Specifications involving initial values

Lex Bijlsma
lex.bijlsma@acm.org

March, 2000

1 Two approaches to the use of initial values

Consider a statespace Ω. Traditionally, we characterize statements over Ω by a pair of predicates over Ω: the Hoare triple notation

$$\{U\} \;\; S \;\; \{V\} \tag{1}$$

signifies

$$[U \;\Rightarrow\; wp.S.V] \,,$$

where the brackets denote universal quantification over Ω. For many purposes, however, it is more practical to use a convention where the postcondition V is not a predicate over Ω but rather over $\Omega \times \Omega_\bullet$, where $\Omega_\bullet$ is a disjoint copy of Ω. Let us call this an *extended* predicate, as opposed to a *plain* predicate that is defined over Ω. If x is the coordinate vector of Ω and $x_\bullet$ that of $\Omega_\bullet$, extended predicates contain both x and $x_\bullet$. The idea is that $x_\bullet$ is used to record the initial value of x. For instance, a statement that squares the value of x may be specified as

$$\{true\} \;\; S \;\; \{x = x_\bullet^2\} \,.$$

A similar notation is used, for instance, in the postcondition notation of the Eiffel programming language [5] (where $x_\bullet$ is called **old** x) and in the OCL specification language [7] (where $x_\bullet$ is called x@**pre**). Its usefulness lies in the fact that it shortens specifications by doing away with the need for most specification variables, without having to drag in the full apparatus of the relational calculus. The extent to which this simple expedient cleans up formulae becomes clear if we observe that the classical criterion for repetition termination [2, (9, 28)]

$$\langle\, \forall \tau :: \{P \wedge B \wedge t = \tau\} \;\; S \;\; \{P \;\wedge\; t < \tau\} \,\rangle$$

can now be shortened to

$$\{P \wedge B\} \;\; S \;\; \{P \;\wedge\; t < t_\bullet\} \,. \tag{2}$$

As suggested by these examples, the intention may be captured by considering $x_\bullet$ as a specification variable and implicitly extending the precondition with a conjunct $x = x_\bullet$. In other words, (1) may be defined for extended V by

$$\langle\, \forall x_\bullet :: [U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.V] \,\rangle \,, \tag{3}$$

where the brackets still quantify over Ω. Some applications of this approach were demonstrated in [3].

A slightly different way of formalizing initial values, used in [4, page 22], is to consider *statements* over $\Omega \times \Omega_\bullet$ as well. That makes $x_\bullet$ into an ordinary coordinate of the state space; in the interpretation of (1), S is then prefixed implicitly with an assignment statement $x_\bullet := x$. This suggests that the meaning of (1) for extended V may alternatively be given by

$$[U \;\Rightarrow\; wp.(x_\bullet := x; S).V]' \;, \tag{4}$$

where the primed brackets quantify over $\Omega \times \Omega_\bullet$.

2 Equivalence of the two approaches

We now show that definitions (3) and (4) are equivalent.

$$\begin{array}{ll}
& \langle\, \forall x_\bullet :: [U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.V] \,\rangle \\
\equiv & \quad \{\text{interchange of quantification}\} \\
& [\langle\, \forall x_\bullet :: U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.V \,\rangle] \\
\equiv & \quad \{\text{shunting}\} \\
& [\langle\, \forall x_\bullet :: x = x_\bullet \;\Rightarrow\; (U \Rightarrow wp.S.V) \,\rangle] \\
\equiv & \quad \{\text{trading}\} \\
& [\langle\, \forall x_\bullet : x = x_\bullet : U \Rightarrow wp.S.V \,\rangle] \\
\equiv & \quad \{\text{one-point rule}\} \\
& [(x_\bullet := x).(U \Rightarrow wp.S.V)] \\
\equiv & \quad \{\text{predicate between brackets is independent of } x_\bullet\,\} \\
& [(x_\bullet := x).(U \Rightarrow wp.S.V)]' \\
\equiv & \quad \{\, U \text{ is independent of } x_\bullet\,\} \\
& [U \;\Rightarrow\; (x_\bullet := x).(wp.S.V)]' \\
\equiv & \quad \{\text{definition of assignment}\} \\
& [U \;\Rightarrow\; wp.(x_\bullet := x).(wp.S.V)]' \\
\equiv & \quad \{\text{definition of sequential composition}\} \\
& [U \;\Rightarrow\; wp.(x_\bullet := x; S).V]' \;.
\end{array}$$

