A  An RSL Primer

This is an ultra-short introduction to the RAISE Specification Language, RSL. Examples follow and expand on the examples of earlier sections.

A.1  Types

The reader is kindly asked to study first the decomposition of this section into its sub-parts and sub-sub-parts.

A.1.1  Type Expressions

Type expressions are expressions whose values are types, that is, possibly infinite sets of values (of “that” type).

Atomic Types  Atomic types have (atomic) values. That is, values which we consider to have no proper constituent (sub-)values, i.e., cannot, to us, be meaningfully “taken apart”.

RSL has a number of built-in atomic types. There are the Booleans, integers, natural numbers, reals, characters, and texts.

Basic Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bool</td>
<td>False, true</td>
</tr>
<tr>
<td>Int</td>
<td>Integers, ..., -2, -1, 0, 1, 2, ...</td>
</tr>
<tr>
<td>Nat</td>
<td>Positive integer values 0, 1, 2, ...</td>
</tr>
<tr>
<td>Real</td>
<td>Values whose numerals can be written as an integer, followed by a period (“.”), followed by a natural number (the fraction).</td>
</tr>
<tr>
<td>Char</td>
<td>Characters, “a”, “b”, ...</td>
</tr>
<tr>
<td>Text</td>
<td>Character strings, “aa”, “aaa”, ..., “abc”, ...</td>
</tr>
</tbody>
</table>

Example 1  Basic Net Attributes:

- For safe, uncluttered traffic, hubs and links can ‘carry’ a maximum of vehicles.
- Links have lengths. (We ignore hub (traversal) lengths.)
- One can calculate whether a link is a two-way link.
type
  MAX = Nat
  LEN = Real
  is_Two_Way_Link = Bool

value
  obs_Max: (H|L) → MAX
  obs_Len: L → LEN
  is_two_way_link: L → is_Two_Way_Link
  is_two_way_link(l) ≡ ∃ lσ:LS • lσ ∈ obs_HΣ(l) ∧ card lσ = 2

End of Example 1

Composite Types

Composite types have composite values. That is, values which we consider to have proper constituent (sub-)values, i.e., can, to us, be meaningfully “taken apart”.

From these one can form type expressions: finite sets, infinite sets, Cartesian products, lists, maps, etc.

Let A, B and C be any type names or type expressions, then:

Composite Type Expressions

[8] A-infset
[9] A × B × ... × C
[10] A∗

7. The set type of finite cardinality set values.
8. The set type of infinite and finite cardinality set values.
9. The Cartesian type of Cartesian values.
10. The list type of finite length list values.
11. The list type of infinite and finite length list values.
12. The map type of finite definition set map values.
13. The function type of total function values.
14. The function type of partial function values.
15. In (A) A is constrained to be:
   • either a Cartesian B × C × ... × D, in which case it is identical to type expression kind 9,
   • or not to be the name of a built-in type (cf., 1–6) or of a type, in which case the parentheses serve as simple delimiters, e.g., (Aω B), or (A∗)-set, or (A-set)list, or (A|B)ω (C|D|(Eω F)), etc.
16. The postulated disjoint union of types A, B, ..., and C.
17. The record type of `mk_id`-named record values `mk_id(av, ..., bv)`, where `av`, ..., `bv`, are values of respective types. The distinct identifiers `sel_a`, etc., designate selector functions.

18. The record type of unnamed record values `(av, ..., bv)`, where `av`, ..., `bv`, are values of respective types. The distinct identifiers `sel_a`, etc., designate selector functions.

**Example 2**

Composite Net Type Expressions:

The type clauses of function signatures:

value

```plaintext
f: A → B
```

often have the type expressions `A` and/or `B` be composite type expressions:

value

```plaintext
obs_Hls: L → HI-set
obs_Lls: H → LI-set
obs_HΣ: H → HT-set
set_HΣ: H × HΣ → H
```

Right-hand sides of type definitions often have composite type expressions:

**Type Definition**

```plaintext
type
N = H-set × L-set
HT = LI × HI × LI
LT' = HI × L1 × HI
```

End of Example 2

**A.1.2 Type Definitions**

Concrete Types Types can be concrete in which case the structure of the type is specified by type expressions:

Type Definition

```plaintext
type
A = Type_expr
```

schematic examples:

- `A1 = B1-set, A2 = B1-infset`
- `A3 = B2 × C1 × D1`
- `B1 = E*, B2 = Eω`
- `C1 = F m G`
- `D1 = H → J, D2 = H ∼ J`
- `K = L | M`
Example 3 ................................................ Composite Net Types:
There are many ways in which nets can be concretely modelled:

- **Sorts + Observers + Axioms:** First we show an example of type definitions without right-hand side, that is, of sort definitions.

  From a net one can observe many things.
  
  Of the things we focus on are the hubs and the links.

  A net contains two or more hubs and one or more links. Possibly other entities and net attributes may also be observable, but we shall not consider those here.

  type
  \[ \text{[sorts]} N_\alpha, H, L, H_I, L_I \]
  value
  \[
  \begin{align*}
  \text{obs}_H: N_\alpha &\to H\text{-set} \\
  \text{obs}_L: N_\alpha &\to L\text{-set}
  \end{align*}
  \]
  axiom
  \[
  \forall n: N_\alpha \cdot \text{card obs}_H(n) > 0 \Rightarrow \text{card obs}_L(n) \geq 1 \land ...
  \]

- **Cartesians + Wellformedness:** A net can be considered as a Cartesian of sets of two or more hubs and sets of one or more links.

  type
  \[ \text{[sorts]} H, L \]
  \[ N_\beta = H\text{-set} \times L\text{-set} \]
  value
  \[
  \begin{align*}
  \text{wf}_N: N_\beta &\to \text{Bool} \\
  \text{wf}_N(hs,ls) &\equiv \text{card hs > 1 } \Rightarrow \text{card ls > 0 } .... \\
  \text{inject}_N: N_\alpha &\to N_\beta \text{ pre: } \text{wf}_N hs,ls \\
  \text{inject}_N(n_\alpha) &\equiv (\text{obs}_H H(n_\alpha), \text{obs}_L L(n_\alpha))
  \end{align*}
  \]

- **Cartesians + Maps + Wellformedness:** Or a net can be described

  a as a triple of b-c-d:

  b hubs (modelled as a map from hub identifiers to hubs),

  c links (modelled as a map from link identifiers to links), and

  d a graph from hub \( h_i \) identifiers \( h_{i_\alpha} \), to maps from identifiers \( l_{ij} \) of hub \( h_i \) connected

  links \( l_{ij} \) to the identifiers \( h_{j_i} \) of link connected hubs \( h_j \).
type
  [sorts] H, HI, L, LI
  [a] N_s = HUBS × LINKS × GRAPH
  [b] HUBS = HI \to H
  [c] LINKS = LI \to L
  [d] GRAPH = HI \to (LI – m > HI)

  – [b,c] hs:HUBS and ls:LINKS are maps from hub (link) identifiers to hubs (links)
    where one can still observe these identifiers from these hubs (link).

  • Example 12 on page 111 defines the well-formedness predicates for the above map types.

Variety of Type Definitions
[1] Type_name = Type_expr /* without | s or subtypes */
[2] Type_name = Type_expr.1 | Type_expr.2 | ... | Type_expr.n
[3] Type_name == mk_id_1(s_a1:Type_name.a1,...,s_ai:Type_name.ai) | ...
                  mk_id_n(s_a1:Type_name.a1,...,s_zk:Type_name.zk)
[4] Type_name :: sel_a:Type_name.a ... sel_z:Type_name.z
[5] Type_name = { | v:Type_name' • \mu(v) |}

where a form of [2–3] is provided by combining the types:

Record Types
Type_name = A | B | ... | Z
A == mk_id_1(s_a1:A.1,...,s_ai:A.i)
B == mk_id_2(s_b1:B.1,...,s_bj:B.j)
...
Z == mk_id_n(s_z1:Z.1,...,s_zk:Z.k)

Types A, B, ..., Z are disjoint, i.e., shares no values, provided all mk_id.k are distinct and
due to the use of the disjoint record type constructor ==.

axiom
  \forall a1:A.1, a2:A.2, ..., ai:Ai •
    s_a1(mk_id_1(a1,a2,...,ai))=a1 \land s_a2(mk_id_1(a1,a2,...,ai))=a2 \land
    ... \land s_ai(mk_id_1(a1,a2,...,ai))=ai \land
  \forall a:A • let mk_id_1(a1',a2',...,ai') = a in
    a1' = s_a1(a) \land a2' = s_a2(a) \land ... \land ai' = s_ai(a) end
Example 4 .......................... Net Record Types: Insert Links:

19. To a net one can insert a new link in either of three ways:

   a) Either the link is connected to two existing hubs — and the insert operation must therefore specify the new link and the identifiers of two existing hubs;

   b) or the link is connected to one existing hub and to a new hub — and the insert operation must therefore specify the new link, the identifier of an existing hub, and a new hub;

   c) or the link is connected to two new hubs — and the insert operation must therefore specify the new link and two new hubs.

   d) From the inserted link one must be able to observe identifier of respective hubs.

20. From a net one can remove a link.\textsuperscript{13} The removal command specifies a link identifier.

\begin{verbatim}
type
  19 Insert == Ins(s_ins:Ins)
  19 Ins = 2xHubs | 1x1nH | 2nHs
  19a 2xHubs == 2oldH(s_hi1:HI,s_l:L,s_hi2:HI)
  19b 1x1nH == 1oldH1newH(s_hi:HI,s_l:L,s_h:H)
  19c 2nHs == 2newH(s_h1:H,s_l:L,s_h2:H)

axiom
  19d ∀ 2oldH(hi',l,hi''):Ins • hi'\neq hi'' ∧ obs_LIs(l)={hi',hi''} ∧
     ∀ 1old1newH(hi,l,h):Ins • obs_LIs(l)={hi,obs_HI(h)} ∧
     ∀ 2newH(h',l,h''):Ins • obs_LIs(l)={obs_HI(h'),obs_HI(h'')}
\end{verbatim}

RSL Explanation

- 19: The type clause type Ins = 2xHubs | 1x1nH | 2nHs introduces the type name Ins and defines it to be the union (|) type of values of either of three types: 2xHubs, 1x1nH and 2nHs.

  19a): The type clause type 2xHubs == 2oldH(s_hi1:HI,s_l:L,s_hi2:HI) defines the type 2xHubs to be the type of values of record type 2oldH(s_hi1:HI,s_l:L,s_hi2:HI), that is, Cartesian-like, or “tree”-like values with record (root) name 2oldH and with three sub-values, like branches of a tree, of types HI, L and HI. Given a value, cmd, of type 2xHubs, applying the selectors s_hi1, s_l and s_hi2 to cmd yield the corresponding sub-values.

\textsuperscript{13}\textsuperscript{13} provided that what remains is still a proper net
19b): Reading of this type clause is left as exercise to the reader.
19c): Reading of this type clause is left as exercise to the reader.
19d): The axiom has three predicate clauses, one for each category of Insert commands.

- The first clause: \( \forall 2\text{oldH}(hi', l, hi''):\text{Ins} \cdot hi' \neq hi'' \land \text{obs}\_\text{HIs}(l) = \{hi', hi''\} \) reads as follows:
  - For all record structures, \( 2\text{oldH}(hi', l, hi'') \), that is, values of type Insert (which in this case is the same as of type \( 2\times\text{Hubs} \)),
  - that is values which can be expressed as a record with root name \( 2\text{oldH} \) and with three sub-values ("freely") named \( hi' \), \( l \) and \( hi'' \)
  - (where these are bound to be of type HI, L and HI by the definition of \( 2\times\text{Hubs} \)),
  - the two hub identifiers \( hi' \) and \( hi'' \) must be different,
  - and the hub identifiers observed from the new link, \( l \), must be the two argument hub identifiers \( hi' \) and \( hi'' \).
- Reading of the second predicate clause is left as exercise to the reader.
- Reading of the third predicate clause is left as exercise to the reader.

The three types \( 2\times\text{Hubs}, 1\times\text{1nH} \) and \( 2\times\text{Hs} \) are disjoint: no value in one of them is the same value as in any of the other merely due to the fact that the record names, \( 2\text{oldH}, 1\text{oldH}1\text{newH} \) and \( 2\text{newH} \), are distinct. This is no matter what the "bodies" of their record structure is, and they are here also distinct: \( (s_{hi1}:\text{HI}, s_{hi2}:\text{HI}), (s_{hi}:\text{HI}, s_{l}:\text{L}, s_{h}:\text{H}) \), respectively \( (s_{h1}:\text{H}, s_{l}:\text{L}, s_{h2}:\text{H}) \).

20: The type clause \( \text{type Remove} == \text{Rmv}(s_{li}:\text{LI}) \)

- (as for Items 19b and 19c))
- defines a type of record values, say \( \text{rmv} \),
- with record name \( \text{Rmv} \) and with a single sub-value, say \( li \) of type \( \text{LI} \)
- where \( li \) can be selected from by \( \text{rmv selector } s_{li} \).

End of RSL Explanation

Example 17 on page 122 presents the semantics functions for \( \text{int\_Insert} \) and \( \text{int\_Remove} \).

End of Example 4

Subtypes

In RSL, each type represents a set of values. Such a set can be delimited by means of predicates. The set of values \( b \) which have type \( B \) and which satisfy the predicate \( P \), constitute the subtype \( A \):
Subtypes

type
A = { | b:B • P(b) | }

Example 5

Net Subtypes:
In Example 3 on page 91 we gave three examples. For the first we gave an example, Sorts + Observers + Axioms, “purely” in terms of sets, see Sorts — Abstract Types below. For the second and third we gave concrete types in terms of Cartesians and Maps.

- In the Sorts + Observers + Axioms part of Example 3
  - a net was defined as a sort, and so were its hubs, links, hub identifiers and link identifiers;
  - axioms – making use of appropriate observer functions - make up the wellformedness condition on such nets.

We now redefine this as follows:

type
[ sorts ] N', H, L, HI, LI
N = { |n:N' • wf_N(n)| }

value
wf_N: N' → Bool
wf_N(n) ≡
∀ n:N • card obs_Hs(n)≥0 ∧ card obs_Ls(n)≥0 ∧
axioms 2.–3., 5.–6., and 8., (Page 13)

- In the Cartesians + Wellformedness part of Example 3
  - a net was a Cartesian of a set of hubs and a set of links
  - with the wellformedness that there were at least two hubs and at least one link
  - and that these were connected appropriately (treated as ...).

We now redefine this as follows:

type
N' = H-set × L-set
N = { |n:N' • wf_N(n)| }

- In the Cartesians + Maps + Wellformedness part of Example 3
An RSL Primer

− a net was a triple of hubs, links and a graph,
− each with their wellformedness predicates.

We now redefine this as follows:

\[
\begin{align*}
\text{type} & \\
\text{[sorts]} & \equiv L, H, LI, HI \\
N' & \equiv HUBS \times LINKS \times GRAPH \\
N & \equiv \{ (hs, ls, g) : N' \land \text{wf}_HUBS(hs) \land \text{wf}_LINKS(ls) \land \text{wf}_GRAPH(g)(hs, ls) \} \\
\text{HUBS}' & \equiv HI \rightarrow m^H \\
\text{HUBS} & \equiv \{ hs : \text{HUBS}' \land \text{wf}_HUBS(hs) \} \\
\text{LINKS}' & \equiv LI \rightarrow L \\
\text{LINKS} & \equiv \{ ls : \text{LINKS}' \land \text{wf}_LINKS(ls) \} \\
\text{GRAPH}' & \equiv HI \rightarrow m (LI \rightarrow m HI) \\
\text{GRAPH} & \equiv \{ g : \text{GRAPH}' \land \text{wf}_GRAPH(g) \} \\
\\text{value} & \\
\text{wf}_GRAPH : GRAPH' \rightarrow (HUBS \times LINKS) \rightarrow \text{Bool} \\
\text{wf}_GRAPH(g)(hs, ls) & \equiv \text{wf}_N(hs, ls, g)
\end{align*}
\]

Example 12 on page 111 presents a definition of \text{wf}_GRAPH.

End of Example 5

Sorts — Abstract Types

Types can be (abstract) sorts in which case their structure is not specified:

\textbf{Sorts}

\textbf{type} \\
A, B, ..., C

Example 6

Net Sorts:

In formula lines of Examples 3–5 we have indicated those type clauses which define sorts, by bracketed [sorts] literals.

End of Example 6

A.2 Concrete RSL Types: Values and Operations

A.2.1 Arithmetic
Arithmetic

type
Nat, Int, Real
value
\(+, -, *, /\, : \text{Nat} \times \text{Nat} \rightarrow \text{Nat} \mid \text{Int} \times \text{Int} \rightarrow \text{Int} \mid \text{Real} \times \text{Real} \rightarrow \text{Real}
\langle, \leq, =, \neq, \geq, \rangle (\text{Nat} | \text{Int} | \text{Real}) \times (\text{Nat} | \text{Int} | \text{Real}) \rightarrow \text{Bool}

A.2.2 Set Expressions

Set Enumerations Let the below a’s denote values of type A, then the below designate simple set enumerations:

Set Enumerations

\{\{}\, \{a\}, \{e_1,e_2,...,e_n\}, ... \subseteq \text{A-set}
\{\{}\, \{a\}, \{e_1,e_2,...,e_n\}, ..., \{e_1,e_2,...\}\} \subseteq \text{A-infset}

Example 7 Set Expressions over Nets:

We now consider hubs to abstract cities, towns, villages, etcetera. Thus with hubs we can associate sets of citizens.

Let c:C stand for a citizen value c being an element in the type C of all such. Let g:G stand for any (group) of citizens, respectively the type of all such. Let s:S stand for any set of groups, respectively the type of all such. Two otherwise distinct groups are related to one another if they share at least one citizen, the liaisons. A network nw:NW is a set of groups such that for every group in the network one can always find another group with which it shares liaisons. Solely using the set data type and the concept of subtypes, we can model the above:

type
\( C \)
\( G' = \text{C-set}, \; G = \{ | g:G' \cdot g\neq\{} \mid \}
\( S = \text{G-set} \)
\( L' = \text{C-set}, \; L = \{ | \ell:L' \cdot \ell\neq\{} \mid \}
\( \text{NW'} = S, \; \text{NW} = \{ | s:S \cdot \text{wf}_S(s) \mid \}

value
\( \text{wf}_S: S \rightarrow \text{Bool} \)
\( \text{wf}_S(s) \equiv \forall g:G \cdot g \in s \Rightarrow \exists g':G \cdot g' \in s \land \text{share}(g,g') \)
share: G\times G \rightarrow \text{Bool}
\( \text{share}(g,g') \equiv g\neq g' \land g \cap g' \neq \{} \)
liaisons: G\times G \rightarrow L
\( \text{liaisons}(g,g') = g \cap g' \text{ pre share}(g,g') \)
Annotations: L stands for proper liaisons (of at least one liaison). G’, L’ and N’ are the “raw” types which are constrained to G, L and N. \{ | binding:type_expr • bool_expr | \} is the general form of the subtype expression. For G and L we state the constraints “in-line”, i.e., as direct part of the subtype expression. For NW we state the constraints by referring to a separately defined predicate. \( \text{wf}_S(s) \) expresses — through the auxiliary predicate — that s contains at least two groups and that any such two groups share at least one citizen. liaisons is a “truly” auxiliary function in that we have yet to “find an active need” for this function!

The idea is that citizens can be associated with more than one city, town, village, etc. (primary home, summer and/or winter house, working place, etc.). A group is now a set of citizens related by some “interest” (Rotary club membership, political party “grassroots”, religion, et.). The reader is invited to define, for example, such functions as: The set of groups (or networks) which are represented in all hubs [or in only one hub]. The set of hubs whose citizens partake in no groups [respectively networks]. The group [network] with the largest coverage in terms of number of hubs in which that group [network] is represented.

End of Example 7

Set Comprehension

The expression, last line below, to the right of the \( \equiv \), expresses set comprehension. The expression “builds” the set of values satisfying the given predicate. It is abstract in the sense that it does not do so by following a concrete algorithm.

Set Comprehension

type
A, B
P = A \rightarrow \text{Bool}
Q = A \sim \rightarrow B
value
comprehend: A-infset \times P \times Q \rightarrow B-infset
comprehend(s,P,Q) \equiv \{ Q(a) | a:A \cdot a \in s \land P(a) \}

Example 8

Item 48 on page 22, the \( \text{wf}_N(\text{hs},l,s,g) \) wellformedness predicate definition, includes:

type
47a. PLAN = HI \rightarrow m^r LHIM
47b. LHIM = LI \rightarrow m^r HI-set
value
48c. no_junk: PLAN \rightarrow \text{Bool}
48c. no_junk(plan) \equiv \text{dom plan} = \cup \{ \text{rng(plan(hi))} | \text{hi:HI} \cdot \text{hi} \in \text{dom plan} \}
It expresses the distributed union of sets \( \text{rng}(\text{plan}(\text{li})) \) of hub identifiers (for each of the \( hi \) indexed maps from (definition set, \( \text{dom} \)) link identifiers to (range set, \( \text{rng} \)) hub identifiers, where \( hi:HI \) ranges over \( \text{dom.plan} \)).

A.2.3 Cartesian Expressions

Cartesian Enumerations

Let \( e \) range over values of Cartesian types involving \( A, B, \ldots, C \), then the below expressions are simple Cartesian enumerations:

**Cartesian Enumerations**

<table>
<thead>
<tr>
<th>type</th>
<th>( A, B, \ldots, C )</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>( (e_1, e_2, \ldots, e_n) )</td>
</tr>
</tbody>
</table>

Example 9

**Cartesian Net Types:**

So far we have abstracted hubs and links as sorts. That is, we have not defined their types concretely. Instead we have postulated some attributes such as: observable hub identifiers of hubs and sets of observable link identifiers of links connected to hubs. We now claim the following further attributes of hubs and links.

- Concrete links have
  - link identifiers,
  - link names – where two or more connected links may have the same link name,
  - two (unordered) hub identifiers,
  - lengths,
  - locations – where we do not presently defined what we main by locations,
  - etcetera

- Concrete hubs have
  - hub identifiers,
  - unique hub names,
  - a set of one or more observable link identifiers,
  - locations,
  - etcetera.
An RSL Primer

\( cL = LI \times LN \times (HI \times HI) \times LOC \times ... \)
\( cH = HI \times HN \times LI-set \times LOC \times ... \)

\[ \text{End of Example 9} \]

A.2.4 List Expressions

List Enumerations  Let \( a \) range over values of type \( A \), then the below expressions are simple list enumerations:

\[
\{ \langle \rangle, \langle e \rangle, ..., \langle e_1,e_2,...,en \rangle, ... \} \subseteq A^* \\
\{ \langle \rangle, \langle e \rangle, ..., \langle e_1,e_2,...,en \rangle, ..., \langle e_1,e_2,...,en,... \rangle, ..., \} \subseteq A^\omega \\
\langle a_{i,j} \ldots a_{i,j} \rangle
\]

The last line above assumes \( a_i \) and \( a_j \) to be integer-valued expressions. It then expresses the set of integers from the value of \( e_i \) to and including the value of \( e_j \). If the latter is smaller than the former, then the list is empty.

List Comprehension

The last line below expresses list comprehension.

List Comprehension

type
\[ A, B, P = A \rightarrow \text{Bool}, Q = A \sim \rightarrow B \]

value
\[ \text{comprehend: } A^\omega \times P \times Q \sim \rightarrow B^\omega \]
\[ \text{comprehend(l,P,Q)} \equiv \\
\{ Q(l(i)) \mid i \in (1..\text{len } l) \cdot P(l(i)) \} \]

Example 10  Routes in Nets:

- A phenomenological (i.e., a physical) route of a net is a sequence of one or more adjacent links of that net.
- A conceptual route is a sequence of one or more link identifiers.
- An abstract route is a conceptual route
– for which there is a phenomenological route of the net for which the link identifiers of the abstract route map one-to-one onto links of the phenomenological route.

type
N, H, L, HI, LI
PR′ = L∗
PR = { | pr:PR ′ • ∃ n:N • wf (pr)(n) }
CR = L ′
AR′ = L ′
AR = { | ar:AR ′ • ∃ n:N • wf (ar)(n) }

value
wf PR: PR ′ → N → Bool
wf PR (pr)(n) ≡
∀ i:Nat • { i,i+1 }⊆ inds pr ⇒
obshls(l(i)) ∩ obs_hls(l(i+1)) ≠ {}
wf AR ′: AR ′ → N → Bool
wf AR (ar)(n) ≡
∃ pr:PR • pr ∈ routes(n) ∧ wf PR (pr)(n) ∧ len pr=len ar ∧
∀ i:Nat • i ∈ inds ar ⇒ obs_L l(pr(i))=ar(i)

• A single link is a phenomenological route.
• If r and r′ are phenomenological routes
  – such that the last link r
  – and the first link of r′
  – share observable hub identifiers,
then the concatenation r ∪ r′ is a route.
This inductive definition implies a recursive set comprehension.
• A circular phenomenological route is a phenomenological route whose first and last links are distinct but share hub identifiers.
• A looped phenomenological route is a phenomenological route where two distinctly positions (i.e., indexed) links share hub identifiers.

value
routes: N → PR-infset
routes(n) ≡
let prs = { {(l)||L•obs_L s(n)} ∪
\[ \bigcup \{ pr \uparrow pr' \mid \text{pr,pr'} : \text{PR} \} \subseteq \text{prs} \land \text{obs}_R(\text{len pr}) \land \text{obs}_R(\text{pr'}(1)) \neq \{ \} \]

\[ \text{prs end} \]

\text{is\_circular: PR} \rightarrow \text{Bool} \\
\text{is\_circular(pr)} \equiv \text{obs}_R(\text{pr}(1)) \land \text{obs}_R(\text{pr}(\text{len pr})) \neq \{ \}

\text{is\_looped: PR} \rightarrow \text{Bool} \\
\text{is\_looped(pr)} \equiv \exists i,j: \text{Nat} \bullet i \neq j \land \{ i,j \} \subseteq \text{index pr} \\
\Rightarrow \text{obs}_R(\text{pr}(i)) \land \text{obs}_R(\text{pr}(j)) \neq \{ \}

- Straight routes are Phenomenological routes without loops.
- Phenomenological routes with no loops can be constructed from phenomenological routes by removing suffix routes whose first link give rise to looping.

value

\text{straight\_routes: N} \rightarrow \text{PR-set} \\
\text{straight\_routes(n)} \equiv \\
\text{let prs} = \text{routes(n)} \text{ in } \{ \text{straight\_route(pr)} \mid \text{pr}\cdot\text{ps} \in \text{prs} \} \text{ end}

\text{straight\_route: PR} \rightarrow \text{PR} \\
\text{straight\_route(pr)} \equiv \langle pr(i) \mid i: \text{Nat} \bullet i \in [1..\text{len pr}] \land pr(i) \notin \text{elems}(\langle pr(j) \mid j: \text{Nat} \bullet j \in [1..i] \rangle) \}

End of Example 10

A.2.5 Map Expressions

**Map Enumerations** Let (possibly indexed) \( u \) and \( v \) range over values of type \( T_1 \) and \( T_2 \), respectively, then the below expressions are simple map enumerations:

\text{type} \\
T_1, T_2 \\
M = T_1 \rightarrow[m] T_2

\text{value} \\
u,u_1,u_2,...,u_n:T_1, v,v_1,v_2,...,v_n:T_2 \\
\{ [ ], [ u \rightarrow v ], ..., [ u_1 \rightarrow v_1, u_2 \rightarrow v_2, ..., u_n \rightarrow v_n ], ... \} \subseteq M

**Map Comprehension** The last line below expresses map comprehension:
Map Comprehension

type
U, V, X, Y
M = U \rightarrow m V
F = U \Rightarrow X
G = V \Rightarrow Y
P = U \rightarrow \text{Bool}

value
comprehend: M \times F \times G \times P \rightarrow (X \rightarrow^m Y)
comprehend(m,F,G,P) \equiv
[ F(u) \mapsto G(m(u)) \mid u:U \cdot u \in \text{dom } m \land P(u) ]

Example 11 ..............................................Concrete Net Type Construction:

- We Define a function $\text{con}[\text{struct}]_N\gamma$ (of the Cartesians + Maps + Wellformedness part of Example 3).
  - The base of the construction is the fully abstract sort definition of $N_\alpha$ in the Sorts + Observers + Axioms part of Example 3 — where the sorts of hub and link identifiers are taken from earlier examples.
  - The target of the construction is the $N_\gamma$ of the Cartesians + Maps + Wellformedness part of Example 3.
  - First we recall the essential types of that $N_\gamma$.

\[
\text{type} \quad N_\gamma = \text{HUBS} \times \text{LINKS} \times \text{GRAPH}
\]
\[
\begin{align*}
\text{HUBS} &= \text{HI} \rightarrow^m H \\
\text{LINKS} &= \text{LI} \rightarrow^m L \\
\text{GRAPH} &= \text{HI} \rightarrow^m (\text{LI} \rightarrow^m \text{HI})
\end{align*}
\]

\[
\text{value} \quad \text{con}_N\gamma : N_\alpha \rightarrow N_\gamma
\]
\[
\begin{align*}
\text{con}_N\gamma(n_\alpha) \equiv
\text{let } \\
hubs &= [ \text{obs}_\text{HI}(h) \mapsto h \mid h: H \cdot h \in \text{obs}_\text{Hs}(n_\alpha) ], \\
\text{links} &= [ \text{obs}_\text{LI}(h) \mapsto l \mid l: L \cdot l \in \text{obs}_\text{Ls}(n_\alpha) ], \\
\text{graph} &= [ \text{obs}_\text{HI}(h) \mapsto [ \text{obs}_\text{LI}(l) \mapsto \iota(\text{obs}_\text{Hls}(l) \setminus \{\text{obs}_\text{HI}(h)\}) \\
\mid l: L \cdot l \in \text{obs}_\text{Ls}(n_\alpha) \land li \in \text{obs}_\text{Lls}(h) ] \\
\mid H: h \cdot h \in \text{obs}_\text{Hs}(n_\alpha) ] \in \\
(\text{hubs}, \text{links}, \text{graph}) \end{align*}
\]

$\iota$: A-set $\sim A$ [A could be LI-set]
$\iota(as) \equiv$ if card as = 1 then let \{a\} = as in a else chaos end end
theorem: 
\[ n_\alpha \text{ satisfies axioms 2.–3., 5.–6., and 8. (Page 13) } \Rightarrow \text{wf}_\gamma (\text{con}_\gamma (n_\alpha)) \]

End of Example 11

A.2.6 Set Operations

Set Operator Signatures

Set Operations

value
1. \( \in \): \( A \times \text{A-infset} \rightarrow \text{Bool} \)
2. \( \notin \): \( A \times \text{A-infset} \rightarrow \text{Bool} \)
3. \( \cup \): \( \text{A-infset} \times \text{A-infset} \rightarrow \text{A-infset} \)
4. \( \cup \): \( (\text{A-infset})\text{-infset} \rightarrow \text{A-infset} \)
5. \( \cap \): \( \text{A-infset} \times \text{A-infset} \rightarrow \text{A-infset} \)
6. \( \cap \): \( (\text{A-infset})\text{-infset} \rightarrow \text{A-infset} \)
7. \( \setminus \): \( \text{A-infset} \times \text{A-infset} \rightarrow \text{A-infset} \)
8. \( \subseteq \): \( \text{A-infset} \times \text{A-infset} \rightarrow \text{Bool} \)
9. \( \subset \): \( \text{A-infset} \times \text{A-infset} \rightarrow \text{Bool} \)
10. \( =: \): \( \text{A-infset} \times \text{A-infset} \rightarrow \text{ Bool} \)
11. \( \neq : \): \( \text{A-infset} \times \text{A-infset} \rightarrow \text{Bool} \)
12. \( \text{card} : \text{A-infset} \rightarrow \text{Nat} \)

Set Examples

Set Examples

eamples
1. \( a \in \{a,b,c\} \)
2. \( a \notin \{\}, a \notin \{b,c\} \)
3. \( \{a,b,c\} \cup \{a,b,d,e\} = \{a,b,c,d,e\} \)
4. \( \cup \{a\}, \{a,b\}, \{a,d\} = \{a,b,d\} \)
5. \( \{a,b,c\} \cap \{c,d,e\} = \{c\} \)
6. \( \cap \{a\}, \{a,b\}, \{a,d\} = \{a\} \)
7. \( \{a,b,c\} \setminus \{c,d\} = \{a,b\} \)
8. \( \{a,b\} \subseteq \{a,b,c\} \)
9. \( \{a,b,c\} \subseteq \{a,b,c\} \)
10. \( \{a,b,c\} = \{a,b,c\} \)
11. \( \{a,b,c\} \neq \{a,b\} \)
12. \( \text{card} \{\} = 0, \text{card} \{a,b,c\} = 3 \)
Informal Explication

21. \( \in \): The membership operator expresses that an element is a member of a set.

22. \( \notin \): The non-membership operator expresses that an element is not a member of a set.

23. \( \cup \): The infix union operator. When applied to two sets, the operator gives the set whose members are in either or both of the two operand sets.

24. \( \cup \): The distributed prefix union operator. When applied to a set of sets, the operator gives the set whose members are in some of the operand sets.

25. \( \cap \): The infix intersection operator. When applied to two sets, the operator gives the set whose members are in both of the two operand sets.

26. \( \cap \): The prefix distributed intersection operator. When applied to a set of sets, the operator gives the set whose members are in some of the operand sets.

27. \( \setminus \): The set complement (or set subtraction) operator. When applied to two sets, the operator gives the set whose members are those of the left operand set which are not in the right operand set.

28. \( \subseteq \): The proper subset operator expresses that all members of the left operand set are also in the right operand set.

29. \( \subset \): The proper subset operator expresses that all members of the left operand set are also in the right operand set, and that the two sets are not identical.

30. \( = \): The equal operator expresses that the two operand sets are identical.

31. \( \neq \): The non-equal operator expresses that the two operand sets are not identical.

32. \texttt{card}: The cardinality operator gives the number of elements in a finite set.

Set Operator Definitions

The operations can be defined as follows (\( \equiv \) is the definition symbol):

Set Operation Definitions

\[
\begin{align*}
\text{value} \\
\text{s'} \cup \text{s''} & \equiv \{a \mid a \in \text{A} \land a \in s' \lor a \in s''\} \\
\text{s'} \cap \text{s''} & \equiv \{a \mid a \in \text{A} \land a \in s' \land a \in s''\} \\
\text{s'} \setminus \text{s''} & \equiv \{a \mid a \in \text{A} \land a \in s' \land a \notin s''\} \\
\text{s'} \subseteq \text{s''} & \equiv \forall \ a \in s' \Rightarrow a \in s'' \\
\text{s'} \subset \text{s''} & \equiv \exists \ a \in s' \land a \notin s''
\end{align*}
\]
s' = s''' ≡ ∀ a:A • a ∈ s' ≡ a ∈ s'' ≡ s' ⊆ s''' ∧ s'' ⊆ s
s' ≠ s'' ≡ s' ∩ s'' ≠ \{\}

\text{card} \ s ≡ 
\text{if} \ s = \{\} \ \text{then} \ 0 \ \text{else} 
\text{let} \ a:A • a \ ∈ \ s \ \text{in} \ 1 + \card (s \ \setminus \ \{a\}) \ \text{end} \ \text{end}

\text{pre} \ s /\ast \ \text{is a finite set} /\ast
\text{card} \ s \equiv \text{chaos} /\ast \ \text{tests for infinity of} \ s /\ast

A.2.7 \ Cartesian \ Operations

\textbf{Cartesian \ Operations}

\textbf{Cartesian \ Operations}

\textbf{Cartesian \ Operations}

\begin{align*}
type & A, B, C \\
g0: G0 = A \times B \times C \\
g1: G1 = (A \times B \times C) \\
g2: G2 = (A \times B) \times C \\
g3: G3 = A \times (B \times C)
\end{align*}

\begin{align*}
\text{value} & \\
va:A, \ vb:B, \ vc:C, \ vd:D
\end{align*}

\begin{align*}
\text{decomposition \ expressions} & \\
\text{let} \ (a1,b1,c1) = g0, \ (va,vb,vc):G0, \\
\text{let} \ ((a1',b1',c1')) = g1, \ ((va, vb), vc):G1 \\
\text{let} \ (((a2,b2),c2)) = g2, \ (va3, vb3, vc3):G2 \\
\text{let} \ ((a3, b3, c3)) = g3, \ (va3, vb3, vc3):G3
\end{align*}

A.2.8 \ List \ Operations

\textbf{List \ Operator \ Signatures}

\textbf{List \ Operator \ Signatures}

\textbf{List \ Operator \ Signatures}

\textbf{List \ Operators}

\begin{align*}
\text{value} & \\
\text{hd:} \ A^\omega \rightarrow A \\
\text{tl:} \ A^\omega \rightarrow A^\omega \\
\text{len:} \ A^\omega \rightarrow \text{Nat} \\
\text{inds:} \ A^\omega \rightarrow \text{Nat-infset} \\
\text{elems:} \ A^\omega \rightarrow \text{A-infset} \\
\text{(.):} \ A^\omega \times \text{Nat} \rightarrow A \\
\wedge: \ A^* \times A^\omega \rightarrow A^\omega \\
\equiv: \ A^\omega \times A^\omega \rightarrow \text{Bool} \\
\neq: \ A^\omega \times A^\omega \rightarrow \text{Bool}
\end{align*}

\textbf{List \ Operation \ Examples}

\textbf{List \ Operation \ Examples}

\textbf{List \ Operation \ Examples}
List Examples

examples
\[ \text{hd}(a_1, a_2, ..., a_m) = a_1 \]
\[ \text{tl}(a_1, a_2, ..., a_m) = (a_2, ..., a_m) \]
\[ \text{len}(a_1, a_2, ..., a_m) = m \]
\[ \text{inds}(a_1, a_2, ..., a_m) = \{1, 2, ..., m\} \]
\[ \text{elems}(a_1, a_2, ..., a_m) = \{a_1, a_2, ..., a_m\} \]
\[ (a_1, a_2, ..., a_m)(i) = a_i \]
\[ (a, b, c) \hat{\cdot} (a, b, d) = (a, b, c, a, b, d) \]
\[ (a, b, c) = (a, b, c) \]
\[ (a, b, c) \neq (a, b, d) \]

Informal Explication

- \textbf{hd}: Head gives the first element in a nonempty list.
- \textbf{tl}: Tail gives the remaining list of a nonempty list when Head is removed.
- \textbf{len}: Length gives the number of elements in a finite list.
- \textbf{inds}: Indices give the set of indices from 1 to the length of a nonempty list. For empty lists, this set is the empty set as well.
- \textbf{elems}: Elements gives the possibly infinite set of all distinct elements in a list.
- \( \ell(i) \): Indexing with a natural number, \( i \) larger than 0, into a list \( \ell \) having a number of elements larger than or equal to \( i \), gives the \( i \)th element of the list.
- \( \hat{\cdot} \): Concatenates two operand lists into one. The elements of the left operand list are followed by the elements of the right. The order with respect to each list is maintained.
- \( = \): The equal operator expresses that the two operand lists are identical.
- \( \neq \): The non-equal operator expresses that the two operand lists are not identical.

