` is nowhere introduced just like that, so the employ must be shorthand for some qualified full `name`. There is only one applicable introduction, namely `Fruit.Pear`. Finally, for `Date` there are two candidates: `Fruit.Date` and `Calendar.Date`. This is ambiguous, and in fact an error. To correct the error, the employ of `Date` should be changed into either `Fruit.Date` or `Calendar.Date`, depending on the intention.

It is possible to give a qualification in one go to all `simple_names` introduced in a `spec`. If  $Q$  is a `qualifier`, and  $S$  is a term denoting a `spec`, then the term  $Q$  qualifying  $S$  denotes the same `spec` as  $S$ , except that each introduction of an `simple_name`  $N$  is replaced by an introduction of the `qualified_name`  $Q.N$ . Employs that before referred to the unqualified introduction are also accordingly qualified, so that they now refer to the qualified introduction. For example, the value of

```
Company qualifying spec
  type Apple
  type Fruit.Apple
  type Fruit.Pear
  type Fruit.Basket = Apple * Pear
end-spec
```

is the same as that of

```
spec
  type Company.Apple
  type Fruit.Apple
  type Fruit.Pear
  type Fruit.Basket = Company.Apple * Fruit.Pear
end-spec
```

```
spec_qualification ::= qualifier qualifying spec_term
qualifier           ::= simple_name
name                ::= simple_name |
                      qualified_name
qualified_name      ::= qualifier . simple_name
```

**Restriction.** A `spec_qualification` is a special kind of translation, allowing for the renaming of `type_names` and `op_names` declared in a `spec`. Like for `spec_translations`, it is not allowed to rename a `type_name` to become the same `name` as a previously existing (and different) `type_name`, or to rename an `op_name` to become the same `name` as a previously existing (and different) `op_name`.

Sample names:

```
Key          **
Calendar.Date Monoid.<*>
```

Sample `spec_qualification`:

```
Weight qualifying /Units#Weights
```

Let  $R$  be the result of elaborating `spec_term`  $S$ . Then the elaboration of  $Q$  qualifying  $S$ , where  $Q$  is a `qualifier`, is  $R$  with each unqualified `type_name`, `op_name` or `claim_name`  $N$  introduced there replaced by the `qualified_name`  $Q.N$ . The same replacement applies to all employs of  $N$  identifying that introduced `simple_name`. As always, the result of the replacement is required to be a well-formed `spec`.

For example, the elaboration of

```
Buffer qualifying spec
  op size : Nat
  axiom LargeSize is size >= 1024
end-spec
```

results in:

```
spec
  op Buffer.size : Nat
  axiom Buffer.LargeSize is Buffer.size >= 1024
end-spec
```

Because of the restriction on collisions, the following is illegal, as `f` in the original `spec` would be renamed to collide with the pre-existing (and distinct!) `X.f`.

```
X qualifying spec
  op X.f : Nat
  def f = 3
end-spec
```

## Translations

```
spec_translation ::= translate spec_term by name_map
name_map         ::= "{" [ name_map_item { , name_map_item } * ] "}"
name_map_item    ::= type_name_map_item |
                    op_name_map_item |
                    wildcard_map_item

type_name_map_item ::= [ type ] name +-> name
op_name_map_item   ::= [ op ] annotable_name +-> annotable_name
annotable_name     ::= name [ type_annotation ]
type_annotation    ::= : type_descriptor
wildcard_map_item  ::= wildcard +-> wildcard
wildcard           ::= simple_wildcard |
                    qualified_wildcard

simple_wildcard     ::= _
qualified_wildcard ::= qualifier . simple_wildcard
```

**Restriction.** The `name_map` of a `spec_translation` may not contain more than one `name_map_item` pertaining to the same `type_name` or the same `op_name` in the `spec` resulting from elaborating the `spec_term`. For example, the following is not a lawful `spec_translation`:

```
translate spec type T end-spec by {T +-> A, T +-> B}
```

**Restriction.** A `spec_translation` may not map two different `type_names` or two different `op_names` to the same `simple_name`. Note that this implies that `type_names` and `op_names` cannot be translated to `simple_names` defined in the base libraries.

Sample `spec_translation`:

```
translate A by {Counter +-> Register, tally +-> incr}
```

Let  $R$  be the result of elaborating `spec_term`  $S$ . In elaborating a `spec_translation`, first any `wildcard_map_items` are expanded as follows. A `simple_wildcard` matches each `simple_name` that is a `type_name` or `op_name` of  $S$ . A `qualified_wildcard`  $Q.$  matches each `qualified_name` having the same `qualifier`  $Q$  that is a `type_name` or `op_name` of  $S$ . A `wildcard_map_item`  $W_0 +-> W_1$  is expanded into a list of `name_map_items` not containing wildcards by taking each `name`  $N$  matched by  $W_0$ , and replacing both `simple_wildcards` occurring in  $W_0 +-> W_1$  by the `simple_name` of  $N$ , that is,  $N$  with a possible qualification stripped off. After expansion, the elaboration of `translate`  $S$  by  $\{M_1 +-> N_1, \dots, M_n +-> N_n\}$  is  $R$  with each occurrence of a `name`  $M_i$  replaced by  $N_i$ . All other names are mapped to themselves, i.e., they are unchanged. The presence of a `type_annotation` in a `name_map_item`, as in  $E +-> \text{cross}$ ,

indicates that the `name_map_item` refers to an `op_name`; additionally, on the left-hand side such an annotation may serve to disambiguate between several synonymous `ops`, and then there must be an `op` in  $R$  of the type given by the `type_descriptor`. If the right-hand side of a `name_map_item` carries a type annotation, its `type_descriptor` must conform to the type of the `op_name` in the resulting `spec`. Without such annotation on either side, if a `name` to be translated is introduced both as a `type_name` and as an `op_name` in  $R$ , it must be preceded by `type` or `op` to indicate which of the two is meant. Otherwise the indication `type` or `op` is not required, but allowed; if present, it must correspond to the kind of `simple_name` (`type_name` or `op_name`) to be translated.

For example, the elaboration of

```
translate spec
  type E
  op i : E
end-spec by {
  E +-> Counter,
  i +-> reset
}
```

results in:

```
spec
  type Counter
  op reset : Counter
end-spec
```

To illustrate the use of wildcards: The elaboration of

```
translate spec
  type M.Length
  op M.+ infixl 25 : M.Length * M.Length -> M.Length
end-spec by {M._ +-> Measure._}
```

results in this `spec`:

```
spec
  type Measure.Length
  op Measure.+ infixl 25 :
    Measure.Length * Measure.Length -> Measure.Length
end-spec
```

A `spec_qualification`  $Q$  qualifying  $S$  is convenient shorthand for the `spec_translation` `translate  $S$  by {_ +->  $Q$ ._}`.

## Substitutions

```
spec_substitution ::= spec_term "[" morphism_term "]"
```

Sample `spec_substitution`:

```
Routing#Basis[morphism /Coll/Lattice ->
                /Coll/LatticeWithTop {} ]
```

The elaboration of `spec_substitution`  $S[M]$  yields the `spec`  $T$  obtained as follows. Let `spec`  $R$  be the result of elaborating  $S$ , and morphism  $N$  that of  $M$ . Let `specs`  $D$  and  $C$  be the domain and codomain of  $N$ . First, remove from  $R$  all declarations of  $D$ , and subject the result to the effect of  $N$ , meaning that all `name` translations of  $N$  and all extensions with declarations are performed. Then add the declarations of  $C$ , but without duplications, i.e., as if  $C$  is imported. The result obtained is  $T$ .

Restriction. Spec  $D$  must be a “sub-spec” of spec  $R$ , meaning that each declaration of  $D$  is also a declaration of  $R$ .

Informally,  $T$  is to  $R$  as  $C$  is to  $D$ .

Except when  $R$  introduces, next to the `type_names` and `op_names` it has in common with  $D$ , new `type_names` or `op_names` that also occur in  $C$ , the result spec  $T$  is a categorical colimit of this pushout diagram:

```

*D* -----> *R*
|             |
|             |
|             |
v             v
*C* -----> *T*

```

Although isomorphic to the result that would be obtained by using a `diagram_colimit`,  $T$  is more “user-oriented” in two ways: the names in  $T$  are names from  $C$ , and claims of  $D$  not repeated in  $C$  are not repeated here either.

For example, assume we have:

```

A = spec
  type Counter
  op reset : Counter
  op tally : Counter -> Counter
  axiom Effect is
    fa (c : Counter) ~(tally c = c)
end-spec

B = spec
  type Register = Nat
  def reset = 0
  def incr c = c+1
end-spec

M = morphism A -> B {Counter +-> Register, tally +-> incr}

AA = spec
  import A
  type Interval = {start: Counter, stop: Counter}
  op isEmptyInterval? : Interval -> Bool
  def isEmptyInterval? {start = x, stop = y} = (x = y)
end-spec

```

Then the result of `AA [M]` is the same as that of this spec:

```

spec
  import B
  type Interval = {start: Register, stop: Register}
  op isEmptyInterval? : Interval -> Bool
  def isEmptyInterval? {start = x, stop = y} = (x = y)
end-spec

```

## Diagram Colimits

```
diagram_colimit ::= colimit diagram_term
```

The result of elaborating a `diagram_colimit` is the spec which is the apex of the cocone forming the colimit in the category of specs and spec\_morphisms. As always, the result is required to be well formed. See further the Specware Tutorial.

## Obligators

```
obligator ::= obligations unit_term
```

Restriction. The `unit_term` of an `obligator` must either be a `spec_term` or a `morphism_term`.

The result of elaborating an `obligator` is a `spec` containing the proof obligations engendered by the `spec` or `morphism` resulting from elaborating its `unit_term`. These proof obligations are expressed as conjectures; they can be discharged by proving them, using `proof_terms`. See further the Specware User Manual.

### 3.3.3 Morphisms

```
morphism_term ::= unit_identifier |
                  spec_morphism
spec_morphism ::= morphism spec_term -> spec_term name_map
```

A morphism is a formal mapping between two expanded `spec_forms` that describes exactly how one is translated or extended into the other. It consists of the two `specs`, referred to as “domain” and “codomain”, and a mapping of all `type_names` and `op_names` introduced in the domain `spec` to `type_names` and `op_names` of the codomain `spec`. To be well-formed, a morphism must obey conditions that express that it is a proper refinement of the domain `spec` into the codomain `spec`.

Restriction. When used as a `morphism_term`, the elaboration of a `unit_identifier` must yield a morphism.

Restriction (“proof obligations”). Given `spec_morphism` `morphism S -> T { M1 +-> N1, . . . Mn +-> Nn }` let *R* be the result of elaborating *S*, and let *S'* be *R* with each occurrence of a `name` *M<sub>i</sub>* replaced by *N<sub>i</sub>*. The same rules apply as for `spec_translation` `translate S by { ... }`, and the result *S'* must be well formed, with the exception that the restriction on `spec_translations` requiring different `type_names` or `op_names` to be mapped to different `simple_names` does not apply here. Let *T'* be the result of elaborating *T*. Then, first, each `type_name` or `op_name` introduced in *S'* must also be introduced in *T'*. Further, no `type_name` or `op_name` originating from a library `spec` (or built in to Specware) may have been subject to translation. Finally, each `claim` in *S'* must be a theorem that follows from the `claims` of *T'*. Collectively, the `claims` in *S'* are known as the *proof obligations* engendered by the morphism. They are the formal expression of the requirement that the step from *S'* to *T'* is a proper refinement.

For example, in

```
S = spec end-spec
T = spec type Bullion = (Char | isAlpha) end-spec
M = morphism S -> T {Bool +-> Bullion}
```

the type-name `Bool`, which is built in to Specware, is subject to translation. Therefore, *M* is not a proper morphism. Further, in

```
S = spec
  op f : Nat -> Nat
  axiom ff is fa(n:Nat) f(n) ~= f(n+1)
end-spec

T = spec
  def f(n:Nat) = n*n rem 5
end-spec

M = morphism S -> T {}
```



axiom `ff` does not follow from (the axiom implied by) the `op_definition` for `f` in `spec T`, since  $f(2) = f(3) = 4$ . Therefore, `M` is not a proper morphism here either.

Sample `spec_morphism`:

```
morphism A -> B {Counter +-> Register, tally +-> incr}
```

The elaboration of `spec_morphism` `morphismS->T{M}` results in the morphism whose domain and codomain are the result of elaborating `S` and `T`, respectively, and whose mapping is given by the list of `name_map_items` in `M`, using `type_annotations` and indicators `type` and `op` as described for `spec_translations`, and extended to all domain `type_names` and `op_names` not yet covered by having these map to themselves. (In particular, `simple_names` from the base-libraries always map to themselves.)

### 3.3.4 Diagrams

```

diagram_term      ::=  unit_identifier |
                        diagram_form
diagram_form      ::=  diagram "{ " diagram_element { , diagram_element } * "}"
diagram_element   ::=  diagram_node |
                        diagram_edge
diagram_node      ::=  simple_name +-> spec_term
diagram_edge      ::=  simple_name : simple_name -> simple_name +-> morphism_term

```

Restriction. When used as a `diagram_term`, the elaboration of a `unit_identifier` must yield a diagram.

Restriction. In a `diagram_term`, the first `simple_name` of each `diagram_node` and `diagram_edge` must be unique (i.e., not be used more than once in that `diagram_term`). Further, for each `diagram_edge`  $E:ND \rightarrow NC \rightarrow M$ , there must be `diagram_nodes`  $ND \rightarrow D$  and  $NC \rightarrow C$  of the `diagram_term` such that, after elaboration,  $M$  is a morphism from  $D$  to  $C$ .

Sample `diagram_term`:

```

diagram {
  A          +-> /Coll/Lattice,
  B          +-> /Coll/LatticeWithTop,
  m : A -> B +-> /Coll/AddTop,
  C          +-> Routing#Basis,
  i : A -> C +-> morphism /Coll/Lattice ->
                        Routing#Basis {}
}

```

The result of elaborating a `diagram_form` is the categorical diagram whose nodes are labeled with the `specs` and whose edges are labeled with the morphisms that result from elaborating the corresponding `spec_terms` and `morphism_terms`.

### 3.3.5 Target Code Terms

```

target_code_term   ::=  generate target_language_name spec_term [ generate_option ]
generate_option    ::=  in string_literal |
                        with unit_identifier
target_language_name ::=  c |
                        java |
                        lisp

```

Sample `target_code_term`:

```
generate lisp /Vessel#Contour
      in "C:/Projects/Vessel/Contour.lisp"
```

The elaboration of a `target_code_term` for a well-formed `spec_term` generates code in the language suggested by the `target_language_name` (currently only C, Java, and Common Lisp); see further the Specware User Manual.

