10. Constraints and generation

Test generation is a process producing data layouts according to a given specification. The specifications are provided in the form of *type declarations* and *constraints*. Constraints are statements that restrict values assigned to data items by test generation.

A constraint can be viewed as a property of a data item or as a relation between several data items. Therefore, it is natural to express constraints using Boolean expressions. Any valid Boolean expression in ***e*** can be turned into a constraint. Also, there are few special syntactic constructs not based on Boolean expressions for defining constraints.

Constraints can be applied to any data types including user-defined scalar types as well as struct and list types. It is natural to mix data types in one constraint, e.g.,

```
keep my_list.has(it == 0xff) => my_struct1 == my_struct2
```

10.1 Types of constraints

Constraints can be subdivided according to several criteria as follows:

a) Explicit or implicit
   1) *Explicit constraints* are those declared using the **keep** statement or inside **keeping {...}** block.
   2) *Implicit constraints* are those imposed by type definitions and variable declarations.

      Implicit constraints are always hard.

Examples

```
x : int[1, 3, 5, 10..100];      \\ is the same as:

x : int;
  keep x in [1, 3, 5, 10..100];

l[20] : list of int;            \\ is the same as:

l : list of int;
  keep l.size() == 20
```

b) Hard or soft
   1) *Hard constraints* are honored whenever the constrained data items are generated. A situation when a hard constraint contradicts other hard constraints, and thus cannot be honored, shall result in an error.
   2) *Soft constraints* are honored if they do not contradict hard constraints or soft constraints honored earlier. If a soft constraint cannot be honored, it is disregarded. (See 10.2.6 for the explanations on how the selection of soft constraints is done.)

c) Simple or compound

   A constraint combining other constraints in a Boolean combination using **not**, **and**, **or**, and => is called *compound*. Otherwise, the constraint is called *simple*.

10.2 Generation concepts

This subclause describes the basic concepts of generation.

10.2.1 Basic flow of generation

Generation can be initiated for any field or variable. For items of struct types, the generation allocates the struct storage and recursively generates all generatable fields of the struct. All fields of a struct are considered generatable, except for the fields prefixed with `!` (see 6.8). There is no specific order in which data items or the fields in a struct hierarchy are generated.

For list items, the generation allocates the list and recursively generates all its elements. There is no specific ordering for whether list items are generated after the size of the list has been fixed or that the items are generated in the order of their indexes. Constraints specified for the items can impose restrictions on the list size or on the items specified earlier in the list.

For scalar types, such as `int`, `uint`, `bool`, etc., the generation only generates the respective value.

The following ordering rules, however, do apply:

a) **pre_generate()** and **post_generate()**
   1) **pre_generate()** of a struct is called after the struct is allocated and initialized using **init()**, but before any of the fields of the struct are generated. In particular, for a struct containing nested structs, the **pre_generate()** method is called before any of the **pre_generate()** methods of the nested structs.
   2) **post_generate()** is called after the generation of all fields of the struct is finished. In particular, for a struct containing nested structs, the **post_generate()** method is called only when all the nested generations are finished.

b) Methods

   A method accepting a generatable item as an argument is called after that item is fully generated.

Example

```
struct s {
    a : int;
    b : t;              // 't' is some other struct type
      keep a == f(b)
}
```

The constraint `a==f(b)` implies `b` is fully generated, including the calls to its **pre_generate()** and **post_generate()** before `f` is called on `b`. See also 10.2.2 and 10.2.3.

10.2.2 Using methods in constraints

Constraint paths can include method calls. The syntax is:

[*simple-path*.]*method-name*([*parameter*, ...])[.*trailing-path*]

where *simple-path* does not include method calls and the following restrictions apply:

— If *simple-path* is generatable, then it is fully generated before the method is called.
— Generatable paths used as parameters of the method are fully generated before the method is called.
— For methods returning pointers to structs, the trailing path is sampled after evaluating the method and used as an input of the constraint.

Example

```
struct s {
    x : int[0..5];
```



```
    q : t;
      keep x < m(q).y;

    m(param:t): t is {
        result = param
    }
};

struct t {
    y : int[0..5]
}
```

In this example, `q` is generated before `x` and then `q` is used as an input in the constraint `x<m(q).y`. If `q.y` generates to `0`, then the constraint `x<m(q).y` fails.

10.2.2.1 Classification of methods

Methods are classified into the following three categories:

a) Methods that behave like mathematical functions (*pure*). The computed result is entirely determined by the arguments passed to the method. Multiple calls to the method with the same parameters always produce the same result.

   The use of such methods in constraints is safe and unrestricted.

b) Methods that observe the "state of the world," but do not change it. Such method can read fields, signals, global configuration flags, etc., and base the computation on that data. Multiple calls to the method with the same parameters can produce different results.

   When using the methods of this category of constraints the following rules apply:

   1) The method shall not base its computation on the items of the current generatable context, unless such items are passed as parameters to the method.

Example

```
struct packet {
    data     : list of byte;
    checksum : uint;
      keep checksum == calc_checksum(data);

    calc_checksum(data:list of byte): uint is {
        // use 'data' to calculate checksum
    }
}
```

   This is correct; `data` is generated before the method is called.

   2) The timing of the call and/or the number of calls to the method cannot be presumed, especially for methods reading values of the real-time or process clocks, operating-system (OS) environment variables, sizes of allocated memory, etc.

Example

```
extend sys {
    l[1000] : list of uint;
      keep for each in l {
        it == read_machine_real_time_clock_msec()
      }
}
```

It is incorrect to assume the method `read_machine_real_time_clock_msec` is called 1000 times, i.e., once for each list element in order (see 10.2.2.2). It is acceptable for the generator to assume this method is a pure function, and thus, call it only once for the list and assign the result to all the list elements. It is also acceptable to assign values to list elements unrelated to their natural order of indexes. Thus (normally in the presence of other constraints), the times read by the method might not be ordered with respect to the list indexes.

c) Methods that observe and change the "state of the world."

The use of such methods in constraints can create problems. Instead, use the corresponding operations within the **post_generate()** method.