3 Intermezzo on *wdec*

Consider (1) with U and V as in (2). Rewriting this in the form of the middle line in the previous derivation, viz.

$$[(x_\bullet := x).(U \Rightarrow wp.S.V)] \;, \tag{5}$$

gives

$$\begin{array}{ll}
& \{P \wedge B\} \;\; S \;\; \{P \;\wedge\; t < t_\bullet\} \\
\equiv & \quad \{(5) \text{ with } U, V := P \wedge B,\; P \;\wedge\; t < t_\bullet\,\} \\
& [(t_\bullet := t).(P \wedge B \;\Rightarrow\; wp.S.(P \;\wedge\; t < t_\bullet))] \\
\equiv & \quad \{\text{conjunctivity of } wp\,\} \\
& [(t_\bullet := t).(P \wedge B \;\Rightarrow\; wp.S.P \;\wedge\; wp.S.(t < t_\bullet))]
\end{array}$$

$$
\begin{array}{ll}
\equiv & \{\text{distribution}\} \\
& [(t_\bullet := t).(P \wedge B \;\Rightarrow\; wp.S.P)] \;\wedge\; [(t_\bullet := t).(P \wedge B \;\Rightarrow\; wp.S.(t < t_\bullet))] \\
\equiv & \{\, P\,,\; B\,,\; S \text{ independent of } t_\bullet \,\} \\
& [P \wedge B \;\Rightarrow\; wp.S.P] \;\wedge\; [P \wedge B \;\Rightarrow\; (t_\bullet := t).(wp.S.(t < t_\bullet))]\,.
\end{array}
$$

Here the first conjunct expresses the invariance of P; the second one is sometimes [1, page 43] written as

$$[P \wedge B \;\Rightarrow\; wdec.S.t]\,.$$

This suggests the formal definition

$$[wdec.S.t \;\equiv\; (t_\bullet := t).(wp.S.(t < t_\bullet))]\,,$$

which is, in fact, precisely the definition given in [6, page 72].

4 Weakening postconditions

The classical theorem about weakening postconditions reads

$$\{U\}\;\; S \;\; \{V\} \;\wedge\; [V \Rightarrow W] \;\Rightarrow\; \{U\}\;\; S \;\; \{W\}\,. \tag{6}$$

Obviously this must be adjusted in the case where V and W are extended predicates, for instance because one must decide what to do with the free $x_\bullet$ now occurring in $[V \Rightarrow W]$. The most obvious solution would be to replace (6) with

$$\{U\}\;\; S \;\; \{V\} \;\wedge\; [V \Rightarrow W]' \;\Rightarrow\; \{U\}\;\; S \;\; \{W\}\,, \tag{7}$$

where the Hoare triples are interpreted as discussed above, and again the primed brackets quantify over $\Omega \times \Omega_\bullet$. However, it turns out that (7), although valid, is too weak to be useful. We shall now derive a better replacement.