The operations can also be defined as follows:

**List Operator “Definitions”**

value
\[ \text{is\_finite\_list}: A^\omega \to \text{Bool} \]
\[ \text{len } q \equiv \begin{cases} \text{case is\_finite\_list}(q) \text{ of} \end{cases} \]
true → if q = ⟨⟩ then 0 else 1 + len tl q end,
false → chaos end

inds q ≡
case is_finite_list(q) of
true → { i | i:Nat ∙ 1 ≤ i ≤ len q },
false → { i | i:Nat ∙ i≠0 } end

elems q ≡ { q(i) | i:Nat ∙ i ∈ inds q }

q(i) ≡
case (q,i) of
(⟨⟩,1) → chaos,
(⟨⟩,1) → let a:A,q′:Q ∙ q=(a)ˆq′ in a end
→ q(i-1)
end

fq ↑ iq ≡
⟨ if 1 ≤ i ≤ len fq then fq(i) else iq(i - len fq) end 
| i:Nat ∙ if len iq≠chaos then i ≤ len fq+len end ⟩
pre is_finite_list(fq)

iq′ = iq” ≡
inds iq’ = inds iq” ∧ ∀ i:Nat ∙ i ∈ inds iq’ ⇒ iq′(i) = iq”(i)

iq’ ≠ iq” ≡ ¬(iq’ = iq”)

A.2.9 Map Operations

Map Operator Signatures and Map Operation Examples

value
m(a): M → A ~ B, m(a) = b

dom: M → A-infset [domain of map]
dom [a1→b1,a2→b2,...,an→bn] = {a1,a2,...,an}

rng: M → B-infset [range of map]
rng [a1→b1,a2→b2,...,an→bn] = {b1,b2,...,bn}

†: M × M → M [override extension]
[ a→b,a′→b′,a″→b″ ] † [ a′′→b″,a′′′→b′′′ ] = [ a→b,a′→b′,a″→b″ ]
\[ \cup : M \times M \to M \] [merge \( \cup \)]
\[ [a \mapsto b, a' \mapsto b', a'' \mapsto b''] \cup [a''' \mapsto b'''] = [a \mapsto b, a' \mapsto b', a'' \mapsto b'', a''' \mapsto b'''] \]

\[ \setminus : M \times A \text{-infset} \to M \] [restriction by]
\[ [a \mapsto b, a' \mapsto b', a'' \mapsto b''] \setminus \{a\} = [a' \mapsto b', a'' \mapsto b'''] \]

\[ \div : M \times A \text{-infset} \to M \] [restriction to]
\[ [a \mapsto b, a' \mapsto b', a'' \mapsto b''] \div \{a', a''\} = [a' \mapsto b', a'' \mapsto b'''] \]

\[ =, \neq : M \times M \to \text{Bool} \]
\[ \circ : (A \mapsto B) \times (B \mapsto C) \to (A \mapsto C) \] [composition]
\[ [a \mapsto b, a' \mapsto b'] \circ [b \mapsto c, b' \mapsto c'] = [a \mapsto c, a' \mapsto c'] \]

**Map Operation Explication**

- **\( m(a) \):** Application gives the element that \( a \) maps to in the map \( m \).
- **\( \text{dom} \):** Domain/Definition Set gives the set of values which \( maps to \) in a map.
- **\( \text{rng} \):** Range/Image Set gives the set of values which \( are mapped to \) in a map.
- **\( \uparrow \):** Override/Extend. When applied to two operand maps, it gives the map which is like an override of the left operand map by all or some “pairings” of the right operand map.
- **\( \cup \):** Merge. When applied to two operand maps, it gives a merge of these maps.
- **\( \setminus \):** Restriction. When applied to two operand maps, it gives the map which is a restriction of the left operand map to the elements that are not in the right operand set.
- **\( \div \):** Restriction. When applied to two operand maps, it gives the map which is a restriction of the left operand map to the elements of the right operand set.
- **\( =, \neq \):** The equal operator expresses that the two operand maps are identical.
- **\( \neq \):** The non-equal operator expresses that the two operand maps are *not* identical.
- **\( \circ \):** Composition. When applied to two operand maps, it gives the map from definition set elements of the left operand map, \( m_1 \), to the range elements of the right operand map, \( m_2 \), such that if \( a \) is in the definition set of \( m_1 \) and maps into \( b \), and if \( b \) is in the definition set of \( m_2 \) and maps into \( c \), then \( a \), in the composition, maps into \( c \).
Example 12  

**Miscellaneous Net Expressions: Maps:**

Example 3 on page 91 left out defining the well-formedness of the map types:

**type**

\[
\begin{align*}
\text{GRAPH} &= \text{HI} \xrightarrow{m^r} (\text{LI} \xrightarrow{m^r} \text{HI-set}) \\
\text{HUBS} &= \text{HI} \xrightarrow{m^r} \text{H} \\
\text{LINKS} &= \text{LI} \xrightarrow{m^r} \text{L} \\
N_\gamma &= \text{HUBS} \times \text{LINKS} \times \text{GRAPH}
\end{align*}
\]

**value**

\[
\begin{align*}
\text{wf}_{\text{HUBS}} : \text{H-set} &\rightarrow \text{Bool} \\
\text{wf}_{\text{HUBS}}(\text{hubs}) &\equiv \forall \text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{hubs} \Rightarrow \text{obs}_{\text{HI}}(\text{hubs}(\text{hi})) = \text{hi} \\
\text{wf}_{\text{LINKS}} : \text{L-set} &\rightarrow \text{Bool} \\
\text{wf}_{\text{LINKS}}(\text{links}) &\equiv \forall \text{li} : \text{LI} \cdot \text{li} \in \text{dom}\ \text{links} \Rightarrow \text{obs}_{\text{LI}}(\text{links}(\text{li})) = \text{li} \\
\text{wf}_{N_\gamma} : N_\gamma &\rightarrow \text{Bool} \\
\text{wf}_{N_\gamma}(\text{hs}, \text{ls}, \text{g}) &\equiv \\
\text{dom}\ \text{hs} &= \text{dom}\ \text{g} \land \\
\bigcup \{\text{dom}\ \text{g}(\text{hi})|\text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{g}\} &= \text{dom}\ \text{links} \land \\
\bigcup \{\text{rng}\ \text{g}(\text{hi})|\text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{g}\} &= \text{dom}\ \text{g} \land \\
\forall \text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{g} \Rightarrow \forall \text{li} : \text{LI} \cdot \text{li} \in \text{dom}\ \text{g}(\text{hi}) \Rightarrow (\text{g}(\text{hi}))(\text{li}) \neq \text{hi} \\
\forall \text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{g} \Rightarrow \exists ! \text{li} : \text{LI} \cdot \text{li} \in \text{dom}\ \text{g}(\text{hi}) \Rightarrow (\text{g}(\text{hi}))(\text{li}) = \text{hi}' \land (\text{g}(\text{hi}'))(\text{li}) = \text{hi}.
\end{align*}
\]

- *Hubs* record the same hubs as do the net corresponding *GRAPH* \((\text{dom}\ \text{hs} = \text{dom}\ \text{g} \land)\).

- *GRAPH* record the same links as do the net corresponding *LINKS* \((\bigcup \{\text{dom}\ \text{g}(\text{hi})|\text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{g}\} = \text{dom}\ \text{links})\).

- The target (or range) hub identifiers of graphs are the same as the domain of the graph \((\bigcup \{\text{rng}\ \text{g}(\text{hi})|\text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{g}\} = \text{dom}\ \text{g})\), that is none missing, no new ones!

- No links emanate from and are incident upon the same hub \((\forall \text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{g} \Rightarrow \forall \text{li} : \text{LI} \cdot \text{li} \in \text{dom}\ \text{g}(\text{hi}) \Rightarrow (\text{g}(\text{hi}))(\text{li}) \neq \text{hi}')\).

- If there is a link from one hub to another in the *GRAPH*, then the same link also connects the other hub to the former \((\forall \text{hi} : \text{HI} \cdot \text{hi} \in \text{dom}\ \text{g} \Rightarrow \forall \text{li} : \text{LI} \cdot \text{li} \in \text{dom}\ \text{g}(\text{hi}) \Rightarrow \exists \text{hi}' : \text{HI} \cdot \text{hi}' \in \text{dom}\ \text{g} \Rightarrow \exists ! \text{li} : \text{LI} \cdot \text{li} \in \text{dom}\ \text{g}(\text{hi}) \Rightarrow (\text{g}(\text{hi}))(\text{li}) = \text{hi}' \land (\text{g}(\text{hi}'))(\text{li}) = \text{hi})\).

End of Example 12

**Map Operation “Redeﬁnitions”**

The map operations can also be deﬁned as follows:
value

\[ \text{rng } m \equiv \{ m(a) \mid a:A \land a \in \text{dom } m \} \]

\[ m \uparrow m_2 \equiv \big( a \mapsto b \mid a:A, b:B \land a \in \text{dom } m_1 \setminus \text{dom } m_2 \lor a \in \text{dom } m_2 \land b = m_2(a) \big) \]

\[ m_1 \cup m_2 \equiv \big( a \mapsto b \mid a:A, b:B \land a \in \text{dom } m_1 \land b = m_1(a) \lor a \in \text{dom } m_2 \land b = m_2(a) \big) \]

\[ m \setminus s \equiv \big( a \mapsto m(a) \mid a:A \land a \in \text{dom } m \setminus s \big) \]

\[ m / s \equiv \big( a \mapsto m(a) \mid a:A \land a \in \text{dom } m \cap s \big) \]

\[ m_1 = m_2 \equiv \text{dom } m_1 = \text{dom } m_2 \land \forall a:A \cdot a \in \text{dom } m_1 \Rightarrow m_1(a) = m_2(a) \]

\[ m_1 \neq m_2 \equiv \neg (m_1 = m_2) \]

\[ m \circ n \equiv \big( a \mapsto c \mid a:A, c:C \land a \in \text{dom } m \land c = n(m(a)) \big) \]

\[ \text{pre } \text{rng } m \subseteq \text{dom } n \]

A.3 The RSL Predicate Calculus

A.3.1 Propositional Expressions

Let identifiers (or propositional expressions) \( a, b, ..., c \) designate Boolean values (true or false [or chaos]). Then:

**Propositional Expressions**

false, true

\( a, b, ..., c \sim a, a \land b, a \lor b, a \Rightarrow b, a=b, a \neq b \)

are propositional expressions having Boolean values. \( \sim, \land, \lor, \Rightarrow, = \) and \( \neq \) are Boolean connectives (i.e., operators). They can be read as: not, and, or, if then (or implies), equal and not equal.

A.3.2 Simple Predicate Expressions

Let identifiers (or propositional expressions) \( a, b, ..., c \) designate Boolean values, let \( x, y, ..., z \) (or term expressions) designate non-Boolean values and let \( i, j, ..., k \) designate number values, then:
Simple Predicate Expressions

false, true
a, b, ..., c
∼a, a∧b, a∨b, a⇒b, a=b, a≠b
x=y, x≠y,
i<j, i≤j, i≥j, i≠j, i≥j, i>j

are simple predicate expressions.

A.3.3 Quantified Expressions

Let X, Y, . . . , C be type names or type expressions, and let P(x), Q(y) and R(z) designate predicate expressions in which x, y and z are free. Then:

Quantified Expressions

∀ x:X • P(x)
∃ y:Y • Q(y)
∃ ! z:Z • R(z)

are quantified expressions — also being predicate expressions.

They are “read” as: For all x (values in type X) the predicate P(x) holds; there exists (at least) one y (value in type Y) such that the predicate Q(y) holds; and there exists a unique z (value in type Z) such that the predicate R(z) holds.

Example 13 Pecadates Over Net Quantities:

From earlier examples we show some predicates:

• Example 1: Right hand side of function definition is_two_way_link(l):
  \exists lσ:LΣ • lσ ∈ obs_HΣ(l)∧\text{card } lσ=2

• Example 3:

  - The Sorts + Observers + Axioms part:
    * Right hand side of the wellformedness function \text{wf}_N(n) definition:
      \forall n:N • \text{card } obs_Hs(n)≥2 ∧ \text{card } obs_Ls(n)≥1 ∧ \text{axioms 2.–3.}, 5.–6., and 8., (Page 13)
    * Right hand side of the wellformedness function \text{wf}_N(hs,ls) definition:
      \text{card } hs≥2 ∧ \text{card } ls≥1 ...

  - The Cartesians + Maps + Wellformedness part:
    * Right hand side of the \text{wf}_HUBS wellformedness function definition:
      \forall hi:HI • hi ∈ \text{dom } hubs ⇒ obs_HHubs(hi)=hi
* Right hand side of the \( \text{wf}_L \text{INKS} \) wellformedness function definition:
\[
\forall \ li:LI \cdot li \in \text{dom} \text{ links} \Rightarrow \text{obs}_L\text{links}(li) = li
\]

* Right hand side of the \( \text{wf}_N(hs,ls,g) \) wellformedness function definition:
\[
\begin{align*}
[c] \text{ dom } hs &= \text{ dom } g \\[d] \cup \{ \text{ dom } g(hi) \mid hi:HL \cdot hi \in \text{ dom } g \} &= \text{ dom } \text{ links} \land \\
[e] \cup \{ \text{ rng } g(hi) \mid hi:HL \cdot hi \in \text{ dom } g \} &= \text{ dom } g \land \\
[f] \forall hi:HL \cdot hi \in \text{ dom } g \Rightarrow \forall li:LI \cdot li \in \text{ dom } g(hi) \Rightarrow (g(hi))(li) \neq hi \\
g] \forall hi:HL \cdot hi \in \text{ dom } g \Rightarrow \forall li:LI \cdot li \in \text{ dom } g(hi) \Rightarrow \\
\exists h':HL \cdot h' \in \text{ dom } g \Rightarrow \exists ! li:LI \cdot li \in \text{ dom } g(hi) \Rightarrow \\
(g(hi))(li) = h' \land (g(h'))(li) = hi
\end{align*}
\]

---

A.4 \( \lambda \)-Calculus + Functions

A.4.1 The \( \lambda \)-Calculus Syntax

\( \lambda \)-Calculus Syntax

**type** /* A BNF Syntax: */
\[
\begin{align*}
(L) &::= (V) \mid (F) \mid (A) \mid (\ (A) \ ) \\
(V) &::= \text{ / } * \text{ variables, i.e. identifiers } * / \\
(F) &::= \lambda (V) \cdot (L) \\
(A) &::= ( \ (L) (L) \ )
\end{align*}
\]

**value** /* Examples */
\[
\begin{align*}
(L) &::= e, f, a, ... \\
(V) &::= x, ... \\
(F) &::= \lambda x \cdot e, ... \\
(A) &::= f a, (f a), f(a), (f)(a), ...
\end{align*}
\]

A.4.2 Free and Bound Variables

**Free and Bound Variables** Let \( x, y \) be variable names and \( e, f \) be \( \lambda \)-expressions.

- (V): Variable \( x \) is free in \( x \).

- (F): \( x \) is free in \( \lambda y \cdot e \) if \( x \neq y \) and \( x \) is free in \( e \).

- (A): \( x \) is free in \( f(e) \) if it is free in either \( f \) or \( e \) (i.e., also in both).
A.4.3 Substitution

In RSL, the following rules for substitution apply:

Substitution of an expression $N$ for all free $x$ in $M$ is expressed: $\text{subst}([N/x]M)$.

Substitution

- $\text{subst}([N/x]x) \equiv N$;
- $\text{subst}([N/x]a) \equiv a$,
  for all variables $a \neq x$;
- $\text{subst}([N/x](P \ Q)) \equiv (\text{subst}([N/x]P) \ \text{subst}([N/x]Q))$;
- $\text{subst}([N/x](\lambda x \ P)) \equiv \lambda y \ P$;
- $\text{subst}([N/x](\lambda y \ P)) \equiv \lambda y \ \text{subst}([N/x]P)$,
  if $x \neq y$ and $y$ is not free in $N$ or $x$ is not free in $P$;
- $\text{subst}([N/x](\lambda y \ P)) \equiv \lambda z \ \text{subst}([N/z]\text{subst}([z/y]P))$,
  if $y \neq x$ and $y$ is free in $N$ and $x$ is free in $P$
  (where $z$ is not free in $(N \ P)$).

