Towards intuitive specifications with ready relations

Ragnhild Kobro Runde
Department of Informatics, University of Oslo, Norway

October 11, 2000

Overview

Basis: A formalism for the specification of interacting objects, presented by Olaf Owe at NWPT'97.

Goal: Make the formalism more intuitive, based on the experiences from a case study ("The RPC-Memory Specification Problem" by Manfred Broy and Leslie Lamport").

Outline of today's presentation:

- Introduction to the formalism and the use of ready relations
- A short example
- The old semantics
- Changing the semantics
- Parallel composition (with example)
- Conclusion

Background

The main principles of the formalism:

- Easy and intuitive specifications
- Abstract, black-box specifications
- Focus on observable actions
- Object-orientation (objects have identity and activity)
- Parallel and non-deterministic objects

Readiness

We use ready relations to specify the possible actions that an object may be engaged in. $\leftarrow$ is used to express immediate readiness, such that $A \leftarrow x$ means that the object A is immediately ready for the event x.

For each object, we may consider the sequence of observable actions that it has been involved in. This gives us an abstract view of the object's state.

A/h denotes the continuation of A after the event-sequence h.

External non-determinism: $A \leftarrow x \wedge A \leftarrow y$ means that A is ready for both x and y (and the environment chooses which one will happen).

Internal non-determinism: $A \leftarrow x \vee A \leftarrow y$ means that A is ready for either x or y, but not necessarily both.

Example: A gambling machine

The gambling machine has the following events:

- $c(v)$ - accept a chip worth v credits from the user.
- $r(v)$ - the player wins v credits.

The machine can now be specified by:

- $\forall v : Nat, h : seq \cdot M/h \leftarrow c(v)$
- $\forall h : seq, v : Nat \; \exists v' : Nat \cdot M/h \vdash c(v) \leftarrow r(v')$
- $\forall v : Nat, h : seq \cdot v > In(h) - Out(h) \Rightarrow M/h \nleftarrow r(v)$

The functions In and Out give the sums of credit points input and output. They may be defined inductively as follows:

$In(\varepsilon) == 0$ $\quad$ $Out(\varepsilon) == 0$

$In(h \vdash c(v)) == In(h) + v$ $\quad$ $Out(h \vdash c(v)) == Out(h)$

$In(h \vdash r(v)) == In(h)$ $\quad$ $Out(h \vdash r(v)) == Out(h) + v$

Semantics

A deterministic object can be described by its trace set, i.e. the possible sequences of events it is ready to accept.

In one particular execution, a non-deterministic object behaves like a deterministic one. Thus, a non-deterministic object can be described by the set of its deterministic instances.

Accordingly, the ready relation must be interpreted as the collection of the corresponding indexed relations (one for each possible execution). This gives that a formula p should be semantically interpreted as $\forall i \cdot p_i$, where p_i is equal to p, but with $\leftarrow$ replaced by $\underset{i}{\leftarrow}$.

$[A]_i^*$ denotes the trace set of object A in execution i. Two objects A and B with the same alphabet are equal if they have the same trace-sets:

$$A = B \triangleq \forall i \cdot [A]_i^* = [B]_i^*$$

In the original formalism, readiness is defined by: $A \underset{i}{\leftarrow} x \triangleq \langle x \rangle \in [A]_i^*$

The dead and the meaningless object

0_s represents the dead object with alphabet s. This is a totally meaningful object, but it will never be able to do anything. Its trace-set is therefore defined by:

$$[0_s]_i^* \triangleq \{\varepsilon\}$$

$\bot_s$ represents the meaningless object with alphabet s. Naturally, it never occurs in a real implementation. However, in a specification, $A/h \vdash x$ will be meaningless if we have $A/h = 0_{\alpha A}$. The meaningless object has an even smaller trace set than the dead object:

$$[\bot_s]_i^* \triangleq \emptyset$$

Redefining the semantics

Readiness according to the original definition: $A \underset{i}{\leftarrow} x \triangleq \langle x \rangle \in [A]_i^*$
Disadvantage: The specification $\forall h \cdot M/h \leftarrow x$ becomes false if M/h happens to be the meaningless object ($\bot_s$). The correct specification must be written:

$$\forall h \cdot M/h \neq \bot \Rightarrow M/h \leftarrow x$$

The assumption $M/h \neq \bot$ is not very intuitive, and easily forgotten. The new semantics of $\underset{i}{\leftarrow}$ makes this assumption redundant:

$$\forall h : s^* \cdot \bot_s \underset{i}{\leftarrow} h$$

$$A \underset{i}{\leftarrow} h \triangleq A \neq \bot \Rightarrow h \in [A]_i^*$$

The new proof system

Based on first order logic with equality, with the addition of the following axioms and the equality proof rule (all of which should be sound):

