More on monotonic predicate transformers and the introduction of dummies (see EWD1117)

We are interested in predicate transformers g such that for any monotonic predicate transformer f

(0) $$[f.b \equiv \langle \exists x : [g.b.x] : f.x \rangle]$$

Thanks to the 1-point rule, the choice of $b \equiv x$ for $g.b.x$ would do the job, but this choice is too specific for our purposes, as it does the job for any f, monotonic or not. We shall therefore follow the usual route of proving (0), on the way collecting the requirements on g that make the proof work. The proof of (0) is a ping pong argument.

Proof For ping we observe

$$\begin{array}{ll} & \langle \exists x : [g.b.x] : f.x \rangle \\ \Leftarrow & \{\text{instantiation with } x := b\} \\ & [g.b.b] \wedge f.b \\ = & \{(1)\} \\ & f.b \end{array}$$,

where we appealed to

(1) $[g.b.b]$;

note that f's monotonicity has not been used.

For pong we observe for any monotonic f

$$
\begin{array}{ll}
 & [f.b \Leftarrow \langle \exists x : [g.b.x] : f.x \rangle] \\
= & \quad \{\text{pred. calc.}\} \\
 & [\langle \forall x : [g.b.x] : f.b \Leftarrow f.x \rangle] \\
= & \quad \{\text{scalar range}\} \\
 & \langle \forall x : [g.b.x] : [f.b \Leftarrow f.x] \rangle \\
\Leftarrow & \quad \{f \text{ is monotonic}\} \qquad\qquad *) \\
 & \langle \forall x : [g.b.x] : [b \Leftarrow x] \rangle \\
= & \quad \{(2)\} \\
 & true
\end{array}
$$

where we appealed to

(2) $\quad [g.b.x] \Rightarrow [x \Rightarrow b] \quad$ for all x ;

note that we did use the monotonicity of f.

<u>Remark</u> The strengthening in the step marked *) is spurious in the sense that we could have quantified universally over all monotonic f. Leaving that range understood, the step in question would have been

$$
\begin{array}{ll}
 & \langle \forall f :: \langle \forall x : [g.b.x] : [f.b \Leftarrow f.x] \rangle \rangle \\
= & \quad \{\Leftarrow \; f \text{ is monotonic}, \\
 & \quad\; \Rightarrow \text{ instantiation with } f := \text{identity function}\} \\
 & \langle \forall x : [g.b.x] : [b \Leftarrow x] \rangle
\end{array}
$$

(End of Remark.)

(End of Proof.)

Collecting requirements (1) and (2) we see that (0) holds if b is <u>the weakest</u>

<u>solution</u> of the equation $x: [g.b.x]$.

The observation that f's conjugate f^* is as monotonic as f, invites us to substitute f^* for f. More precisely, (0) with $f,g := f^*, \neg h^*$ yields

$$[f^*.b \equiv \langle \exists x: [\neg h^*.b.x] : f^*.x \rangle] \qquad ;$$

the definition of * yields

$$[\neg f.(\neg b) \equiv \langle \exists x: [h.(\neg b).(\neg x)] : \neg f.(\neg x) \rangle] \qquad ,$$

which can be simplified by $b, x := \neg b, \neg x$ to

$$[\neg f.b \equiv \langle \exists x: [h.b.x] : \neg f.x \rangle] \qquad ;$$

now de Morgan yields what we were heading for:

(3) $\quad [f.b \equiv \langle \forall x: [h.b.x] : f.x \rangle]$

holds for monotonic f if b is <u>the strongest solution</u> of the equation $x: [h.b.x]$, the latter condition being captured by

(4) $\quad [h.b.b]$

(5) $\quad [h.b.x] \Rightarrow [b \Rightarrow x] \quad$ for all x .

* * *

(1) and (4) can be reformulated as

(1') $\quad [x \equiv b] \Rightarrow [g.b.x] \quad$ for all x

(4') $\quad [x \equiv b] \Rightarrow [h.b.x] \quad$ for all x .

These formulae tell us that the strongest choices for the ranges in (0) and (3) are both $[x \equiv b]$; the 1-point rules result. More interesting are the weakest possible choices for g and h respectively: (2) and (5) give us those bounds, yielding

(6) $\quad [f.b \equiv \langle \exists x : [x \Rightarrow b] : f.x \rangle]$

(7) $\quad [f.b \equiv \langle \forall x : [b \Rightarrow x] : f.x \rangle]$,

minor generalizations of the 2 formulae given in EWD1117 (where $f.x$ was a boolean scalar).

* * *

This note has been written for the following reasons.

- In EWD1117, nothing was proved.
- I did not know that the one formula was the conjugate of the other.
- I did not know that the ranges in (6) and (7) could be derived as weakest solutions, nor was I aware of the relation with the 1-point rule.
- I would like to point out a special property of formulae (6) and (7) — when universally quantified over b —. We have derived them for monotonic f, but, conversely, their validity implies that f is monotonic, for, <u>independently of f</u>, the right-hand sides are expressions

that monotonically depend on b . I don't know yet of an example where it comes in handy, but (6) and (7) give us the opportunity of incorporating in calculations the monotonicity of functions by the rewriting of subexpressions.

In view of the rising interest in monotonic predicate transformers, the above is definitely something to keep in mind.

Nuenen, 17 December 1992

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