A.4.4 $\alpha$-Renaming and $\beta$-Reduction

$\alpha$ and $\beta$ Conversions

- $\alpha$-renaming: $\lambda x \ M$
  If $x$, $y$ are distinct variables then replacing $x$ by $y$ in $\lambda x \ M$ results in $\lambda y \ \text{subst}([y/x]M)$.
  We can rename the formal parameter of a $\lambda$-function expression provided that no free variables of its body $M$ thereby become bound.

- $\beta$-reduction: $(\lambda x \ M)(N)$
  All free occurrences of $x$ in $M$ are replaced by the expression $N$ provided that no free variables of $N$ thereby become bound in the result. $(\lambda x \ M)(N) \equiv \text{subst}([N/x]M)$

Example 14 ................................................................. Network Traffic:

We model traffic by introducing a number of model concepts. We simplify, without losing the essence of this example, namely to show the use of $\lambda$–functions, by omitting consideration of dynamically changing nets. These are introduced next:

- Let us assume a net, $n:N$. 

November 1, 2010, 15:25, Budapest Lectures, Oct. 11–22, 2010
There is a dense set, $T$, of times – for which we omit giving an appropriate definition.

There is a sort, $V$, of vehicles.

$TS$ is a dense subset of $T$.

For each $ts:TS$ we can define a minimum and a maximum time.

The $MIN$ and $MAX$ functions are meta-linguistic, that is, are not defined in our formal specification language RSL, but can be given a satisfactory meaning.

At any moment some vehicles, $v:V$, have a $pos:Position$ on the net and $VP$ records those.

A $Position$ is either on a link or at a hub.

An $onLink$ position can be designated by the link identifier, the identifiers of the from and to hubs, and the fraction, $f:F$, of the distance down the link from the from hub to the to hub.

An $atHub$ position just designates the hub (by its identifier).

Traffic, $tf:TF$, is now a continuous function from $Time$ to $NP$ ("recordings").

Modelling traffic in this way, in fact, in whichever way, entails a ("serious") number of well-formedness conditions. These are defined in $wf_{TF}$ (omitted: ...).

\begin{verbatim}
value
n:N
type
T, V
TS = T-infset

axiom
\forall ts:TS \cdot \exists tmin,tmax:T: tmin \in ts \land tmax \in ts \land \forall t:T: t \in ts \Rightarrow tmin \leq t \leq tmax
[that is: ts = \{MIN(ts) .. MAX(ts)\}]

type
VP = V \infset Pos
TF' = T \to VP,
TF = \{ |tf:TF \cdot wf_{TF}(tf(n)) | \}
Pos = onL | atH
onL == mkLPos(hi:HI,li:LI,f:F,hi:HI), atH == mkHPos(hi:HI)

value
wf_{TF}: TF \to N \to Bool
wf_{TF}(tf)(n) \equiv ...

DOMIN: TF \to TS
MIN, MAX: TS \to T
\end{verbatim}
We have defined the continuous, composite entity of traffic. Now let us define an operation of inserting a vehicle in a traffic.

- To insert a vehicle, $v$, in a traffic, $tf$, is prescribable as follows:
  - the vehicle, $v$, must be designated;
  - a time point, $t$, "inside" the traffic $tf$ must be stated;
  - a traffic, $vtf$, from time $t$ of vehicle $v$ must be stated;
  - as well as traffic, $tf$, into which $vtf$ is to be "merged".

- The resulting traffic is referred to as $tf'$.

\[
\text{value} \quad \text{insert}_V : V \times T \times TF \rightarrow TF \rightarrow TF
\]
\[
\text{insert}_V(v,t,vtf)(tf) \rightarrow tf'
\]

- The function $\text{insert}_V$ is here defined in terms of a pair of pre/post conditions.

- The pre-condition can be prescribed as follows:
  - The insertion time $t$ must be within to open interval of time points in the traffic $tf$ to which insertion applies.
  - The vehicle $v$ must not be among the vehicle positions of $tf$.
  - The vehicle must be the only vehicle "contained" in the "inserted" traffic $vtf$.

\[
\text{pre: MIN}(\text{DOMAIN}(tf)) \leq t \leq \text{MAX}(\text{DOMAIN}(tf)) \land
\forall t':T \cdot t' \in \text{DOMAIN}(tf) \Rightarrow v \not\in \text{dom}(tf(t')) \land
\text{MIN}(\text{DOMAIN}(vtf)) = t \land
\forall t':T \cdot t' \in \text{DOMAIN}(vtf) \Rightarrow \text{dom}(vtf(t')) = \{v\}
\]

- The post condition "defines" $tf'$, the traffic resulting from merging $vtf$ with $tf$:
  - Let $ts$ be the time points of $tf$ and $vtf$, a time interval.
  - The result traffic, $tf'$, is defines as a $\lambda$-function.
  - For any $t''$ in the time interval
    - if $t''$ is less than $t$, the insertion time, then $tf'$ is as $tf$;
    - if $t''$ is $t$ or larger then $tf'$ applied to $t''$, i.e., $tf'(t'')$
      \* for any $v' : V$ different from $v$ yields the same as $(tf(t))(v')$,
      \* but for $v$ it yields $(vtf(t))(v)$.
post: $t'_f = \lambda t''$.

let $t_s = \text{DOMAIN}(t_f) \cup \text{DOMAIN}(v_{tf})$ in

if $\text{MIN}(t_s) \leq t'' \leq \text{MAX}(t_s)$

then

$((t'' < t) \rightarrow t_f(t''),$

$(t'' \geq t) \rightarrow [v' \mapsto \text{if } v' \neq v \text{ then } (t_f(t))(v') \text{ else } (v_{tf}(t))(v) \text{ end}$

$|v':V \cdot v' \in \text{vehicles}(t_f))$

else chaos end

end

assumption: $\text{wf}_{TF}(v_{tf}) \land \text{wf}_{TF}(t_f)$

theorem: $\text{wf}_{TF}(t'_f)$

value

vehicles: $TF \rightarrow V\text{-set}$

vehicles($t_f$) $\equiv \{v|t:T,v:V \cdot t \in \text{DOMAIN}(t_f) \land v \in \text{dom} \ t_f(t)\}$

We leave it as an exercise for the reader to define functions for: removing a vehicle from a traffic, changing to course of a vehicle from an originally (or changed) vehicle traffic to another. etcetera.

End of Example 14

A.4.5 Function Signatures

For sorts we may want to postulate some functions:

Sorts and Function Signatures

type

$A, B, ..., C$

value

$\text{obs}_B: A \rightarrow B$

$\text{obs}_C: A \rightarrow C$

These functions cannot be defined. Once a domain is presented in which sort $A$ and sorts or types $B, ..., C$ occurs these observer functions can be demonstrated.

Example 15 Hub and Link Observers:

Let a net with several hubs and links be presented. Now observer functions $\text{obs}_H$ and $\text{obs}_L$s can be demonstrated: one simply “walks” along the net, pointing out this hub and that link, one-by-one until all the net has been visited.

The observer functions $\text{obs}_H$ and $\text{obs}_L$ can be likewise demonstrated, for example: when a hub is “visited” its unique identification can be postulated (and “calculated") to be the unique
geographic position of the hub one which is not overlapped by any other hub (or link), and likewise for links.

End of Example 15

A.4.6 Function Definitions

Functions can be defined explicitly:

type
A, B

g: A \rightarrow B \ [a \text{ partial function}]
g(a_{\text{expr}}) \equiv b_{\text{expr}}

value
f: A \rightarrow B \ [a \text{ total function}]
f(a_{\text{expr}}) \equiv b_{\text{expr}}

pre P(a_{\text{expr}})
P: A \rightarrow \text{Bool}

a_{\text{expr}}, b_{\text{expr}} \text{ are } A, \text{ respectively } B \text{ valued expressions of any of the kinds illustrated in earlier and later sections of this primer.}

Or functions can be defined implicitly:

type
A, B, \ldots, C, D

g: A \simrightarrow B \ [a \text{ partial function}]
g(a_{\text{expr}}) \equiv b_{\text{expr}}

value
f: A \rightarrow B
f(a_{\text{expr}}) \equiv b_{\text{expr}}
g(a_{\text{expr}}) \equiv b_{\text{expr}}

\text{pre } P(a_{\text{expr}}, b)
P: A \times B \rightarrow \text{Bool}

\text{post } P(a_{\text{expr}}, b)
P': A \rightarrow \text{Bool}

where \( b \) is just an identifier.

The symbol \( \simrightarrow \) indicates that the function is partial and thus not defined for all arguments. Partial functions should be assisted by preconditions stating the criteria for arguments to be meaningful to the function.

Finally, functions, \( f, g, \ldots, h \), can be defined in terms of axioms over function identifiers, \( f, g, \ldots, h \), and over identifiers of function arguments and results.

type
A, B, \ldots, C, D

g: A \simrightarrow B

value
f: A \rightarrow B, g: B \rightarrow C, \ldots, h: C \rightarrow D
f(a_{\text{expr}}) \equiv b_{\text{expr}}
g(a_{\text{expr}}) \equiv b_{\text{expr}}

\text{pre } P(a_{\text{expr}})
P: A \rightarrow \text{Bool}

\text{post } P(a_{\text{expr}}, b)

\text{pre } P'(a_{\text{expr}})
P': A \rightarrow \text{Bool}

axiom
\forall a: A, b: B, \ldots, c: C, d: D
\quad P_1(f, g, \ldots , h, a, b, \ldots , c, d) \land \ldots \land P_n(f, g, \ldots , h, a, b, \ldots , c, d)

where \( P_1, \ldots, P_m \) and \( Q_1, \ldots, Q_n \) designate suitable predicate expressions.
Example 16 .................................................. Axioms over Hubs, Links and Their Observers:

The axioms displayed in Items 2–3 and 5–8 on Page 13 of Sect. 2.1 demonstrates how a number of entities and observer functions are constrained (that is, partially defined) by function signatures.

..........................................................End of Example 16

A.5 Other Applicative Expressions

A.5.1 Simple let Expressions

Simple (i.e., nonrecursive) let expressions:

Let Expressions

let a = E \_d in \_b(a) end

is an “expanded” form of:

\((\lambda a.\_b(a))(\_d)\)

A.5.2 Recursive let Expressions

Recursive let expressions are written as:

Recursive let Expressions

let f = \lambda a.\_E(f,a) in \_B(f,a) end

let f = (\lambda g.\lambda a.\_E(g,a))(f) in \_B(f,a) end

let f = F(f) in \_E(f,a) end where \_F = \lambda g.\lambda a.\_E(g,a)

let f = Y\_F in \_B(f,a) end where Y\_F = F(Y\_F)

We read \_f = Y\_F as “\_f is a fix point of \_F”.

A.5.3 Non-deterministic let Clause

The non-deterministic let clause:

let a:A \_P(a) in \_B(a) end

expresses the non-deterministic selection of a value a of type A which satisfies a predicate \_P(a) for evaluation in the body \_B(a). If no a:A \_P(a) the clause evaluates to chaos.
A.5.4 Pattern and "Wild Card" let Expressions

Patterns and wild cards can be used:

Patterns

\[
\text{let } \{a\} \cup s = \text{set in ... end}
\]

\[
\text{let } \{a, \_\} \cup s = \text{set in ... end}
\]

\[
\text{let } (a, b, \ldots, c) = \text{cart in ... end}
\]

\[
\text{let } (a, \_\ldots, c) = \text{cart in ... end}
\]

\[
\text{let } (a)^\ell = \text{list in ... end}
\]

\[
\text{let } (a, b)^\ell = \text{list in ... end}
\]

\[
\text{let } [a \mapsto b] \cup m = \text{map in ... end}
\]

\[
\text{let } [a \mapsto \_] \cup m = \text{map in ... end}
\]

A.5.5 Conditionals

Various kinds of conditional expressions are offered by RSL:

Conditionals

\[
\text{if } b_{\text{expr}} \text{ then } c_{\text{expr}} \text{ else } a_{\text{expr}} \text{ end}
\]

\[
\text{if } b_{\text{expr}} \text{ then } c_{\text{expr}} \text{ end } \equiv \text{ /* same as: */}
\]

\[
\text{if } b_{\text{expr}} \text{ then } c_{\text{expr}} \text{ else skip end}
\]

\[
\text{if } b_{\text{expr}_1} \text{ then } c_{\text{expr}_1}
\]

\[
\text{elsif } b_{\text{expr}_2} \text{ then } c_{\text{expr}_2}
\]

\[
\text{elsif } b_{\text{expr}_3} \text{ then } c_{\text{expr}_3}
\]

\[
\text{... elsif } b_{\text{expr}_n} \text{ then } c_{\text{expr}_n} \text{ end}
\]

\[
\text{case expr of}
\]

\[
\text{choice_pattern}_1 \rightarrow \text{expr}_1,
\]

\[
\text{choice_pattern}_2 \rightarrow \text{expr}_2,
\]

\[
\text{... choice_pattern}_n \text{ or wild card } \rightarrow \text{expr}_n \text{ end}
\]
Example 17 ................. Choice Pattern Case Expressions: Insert Links:

We consider the meaning of the Insert operation designators.

33. The insert operation takes an Insert command and a net and yields either a new net or chaos for the case where the insertion command “is at odds” with, that is, is not semantically well-formed with respect to the net.

34. We characterise the “is not at odds”, i.e., is semantically well-formed, that is:

- \( \text{pre}_\text{int}\_\text{Insert}(\text{op})(hs,ls) \),

as follows: it is a propositional function which applies to Insert actions, \( \text{op} \), and nets, (\( hs,ls \)), and yields a truth value if the below relation between the command arguments and the net is satisfied. Let (\( hs,ls \)) be a value of type N.

