A simple theorem?

In this note I use square brackets to denote universal quantification over the free variables occurring in the enclosed.

Theorem Let w, x, y, and z be variables ranging over the same non-empty domain and let p be a two-place predicate on that domain. Let the two-place predicate Q be the strongest solution of

$$X: [X.x.y \equiv p.x.y \vee (\underline{E}z :: p.x.z \wedge X.z.y)] \quad ; \qquad (0)$$

let the two-place predicate R be the strongest solution of

$$X: [X.x.y \equiv p.x.y \vee (\underline{E}w :: X.x.w \wedge p.w.y)] \quad . \qquad (1)$$

Then

$$[Q.x.y \equiv R.x.y] \quad . \qquad (2)$$

The above theorem belongs to the folklore I grew up with in the sense that I never bothered to prove it, because it was so obvious. Regard the elements of the domain as the nodes of a graph and attach to p.x.y the meaning "there is an arrow from x to y"; then, "obviously" Q.x.y means "there is a non-empty path from x to y" and so does R.x.y , hence (2) . I always felt that, when challenged, I would be able to prove it, say by mathematical induction over the path length. When I tried to prove the theorem — secundum regulas artis — the latter hunch turned out to be wrong.

<u>Proof</u> The right-hand sides of (0) and (1) being monotonic functions of X , the strongest solutions of these equations exist – Knaster-Tarski – and are also the strongest solutions of the corresponding equations with $\equiv$ replaced by $\Leftarrow$, i.e.

$$[Q'.x.y \Leftarrow p.x.y \vee (\underline{E}z :: p.x.z \wedge Q'.z.y)] \Rightarrow [Q.x.y \Rightarrow Q'.x.y] \qquad (3)$$

$$[R'.x.y \Leftarrow p.x.y \vee (\underline{E}w :: R'.x.w \wedge p.w.y)] \Rightarrow [R.x.y \Rightarrow R'.x.y] \quad . \qquad (4)$$

Predicates Q and R being defined as strongest solutions, we prove (2) by showing that each side implies the other.

$[Q.x.y \Rightarrow R.x.y]$

0 $\Leftarrow$ { $Q' := R$ in (3)}

$[R.x.y \Leftarrow p.x.y \vee (\underline{E}z :: p.x.z \wedge R.z.y)]$

1 $=$ { since R solves (1): $[R.x.y \Leftarrow p.x.y]$ }

$[R.x.y \Leftarrow (\underline{E}z :: p.x.z \wedge R.z.y)]$

2 $=$ {predicate calculus}

$[R.x.y \Leftarrow p.x.z \wedge R.z.y]$

3 $=$ {predicate calculus}

$[R.z.y \Rightarrow R.x.y \vee \neg p.x.z]$

4 $=$ {renaming the dummies: $x,z := z,x$ }

$[R.x.y \Rightarrow R.z.y \vee \neg p.z.x]$

5 $\Leftarrow$ { $R'.x.y := R.z.y \vee \neg p.z.x$ in (4)}

$[R.z.y \vee \neg p.z.x \Leftarrow$

$\qquad p.x.y \vee (\underline{E}w :: (R.z.w \vee \neg p.z.x) \wedge p.w.y)]$

6 $\Leftarrow$ {predicate calculus}

$[R.z.y \Leftarrow (p.z.x \wedge p.x.y) \vee (\underline{E}w :: R.z.w \wedge p.w.y)]$

7 $\Leftarrow$ {from (1): $[R.z.x \Leftarrow p.z.x]$ }

$[R.z.y \Leftarrow (R.z.x \wedge p.x.y) \vee (\underline{E}w :: R.z.w \wedge p.w.y)]$

8 $\quad = \{$ predicate calculus $\}$
$[R.z.y \Leftarrow (\mathbf{E}w :: R.z.w \wedge p.w.y)]$
9 $\quad = \{$ R solves (1) $\}$
true .

The proof of $[Q.x.y \Leftarrow R.x.y]$ is too similar to be given in full.

(End of Proof.)

I was surprised by the amount of shuffling involved, but very pleased because all the steps were —by now— so familiar and so clearly suggested by the circumstances:

step 0: Here we have no choice: for the demonstrandum it is irrelevant that Q is a solution of (0) as it would also hold, were Q stronger; the conclusion has to be drawn from the knowledge what Q implies, i.e. (3). The step is the substitution dictated by the circumstances.

step 1: This is the recognition that of our two independent proof obligations, one is trivial.

step 2: A syntactical simplification.

step 3: Known as "the shunting trick", useful because it enables us to get in the demonstrandum an isolated R as the antecedent, a form required for the application of (4)

step 4: A clerical precaution so as to avoid errors in a nested substitution.

step 5: The actual subsitution in the application of (4)

step 6: "Unshunting" to begin with, as it allows the simplification of omitting the disjunct "¬ p.z.x" from the existentially quantified expression. By then I saw the job was done and could afford to omit the conjunct p.z.x from the existential quantification.

step 7: This step has been introduced to separate the explicit appeal to R being a solution of (1) from the next step.

step 8: This subsumes the one proof obligation in the other.

step 9: A final appeal to (1) settles the question.

Because in the original demonstrandum it is clearly irrelevant that R has been defined as a <u>strongest</u> solution the later appeal to (4) may surprise the reader. That appeal, however, occurs after step 0, in which we could not avoid to strengthen the demonstrandum.

Austin, 1 November 1985

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