### 3.3.6 Proof Terms

```
proof_term      ::=  prove claim_name in spec_term
                  [ with prover_name ]
                  [ using claim_list ]
                  [ options prover_options ]
prover_name     ::=  snark
claim_list      ::=  claim_name { , claim_name }*
prover_options  ::=  string_literal
```

**Restriction.** The `claim_names` must occur as `claim_names` in the `spec` that results from elaborating the `spec_term`.

Sample `proof_term`:

```
prove Effect in obligations M
      options "(use-paramodulation t)"
```

The elaboration of a `proof_term` invokes the prover suggested by the `prover_name` (currently only SNARK). The property to be proved is the `claim` of the first `claim_name`; the `claim_list` lists the hypotheses (assumptions) that may be used in the proof. The `prover_options` are prover-specific and are not further described here. For details, see the Specware User Manual.

## 3.4 Declarations

```
declaration ::= import_declaration |
               type_declaration |
               op_declaration |
               claim_declaration |
               definition
definition  ::= type_definition |
               op_definition
equals     ::= is |
               =
```

Sample declarations:

```
import Lookup
type Key
type Key = String
op present : Database * Key -> Bool
def present(db, k) = embed? Some (lookup (db, k))
axiom norm_idempotent is fa(x) norm (norm x) = norm x
```

### 3.4.1 Import-declarations

A `spec` may contain one or more `import_declarations`. On elaboration, these are “expanded”. The effect is as if the bodies of these imported `specs` (themselves in elaborated form, which means that all `import_declarations` have been expanded, all translations performed and all shorthand employs of names have been resolved to full names, after which only declarations or definitions of types, ops and claims are left) is inserted in place in the receiving `spec`.

For example, the result of

```
spec
  import spec
      type A.Z
      op b : Nat -> Z
    end
  def A.Z = String
  def b = toString
end-spec
```

is this “expanded” `spec`:

```
spec
  type A.Z
  op b : Nat -> A.Z
  def A.Z = String
  def b = toString
end-spec
```

For this to be well formed, the imported `specs` must be well formed by themselves; in addition, the result of expanding them in place must result in a well-formed `spec`.

There are a few restrictions, which are meant to catch unintentional naming mistakes. First, if two different imported `specs` each introduce a type or `op` with the same (full) `name`, the introductions must be identical declarations or definitions, or one may be a declaration and the other a “compatible” definition. For example, given

```
S1 = spec op e : Integer end
S2 = spec op e : Char end
S3 = spec def e = 0 end
```

the `specs` `S1` and `S3` can be imported together, but all other combinations of two or more co-imported `specs` result in an ill-formed `spec`. This restriction is in fact a special case of the general requirement that import expansion must result in a well-formed `spec`. Secondly, a `type_name` introduced in any of the imported `specs` cannot be re-introduced in the receiving `spec` except for the case of an “imported” declaration together with a definition in the receiving `spec`. Similarly for `op_names`, with the addition that an `op_definition` in the receiving `spec` must be compatible with an `op_declaration` for the same `name` in an imported `spec`. The latter is again a special case of the general requirement that import expansion must result in a well- formed `spec`.

What is specifically excluded by the above, is giving a definition of a type or `op` in some `spec`, import it, and then redefining or declaring that type or `op` with the same full `name` in the receiving `spec`.

```
import_declaration ::= import spec_term { , spec_term }*
```

Sample `import_declaration`:

```
import Lookup
```

An `import_declaration` of the form `import S1 , ... , Sn`, where  $n > 1$ , is equivalent to the sequence of `import_declarations`:

```
import S1
...
import S2
```

An `import_declaration` is contained in some `spec_form`, and to elaborate that `spec_form` the `spec_terms` of its `import_declarations` are elaborated first, giving a sequence of `specs`. The `import_declaration` has then the effect as if the declarations of the imported `specs` as elaborated are expanded in place, replacing the `import_declaration`. This cascades: if `spec A` imports `B`, and `spec B` imports `C`, then effectively `spec A` also imports `C`. An important difference with earlier versions of Specware than version 4 is that multiple imports of the same `spec` have the same effect as a single import.

If `spec A` is imported by `B`, each model of `B` is necessarily a model of `A` (after “forgetting” any `simple_names` newly introduced by `B`). So `A` is then refined by `B`, and the morphism from `A` to `B` is known as the “import morphism”. As it does not involve translation of `type_names` or `op_names`, it can be denoted by `morphism A -> B { }`.

### 3.4.2 Type-declarations

```
type_declaration      ::=  type type_name
                        [ formal_type_parameters ]
formal_type_parameters ::=  local_type_variable |
                        ( local_type_variable_list )
local_type_variable   ::=  simple_name
local_type_variable_list ::=  local_type_variable { , local_type_variable }*
```

Restriction. Each `local_type_variable` of the `formal_type_parameters` must be a different `simple_name`.

Sample `type_declarations`:

```
type Date
type Array a
type Map(a, b)
```

Every `type_name` used in a `spec` must be declared or defined (in the same `spec` or in an imported `spec`, including the “base-library” `specs` that are always implicitly imported) in a `type_declaration` or `type_definition`. A `type_name` may have *type parameters*. Given the example `type_declarations` above, some valid `type_descriptors` that can be used in this context are `Array Date`, `Array (Array Date)` and `Map (Nat, Bool)`.

Restriction. Except for the exception provided in the next paragraph, `type_names` may not be redeclared and/or redefined, whether in the same `spec` or after having been declared/defined in an imported `spec`, not even when both declarations or definitions are identical.

In Specware 4.2, a type may be declared in a `type_declaration` and in the same context also be defined in a `type_definition`.

In a model of the `spec`, a type is assigned to each unparameterized `type_name`, while an infinite *family* of types is assigned to parameterized `type_names` “indexed” by tuples of types, that is, there is one family member, a type, for each possible assignment of types to the `local_type_variables`. So for the above example `type_declaration` of `Array` one type must be assigned to `Array Nat`, one to `Array Bool`, one to `Array (Array Date)`, and so on. These assigned types could all be the same type, or perhaps all different, as long as the model respects typing.

### 3.4.3 Type-definitions

```

type_definition      ::=  type_abbreviation | new_type_definition
type_abbreviation    ::=  type type_name
                        [ formal_type_parameters ] = type_descriptor
new_type_definition  ::=  type type_name
                        [ formal_type_parameters ] = new_type_descriptor

```

**Restriction.** Each `local_type_variable` of the `formal_type_parameters` must be a different `simple_name`.

Sample `type_abbreviations`:

```

type MyFun = Nat -> Nat
type MyProd = Nat * Nat
type MyProd2 = MyProd
type Date = {year : Nat, month : Nat, day : Nat}
type Array a = List a
type PosNat = (Nat | positive?)
type PosNat2 = {x:Nat | positive? x}
type Map(a, b) = (Array (a * b) | key_uniq?)

```

Sample `new_type_definitions`:

```

type Tree          a = | T.Leaf a | T.Fork (Tree a * Tree a)
type Bush          a = | B.Leaf a | B.Fork (Tree a * Tree a)
type Z3 = Nat / (fn (m, n) -> m rem 3 = n rem 3)

```

**Restriction.** If the `type_name` of a `type_definition` was previously declared in a `type_declaration`, either the `declaration` and `definition` both must contain no `formal_type_parameters`, or they must agree in the number of `local_type_variables` in their `formal_type_parameters`.

In each model, the type assigned to the `type_name` of a `type_abbreviation` must be the same as the right-hand-side `type_descriptor`, while that assigned to the `type_name` of a `new_type_definition` must be isomorphic to the type of the `new_type_descriptor`. Thus, while `Array Nat` and `List Nat` from the examples denote the same type, the types assigned to `Tree Nat` and `Bush Nat` are equivalent but not necessarily equal, and commingling them in a `spec` results in a type error.

For parameterized types, this extends to all possible assignments of types to the `local_type_variables`, taking the right-hand `type_descriptors` and `new_type_descriptors` as interpreted under each of these assignments. So, for the example, `Map(Nat, Char)` is the same type as `(Array (Nat * Char) | key_uniq?)`, and so on.

With *recursive* `type_definitions`, there are additional requirements. Consider

```

type Stack a =
  | Empty
  | Push {top : a, pop : Stack a}

```

This means that for each type `a` there is a value `Empty` of type `Stack a`, and further a function `Push` that maps values of type `{top : a, pop : Stack a}` to `Stack a`. Furthermore, the type assigned to `Stack a` must be such that all its inhabitants can be constructed *exclusively* and *uniquely* in this way: there is one inhabitant `Empty`, and all others are the result of a `Push`. Finally – this is the point – the type in the model must be such that its inhabitants can be constructed this way in a *finite number of steps*. So there can be no “bottom-less” stacks: deconstructing a stack using

```

op [a] hasBottom? (s : Stack a) : Bool =
  case s of

```

```

| Empty -> true
| Push {top, pop = rest} -> hasBottom? rest

```

is a procedure that is guaranteed to terminate, always resulting in `true`.

In general, `type_definitions` generate implicit axioms, which for recursive definitions imply that the type is not “larger” than necessary. In technical terms, in each model, the type is the least fixpoint of a recursive domain equation.

### 3.4.4 Op-declarations

```

op_declaration      ::= op [ type_variable_binder ] formal_expression
                        [ fixity ] type_annotation [ = expression ] |
                        op formal_expression [ fixity ]
                        polytype_annotation [ = expression ]
polytype_annotation ::= : type_variable_binder type_descriptor
type_variable_binder ::= "[" local_type_variable_list "]"
formal_expression   ::= op_name | formal_application
formal_application   ::= formal_application_head formal_parameter
formal_application_head ::= op_name | formal_application
formal_parameter     ::= closed_pattern |
                        "(" pattern "|" expression ")"
fixity               ::= associativity priority
associativity        ::= infixl | infixr
priority             ::= nat_literal

```

Note that the `formal_expression` of an `op_declaration` always uses prefix notation, even for `infix_operators`.

Sample `op_declarations`:

```

op usage : String

op usage : String = "Usage: Lookup key [database]"

op [a,b,c] o infixl 24 :          (b -> c) * (a -> b) -> a -> c
op          o infixl 24 : [a,b,c] (b -> c) * (a -> b) -> a -> c

op f (s : String) ((i, j) : Nat * Nat | i < j) (c : Char) : String =
  substring (s, i, j) ^ toString c

```

The placement of a `type_variable_binder`, if present, is of no significance; the two declarations given above for `op o` are completely equivalent. Note that the presence of a `type_annotation` or `polytype_annotation` is mandatory even if the type can be determined from a defining `expression`, as in the second example for `op usage` above.

The meaning of a `formal_parameter`  $(P|E)$  is the same as that of the `formal_parameter`  $((P) : \{(P) : T|E\})$ , in which  $T$  is a `type_descriptor` such that in the context the `annotated_pattern`  $(P) : T$  is type-correct. If no such `type_descriptor` exists, or its type cannot be unambiguously be determined, the `formal_parameter` is type- incorrect. For example, in the `declaration` for `f` above, the `formal_parameter`  $((i, j) : \text{Nat} * \text{Nat} | i < j)$  is a shorthand notation for  $((i, j) : \text{Nat} * \text{Nat}) : \{((i, j) : \text{Nat} * \text{Nat}) : \text{Nat} * \text{Nat} | i < j\})$ , which can be simplified to  $((i, j) : \{((i, j) : \text{Nat} * \text{Nat} | i < j)\})$ .

**Restriction.** The restricting `expression` following a vertical bar in a `formal-parameter` must not refer to local variables introduced by preceding `formal_parameters`. (To do so would effectively create dependent types, which are currently not supported.)

An `op_declaration` of the form `op B F X A = E`, in which  $B$  is an optional `type_variable_binder`,  $F$  is a `formal_expression`,  $X$  is an optional `fixity`,  $A$  is a `type_annotation` and  $E$  is an `expression`, is equivalent to the `op_declaration` `op B F X A` followed by the `op_definition` `def op B F = E`.

In an `op_declaration` of the form `op N : T`, in which  $N$  is an `op_name`,  $N$  is declared to have type  $T$ . An `op_declaration` of the form `op H (P : S) : T`, in which  $P$  is a `pattern` whose type is given by `type_descriptor`  $T$ , is equivalent to `op H : S → T`. So the `simple_names` used as `local_variables` in each `formal_parameter` are only bound to that `formal_parameter`, and are further irrelevant for its type. For example, the `op_declaration` of `f` above is equivalent to the following:

```
op f : String -> {(i, j) : Nat * Nat | i < j} -> Char -> String
def f s (i, j) c = substring (s, i, j) ^ toString c
```

in which the `type_annotations` in the `op_definition` have been omitted as being redundant.

**Restriction.** User-defined `ops` may not be “overloaded”, or otherwise be redeclared and/or redefined, whether in the same `spec` or after having been defined in an imported `spec`, not even when both declarations or definitions are identical.

However, one can get the effect of overloading by declaring distinct `ops` with different qualifiers for the same unqualified name, e.g.

```
op Table.length : Table -> Nat
op Vector.length : Vector -> Nat
```

Here, subsequent references of the form `length` may be resolved to refer to `Table.length` or `Vector.length` as appropriate, provided exactly one is type-consistent in the context of the reference.

An `op_declaration` introduces an `op` with an associated type. The type can be “monomorphic”, like `String`, or “polymorphic” (indicated by a `type_variable_binder`). In the latter case, an indexed family of values is assigned to parameterized `type_names` “indexed” by tuples of types, that is, there is one family member, a typed value, for each possible assignment of types to the `local_type_variables` of the `type_variable_binder`, and the type of that value is the result of the corresponding substitution of types for `local_type_variables` on the polymorphic type of the `op`. In the examples above, the two forms given for the declaration of polymorphic `o` are entirely equivalent; they can be thought of as introducing a family of (fictitious) `ops`, one for each possible assignment to the `local_type_variables`  $a, b$  and  $c$ .

```
oNat,String,Char : (String -> Char) * (Nat -> String) -> Nat -> Char
oNat,Nat,Bool : (Nat -> Bool) * (Nat -> Nat) -> Nat -> Bool
oChar,Bool,Nat : (Bool -> Nat) * (Char -> Bool) -> Char -> Nat
```

and so on. Any `op_definition` for `o` must be likewise accommodating.

