More annotated proofs (a sequel to 1143)

From the collection of WF & AvG, we consider the theorem

(0) $[x \Rightarrow J] \wedge [y \Rightarrow J] \;\Rightarrow\; [x;y \equiv x \wedge y]$.

How do we prove this? Well, to the left we have "J", which does not occur to the right, where we have ";", which does not occur to the left. Hence we need a connection between "J" and ";", which is, of course, that "J" is the neutral element of ";". We can go further: because what the antecedent states about "J" is symmetric in x and y, which in the consequent occur as left- and right-hand argument of the ";", we can expect to need that "J" is, both, the left-neutral and the right-neutral element of the composition.

In view of the above it is tempting to start a weakening chain at the antecedent and head for the expression $x;y$. Thus we observe

$$
\begin{array}{ll}
 & [x \Rightarrow J] \wedge [y \Rightarrow J] \\
\Rightarrow & \quad \{;\ \text{monotonic in both arguments}\} \\
 & [x;y \Rightarrow J;y] \wedge [x;y \Rightarrow x;J] \\
= & \quad \{J \text{ is left- and right-neutral element of } ;\} \\
 & [x;y \Rightarrow y] \wedge [x;y \Rightarrow x] \\
= & \quad \{\text{predicate calculus}\} \\
 & [x;y \Rightarrow x \wedge y]
\end{array}
$$

So ping has been proved; note that, in the mean time, we have used composition's monotonicity. We still have to show pong:

(1) $[x \Rightarrow J] \wedge [y \Rightarrow J] \;\Rightarrow\; [x \wedge y \Rightarrow x;y]$.

The antecedent -and we have used this in the proof of ping- implies that the prefix operators like "$x;$" and the postfix operators like "$;y$"Γ. If we wish to use that to strengthen $[x \wedge y \Rightarrow x;y]$, we have to strengthen a term in the consequent. Hence some shunting seems indicated:

$$
\begin{array}{ll}
 & [x \wedge y \Rightarrow x;y] \\
= & \quad \{\text{shunting}\} \\
 & [x \Rightarrow x;y \vee \neg y] \\
= & \quad \{J \text{ neutral element}\} \\
 & [x \Rightarrow x;y \vee J;\neg y] \\
\Leftarrow & \quad \{[x \Rightarrow J]\} \\
 & [x \Rightarrow x;y \vee x;\neg y] \\
= & \quad \{;\text{ over } \vee\} \\
 & [x \Rightarrow x;(y \vee \neg y)] \\
= & \quad \{\text{predicate calculus}\} \\
 & [x \Rightarrow x;\mathit{true}] \\
= & \quad \{\text{relational calculus}\} \\
 & \mathit{true}
\end{array}
$$

Γ are strengthening.

The way in which the symmetry is destroyed in the shunting step is strange and surprising. (My first proof shunted to $[x;y \vee \neg x \vee \neg y]$ and maintained the symmetry between x and y as much as possible.) The surprise reflects that if we drop in the antecedent one of the conjuncts, it is still a theorem. In the mean time, we have also used composition's distribution over $\vee$; in the sequence "monotonic", "distributing over $\vee$", "universally disjunctive" was that the next stronger property of composition to be taken into account, thus presenting a further invitation to do some shunting.

* * *

The next theorem we owe to the WF&AvG is

For p a left-condition

(2) $[p;p \equiv p]$

where — see EWD1143 — we characterize p's being a left-condition by

(3) $[p;x \Rightarrow p]$ for all x

Remark Note similarity and difference between (3) and our consequences of $[y \Rightarrow J]$ in the previous example, such as

$$[x;y \Rightarrow x] \text{ for all } x \quad .$$

Not surprisingly, our current proof shows structural similarities with the previous one. (End of Remark.)

Again, ping is a walk-over:

$$
\begin{array}{ll}
 & \text{true} \\
= & \{ (3) \text{ with } x := p \} \\
 & [p;p \Rightarrow p] \quad .
\end{array}
$$

When we tackled pong in class -without all these preliminaries- and looked at our proof obligation

$$[p \Rightarrow p;p] \quad \text{for left-condition } p,$$

we took the standard approach of listing the "direct consequences" or "simple properties" of the ingredients

- logical expressions built from left-conditions are left-conditions ; having only left-condition p this leads to $\neg p$ being a left-condition:

(4) $\qquad [\neg p; x \Rightarrow \neg p]$ for all x .

