Two proofs to remember (for our files)

At the ETAC's session of January 2, 1990, Edsger W. Dijkstra showed us two proofs that are so typical - and so beautiful - that we should not forget them. They are of a type that some of us may have seen before, but we never took the trouble to focus on them explicitly. Hence this note.

Theorem 0

Predicate transformers f and g satisfying

(0) $[f.X \vee Y] \equiv [X \vee g.Y]$ for all X, Y,

are universally conjunctive.

Proof

Predicate transformer f is universally conjunctive means

(1) $[\ f.(\underline{A}X :: X) \equiv (\underline{A}X :: f.X)\ ]$,

for whatever range of the quantification. So (1) is our demonstrandum.

It has the shape $[A \equiv B]$, and more specifically, A has the shape f.C. Premise (0) tells us how to manipulate expressions of the form $[f.X \vee Y]$. The question then becomes whether we can reformulate $[A \equiv B]$ into an expression containing $[A \vee Y]$ as a subexpression. Here we apply a trick that, when encountered for the first time, comes as a big surprise

but deserves to be raised to the level of standard methods (by virtue of its simplicity and potential effectiveness). The trick is to apply rewrite rule

(2) $\quad [A \equiv B] \equiv (\underline{A}Y :: [A \vee Y] \equiv [B \vee Y])$, for all A, B .

which allows us to show $[A \equiv B]$ by showing that for any Y . $[A \vee Y] \equiv [B \vee Y]$.

For our current example we can therefore proceed as follows. For any Y we observe

$[f.(\underline{A}X :: X) \vee Y]$

= { the only thing we can do is to apply (0) }

$[(\underline{A}X :: X) \vee g.Y]$

= { we introduced an occurrence of g which, sooner or later, has to disappear again, by a next application of (0) . But we don't want to undo the first step. Fortunately there is one more manipulative possibility, by using that $\vee$ distributes over $\underline{A}$. }

$[(\underline{A}X :: X \vee g.Y)]$

= { the term is almost the right-hand side of (0), except the square brackets are missing. Fortunately there is one more manipulative possibility, viz. by using that $[\,]$ distributes over $\underline{A}$. }

$(\underline{A}X :: [X \vee g.Y])$

= { now we use (0), which we had to use a second time }

$$
\begin{array}{ll}
 & (\underline{A}X :: [\, f.X \;\vee\; Y \,]\,) \\
= & \quad \{ \text{ now that (0) has done its work, the rest of the calculation merely undoes the part of the above manipulations not pertaining to (0) } \} \\
 & [\,(\underline{A}X :: f.X \;\vee\; Y\,)\,] \\
= & \quad \{\} \\
 & [\,(\underline{A}X :: f.X) \;\vee\; Y\,]\,,
\end{array}
$$

and this is it.

(End of Proof of Theorem 0.)

The reason that in the above calculation the hints are recorded so lavishly is to indicate that, once the decision to use (2) has been taken, the rest of the proof is really of the type "there is only one thing that you can reasonably do". The same holds for the proof of

Theorem 1

Predicate transformer $\hookrightarrow$ (denoted as prefix operator) satisfying (3a) and (3b)

(3a) $[\, X \Leftarrow \hookrightarrow Y \,] \equiv [\, Y \Leftarrow \hookrightarrow X \,]$ for all X, Y,

(3b) $[\, X \Rightarrow \hookrightarrow Y \,] \equiv [\, Y \Rightarrow \hookrightarrow X \,]$ for all X, Y,

also satisfies the "Laws of de Morgan", i.e.

(4a) $[\, \hookrightarrow (\underline{A}X :: X) \;\equiv\; (\underline{E}X :: \hookrightarrow X)\,]$ and

(4b) $[\, \hookrightarrow (\underline{E}X :: X) \;\equiv\; (\underline{A}X :: \hookrightarrow X)\,]$.

Proof

In showing the equivalences (4a) and (4b) we use a trick similar to the one in the proof of Theorem 0, this time by applying

one of the rewrite rules

(5a) $[A \equiv B] \equiv (\underline{A}\, Y :: [Y \Leftarrow A] \equiv [Y \Leftarrow B])$

(5b) $[A \equiv B] \equiv (\underline{A}\, Y :: [Y \Rightarrow A] \equiv [Y \Rightarrow B])$,

for all A, B.

(Note that (5a) and (5b) are just different renderings of (2): (2) with $A, B := \neg A, \neg B$ yields (5a) and (2) with dummy transformation $Y := \neg Y$ yields (5b). Renderings (5a) and (5b) have been chosen because their shapes match premises (3a) and (3b) more directly.)

Now the question arises which of the two rules (5a) or (5b) to use in proving, say, (4b) – if the choice matters at all –. Expression A has the shape $\circlearrowleft C$ and premises (3a) and (3b) tell us how to manipulate $[Y \Leftarrow \circlearrowleft C]$ and $[Y \Rightarrow \circlearrowleft C]$. So the macroscopic structure of A offers no clue, at the outset. Perhaps B's does. Expression B is a universal quantification, and now we see that $[Y \Leftarrow B]$, as occurring in (5a), is nearly hopeless, whereas $[Y \Rightarrow B]$ is not. Thus the choice to prove (4b) by using (5b) is almost forced. The ensuing calculation offers no further surprises.

We observe that for any Y.

$$
\begin{array}{ll}
 & [\, Y \Rightarrow \sim (\underline{E}X :: X)\,] \\
= & \quad \{ (3b) \} \\
 & [\, (\underline{E}X :: X) \Rightarrow \sim Y\,] \\
= & \quad \{ \text{pred. calc.} \} \\
 & [\, (\underline{A}X :: X \Rightarrow \sim Y)\,] \\
= & \quad \{ \text{pred. calc.} \} \\
 & (\underline{A}X :: [\, X \Rightarrow \sim Y\,]\,) \\
= & \quad \{ (3b) \} \\
 & (\underline{A}X :: [\, Y \Rightarrow \sim X\,]\,) \\
= & \quad \{ \text{pred. calc.} \} \\
 & [\, (\underline{A}X :: Y \Rightarrow \sim X)\,] \\
= & \quad \{ \text{pred. calc.} \} \\
 & [\, Y \Rightarrow (\underline{A}X :: \sim X)\,] \; .
\end{array}
$$

(End of Proof of Theorem 1.)

* * *

So much for the two beautiful proofs. A more precise investigation of the rôles played by rules like (2), (5a), and (5b) will (have to) be the subject of a different note, so that what we now called a trick will emerge as a conscious design decision tomorrow.

W.H.J. Feijen

Sterksel, 4 January 1990.