Only binary `ops` (those having some type  $S * T \rightarrow U$ ) may be declared with a `fixity`. When declared with a `fixity`, the `op` may be used in infix notation, and then it is called an `infix_operator`. For `o` above, this means that `o (f, g)` and `f o g` may be used, interchangeably, with no difference in meaning. If the `associativity` is `infixl`, the `infix_operator` is called *left-associative*; otherwise, if the `associativity` is `infixr`, it is called *right-associative*. If the `priority` is `priorityN`, the operator is said to have *priority N*. The `nat_literal`  $N$  stands for a natural number; if `infix_operator`  $O1$  has priority  $N1$ , and  $O2$  has priority  $N2$ , with  $N1 < N2$ , we say that  $O1$  has *lower priority* than  $O2$ , and that  $O2$  has *higher priority* than (or *takes priority over*)  $O1$ . For the role of the `associativity` and `priority`, see further at [Applications](#).

### 3.4.5 Op-definitions

```
op_definition ::= def [ op ] [ type_variable_binder ] formal_expression [ type_annotation ]
               def [ op ] formal_expression polytype_annotation = expression
```

Sample `op_definitions`:

```
def op usage = "Usage: Lookup key [database]"

def [a,b,c] o(f : b -> c, g: a -> b) : a -> c =
  fn (x : a) -> f(g x)

def o : [a,b,c] (b -> c) * (a -> b) -> a -> c =
  fn (f, g) -> fn (x) -> f(g x)

def o (f, g) x = f(g x)
```

The keyword `op` may be omitted after `def` unless the part between the keyword `def` and the `=` has the syntactic form of a `name N` followed by an optional `formal_type_parameters`, where the `name N` is declared or defined in the context as a `type_name`. As for `op_declarations`, the placement of any `type_variable_binder` is of no significance.

Restriction. See the restriction under *Op-declarations* on redeclaring/redefining ops.

Note that a `formal_expression` always contains precisely one `op_name`, which is the `op` being defined by the `op_definition`. Note further that the `formal_expression` of an `op_definition` always uses prefix notation, even for `infix_operators`.

Restriction. The type information, if any, presented in an `op_definition` must be consistent with the type specified by the preceding `op_declaration`. For example, the presence of a `type_variable_binder` signals that the `op` being defined is polymorphic, but then the `op_declaration` must contain an identical `type_variable_binder`. (A `type_variable_binder` may be needed to introduce `local_type_variables` for employ in `type_annotations` within the defining `expression`, as exemplified in the first definition for `o`.)

In Specware 4.2, an `op` still may be defined without having been previously declared, but *this is now a deprecated feature*. When an `op` is defined without having been declared, the `op_definition` generates an implicit `op_declaration` for the `op`, provided a monomorphic type for the `op` can be unambiguously determined from the `op_definition` together with the uses of the `op` in applications and other contexts, so that all expressions can be assigned a type in the context in which they occur. This feature may not persist in future releases, so users are advised to provide an `op_declaration` somewhere before each `op_definition`, either in the same `spec` or (more typically) in an imported `spec`. Alternatively, the newly expanded syntax for `op_definitions` makes it simple to both give a unique type to and define an `op` within one `declaration`.

In a model of the `spec`, an indexed family of typed values is assigned to a polymorphic `op`, with one family member for each possible assignment of types to the `local_type_variables` of the `type_variable_binder`, and the type of that value is the result of the corresponding `type_instantiation` for the polymorphic type of the `op`. Thus, we can reduce the meaning of a polymorphic `op_definition` to a family of (fictitious) monomorphic `op_definitions`.

An `op_definition` with `formal_application`

```
def op *H* *P* = *E*
```

in which `H` is a `formal_application_head`, `P` is a `formal_parameter` and `E` an `expression`, is equivalent to the `op_definition`

```
def op *H* = fn *P* -> *E*
```

For example,

```
def o (f, g) x = f(g x)
```



is equivalent to

```
def o (f, g) = fn x -> f(g x)
```

which in turn is equivalent to

```
def o = fn (f, g) -> fn x -> f(g x)
```

By this deparameterizing transformation for each `formal_parameter`, an equivalent unparameterized `op_definition` is reached. The semantics is described in terms of such `op_definitions`.

In each model, the typed value assigned to the `op` being defined must be the same as the value of the right-hand-side `expression`. For polymorphic `op_definitions`, this extends to all possible assignments of types to the `local_type_variables`.

An `op_definition` can be thought of as a special notation for an axiom. For example,

```
op double : [a] a -> a * a
def double x = (x, x)
```

can be thought of as standing for:

```
op double : [a] a -> a * a

axiom double_def is
  [a] fa(x : a) double x = (x, x)
```

In fact, Specware generates such axioms for use by provers. But in the case of recursive definitions, this form of axiomatization does not adequately capture the meaning. For example,

```
def f (n : Nat) : Nat = 0 * f n
```

is an improper `definition`, while

```
axiom f_def is
  fa(n : Nat) f n = 0 * f n
```

characterizes the function that maps every natural number to 0. The issue is the following. Values in models can not be *undefined* and functions assigned to `ops` must be *total*. But in assigning a meaning to a recursive `op_definition`, we – temporarily – allow *undefined* and partial functions (functions that are not everywhere defined on their domain type) to be assigned to recursively defined `ops`. In the thus extended class of models, the recursive `ops` must be the least-defined solution to the “axiomatic” equation (the least fixpoint as in domain theory), given the assignment to the other `ops`. For the example of `f` above this results in the everywhere undefined function, since 0 times *undefined* is *undefined*. If the solution results in an undefined value or a function that is not total (or for higher-order functions, functions that may return non-total functions, and so on), the `op_definition` is improper. Although Specware 4.2 does attempt to generate proof obligations for this condition, it currently covers only “simple” recursion, and not mutual recursion or recursion introduced by means of higher-order functions.

Functions that are determined to be the value of an `expression`, but that are not assigned to `ops`, need not be total, but the context must enforce that the function can not be applied to values for which it is undefined. Otherwise, the `spec` is ill formed.

### 3.4.6 Claim-declarations

```
claim_declaration ::= claim_kind claim_name is claim [ proof_script ]
claim_kind        ::= axiom | theorem | conjecture
claim_name        ::= name
claim             ::= [ type_variable_binder ] expression
```

Sample `claim_declarations`:

```
axiom norm_idempotent is
  norm o norm = norm

theorem o_assoc is
  [a,b,c,d] fa(f : c -> d, g : b -> c, h : a -> b)
    f o (g o h) = (f o g) o h

conjecture pivot_hold is
  let p = pivot hold in
    fa (n : {n : Nat | n < p}) ~ (hold n = hold p)
```

`Proof_scripts` are currently only available for use with Isabelle, and are not described here. For further details, see the Specware to Isabelle Translator Manual.

**Restriction.** The type of the `claim` must be `Bool`.

**Restriction.** A `claim` must not be an `expression` whose first symbol is `[`. In order to use such an `expression` as a `claim`, it can be parenthesized, as in

```
axiom nil_fits_nil is ([ ] fits [ ])
```

This restriction prevents ambiguities between `claims` with and without `type_variable_binders`.

When a `type_variable_binder` is present, the `claim` is polymorphic. A polymorphic `claim` may be thought of as standing for an infinite family of monomorphic `claims`, one for each possible assignment of types to the `local_type_variables`.

The `claim_kind` theorem should only be used for `claims` that have actually been proved to follow from the (explicit or implicit) axioms. In other words, giving them axiom status should not change the class of models. Theorems can be used by provers.

Conjectures are meant to represent proof obligations that should eventually attain theoremhood. Like theorems, they can be used by provers. This is only sound if circularities (vicious circles) are avoided. This kind of `claim` is usually created automatically by the elaboration of an `obligator`, but can also be created manually.

The Specware system passes on the `claim_name` of the `claim_declaration` with the `claim` for purposes of identification. Both may be transformed to fit the requirements of the prover, and appear differently there. Not all `claims` can be faithfully represented in all provers, and even when they can, the logic of the prover may not be up to dealing with them.

**Remark.** It is a common mistake to omit the part “`claim_name` is” from a `claim_declaration`. A defensive style against this mistake is to have the `claim` always start on a new text line. This is additionally recommended because it may become required in future revisions of Metaslang.

## 3.5 Type-descriptors

```
type_descriptor      ::= type_arrow | slack_type_descriptor
new_type_descriptor  ::= type_sum | type_quotient
slack_type_descriptor ::= type_product | tight_type_descriptor
tight_type_descriptor ::= type_instantiation | closed_type_descriptor
closed_type_descriptor ::= type_name | Bool | local_type_variable |
                           type_record | type_restriction |
                           type_comprehension | ( type_descriptor )
```

Note that in Specware 4.2, `new_type_descriptors` now may appear only as the right-hand-side of a `type_definition`. In other words, sum and quotient types no longer may appear anonymously. For example, they may not be used in an `annotated_pattern` or an `annotated_expression`. Thus the following `spec` is no longer legal:

```
spec
  type T
  op f : T -> Nat
  op q : T * T -> Bool
  op q_f (x : T / q) : Nat = let quotient[T / q] y = x in f y
end-spec
```

but can be expressed legally as follows:

```
spec
  type T
  op f : T -> Nat
  op q : T * T -> Bool
  type Q = T / q
  op q_f (x : Q) : Nat = let quotient[Q] y = x in f y
end-spec
```

(The distinctions “`slack_`”, “`tight_`” and “`closed_`” before “`type_descriptor`” have no semantic significance. The distinction merely serves the purpose of diminishing the need for parenthesizing in order to avoid grammatical ambiguities.)

Sample `type_descriptors`:

```
List String * Nat -> Option String
a * Order a * a
PartialFunction (Key, Value)
Key
Bool
a
{center : XYpos, radius : Length}
(Nat | even)
{k : Key | present (db, k)}
(Nat * Nat)
```

Sample `new_type_descriptors`:

```
| Point XYpos | Line XYpos * XYpos
Nat / (fn (m, n) -> m rem 3 = n rem 3)
```

The meaning of the `type_descriptor` `Bool` is the “inbuilt” type inhabited by the two logical (truth) values `true` and `false`. The meaning of a parenthesized `type_descriptor` `( T )` is the same as that of the enclosed `type_descriptor` `T`.

The various other kinds of `type_descriptors` and `new_type_descriptors` not defined here are described each in their following respective sections, with the exception of `local_type_variable`, whose (lack of) meaning as a `type_descriptor` is described below.

**Restriction.** A `local_type_variable` may only be used as a `type_descriptor` if it occurs in the scope of a `formal_type_parameters` or `type_variable_binder` in which it is introduced.

**Disambiguation.** A single `simple_name` used as a `type_descriptor` is a `local_type_variable` when it occurs in the scope of a `formal_type_parameters` or `type_variable_binder` in which it is introduced, and then it identifies the textually most recent introduction. Otherwise, the `simple_name` is a `type_name`.

A `local_type_variable` used as a `type_descriptor` has no meaning by itself, and where relevant to the semantics is either “indexed away” (for parameterized types) or “instantiated away” (when introduced in a

`formal_type_parameters` or `type_variable_binder`) before a meaning is ascribed to the construct in which it occurs. Textually, it has a scope just like a plain `local_variable`.

### 3.5.1 Type-sums

```
type_sum      ::=  type_summand { type_summand }*
type_summand ::=  "|" constructor [ slack_type_descriptor ]
constructor   ::=  name
```

Sample `type_sum`:

```
| Point XYpos | Line XYpos * XYpos
```

**Restriction.** The constructors of a `type_sum` must all have different `simple_names` even if they have different qualifiers, so the following is illegal:

```
| Start.Point XYpos | End.Point XYpos * XYpos
```

Also, note that since a `type_sum` is a `new_type_descriptor`, it may appear only on the right hand side of a `new_type_definition`.

The ordering of the `type_summands` has no significance: `| Zero | Succ Peano` denotes the same “sum type” as `| Succ Peano | Zero`.

A `type_sum` denotes a *sum type*, which is a type that is inhabited by “tagged values”. A tagged value is a pair  $(C, v)$ , in which  $C$  is a `constructor` and  $v$  is a typed value.

A `type_sum` introduces a number of `constructor ops`, one for each `type_summand`, along with implicit axioms described below.

For a `type_sum`  $T$  with `type_summand`  $C$   $S$ , in which  $C$  is a `constructor` and  $S$  a `type_descriptor`, the corresponding `op` introduced is typed as follows:

```
op C : S -> T
```

It maps a value  $v$  of type  $S$  to the tagged value  $(C, v)$ . If the `type_summand` is a single *parameter-less constructor* (the `slack_type_descriptor` is missing), the `op` introduced is typed as follows:

```
op C : T
```

It denotes the tagged value  $(C, ())$ , in which  $()$  is the inhabitant of the unit type (see under *Type-records*).

The sum type denoted by the `type_sum` then consists of the union of the ranges (for parameter-less constructors the values) of the `ops` for all constructors.

The `constructor ops` are individually, jointly and severally *injective*, and jointly *surjective*.

This means, first, that for any pair of constructors  $C1$  and  $C2$  of any `type_sum`, and for any pair of values  $v1$  and  $v2$  of the appropriate type (to be omitted for parameter-less constructors), the value of  $C1\ v1$  is only equal to  $C2\ v2$  when  $C1$  and  $C2$  are the same `constructor`, and  $v1$  and  $v2$  are both absent or are the same value. In other words, whenever the `constructors` are different or the values are different, the results are different.

Secondly, for any value  $u$  of any sum type, there is a `constructor`  $C$  of that sum type and a value  $v$  of the appropriate type (to be omitted for parameter-less constructors), such that the value of  $C\ v$  is  $u$ . In other words, all values of a sum type can be constructed with an `constructor op`.

For example, consider

```

type Peano =
  | Zero
  | Succ Peano

```

This means that there is a value `Zero` of type `Peano`, and further a function `Succ` that maps values of type `Peano` to type `Peano`. Then `Zero` and `Succ n` are guaranteed to be different, and each value of type `Peano` is either `Zero : Peano`, or expressible in the form `Succ (n : Peano)` for a suitable [expression](#) `n` of type `Peano`. Subtypes of a type can only be made with a [type\\_restriction](#), for instance as in `(Peano | embed? Zero).` For recursively defined `type_sums`, see also the discussion under [Type-definitions](#).

### 3.5.2 Type-arrows

```

type_arrow    ::=  arrow_source -> type_descriptor
arrow_source  ::=  type_sum |
                  slack_type_descriptor

```

Sample `type_arrow`:

```
(a -> b) * b -> List a -> List b
```

In this example, the `arrow_source` is `(a -> b) * b`, and the (target) `type_descriptor` `List a -> List b`.

