Perry Moerland's proof of Carel Scholten's theorem

At the last session of the ETAC, Perry Moerland showed a proof of a conjecture of Carel Scholten's (which neither Carel nor I had been able to prove). Perry's proof, which is very short, deserves recording because it has a few nice features.

About predicate transformers f and g we are given

(0) f is monotonic

(1) $f \circ g$ is the identity function

(2) $g \circ f$ is the identity function ,

and we have to prove

(3) g is monotonic.

* * *

A few naive efforts suggest that the theorem would not hold for monotonicity with respect to an arbitrary partial order and that we have to take some special properties of the implication into account, such as its relation to the negation. One way of introducing the negation is by shunting, another one is by considering the conjugates — $[f^{*}.X \equiv \neg f.(\neg X)]$, etc. — .

We choose the latter, inspired by

(i) what is given about the pair f, g , also holds for the pair f^*, g^* , and

(ii) the conjugate allows us to rephrase (3) as

(3') $\quad [X \vee Y] \Rightarrow [g^*.X \vee g.Y]$ for all X, Y .

For the first bold step, it helps to remember the Mother of All Inference Rules

(4) $\quad [P \vee Q] \wedge [R \vee S] \Rightarrow$
$\quad [P \vee (Q \wedge R) \vee S]$,

which is used to introduce into the consequent of (3') the term $g.X$ — alternatively we could have introduced the other "in between term" $g^*.Y$ — :

$[g^*.X \vee g.Y]$
$=$ {predicate calculus}
$[g^*.X \vee (\neg g.X \wedge g.X) \vee g.Y]$
$=$ { def. of conjugate}
$[g^*.X \vee (g^*.(\neg X) \wedge g.X) \vee g.Y]$
$\Leftarrow$ { (4)}
$[g^*.X \vee g^*.(\neg X)] \wedge [g.X \vee g.Y]$
$\Leftarrow$ {Lemma 0, twice}
$[X \vee \neg X] \wedge [X \vee Y]$
$=$ {predicate calculus}
$[X \vee Y]$

where we used

<u>Lemma 0</u> For all X, Y

$$[X \vee Y] \Rightarrow [g.X \vee g.Y] \qquad \text{and}$$

$$[X \vee Y] \Rightarrow [g^*.X \vee g^*.Y]$$

<u>Proof</u> We only prove the first implication

$[g.X \vee g.Y]$
$\Leftarrow$ {Lemma 1 with $X := g.X \vee g.Y$}
$[f.(g.X \vee g.Y)]$
$\Leftarrow$ {(0), i.e. f is monotonic}
$[f.(g.X) \vee f.(g.Y)]$
$=$ {(1), i.e. $f \circ g$ is identity function}
$[X \vee Y]$

(End of Proof)

After the appeal to (4), the emergence of Lemma 0 is not too surprising, for it is just what we need. The same holds for the emergence of Lemma 1 in the last proof above; it is just what we need for we need to eliminate g-applications in a strengthening chain, and g can be eliminated by applying f to it.

<u>Lemma 1</u> For all X: $[f.X] \Rightarrow [X]$ and

$[f^*.X] \Rightarrow [X]$

<u>Proof</u> Again, we only prove the first implication. This little proof, I think, is surprising. In a weakening chain we have to eliminate f;

(2) not having been used yet, g-application is the appropriate mechanism for the elimination of f. So little being known about g, Leibniz's Principle has to justify the weakening in the step where g is applied. This application is surrounded by introduction and removal of ≡ . We observe for any X:

$$
\begin{array}{ll}
 & [f.X] \\
\Rightarrow & \quad \{\text{predicate calculus}\} \\
 & [f.true \Rightarrow f.X] \\
= & \quad \{f \text{ monotonic, i.e. } [f.true \Leftarrow f.X]\} \\
 & [f.true \equiv f.X] \\
\Rightarrow & \quad \{\text{Leibniz}\} \\
 & [g.(f.true) \equiv g.(f.X)] \\
= & \quad \{(2)\text{, i.e. } g\circ f \text{ is identity}\} \\
 & [true \equiv X] \\
= & \quad \{\text{predicate calculus}\} \\
 & [X] \quad .
\end{array}
$$

(End of Proof)

This last proof is something to remember. (A short proof of the whole theorem has been published by J.C.S.P. van der Woude in "C.S. Scholten Dedicata".)

Nuenen, 27 December 1992

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