Towards intuitive specifications with ready relations

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

September 15, 2000

At NWPT'97, Olaf Owe presented a formalism for specification of interacting objects [Owe98]. His formalism was based upon the concept of ready-set semantics, as opposed to CSP’s failure-set semantics [Hoa85]. As in CSP, the formalism considers the sequence of observable actions that each object has been involved in. However, specifications are interpreted for a given, but arbitrary execution, allowing specification of both internal and external nondeterminism in an intuitive way (no additional operators needed).

The ready relations are used to specify the possible actions that an object may be engaged in. The symbol $\leftrightarrow$ is used to express immediate readiness, such that $A \leftrightarrow x$ means that the object $A$ is immediately ready for the event $x$. The object expression $A=h$ denotes the continuation of the object $A$ after the event-sequence $h$.

The object-constant 0 represents an object in deadlock, whereas $\bot$ is the meaningless object. Of course, the meaningless object never occurs in an implementation. However, it is difficult to construct a syntax that doesn’t allow it to be specified. For instance, there is usually nothing wrong with the object expression $A/h \vdash x$ (the object $A$ after the sequence of $h$ extended with $x$), but the expression is meaningless if $A/h = 0$, since the dead object has no possible continuation. As a consequence, specifications written in the style of [Owe98], usually has the form:

$$A/h \neq \bot \Rightarrow A/h \leftrightarrow x$$  \hspace{1cm} (1)

The assumption $A/h \neq \bot$ is necessary, since $\bot \leftrightarrow x$ is always false.

We propose a change to the semantics of $\leftrightarrow$ in connection with $\bot$, such that the formula $\bot \leftrightarrow x$ becomes trivially true, and (1) can be shortened to $A/h \leftrightarrow x$, which is also what many people would have written in the first place. This change leads to greater complexity of the underlying semantics, and as a consequence more complex proofs at this semantic level. The intention is that people using the formalism shouldn’t need to worry about the semantics anyway, so this increase in complexity should be outweighed by the benefits coming from shorter and more intuitive specifications.

In accordance with the “don’t think about the meaningless”-approach, we suggest that a parallel composition (denoted by $||$) should only be considered meaningless if all of its components are. This is in contrast to [Owe98], where
$B \parallel \bot = \bot$ regardless of whether $B$ is meaningful or not. With our approach, we do however maintain the desirable axiom that a parallel composition is ready for an event if and only if all of its components are. For objects $A$ and $B$ with the same alphabet, this can be written as:

\[
(A \parallel B)/h \leftarrow x \Leftrightarrow A/h \leftarrow x \land B/h \leftarrow x
\]  

(2)

References