Example

```
struct packet {
    data : list of data_item;

    post_generate() is {
        var id;

        for each in data do {
            if it.x < 100 then {
                it.id = id;
                id += 1
            }
        }
    }
}
```

In general, it is impossible to classify methods automatically into the preceding three categories. Therefore, the following warnings shall be used if a method calling issue occurs:

— *method call warning #1*: a method used in a constraint contains a non-local path anywhere in its body.

— *method call warning #2*: a method used in a constraint contains an explicit assignment to a non-local path.

10.2.2.2 Number of calls

A method used in constraints can be called zero or more times. The number of calls to a method is irrelevant for the semantics of the constraint if the method behaves as a *pure* function [see 10.2.2.1, category a)]. However, the results of generation can differ depending on the number of calls for the methods with side effects. Therefore, avoid using the methods of category c), and only use methods of category b) with caution.

10.2.3 Generatable paths and the sampling of inputs

The purpose of constraints is to constrain *generatable items*, i.e., those items that can be assigned random values (by the generator) satisfying the constraints. Thus, it is important to define which items are considered generatable and when.

In the context of the initial generation, all fields of **sys** and all fields of nested structs are generatable, except the fields declared as non-generatable (using the `!` prefix).

In the context of a **gen** *item* action (see 10.5.1), *item* is generatable and, if *item* is of a struct type, all its nested fields are generatable—except the fields marked with `!`. If **gen** *item* action applies to a field defined

as non-generatable, the *item* becomes generatable; however, any nested non-generatable fields remain non-generatable.

Example

```
struct packet {
    x : int;
   !y : int
};

extend sys {
    p1 : packet;     -- generated during pre-generation
   !p2 : packet;     -- skipped during pre-generation

    post_generate() is also {
        gen p2       -- this allocates p2 and generates p2.x but not p2.y
    }
}
```

Data items in constraints are referenced by using *paths* (see 4.3.4). In generation context, each path is either generatable or non-generatable. *Generatable paths* refer to items that are assigned values during the generation with respect to the corresponding constraints. Each constraint shall have all its inputs sampled before the items referenced by the generatable paths are generated.

Non-generatable paths refer to items that are not affected by generation, but those items might affect generatable items. Thus, non-generatable paths refer to *inputs* of constraints. A path is *non-generatable* if

a) it is an absolute path (e.g., `sys.counter`).

b) it includes method calls (e.g., `x.y.m().z`).

c) it includes *do-not-gen* fields (e.g., `x.y.non_gen_field.z`).

d) the path is **me** (e.g., `keep root_node => parent == me;`).

Otherwise, the path is generatable.

An otherwise generatable path can be defined as input to a constraint using the **read_only()** syntax, e.g., `keep x<read_only(y)`. In this case, the set of values `y` can take is unaffected by the constraints on `x`. The parameter `y` is treated as an input.

Arbitrary expressions can be used as arguments of **read_only()**. For example, in `keep x<read_only(y+z)`, both `y` and `z` become inputs of the constraint. The constraint resolution engine generates `y` and `z` (unaffected by the possible values of `x`) and computes their sum, which is then used as an input in the constraints.

Semantically, **read_only()** can be viewed as an identity function

read_only(*arg* : TYPE**) is {** *result* **=** *arg* **}**

defined for each type TYPE known to the generator. The use of **read_only()** in constraints is thus identical to the use of such an identity function.

A constraint that has no generatable paths with respect to the current generation context shall be reported as an error.

10.2.4 Special cases of inputs in constraints

For some constraints, it is convenient to assume some of the parameters are always treated as inputs. One natural example is *method calls*. For a constraint, such as `keep x==f(y,z)`, `y` and `z` are presumed to be generated first and then their values are used as inputs in the context of `x==f(y,z)`. If `x` cannot accept the value returned by the call to `f(y,z)`, the generation results in a contradiction error. Thus, given the values of arguments, the constraint resolution engine is presumed to be able to compute and assign the value of the method/function call. The converse is not presumed, however.

There are four kinds of constraints treating some of their parameters as inputs, even if these parameters represent generatable paths.

a) *method calls*: all arguments of a method call are treated as inputs.

b) *bit slice*: the two boundaries *i* and *j* of a bit slice, such as in `keep x[j:i]==y`, are treated as inputs. It means that *i* and *j* are generated first and their values used as inputs for solving it with respect to `x` and `y`. Thus, the constraint resolution engine is not required to deduce the values of the bit slice boundaries. Namely,

```
keep 0b101010010101[j:i] == 0b100
```

is allowed to cause a contradiction error.

c) *list segments*: in an expression `l[i..j]`, the segment boundaries *i* and *j* are treated as inputs in the generation of `l`. Thus, a constraint such as

```
keep ({1; 2; 3; 4; 5})[i..j] in {2; 3}
```

is allowed to cause a contradiction error.

d) *shift operations*: in expressions such as `x<<k` and `x>>k`, the number of bits for shifting is treated as input. Thus, a constraint such as

```
keep 0b1110011010 >> k == 0b1110
```

is allowed to cause a contradiction error.

10.2.5 Scope of constraints

A constraint can be either applicable or inapplicable depending on the context of generation. There are two basic rules governing that aspect of generation.

a) All constraints defined for **sys** and any of the nested structs are applicable during the initial generation.

b) For generation started by the **gen** *item* action (see 10.5.1), the following are applicable:

   1) The constraints defined within the optional *constraints* block.

   2) All constraints defined in the type of *item*, if *item* is of a struct type.

   3) All constraints referring to *item* in this struct (**me**) and in the struct hierarchy containing **me**.

Example

```
struct packet {
    x : uint;
    y : uint;
      keep x < y
};

extend sys {
   !p1 : packet;
```



```
        keep p1.y == 8;
    !p2 : packet;

    post_generate() is also {
        gen p1 keeping {it.x > 5};
        p2 = new;
        gen p2.x
    }
}
```

The generation of `p1` succeeds. The applicable constraints here are `p1.x>5` (by rule b1), `p1.x<p1.y` (by rule b2), and `p1.y==8` (by rule b3) Thus, `p1.y` becomes `8` and `p1.x` becomes either `6` or `7`.