- $\Rightarrow$ can be expressed with $(\wedge \equiv)$, $(\vee \equiv)$, or $(\neg \vee)$; further shunting and contrapositive ;
  $\Rightarrow$ is transitive

- ; is monotonic , distributes over $\vee$,
  is universally disjunctive ;
  ; has an identity element
  ; is associative

Looking at these properties we concluded that they suggested to use the implication in the proof obligation for the introduction of $\neg$ and $\vee$, and (after some polishing) we came up with

$$\begin{array}{ll}
 & [p \Rightarrow p;p] \\
= & \quad \{ \text{sort of shunting} \} \\
 & [p \Rightarrow p;p \lor \neg p] \\
\Leftarrow & \quad \{ (4) \text{ with } x := p \} \\
 & [p \Rightarrow p;p \lor \neg p;p] \\
= & \quad \{ ; \text{ over } \lor \} \\
 & [p \Rightarrow (p \lor \neg p);p] \\
= & \quad \{ \text{pred. calc.} \} \\
 & [p \Rightarrow true;p] \\
= & \quad \{ \text{rel. calc.} \} \\
 & true.
\end{array}$$

Remark The "sort of shunting" – instead of eliminating the $\Rightarrow$ by rewriting the demonstrandum as $[\neg p \lor p;p]$ – was introduced in the polishing phase; it is purely cosmetic. (End of Remark.)

Remark In the context in which this problem was posed,

(5) $[(p \land x);y \equiv p \land x;y]$ for left-condition p

had been established. Rutger M. Dijkstra used it to establish (2) without ping-pong argument:

$$\begin{array}{ll}
 & true \\
= & \quad \{ (5) \text{ with } x,y := true, p \} \\
 & [(p \land true);p \equiv p \land true;p] \\
= & \quad \{ \text{pred. calc. ; rel. calc.} \} \\
 & [p;p \equiv p] \quad .
\end{array}$$

(End of Remark.)

* * *

It is customary to denote the strongest solution of

$$x: [J \vee a;x \Rightarrow x]$$

by a^* – read "a star" and called "the reflexive transitive closure of a"– . In EWD1136 we compared proofs for the theorem that, in our new terminology, the strongest solution of

$$x: [b \vee a;x \Rightarrow x]$$

is $a^*;b$. Knowing the theorem of Knaster-Tarski, we see that all this is expressed by

(6) $\quad [J \vee a;a^* \equiv a^*]$

(7) $\quad [b \vee a;x \Rightarrow x] \Rightarrow [a^*;b \Rightarrow x]$

(Formula (6) expresses that a^* solves the first equation; (7) with $b{:=}J$ expresses that a^* implies all its solutions. Applying the postfix operator ";b" to both sides of (6) tells us that $a^*;b$ solves the second equation, while (7) expresses that $a^*;b$ implies all its solutions.)

Following the traditions, we shall give the postfix operator $*$ in its exponential position a higher binding power than all other (relational and logical) operators. (In a note about notation, I should probably argue in favour of a prefix operator, but this note is about proof design.)

We are now going to show that $\sim$ and * commute -distribute over each other- , i.e.

(8) $\quad [(\sim s)^* \equiv \sim s^*]$

Because of the structure of (7), proofs of theorems about extreme solutions are often ping-pong arguments. We shall first demonstrate ping: it is a proof largely constructed on the principle "there is only one thing you can do". [It is therefore not a tribute to RMD, who produced the following proof almost verbatim.]

$$\begin{array}{ll}
 & [(\sim s)^* \Rightarrow \sim s^*] \\
\Leftarrow & \quad \{(7) \text{ with } a, b, x := \sim s, J, \sim s^*\} \\
 & [J \vee \sim s ; \sim s^* \Rightarrow \sim s^*] \\
= & \quad \{\text{relational calculus, applying} \sim \text{to both sides}\} \\
 & [J \vee s^* ; s \Rightarrow s^*]
\end{array}$$

The first step is dictated, because (7) is our only tool for concluding that a closure implies something. The "intuitive" calculator will justify the next step as "cleaning up", as a way of removing a large number of tildes. The conscious calculator will realize, that we can deal - see (7)- with a demonstrandum where the closure is the <u>left</u> argument of a composition; hence the decision to apply $\sim$ to both sides. Next, heading for a re-application of (7), we had better find a way of removing "$J \vee$" from the antecedent.

The only other place where J occurs is (6), so that is what we appeal to — in the hint I have recorded the direction of the appeal —

$$\begin{array}{ll} & [\mathrm{J} \vee s^*;s \Rightarrow s^*] \\ \Leftarrow & \quad \{(6)\Rightarrow \text{ with } a := s\} \\ & [\mathrm{J} \vee s^*;s \Rightarrow \mathrm{J} \vee s;s^*] \\ \Leftarrow & \quad \{\text{monotonicity of } \vee\} \\ & [s^*;s \Rightarrow s;s^*] \end{array}$$

and now we have again a demonstrandum with an antecedent to which (7) is applicable. So full of faith we continue:

$$\begin{array}{ll} & [s^*;s \Rightarrow s;s^*] \qquad \ddagger \\ \Leftarrow & \quad \{(7) \text{ with } a,b,x := s, s, s;s^*\} \\ & [s \vee s;s;s^* \Rightarrow s;s^*] \\ = & \quad \{;\text{ over } \vee\} \\ & [s;(\mathrm{J} \vee s;s^*) \Rightarrow s;s^*] \\ \Leftarrow & \quad \{;\text{ monotonic in 2nd argument}\} \\ & [\mathrm{J} \vee s;s^* \Rightarrow s^*] \\ = & \quad \{(6)\Rightarrow \text{ with } a := s\} \\ & \mathit{true} \qquad . \end{array}$$

In passing we note that we did not need the theorem of Knaster-Tarski: the proof could as well have been carried out, had (6) been replaced by the — formally much! — weaker

(6') $\qquad [\mathrm{J} \vee a;a^* \Rightarrow a^*]$.

