Why the importance of continuity seems to be overrated

Without an appeal to continuity and without using fixed-point induction, we shall prove the following theorem.

Theorem Let $(C,<)$ be a well-founded set. Let predicates B and P, statement S, and function t be such that

$$[P \Rightarrow t \text{ in } C] \qquad (0)$$

and with fresh "thought variable" y

$$[B \wedge P \Rightarrow wp("y:=t", wp(S, P \wedge t<y))] \quad . \qquad (1)$$

Then $$[P \Rightarrow wp("\underline{do}\ B \rightarrow S\ \underline{od}", true)] \quad , \qquad (2)$$

in which the right-hand side is defined as the strongest solution of

$$X: [\ wp(S,X) \vee \neg B \equiv X] \quad . \qquad (3)$$

Ad (0). Note that t is a function on state space, whose value may belong to C or not; hence t in C stands for a predicate on state space.

Ad (1). Note that (1) subsumes the traditional

$$[P \wedge B \Rightarrow (\underline{E}x: x \text{ in } C: x<t)] \quad , \qquad (4)$$

i.e. $P \wedge B$ implies that t is not a minimal value.

Proof. Equation (3) has a strongest solution since wp (S,?) is conjunctive and, hence, monotonic. Let X be the strongest solution of (3). Since we can conclude from (0)

$$[P \Rightarrow (\underline{E}\, x: x \underline{in} C: t = x)] \quad ,$$

(2) -i.e. $[P \Rightarrow X]$- is proved by demonstrating

$$[P \wedge (\underline{E}\, x: x \underline{in} C: t = x) \Rightarrow X]$$

or, equivalently

$$(\underline{A}\, x: x \underline{in} C: [P \wedge t = x \Rightarrow X]) \quad . \quad (5)$$

In view of C's well-foundedness, (5) will be shown by mathematical induction, i.e. for any x in C, we shall derive $[P \wedge t = x \Rightarrow X]$ under the hypothesis

$$(\underline{A}\, y: y \underline{in} C \wedge y < x: [P \wedge t = y \Rightarrow X])$$

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

$$(\underline{A}\, y: y \underline{in} C \wedge y < x: [P \wedge t = y \wedge y \underline{in} C \wedge y < x \Rightarrow X])$$

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

$$(\underline{A}\, y: y \underline{in} C \wedge y < x: [P \wedge t = y \wedge t \underline{in} C \wedge t < x \Rightarrow X])$$

$$= \{\text{predicate calculus, P and X not containing } y\}$$

$$(\underline{A}\, y: y \underline{in} C \wedge y < x: [P \wedge t \underline{in} C \wedge t < x \Rightarrow X])$$

$$= \{(0)\}$$

$$(\underline{A}\, y: y \underline{in} C \wedge y < x: [P \wedge t < x \Rightarrow X])$$

Hence, the hypothesis implies $[P \wedge t < x \Rightarrow X]$ for all x such that the range for y is nonempty, i.e. all x that is non-minimal. For minimal x, $[P \wedge t < x \Rightarrow X]$ follows on account of (0) and the definition of minimality.

Next we observe for an x in C and any Z

$[Z \equiv B \wedge P \wedge t=x]$
$\Rightarrow$ {(1)}
$[Z \Rightarrow wp("y:=t", wp(S, P \wedge t<y)) \wedge t=x]$
= {Axiom of Assignment; conjunctivity of wp}
$[Z \Rightarrow wp("y:=t", wp(S, P \wedge t<y) \wedge y=x)]$
= {$[wp(S,Q) \wedge y=x \equiv wp(S, Q \wedge y=x)]$ since the thought variables x and y don't occur in S}
$[Z \Rightarrow wp("y:=t", wp(S, P \wedge t<y \wedge y=x))]$
$\Rightarrow$ {monotonicity of wp}
$[Z \Rightarrow wp("y:=t", wp(S, P \wedge t<x))]$
= {y is a thought variable}
$[Z \Rightarrow wp(S, P \wedge t<x)]$
$\Rightarrow$ {hypothesis, (0) and monotonicity}
$[Z \Rightarrow wp(S, X)]$.

Eliminating Z, we conclude under the hypothesis

$[B \wedge P \wedge t=x \Rightarrow wp(S, X)]$
= {predicate calculus}
$[P \wedge t=x \Rightarrow wp(S, X) \vee \neg B]$
= {X is a solution of (3)}
$[P \wedge t=x \Rightarrow X]$

(End of Proof.)

Remark. We gave a number to (4), expecting to need to refer to it. The need did not arise. (End of Remark)

* * *

The theorem is well-known for or-continuous wp(S,?) and natural t. The continuity permits us to write the strongest solution of (3) in closed form, viz. as the limit of a weakening chain. I (=EWD) used this expression a decade ago to prove the restricted theorem, but that proof was by no means simpler than our current one.

The above proof casts serious doubts on the supposed need of fancy things such as transfinite induction for reasoning about programs with unbounded nondeterminacy (as we might, for instance, encounter in an abstract program containing the unrefined statement "establish P" or with fair interleaving of the atomic actions of concurrent programs). This is a very nice thought.

drs. A.J.M. van Gasteren
BP Venture Research Fellow
Dept. of Mathematics and
Computing Science
University of Technology
5600 MB EINDHOVEN
The Netherlands

27 February 1984

prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow
Plataanstraat 5
5671 AL NUENEN
The Netherlands