The generation of `p2.x` fails. For `p2` allocated using `new`, `p2.x=0` and `p2.y=0`. The only applicable constraints in this case is `p2.x<p2.y` (by rule b3). `p2.y` is not a generatable item here in the context of `gen p2.x` (see 10.2.3); it is used as input, so the constraint is equivalent to `p2.x < 0`. Since `x` is a **uint**, the constraint is not satisfiable.

10.2.6 Soft constraints

A constraint can be declared as soft by prefixing it with the **soft** keyword in the declaration. See also 10.4.5.

```
keep soft constraint;
gen item keeping {soft constraint; ...};
keep soft item = select {...}
```

Intuitively, soft constraints are satisfied if possible and otherwise disregarded. Soft constraints suggest default values and relations that can be overridden by hard or other soft constraints. They are considered with respect to the order of importance, which is a reverse of the (textual) order of soft constraints in the model.

The following properties of soft constraints also apply:

a) Assume two soft constraints c_1 and c_2, such that c_1 is more important than c_2. Then the generator shall always produce a solution satisfying c_1, if one exists. It is also required that the generator find a solution satisfying both c_1 and c_2, if it exists.

b) Assume a collection of data items (fields and/or variables) $x_1 \ldots x_n$, a collection of constraints $c_1 \ldots c_k$ linking the data items, and a solution exists satisfying all $c_1 \ldots c_k$. Then a solution needs to be found for {soft c_1;...;soft c_k} such that all soft constraints are satisfied.

Informally, this property means that in the absence of hard constraints, soft constraints act as hard, except for those cases causing contradictions.

Example

```
struct s {
    x : int;
    y : int;
    z : int;
      keep x in [1..100];
      keep x < y or y < z
}
```

is the same as

```
struct s {
    x : int;
```

```
        y : int;
        z : int;
          keep soft x in [1..100];
          keep soft x < y or y < z
    }
```

10.2.6.1 keep gen-item.reset_soft()

Purpose	Quit evaluation of soft constraints for a field
Category	Struct member
Syntax	**keep** *gen-item*.**reset_soft()**
Parameters	*gen-item* A generatable item (see 10.4.12).

This causes the program to quit the evaluation of soft value constraints for the specified field. Soft constraints for other fields are still evaluated. Soft constraints are considered in reverse order to the order in which they are defined in the ***e*** code.

The syntax **keep** *gen-item*.**reset_soft()** is used for discarding soft constraints referring to the *gen-item* loaded so far. Soft constraints not referring to *gen-item* or soft constraints referring to *gen-item*, but loaded later, are taken into account by the constraint resolution engine. The main use of this feature is for overloading the default "soft" behavior of a model.

Syntax example:

```
keep c.reset_soft()
```

10.2.6.2 keep soft... select

Purpose	Constrain distribution of values	
Category	Struct member	
Syntax	**keep soft** *gen-item*==**select** {*weight*: *value*; ...}	
Parameters	*gen-item*	A generatable item of type list (see 10.4.12).
	weight	Any **uint** expression. Weights are proportions; they do not have to add up to 100. A relatively higher weight indicates a greater probability that the value is chosen.
	value	*value* is one of the following: a) **range-list**—A range list such as `[2..7]`. A select expression with a range list selects the portion of the current range that intersects with the specified range list. b) **exp**—A constant expression. A select expression with a constant expression (usually a single number) selects that number, if it is part of the current range. c) **others**—Selects the portions of the current range that do not intersect with other select expressions in this constraint. Using a weight of `0` for **others** causes the constraint to be ignored, i.e., the effect is the same as if the **others** option were not entered at all. d) **pass**—Ignores this constraint and keeps the current range as is. e) **edges**—Selects the values at the extreme ends of the current range(s). f) **min**—Selects the minimum value of the *gen-item*. g) **max**—Selects the maximum value of the *gen-item*.

This specifies the relative probability that a particular value or set of values is chosen from the current range of legal values. The current range is the range of values as reduced by hard constraints and by soft constraints that have already been applied. A weighted value shall be assigned with the probability of

weight/(*sum of all weights*)

Weights are treated as integers. If an expression is used for a *weight*, the value of the expression shall be smaller than the maximum integer size (`MAX_INT`).

Like other soft constraints, **keep soft select** is order dependent (see 10.2.6) and shall not be met if it conflicts with hard constraints or soft constraints that have already been applied. In those cases where some values conflict with other constraints, **keep soft select** shall bias the distribution based on the remaining permissible values.

Syntax example:

```
keep soft me.opcode == select {
    30 : ADD;
    20 : ADDI;
    10 : [SUB, SUBI]
}
```

10.2.7 Constraining non-scalar data types

This subclause describes constraining structs and lists.

10.2.7.1 Constraining structs

There are two basic constraints that apply to structs: struct equality and struct inequality. Other constraints affecting items of struct types (such as list constraints with structs as list elements) can be equivalently expressed using these basic constraints and Boolean combinators.

10.2.7.1.1 Struct equality

Struct equality constrains two structs to share the same struct layout, i.e., it *aliases* two struct pointers.

Example

```
struct packet {
    x : int;
    y : int
};

extend sys {
    p1 : packet;
    p2 : packet;
      keep p1 == p2;

    post_generate() is also {
        p1.x = 5
    }
}
```

This causes `p1` and `p2` to represent the same struct, i.e., `sys.p1` and `sys.p2` can be viewed as pointers pointing to the same place in memory. Thus, the assignment in `post_generate` has the same effect on both structures, i.e., `sys.p1.x = sys.p2.x = 5`.

In contrast,

```
struct packet {
    x : int;
    y : int
};

extend sys {
    p1 : packet;
    p2 : packet;
      keep p1.x == p2.x;
      keep p1.y == p2.y;
post_generate() is also {
        p1.x = 5
    }
}
```

The first two lines in “extend sys” define two structures with the same contents, `sys.p1` and `sys.p2`. Then the assignment in `post_generate` changes the value of `sys.p1.x`, but not of `sys.s2.x`. Thus, at the end `sys.p1.x=5`, while `sys.p2.x` is set to a random value from the range `[MIN_INT.. MAX_INT]`. Of course, this value could be `5` as well, but the chance for that is 1/(2^32). Thus, most likely at the end `sys.p1.x != sys.p2.x`.