35. If the command is of the form \( 2\text{oldH}(hi',l,hi'') \) then

- \( ^*1 \) \( hi' \) must be the identifier of a hub in \( hs \),
- \( ^*2 \) \( l \) must not be in \( ls \) and its identifier must (also) not be observable in \( ls \), and
- \( ^*3 \) \( hi'' \) must be the identifier of a(nother) hub in \( hs \).

36. If the command is of the form \( 1\text{oldH1newH}(hi,l,h) \) then

- \( ^*1 \) \( hi \) must be the identifier of a hub in \( hs \),
- \( ^*2 \) \( l \) must not be in \( ls \) and its identifier must (also) not be observable in \( ls \), and
- \( ^*3 \) \( h \) must not be in \( hs \) and its identifier must (also) not be observable in \( hs \).

37. If the command is of the form \( 2\text{newH}(h',l,h'') \) then

- \( ^*1 \) \( h' \) — left to the reader as an exercise (see formalisation !),
- \( ^*2 \) \( l \) — left to the reader as an exercise (see formalisation !), and
- \( ^*3 \) \( h'' \) — left to the reader as an exercise (see formalisation !).

Conditions concerning the new link (second \( ^*s \), \( ^*2 \), in the above three cases) can be expressed independent of the insert command category.

\[
\begin{align*}
\text{value} & \quad 33 \quad \text{int}\_\text{Insert}: \text{Insert} \to N \sim N \\
34' \quad \text{pre}_\text{int}\_\text{Insert}: \text{Ins} \to N \to \text{Bool} \\
34'' \quad \text{pre}_\text{int}\_\text{Insert}(\text{Ins}(\text{op}))(hs,ls) \equiv \\
\quad ^*2 \quad s_{\text{J}}(\text{op}) \notin ls \land \text{obs}_{\text{L}}(s_{\text{J}}(\text{op})) \notin \text{iols}(ls) \land \\
\quad \quad \text{case } \text{op} \text{ of} \\
\quad \quad \quad \quad 35) \quad 2\text{oldH}(hi',l,hi'') \to \{hi',hi''\} \in \text{iohs}(hs),
\end{align*}
\]
36) \[ \text{1oldH1newH}(hi,l,h) \rightarrow \]
\[ hi \in \text{iohs}(hs) \land h \notin hs \land \text{obs}_H(h) \notin \text{iohs}(hs), \]
37) \[ \text{2newH}(h',l,h'') \rightarrow \]
\[ \{h',h''\} \cap hs = \{\} \land \{\text{obs}_H(h'),\text{obs}_H(h'')\} \cap \text{iohs}(hs) = \{\} \]
\[ \text{end} \]

RSL Explanation

- 33: The value clause value int\_Insert: Insert \(\sim\) N names a value, int\_Insert, and defines its type to be Insert \(\sim\) N, that is, a partial function \(\sim\) from Insert commands and nets (N) to nets. (int\_Insert is thus a function. What that function calculates will be defined later.)

- 34': The predicate pre\_int\_Insert: Insert \(\sim\) N \(\rightarrow\) Bool function (which is used in connection with int\_Insert to assert semantic well-formedness) applies to Insert commands and nets and yield truth value true if the command can be meaningfully performed on the net state.

- 34'': The action pre\_int\_Insert(op)(hs,ls) (that is, the effect of performing the function pre\_int\_Insert on an Insert command and a net state is defined by a case distinction over the category of the Insert command. But first we test the common property:

- 2\*: s\_L(op)\(\notin\)ls\&\text{obs}_L(s\_L(op))\(\notin\)ols(ls), namely that the new link is not an existing net link and that its identifier is not already known.

- 35): If the Insert command is of kind 2oldH(h'i',l,h'i'') then \{h'i',h'i''\} \(\in\) iohs(hs), that is, then the two distinct argument hub identifiers must not be in the set of known hub identifiers, i.e., of the existing hubs hs.

- 36): If the Insert command is of kind 1oldH1newH(hi,l,h) then ... exercise left as an exercises to the reader.

- 37): If the Insert command is of kind 2newH(h',l,h'') ... exercise left as an exercises to the reader. The set intersection operation is defined in Sect. A.2.6 on page 105 Item 25 on page 106.

End of RSL Explanation

38. Given a net, (hs,ls), and given a hub identifier, (hi), which can be observed from some hub in the net, xtr\_H(hi)(hs,ls) extracts the hub with that identifier.

39. Given a net, (hs,ls), and given a link identifier, (li), which can be observed from some link in the net, xtr\_L(li)(hs,ls) extracts the hub with that identifier.
value
38: \text{\texttt{xtr}}_H : \texttt{H} \rightarrow \texttt{N} \sim H
39: \text{\texttt{xtr}}_L : \texttt{H} \rightarrow \texttt{N} \sim H

\text{RSL Explanation}

- 38: Function application \text{\texttt{xtr}}_H(h_i)(h_s, \_\_) yields the hub \( h \), i.e. the value \( h \) of type \( H \), such that \( \langle \cdot \rangle \) \( h \) is in \( h_s \) and \( h \) has hub identifier \( h_i \).
- 38: The wild-card, \_\_, expresses that the extraction (\text{\texttt{xtr}}_H) function does not need the \( L \)-set argument.
- 39: Left as an exercise for the reader.

End of RSL Explanation

40. When a new link is joined to an existing hub then the observable link identifiers of that hub must be updated to reflect the link identifier of the new link.

41. When an existing link is removed from a remaining hub then the observable link identifiers of that hub must be updated to reflect the removed link (identifier).

value
\text{\texttt{aLI}} : \texttt{H} \times \texttt{LI} \rightarrow \texttt{H}, \text{\texttt{rLI}} : \texttt{H} \times \texttt{LI} \sim \texttt{H}

\text{RSL Explanation}

- 40: The add link identifier function \text{\texttt{aLI}}:
  - The function definition clause \text{\texttt{aLI}}(h,li) as \( h' \) defines the application of \text{\texttt{aLI}} to a pair \( (h,li) \) to yield an update, \( h' \) of \( h \).
  - The pre-condition \text{\texttt{pre}} li \not\in \text{\texttt{obs}}_L(h) expresses that the link identifier \( li \) must not be observable \( h \).
The post-condition \( \text{post } \text{obs}_{\text{Lls}}(h) = \text{obs}_{\text{Lls}}(h') \setminus \{li\} \land \text{non}_{\text{Ll}}\text{eq}(h,h') \) expresses that the link identifiers of the resulting hub are those of the argument hub except \( \setminus \) that the argument link identifier is not in the resulting hub.

41: The remove link identifier function \( rLI \):

- The function definition clause \( rLI(h',li) \) as \( h \) defines the application of \( rLI \) to a pair \( (h',li) \) to yield an update, \( h \) of \( h' \).
- The pre-condition clause \( \text{pre } li \in \text{obs}_{\text{Lls}}(h') \land \text{card } \text{obs}_{\text{Lls}}(h') \geq 2 \) expresses that the link identifier \( li \) must not be observable \( h \).
- post-condition clause \( \text{post } \text{obs}_{\text{Lls}}(h) = \text{obs}_{\text{Lls}}(h') \setminus \{li\} \land \text{non}_{\text{Ll}}\text{eq}(h,h') \) expresses that the link identifiers of the resulting hub are those of the argument hub except that the argument link identifier is not in the resulting hub.

End of RSL Explanation

42. If the Insert command is of kind 2\text{newH}(h',l,h'') then the updated net of hubs and links, has

- the hubs \( hs \) joined, \( \cup \), by the set \( \{h',h''\} \) and
- the links \( ls \) joined by the singleton set of \( \{l\} \).

43. If the Insert command is of kind 1\text{oldH}1\text{newH}(hi,l,h) then the updated net of hubs and links, has

43.1 : the hub identified by \( hi \) updated, \( hi' \), to reflect the link connected to that hub.
43.2 : The set of hubs has the hub identified by \( hi \) replaced by the updated hub \( hi' \) and the new hub.
43.3 : The set of links augmented by the new link.

44. If the Insert command is of kind 2\text{oldH}(hi',l,hi'') then

44.1–.2 : the two connecting hubs are updated to reflect the new link,
44.3 : and the resulting sets of hubs and links updated.

\[
\text{int}\text{.Insert}(op)(hs,ls) \equiv \\
\star_i \text{ case } op \text{ of } \\
42 \ 2\text{newH}(h',l,h'') \rightarrow (hs \cup \{h',h''\},ls \cup \{l\}), \\
43 \ 1\text{oldH}1\text{newH}(hi,l,h) \rightarrow \\
43.1 \ \text{let } h' = a\text{Ll}(\text{xtr}_{\text{H}}(hi,hs),\text{obs}_{\text{Ll}}(l)) \text{ in } \\
43.2 \ (hs \setminus \{\text{xtr}_{\text{H}}(hi,hs)\} \cup \{h,h'\},ls \cup \{l\}) \text{ end, } \\
44 \ 2\text{oldH}(hi',l,hi'') \rightarrow
\]

November 1, 2010, 15:25, Budapest Lectures, Oct. 11–22, 2010
© Dines Bjørner 2010, Fredsvej 11, DK–2840 Holte, Denmark
let \( hs^\delta = \{ aLI(x_{tr}H(h_i',hs),obs\_LI(l)) \}, \)

\[ aLI(x_{tr}H(h_i'',hs),obs\_LI(l)) \} \text{ in} \]

\[ (hs\setminus \{ x_{tr}H(h_i',hs),x_{tr}H(h_i'',hs) \} \cup \hs^\delta,ls \cup \{ l \}) \text{ end} \]

\[ \star_j \text{ end} \]

\[ \star_k \text{ pre pre\_int\_Insert(op)(hs,ls)} \]

**RSL Explanation**

- \( \star_i \rightarrow \star_j \): The clause case op of \( p_1 \rightarrow c_1, p_2 \rightarrow c_2, \ldots p_n \rightarrow c_n \text{ end} \) is a conditional clause.

- \( \star_k \): The pre-condition expresses that the insert command is semantically well-formed — which means that those reference identifiers that are used are known and that the new link and hubs are not known in the net.

- \( \star_i + 42 \): If op is of the form \( 2\text{newH}(h_i',l,h_i'') \) then — the narrative explains the rest;

  else

- \( \star_i + 43 \): If op is of the form \( 1\text{oldH1newH}(hi,l,h) \) then

  - 43.1: \( h_i' \) is the known hub (identified by \( hi \)) updated to reflect the new link being connected to that hub,

  - 43.2: and the pair \( ([\text{updated hs,updated ls}]) \) reflects the new net: the hubs have the hub originally known by \( hi \) replaced by \( h_i' \), and the links have been simple extended \( (\cup) \) by the singleton set of the new link;

  else

- \( \star_i + 44 \): If op is of the form \( 2\text{oldH}(h_i',l,hi'') \) then

  - 44.1: the first element of the set of two hubs \( (\hs^\delta) \) reflect one of the updated hubs,

  - 44.2: the second element of the set of two hubs \( (\hs^\delta) \) reflect the other of the updated hubs,

  - 44.3: the set of two original hubs known by the argument hub identifiers are removed and replaced by the set \( \hs^\delta \);

  else — well, there is no need for a further ‘else’ part as the operator can only be of either of the three mutually exclusive forms!

**End of RSL Explanation**

45. The remove command is of the form \( \text{Rmv(li)} \) for some \( li \).

46. We now sketch the meaning of removing a link:
a) The link identifier, \( li \), is, by the \texttt{pre} \texttt{int}\_Remove\texttt{pre}\-condition, that of a link, \( l \), in the net.

b) That link connects to two hubs, let us refer to them as \( h' \) and \( h'' \).

c) For each of these two hubs, say \( h \), the following holds wrt. removal of their connecting link:
   i. If \( l \) is the only link connected to \( h \) then hub \( h \) is removed. This may mean that
      - either one
      - or two hubs
      are also removed when the link is removed.
   ii. If \( l \) is not the only link connected to \( h \) then the hub \( h \) is modified to reflect that
      it is no longer connected to \( l \).

d) The resulting net is that of the pair of adjusted set of hubs and links.

\[
\begin{align*}
45 & \text{int\_Remove: } \text{Rmv} \rightarrow \text{N} \sim \text{N} \\
46 & \text{int\_Remove(Rmv(li))(hs,ls) } \equiv \\
46a) & \text{let } l = \text{xtr}\_L(li)(ls), \{hi',hi''\} = \text{obs}\_Hls(l) \text{ in} \\
46b) & \text{let } \{h',h''\} = \{\text{xtr}\_H(hi',hs),\text{xtr}\_H(hi''hs)\} \text{ in} \\
46c) & \text{let } hs' = \text{cond}\_\text{rmv(h',hs)} \cup \text{cond}\_\text{rmv(H(h''hs,hs) in} \\
46d) & (hs\\{h',h''\} \cup hs',ls\{l\}) \text{ end end end} \\
46a) & \text{pre } li \in \text{iols(ls)}
\end{align*}
\]

\[
\begin{align*}
\text{cond}\_\text{rmv: } & \text{LI } \times \text{H } \times \text{H-set } \rightarrow \text{H-set} \\
\text{cond}\_\text{rmv(l,h,hs) } \equiv \\
46(c)i) & \text{if } \text{obs}\_\text{Hls(h)}=\{li\} \text{ then } \{} \\
46(c)ii) & \text{else } \{\text{sL}(li,h)\} \text{ end} \\
\text{pre } li \in \text{obs}\_\text{Hls(h)}
\end{align*}
\]

\textbf{RSL Explanation}

- 45: The \texttt{int\_Remove} operation applies to a remove command \texttt{Rmv(li)} and a net \((hs,ls)\) and yields a net — provided the remove command is semantically well-formed.