The function type  $S \rightarrow T$  is inhabited by precisely all *partial or total* functions from  $S$  to  $T$ . That is, function  $f$  has type  $S \rightarrow T$  if, and only if, for each value  $x$  of type  $S$  such that the value of  $f\ x$  is defined, that value has type  $T$ . Functions can be constructed with `lambda_forms`, and be used in applications.

In considering whether two functions (of the same type) are equal, only the meaning on the domain type is relevant. Whether a function is undefined outside its domain type, or might return some value of some type, is immaterial to the semantics of Metaslang. (For a type- correct [spec](#), the difference is unobservable.)

### 3.5.3 Type-products

```

type_product  ::=  tight_type_descriptor * tight_type_descriptor { * tight_type_descriptor

```

Sample `type_product`:

```
(a -> b) * b * List a
```

Note that a `type_product` contains at least two constituent `tight_type_descriptors`.

A `type_product` denotes a *product type* that has at least two “component types”, represented by its `tight_type_descriptors`. The ordering of the component types is significant: unless  $S$  and  $T$  are the same type, the product type  $S * T$  is different from the type  $T * S$ . Further, the three types  $(S * T) * U$ ,  $S * (T * U)$  and  $S * T * U$  are all different; the first two have two component types, while the last one has three. The inhabitants of the product type  $T_1 * T_2 * \dots * T_n$  are precisely all  $n$ -tuples  $(v_1, v_2, \dots, v_n)$ , where each  $v_i$  has type  $T_i$ , for  $i = 1, 2, \dots, n$ . Values of a product type can be constructed with `tuple_displays`, and component values can be extracted with `tuple_patterns` as well as with `projectors`.

### 3.5.4 Type-instantiations

```

type_instantiation      ::=  type_name actual_type_parameters
actual_type_parameters ::=  closed_type_descriptor |
                             ( proper_type_list )
proper_type_list        ::=  type_descriptor , type_descriptor { , type_descriptor }*

```

Sample `type_instantiation`:

```
Map (Nat, Bool)
```

**Restriction.** The `type_name` must have been declared or defined as a parameterized type (see *Type-declarations*), and the number of `type_descriptors` in the `actual_type_parameters` must match the number of `local_type_variables` in the `formal_type_parameters` of the `type_declaration` and/or `type_definition`.

The `type_descriptor` represented by a `type_instantiation` is the type assigned for the combination of types of the `actual_type_parameters` in the indexed family of types for the `type_name` of the `type_instantiation`.

### 3.5.5 Type-names

```
type_name ::= name
```

Sample `type_names`:

```
Key
Calendar.Date
```

**Restriction.** A `type_name` may only be used if there is a `type_declaration` and/or `type_definition` for it in the current `spec` or in some `spec` that is imported (directly or indirectly) in the current `spec`. If there is a unique `qualified_name` for a given unqualified ending, the qualification may be omitted for a `type_name` used as a `type_descriptor`.

The type of a `type_name` is the type assigned to it in the model. (In this case, the context can not have superseded the original assignment.)

### 3.5.6 Type-records

```

type_record      ::=  "{" [ field_typer_list ] "}" |
                       ( )
field_typer_list ::=  field_typer { , field_typer }*
field_typer      ::=  field_name type_annotation
field_name       ::=  simple_name

```

Sample `type_record`:

```
{center : XYpos, radius : Length}
```

**Restriction.** The `field_names` of a `type_record` must all be different.

Note that a `type_record` contains either no constituent `field_typer`s, or else at least two.

A `type_record` is like a `type_product`, except that the components, called “fields”, are identified by `name` instead of by position. The ordering of the `field_typer`s has no significance: `{center : XYpos, radius : Length}` denotes the same *record type* as `{radius : Length, center : XYpos}`.

Therefore we assume in the following, without loss of generality, that the fields are ordered lexicographically according to their `field_names` (as in a dictionary: `a` comes before `ab` comes before `b`) using some fixed collating order for all marks that may comprise a `name`. Then each field of a record type with  $n$  fields has a *position* in the range 1 to  $n$ . The inhabitants of the record type  $\{ F_1 : T_1, F_2 : T_2, \dots, F_n : T_n \}$  are precisely all  $n$ -tuples  $(v_1, v_2, \dots, v_n)$ , where each  $v_i$  has type  $T_i$ , for  $i = 1, 2, \dots, n$ . The `field_names` of that record type are the `field_names`  $F_1, \dots, F_n$ , and, given the lexicographic ordering, `field_name`  $F_i$  selects position  $i$ , for  $i = 1, 2, \dots, n$ . Values of a record type can be constructed with `record_displays`, and field values can be extracted with `record_patterns` and (as for product types) with `projectors`.

For the `type_record {}`, which may be equivalently written as `()`, the record type it denotes has zero components, and therefore no `field_names`. This zero-component type has precisely one inhabitant, and is called the *unit type*. The unit type may equally well be considered a product type, and is the only type that is both a product and a record type.

### 3.5.7 Type-restrictions

```
type_restriction ::= ( slack_type_descriptor "|" expression )
```

Sample `type_restriction`:

```
(Nat | even)
```

**Restriction.** In a `type_restriction`  $(T|P)$ , the `expression`  $P$  must be a predicate on the type  $T$ , that is,  $P$  must be a function of type  $T \rightarrow \text{Bool}$ .

Note that the parentheses in  $(T|P)$  are mandatory.

The inhabitants of type  $(T|P)$  are precisely the inhabitants of type  $T$  that satisfy the predicate  $P$ , that is, they are those values  $v$  for which the value of  $P\ v$  is `true`.

If  $P1$  and  $P2$  are the same function, then  $(T|P1)$  and  $(T|P2)$  are equivalent, that is, they denote the same type. Furthermore,  $(T| \text{fn } _ \rightarrow \text{true})$  is equivalent to  $T$ .

The type  $(T|P)$  is called a *subtype* of *supertype*  $T$ . Values can be shuttled between a subtype and its supertype and vice versa, in the direction from supertype to subtype only if the value satisfies predicate  $P$ .

For example, in the `expression` `-1` the `nat_literal` `1` of type `Nat` is implicitly “coerced” to type `Integer` to accommodate the unary negation operator `-`, which has type `Integer  $\rightarrow$  Integer`.

Likewise,

in the `expression` `7 div 2` the `nat_literal` `2` of type `Nat` is implicitly “coerced” to type `PosNat`, a subtype of `Nat`, to accommodate the division operator `div`, whose second argument has type `PosNat`. But note that this engenders the proof obligation that the value satisfies the predicate of the subtype.

These coercions extend to composed types. For example, an `expression` of type `List PosNat` may be used where a value of type `List Nat` is required. Conversely, an `expression` of type `List Nat` may be used in a context requiring `List PosNat` if the corresponding proof obligation can be discharged, namely that the value of the `expression`, in its context, satisfies the predicate `all posNat?` testing whether all elements of a list of naturals are positive.

### 3.5.8 Type-comprehensions

```
type_comprehension ::=  "{" annotated_pattern "|" expression "}"
```

Sample `type_comprehension`:

```
{n : Nat | even n}
```

Restriction. In a `type_comprehension`  $\{P:T|E\}$ , the `expression`  $E$  must have type `Bool`.

Type comprehensions provide an alternative notation for type restrictions that is akin to the common mathematical notation for set comprehensions. The meaning of `type_comprehension`  $\{P:T|E\}$  is the same as that of the `type_restriction`  $(T \mid \text{fn } P \rightarrow E)$ . So the meaning of the example `type_comprehension` above is  $(\text{Nat} \mid \text{fn } n \rightarrow \text{even } n)$ .

### 3.5.9 Type-quotients

```
type_quotient ::=  closed_type_descriptor / closed_expression
```

Sample `type_quotient`:

```
Nat / (fn (m, n) -> m rem 3 = n rem 3)
```

Restriction. In a `type_quotient`  $T/q$ , the `expression`  $q$  must be a (binary) predicate on the type  $T * T$  that is an equivalence relation, as explained below.

Also, note that since a `type_quotient` is a `new_type_descriptor`, it may appear only as the right-hand side of a `new_type_definition`.

Equivalence relation. Call two values  $x$  and  $y$  of type  $T$  “ $q$ -related” if  $(x, y)$  satisfies  $q$ . Then  $q$  is an *equivalence relation* if, for all values  $x, y$  and  $z$  of type  $T$ ,  $x$  is  $q$ -related to itself,  $y$  is  $q$ -related to  $x$  whenever  $x$  is  $q$ -related to  $y$ , and  $x$  is  $q$ -related to  $z$  whenever  $x$  is  $q$ -related to  $y$  and  $y$  is  $q$ -related to  $z$ . The equivalence relation  $q$  then partitions the inhabitants of  $T$  into *equivalence classes*, being the maximal subsets of  $T$  containing mutually  $q$ -related members. These equivalence classes will be called “ $q$ -equivalence classes”.

The inhabitants of the *quotient type*  $T / q$  are precisely the  $q$ -equivalence classes into which the inhabitants of  $T$  are partitioned by  $q$ . For the example above, there are three equivalence classes of natural numbers leaving the same remainder on division by 3: the sets  $\{0, 3, 6, \dots\}$ ,  $\{1, 4, 7, \dots\}$  and  $\{2, 5, 8, \dots\}$ , and so the quotient type has three inhabitants.



## 3.6 Expressions

```

expression      ::=  lambda_form | case_expression | let_expression |
                      if_expression | quantification | unique_solution |
                      annotated_expression | tight_expression

tight_expression ::=  application | closed_expression
closed_expression ::= op_name | local_variable | literal |
                      field_selection | tuple_display | record_display |
                      sequential_expression | list_display | monadic_expression |
                      structor | ( expression ) | ( inbuilt_op )

inbuilt_op      ::=  inbuilt_prefix_op |
                      inbuilt_infix_op

inbuilt_prefix_op ::= ~
inbuilt_infix_op  ::= <=> |
                      => |
                      "<|'|>" |
                      & |
                      = |
                      ~= |
                      |lt||lt|

```

(The distinctions `tight_` and `closed_` for expressions lack semantic significance, and merely serve the purpose of avoiding grammatical ambiguities.)

Sample expressions:

```

fn (s : String) -> s ^ "."
case z of {re = x, im = y} -> {re = x, im = -y}
let x = x + 1 in f(x, x)
if x <= y then x else y
fa(x,y) (x <= y) <=> ((x<y) or (x = y))
f(x, x)
[] : List Arg
abs(x-y)
++
x
3260
z.re
("George", Poodle : Dog, 10)
{name = "George", kind = Poodle : Dog, age = 10}
(writeLine "key not found"; embed Missing)
["Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"]
project 2
(n + 1)
(())

```

**Restriction.** Like all polymorphic or type-ambiguous constructs, an `expression` can only be used in a context if its type can be inferred uniquely, given the `expression` and the context. This restriction will not be repeated for the various kinds of expressions defined in the following subsections.

The meaning of a parenthesized `expression` ( $E$ ) is the same as that of the enclosed `expression`  $E$ . The meaning of the parenthesized `inbuilt_prefix_op` ( $P$ ) is the same as that of the `lambda_form` `fn x -> P x`. The meaning of a parenthesized `inbuilt_infix_op` ( $I$ ) is the same as that of the `lambda_form` `fn (x, y) -> x I y`. Note that this function is strict in both arguments, unlike  $I$  itself.

The various other kinds of expressions not defined here are described each in their following respective sections,

with the exception of `local_variable`, whose meaning as an `expression` is described below.

**Restriction.** A `local_variable` may only be used as an `expression` if it occurs in the scope of the `local_variable_list` of a quantification or of a `variable_pattern` in which it is introduced.

**Disambiguation.** A single `simple_name` used as an `expression` is a `local_variable` when it occurs in the scope of a `local_variable_list` or `variable_pattern` in which a synonymous `local_variable` is introduced, and then it identifies the textually most recent introduction. Otherwise, the `simple_name` is an `op_name`.

A `local_variable` used as an `expression` has the typed value assigned to it in the environment.

### 3.6.1 Lambda-forms

```
lambda_form ::= fn match
```

Sample `lambda_forms`:

```
fn (s : String) -> s ^ "."

fn | Point _      -> 0
   | Line(z0, z1) -> dist(z0, z1)
```

The value of a `lambda_form` is a partial or total function. If the value determined for a `lambda_form` as described below is not a total function, the context must enforce that the function can not be applied to values for which it is undefined. Otherwise, the `spec` is ill formed. Specware 4.2 does not attempt to generate proof obligations for establishing this.

The type of a `lambda_form` is that of its `match`. The meaning of a given `lambda_form` of type  $S \rightarrow T$  is the function  $f$  mapping each inhabitant  $x$  of  $S$  to a value  $y$  of type  $T$ , where  $y$  is the return value of  $x$  for the `match` of the `lambda_form`. If the `match` accepts each  $x$  of type  $S$  (for acceptance and return value, see the section on *Matches*) function  $f$  is total; otherwise it is partial, and undefined for those values  $x$  rejected.

In case of a recursive definition, the above procedure may fail to determine a value for  $y$ , in which case function  $f$  is not total, but undefined for  $x$ .

### 3.6.2 Case-expressions

```
case_expression ::= case expression of match
```

Sample `case_expressions`:

```
case z of {re = x, im = y} -> {re = x, im = -y}

case s of
  | Empty -> true
  | Push {top = _, pop = rest} -> hasBottom? rest
```

The value of a `case_expression` `caseE of M` is the same as that of the `application` `(fn M) (E)`.

### 3.6.3 Let-expressions

```

let_expression      ::=  let let_bindings in expression
let_bindings        ::=  recless_let_binding |
                           rec_let_binding_sequence
recless_let_binding  ::=  pattern equals expression
rec_let_binding_sequence ::=  rec_let_binding { rec_let_binding }*
rec_let_binding      ::=  def simple_name
                           formal_parameter_sequence [ type_annotation ]
                           equals expression
formal_parameter_sequence ::=  formal_parameter { formal_parameter }*

```

Sample let\_expressions:

```

let x = x + e in f(x, x)
let def f x = x + e in f (f x)

```

In the case of a `recless_let_binding` (recless = recursion- less), the value of the `let_expression`  $\text{let } P=A \text{ in } E$  is the same as that of the `application`  $(\text{fn } P \rightarrow E) \ (A)$ . For the first example above, this amounts to  $f(x + e, x + e)$ . Note that  $x = x + e$  is not interpreted as a recursive definition.