10.2.7.1.2 Struct inequality

Struct inequality states that two struct pointers cannot be aliased, although they can still have the identical contents. Normally, struct inequality only makes sense for structs with a finite set of possible values (see 10.2.7.2).

Example

```
struct packet {
    x : int;
    y : int
};

extend sys {
    p1 : packet;
    p2 : packet;
      keep p1 in sys.list_of_input_packets;
      keep p2 in sys.list_of_input_packets;
      keep p1 != p2;
      keep p1.x == p2.x;
      keep p1.y == p2.y
}
```

This code constrains both `p1` and `p2` to be elements of a (pre-built) list of input packets, such that `p1` and `p2` are distinct packets and have the same contents. The generation succeeds if and only if (**iff**) the list `sys.list_of_ input_packets` contains repetitions. There is no contradiction in the fact `p1` and `p2` are different structs with identical contents.

10.2.7.2 Allocation versus aliasing

By default, a new structure is allocated for each item of a struct type. The only exception to that are the cases when the range of possible structs is limited by constraints to a finite number of choices.

Example

```
p : packet;
  keep (packet == sys.input_packet1) or (packet == sys.input_packet2)
```

In this example, the range of values for `packet` is limited by the values `sys.input_packet1` and `sys.input_packet2`, where both values are pre-built structures, i.e., inputs to the constraint. In contrast,

```
keep packet != sys.input_packet1
```

does not limit the choices of `packet` to a finite set. Here, there are an infinite number of ways to allocate `packet` so that it does not point to `sys.input_packet1`. Thus, the system allocates a `NEW` struct for `packet` in this case. This behavior makes struct inequality redundant for those cases where the set of potential struct values is unlimited.

10.2.7.3 Constraining lists

This subclause describes constraining lists. See also Table 25.

10.2.7.3.1 List equality

List equality constraint states that two lists contain the same elements in the same order.

Example

```
extend sys {
    l1 : list of int;
    l2 : list of int;
   !x  : int;
      keep l1 == l2;

    post_generate() is also {
        x = l2.pop()
    }
}
```

This generates two identical lists `l1` and `l2`. Then, `post_generate()` removes the last element of `l2` and preserves it in `x`. `l1` and `l2` are not aliased to the same list by the list equality constraint; they are "copies." Therefore, `l2.pop()` does not remove the last value of `l1`.

10.2.7.3.2 List inequality

The list inequality constraint (`l1 != l2`) states that the items of list type `l1` and `l2` are different. Namely:

a) The number of elements in the lists is different; or

b) The number of elements is the same and there is an index *i* such that

```
l1[i] != l2[i]
```

10.2.7.3.3 List item

The syntax *generatable_path_to_list*[*index*] provides a generatable path of a list element. This syntax can be used in constraints as any other generatable path. List item constraints are fully solvable. Thus, the constraint can be used in several different modes.

Examples

```
keep sys.packets[5] == x;      -- element extraction from fixed list
keep l[7] < 25;                -- constraining certain element of list
keep sys.packets[i].id == 10;  -- index look-up for fixed list and value
keep l[i] < x                  -- multi-way constraint
```

10.2.7.3.4 Item in list

The expression *item* **in** *list* states that *item* is an element of the *list*. Note that a constraint such as

```
keep x in l
```

also implies that `l` includes at least one element, i.e., it is non-empty.

10.2.7.3.5 List in list

The syntax *list1* **in** *list2* provides the way of constraining two lists *list1* and *list2* so *list1* is a (possibly permuted) *sublist* of *list2*. *list1* is a possibly permuted sublist of *list2* if for every valid index *i* in *list1* there exists a matching valid index *j* in *list2* such that `list1[i]==list2[j]`. Every index *j* of *list2* is represented at most once in *list1*.

Informally, this definition means *list1* can be obtained from *list2* by a number (possibly zero) of **delete** operations of elements of *list2* and then applying **is_a_permutation(***list2***)**.

Examples

`{1;2;3}` is a sublist of `{0;1;3;2;3}`

`{1;2;3}` is a permuted sublist of `{1;3;2}`

`{1;1;2}` is a sublist of `{1;3;1;4;2}`

`{1;1;2}` is NOT a sublist of `{1;2;2;3}`

`{1;1;2}` is a permuted sublist of `{2;1;1}`

10.2.7.3.6 Permutations

The syntax *list1***.is_a_permutation(***list2***)** states that *list1* is a permutation of *list2*. The lists *list1* and *list2* contain exactly the same elements and the same numbers of repetitions of each element.

Examples

`{2;3;1}` is a permutation of `{1;2;3}`

`{2;3}` is not a permutation of `{1;2;3}`

`{1;2;3}` is a permutation of `{1;2;3}`

`{2;3;2;1}` is NOT a permutation of `{1;2;3}`

is_a_permutation is a symmetric property, i.e., *list1* is a permutation of *list2* **iff** *list2* is a permutation of *list1*. Thus, the following two constraints are equivalent:

```
keep list1.is_a_permutation(list2);
keep list2.is_a_permutation(list1)
```

10.2.7.3.7 List attributes

There are several properties of lists that can be constrained using the *attribute* syntax, **list.***attribute***(...)**.

list.size()—constrains the size of the list, e.g., `keep my_list.size() in [5..8]`
`my_list` can have `5`,`6`,`7`, or `8` elements.

list.count(*exp***)**—counts the number of list elements satisfying *exp* that have a Boolean type, e.g., `keep my_list.count(it == 3) == 5`
the number `3` appears exactly five times in `my_list`.

list.has(*exp***)**—verifies at least one item of the list satisfies the Boolean *exp*. This is the same as `list.count(`*exp*`) > 0`.

list.unique(*exp***)**—constrains the elements satisfying the Boolean *exp* so they are unique within the list, e.g., `keep my_list.unique(it.is a(RED packet))`
ensures there are no duplicate `RED` packets in `my_list`.

list.sum(*exp***)**—constrains the sum of the list elements satisfying *exp* containing a Boolean type. The attribute applies only to lists of numeric type, e.g., `keep my_list.sum(it) == 100`
for the elements of `my_list` in the range [`0..20`] is `100`.

