More about unique solutions and well-foundedness, courtesy Rutger M. Dijkstra

Here is an account of (part of) yesterday's ETAC; more in particular this note records a theorem and its proof, presented to us by Rutger Dijkstra. The theorem says that $*r;y;s*$ is the unique solution of

$$x: [x \equiv r;x \vee y \vee x;s]$$

for left-founded (see later) relation r, right-founded relation s, and arbitrary relation y.

* * *

Let us first summarize the facts that we know about the somewhat simpler $*r;y$ and $y;s*$.

For arbitrary relations r, s, and y we have

(0a) $*r;y$ is the least/strongest solution of
$x: [x = r;x \vee y]$

(0b) $y;s*$ is the least solution of
$x: [x = y \vee x;s]$

Remark For lack of a better alternative, we rather inelegantly use "*" both as a prefix and as a postfix operator.

▨

Now, one of the theorems mentioned by Rutger was the "combination" of (0a) and (0b). (It was only mentioned in passing.) The theorem reads:

(0c) $*r;y;s*$ is the least solution of
$x: [x \equiv r;x \vee y \vee x;s]$.

Proving (0c) from (0a) and (0b) is a rather ~~straightforward~~ exercise, which we leave to the reader. Note that, if we can assume that *false and false* are equal to the identity element ⌋ of operator ";", the reverse is also possible: in that case, (0a) and (0b) are instances of (0c) - with $s := false$ and $r := false$, respectively.

The more important fact to be mentioned is that for "properly founded" r and s, the least solutions in (0) are unique solutions of their equations. More precisely, we have

(1a) r is left-founded $\Rightarrow$
$\langle \forall x,y :: [x \equiv r;x \vee y] \equiv [x \equiv *r;y] \rangle$

(1b) s is right-founded $\Rightarrow$
$\langle \forall x,y :: [x \equiv y \vee x;s] \equiv [x \equiv y;s*] \rangle$.

Remark We did the nice exercise of proving (1a) - and, by symmetry, (1b) as well - using definitions

$$r \text{ left-founded} \equiv \langle \forall x :: [x \Rightarrow r;x] \Rightarrow [x \Rightarrow \text{false}] \rangle$$
$$s \text{ right-founded} \equiv \langle \forall x :: [x \Rightarrow x;s] \Rightarrow [x \Rightarrow \text{false}] \rangle .$$

We omit the proof here, because it has been recorded before.

In fact, the implications in (1a) and (1b) are genuine equivalences. A proof of this was discussed by the Club as well. We may come back to this proof obligation later.

■ Remark.

* * *

Now, the theorem that was the incentive for writing this note, is a "combination" of (1a) and (1b), just like (0c) is a combination of (0a) and (0b):

(1c) r left-founded $\wedge$ s right-founded $\Rightarrow$
$\langle \forall x,y :: [x = r;x \vee y \vee x;s] \equiv [x = *r;y;s*] \rangle$

Note that, again, under the assumption that $*\text{false}$ and $\text{false}*$ equal $\mathbb{J}$, properties (1a) and (1b) are instances of (1c): fortunately, false is a well-founded relation.

Proof of (1c) For any x and y we calculate

$$[x \equiv r;x \vee y \vee x;s]$$
$$\equiv \quad \{ \text{(1a) with } y := y \vee x;s \text{, using that } r \text{ is left-founded} \}$$

$$
\begin{array}{ll}
 & [x \equiv *r;(y \vee x;s)] \\
\equiv & \quad \{\ ;\ \text{over}\ \vee\ \} \\
 & [x \equiv *r;y \vee *r;x;s] \\
\equiv & \quad \{\ \text{preparing the use of (1b):} \\
 & \qquad \bullet\ [*r;x \equiv x],\quad \text{(discussed below)} \\
 & \quad \} \\
 & [x \equiv *r;y \vee x;s] \\
\equiv & \quad \{\ \text{(1b) with } y := *r;y\ ,\ \text{using that} \\
 & \qquad s \text{ is right-founded} \\
 & \quad \} \\
 & [x \equiv *r;y;s*]\ .
\end{array}
$$

Now we are done, provided we can discard the assumption $[*r;x \equiv x]$, which more or less presented itself because of our wish to apply (1b). It definitely isn't a theorem, not even for left-founded r; in fact, left-foundedness has nothing to do with it, as will become clear shortly. Let us investigate the situation in a somewhat more general way.

Intermezzo. The situation we are in is as follows. We want to prove something of shape $[A \equiv B]$, but sofar we have only proved $[p \Rightarrow (A \equiv B)]$, for some p, i.e. we've proved $[p \wedge A \equiv p \wedge B]$. This shows that we have reached our goal if we can prove both

$$[A \Rightarrow p] \quad \text{and} \quad [B \Rightarrow p]\ .$$

■ Intermezzo.

The Intermezzo shows that (1c) is okay provided we can prove

(2) $[x \equiv r;x \vee y \vee x;s] \Rightarrow [*r;x \equiv x]$ and

(3) $[x \equiv *r;y;s*] \Rightarrow [*r;x \equiv x]$.

Indeed we can. The validity of (2) is based on the validity of

(4) if $[r;x \Rightarrow x]$ then $[*r;x \Rightarrow x]$,

which is a useful property in its own right, and the validity of (3) follows from property $[*r;*r \equiv *r]$. (The detailed proofs are left to the reader.)

Now we have finally completed the proof of theorem (1c).

* * * *

Waalre, 11th December 1996

W.H.J. Feijen
A.J.M. van Gasteren