A sequel to EWD822

by Edsger W. Dijkstra and C.S. Scholten

In EWD822 it was boldly stated that wp(S,?) is infinitely conjunctive. Neither there, nor in "A Discipline of Programming" this has been proved. It follows from our exercises with wlp in EWD816; the purpose of this note is to explore more direct proofs. Out of methodological interest we investigated what a proof looks like if wp(DO,R) is defined as the strongest solution of

(0) $X: [X = (\neg B \vee wp(S,X)) \wedge (B \vee R)]$.

In our exploration we shall not require wp(S,?) in (0) to be or-continuous; as a result, our conclusions will also have a bearing on the case of unbounded nondeterminacy. We shall, however, use that wp(S,?) is infinitely conjunctive.

To begin with, we observe that (0) is of the form

(1) $X: [X = b\,X\,R]$

in which b is "infinitely doubly conjunctive", i.e. satisfies

(2) $[b\,(\underline{A}i :: X.i)(\underline{A}i :: Y.i) = (\underline{A}i :: b\,(X.i)(Y.i))]$
for all predicate sequences (X.i) and (Y.i) $(i \geq 0)$.

This is a consequence of the general formula

(3) $[(\underline{A}i :: (\neg B \vee X.i) \wedge (B \vee Y.i)) =$
$(\neg B \vee (\underline{A}i :: X.i)) \wedge (B \vee (\underline{A}i :: Y.i))]$

and the fact that wp(S,?) is infinitely conjunctive. From its being infinitely doubly conjunctive it follows that b is infinitely conjunctive, and hence conjunctive and monotonic, in both its arguments. Another consequence is

(4) $[P \Rightarrow Q] \Rightarrow [\, b\,(X \wedge Y)\,P = b\,X\,P \wedge b\,Y\,Q\,]$.

Our target is now to prove Lemma 0, which expresses the infinite conjunctivity of wp(DO,R) defined as strongest solution of (0).

Lemma 0. Let the (two-argument) predicate transformer b be infinitely doubly conjunctive. Let $R.i$ $(i \geq 0)$ be an infinite sequence of predicates. Let P be the strongest solution of

(5) $X: [\, b\,X\,(\underline{A}\, i :: R.i) = X\,]$;

let $Q.j$ $(j \geq 0)$ be the strongest solution of

(6) $X: [\, b\,X\,(R.j) = X\,]$.

Then $[P = (\underline{A}\, j :: Q.j)]$.

Proof. Since b is monotonic in its first argument —see EWD822—, P is also the strongest solution of

(5') $X: [\, b\,X\,(\underline{A}\, i :: R.i) \Rightarrow X\,]$.

Similarly, $Q.j$ is also the strongest solution of

(6') $X: [\, b\,X\,(R.j) \Rightarrow X\,]$.

Apparently unavoidably, the proof consists of two parts: we have to show that $(\underline{A}j :: Qj)$ is a solution of (5) -or (5')- and that it is its strongest one; we have chosen (5').

The first part is straightforward: we have for any Z

$$
\begin{array}{ll}
 & [Z = b\ (\underline{A}j :: Qj)\ (\underline{A}i :: Ri)] \\
= & \{\ b \text{ is infinitely doubly conjunctive}\ \} \\
 & [Z = (\underline{A}j :: b\ (Qj)\ (Rj))] \\
\Rightarrow & \{(6')\} \\
 & [Z \Rightarrow (\underline{A}j :: Qj)]
\end{array}
$$

Hence $(\underline{A}j :: Qj)$ is a solution of (5'); P being its strongest solution, we have proved $[P \Rightarrow (\underline{A}j :: Qj)]$.

Note. In the above appeal to (6') we have only used that Qj is a solution of (6'). (End of Note.)

The difficulty of the second part, viz. the proof of $[(\underline{A}j :: Qj) \Rightarrow P]$, is the exploitation of the fact that the Qj are the strongest solutions of (6) and (6'). To this end we observe first

$$
\begin{array}{ll}
 & [(\underline{A}i :: Qi) \Rightarrow P] \\
= & \{\ \text{predicate calculus, for some chosen } j\ \} \\
 & [Qj \wedge (\underline{A}i :: Qi) \Rightarrow P] \\
= & \{\ \text{definition of implication and de Morgan}\ \} \\
 & [Qj \Rightarrow (\underline{E}i :: \neg Qi) \vee P] \quad ;
\end{array}
$$

Qj being defined as the strongest solution of (6'), the last line can be proved by showing that $(\underline{E}i :: \neg Qi) \vee P$ is a solution of (6').