10.2.7.3.8 Constraining all list items: keep for each

Purpose	Constrain list items	
Category	Struct member	
Syntax	**keep for each** [(*item-name*)] [**using** [**index** (*index-name*)] [**prev** (*prev-name*)]] **in** *gen-item* [**do**] {(*constraint-bool-exp* | *nested-for-each*)**;** ...}	
Parameters	*item-name*	An optional name used as a local variable referring to the current item in the list. The default is **it**.
	index-name	An optional name referring to the index of the current item in the list. The default is **index**.
	prev-name	An optional name referring to the previous item in the list. The default is **prev**.
	gen-item	A generatable item of type list (see 10.4.12).
	constraint-bool-exp	A simple or a compound Boolean expression (see 10.4.11).
	nested-for-each	A nested **for each** block, with the same syntax as the enclosing **for each** block, except that `keep` is omitted.

This defines a value constraint on multiple list items. The following restrictions also apply:

— **for each** constraints can be nested. The parameters *item-name*, *index-name*, and *prev-name* of a nested **for each** can shadow the names used in the outer **for each** blocks. In particular, if the optional names are unspecified, then the default names **it**, **index**, and **prev** refer to the corresponding details of the innermost **for each** block.

— Within a **for each** constraint, **index** represents a running index in the list, which is treated as a constant with respect to each list item.

— Generated items need to be referenced by using a pathname that starts either with **it**, **prev**, or the optional *item-name* or *prev-name*, respectively. Items whose pathname does not start with **it** can only be sampled; their generated values cannot be constrained.

— If a **for each** constraint is contained in a **gen ... keeping** action, the iterated variable needs to be named first.

Syntax example:

```
keep for each (p) in pkl do {
    soft p.protocol in [atm, eth]
}
```

10.2.7.3.9 All solutions

This feature generates lists of structs covering all possible combinations of values for certain fields. The syntax is *list*.**is_all_iterations(**.*fieldname***,** ...**),** where *list* is a list of elements and *fieldname***,** ... are field names of some struct type `T`. The arguments of **is_all_iterations** are unique, i.e., there are no repetitions in the list of fields. All fields shall be defined under the base type `T`, i.e., fields defined in **when** subtypes or **like** successors are not allowed.

Example

```
struct s {
    b1 : bool;
    b2 : bool;
    x  : int
};

extend sys {
    l : list of s;
      keep l.is_all_iterations(.b1, .b2)
}
```

The resulting `sys.l` includes four elements for all four combinations of `TRUE`/`FALSE` of `b1` and `b2`. The values of `x` are chosen randomly.

10.3 Type constraints

This subclause describes how to use type constraints to restrict the declared type of a field to one of its **like** or **when** subtypes for a given context. A constraint prefixed with the **type** modifier is both (a) enforced by the generator (like a regular constraint) and (b) presupposed at compile time for purposes of type checking. Expressions for which type constraints apply are automatically downcast to the specified subtype wherever required. This saves explicit downcasting ["is_a()" and "as a" operators] for the expression and lets the downcast expression be used as a generatable term (rather than input) in constraint contexts.

10.3.1 keep type

Purpose	Refine the type of a field to one of its subtypes for the specified context	
Category	Struct member	
Syntax	**keep type** [**me.**]*field-name* **is a** *type* **keep type** [**me.**]*field-name*.*property-name* == [**me.**]*my-property-name* **keep for each** [(*item-name*)] **in** *list-field-name* **{** … **type** *item-name* **is a** *type*; … **}** **keep for each** [(*item-name*)] **in** *list-field-name* **{** … **type** *item-name*.*property-name* == [**me.**]*my-property-name*; … **}**	
Parameters	*field-name*	The name of a struct field in the enclosing struct.
	type	The name of a struct or unit type.
	property-name	The name of an enumerated or Boolean const field.
	my-property-name	The name of a field of the same type as the *property-name* in this constraint.
	item-name	An optional name used as a local variable referring to the current item in the list. The default is **it**.
	list-field-name	The name of a field of typelist of struct (or unit) in the enclosing struct.

A type constraint can be put either on a field of a struct type or on a list field of a struct type. The declaration is similar to a regular constraint inside a **keep** struct member, or, in the list case, inside a **keep for each** construct, with the **type** keyword prefixing the expression.

The **type** keyword is a constraint modifier syntactically analogous to **soft**. However, unlike **soft**, it can modify only specific constraint expressions and can appear only in restricted contexts.

The type correlation can be fixed or, when the correlated types are **when** subtypes, variable. The former case is expressed using the **is a** operator. In the latter case the determinant property (the **when** determinant) of the referenced struct is equated to a determinant property of the same type in the declaring struct type.

Type constraints affect the static semantics of field-access expressions of the form *instance-expression*.*field-name* (field-access in which *instance-expression* is omitted is equivalent to one having **me** as the *instance-expression*). Typically the static type of a field-access expression is determined according to the type of the field as it was initially declared in the struct type of *instance-expression* (or in one of its supertypes). Type constraints tying the static type of *instance-expression* with a subtype of the field's declared type can change this rule. If the context in which the field-access occurs requires the subtype, the field-access is automatically downcast. In this case, a runtime check is added to ensure that the casting is justified, and an error is issued if it is not. The runtime check involves a minor overhead, not more than that required by the **as_a()** operator.

NOTE

— In the Boolean expression following **type**, operators other than == and **is a** are not allowed.
For example, the following is not allowed:

```
keep type TRUE => engine is a FORD engine // not allowed
```

— The **for each** clause must occur immediately after **keep**. For example, the following is not allowed:

```
keep my_doors.size() > 4 => for each in my_doors { // not allowed
    type it is a small door
}
```

— Type constraints can equate only constant fields, so the **const** keyword must appear in the declaration of fields involved in equality constraints.

