ATAC's proof of Scholten's theorem

In a recent letter, W.H.J. Fegen wrote me that C.S. Scholten had offered the following theorem to the ETAC.

(0) Let predicate transformers p and q satisfy

$$[p.X \vee Y] \equiv [X \vee q.Y] \quad \text{for all } X, Y \quad ;$$

(1) let, for all X, $h.X$ be the weakest solution of

$$Y: [Y \equiv X \wedge p.Y] \quad ;$$

(2) let, for all X, $k.X$ be the weakest solution of

$$Y: [Y \equiv X \wedge q.Y] \quad .$$

Then predicate transformers h and k satisfy

(3) $[h.A \vee B] \equiv [A \vee k.B]$ for all A, B .

This note records the proof that the ATAC designed on its session of 28 March 1989. We first give the three crucial lemmata, postponing their discussion until later.

From (0) one can conclude

Lemma 0 Predicate transformers p, q are universally conjunctive

and the generalization of (0)

Lemma 1 $(\underline{A}n: 0 \leq n: [p^n.X \vee Y] \equiv [X \vee q^n.Y])$ for all X,Y .

From Lemma 0 follows the monotonicity of p,q and hence, on account of Knaster-Tarski, the existence of h and k . From Lemma 0 follows the *and*-continuity of the right-hand sides of (1) and (2), which leads to

Lemma 2 For all X

$[h.X \equiv (\underline{A}n : 0 \leq n : p^n.X)]$ and, similarly,

$[k.X \equiv (\underline{A}n : 0 \leq n : q^n.X)]$.

Proof of (3) We observe for any A,B

$$
\begin{array}{ll}
 & [h.A \vee B] \\
= & \quad \{\text{Lemma 2}\} \\
 & [(\underline{A}n :: p^n.A) \vee B] \\
= & \quad \{\vee \text{ over } \underline{A}\} \\
 & [(\underline{A}n :: p^n.A \vee B)] \\
= & \quad \{\text{interchange}\} \\
 & (\underline{A}n :: [p^n.A \vee B]) \\
= & \quad \{\text{Lemma 2}\} \\
 & (\underline{A}n :: [A \vee q^n.B]) \\
= & \quad \{\text{interchange}\} \\
 & [(\underline{A}n :: A \vee q^n.B)] \\
= & \quad \{\vee \text{ over } \underline{A}\} \\
 & [A \vee (\underline{A}n :: q^n.B)] \\
= & \quad \{\text{Lemma 2}\} \\
 & [A \vee k.B] \quad .
\end{array}
$$

(End of Proof of (3).)

We shall not repeat here the proof of Lemma 0, which we have given many times; we only recall that, like the proof of (3), it relies on the distribution of $\vee$ over $\underline{A}$ and the interchange of "everywhere" with universal quantification.

<u>Proof of Lemma 1</u> . By induction over n .

We observe that for $n = 0$ -and for $n = 1$!-

(4) $\quad [p^n.X \vee Y] \equiv [X \vee q^n.Y] \quad$ for all X, Y .

Next we observe for any X, Y

$$
\begin{array}{ll}
 & [p^{n+1}.X \vee Y] \\
= & \quad \{\text{def. of functional iteration}\} \\
 & [p^n.(p.X) \vee Y] \\
= & \quad \{(4) \text{ with } X := p.X\} \\
 & [p.X \vee q^n.Y] \\
= & \quad \{(0) \text{ with } Y := q^n.Y\} \\
 & [X \vee q.(q^n.Y)] \\
= & \quad \{\text{def. of functional iteration}\} \\
 & [X \vee q^{n+1}.Y] \qquad .
\end{array}
$$

(End of Proof.)

<u>Remark</u> Functional iteration can be defined recursively by $f^{n+1}.X = f.(f^n.X)$ or $f^{n+1}.X = f^n.(f.X)$; note that the above proof uses both definitions. (End of Remark.)

