Our book's omission on quantification over scalar subtypes

In our book [DS90], we failed to introduce scalars of type T as a subtype of structures of type T, and consequently, our use of the expression "of the same type" is sometimes ambiguous. In the rest of this text, x, y stand for dummies of type structure of type T, and c for a scalar dummy of type T.

In [AB36], Lex Bijlsma rightly points out that our text can be interpreted as suggesting the truth of the generally false

$$[\langle \forall c : [c = x] : f.c \rangle \equiv f.x]$$

and that our text fails to deal explicitly with the theorem that for punctual f

(0) $\quad [\langle \forall c : c = x : f.c \rangle \equiv f.x]$

(a theorem which is used!). The purpose of this note is to remedy this situation.

* * *

We shall use for the subtype relation between x and c the postulate

(1) $\quad \langle \forall c :: \langle \exists x :: [x = c] \rangle \rangle$,

from which — since $[[X] \Rightarrow X]$ —

(2) $\langle\forall c :: [\langle\exists x :: x = c\rangle]\rangle$

follows. Furthermore, the fact that c is not just a subtype of the structure x but is the corresponding scalar type leads to the postulate

(3) $\langle\forall x :: [\langle\exists c :: c = x\rangle]\rangle$.

Finally we recall the definition of f's punctuality:

(4) $[\langle\forall x, y :: x = y \Rightarrow f.x = f.y\rangle]$;

for boolean f, predicate calculus allows us to rewrite (4) as

(5) $[\langle\forall x, y :: x = y \Rightarrow f.x \equiv x = y \Rightarrow f.y\rangle]$.

Just to be on the -very- safe side, we check that a formula universally quantified over x may be instantiated with $x := c$, i.e. we shall prove for non necessarily punctual g

(6) $[\langle\forall x :: g.x\rangle \Rightarrow \langle\forall c :: g.c\rangle]$.

To this end we observe

$$
\begin{array}{ll}
 & \langle\forall c :: g.c\rangle \\
= & \quad \{(1)\} \\
 & \langle\forall c :: \langle\exists x :: [x = c]\rangle \Rightarrow g.c\rangle \\
= & \quad \{\text{predicate calculus}\} \\
 & \langle\forall c :: \langle\forall x :: [x = c] \Rightarrow g.c\rangle\rangle
\end{array}
$$

$$
\begin{array}{ll}
= & \{\text{interchange; Leibniz}\} \\
& \langle \forall x :: \langle \forall c :: [x=c] \Rightarrow g.x \rangle\rangle \\
= & \{\text{predicate calculus}\} \\
& \langle \forall x :: \langle \exists c :: [x=c]\rangle \Rightarrow g.x \rangle \\
\Leftarrow & \{\text{predicate calculus}\} \\
& \langle \forall x :: g.x \rangle
\end{array}
$$

Note The first step is not such a rabbit when we realize (i) that we have to use (1) in a strengthening chain, (ii) that we have to introduce a quantification over x, and (iii) Leibniz is needed to relate $g.c$ to $g.x$ (End of Note.)

The proof of (0) is by a ping-pong argument; pong being the easiest, we do that one first.

Proof of (0), [LHS ⇐ RHS]

$$
\begin{array}{ll}
& [\langle \forall c : c=x : f.c\rangle \Leftarrow f.x] \\
\Leftarrow & \{(6)\} \\
& [\langle \forall y : y=x : f.y\rangle \Leftarrow f.x] \\
= & \{\text{pred. calc.}\} \\
& [\langle \forall y : y=x : f.y \Leftarrow f.x\rangle] \\
\Leftarrow & \{\text{pred. calc.}\} \\
& [\langle \forall y :: y=x \Rightarrow (f.y \equiv f.x)\rangle] \\
= & \{(4),\ f \text{ is punctual}\} \\
& \text{true.}
\end{array}
$$

(End of Proof of (0), [LHS ⇐ RHS].)

We have not made use yet of (3). We are going to do that by showing, in preparation of the proof of ping, that for punctual f

(7) $\qquad [\langle\forall x :: f.x\rangle \equiv \langle\forall c :: f.c\rangle]$.

The proof is remarkably similar to the earlier proof of (6). We observe for punctual f :

$$
\begin{array}{ll}
 & \langle\forall x :: f.x\rangle \\
= & \quad \{(3)\} \\
 & \langle\forall x :: \langle\exists c :: c = x\rangle \Rightarrow f.x\rangle \\
= & \quad \{\text{pred. calc.}\} \\
 & \langle\forall x :: \langle\forall c :: c = x \Rightarrow f.x\rangle\rangle \\
= & \quad \{\text{interchange; (5) \& (6), } f \text{ is punctual}\} \\
 & \langle\forall c :: \langle\forall x :: x = c \Rightarrow f.c\rangle\rangle \\
= & \quad \{\text{pred. calc.}\} \\
 & \langle\forall c :: \langle\exists x :: x = c\rangle \Rightarrow f.c\rangle \\
= & \quad \{(2)\} \\
 & \langle\forall c :: f.c\rangle \quad ,
\end{array}
$$

and after this demonstration of (7), the proof of ping is a walk-over.

<u>Proof of (0), [LHS ⇒ RHS]</u>

We observe for punctual f

$$
\begin{array}{ll}
 & \langle\forall c : c = x : f.c\rangle \\
= & \quad \{(7),\ ? = x \text{ and } f \text{ both punctual}\} \\
 & \langle\forall y : y = x : f.y\rangle
\end{array}
$$

$\Rightarrow$ {instantiation $y := x$}

$x = x \Rightarrow f.x$

$=$ {predicate calculus}

$f.x$

and this concludes the proof of (0).

This proof became longer than I had expected. I don't feel guilty about postulating (1) and (3) here, but it is bad that they don't occur in our book.

[AB36] A. Bijlsma, "A case of context dependence in predicate calculus", September 14, 1993, Technical University Eindhoven

[DS90] Edsger W. Dijkstra & Carel S. Scholten "Predicate Calculus and Program Semantics", Springer-Verlag, 1990

Austin, 22 August 1994

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA