The proof of the pudding

(This note is not self-contained, but a sequel of EWD945; formulae are numbered here starting at (5), the lower numbers referring to EWD945.)

Let S be the strongest solution of

$$X: [X.x.y \equiv p.x.y \vee (\underline{E}w : X.x.w \wedge X.w.y)] \qquad (5)$$

As before we have

$$[S'.x.y \Leftarrow p.x.y \vee (\underline{E}w : S'.x.w \wedge S'.w.y)]$$
$$\Rightarrow [S.x.y \Rightarrow S'.x.y] \qquad (6)$$

We then have $[Q.x.y \equiv S.x.y]$ (7)

Note A proof of (7) is, for reasons of symmetry, also a proof of

$$[R.x.y \equiv S.x.y] \qquad (8)$$

and, hence an alternative proof of the theorem of EWD945. (End of Note).

Let us proceed as before.

$[Q.x.y \Rightarrow S.x.y]$

$\Leftarrow$ { $Q' := S$ in (3)}

$[S.x.y \Leftarrow p.x.y \vee (\underline{E}z :: p.x.z \wedge S.z.y)]$

$\Leftarrow$ { since S solves (5): $[S.x.z \Leftarrow p.x.z]$

$[S.x.y \Leftarrow p.x.y \vee (\underline{E}z :: S.x.z \wedge S.z.y)]$

$=$ { since S solves (5)}

true .

Here, a little theorem is trying to get out; see below

$$[Q.x.y \Leftarrow S.x.y]$$
$$\Leftarrow \quad \{ S' := Q \ \text{ in } (6) \}$$
$$[Q.x.y \Leftarrow p.x.y \vee (\underline{E}w : Q.x.w \wedge Q.w.y)]$$
$$= \quad \{ \text{since } Q \text{ solves } (0) : [Q.x.y \Leftarrow p.x.y] \}$$
$$[Q.x.y \Leftarrow (\underline{E}w : Q.x.w \wedge Q.w.y)]$$
$$= \quad \{ \text{predicate calculus} \}$$
$$[Q.x.y \Leftarrow Q.x.w \wedge Q.w.y]$$
$$= \quad \{ \text{predicate calculus} \} \qquad\qquad *)$$
$$[Q.x.w \Rightarrow Q.x.y \vee \neg Q.w.y]$$
$$= \quad \{ \text{renaming the dummies: } w,y := y,w \}$$
$$[Q.x.y \Rightarrow Q.x.w \vee \neg Q.y.w]$$
$$\Leftarrow \quad \{ Q'.x.y := Q.x.w \vee \neg Q.y.w \ \text{ in } (3) \}$$
$$[Q.x.w \vee \neg Q.y.w \Leftarrow$$
$$p.x.y \vee (\underline{E}z :: p.x.z \wedge (Q.z.w \vee \neg Q.y.w))]$$
$$\Leftarrow \quad \{ \text{predicate calculus} \}$$
$$[Q.x.w \Leftarrow p.x.y \wedge Q.y.w \vee (\underline{E}z :: p.x.z \wedge Q.z.w)]$$
$$= \quad \{ \text{predicate calculus} \}$$
$$[Q.x.w \Leftarrow (\underline{E}z :: p.x.z \wedge Q.z.w)]$$
$$= \quad \{ Q \text{ solves } (0) \}$$
$$\text{true}$$

(End of Proof.)

The moral of the above is that, instead of proving the mutual implications of Q and R directly —as I did in EWD945— I should have proved their equivalence with S, as done here. (Before starting on EWD945, I considered the introduction of S, but preferred the symmetric proof obligation to start with, so as to reduce the amount of work.)

The title of this note was chosen as soon as I had decided to write it without any prior exploration, just to check whether my heuristics would work again. They did! (In the first proof, on EWD946-0, I had introduced the superfluous step of removing the conjunct $p.x.y$ from the right-hand side, mechanically copying what I had done in EWD945. This superfluous step has been removed with the aid of glue and scissors.)

The step, marked *) contains a choice. Why not

$$[Q.w.y \Rightarrow Q.x.y \vee \neg Q.x.w] \qquad ?$$

Well, that is because we are heading for an application of (3). In the case of R, the other choice should have been made.

*
* *

Equation (0) can be obtained by replacing in the right-hand side of (5) one of the occurrences of the unknown by a lower bound of the right-hand side —viz. X by p —. This transformation can only strengthen the strongest solution, as shown below.

<u>The little theorem</u> Let k and f be monotonic functions of their arguments and such that

$$(\underline{A}X:: [k.X \Rightarrow f.X.X]) \quad ; \qquad (9)$$

let S be the strongest solution of

$$X: [f.X.X \equiv X] \quad ; \qquad (10)$$

let Q be the strongest solution of

$$X: [f.X.(k.X) \equiv X] \quad . \qquad (11)$$

Then $\quad [Q \Rightarrow S] \quad .$

Little proof.

$$
\begin{array}{ll}
 & [Q \Rrightarrow S] \\
\Leftarrow & \{\text{def. of } Q \text{ by (11)}\} \\
 & [f.S.(k.S) \Rrightarrow S] \\
= & \{S \text{ solves (10)}\} \\
 & [f.S.(k.S) \Rrightarrow f.S.S] \\
\Leftarrow & \{f \text{ is monotonic in 2}^{\text{nd}} \text{ argument}\} \\
 & [k.S \Rrightarrow S] \\
= & \{S \text{ solves (10)}\} \\
 & [k.S \Rrightarrow f.S.S] \\
\Leftarrow & \{\text{instantion of (9): } x := S\} \\
 & \text{true} \ .
\end{array}
$$

(End of Little proof.)

Remark For the sake of the above proof I could have defined S as any solution of

$$X : [f.X.X \Rrightarrow X] \quad ,$$

but this I did not know beforehand, hence (10). (End of Remark.)

Deriving proofs like in this note gets more and more the flavour of "turning the handle": an appropriate choice of identifier becomes one of the major decisions.

Austin, 4 November 1985

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