Guided by necessity

It is our purpose to prove for a non-empty set W of predicates

(0) $$[(\underline{A}X: X \in W: X) \Rightarrow (\underline{E}Y: Y \in W: Y)] \ .$$

The restriction to non-empty W is essential, for with $W := \emptyset$, (0) reduces to $[\text{true} \Rightarrow \text{false}]$, which is false. Our demonstration of (0) therefore has to use the fact that W is non-empty, more precisely, has to contain a valid step that would be invalid for empty W. Well-known steps only valid for non-empty W are the restricted distributions

(1) $$[Q \wedge (\underline{A}X: X \in W: X) \equiv (\underline{A}X: X \in W: Q \wedge X)]$$

(2) $$[Q \vee (\underline{E}Y: Y \in W: Y) \equiv (\underline{E}Y: Y \in W: Q \vee Y)] \ ,$$

and we propose to use (at least) one of the above two to demonstrate (0) in the form

(3) $$[(\underline{A}X: X \in W: X) \vee (\underline{E}Y: Y \in W: Y) \equiv (\underline{E}Y: Y \in W: Y)] \ .$$

To this end we observe for any non-empty W

$$\begin{aligned} & (\underline{A}X: X \in W: X) \vee (\underline{E}Y: Y \in W: Y) \\ = & \quad \{ (2) \text{ with } Q := (\underline{A}X: X \in W: X) \text{ and } W \text{ non-empty} \} \\ & (\underline{E}Y: Y \in W: (\underline{A}X: X \in W: X) \vee Y) \\ = & \quad \{ \text{instantiation} \} \\ & (\underline{E}Y: Y \in W: Y) \ . \end{aligned}$$

The above proof is correct, but there is a little bit more to it. When we rewrite (1) and (2) as mutual implications we see that in both cases one of the two implications also holds for empty W, and our proof has to use one of the others: for non-empty W

(4) $[Q \wedge (\underline{A}X: X \in W: X) \Leftarrow (\underline{A}X: X \in W: Q \wedge X)]$

(5) $[Q \vee (\underline{E}Y: Y \in W: Y) \Rightarrow (\underline{E}Y: Y \in W: Q \vee Y)]$.

We have to use one of these, for (4) and (5) are the ones that are invalid for empty W.

This immediately raises the question of whether our proof of (3) —phrased in terms of equivalences— can be viewed as a strengthening chain or a weakening one. Our demonstrandum (3) is of the form $[P \vee Q \equiv Q]$; since $[P \vee Q \Leftarrow Q]$ follows from predicate calculus, our obligation is to show $[P \vee Q \Rightarrow Q]$. Since our proof of (3) starts at the left-hand side, it is therefore "really" a weakening chain. But that tells us that we can use (4) only to take a Q outside a universal quantification, and (5) only to bring a Q inside an existential one. And, indeed, the latter "weakening" step is in essence the first step of our proof of (3).

* * *

There was something remarkable going on in the above. Under the condition $\neg(W=\emptyset)$, our proof obligation was of the form

(6) $\quad [P \Rightarrow Q]$;

we rewrote that as $[P \vee Q \equiv Q]$ to eliminate the implication, and immediately reintroduced it again by writing our proof obligation as

(7) $\quad [P \vee Q \Rightarrow Q]$!

Since in the transition from (6) to (7) we have weakened the antecedent, it looks as if we have formally made things harder, but this is not the case: from a weakening chain from P to Q, we can construct a weakening chain from $P \vee Q$ to $Q \vee Q$ and, thanks to the idempotence of $\vee$, also one from $P \vee Q$ to Q. What the transition from (6) to (7) bought us, is that with (7) we have a clearly "more complicated side" to start with, which gives us more manipulative opportunities and hints.

(The alternative is to rewrite (6) as

(8) $\quad [P \wedge Q \Leftarrow P]$

and to transform $P \wedge Q$ via a strengthening chain into P.)

* * *

I do not exclude that on closer scruting we decide that the use of $\Rightarrow$ and $\Leftarrow$ in the data (4) and (5) and in the demonstranda (7) and (8) are to be considered as a misuse of notation. We could conclude that what we really would like to have is some sort of directed equivalence, say an equivalence between terms such that the implication in the one direction is a tautology.

Austin, 25 March 1991

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