In case of a `rec_let_binding_sequence` (rec = recursive), the `rec_let_bindings` have the role of “local” `op_definitions`; that is, they are treated exactly like `op_definitions` except that they are interpreted in the local environment instead of the global model. For the second example above, this amounts to  $(x + e) + e$ . (If  $e$  is a `local_variable` in this scope, the definition of  $f$  can not be “promoted” to an `op_definition`, which would be outside the scope binding  $e$ .) A `spec` with `rec_let_bindings` can be transformed into one without such by creating `op_definitions` for each `rec_let_binding` that take additional arguments, one for each of the `local_variables` referenced. For the example, in which  $f$  references `local_variable`  $e$ , the `op_definition` for the “extended” `op`  $f \setminus \setminus : \text{sup} : '+' \setminus ' e$  would be `def f \setminus \setminus : \text{sup} : '+' \setminus ' e x = x + e`, and the `let_expression` would become  $f \setminus \setminus : \text{sup} : '+' \setminus ' e \ (f \setminus \setminus : \text{sup} : '+' \setminus ' e \ x)$ . The only difference in meaning is that the models of the transformed `spec` assign a value to the newly introduced `op`  $f \setminus \setminus : \text{sup} : '+' \setminus '$ .

Note that the first occurrence of  $x$  in the above example of a `rec_let_binding` is a `variable_pattern` and the second-occurrence is in its scope; the third and last occurrence of  $x$ , however, is outside the scope of the first  $x$  and identifies an `op` or `local_variable`  $x$  introduced elsewhere. So, without change in meaning, the `rec_let_binding` can be changed to:

```

let def f xena = xena + e in f (f x)

```

### 3.6.4 If-expressions

```

if_expression ::=  if expression then expression else expression

```

Sample if\_expression:

```

if x <= y then x else y

```

The value of an `if_expression`  $\text{if } B \text{ then } T \text{ else } F$  is the same as that of the `case_expression` `case B of true -> (T) | false -> (F)`.

### 3.6.5 Quantifications

```

quantification      ::=  quantifier ( local_variable_list ) expression
quantifier          ::=  fa | ex | ex1
local_variable_list ::=  annotable_variable { , annotable_variable } *
annotable_variable  ::=  local_variable [ type_annotation ]
local_variable      ::=  simple_name

```

Sample quantifications:

```

fa(x) norm (norm x) = norm x
ex(e : M) fa(x : M) x <*< e = x & e <*< x = x

```

Restriction. Each `local_variable` of the `local_variable_list` must be a different `simple_name`.

Quantifications are non-constructive, even when the domain type is finitely enumerable. The main uses are in `type_restrictions` and `type_comprehensions`, and `claims`. The type of a `quantification` is `Bool`. There are three kinds of quantifiers: `fa`, for “universal quantifications” (`fa` = for all); `ex`, for “existential quantifications” (`ex` = there exists); and `ex1`, for “uniquely existential quantifications” (`ex1` = there exists one).

The value of a `quantification` `fa (V)E`, in which `V` is a `local_variable_list` and `E` is an `expression`, is determined as follows. Let  $M$  be the `match (V) ->E`. If  $M$  has return value `true` for each value  $x$  in its domain, the value of the `quantification` is `true`; otherwise it is `false`.

The value of a `quantification` `ex (V)E` in which `V` is a `local_variable_list` and `E` is an `expression`, is determined as follows. Let  $M$  be the `match (V) ->E`. If  $M$  has return value `true` for at least one value  $x$  in its domain, the value of the `quantification` is `true`; otherwise it is `false`.

The value of a `quantification` `ex1 (V)E` in which `V` is a `local_variable_list` and `E` is an `expression`, is determined as follows. Let  $M$  be the `match (V) ->E`. If  $M$  has return value `true` for precisely one value  $x$  in its domain, the value of the `quantification` is `true`; otherwise it is `false`.

Note that a `quantifier` must be followed by an opening parenthesis ( . So `fa x (x = x)`, for example, is ungrammatical.

### 3.6.6 Unique-solutions

```

unique_solution ::=  the ( local_variable_list ) expression

```

Sample `unique_solution`:

```

the(x : S) f(x) = y

```

Restriction, Each `local_variable` of the `local_variable_list` must be a different `simple_name`.

Restriction. The type of the `expression` must be `Bool`.

Restriction. A `unique_solution` `the (V)E` may only be used in a context where the value of `ex1 (V)E` is `true`.

Unique\_solutions are non-constructive, even when the domain type is finitely enumerable. The type of a `unique_solution` is the type of its `local_variable_list`.

The value of a `unique_solution` `the (V)E`, in which `V` is a `local_variable_list` and `E` is an `expression`, is determined as follows. Let  $M$  be the `match (V) ->E`. The value of the `unique_solution` is then the unique value  $x$  in the domain of  $M$  such that the `match (V) ->E` has return value `true` for  $x$ .

### 3.6.7 Annotated-expressions

`annotated_expression ::= tight_expression type_annotation`

Restriction. In an `annotated_expression`  $E : T$ , the `expression`  $E$  must have type  $T$ .

Sample `annotated_expression`:

```
[] : List Arg
Positive : Sign
```

The value of an `annotated_expression`  $E : T$  is the value of  $E$ .

The type of some expressions is polymorphic. For example, for any type  $T$ , `[]` denotes the empty list of type `List  $T$` . Likewise, constructors of parameterized sum types can be polymorphic, as the constructor `None` of

```
type Option a = | Some a | None
```

### 3.6.8 Applications

```
application          ::= prefix_application | infix_application
prefix_application   ::= application_head actual_parameter
application_head     ::= closed_expression | inbuilt_prefix_op | prefix_application
actual_parameter     ::= closed_expression
infix_application    ::= operand infix_operator operand
operand              ::= tight_expression
infix_operator       ::= op_name |
                       inbuilt_infix_op
```

Sample applications:

```
f (x, x)
f x (g y)
x + 1
```

Restriction. An `infix_operator`, whether qualified or unqualified, can not be used without more as an `actual_parameter` or `operand` (and in the case of an `inbuilt_op`, it can not be used without more as any other kind of `expression` either). To use an `infix_operator` in such cases, it must be enclosed in parentheses, as for example in the prefix applications `foldl (+) 0` and `foldl ( *) 1` or the `infix_application` `(<) o ival`. Note the space between “(” and “\*”, since without space “(” signals the start of a `comment`.

Restriction. An `op_name` can be used as an `infix_operator` only if it has been declared as such in an `op_declaration` (see under *Op-declarations*).

Disambiguation. An `infix_application`  $P M Q N R$ , in which  $P$ ,  $Q$  and  $R$  are operands and  $M$  and  $N$  are `infix_operators`, is interpreted as either  $(*P M Q*) N R$  or  $*P M* (*Q N R*)$ . The choice is made as follows. If  $M$  has higher priority than  $N$ , or the priorities are the same but  $M$  is left-associative, the interpretation is  $(*P M Q*) N R$ . In all other cases the interpretation is  $*P M* (*Q N R*)$ . For example, given

```
op @ infixl 10: Nat * Nat -> Nat
op ** infixr 20: Nat * Nat -> Nat
```

the following interpretations hold:

```

1 ** 2 @ 3 = (1 ** 2) @ 3
1 @ 2 @ 3 = (1 @ 2) @ 3
1 @ 2 ** 3 = 1 @ (2 ** 3)
1 ** 2 ** 3 = 1 ** (2 ** 3)

```

Note that no type information is used in the disambiguation. If  $(1 @ 2) ** 3$  is type-correct but  $1 @ (2 ** 3)$  is not, the `expression`  $1 @ 2 ** 3$  is type-incorrect, since its interpretation is.

For the application of this disambiguation rule, the `inbuilt_ops` have `fixity` as suggested by the following pseudo-op\_declarations:

```

op <=> infixr 12 : Bool * Bool -> Bool
op => infixr 13 : Bool * Bool -> Bool
op || infixr 14 : Bool * Bool -> Bool
op && infixr 15 : Bool * Bool -> Bool
op = infixr 20 : [a] a * a -> Bool
op ~= infixr 20 : [a] a * a -> Bool
op << infixl 25 : { *x*:A*, ... , *y*:B*, ... } * { *x*:A*, ... , *z*:C*, ... }
      -> { *x*:A*, ... , *y*:B*, ... , *z*:C*, ... }

```

Restriction. In an `application`  $H P$ , in which  $H$  is an `application_head` and  $P$  an `actual_parameter`, the type of  $(H)$  must be some function type  $S \rightarrow T$ , and then  $P$  must have the domain type  $S$ . The type of the whole `application` is then  $T$ . In particular, in an `application`  $\sim P$  the type of both  $P$  and the `application` is `Bool`.

The meaning of `prefix_application`  $\sim P$  is the same as that of the `if_expression` `if P then false else true`.

The value of `prefix_application`  $H P$ , in which `application_head`  $H$  is a `closed_expression` or another `prefix_application`, is the value returned by function  $(H)$  for the argument value  $P$ .

The meaning of `infix_application`  $P N Q$ , in which  $P$  and  $Q$  are operands and  $N$  is an `op_name`, is the same as that of the `prefix_application`  $N(P, Q)$ .

The meaning of `infix_application`  $P \Rightarrow Q$ , in which  $P$  and  $Q$  are operands, is the same as that of the `if_expression` `if P then Q else true`.

The meaning of `infix_application`  $P || Q$ , in which  $P$  and  $Q$  are operands, is the same as that of the `if_expression` `if P then true else Q`.

The meaning of `infix_application`  $P \&\& Q$ , in which  $P$  and  $Q$  are operands, is the same as that of the `if_expression` `if P then Q else false`.

The value of `infix_application`  $P = Q$ , in which  $P$  and  $Q$  are operands, is `true` if  $P$  and  $Q$  have the same value, and `false` otherwise.  $P$  and  $Q$  must have the same type, or else have types that are subtypes of the same supertype. In the latter case, the comparison is the same as for the values of the operands coerced to the supertype, so, for example, the value of  $(1:\text{Nat}) = (1:\text{PosNat})$  is `true`.

The meaning of `infix_application`  $P \sim Q$ , in which  $P$  and  $Q$  are operands, is the same as that of the `prefix_application`  $\sim (P = Q)$ .

An `infix_application`  $P << Q$  is also called a “record update”. In a record update  $P << Q$ , in which  $P$  and  $Q$  are operands,  $P$  and  $Q$  must have record types, referred to as  $S$  and  $T$ , respectively. Moreover, for each `field_name`  $F$  these types  $S$  and  $T$  have in common, the field types for  $F$  in  $S$  and  $T$  must be the same, or be subtypes of the same supertype. The type of  $P << Q$  is then the record type  $R$  whose `field_names` are formed by the union of the `field_names` of  $S$  and  $T$ , where for each `field_name`  $F$  in that union, the type of field  $F$  in  $R$  is that of field  $F$  in  $T$  if  $F$  is a field of  $T$ , and otherwise the type of field  $F$  in  $S$ . Likewise, the value of  $P << Q$  is the record value of type  $R$  whose field value of each field  $F$  is that of field  $F$  in  $Q$  if  $F$  is a field of  $T$ , and otherwise the field value of field  $F$  in  $P$ . So, for example, the value of  $\{a=1, b=\#z\} << \{a=2, c=\text{true}\}$  is  $\{a=2, b=\#z, c=\text{true}\}$ : fields of the right-hand side `operand` take precedence over the left-hand side when present in both.

### 3.6.9 Op-names

```
op_name ::= name
```

Sample op\_names:

```
length
>=
DB_LOOKUP.Lookup
```

**Restriction.** An `op_name` may only be used if there is an `op_declaration` and/or `op_definition` for it in the current `spec` or in some `spec` that is imported (directly or indirectly) in the current `spec`. If there is a unique `qualified_name` for a given unqualified ending that is type-correct in the context, the qualification may be omitted for an `op_name` used as an `expression`. So overloaded ops may only be used as such when their type can be disambiguated in the context.

The value of an `op_name` is the value assigned to it in the model. (In this case, the context can not have superseded the original assignment.)

### 3.6.10 Literals

```
literal ::= bool_literal | nat_literal | char_literal | string_literal
```

Sample literals:

```
true
3260
#z
"On/Off switch"
```

**Restriction:** No whitespace is allowed anywhere inside any kind of `literal`, except for “significant” whitespace in `string_literals`, as explained there.

Literals provide denotations for the inhabitants of the inbuilt and “base-library” types `Bool`, `Nat`, `Char` and `String`. The value of a `literal` is independent of the environment.

(There are no literals for the base-library type `Integer`. For non-negative integers, a `nat_literal` can be used. For negative integers, apply the unary base-library `op -`, which negates an integer: `-1` denote the negative integer `-1`.)

#### Bool-literals

```
bool_literal ::= true |
               false
```

Sample bool\_literals:

```
true
false
```

The type `Bool` has precisely two inhabitants, the values of `true` and `false`.

## Nat-literals

```
nat_literal      ::=  decimal_digit { decimal_digit }* |
                      0 X hexadecimal_digit { hexadecimal_digit }* |
                      0 x hexadecimal_digit { hexadecimal_digit }* |
                      0 O octal_digit { octal_digit }* |
                      0 o octal_digit { octal_digit }* |
                      0 B binary_digit { binary_digit }* |
                      0 b binary_digit { binary_digit }*
hexadecimal_digit ::=  decimal_digit |
                      a | b | c | d | e | f |
                      A | B | C | D | E | F
octal_digit      ::=  0 | 1 | 2 | 3 | 4 |
                      5 | 6 | 7
binary_digit     ::=  0 | 1
```

Sample nat\_literals:

```
3260
007
0Xdeadbeef
00777
0b111001111
```

The `type_descriptor` `Nat` is, by definition, the subtype of `Integer` restricted to the non-negative integers 0, 1, 2,

... , which we identify with the natural numbers. The value of a `nat_literal` composed entirely of `decimal_digits` is the natural number of which it is a decimal representation; for example, the `nat_literal` 3260 denotes the natural number 3260. If the `nat_literal` starts with 0X or 0x, its value is the natural number of which the following sequence of `hexadecimal_digits` is a hexadecimal representation. For example, 0x17B denotes the value  $1 \times 16^2 + 7 \times 16 + 11 = 379$ . Likewise, 0O or 0o (a digit 0 followed by an uppercase letter O or a lower case letter o) introduces an octal representation, and 0B or 0b a binary representation. Leading digits 0 have no significance: both 007 and 7 denote the number 7.