— Type constraints in general affect code from that point onwards. This includes type constraints that appear inside a **for each** clause, in which case other expressions in the same scope after the declaration (but not before it) can assume automatic casting.

— Type constraints cannot appear inside a **gen** action.

— The **soft** keyword cannot be used with type constraints.

— As with non-type constraints, the determinant field of the when subtype is assigned only during generation. Thus the **pre_generate()** method of the type specified in the type constraint is not called during generation.

— A field's type may be restricted by more than one type constraint with respect to different "when" dimensions (determinant fields).

Syntax example:

```
keep type f.p1 == p1;
keep for each in lf {
    type it is a B S1
}
```

10.3.2 Type constraints and struct fields

Automatic casting of a struct-reference field is performed in any context that requires it, including the following:

— Struct-member access

— Assignment

— Parameter passing

10.3.3 Type constraints and list fields

When the type relation is one-to-many, in other words, when a list field is concerned, automatic casting is applied not to the list itself but to its elements. Automatic casting affects list operators whose result type is the element type, such as indexing (the [] operator) and **pop()**. It also affects the iteration variable inside the **for each** construct, both in procedural and in constraint contexts.

10.3.4 Type constraints and like subtypes

Type constraints work just as well for **like** subtypes of the declared type of the field. They apply to the two "**is a**" forms of the **keep type** struct member.

Note that type constraints with **like** subtypes cannot make the actual **like** type of a generated field dependent on a **when** determinant. In other words, they may not figure under a **when** subtype if they affect a field not declared in the same subtype. This is an error: the constraint is unenforceable.

10.4 Defining constraints

This subclause describes the constructs used to define constraints. See also 4.10.

10.4.1 keep

Purpose	Define a hard value constraint	
Category	Struct member	
Syntax	**keep** [*name* **is [only]**] *constraint-bool-exp*	
Parameters	*name*	Optional identifier for constraint overriding and reference by tools.
	constraint-bool-exp	A simple or a compound Boolean expression (see 10.4.11).

This states restrictions on the values generated for fields in the struct or its subtree, or describes required relationships between field values and other items in the struct or its subtree.

Hard constraints are applied whenever the enclosing struct is generated. For any **keep** constraint in a generated struct, the generator either meets the constraint or issues a constraint contradiction message. If the **keep** constraint appears under a **when** construct, the constraint is considered only if the **when** condition is true.

Syntax example (un-named constraint):

```
keep kind != tx or len == 16
```

Syntax example (named constraint):

```
keep address_range is soft addr in [0..9]
```

10.4.1.1 Constraint overriding

Every named constraint must have exactly one actual definition per struct type. An initial definition of a constraint in a struct type may be overridden in **like** and **when** subtypes or in later extensions of the same struct—any number of times—using the **is only** modifier.

The semantics of constraint overriding is identical to that of overriding other extendable struct members, such as methods. A constraint can be redefined in different when subtypes (even if they are not contradictory), and the latest definition that applies to the generated subtype is chosen (for ordering definitions see Annex B).

Example:

```
struct packet {
   size: [big, small];
   data: list of byte;
      keep data_size is undefined; // abstract constraint

   when big packet {
      keep data_size is all of { // concrete definition for big packets
         data.size() > 10;
         data.size() < 20
      }
   }
}
```

10.4.2 keep is undefined

Purpose	Define an abstract constraint
Category	Struct member
Syntax	**keep** *name* **is undefined**
Parameters	*name* Optional identifier for constraint overriding and reference by tools.

The **undefined** keyword can be used to declare an abstract property that will be defined later using a **keep is only** struct member with the same name.

Trying to generate an instance of a struct type for which a constraint was left undefined results in an error.

10.4.3 keep all of {...}

Purpose	Define a constraint block	
Category	Struct member	
Syntax	**keep** [*name* **is [only]**] **all of** {*constraint-bool-exp*; ...}	
Parameters	*name*	Optional identifier for constraint overriding and reference by tools.
	constraint-bool-exp	A simple or a compound Boolean expression (see 10.4.11).

A **keep** constraint block is exactly equivalent to a **keep** constraint for each constraint Boolean expression in the block. The **all of** block can be used as a constraint Boolean expression itself.

Syntax example:

```
keep all of {
    kind != tx;
    len == 16
}
```

10.4.4 keep struct-list.is_all_iterations()

Purpose	Cause a list of structs to have all iterations of a field	
Category	Constraint-specific list method	
Syntax	**keep** [*name* **is [only]**] *gen-item*.**is_all_iterations(**.*field-name*: exp**,** ...**)**	
Parameters	*name*	Optional identifier for constraint overriding and reference by tools.
	gen-item	A generatable item of type list of struct (see 10.4.12).
	field-name	The name of a scalar field of a struct. The field name shall be prefixed by a period (**.**). The order of fields in this list does not affect the order in which they are iterated. The specified field that is defined first in the struct is the one that is iterated first.

This causes a list of structs to have all legal, non-contradicting iterations of the fields specified in the field list. Fields not included in the field list are not iterated; their values can be constrained by other relevant constraints. The highest value always occupies the last element in the list.

Soft constraints on fields specified in the field list are skipped. All other relevant hard constraints on the list and on the struct are applied. If these constraints reduce the ranges of some of the fields in the field list, then the generated list is also reduced.

The following restrictions also apply:

— The number of iterations in a list produced by *list***.is_all_iterations()** is the product of the number of possible values in each field in the list. Use the **absolute_max_list_size** generation configuration option to set the maximum number of iterations allowed in a list (the default is 524 288).

— The *list***.is_all_iterations()** method shall only be used in a constraint Boolean expression.

— The fields to be iterated shall be of a scalar type, not a list or struct type.

Syntax example:

```
keep packets.is_all_iterations(.kind, .protocol)
```

10.4.5 keep soft

Purpose	Define a soft value constraint	
Category	Struct member	
Syntax	**keep** [*name* **is [only]**] **soft** *constraint-bool-exp*	
Parameters	*name*	Optional identifier for constraint overriding and reference by tools.
	constraint-bool-exp	A simple Boolean expression (see 10.4.11).

