A theorem of Scholten's once more (see EWD1048)

The other week I stumbled across EWD1048, which records how the ATAC had proved a theorem of Carel Scholten's. Seeing the theorem and its proof I felt that we should now be able to design a much simpler proof, and that is what the ETAC did on 1992.08.18 .

To begin with, we reformulated the theorem, introducing as many implications as possible so as to ease monotonicity considerations.

Let p and q satisfy

(0) $[p.X \Rightarrow Y] \equiv [X \Rightarrow q.Y]$ for all X, Y.

<u>Note</u> The original theorem formulated the relation between p's conjugate and q, and instead of the implications in (0), it had disjunctions. With Galois connections en vogue as they are, formulation (0) now seems preferable. (End of Note.)

Let $h.X$ be the strongest solution of

$$Y: [X \vee p.Y \Rightarrow Y]$$

Because it follows from (0) that p is monotonic, this strongest solution exists.

<u>Note</u> In the original theorem, the equation had

an $\equiv$ where our equation has an $\Rightarrow$. Knaster-Tarski tells us that the two equations have the same strongest solution. (End of Note.)

In formula, we know that $h.X$ implies all solutions, i.e. —with some predicate calculus—

(1) $\quad [X \Rightarrow Y] \wedge [p.Y \Rightarrow Y] \;\Rightarrow\; [h.X \Rightarrow Y]$
for all X, Y

and that $h.X$ is a solution, i.e.

(2a) $\quad [X \Rightarrow h.X] \qquad$ for all X
(2b) $\quad [p.(h.X) \Rightarrow h.X] \qquad$ for all X .

Let $k.X$ be the weakest solution of

$$Y: [Y \Rightarrow X \wedge q.Y]$$

i.e. (similarly)

(3) $\quad [Y \Rightarrow X] \wedge [Y \Rightarrow q.Y] \;\Rightarrow\; [Y \Rightarrow k.X]$
for all X, Y

(4a) $\quad [k.X \Rightarrow X] \qquad$ for all X
(4b) $\quad [k.X \Rightarrow q.(k.X)] \qquad$ for all X .

Then

(5) $\quad [h.A \Rightarrow B] \;\equiv\; [A \Rightarrow k.B] \quad$ for all A, B .

<u>Proof</u> We show LHS $\Rightarrow$ RHS: we observe for any A, B

$$
\begin{array}{ll}
 & [A \Rightarrow k.B] \\
\Leftarrow & \{ (2a) \text{ with } X := h.A \} \\
 & [h.A \Rightarrow k.B] \\
\Leftarrow & \{ (3) \text{ with } X, Y := B, h.A \} \\
 & [h.A \Rightarrow B] \wedge [h.A \Rightarrow q.(h.A)] \\
\Leftarrow & \{ (0)\Rightarrow, \text{ with } X, Y := h.A, h.A \} \\
 & [h.A \Rightarrow B] \wedge [p.(h.A) \Rightarrow h.A] \\
= & \{ (2b) \text{ with } X := A \} \\
 & [h.A \Rightarrow B] \quad .
\end{array}
$$

The proof LHS $\Leftarrow$ RHS uses similarly $(0)\Leftarrow$, (1), (4a) and (4b).

(End of Proof.)

* * *

This is a very satisfactory proof: the complete proof consists of 8 steps, each of them using 1 of the 8 independent givens, each of which is therefore appealed to once. (In the original EWD1048 version it was clearer that $8 = 4+4$: the symmetry between $\Rightarrow$ and $\Leftarrow$ was more obvious.)

In the above, we have constructed a strengthening chain in which k is eliminated —via (3)— and h is introduced —via (2a)— , but please note the order! In (3), the consequent is an (anti)monotonic function of Y , while the antecedent is <u>not</u>. When you start your proof with

$$[A \Rightarrow k.B]$$
$$\Leftarrow \quad \{(3) \text{ with } X,Y := B,A\}$$
$$[A \Rightarrow B] \wedge [A \Rightarrow q.A]$$

you can continue strengthening by weaking the antecedents with (2a):

$$\Leftarrow \quad \{(2a) \text{ with } X := h.A\}$$
$$[h.A \Rightarrow B] \wedge [h.A \Rightarrow q.A]$$

but now you are stuck because (the consequent in) the second conjunct is too strong, and there is no nonweakening way of transforming $q.A$ into $q.(h.A)$.

The moral of the story is: when appealing to the extremal property — in this example (1) or (3) —, be aware of the loss of (anti)monotonicity — here in Y — when going from consequent to antecedent.

Austin, 29 August 1992

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