Note that hexadecimal, octal, and binary literals are converted to an internal representation that does not retain their base. For example, given

```
Ned = spec
  op N : Nat = 0x17B
end-spec
```

the Specware Shell command `show Ned` will print as

```
spec
  op N : Nat = 379
end-spec
```



## Char-literals

```

char_literal      ::= #char_literal_glyph
char_literal_glyph ::= char_glyph |
                        "
char_glyph         ::= letter | decimal_digit | other_char_glyph
other_char_glyph  ::= ! | : | @ | # | * | % |
                        ^ | & | * | ( | ) | _ |
                        - | + | = | " | " | ~ | ` |
                        . | , | < | > | ? | / |
                        ; | " | "[" | "]" | "{" | " |
                        \ | \ | \a | \b | \t |
                        \n | \v | \f | \r | \s |
                        \x hexadecimal_digit hexadecimal_digit

```

Sample char\_literals:

```

#z
#\x7a

```

The type `Char` is inhabited by the 256 8-bit *characters* occupying decimal positions 0 through 255 (hexadecimal positions 00 through FF) in the ISO 8859-1 code table. The first 128 characters of that code table are the traditional ASCII characters (ISO 646). (Depending on the operating environment, in particular the second set of 128 characters – those with “the high bit set” – may print or otherwise be visually presented differently than intended by the ISO 8859-1 code.) The value of a `char_literal` is a character of type `Char`.

The value of a `char_literal` `#G`, where `G` is a `char_glyph`, is the character denoted by `G`. For example, `#z` is the character that prints as `z`. The two-mark `char_literal` `#"` provides a variant notation of the three- mark `char_literal` `#\"` and yields the character `"` (decimal position 34).

Each one-mark `char_glyph` `C` denotes the character that “prints” as `C`. The two-mark `char_glyph` `\\` denotes the character `\` (decimal position 92), and the two-mark `char_glyph` `\"` denotes the character `"` (decimal position 34).

Notations are provided for denoting eight “non-printing” characters, which, with the exception of the first, are meant to regulate lay-out in printing; the actual effect may depend on the operating environment:

glyph	decimal	name
<code>\a</code>	7	bell
<code>\b</code>	8	backspace
<code>\t</code>	9	horizontal tab
<code>\n</code>	10	newline
<code>\v</code>	11	vertical tab
<code>\f</code>	12	form feed
<code>\r</code>	13	return
<code>\s</code>	32	space

Finally, every character can be obtained using the hexadecimal representation of its position. The four-mark `char_glyph` `\xH1H0` denotes the character with hexadecimal position `H1 H0`, which is decimal position 16 times the decimal value of `hexadecimal_digit` `H1` plus the decimal value of `hexadecimal_digit` `H0`, where the decimal value of the digits 0 through 9 is conventional, while the six extra digits A through F correspond to 10 through 15. The case (lower or upper) of the six extra digits is not significant. For example, `\x7A` or equivalently `\x7a` has decimal position 16 times 7 plus 10 = 122, and either version denotes the character `z`. The “null” character can be obtained by using `\x00`.

## String-literals

```
string_literal      ::=  "string_body"  
string_body        ::=  { string_literal_glyph }*  
string_literal_glyph ::=  char_glyph | significant_whitespace  
significant_whitespace ::=  space | tab | newline
```

The presentation of a `significant_whitespace` is the whitespace suggested by the `name` (space, tab or newline).

Sample `string_literals`:

```
" "  
"see page"  
"see\spage"  
"the symbol ' is a single quote"  
"the symbol \" is a double quote"
```

The type `String` is inhabited by the *strings*, which are (possibly empty) sequences of characters. The type `String` is primitive; it is a different type than the isomorphic type `List Char`, and the list operations can not be directly applied to strings.

The value of a `string_literal` is the sequence of characters denoted by the `string_literal_glyphs` comprising its `string_body`, where the value of a `significant_whitespace` is the whitespace character suggested by the `name` (space, horizontal tab or newline). For example, the `string_literal` `"seepage"` is different from `"see page"`; the latter denotes an eight-character string of which the fourth character is a space. The space can be made explicit by using the `char_glyph` `\s`.

When a double-quote character `"` is needed in a string, it must be escaped, as in `"[6'2\"]"`, which would print like this: `[6'2"]`.

### 3.6.11 Field-selections

```
field_selection ::=  closed_expression . field_selector  
field_selector  ::=  nat_literal | field_name
```

Disambiguation. A `closed_expression` of the form `M.N`, in which `M` and `N` are `simple_names`, is interpreted as an `op` if `M.N` occurs as the `op_name` of an `op_declaration` or `op_definition` in the `spec` in which it occurs or in the set of `simple_names` imported from another `spec` through an `import_declaration`. Otherwise, `M.N` is interpreted as a `field_selection`. (The effect of a `field_selection` can always be obtained with a `projector`.)

Sample `field_selections`:

```
triple.2  
z.re
```

A `field_selection` `E.F` is a convenient notation for the equivalent `expression` `(project F E)`. (See under *Projectors*.)

### 3.6.12 Tuple-displays

```
tuple_display      ::=  ( tuple_display_body )  
tuple_display_body ::=  [ expression , expression { , expression }* ]
```

Sample `tuple_display`:

```
("George", Poodle : Dog, 10)
```

Note that a `tuple_display_body` contains either no expressions, or else at least two.

The value of a `tuple_display` whose `tuple_display_body` is not empty, is the tuple whose components are the respective values of the expressions of the `tuple_display_body`, taken in textual order. The type of that tuple is the “product” of the corresponding types of the components. The value of `()` is the empty tuple, which is the sole inhabitant of the unit type `()`. (The fact that the notation `()` does double duty, for a `type_descriptor` and as an `expression`, creates no ambiguity. Note also that – unlike the empty `list_display []` – the `expression ()` is monomorphic, so there is no need to ever annotate it with a `type_descriptor`.)

### 3.6.13 Record-displays

```
record_display      ::=  "{ " record_display_body " } "
record_display_body ::=  [ field_filler { , field_filler } * ]
field_filler        ::=  field_name = expression
```

Sample `record_display`:

```
{name = "George", kind = Poodle : Dog, age = 10}
```

The value of a `record_display` is the record whose components are the respective values of the expressions of the `record_display_body`, taken in the lexicographic order of the `field_names`, as discussed under *\*Type-records\**. The type of that record is the record type with the same set of `field_names`, where the type for each `field_name F` is the type of the corresponding type of the component selected by `F` in the record. The value of `{ }` is the empty tuple, which is the sole inhabitant of the unit type `()`. (For expressions as well as for `type_descriptors`, the notations `{ }` and `()` are fully interchangeable.)

### 3.6.14 Sequential-expressions

```
sequential_expression  ::=  ( open_sequential_expression )
open_sequential_expression ::=  void_expression ; sequential_tail
void_expression        ::=  expression
sequential_tail         ::=  expression | open_sequential_expression
```

Sample `sequential_expression`:

```
(writeLine "key not found"; embed Missing)
```

A `sequential_expression ( V ; T )` is equivalent to the `let_expression let _ = V in ( T )`. So the value of a `sequential_expression ( V1 ; ... ; Vn ; E )` is the value of its last constituent `expression E`.

Sequential-expressions can be used to achieve non-functional “side effects”, effectuated by the elaboration of the `void_expressions`, in particular the output of a message. This is useful for tracing the execution of generated code. The equivalent effect of the example above can be achieved by a `let_binding`:

```
let _ = writeLine "key not found" in
embed Missing
```

(If the intent is to temporarily add, and later remove or disable the tracing output, this is probably a more convenient style, as the modifications needed concern a single full text line.) Any values resulting from elaborating the `void_expressions` are discarded.

### 3.6.15 List-displays

```
list_display      ::=  "[" list_display_body "]"
list_display_body ::=  [ expression { , expression }* ]
```

Sample `list_display`:

```
["Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"]
```

Restriction. All expressions of the `list_display_body` must have the same type.

Note that a `list_display []` with empty `list_display_body` is polymorphic, and may need to be type-disambiguated, for example with a `type_annotation`. In a case like `[[], [1]]`, there is no need to disambiguate `[]`, since the above restriction already implies that `[]` here has the same type as `[1]`, which has type `List Nat`.

The parameterized type `List`, although a base-library type, is actually not primitive, but defined by:

```
type List a =
  | Nil
  | Cons a * List a
```

The empty `list_display []` denotes the same list as the `expression Nil`, a singleton `list_display [E]` denotes the same list as the `expression Cons (E, Nil)`, and a multi-element `list_display [E1, E2, ..., En]` denotes the same list as the `expression Cons(E1, Cons (E2, ..., Cons (En, Nil)))`.

### 3.6.16 Monadic-expressions

```
monadic_expression      ::=  "{ " open_monadic_expression "}"
open_monadic_expression ::=  monadic_statement ; monadic_tail
monadic_statement       ::=  expression | monadic_binding
monadic_binding         ::=  pattern <- expression
monadic_tail            ::=  expression | open_monadic_expression
```

Sample `monadic_expression`:

```
{x <- a; y <- b; f(x, y)}
```

Restriction. Monadic-expressions can only be used in a context containing the following `spec`, or a refinement thereof, possibly qualified, as a sub-`spec` (see under *Substitutions*):

```
spec
  type Monad a

  op monadBind : [a,b] (Monad a) * (a -> Monad b) -> Monad b
  op monadSeq  : [a,b] (Monad a) *      (Monad b) -> Monad b
  op return   : [a] a -> Monad a

  axiom left_unit is
    [a,b] fa (f : a -> Monad b, x : a)
      monadBind (return x, f) = f x

  axiom right_unit is
    [a] fa (m : Monad a)
      monadBind (m, return) = m

  axiom associativity is
```

```

[a,b,c] fa (m : Monad a, f : a -> Monad b, h : b->Monad c)
  monadBind (m, (fn x -> monadBind (f x, h))) =
  monadBind (monadBind (m, f), h)

axiom non_binding_sequence is
[a] fa (f : Monad a, g : Monad a)
  monadSeq (f, g) = monadBind (f, fn _ -> g)

end-spec

```

(This `spec` can be found, qualified with `Monad`, in the library `spec /Library/General/Monad`.) A `monadic_expression` may further only be used when the non-monadic `expression` it is equivalent to (see below) is itself a valid `expression`.

A `monadic_expression`  $\{ M \}$  is equivalent to the `open_monadic_expression`  $M$ .

A `monadic_tail`  $E$ , where  $E$  is an `expression`, is equivalent to the `expression`  $E$ .

A `monadic_tail`  $M$ , where  $M$  is an `open_monadic_expression`, is equivalent to the `open_monadic_expression`  $M$ .

An `open_monadic_expression`  $E ; T$ , where  $E$  is an `expression`, is equivalent to the `application` `monadSeq (E, T')`, where  $T'$  is an `expression` that is equivalent to the `monadic_tail`  $T$ .

An `open_monadic_expression`  $P <- E ; T$  is equivalent to the `application` `monadBind (E, fn P -> T')`, where  $T'$  is an `expression` that is equivalent to the `monadic_tail`  $T$ .

### 3.6.17 Structors

```

structor ::= projector | quotienter | chooser | embedding_test

```

The `structors` are a medley of constructs, all having polymorphic or type-ambiguous function types and denoting special functions that go between structurally related types, the destructors of product types.

Restriction. Like all polymorphic or type-ambiguous constructs, a `structor` can only be used in a context where its type can be inferred uniquely. This restriction will not be repeated for the various kinds of `structors` described in the following subsections.

For example, the following well-formed `spec` becomes ill formed when any of the `type_annotations` is omitted:

```

spec
  def [a] p2 = project 2 : String * a -> a
  def      q2 = project 2 : String * Nat -> Nat
end-spec

```

#### Projectors

```

projector ::= project field_selector

```

Sample projectors:

```

project 2
project re

```

When the `field_selector` is some `nat_literal` with value  $i$ , it is required that  $i$  be at least 1. The type of the `projector` is a function type (whose domain type is a product type) of the form  $T_1 * T_2 * \dots * T_n \rightarrow T_i$ ,

where  $n$  is at least  $i$ , and the value of the `projector` is the function that maps each  $n$ -tuple  $(v_1, v_2, \dots, v_n)$  inhabiting the domain type to its  $i$ th component  $v_i$ .

When the `field_selector` is some `field_name`  $F$ , the type of the `projector` is a function type (whose domain type is a record type) of the form  $\{F_1 : T_1, F_2 : T_2, \dots, F_n : T_n\} \rightarrow T_i$ , where  $F$  is the same `field_name` as  $F_i$  for some natural number  $i$  in the range 1 through  $n$ . Assuming that the fields are lexicographically ordered by `field_name` (see under *Type-records*), the value of the `projector` is the function that maps each  $n$ -tuple  $(v_1, v_2, \dots, v_n)$  inhabiting the domain type to its  $i$ th component  $v_i$ .

## Quotienters

```
quotienter ::= quotient "[" type_name "]"
```

Sample `quotienter`:

```
quotient[Q]
```

Restriction. In a `quotienter` `quotient[Q]`,  $Q$  must be defined as a *quotient type*.

The type of `quotienter` `quotient[Q]`, where  $Q$  is defined by `type Q = T / q`, is the function type  $T \rightarrow Q$ , that is, it goes from the base type to the quotient type. The value of the `quotienter` is the function that maps each inhabitant of type  $T$  to the  $q$ -equivalence class inhabiting  $Q$  of which it is a member.

For example, given

```
op congMod3 : Nat * Nat -> Bool =
  (fn (m, n) -> m rem 3 = n rem 3)
```

```
type Z3 = Nat / congMod3
```

we have the typing

```
quotient[Z3] : Nat -> Z3
```

and the function maps, for example, the number 5 to the equivalence class  $\{2, 5, 8, \dots\}$ , which is one of the three inhabitants of  $Z3$ .

## Choosers

```
chooser ::= choose "[" type_name "]"
```

Sample `chooser`:

```
choose[Q]
```

Restriction. In a `chooser` `choose[Q]`,  $Q$  must be defined as a *quotient type*.

The type of `chooser` `choose[Q]`, where  $Q = T/q$ , is a function type of the form  $F \rightarrow (Q \rightarrow R)$ , where  $F$  is the subtype of  $T \rightarrow R$  consisting of the  $q$ -constant (explained below) functions. Expressed more formally,  $F$  is the type  $\{f : T \rightarrow R \mid \text{fa}((x, y) : T * T) \ q(x, y) \Rightarrow f\ x = f\ y\}$ , where the `simple_names`  $f, x$  and  $y$  must be replaced by “fresh” `simple_names` not clashing with `simple_names` already in use in  $T, R$  or  $q$ .