This suggests default values for fields or variables in the struct or its subtree, or describes suggested relationships between field values and other items in the struct or its subtree. The following restrictions apply:

— Soft constraints are order dependent (see 10.2.6) and shall not be met if they conflict with hard constraints or soft constraints that have already been applied.

— The **soft** keyword shall not be used in compound Boolean expressions.

— Individual constraints inside a constraint block can be soft constraints.

— Because soft constraints only suggest default values, it is better not to use them to define architectural constraints.

Syntax example:

```
keep soft legal
```

10.4.6 keep gen ... before

Purpose	Modify the generation order	
Category	Struct member	
Syntax	**keep gen (***gen-item*: exp**, ...) before (***gen-item*: exp**, ...)**	
Parameters	*gen-item*	An expression that returns a generatable item. The parentheses [( )] are required. See also 10.4.12.

This requires the generatable items specified in the first list to be generated before the items specified in the second list. This constraint can be used to influence the distribution of values by preventing soft value constraints from being consistently skipped (see 10.2). The following restrictions also apply:

— This constraint itself can cause constraint cycles. If a constraint cycle involving one of the fields in the **keep gen** ... **before** constraint exists and if the **resolve_cycles** generation configuration option is `TRUE`, the constraint can be ignored if the program cannot satisfy both it and other constraints that conflict with it.

— This constraint cannot appear on the LHS of a implication operator (=>).

Syntax example:

```
keep gen (y) before (x)
```

10.4.7 keep soft gen ... before

Purpose	Suggest order of generation	
Category	Struct member	
Syntax	**keep soft gen (***gen-item*: exp**, ...) before (***gen-item*: exp**, ...)**	
Parameters	*gen-item*	An expression that returns a generatable item. The parentheses [( )] are required. See also 10.4.12.

This modifies the *soft* generation order by recommending the fields specified in the first field list be generated before the fields specified in the second field list. This soft generation order is second in priority to the hard generation order created by dependencies between parameters and **keep gen before** constraints.

This constraint can be used to suggest a generation order that is later overridden in individual tests with a hard order constraint. This constraint cannot appear on the LHS of a implication operator (=>).

Syntax example:

```
keep soft gen (y) before (x)
```

10.4.8 keep gen_before_subtypes()

Purpose	Specify a **when** determinant field for deferred generation	
Category	Struct member	
Syntax	**keep gen_before_subtypes(***determinant-field*: field**, ...)**	
Parameters	*determinant-field*	An expression that evaluates to the name of a field in the struct type. The field shall have at least one value that is used as a **when** determinant for a subtype definition. If the field is not a **when** determinant field, a warning is issued and the constraint is ignored. Multiple field expressions can be entered, separated by commas (**,**).

To speed up generation of structs with multiple **when** subtypes, this type of constraint, called a *subtype optimization constraint*, causes the generator engine to wait until a **when** determinant value is generated for a specified field before it analyzes constraints and generates fields under the **when** subtype.

When no subtype optimization constraints are present in a struct, the generator analyzes all of the constraints and fields in the struct before it generates the struct, even those constraints and fields that are defined under **when** subtypes. When a subtype optimization constraint is present, the generator initially analyzes only the constraints and fields of the base struct type. When a subtype optimization **when** determinant is encountered, the generator analyzes the associated **when** subtype and then generates it.

The following considerations also apply:

— Subtype optimization can handle multiple determinants. Subtypes are analyzed and generated in the order in which their **when** determinants are encountered.

— If multiple determinants are specified, and some of them are subtype optimization determinants while others are not, then a subtype that is a result of multiple inheritance of a subtype optimization determinant and a non-subtype optimization determinant shall be treated the same.

— The generator engine's ability to resolve contradictions is diminished somewhat by subtype optimization constraints. Specifically, the generator might not be able to resolve contradictions arising from constraints under subtypes that involve fields of the base type.

— The analysis and generation is recursive. If a subtype contains another determinant that is specified in a subtype optimization constraint, then that sub-subtype is analyzed and generated as soon as its determinant field is generated under the higher-level subtype.

Syntax example:

```
keep gen_before_subtypes(format)
```

10.4.9 keep reset_gen_before_subtypes()

Purpose	Disable all previous **keep gen_before_subtypes()** subtype optimization constraints
Category	Struct member
Syntax	**keep reset_gen_ before_subtypes()**

When subtype optimization is turned off by default, this constraint causes the generator to ignore all previously defined **gen_before_subtypes()** constraints for the enclosing struct or unit. Any such constraints defined after the reset shall be followed.

When subtype optimization is turned on by default, this constraint turns off subtype optimization for the enclosing struct or unit. When subtype optimization is forced on or off, this constraint has no effect.

Syntax example:

```
keep reset_gen_before_subtypes()
```

10.4.10 read_only()

Purpose	Modify generation sequence
Category	Pseudo-method
Syntax	**read_only(***item*: exp**)**
Parameters	*item* A legal ***e*** expression.

This generates values for any data items that are contained in the expression and returns the value of the expression. This method affects generation order and also makes the constraint unidirectional.

Example

```
keep a == read_only(b + c)
```

This constraint has two results:

— `b` and `c` are generated before `a`.

— The value of `a` cannot otherwise be constrained.

Syntax example:

```
keep i < read_only(j)
```

10.4.11 constraint-bool-exp

Purpose	Define a constraint on a generatable item	
Category	Expression	
Syntax	*bool-exp* [**or** | **and** | => *bool-exp*] ...	
Parameters	*bool-exp*	An expression that returns either `TRUE` or `FALSE` when evaluated at runtime.

A *constraint Boolean expression* is a simple or compound Boolean expression that describes the legal values for at least one generatable item or constrains the relation of one generatable item with others. A compound Boolean expression is composed of two or more simple expressions joined with the **or**, **and**, or implication (=>) operators. Table 25 shows the ***e*** special constructs that are useful in constraint Boolean expressions.