I interpret this observation as a further confirmation of my suspicion that it is misleading to call a^* "the strongest fixpoint of $\langle \lambda x : \mathrm{J} \vee a;x \rangle$": there are too many arguments in which the "being a fixpoint" is not relevant.

Having proved ping: $[(\sim s)^* \Rightarrow \sim s^*]$ for all s, pong is now easy: the calculation below

$\quad$ true

$=\quad$ {ping with $s := \sim s$}

$\quad [(\sim\sim s)^* \Rightarrow \sim(\sim s)^*]$

$=\quad$ {$\sim$ is an involution}

$\quad [s^* \Rightarrow \sim(\sim s)^*]$

$=\quad$ {transposition}

$\quad [\sim s^* \Rightarrow (\sim s)^*]$

establishes pong, and hence (8) has been proved.

Reading the proof on the previous page, line ‡ shows that we have proved a next ping: $[s^*; s \Rightarrow s; s^*]$ for all s. The calculation below

$\quad$ true

$=\quad$ {ping with $s := \sim s$}

$\quad [(\sim s)^*; \sim s \Rightarrow \sim s; (\sim s)^*]$

$=\quad$ {(8)}

$\quad [\sim s^*; \sim s \Rightarrow \sim s; \sim s^*]$

$=\quad$ {rel. calc.}

$\quad [\sim(s; s^*) \Rightarrow \sim(s^*; s)]$

$=\quad$ {transposition}

$$[\ s;s^* \Rightarrow s^*;s\ ]$$

establishes the corresponding pong, hence

(9) $\quad [\ s^*;s \equiv s;s^*\ ]$.

* * *

As a final example of the use of (6) and (7) we shall show that $*$ is a closure, i.e. monotonic, weakening, and idempotent.

<u>* is monotonic</u>. We have to show for arbitrary s and t that

$$[s \Rightarrow t] \Rightarrow [s^* \Rightarrow t^*] \quad .$$

The proof is standard:

$\quad [\ s^* \Rightarrow t^*]$

$\Leftarrow \quad \{(7) \text{ with } a,b,x := s, J, t^*\}$

$\quad [J \vee s;t^* \Rightarrow t^*]$

$\Leftarrow \quad \{(6)\Rightarrow \text{with } a := t\}$

$\quad [J \vee s;t^* \Rightarrow J \vee t;t^*]$

$\Leftarrow \quad \{\text{monotonicities}\}$

$\quad [s \Rightarrow t]$.

Note that we did not need Knaster-Tarski.

<u>Remark</u> The fact that we first appealed to (7) and then to (6) is not essential, but in this order it works better; in the other order we would need a second appeal to (6). (End of Remark.)

* is weakening We have to show for arbitrary s that

$$[s \Rightarrow s^*] \quad .$$

Since this is a demonstrandum with s^* as consequent, (7) is in this context irrelevant, and we shall only appeal to (6). This is perhaps the place to remark that (when we are not interested in Knaster-Tarski) we can draw to separate conclusions from (6)

(10) $\quad [J \Rightarrow a^*]$

(11) $\quad [a;a^* \Rightarrow a^*] \quad .$

We now observe

$$\begin{array}{ll} & s^* \\ \Leftarrow & \{(11) \text{ with } a:=s\} \\ & s;s^* \\ \Leftarrow & \{(10) \text{ with } a:=s \text{ , monotonicity of } ;\} \\ & s;J \\ = & \{\text{relational calculus}\} \\ & s \quad . \end{array}$$

* is idempotent We have to show for arbitrary s that $[s^{**} \equiv s^*]$, but since we have just shown that * is weakening, it suffices to show that for any s

$$[s^{**} \Rightarrow s^*] \quad .$$

To this end we observe for any s

$[s^{**} \Rightarrow s^*]$

$\Leftarrow \quad \{(7) \text{ with } a, b, x := s^*, J, s^*\}$

$[J \vee s^*; s^* \Rightarrow s^*]$

$= \quad \{(10) \text{ with } a := s\}$

$[s^*; s^* \Rightarrow s^*]$

$\Leftarrow \quad \{(7) \text{ with } a, b, x := s, s^*, s^*\}$

$[s^* \vee s; s^* \Rightarrow s^*]$

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

$[s; s^* \Rightarrow s^*]$

$= \quad \{(11) \text{ with } a := s\}$

true.

* *

In the above proof I can think of only one place where we could have gone wrong:

$[s^*; s^* \Rightarrow s^*]$

$\Leftarrow \quad \{\text{monotonicity}\}$

$[s^* \Rightarrow J]$.

With the amount of annotation decreasing so rapidly, this EWD had better be concluded.

Austin, 13 November 1992

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