The value of the `chooser` is the function mapping each  $q$ -constant (explained below) function  $f$  inhabiting type  $T \rightarrow R$  to the function of type  $Q \rightarrow R$  that maps each inhabitant  $C$  of  $Q$  to  $f\ x$ , where  $x$  is any member of  $C$ . Expressed symbolically, using a pseudo-function `any` that arbitrarily picks any member from a nonempty set, this is the function

```
fn f -> fn C -> f (any C)
```

The requirement of  $q$ -constancy on  $f$  is precisely what is needed to make this function insensitive to the choice made by `any`.

Function  $f$  is  $q$ -constant if, for each  $q$ -equivalence class  $C$  inhabiting  $Q$ ,  $f\ x$  equals  $f\ y$  for any two values  $x$  and  $y$  that are members of  $C$ , or  $f$  is undefined on all members of  $C$ . (Since the result of  $f$  is constant across each equivalence class, it does not matter which of its elements is selected by `any`.) For example – continuing the example of the previous section – function `fn n -> n*n rem 3` is `congMod3`-constant; for the equivalence class  $\{2, 5, 8, \dots\}$ , for example, it maps each member to the same value 1. So `choose[Z3] (fn n -> n*n rem 3)` maps the inhabitant  $\{2, 5, 8, \dots\}$  of type `Z3` to the natural number 1.

The meaning of `choose[Q] (fn x -> E)` is the same as that of the `let_expression` `let quotient[Q] x = A in E`. Indeed, often a `quotient_pattern` offers a more convenient way of expressing the intention of a `chooser`. Note, however, the remarks on the proof obligations for `quotient_patterns`.

## Embedding-tests

```
embedding_test ::= embed? constructor
```

Sample `embedding_test`:

```
embed? Cons
```

**Restriction.** The type of an `embedding_test embed? C` must be of the form  $T \rightarrow \text{Bool}$ , where  $T$  is a sum type that has a `constructor C`.

The value of `embedding_test embed? C` is the predicate that returns `true` if the argument value – which, as inhabitant of a sum type, is tagged – has tag  $C$ , and otherwise `false`. The `embedding_test` can be equivalently rewritten as

```
fn
| C _ -> true
| _   -> false
```

where the wildcard `_` in the first `branch` is omitted when  $C$  is parameter-less.

In plain words, `embed? C` tests whether its sum-typed argument has been constructed with the `constructor C`. It is an error when  $C$  is not a constructor of the sum type.

## 3.7 Matches and Patterns

### 3.7.1 Matches

```
match  ::= [ "|" ] branch { "|" branch }*
branch ::= pattern [ guard ] -> expression
guard  ::= "|" expression
```

Sample matches:

```
{re = x, im = y} -> {re = x, im = -y}

Empty -> true
| Push {top = _, pop = rest} -> hasBottom? rest
```

```
| Empty -> true
| Push {top = _, pop = rest} -> hasBottom? rest

| Line(z0, z1) | z0 ~= z1 -> dist(z0, z1)
```

Restriction. In a `match`, given the environment, there must be a unique type  $S$  to which the `pattern` of each `branch` conforms, and a unique type  $T$  to which the `expression` of each `branch` conforms, and then the `match` has type  $S \rightarrow T$ . The `pattern` of each `branch` then has type  $S$ .

Restriction. The type of the `expression` of a `guard` must be `Bool`

Disambiguation. If a `branch` could belong to several open `matches`, it is interpreted as being a `branch` of the textually most recently introduced `match`. For example,

```
case x of
| A -> a
| B -> case y of
| C -> c
| D -> d
```

is not interpreted as suggested by the indentation, but as

```
case x of
| A -> a
| B -> (case y of
| C -> c
| D -> d)
```

If the other interpretation is intended, the `expression` introducing the inner `match` needs to be parenthesized:

```
case x of
| A -> a
| B -> (case y of
| C -> c)
| D -> d
```

Acceptance and return value  $y$ , if any, of a value  $x$  for a given `match` are determined as follows. If each `branch` of the `match` rejects  $x$  (see below), the whole `match` rejects  $x$ , and does not return a value. Otherwise, let  $B$  stand for the textually first `branch` accepting  $x$ . Then  $y$  is the return value of  $x$  for  $B$ .

The meaning of a “guardless” `branch`  $P \rightarrow R$ , where  $P$  is a `pattern` and  $R$  an `expression`, is the same as that of the `branch`  $P \mid \text{true} \rightarrow R$  with a `guard` that always succeeds.

Acceptance and return value  $y$ , if any, of a value  $x$  for a `branch`  $P \mid G \rightarrow R$  in an environment  $C$  are determined as follows. If `pattern`  $P$  rejects  $x$ , the `branch` rejects  $x$ , and does not return a value. (For acceptance by a `pattern`, see under *Patterns*.) Otherwise, let  $C'$  be environment  $C$  extended with the acceptance binding of `pattern`  $P$  for  $x$ . If `pattern`  $P$  accepts  $x$ , but the value of `expression`  $G$  in the environment  $C'$  is false, the `branch` also rejects  $x$ , and does not return a value. Otherwise, when the `pattern` accepts  $x$  and the `guard` succeeds, the `branch` accepts  $x$  and the return value  $y$  is the value of `expression`  $R$  in the environment  $C'$ .

For example, in

```
case z of
| (x, true) -> Some x
| (_, false) -> None
```

if  $z$  has value  $(3, \text{true})$ , the first branch accepts this value with acceptance binding  $x = 3$ . The value of `Some x` in the extended environment is then `Some 3`. If  $z$  has value  $(3, \text{false})$ , the second branch accepts this value with



empty acceptance binding (empty since there are no “accepting” `local_variables` in `pattern (_, false)`), and the return value is `None` (interpreted in the original environment).

Here is a way of achieving the same result using a `guard`:

```
case z of
  | (x, b) | b -> Some x
  | _       -> None
```

### 3.7.2 Patterns

```
pattern      ::= annotated_pattern | tight_pattern
tight_pattern ::= aliased_pattern | cons_pattern | embed_pattern |
                  quotient_pattern | closed_pattern
closed_pattern ::= variable_pattern | wildcard_pattern | literal_pattern | list_pattern
                  tuple_pattern | record_pattern | ( pattern )
```

(As for expressions, the distinctions `tight_` and `closed_` for patterns have no semantic significance, but merely serve to avoid grammatical ambiguities.)

```
annotated_pattern ::= pattern type_annotation
aliased_pattern   ::= variable_pattern as tight_pattern
cons_pattern      ::= closed_pattern :: tight_pattern
embed_pattern     ::= constructor [ closed_pattern ]
quotient_pattern  ::= quotient "[" type_name "]"
variable_pattern  ::= local_variable
wildcard_pattern  ::= _
literal_pattern   ::= literal
list_pattern      ::= "[" list_pattern_body "]"
list_pattern_body ::= [ pattern { , pattern }* ]
tuple_pattern     ::= ( tuple_pattern_body )
tuple_pattern_body ::= [ pattern , pattern { , pattern }* ]
record_pattern    ::= "{" record_pattern_body "}"
record_pattern_body ::= [ field_patterner { , field_patterner }* ]
field_patterner   ::= field_name [ equals pattern ]
```

Sample patterns:

```
(i, p) : Integer * Bool
z as {re = x, im = y}
hd :: tail
Push {top, pop = rest}
embed Empty
x
_
#z
[0, x]
(cl as (0, _), x)
{top, pop = rest}
```

**Restriction.** Like all polymorphic or type-ambiguous constructs, a `pattern` may only be used in a context where its type can be uniquely inferred.

**Disambiguation.** A single `simple_name` used as a `pattern` is an `embed_pattern` if it is a `constructor` of the type of the `pattern`. Otherwise, the `simple_name` is a `variable_pattern`.

Restriction. Each `local_variable` in a `pattern` must be a different `simple_name`, disregarding any `local_variables` introduced in expressions or `type_descriptors` contained in the `pattern`. (For example, `Line (z, z)` is not a lawful `pattern`, since `z` is repeated; but `n : {n : Nat | n < p}` is lawful: the second `n` is “shielded” by the `type_comprehension` in which it occurs.)

To define acceptance and acceptance binding (if any) for a value and a `pattern`, we introduce a number of auxiliary definitions.

The *accepting* `local_variables` of a `pattern`  $P$  are the collection of `local_variables` occurring in  $P$ , disregarding any `local_variables` introduced in expressions or `type_descriptors` contained in the  $P$ . For example, in `pattern`  $u : \{v : S \mid p\} v$ ,  $u$  is an accepting `local_variable`, but  $v$  is not. (The latter is an accepting `local_variable` of `pattern`  $v : S$ , but not of the larger `pattern`.)

The *expressive descendants* of a `pattern` are a finite set of expressions having the syntactic form of `patterns`, as determined in the following three steps (of which the order of steps 1 and 2 is actually immaterial).

1. From `pattern`  $P$ , form some *tame variant*  $P_t$  by replacing each `field_patterner` consisting of a single `field_name`  $F$  by the `field_patterner`  $F=F$  and replacing each `wildcard_pattern`  $\_$  in  $P$  by a unique fresh `simple_name`, that is, any `simple_name` that does not already occur in the `spec`, directly or indirectly through an import. For example, assuming that the `simple_name` `v7944` is fresh, a tame variant of:

```
s0 as _ :: s1 as (Push {top, pop = rest}) :: ss
```

is:

```
s0 as v7944 :: s1 as (Push {top = top, pop = rest}) :: ss
```

2. Next, from  $P_t$ , form a (tamed) *construed version*  $P_{tc}$  by replacing each constituent `cons_pattern`  $H : T$  by the `embed_pattern` `Cons (H, T)`, where `Cons` denotes the `constructor` of the parameterized type `List`. For the example, the construed version is:

```
s0 as Cons (v7944,
            s1 as Cons (Push {top = top, pop = rest}, ss))
```

3. Finally, from  $P_{tc}$ , form the set  $ED_P$  of *expressive descendants* of  $P$ , where `expression`  $E$  is an expressive descendant if  $E$  can be obtained by repeatedly replacing some constituent `aliased_pattern`  $L$  as  $R$  of  $P_{tc}$  by one of the two `patterns`  $L$  and  $R$  until no `aliased_patterns` remain, and then interpreting the result as an `expression`. For the example, the expressive descendants are the three expressions:

```
s0
Cons (v7944, s1)
Cons (v7944, Cons (Push {top = top, pop = rest}, ss))
```

An *accepting binding* of a `pattern`  $P$  for a value  $x$  in an environment  $C$  is some binding  $B$  of typed values to the accepting `local_variables` of the *tame variant*  $P_t$ , such that the value of each expressive descendant  $E$  in  $ED_P$  in the environment  $C$  extended with binding  $B$ , is the same typed value as  $x$ .

Acceptance and acceptance binding, if any, for a value  $x$  and a `pattern`  $P$  are then determined as follows. If there is no accepting binding of  $P$  for  $x$ ,  $x$  is rejected. If an accepting binding exists, the value  $x$  is accepted by `pattern`  $P$ . There is a unique binding  $B$  among the accepting bindings in which the type of each assigned value is as “restricted” as possible in the subtype-supertype hierarchy without violating well-typedness constraints (in other words, there are no avoidable implicit coercions). The acceptance binding is then the binding  $B$  *projected on* the accepting `local_variables` of  $P$ .

For the example, the accepting `local_variables` of  $P_t$  are the six `local_variables` `s0`, `s1`, `ss`, `rest` and `v7944`. In general, they are the accepting `local_variables` of the original `pattern` together with any fresh `simple_names` used for taming. Let the value  $x$  being matched against the pattern be:

```
Cons (Empty, Cons (Push {top = 200, pop = Empty}, Nil))
```

Under the accepting binding:

```
s0 = Cons (Empty, Cons (Push {top = 200, pop = Empty}, Nil))
s1 = Cons (Push {top = 200, pop = Empty}, Nil)
ss = Nil
top = 200
rest = Empty
v7944 = Empty
```

the value of each  $E$  in  $ED_P$  amounts to the value  $x$ . Therefore,  $x$  is accepted by the original `pattern`, with acceptance binding:

```
s0 = Cons (Empty, Cons (Push {top = 200, pop = Empty}, Nil))
s1 = Cons (Push {top = 200, pop = Empty}, Nil)
ss = Nil
top = 200
rest = Empty
```

obtained by “forgetting” the fresh `simple_name` `v7944`.



---

# METASLANG GRAMMAR

This appendix lists the grammar rules of the Metaslang specification language. These rules are identical to those of the Chapter on *Metaslang*. They are brought together here, without additional text, for easy reference.

## A.1 The Grammar Description Formalism

```
wiffle ::= waffle [ waffle_tail ] |  
         piffle { + piffle }*
```

```
piffle ::= 1 | M { piffle }*
```

## A.2 The Grammar

### A.2.1 Models

```
op ::= op_name
```

```
spec ::= spec_form
```

## A.2.2 Symbols and Names

```
symbol ::= simple_name |
        literal |
        special_symbol

simple_name ::= first_syllable { _ next_syllable }*
first_syllable ::= first_word_syllable |
                  non_word_syllable
next_syllable ::= next_word_syllable |
                 non_word_syllable
first_word_syllable ::= word_start_mark { word_continue_mark }*
next_word_syllable ::= word_continue_mark { word_continue_mark }*
word_start_mark ::= letter
word_continue_mark ::= letter |
                    decimal_digit |
                    " |
                    ?

letter ::= A | B | C | D | E | F | G |
         H | I | J | K | L | M | N | O |
         P | Q | R | S | T | U | V |
         W | X | Y | Z | a | b |
         c | d | e | f | g | h |
         i | j | k | l | m | n |
         o | p | q | r | s | t |
         u | v | w | x | y | z

decimal_digit ::= 0 | 1 | 2 | 3 | 4 | 5 |
                6 | 7 | 8 | 9

non_word_syllable ::= non_word_mark { non_word_mark }*
non_word_mark ::= ` | ~ | ! | @ | * | ^ | & |
                * | - | = | + | \ | " | " | : |
                < | < | / | " | ?

special_symbol ::= _ | ( | ) | "[" | "]" | "{" | "}" |
                 ; | , | .
```

## A.2.3 Comments

```
comment ::= line_end_comment |
            block_comment

line_end_comment ::= % line_end_comment_body
line_end_comment_body ::= any_text_up_to_end_of_line
block_comment ::= (* block_comment_body *)
block_comment_body ::= any_text_including_newlines_and_nested_block_comments
```

## A.2.4 Units

```

unit_definition      ::=  unit_identifier = unit_term
unit_term            ::=  spec_term | morphism_term | diagram_term |
                           target_code_term | proof_term
specware_file_contents ::=  unit_term |
                           infile_unit_definition { infile_unit_definition }*
infile_unit_definition ::=  fragment_identifier = unit_term
fragment_identifier  ::=  simple_name

```

## A.2.5 Unit Identifiers

```

unit_identifier      ::=  swpath_based_path |
                           relative_path
swpath_based_path    ::=  / relative_path
relative_path        ::=  { path_element / }* path_element [ # fragment_identifier ]
path_element         ::=  path_mark { path_mark }*
path_mark            ::=  letter | decimal_digit | ! | * | & | " | + |
                           - | = | @ | ^ | ` | ~ | .