Table 25—Constraining Boolean expressions

Constraint	Definition
soft	A keyword that indicates the constraint is either a soft value constraint or a soft order constraint. See 10.4 for a definition of these types of constraints.
soft...select	An expression that constrains the distribution of values.
.reset_soft()	A pseudo-method that causes the test generator to quit evaluation of soft constraints for a field, in effect, removing previously defined soft constraints.
.is_all_iterations()	A list method used only within constraint Boolean expressions that causes a list of structs to have all legal, non-contradicting iterations of the specified fields.
.is_a_permutation()	A list method that can be used within constraint Boolean expressions to constrain a list to have the same elements as another list.
[not] in	An operator that can be used within constraint Boolean expressions to constrain an item to a range of values or a list to be a subset of another list; or when used with **not**, to be outside the range or absent from another list.
is [not] a	An operator that checks the subtype of a struct.

The following considerations also apply:

— The **soft** keyword can be used in simple Boolean expressions, but not in compound Boolean expressions.

— The order of precedence for Boolean operators is: **and**, **or**, =>. A compound expression containing multiple Boolean operators of equal precedence is evaluated from left to right, unless parentheses [`()`] are used to indicate expressions of higher precedence.

— Any ***e*** operator can be used in a constraint Boolean expression. However, certain operators can affect generation order or can create an constraint that is not enforceable.

— In compound expressions where multiple implication operators are used, the order in which the operations are performed is significant. For example, in the following constraint, the first expression (`a => b`) is evaluated first by default:

```
keep a => b => c;               // is equivalent to:
keep (not a or b) => c;         // is equivalent to:
keep a and (not b) or c
```

However, adding parentheses around the expression (`b => c`) causes it to be evaluated first, with very different results.

```
keep a => (b => c);             // is equivalent to:
keep a => (not b) or c;         // is equivalent to:
keep (not a) or (not b) or c
```

Examples

The following are examples of simple constraint Boolean expressions:

```
not short        // where "short" is of type "bool"
long == TRUE
soft x > y
x + z == y + 7
```

The following are examples of compound constraint Boolean expressions:

```
x > 0 and soft x < y
is_a_good_match(x, y) => z < 1024
color != red or resolution in [900..999]
packet is a good packet => length in [0..1023]
```

See also 5.1.1.

Syntax example:

```
z == x + y
```

10.4.12 gen-item

Purpose	Identifies a generatable item
Category	Expression
Syntax	[**me.**]*field1-name*[.*field2-name* ...] | **it** | [**it**].*field1-name*[.*field2-name* ...]
Parameters	*field-name* The name of a field in the current struct or struct type.

A *generatable item* is an operand in a Boolean expression that describes the legal values for that generatable item or constrains its relation with another generatable item. Every constraint shall have at least one generatable item or an error shall be issued.

In a **keep** constraint, the syntax for specifying a generatable item is a path starting with **me** of the struct containing the constraint and ending with a field name. In a **gen** action, the syntax for specifying a generatable item is a path starting with **it** of the struct containing the constraint and ending with a field name.

A generatable item cannot have an indexed reference in it, except as the last item in the path. See also 4.3.3.

Syntax example:

```
me.protocol
```

10.5 Invoking generation

There are two ways of invoking generation, as follows:

a) Generation is invoked automatically when generating the tree of structures starting at **sys**.

b) Generation can be called for any data item by using the **gen** action. The scope of this type of generation is restricted (see 10.5.1). The generation order is (recursively):

   1) Allocate the new struct
   2) Call **pre_generate()**
   3) Perform generation
   4) Call **post_generate()**

10.5.1 gen

Purpose	Generate values for an item	
Category	Action	
Syntax	**gen** *gen-item* [**keeping** {[**it**].*constraint-bool-exp***;** ...}]	
Parameters	*gen-item*	A generatable item. If the expression is a struct, it is automatically allocated, and all fields under it are generated recursively, in depth-first order.
	constraint-bool-exp	A simple or compound Boolean expression (see 10.4.11).

This generates a random value for the instance of the item specified in the expression and stores the value in that instance, while considering all the constraints specified in the **keeping** block, as well as other relevant constraints at the current scope on that item or its children. Constraints defined at a higher scope than the enclosing struct are not considered.

The following considerations also apply:

— Values for particular struct instances, fields, or variables can be generated during simulation (on-the-fly generation) by using the **gen** action.
— This constraint can also be used to specify constraints that apply only to one instance of the item.
— The **soft** keyword can be used in the list of constraints within a **gen** action.
— The earliest the **gen** action can be called is from a struct's **pre_generate()** method.
— The generatable item for the **gen** action cannot include an index reference.
— If a **gen ... keeping** action contains a **for each** constraint, the iterated variable needs to be named.

Syntax example:

```
gen next_packet keeping {
    .kind in [normal, control]
}
```

10.5.2 pre_generate()

Purpose	Method run before generation of struct
Category	Method of **any_struct**
Syntax	[*struct-exp*.]**pre_generate()**
Parameters	*struct-exp* An expression that returns a struct. The default is the current struct.

The **pre_generate()** method is run automatically after an instance of the enclosing struct is allocated, but before generation is performed. This method is initially empty, but can be extended to apply values procedurally to prepare constraints for generation. It can also be used to simplify constraint expressions before they are analyzed by the constraint resolution engine.

NOTE—Prefix the ! character (see 6.8) to the name of any field whose value is determined by **pre_generate()**. Otherwise, normal generation overwrites this value.

Syntax example:

```
pre_generate() is also {
    m = 7
}
```

10.5.3 post_generate()

Purpose	Method run after generation of struct
Category	Predefined method of **any_struct**
Syntax	[*struct-exp*.]**post_generate()**
Parameters	*struct-exp* An expression that returns a struct. The default is the current struct.

The **post_generate()** method is run automatically after an instance of the enclosing struct is allocated and both pre-generation and generation have been performed. This method can be extended for **any_struct** to manipulate values produced during generation. It can also be used to derive more complex expressions or values from the generated values.

Syntax example:

```
post_generate() is also {
    m = m1 + 1
}
```