- (A1) $\vdash A/\varepsilon = A$
- (A2) $\vdash A/h/h' = A/h;h'$
- (A3) $\vdash A \leftarrow h \Rightarrow h \in (\alpha A)^*$
- (A4) $\vdash A \leftarrow h;h' \Leftrightarrow A \leftarrow h \ \wedge \ A/h \leftarrow h'$
- (A5) $\vdash A \leftarrow h \Rightarrow A = \bot \vee A/h \neq \bot$
- (A6) $\vdash \bot_s \leftarrow h$
- (A7) $\vdash \bot/h = \bot$
- (A8) $\vdash \forall x \cdot 0_s \nleftarrow x$
- (A9) $\vdash \forall x \cdot 0/\langle x \rangle \leftarrow h$
- (equality) $\dfrac{\vdash \forall h \cdot A \leftarrow h \Leftrightarrow B \leftarrow h \qquad \vdash A \neq \bot_{\alpha A} \qquad \vdash B \neq \bot_{\alpha B}}{\vdash A = B}$

Parallel composition

Proposal: We ignore the meaningless as much as possible, wanting $A \parallel \bot = A$.

A desired axiom for parallel composition of objects A and B with the same alphabet is: $(A \parallel B) \leftarrow x \Leftrightarrow A \leftarrow x \wedge B \leftarrow x$

Left hand-side semantically: $(A \parallel B) \neq \bot \Rightarrow x \in [A \parallel B]_i^*$
Right hand-side semantically: $(A \neq \bot \Rightarrow x \in [A]_i^*) \wedge (B \neq \bot \Rightarrow x \in [B]_i^*)$

For $A \neq \bot$ and $B \neq \bot$ we need $[A \parallel B]_i^* = [A]_i^* \cap [B]_i^*$.
For $A = \bot$ or $B = \bot$ we need to keep the trace set of the object not equal to $\bot$, that is $[A \parallel B]_i^* = [A]_i^* \cup [B]_i^*$

This yields the definition:
$[A \parallel B]_i^* \triangleq$
$\{h \mid A \neq \bot \wedge B \neq \bot \wedge h \in [A]_i^* \cap [B]_i^*\} \cup \{h \mid (A = \bot \vee B = \bot) \wedge h \in [A]_i^* \cup [B]_i^*\}$

Example: A gambling hall

We have n different gambling machines, indexed from 1 to n. Each machine M_i has two events, get chip ($c_i(v)$) and return credits ($r_i(v)$). Specification for M_i:

- $\forall v, h \cdot\ M_i/h \leftarrow c_i(v)$
- $\forall v, h \cdot\ M_i/h \leftarrow r_i(0)$
- $\forall v, h \cdot\ M_i/h \vdash c_i(v) \leftarrow r_i(2 * v)$

We specify a boss that makes sure the gambling hall as a whole has a profit of at least 20%:

- $\forall v, h, i \cdot\ B/h \leftarrow c_i(v)$
- $\forall v, h, i \cdot\ B/h \leftarrow r_i(0) \vee B/h \leftarrow r_i(v)$
- $\forall v, h, i \cdot\ v > In(h) * 0.8 - Out(h) \Rightarrow B/h \nleftarrow r_i(v)$

The functions In and Out are as before, only adjusted for the i-index.

Example: The gambling hall implements the gambling machine

For simplicity, we show the implementation with only one machine in the hall ($n = 1$). The gambling hall will then be written $M_1 \parallel B$.

- Prove: $\forall v, h \cdot (M_1 \parallel B)/h \leftarrow c_1(v)$.
  Using the axiom for parallel composition, we must prove
  a) $\forall v, h \cdot M_1/h \leftarrow c_1(v)$ (trivial)
  b) $\forall v, h \cdot B/h \leftarrow c_1(v)$ (trivial)
- Prove: $\forall h, v\ \exists v' \cdot (M_1 \parallel B)/h \vdash c_1(v) \leftarrow r_1(v')$
  a) The specification of M_1 gives $M_1/h \vdash c_1(v) \leftarrow r_1(0)$ and $M_1/h \vdash c_1(v) \leftarrow r_1(2 * v)$, i.e. both $v' = 0$ and $v' = 2 * v$ are possible.
  b) The specification of B gives either $B/h \vdash c_1 \leftarrow r_1(0)$ or $B/h \vdash c_1 \leftarrow r_1(2 * v)$, assuring that either $v' = 0$ or $v' = 2 * v$ will be possible for the parallel composition.
- Prove: $\forall v, h \cdot v > In(h) - Out(h) \Rightarrow (M_1 \parallel B)/h \nleftarrow r_1(v)$
  To prove that a parallel composition is *not* ready for an event, it is enough to prove that the event is not possible for one of the components. For $v > In(h) - Out(h)$, we will also have $v > In(h) * 0.8 - Out(h)$ and the specification of B will give $B/h \nleftarrow r_1(v)$.

Conclusion

We have achieved a more intuitive formalism by:

- Changing the semantics of the ready relation ($\leftarrow$)
- Building a new, sound proof system
- Proving that parallel composition with the new semantics can be handled very nicely.

Further work:

- Liveness (general readiness) with the new semantics
- Completeness of the proof system
- (Real-time)