<u>Proof of Lemma 2</u> The proof consists of showing that

(i) $(\underline{A}n: 0\leq n: p^n.X)$ solves

(5) $\quad Y: [Y \equiv X \wedge p.Y]$, and that

(ii) any solution Z of (5) satisfies

(6) $\quad [\,Z \Rightarrow (\underline{A}n: 0\leq n: p^n.X)\,]$.

<u>ad (i)</u> $\quad X \wedge p.(\underline{A}n: 0\leq n: p^n.X)$

$=\quad \{p \text{ universally conjunctive}\}$

$\quad X \wedge (\underline{A}n: 0\leq n: p.(p^n.X))$

$=\quad \{\text{def. of functional iteration}\}$

$\quad p^0.X \wedge (\underline{A}n: 0\leq n: p^{n+1}.X)$

$=\quad \{\text{predicate calculus}\}$

$\quad (\underline{A}n: 0\leq n: p^n.X)$

<u>ad (ii)</u> We observe for any solution Z of (5)

(7) $\quad [\,Z \Rightarrow X\,]$ and

(8) $\quad [\,Z \Rightarrow p.Z\,]$.

Hence

$\quad [\,Z \Rightarrow (\underline{A}n:: p^n.X)\,]$

$\Leftarrow\quad \{(7) \text{ and monotonicity of } \underline{A} \text{ and of } p^n\}$

$\quad [\,Z \Rightarrow (\underline{A}n:: p^n.Z)\,]$

$=\quad \{\text{predicate calculus}\}$

$\quad (\underline{A}n:: [\,Z \Rightarrow p^n.Z\,])$

which is shown by mathematical induction. We observe $[\,Z \Rightarrow p^0.Z\,]$ and

$[Z \Rightarrow p^{n+1}.Z]$

$\Leftarrow$ $\{$transitivity of $\Rightarrow\}$

$[Z \Rightarrow p.Z] \wedge [p.Z \Rightarrow p^{n+1}.Z]$

$=$ $\{(8)\}$

$[p.Z \Rightarrow p^{n+1}.Z]$

$\Leftarrow$ $\{$ monotonicity of $p\}$

$[Z \Rightarrow p^{n}.Z]$.

(End of Proof of Lemma 2)

Remark Originally we intended to prove Lemma 2 using the well-known closed form for the weakest fixpoint of an and-continuous function. However, p being universally conjunctive, it turned out to be simpler not to use that closed form and to prove Lemma 2 from first principles. (End of Remark.)

* * *

The reason for devoting a note to this theorem of Scholten's is that my first effort to prove it went awry; in my first effort, I used my standard heuristics, which were thus shown not to be infallible. I tried — h.A and k.B being given as extreme solutions — to prove (3) by mutual implication and tried to show LHS ⇒ RHS

$[A \vee k.B]$

$=$ $\{$predicate calculus$\}$

$[\neg A \Rightarrow k.B]$

$\Leftarrow$ $\{$ $k.B$ is the weakest sol. of $Y{:}[Y \Rightarrow B \wedge q.Y]$

$[\neg A \Rightarrow B \wedge q.(\neg A)]$

= {predicate calculus}
$[A \vee B] \wedge [A \vee q.(\neg A)]$
= {(0)}
$[A \vee B] \wedge [p.A \vee \neg A]$
⇐ {because of (1) $[h.A \Rightarrow A]$; predicate calculus}
$[h.A \vee B] \wedge [A \Rightarrow p.A]$

and there I was stuck: I had no way of meeting the remaining proof obligation $[h.A \vee B] \Rightarrow [A \Rightarrow p.A]$. The moral of the story is probably (possibly?) that we have to consider the truth of $[A \vee k.B]$ for values of $\neg A$ that fail to solve the tolerant equation of which $k.B$ is the weakest solution.

After this failure, the ATAC tried to establish (3) directly by equational reasoning. It has the added advantage of not destroying the symmetry between the two sides of (3); moreover, (0), which has to be used, has the same form.

Inks Lake State Park
31 March 1989

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