$$
\begin{array}{ll}
 & \text{true} \\
= & \{\text{predicate calculus}\} \\
 & [(\underline{A}i::Qi)\wedge P \Rightarrow P] \\
\Rightarrow & \{b \text{ is monotonic in its first argument}\} \\
 & [\,b\,((\underline{A}i::Qi)\wedge P)\,(\underline{A}i::Ri) \Rightarrow b\,P\,(\underline{A}i::Ri)] \\
\Rightarrow & \{P \text{ is a solution of } (5')\} \\
 & [b\,((\underline{A}i::Qi)\wedge P)\,(\underline{A}i::Ri) \Rightarrow P] \\
= & \{\text{predicate calculus}\} \\
 & [b\,(((\underline{E}i::\neg Qi)\vee P)\wedge(\underline{A}i::Qi))\,(\underline{A}i::Ri) \Rightarrow P] \\
= & \{(4), \text{ since for some chosen } j\ \ [(\underline{A}i::Ri)\Rightarrow Rj]\} \\
 & [b\,((\underline{E}i::\neg Qi)\vee P)\,(Rj)\wedge b\,(\underline{A}i::Qi)(\underline{A}i::Ri) \Rightarrow P] \\
= & \{b \text{ is infinitely doubly conjunctive}\} \\
 & [b\,((\underline{E}i::\neg Qi)\vee P)(Rj)\wedge(\underline{A}i::b\,(Qi)(Ri)) \Rightarrow P] \\
= & \{Q\text{'s are solutions of } (6)\} \\
 & [b\,((\underline{E}i::\neg Qi)\vee P)(Rj)\wedge(\underline{A}i::Qi) \Rightarrow P] \\
= & \{\text{definition of implication and de Morgan}\} \\
 & [b\,((\underline{E}i::\neg Qi)\vee P)(Rj) \Rightarrow (\underline{E}i::\neg Qi)\vee P]
\end{array}
$$

Note From the above proof it follows that for $[(\underline{A}i::Qi)=P]$ to hold, only one of the Qi – viz. Qj – needs to be the strongest solution of (6), while for the others it suffices to be a solution of (6). (End of Note.)
(End of Proof.)

* * *

Perhaps a much simpler proof exists; if so, we were so far unable to construct it. The above proof leaves us with mixed feelings. That, suddenly, implications pop up all over the pages was only to be expected. But though its individual steps are simple, we take no offence when the last part is characterized as a piece of tricky shunting. It is really not nice; note, for instance, that on the one hand we use that Qj is the strongest solution

of (6') – and we had to, since we could not prevent the implications from creeping in – while at the very end it is essential that the Q's are solutions of the "stronger" equation (6). In short: without the bit of theory developed in EWD822, this proof would have been impossible.

* * *

We can somewhat simplify the proof of Lemma 0 by essentially concentrating the "tricky shunting" in the proof of Lemma 1. The (two-argument) predicate transformer b is "doubly conjunctive" means

$$[\, b\,(X \wedge X')\,(R \wedge R') = b\,X\,R \wedge b\,X'\,R' \,] \quad \text{for any } X, X', R, R'.$$

Lemma 1. Let b be a doubly conjunctive predicate transformer. Let P be the strongest solution of

$$(7) \qquad X : [\, b\,X\,R = X \,] \quad ;$$

let Q be a solution of (7); let H be the strongest solution of

$$(8) \qquad X : [\, b\,X\,T = X \,] \quad .$$

Then $[\, P = Q \wedge H \,]$

Proof. We first show $[\, P \Rightarrow Q \wedge H \,]$ by demonstrating that $Q \wedge H$ is a solution of (7). We have for any Z

$$\begin{aligned}
& [\, Z = b\,(Q \wedge H)\,R \,] \\
= \; & \{\, b \text{ is doubly conjunctive} \,\} \\
& [\, Z = b\,Q\,R \wedge b\,H\,T \,] \\
= \; & \{\, Q \text{ and } H \text{ are solutions of (7) and (8) respectively} \,\} \\
& [\, Z = Q \wedge H \,]
\end{aligned}$$

We now show $[Q \wedge H \Rightarrow P]$, i.e. $[H \Rightarrow P \vee \neg Q]$ by showing that $P \vee \neg Q$ is a solution of $X : [b\,X\,T \Rightarrow X]$, of which H is the strongest solution.

$$
\begin{array}{ll}
 & \text{true} \\
= & [\,b\,(P \wedge Q)\,R = b\,(P \wedge Q)\,R\,] \\
= & \{\text{predicate calculus}\} \\
 & [\,b\,((P \vee \neg Q) \wedge Q)\,R = b\,(P \wedge Q)\,R\,] \\
= & \{b \text{ is doubly conjunctive}\} \\
 & [\,b\,(P \vee \neg Q)\,T \wedge b\,Q\,R = b\,P\,R \wedge b\,Q\,R\,] \\
= & \{P \text{ and } Q \text{ are solutions of (7)}\} \\
 & [\,b\,(P \vee \neg Q)\,T \wedge Q = P \wedge Q\,] \\
\Rightarrow & \{\text{predicate calculus}\} \\
 & [\,b\,(P \vee \neg Q)\,T \Rightarrow P \vee \neg Q\,]
\end{array}
$$

(End of Proof.)

Lemma 0 is now easily proved: straightforward substitution shows that the infinite conjunction of arbitrary solutions Q'_j of (6) is a solution P' of (5), i.e. $[P' = (\underset{j}{A} :: Q'_j)]$. Taking at both sides the conjunction with H then yields Lemma 0.

In this last version, the meaning of the adjective "strongest" is only used in the proof of Lemma 1. From then onwards we only use the equality expressed by Lemma 1. We expect this to be the case in very many proofs; it is very much like separating a proof of total correctness in a proof of partial correctness and a proof of termination: the H of Lemma 1 plays the rôle of $wp\,(DO, T)$.

9 May 1982

drs. C.S. Scholten
Scientific Adviser
Philips Research Laboratories
5600 MD EINDHOVEN
The Netherlands

prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow
Plataanstraat 5
5671 AL NUENEN
The Netherlands