- 46: To Remove a link identifier by \( li \) from the net \((hs,ls)\) can be formalised as follows:
   - 46a): obtain the link \( l \) from its identifier \( li \) and the set of links \( ls \), and
   - 46a): obtain the identifiers, \( \{hi',hi''\} \), of the two distinct hubs to which link \( l \) is connected;
   - 46b): then obtain the hubs \( \{h',h''\} \) with these identifiers;
   - 46c): now examine \texttt{cond}\_\text{rmv} each of these hubs (see Lines 46(c)i)–46(c)ii)).
The examination function $\text{cond\_rmv}$ either yields an empty set or the singleton set of one modified hub (a link identifier has been removed).

- 46c) The set, $h'$, of zero, one or two modified hubs is yielded.
- That set is joined to the result of removing the hubs $\{h',h''\}$ and the set of links that result from removing $l$ from $l_s$.

The conditional hub remove function $\text{cond\_rmv}$

- 46(c)i): either yields the empty set (of no hubs) if $l_i$ is the only link identifier $\text{inh}$,
- 46(c)ii): or yields a modification of $h$ in which the link identifier $l_i$ is no longer observable.

End of RSL Explanation

End of Example 17

A.5.6 Operator/Operand Expressions

Operator/Operand Expressions

\[
\langle \text{Expr} \rangle ::= \\
\text{\langle Prefix\_Op \rangle \langle Expr \rangle} \\
| \text{\langle Expr \rangle \langle Infix\_Op \rangle \langle Expr \rangle} \\
| \text{\langle Expr \rangle \langle Suffix\_Op \rangle} \\
| \ldots
\]

\[
\langle Prefix\_Op \rangle ::= \\
- | \sim | \cup | \cap | \text{card} | \text{len} | \text{inds} | \text{elems} | \text{hd} | \text{tl} | \text{dom} | \text{rng}
\]

\[
\langle Infix\_Op \rangle ::= \\
= | \neq | \equiv | + | - | \ast | \uparrow | / | \preceq | \succeq | \prec | \succ | \Leftarrow | \Rightarrow \\
| \in | \notin | \cup | \cap | \setminus | \subseteq | \supseteq | \subset | \supset | \wedge | \vee | \Rightarrow
\]

\[
\langle Suffix\_Op \rangle ::= \\
!
\]

A.6 Imperative Constructs

A.6.1 Statements and State Changes

Often, following the RAISE method, software development starts with highly abstract, sorts and applicative constructs which, through stages of refinements, are turned into concrete types and imperative constructs.

Imperative constructs are thus inevitable in RSL.

Unit value

\[
\text{stmt: Unit } \rightarrow \text{Unit}
\]

\[
\text{stmt()}\]

© Dines Bjørner 2010, Fredsvej 11, DK–2840 Holte, Denmark

• The **Unit** clause, in a sense, denotes “an underlying state”
  – which we, for simplicity, can consider as
  – a mapping from identifiers of declared variables into their values.

• Statements accept no arguments and, usually, operate on the state
  – through “reading” the value(s) of declared variables and
  – through “writing”, i.e., assigning values to such declared variables.

• Statement execution thus changes the state (of declared variables).

• **Unit** $\rightarrow$ **Unit** designates a function from states to states.

• Statements, **stmt**, denote state-to-state changing functions.

• Affixing () as an “only” arguments to a function “means” that () is an argument of type **Unit**.

### A.6.2 Variables and Assignment

**Variables and Assignment**

0. **variable** $v$: Type := expression

1. $v := expr$

### A.6.3 Statement Sequences and **skip**

Sequencing is expressed using the ‘;’ operator. **skip** is the empty statement having no value or side-effect.

2. **skip**

3. **stmt**$_1$; **stmt**$_2$;...; **stmt**$_n$

### A.6.4 Imperative Conditionals

4. **if** $expr$ **then** **stmt**$_c$ **else** **stmt**$_a$ **end**

5. **case** $e$ **of**: $p_1$ $\rightarrow$ **S**$_1$($p_1$),..., $p_n$ $\rightarrow$ **S**$_n$($p_n$) **end**
A.6.5 **Iterative Conditionals**

6. \texttt{while expr do stmt end}
7. \texttt{do stmt until expr end}

A.6.6 **Iterative Sequencing**

8. \texttt{for i in list \cdot P(list(i)) do S(list(i)) end}
9. \texttt{for e in set \cdot P(e) do S(e) end}

A.7 **Process Constructs**

A.7.1 **Process Channels**

Let \( A, B \) and \( C \) stand for three types of (channel) messages and \( i: \text{IIdx}, j: \text{JIdx} \) for channel array indexes, then:

\[
\text{Process Channels}
\]

\[
\text{channel c:A}
\]
\[
\text{channel \{k[i]:\text{IIdx}\}:B}
\]
\[
\{c[i,j]:\text{JIdx}\}:C
\]

declare a channel, \( c \), and a set (an array) of channels, \( k[i] \), capable of communicating values of the designated types \( (A \) and \( B \)).

**Example 18** .................... **Modelling Connected Links and Hubs:**

Examples (18–21) of this section, i.e., Sect. A.7 are building up a model of one form of meaning of a transport net. We model the movement of vehicles around hubs and links. We think of each hub, each link and each vehicle to be a process. These processes communicate via channels.

- We assume a net, \( n : N \), and a set, \( vs \), of vehicles.
- Each vehicle can potentially interact
  - with each hub and
  - with each link.
- Array channel indices \( (vi,hi):\text{IVH} \) and \( (vi,li):\text{IVL} \) serve to effect these interactions.
- Each hub can interact with each of its connected links and indices \( (hi,li):\text{IHL} \) serves these interactions.
An RSL Primer

\begin{center}
\begin{verbatim}

\textbf{type}
\begin{verbatim}
N, V, VI
\end{verbatim}
\textbf{value}
\begin{verbatim}
n:N, vs:V-set
obs\_VI: V \rightarrow VI
\end{verbatim}
\textbf{type}
\begin{verbatim}
H, L, HI, LI, M
IVH = VI \times HI, IVL = VI \times LI, IHL = HI \times LI
\end{verbatim}

\begin{itemize}
\item We need some auxiliary quantities in order to be able to express subsequent channel declarations.
\item Given that we assume a net, \( n : N \) and a set of vehicles, \( vs : V S \), we can now define the following (global) values:
\begin{itemize}
\item the sets of hubs, \( hs \), and links, \( ls \) of the net;
\item the set, \( ivhs \), of indices between vehicles and hubs,
\item the set, \( ivls \), of indices between vehicles and links, and
\item the set, \( ihls \), of indices between hubs and links.
\end{itemize}
\item We are now ready to declare the channels:
\begin{itemize}
\item a set of channels, \( \{vh[i] | i:IVH \cdot i \in ivhs\} \) between vehicles and all potentially traversable hubs;
\item a set of channels, \( \{vh[i] | i:IVH \cdot i \in ivhs\} \) between vehicles and all potentially traversable links; and
\item a set of channels, \( \{hl[i] | i:IHL \cdot i \in ihls\} \), between hubs and connected links.
\end{itemize}
\end{itemize}
\end{verbatim}
\end{center}

\begin{center}
\textbf{value}
\begin{verbatim}
hs:H-set = obs\_Hs(n), ls:L-set = obs\_Ls(n)
his:HI-set = \{obs\_HI(h) | h:H \in hs\}, lis:LI-set = \{obs\_LI(l) | l:L \in ls\},
ivhs:IVH-set = \{(obs\_VI(v),obs\_HI(h)) | v:V, h:H \in vs \land h \in hs\}
ivls:IVL-set = \{(obs\_VI(v),obs\_LI(l)) | v:V, l:L \in vs \land l \in ls\}
ihls:IHL-set = \{(hi,li) | h:H, (hi,li):IHL \cdot h \in hs \land hi = obs\_HI(h) \land li = obs\_LI(ls(h))\}
\end{verbatim}
\end{center}
A.7.2 **Process Definitions**

A process definition is a function definition. The below signatures are just examples. They emphasise that process functions must somehow express, in their signature, via which channels they wish to engage in input and output events.

Processes $P$ and $Q$ are to interact, and to do so “ad infinitum”. Processes $R$ and $S$ are to interact, and to do so “once”, and then yielding $B$, respectively $D$ values.

$$
\begin{align*}
\text{value} & \\
P : \text{Unit} \to \text{in c out} \{k[i] : \text{IIdx}\} \text{ Unit} & \\
Q : i : \text{KIdx} \to \text{out c in} \ k[i] \text{ Unit} & \\
\end{align*}
$$

$P() \equiv \ldots \ c \ ? \ \ldots \ k[i] ! e \ldots ; P()$

$Q(i) \equiv \ldots \ c ! e \ldots \ k[i] ? \ldots ; Q(i)$

---

**Example 19** ................. Communicating Hubs, Links and Vehicles:

- Hubs interact with links and vehicles:
  - with all immediately adjacent links,
  - and with potentially all vehicles.
- Links interact with hubs and vehicles:
  - with both adjacent hubs,
  - and with potentially all vehicles.
Vehicles interact with hubs and links:

- with potentially all hubs.
- and with potentially all links.

\[ \text{value} \]

hub: \( hi:HL \times h:H \rightarrow \text{in}, \text{out} \ {\{ hl[(hi,li)] | li:LI \land li \in \text{obs}_Lls(h) \} } \)

\[ \text{in, out} \ {\{ vh[(vi,hi)] | vi:VI \land vi \in \text{vis} \} } \quad \text{Unit} \]

link: \( li:LI \times l:L \rightarrow \text{in}, \text{out} \ {\{ hl[(hi,li)] | hi:HI \land hi \in \text{obs}_Hls(l) \} } \)

\[ \text{in, out} \ {\{ vl[(vi,li)] | vi:VI \land vi \in \text{vis} \} } \quad \text{Unit} \]

vehicle: \( vi:VI \rightarrow (\text{Pos} \times \text{Net}) \rightarrow v:V \rightarrow \text{in}, \text{out} \ {\{ vh[(vi,hi)] | hi:HI \land hi \in \text{his} \} } \quad \text{Unit} \)

\[ \text{in, out} \ {\{ vl[(vi,li)] | li:LI \land li \in \text{lis} \} } \quad \text{Unit} \]

End of Example 19

A.7.3 Process Composition

Let \( P \) and \( Q \) stand for names of process functions, i.e., of functions which express willingness to engage in input and/or output events, thereby communicating over declared channels. Let \( P \) and \( Q \) stand for process expressions, and let \( P_i \) stand for an indexed process expression, then:

\[ P \parallel Q \] Parallel composition
\[ P \top Q \] Nondeterministic external choice (either/or)
\[ P \downarrow Q \] Nondeterministic internal choice (either/or)
\[ P \parallel Q \] Interlock parallel composition
\[ O \{ P_i | i:Idx \} \] Distributed composition, \( O = \parallel, \top, \downarrow, \parallel \)

express the parallel (\( || \)) of two processes, or the nondeterministic choice between two processes: either external (\( \top \)) or internal (\( \downarrow \)). The interlock (\( \parallel \)) composition expresses that the two processes are forced to communicate only with one another, until one of them terminates.

Example 20  Modelling Transport Nets:

- The net, with vehicles, potential or actual, is now considered a process.
- It is the parallel composition of
  - all hub processes,
  - all link processes and
  - all vehicle processes.
value
net: N → V-set → Unit
net(n)(vs) ≡
  \| \{ hub( obs_HI(h))(h)|h:H \in obs_Hs(n) \} \| 
  \| \{ link( obs_LI(l))(l)|l:L \in obs_Ls(n) \} \| 
  \| \{ vehicle(obs_VI(v))(obs_PN(v))(v)|v:V \in vs \} \|

obs_PN: V → (Pos × Net)

• We illustrate a schematic definition of simplified hub processes.

• The hub process alternates, internally non-deterministically, \[ \| \], between three sub-processes
  – a sub-process which serves the link-hub connections,
  – a sub-process which serves those vehicles which communicate that they somehow wish to enter or leave (or do something else with respect to) the hub, and
  – a sub-process which serves the hub itself — whatever that is!

hub(hi)(h) ≡
  \[ \| \{ \text{let } m = hl[(hi,li)] \ ? \text{ in } \text{hub(hi)}(E_{hl}(li)(m)(h)) \text{ end}|i:L \in \text{obs}_L(h) \} \| \]
  \[ \| \{ \text{let } m = vh[(vi,hi)] \ ? \text{ in } \text{hub(vi)}(E_{hv}(vi)(m)(h)) \text{ end}|v:V \in vs \} \| \]
  \[ \| \text{hub(hi)}(E_{hown}(h)) \| \]

• The three auxiliary processes:
  – \( E_{hl} \) update the hub with respect to (wrt.) connected link, \( li \), information \( m \),
  – \( E_{hv} \) update the hub with wrt. vehicle, \( vi \), information \( m \),
  – \( E_{hown} \) update the hub with wrt. whatever the hub so decides. An example could be signalling dependent on previous link-to-hub communicated information, say about traffic density.

\( E_{hl}: LI \rightarrow M \rightarrow H \rightarrow H \)  
\( E_{hv}: VI \rightarrow M \rightarrow H \rightarrow H \)  
\( E_{hown}: H \rightarrow H \)

The reader is encouraged to sketch/define similarly schematic link and vehicle processes.

End of Example 20
A.7.4 Input/Output Events  

Let $c$ and $k[i]$ designate channels of type $A$ and $e$ expression values of type $A$, then:

1. $c?, k[i]?$ input $A$ value
2. $c!e, k[i]!e$ output $A$ value

value

3. $P: ... \rightarrow \text{out} \ c \ ... \ , \ P(...) \equiv \ ... \ c!e \ ...$ offer an $A$ value,
4. $Q: ... \rightarrow \text{in} \ c \ ... \ , \ Q(...) \equiv \ ... \ c? \ ...$ accept an $A$ value
5. $S: ... \rightarrow \ ... \ , \ S(...) = P(...) \parallel Q(...) \text{ synchronise and communicate}$

[5] expresses the willingness of a process to engage in an event that [1,3] “reads” an input, respectively [2,4] “writes” an output. If process $P$ reaches the $c!e$ “program point before” process $Q$ ‘reaches program point’ $c?$ then process $P$ “waits” on $Q$ — and vice versa. Once both processes have reached these respective program points they “synchronise while communicating the message value $e$.