$$
\begin{array}{ll}
& \{U\}\;\; S \;\; \{W\} \\
\equiv & \{(3) \text{ with } V := W\,\} \\
& \langle\, \forall x_\bullet :: [U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.W]\,\rangle \\
\equiv & \{\text{see Lemma below; } U_\bullet \text{ abbreviates } (x := x_\bullet).U\,\} \\
& \langle\, \forall x_\bullet :: [U \;\wedge\; U_\bullet \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.W]\,\rangle \\
\equiv & \{\text{shunting}\} \\
& \langle\, \forall x_\bullet :: [U_\bullet \;\Rightarrow\; (U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.W)]\,\rangle \\
\equiv & \{\, U_\bullet \text{ is independent of state}\} \\
& \langle\, \forall x_\bullet :: U_\bullet \;\Rightarrow\; [U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.W]\,\rangle \\
\equiv & \{\text{trading}\} \\
& \langle\, \forall x_\bullet : U_\bullet : [U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.W]\,\rangle \\
\Leftarrow & \{\text{transitivity}\} \\
& \langle\, \forall x_\bullet : U_\bullet : [U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.V] \;\wedge\; [wp.S.V \;\Rightarrow\; wp.S.W]\,\rangle \\
\Leftarrow & \{\text{monotonicity of } wp\,\} \\
& \langle\, \forall x_\bullet : U_\bullet : [U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.V] \;\wedge\; [V \Rightarrow W]\,\rangle \\
\equiv & \{\text{term split}\} \\
& \langle\, \forall x_\bullet : U_\bullet : [U \;\wedge\; x = x_\bullet \;\Rightarrow\; wp.S.V]\,\rangle \;\;\wedge\;\; \langle\, \forall x_\bullet : U_\bullet : [V \Rightarrow W]\,\rangle
\end{array}
$$

$\Leftarrow$ {formal weakening of domain}
$\langle\, \forall x_\bullet :: [U \ \wedge\ x = x_\bullet \ \Rightarrow\ wp.S.V] \,\rangle \ \wedge\ \langle\, \forall x_\bullet : U_\bullet : [V \Rightarrow W] \,\rangle$
$\equiv$ {(3)}
$\{U\}\ \ S\ \ \{V\} \ \wedge\ \langle\, \forall x_\bullet : U_\bullet : [V \Rightarrow W] \,\rangle$.

This shows that a better replacement for (7) is

Theorem 1 *For plain U and extended V, W,*

$$\{U\}\ \ S\ \ \{V\} \ \wedge\ \langle\, \forall x_\bullet : U_\bullet : [V \Rightarrow W] \,\rangle \ \Rightarrow\ \ \{U\}\ \ S\ \ \{W\} \tag{8}$$

where $U_\bullet$ is short for $(x := x_\bullet).U$.

As an example, we observe that

$$\{x > 0\}\ \ S\ \ \{x = x_\bullet\}$$

implies

$$\{x > 0\}\ \ S\ \ \{x > 0\}\ ,$$

because

$$\langle\, \forall x_\bullet : x_\bullet > 0 : [x = x_\bullet \ \Rightarrow\ x > 0] \,\rangle\ .$$

In this case the stronger requirement from (7), viz.

$$[x = x_\bullet \ \Rightarrow\ x > 0]'$$

does not hold.

(At this point, it may be remarked in passing that the theorem about strengthening preconditions carries no surprises of this kind and is just what you would expect it to be.)

In the derivation of (8), the following auxiliary result was used.

Lemma *For every predicate P,*

$$[P \ \wedge\ x = x_\bullet \ \equiv\ P \ \wedge\ (x := x_\bullet).P \ \wedge\ x = x_\bullet]\ .$$

Proof By propositional calculus, the above equivalence may be rewritten as

$$[P \ \wedge\ x = x_\bullet \ \Rightarrow\ (x := x_\bullet).P]\ .$$

This is easily proved:

$P \ \wedge\ x = x_\bullet$
$\Rightarrow$ {instantiation}
$\langle\, \exists x :: P \ \wedge\ x = x_\bullet \,\rangle$
$\equiv$ {trading}
$\langle\, \exists x : x = x_\bullet : P \,\rangle$
$\equiv$ {one-point rule}
$(x := x_\bullet).P$.

5 Sequential composition

The classical theorem about sequential composition reads

$$\{U\}\ \ S\ \ \{V\}\ \ \wedge\ \ \{V\}\ \ T\ \ \{W\}\ \ \Rightarrow\ \ \{U\}\ \ S;\, T\ \ \{W\}\,.$$

When preconditions and postconditions are no longer of the same type, this rule needs adjusting. We have, for plain U and extended V, W,

$$\begin{array}{ll}
& \{U\}\ \ S;\, T\ \ \{W\} \\
\equiv & \quad \{(4) \text{ with } S, V := (S;T), W\ \} \\
& [U\ \Rightarrow\ wp.(x_\bullet := x;\ S;\ T).W]' \\
\equiv & \quad \{\text{definition of sequential composition}\} \\
& [U \Rightarrow wp.(x_\bullet := x;\ S).(wp.T.W)]' \\
\equiv & \quad \{(4) \text{ with } V := wp.T.W\ \} \\
& \{U\}\ \ S\ \ \{wp.T.W\} \\
\Leftarrow & \quad \{\text{previous section}\} \\
& \{U\}\ \ S\ \ \{V\}\ \ \wedge\ \ \langle\, \forall x_\bullet : U_\bullet : [V\ \Rightarrow\ wp.T.W]\,\rangle\,,
\end{array}$$

which proves

Theorem 2 *For plain U and extended V, W,*

$$\{U\}\ \ S\ \ \{V\}\ \ \wedge\ \ \langle\, \forall x_\bullet : U_\bullet : [V\ \Rightarrow\ wp.T.W]\,\rangle\ \ \Rightarrow\ \ \{U\}\ \ S;\, T\ \ \{W\}\,.$$

As an example of the application of this rule, observe that

$$\{x > 0\}\ \ S\ \ \{x = x_\bullet - 1\}$$

and

$$\{x \geq 0\}\ \ T\ \ \{x = x_\bullet + 2\} \tag{9}$$

imply

$$\{x > 0\}\ \ S;\, T\ \ \{x = x_\bullet + 1\}$$

because

$$\begin{array}{ll}
& \langle\, \forall x_\bullet : x_\bullet > 0 : [x = x_\bullet - 1\ \Rightarrow\ wp.T.(x = x_\bullet + 1)]\,\rangle \\
\equiv & \quad \{\text{dummy transformation } x_\bullet := x_\bullet + 1\ \} \\
& \langle\, \forall x_\bullet : x_\bullet \geq 0 : [x = x_\bullet\ \Rightarrow\ wp.T.(x = x_\bullet + 2)]\,\rangle \\
\equiv & \quad \{\text{using the domain to rewrite the antecedent of the implication}\} \\
& \langle\, \forall x_\bullet : x_\bullet \geq 0 : [x \geq 0\ \wedge\ x = x_\bullet\ \Rightarrow\ wp.T.(x = x_\bullet + 2)]\,\rangle \\
\Leftarrow & \quad \{\text{formal weakening of the domain}\} \\
& \langle\, \forall x_\bullet :: [x \geq 0\ \wedge\ x = x_\bullet\ \Rightarrow\ wp.T.(x = x_\bullet + 2)]\,\rangle \\
\equiv & \quad \{(3)\} \\
& \{x \geq 0\}\ \ T\ \ \{x = x_\bullet + 2\} \\
\equiv & \quad \{(9)\} \\
& \mathit{true}\,.
\end{array}$$

References

[1] Edsger W. Dijkstra, *A discipline of programming*. Prentice-Hall, Englewood Cliffs NJ, 1976.

[2] Edsger W. Dijkstra and Carel S. Scholten, *Predicate calculus and program semantics*. Springer-Verlag, New York, 1990.

[3] A.J.M. van Gasteren and A. Bijlsma, 'An extension of the program derivation format', in: David Gries and Willem-Paul de Roever (eds.), *Programming Concepts and Methods (PROCOMET '98)*. Chapman & Hall, London, 1998; pp. 167–183.

[4] K. Rustan M. Leino, *Toward reliable modular programs*. Ph.D. thesis, California Institute of Technology, Pasadena, 1995.

[5] Bertrand Meyer, *Object-oriented software construction*, 2nd ed. Prentice Hall PTR, Upper Saddle River NJ, 1997.

[6] M. Rem, *Associons and the closure statement*. Mathematical Centre Tracts 76. Mathematisch Centrum, Amsterdam, 1976.

[7] Jos Warmer and Anneke Kleppe, *The Object Constraint Language: precise modeling with UML*. Addison-Wesley, Reading MA, 1999.