```

## A.2.6 Specs

```

spec_term ::=  unit_identifier |
               spec_form |
               spec_qualification |
               spec_translation |
               spec_substitution |
               diagram_colimit |
               obligator

```

## A.2.7 Spec Forms

```

spec_form ::=  spec { declaration }* end-spec

```

## A.2.8 Qualifications

```

spec_qualification ::=  qualifier qualifying spec_term
qualifier           ::=  simple_name
name                ::=  simple_name |
                           qualified_name
qualified_name       ::=  qualifier . simple_name

```

## A.2.9 Translations

```
spec_translation    ::=  translate spec_term by name_map
name_map            ::=  "{" [ name_map_item { , name_map_item }* ] "}"
name_map_item       ::=  type_name_map_item |
                           op_name_map_item |
                           wildcard_map_item

type_name_map_item  ::=  [ type ] name +-> name
op_name_map_item    ::=  [ op ] annotable_name +-> annotable_name
annotable_name      ::=  name [ type_annotation ]
type_annotation     ::=  : type_descriptor
wildcard_map_item   ::=  wildcard +-> wildcard
wildcard            ::=  simple_wildcard |
                           qualified_wildcard

simple_wildcard      ::=  _
qualified_wildcard  ::=  qualifier . simple_wildcard
```

## A.2.10 Substitutions

```
spec_substitution  ::=  spec_term "[" morphism_term "]"
```

## A.2.11 Diagram Colimits

```
diagram_colimit    ::=  colimit diagram_term
```

## A.2.12 Obligators

```
obligator          ::=  obligations unit_term
```

## A.2.13 Morphisms

```
morphism_term      ::=  unit_identifier |
                           spec_morphism
spec_morphism       ::=  morphism spec_term -> spec_term name_map
```



### A.2.14 Diagrams

```

diagram_term      ::=  unit_identifier |
                        diagram_form
diagram_form      ::=  diagram "{" diagram_element { , diagram_element }* "}"
diagram_element   ::=  diagram_node |
                        diagram_edge
diagram_node      ::=  simple_name +-> spec_term
diagram_edge      ::=  simple_name : simple_name -> simple_name +-> morphism_term

```

### A.2.15 Target Code Terms

```

target_code_term   ::=  generate target_language_name spec_term [ generate_option ]
generate_option    ::=  in string_literal |
                        with unit_identifier
target_language_name ::=  c |
                        java |
                        lisp

```

### A.2.16 Proof Terms

```

proof_term         ::=  prove claim_name in spec_term
                        [ with prover_name ]
                        [ using claim_list ] :
                        [ options prover_options ]
prover_name        ::=  snark
claim_list         ::=  claim_name { , claim_name }*
prover_options     ::=  string_literal

```

### A.2.17 Declarations

```

declaration ::=  import_declaration | type_declaration |
                op_declaration | claim_declaration |
                definition
definition  ::=  type_definition | op_definition
equals     ::=  is | =

```

### A.2.18 Import-declarations

```

import_declaration ::=  import spec_term { , spec_term }*

```

### A.2.19 Type-declarations

```
type_declaration      ::= type type_name [ formal_type_parameters ]
formal_type_parameters ::= local_type_variable |
                           ( local_type_variable_list )
local_type_variable   ::= simple_name
local_type_variable_list ::= local_type_variable { , local_type_variable }*
```

### A.2.20 Type-definitions

```
type_definition      ::= type_abbreviation |
                        new_type_definition
type_abbreviation    ::= type type_name [ formal_type_parameters ]
                        equals type_descriptor
new_type_definition  ::= type type_name [ formal_type_parameters ]
                        equals new_type_descriptor
```

### A.2.21 Op-declarations

```
op_declaration       ::= op [ type_variable_binder ] formal_expression
                        [ fixity ] type_annotation [ equals expression ] |
                        op formal_expression [ fixity ] polytype_annotation
                        [ equals expression ]
polytype_annotation  ::= : type_variable_binder type_descriptor
type_variable_binder ::= "[" local_type_variable_list "]"
formal_expression    ::= op_name |
                        formal_application
formal_application    ::= formal_application_head formal_parameter
formal_application_head ::= op_name |
                        formal_application
formal_parameter      ::= closed_pattern |
                        "(" pattern "|" expression ")"
fixity                ::= associativity priority
associativity         ::= infixl |
                        infixr
priority              ::= nat_literal
```

### A.2.22 Op-definitions

```
op_definition ::= def [ op ] [ type_variable_binder ] formal_expression
                  [ type_annotation ] equals expression |
                  def [ op ] formal_expression polytype_annotation equals expression
```

### A.2.23 Claim-declarations

```

claim_declaration ::= claim_kind claim_name is claim [ proof_script ]
claim_kind        ::= axiom | theorem | conjecture
claim_name        ::= name
claim             ::= [ type_variable_binder ] expression

```

### A.2.24 Type-descriptors

```

type_descriptor      ::= type_arrow | slack_type_descriptor
new_type_descriptor  ::= type_sum | type_quotient
slack_type_descriptor ::= type_product | tight_type_descriptor
tight_type_descriptor ::= type_instantiation | closed_type_descriptor
closed_type_descriptor ::= type_name | Bool |
                           local_type_variable | type_record |
                           type_restriction | type_comprehension |
                           ( type_descriptor )

```

### A.2.25 Type-sums

```

type_sum      ::= type_summand { type_summand }*
type_summand  ::= "\" constructor [ slack_type_descriptor ]
constructor   ::= name

```

### A.2.26 Type-arrows

```

type_arrow  ::= arrow_source -> type_descriptor
arrow_source ::= type_sum |
                  slack_type_descriptor

```

### A.2.27 Type-products

```

type_product ::= tight_type_descriptor * tight_type_descriptor
               { * tight_type_descriptor }*

```

### A.2.28 Type-instantiations

```

type_instantiation      ::= type_name actual_type_parameters
actual_type_parameters  ::= closed_type_descriptor |
                           ( proper_type_list )
proper_type_list        ::= type_descriptor , type_descriptor { , type_descriptor }*

```

### A.2.29 Type-names

```
type_name ::= name
```

### A.2.30 Type-records

```
type_record      ::=  "{" [ field_typer_list ] "}" |  
                    ( )  
field_typer_list ::=  field_typer { , field_typer }*  
field_typer      ::=  field_name type_annotation  
field_name       ::=  simple_name
```

### A.2.31 Type-restrictions

```
type_restriction ::=  ( slack_type_descriptor "|" expression )
```

### A.2.32 Type-comprehensions

```
type_comprehension ::=  "{" annotated_pattern "|" expression "}"
```

### A.2.33 Type-quotients

```
type_quotient ::=  closed_type_descriptor / closed_expression
```

### A.2.34 Expressions

```

expression      ::=  lambda_form | case_expression | let_expression |
                    if_expression | quantification | unique_solution |
                    annotated_expression | tight_expression

tight_expression ::=  application | closed_expression

closed_expression ::=  op_name | local_variable | literal |
                      field_selection | tuple_display | record_display |
                      sequential_expression | list_display | monadic_expression |
                      structor | ( expression ) | ( inbuilt_op )

inbuilt_op      ::=  inbuilt_prefix_op |
                    inbuilt_infix_op

inbuilt_prefix_op ::=  ~

inbuilt_infix_op  ::=  <=> |
                     => |
                     " | ' | " |
                     && |
                     = |
                     ~= |
                     |lt||lt|

```

### A.2.35 Lambda-forms

```

lambda_form ::=  fn match

```

### A.2.36 Case-expressions

```

case_expression ::=  case expression of match

```

### A.2.37 Let-expressions

```

let_expression      ::=  let let_bindings in expression
let_bindings        ::=  recless_let_binding |
                        rec_let_binding_sequence
recless_let_binding  ::=  pattern equals expression
rec_let_binding_sequence ::=  rec_let_binding { rec_let_binding }*
rec_let_binding      ::=  def simple_name formal_parameter_sequence
                        [ type_annotation ] equals expression
formal_parameter_sequence ::=  formal_parameter { formal_parameter }*

```

### A.2.38 If-expressions

```

if_expression ::=  if expression then expression else expression

```

### A.2.39 Quantifications

```
quantification      ::= quantifier ( local_variable_list ) expression
quantifier          ::= fa | ex | ex1
local_variable_list ::= annotable_variable { , annotable_variable }*
annotable_variable  ::= local_variable [ type_annotation ]
local_variable      ::= simple_name
```

### A.2.40 Unique-solutions

```
unique_solution ::= the ( local_variable_list ) expression
```

### A.2.41 Annotated-expressions

```
annotated_expression ::= tight_expression type_annotation
```

### A.2.42 Applications

```
application      ::= prefix_application |
                    infix_application
prefix_application ::= application_head actual_parameter
application_head  ::= closed_expression | inbuilt_prefix_op | prefix_application
actual_parameter  ::= closed_expression
infix_application ::= operand infix_operator operand
operand           ::= tight_expression
infix_operator    ::= op_name | inbuilt_infix_op
```

### A.2.43 Op-names

```
op_name ::= name
```

### A.2.44 Literals

```
literal ::= bool_literal | nat_literal | char_literal | string_literal
```

### A.2.45 Bool-literals

```
bool_literal ::= true | false
```

## A.2.46 Nat-literals

```

nat_literal      ::=  decimal_digit { decimal_digit }* |
                      0 X hexadecimal_digit { hexadecimal_digit }* |
                      0 x hexadecimal_digit { hexadecimal_digit }* |
                      0 O octal_digit { octal_digit }* |
                      0 o octal_digit { octal_digit }* |
                      0 B binary_digit { binary_digit }* |
                      0 b binary_digit { binary_digit }*
hexadecimal_digit ::=  decimal_digit |
                      a | b | c | d | e | f | A |
                      B | C | D | E | F
octal_digit      ::=  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7
binary_digit     ::=  0 | 1

```

## A.2.47 Char-literals

```

char_literal     ::=  #char_literal_glyph
char_literal_glyph ::=  char_glyph |
                        "
char_glyph       ::=  letter |
                        decimal_digit |
                        other_char_glyph
other_char_glyph ::=  ! | : | @ | # | $ | % | ^ |
                        & | * | ( | ) | _ | - | + |
                        = | " | " | ~ | ` | . | , | < |
                        < | ? | / | ; | " | "[" | "]" |
                        "{ | } | \ | \ | \a | \b | \t |
                        \n | \v | \f | \r | \s |
                        \x hexadecimal_digit hexadecimal_digit

```

## A.2.48 String-literals

```

string_literal   ::=  " string_body "
string_body      ::=  { string_literal_glyph }*
string_literal_glyph ::=  char_glyph |
                          significant_whitespace
significant_whitespace ::=  space | tab | newline

```

## A.2.49 Field-selections

```

field_selection  ::=  closed_expression . field_selector
field_selector   ::=  nat_literal |
                      field_name

```

### A.2.50 Tuple-displays

```
tuple_display      ::= ( tuple_display_body )
tuple_display_body ::= [ expression , expression { , expression }* ]
```

### A.2.51 Record-displays

```
record_display      ::= "{ " record_display_body "}"
record_display_body ::= [ field_filler { , field_filler }* ]
field_filler        ::= field_name equals expression
```

### A.2.52 Sequential-expressions

```
sequential_expression ::= ( open_sequential_expression )
open_sequential_expression ::= void_expression ; sequential_tail
void_expression        ::= expression
sequential_tail        ::= expression | open_sequential_expression
```

### A.2.53 List-displays

```
list_display      ::= "[ " list_display_body "]"
list_display_body ::= [ expression { , expression }* ]
```

### A.2.54 Monadic-expressions

```
monadic_expression  ::= "{ " open_monadic_expression "}"
open_monadic_expression ::= monadic_statement ; monadic_tail
monadic_statement   ::= expression |
                        monadic_binding
monadic_binding      ::= pattern <- expression
monadic_tail        ::= expression |
                        open_monadic_expression
```

### A.2.55 Structors

```
structor ::= projector | quotienter | chooser | embedding_test

projector ::= project field_selector

quotienter ::= quotient "[ " type_name "]"
```



```
chooser ::= choose "[" type_name "]"
```

```
embedding_test ::= embed? constructor
```

## A.2.56 Matches

```
match ::= [ "|" ] branch { "|" branch }*
branch ::= pattern [ guard ] -> expression
guard ::= "|" expression
```

## A.2.57 Patterns

```
pattern ::= annotated_pattern |
          tight_pattern
tight_pattern ::= aliased_pattern |
                 cons_pattern |
                 embed_pattern |
                 quotient_pattern |
                 closed_pattern
closed_pattern ::= variable_pattern |
                  wildcard_pattern |
                  literal_pattern |
                  list_pattern |
                  tuple_pattern |
                  record_pattern |
                  ( pattern )

annotated_pattern ::= pattern type_annotation
aliased_pattern  ::= variable_pattern as tight_pattern
cons_pattern     ::= closed_pattern :: tight_pattern
embed_pattern    ::= constructor [closed_pattern ]
quotient_pattern ::= quotient "[" type_name "]"
variable_pattern ::= local_variable wildcard_pattern: _
literal_pattern  ::= literal
list_pattern     ::= "[" list_pattern_body "]"
list_pattern_body ::= [ pattern { , pattern }* ]
tuple_pattern    ::= ( tuple_pattern_body )
tuple_pattern_body ::= [ pattern , pattern { , pattern }* ]
record_pattern   ::= "{" record_pattern_body "}"
record_pattern_body ::= [ field_patternner { , field_patternner }* ]
field_patternner  ::= field_name [ equals pattern ]
```



# INBUILTS

This appendix provides a brief description of the “inbuilt” types and operators. For the sake of brevity, `infixl` is abbreviated below to `L` and `infixr` to `R`.