The process function definitions (i.e., their bodies) express possible [output/input] events.

Example 21 Modelling Vehicle Movements:

- Whereas hubs and links are modelled as basically static, passive, that is, inert, processes we shall consider vehicles to be “highly” dynamic, active processes.

- We assume that a vehicle possesses knowledge about the road net.
  - The road net is here abstracted as an awareness of
    - which links, by their link identifiers,
    - are connected to any given hub, designated by its hub identifier,
    - the length of the link,
    - and the hub to which the link is connected “at the other end”, also by its hub identifier

- A vehicle is further modelled by its current position on the net in terms of either hub or link positions
  - designated by appropriate identifiers
  - and, when “on a link” “how far down the link”, by a measure of a fraction of the total length of the link, the vehicle has progressed.

\begin{align*}
\text{type} & \quad \text{Net} = HI \stackrel{m}{\rightarrow} (LI \stackrel{m}{\rightarrow} HI) \\
\text{Pos} & = \text{atH} | \text{onL} \\
\text{atH} & = \text{mk}_\text{atH}(hi:HI) \\
\text{onL} & = \text{mk}_\text{onL}(fhi:HI, li:LI, f:F, thi:HI) \\
F & = \{ |f: \text{Real} \cdot 0 \leq f \leq 1 | \}
\end{align*}
We first assume that the vehicle is at a hub.

There are now two possibilities (1–2 versus [4–8]).

- Either the vehicle remains at that hub
  - [1] which is expressed by some non-deterministic wait
  - [2] followed by a resumption of being that vehicle at that location.
- [3] Or the vehicle (driver) decides to “move on”:
  - [5] Onto a link, \(li\),
  - [4] among the links, \(lis\), emanating from the hub,
  - [6] and towards a next hub, \(hi'\).
- [4,6] The \(lis\) and \(hi'\) quantities are obtained from the vehicles own knowledge of the net.
- [7] The hub and the chosen link are notified by the vehicle of its leaving the hub and entering the link,
- [8] whereupon the vehicle resumes its being a vehicle at the initial location on the chosen link.

- The vehicle chooses between these two possibilities by an internal non-deterministic choice ([3]).

\[
\text{type } M = \text{mk}_L(H(li:LI, hi:HI)) \mid \text{mk}_H(L(hi:HI, li:LI))
\]

\[
\text{value vehicle: } VI \rightarrow (\text{Pos} \times \text{Net}) \rightarrow V \rightarrow \text{Unit}
\]

\[
\text{vehicle(vi)}(\text{mk}_\text{atH}(hi), \text{net})(v) \equiv
\begin{align*}
\hline
[1] & (\text{wait} ; \\
[2] & \text{vehicle(vi)}(\text{mk}_\text{atH}(hi), \text{net})(v)) \\
[3] & [ \\
[4] & (\text{let } \text{lis}=\text{dom net(hi)} \text{ in} \\
[5] & \text{let } li:LI \in \text{lis in} \\
[6] & \text{let } hi'=(\text{net(hi)})(li) \text{ in} \\
[7] & (\text{vh}[vi,hi)]!\text{mk}_H(L(hi,li)||vl[vi,li]}!\text{mk}_H(L(hi,li))); \\
[8] & \text{vehicle(vi)}(\text{mk}_\text{onL}(hi,li,0,hi'), \text{net})(v) \\
[9] & \end{endendend)}
\]

We then assume that the vehicle is on a link and at a certain distance “down”, \(f\), that link.
There are now two possibilities ([1–2] versus [4–7]).

- Either the vehicle remains at that hub
  - [1'] which is expressed by some non-deterministic \( \text{wait} \)
  - [2'] followed by a resumption of being that vehicle at that location.
- [3'] Or the vehicle (driver) decides to “move on”.
- [4'] Either
  - [5'] The vehicle is at the very end of the link and signals the link and the hub of its leaving the link and entering the hub,
  - [6'] whereupon the vehicle resumes its being a vehicle at hub \( h' \).
- [7'] or the vehicle moves further down, some non-zero fraction down the link.

- The vehicle chooses between these two possibilities by an internal non-deterministic choice ([3]).

\[
\begin{align*}
type & \quad M ::= \mathit{mk}_L\mathit{H}(li;LI,hi;HI) \mid \mathit{mk}_H\mathit{L}(hi;HI,li;LI) \\
value & \quad \delta:\mathit{Real} = \mathit{move}(h,f) \quad \text{axiom} \quad 0 < \delta \ll 1 \\
vehicle(vi)(\mathit{mk}_{\mathit{onL}}(hi,li,f,hi'),\mathit{net})(v) & \equiv \\
[1'] \quad (\text{wait} ; \\
[2'] \quad \text{vehicle}(vi)(\mathit{mk}_{\mathit{onL}}(hi,li,f,hi'),\mathit{net})(v)) \\
[3'] \quad [ \\
[4'] \quad (\text{case } f \text{ of} \\
[5'] \quad 1 \rightarrow ((\text{vl}[vi,hi']!\mathit{mk}_L\mathit{H}(li,hi')||\text{vh}[vi,li]!\mathit{mk}_L\mathit{H}(li,hi')); \\
[6'] \quad \text{vehicle}(vi)(\mathit{mk}_{\mathit{atH}}(hi'),\mathit{net})(v)), \\
[7'] \quad \_ \rightarrow \text{vehicle}(vi)(\mathit{mk}_{\mathit{onL}}(hi,li,f+\delta,hi'),\mathit{net})(v) \\
[8'] \quad \text{end}) \\
\end{align*}
\]

\[\text{move: } H \times F \rightarrow F\]

End of Example 21

A.8 Simple RSL Specifications

Besides the above constructs RSL also possesses module-oriented scheme, class and object constructs. We shall not cover these here. An RSL specification is then simply a sequence of one or more clusters of zero, one or more sort and/or type definitions, zero, one or more variable declarations, zero, one or more channel declarations, zero, one or more value definitions (including functions) and zero, one or more and axioms. We can illustrate these specification components schematically:
The ordering of these clauses is immaterial. Intuitively the meaning of these definitions and declarations are the following.

The type clause introduces a number of user-defined type names; the type names are visible anywhere in the specification; and either denote sorts or concrete types.

The variable clause declares some variable names; a variable name denote some value of declared type; the variable names are visible anywhere in the specification: assigned to (‘written’) or values ‘read’.

The channel clause declares some channel names; either simple channels or arrays of channels of some type; the channel names are visible anywhere in the specification.

The value clause bind (constant) values to value names. These value names are visible anywhere in the specification. The specification

The indexed sort or type names, \( A \) and the indexed function names, \( d \), are defined elsewhere in the specification. The index value names, \( v \) are usually names of bound ‘variables’ of universally or existentially quantified predicates of the indexed (“comma”-separated) \( P \).
Example 22 ......................................................... A Neat Little “System”:

We present a self-contained specification of a simple system: The system models vehicles moving along a net, vehicle, the recording of vehicles entering links, enter_sensor, the recording of vehicles leaving links, leave_sensor, and the road_pricing payment of a vehicle having traversed (entered and left) a link. Note that vehicles only pay when completing a link traversal; that ‘road pricing’ only commences once a vehicle enters the first link after possibly having left an earlier link (and hub); and that no road_pricing payment is imposed on vehicles entering, staying-in (or at) and leaving hubs.

We assume the following: that each link is somehow associated with two pairs of sensors: a pair of enter and leave sensors at one end, and a pair of enter and leave sensors at the other end; and a road pricing process which records pairs of link enterings and leavings, first one, then, after any time interval, the other, with leavings leading to debiting of traversal fees; Our first specification define types, assume a net value, declares channels and state signatures of all processes.

- ves stand for vehicle entering (link) sensor channels,
- vls stand for vehicle leaving (link) sensor channels,
- rp stand for ‘road pricing’ channel
- enter_sensor(hi,li) stand for vehicle entering [sensor] process from hub hi to link (li).
- leave_sensor(li,hi) stand for vehicle leaving [sensor] process from link li to hub (hi).
- road_pricing() stand for the unique ‘road pricing’ process.
- vehicle(vi)(...) stand for the vehicle vi process.

\[
\text{type} \\
\text{N, H, HI, LI, VI} \\
\text{RPM} \Rightarrow \text{mk}_{\text{Enter}}(\text{VI,LI}) | \text{mk}_{\text{Leave}}(\text{VI,LI}) \\
\text{value} \\
n:N \\
\text{channel} \\
\{ \text{ves}[\text{obs}_{\text{HL}}(h),li]|h: H \in \text{obs}_{\text{HS}}(n) \land li \in \text{obs}_{\text{LIs}}(h) \} : \text{VI} \\
\{ \text{vls}[li,\text{obs}_{\text{HL}}(h)]|h: H \in \text{obs}_{\text{HS}}(n) \land li \in \text{obs}_{\text{LIs}}(h) \} : \text{VI} \\
\text{rp:RPM} \\
\text{type} \\
\text{Fee, Bal} \\
\text{LVS} \Rightarrow \text{LI} \rightarrow \text{VI-set}, \text{FEE} \Rightarrow \text{LI} \rightarrow \text{Fee}, \text{ACC} \Rightarrow \text{VI} \rightarrow \text{Bal} \\
\text{value} \\
\text{link: (LI \times L) \rightarrow Unit} \\
\text{enter_sensor: (HI \times LI) \rightarrow in ves[hi,li], out rp Unit}
To understand the sensor behaviours let us review the vehicle behaviour. In the vehicle behaviour defined in Example 21, in two parts, Page 136 and Page 137 we focus on the events [7] where the vehicle enters a link, respectively [5′] where the vehicle leaves a link. These are summarised in the schematic reproduction of the vehicle behaviour description. We redirect the interactions between vehicles and links to become interactions between vehicles and enter and leave sensors.

value
\[ \delta : \text{Real} = \text{move}(h,f) \quad \text{axiom} \quad 0 < \delta < 1 \]
move: \( H \times F \rightarrow F \)
vehicle: \( V I \rightarrow (\text{Pos} \times \text{Net}) \rightarrow V \rightarrow \text{Unit} \)
vehicle\((vi)\)(pos,net)(v) \:\equiv \:
[1] \ (\text{wait}) ;
[2] \ vehicle\((vi)\)(pos,net)(v))
[3] \end
\quad \text{case} \ pos \ of
\quad \text{mk}_\text{atH}(hi) \rightarrow
[4–6] \ (\text{let} \ lis=\text{dom}(hi) \ \text{in} \ \text{let} \ li:L Li li \in \ lis \ \text{in} \ \text{let} \ hi\prime=(\text{net}(hi))(li) \ \text{in}
[7] \ \text{ves}[hi,li]!vi;
[8] \ vehicle\((vi)\)(\text{mk}_\text{onL}(hi,li,0,hi\prime),\text{net})(v)
[9] \end \end \end
\quad \text{mk}_\text{onL}(hi,li,f,hi\prime) \rightarrow
[4′] \ (\text{case} \ f \ of
[5′–6′] \ 1 \rightarrow (\text{vls}[li,hi]!vi; \ vehicle\((vi)\)(\text{mk}_\text{atH}(hi\prime),\text{net})(v))
[7′] \ _ \rightarrow \ vehicle\((vi)\)(\text{mk}_\text{onL}(hi,li,f+\delta,hi\prime),\text{net})(v)
[8′] \end \end
\end
\end

- As mentioned on Page 139 link behaviours are associated with two pairs of sensors:
  - a pair of enter and leave sensors at one end, and
  - a pair of enter and leave sensors at the other end;

value
link\((li)\)(l) \equiv
\quad \text{let} \ \{hi, hi\prime\} = \text{obs_Hls}(l) \ \text{in}
\quad \text{enter}_\text{sensor}(hi,li) || \text{leave}_\text{sensor}(li,hi) ||
\quad \text{enter}_\text{sensor}(hi\prime,li) || \text{leave}_\text{sensor}(li,hi\prime) \ \text{end}
\quad \text{enter}_\text{sensor}(hi,li) \equiv
\quad \text{let} \ vi = \text{ves}[hi,li]? \ \text{in} \ \text{rp!mk}_\text{Enter_LI}(vi,li); \ \text{enter}_\text{sensor}(hi,li) \ \text{end}
\quad \text{leave}_\text{sensor}(li,hi) \equiv
\quad \text{let} \ vi = \text{ves}[li,hi]? \ \text{in} \ \text{rp!mk}_\text{Leave_LI}(vi,li); \ \text{enter}_\text{sensor}(li,hi) \ \text{end}
• The LVS component of the \textit{road\textunderscore pricing} behaviour serves,
  – among other purposes that are not mentioned here,
  – to record whether the movement of a vehicle’s “originates” along a link or not.

• Otherwise we leave it to the reader to carefully read the formulas.

\begin{verbatim}
value
  payment: VI × LI → (ACC × FEE) → ACC
  payment(vi,li)(fee,acc) ≡
    let bal' = if vi ∈ dom acc then add(acc(vi),fee(li)) else fee(li) end
    in acc ‖ [vi ↔ bal'] end
  add: Fee × Bal → Bal [add fee to balance]
  road\textunderscore pricing(lvs,fee,acc) ≡ in rp
    let m = rp? in
    case m of
      mk Enter LI(vi,li) →
        road\textunderscore pricing(lvs[li→lvs(li)∪\{vi}\],fee,acc),
      mk Leave LI(vi,li) →
        let lvs' = if vi ∈ lvs(li) then lvs[li→lvs(li)\{vi}\] else lvs end,
        acc' = payment(vi,li)(fee,acc) in
        road\textunderscore pricing(lvs',fee,acc')
    end end end
\end{verbatim}

End of Example 22