Mathematical Induction Synthesized

Let f be a monotonic predicate transformer and let q be the strongest solution of $p: [f.p \Rightarrow p]$. Then, by definition,

(0) $[f.q \Rightarrow q]$

(1) $[f.p \Rightarrow p] \Rightarrow [q \Rightarrow p]$ for all p.

The first theorem of this note is that <u>for monotonic f</u>, (1) can be strengthened to

(2) $[q \Rightarrow (f.p \Rightarrow p)] \Rightarrow [q \Rightarrow p]$ for all p.

<u>Proof</u> We observe for any p

$$
\begin{array}{ll}
 & [q \Rightarrow (f.p \Rightarrow p)] \\
= & \quad \{\text{pred. calc.}\} \\
 & [q \wedge f.p \Rightarrow p] \\
= & \quad \{\text{pred. calc.}\} \\
 & [q \wedge f.p \Rightarrow q \wedge p] \\
\Rightarrow & \quad \{(0),\ (\text{anti}) \text{monotonicity of } \wedge, \Rightarrow\} \\
 & [f.q \wedge f.p \Rightarrow q \wedge p] \\
\Rightarrow & \quad \{f \text{ is monotonic, i.e. } f.(q \wedge p) \Rightarrow f.q \wedge f.p\} \\
 & [f.(q \wedge p) \Rightarrow q \wedge p] \\
\Rightarrow & \quad \{(1) \text{ with } p := q \wedge p\} \\
 & [q \Rightarrow q \wedge p] \\
= & \quad \{\text{pred. calc.}\} \\
 & [q \Rightarrow p] \quad .
\end{array}
$$

(End of Proof.)

Formula (2) can be rewritten (by predicate calculus) as

(3) $\quad [f.p \Rightarrow (q \Rightarrow p)] \Rightarrow [q \Rightarrow p]$

from which, by using the monotonicity of f once more, we can derive

(4) $\quad [f.(q \Rightarrow p) \Rightarrow (q \Rightarrow p)] \Rightarrow [q \Rightarrow p]$

* * *

We now consider for $f.p$ the choice $\neg(s;\neg p)$, that is, let q now be the strongest solution of $p: [p \vee s;\neg p]$. Then, by definition,

(5) $\quad [q \vee s;\neg q]$

(6) $\quad [p \vee s;\neg p] \Rightarrow [q \Rightarrow p]$

Our second theorem is that with this choice of f, q is a left-condition, i.e. $[q;true \Rightarrow q]$.

Proof We observe

$$
\begin{array}{ll}
 & [q;true \Rightarrow q] \\
= & \quad \{left\text{-}exchange\} \\
 & [\neg q;\sim true \Rightarrow \neg q] \\
= & \quad \{contrapositive,\ [true \equiv \sim true]\} \\
 & [q \Rightarrow \neg(\neg q;true)] \\
\Leftarrow & \quad \{(6) \text{ with } p := \neg(\neg q;true)\} \\
 & [\neg(\neg q;true) \vee s;\neg q;true] \\
= & \quad \{pred.calc.\}
\end{array}
$$

$$
\begin{array}{ll}
 & [\ \neg q ; true \ \Rightarrow\ s ; \neg q ; true\ ] \\
\Leftarrow & \quad \{ \text{monotonicity of } ; \} \\
 & [\ \neg q \ \Rightarrow\ s ; \neg q\ ] \\
= & \quad \{ (s) \\
 & true \quad .
\end{array}
$$

(End of Proof?)

* * *

Let us apply (4) with the last choice for f. Some manipulation yields

$$[\, q \Rightarrow (\neg(s ; (q \wedge \neg p)) \Rightarrow p)\,] \Rightarrow [\, q \Rightarrow p\,] \quad .$$

Taking for q also a left-condition, we now translate into the standard model with

q	yielding	$Q.x$
p	yielding	$P.x$
s	yielding	$x > y$
$[\ldots]$	yielding	$\langle \forall x,y :: \ldots\ldots \rangle$.

Since everything reduces to left-conditions, the universal quantification over y can be dropped. The translation of $s ; (q \wedge \neg p)$ is

$$\langle \exists z :: x > z \wedge Q.z \wedge \neg P.z \rangle \quad .$$

The whole translation yields

$$\langle \forall x : Q.x : \langle \forall z : x > z \wedge Q.z : P.z \rangle \Rightarrow P.x \rangle \Rightarrow \langle \forall x : Q.x : P.x \rangle$$

i.e. q emerges as the characterization of the "domain" over which s is well-founded.

Traditionally, well-foundedness is defined for a (domain, relation)-pair. The moral of the story is that we can start with the relation, and any relation then yields the domain over which it is well-founded. Instead of starting with (the natural numbers, $x > y$), we can start with the relation $x > y \wedge y \geq 0$ on the type integer. The corresponding "domain" then follows. It also shows that any relation can be used to do mathematical induction with; if, however, that domain is empty, the induction principle is not very useful.

* * *

Once more I shall show that a relation s and its transitive closure r are equally well-founded; this now means that, with

(7) $[r \equiv s \vee s;r]$

the equations

$$p: [p \vee s;\neg p] \quad \text{and} \quad p: [p \vee r;\neg p]$$

have the same strongest solution. To save negation signs, we shall show instead that the equations

$$p: [p \Rightarrow s;p] \quad \text{and} \quad p: [p \Rightarrow r;p]$$

have the same weakest solution. That is, with q determined by

(8) $[q \Rightarrow s;q]$ and

(9) $[p \Rightarrow s;p] \Rightarrow [p \Rightarrow q]$

we have to show

(10) $[q \Rightarrow r;q]$ and

(11) $[p \Rightarrow r;p] \Rightarrow [p \Rightarrow q]$.

Proof To demonstrate (10) we observe

$$
\begin{array}{ll}
 & [q \Rightarrow r;q] \\
\Leftarrow & \quad \{\text{monotonicity of } ; \text{ and } \Rightarrow\} \\
 & [q \Rightarrow s;q] \wedge [s \Rightarrow r] \\
= & \quad \{(8) \text{ and } (7)\} \\
 & \text{true}
\end{array}
$$

To demonstrate (11) we observe

$$
\begin{array}{ll}
 & [p \Rightarrow r;p] \\
= & \quad \{\text{pred. calc.}\} \\
 & [p \vee r;p \Rightarrow r;p] \\
= & \quad \{(7)\} \\
 & [p \vee r;p \Rightarrow (s \vee s;r);p] \\
= & \quad \{; \text{ over } \vee\} \\
 & [p \vee r;p \Rightarrow s;p \vee s;r;p] \\
= & \quad \{; \text{ over } \vee\} \\
 & [p \vee r;p \Rightarrow s;(p \vee r;p)] \\
\Rightarrow & \quad \{(9) \text{ with } p := p \vee r;p\} \\
 & [p \vee r;p \Rightarrow q] \\
\Rightarrow & \quad \{\text{pred. calc.}\} \\
 & [p \Rightarrow q]
\end{array}
$$

(End of Proof.)

The last theorem was independently proved by J.R. Rao, who subsequently assisted me in the phrasing of the above proof. The above proof is independent of the question of whether (7) determines r uniquely; I like it because it uses of the relational calculus only that composition is associative and distributes over disjunction.

* * *

I found these results essentially last week on my trip to Poughkeepsie and to Ithaca. When I came home I found among the mail a copy of a manuscript by Rutger M. Dykstra. It is a manuscript of 74 pages with what looks like a beautiful theory. On the last page but two it casually mentions as a corollary "$\neg s^{\infty} \wedge s$ is left-founded for all s" (Legenda: s^{∞} denotes the weakest solution of $p: [p \Rightarrow s;p]$.) It very much looks as if I can now leave the relational calculus in the more expert hands of the younger generation.

Austin, 17 April 1992

prof. dr. Edsger W. Dykstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78750 - 1188, USA