The termination theorem for unconstrained nondeterminacy

Without appeal to continuity we shall prove the following theorem.

Theorem Let $(C,<)$ be a well-founded set. Let statement S, predicates B and P and function t on state space satisfy

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

and —with fresh "thought variable" y—

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

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

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 is a predicate on state space. (End of Ad (0).)

Proof. Equation (3) has a strongest solution since $wp(S,?)$ is conjunctive and, hence, monotonic. Let X be the strongest solution of (3).

Since (0) is the same as

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

(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,

$$(\underline{A}x: x\ \underline{in}\ C: [P \wedge t=x \Rightarrow X]) \quad . \quad (4)$$

In view of C's well-foundedness, we shall prove (4) by mathematical induction, i.e. for any x in C we shall derive $[P \wedge t=x \Rightarrow X]$ under the hypothesis

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

To begin with we observe

$$
\begin{array}{ll}
 & (5) \\
= & \{\text{interchange of quantifications}\} \\
 & [(\underline{A}y: y\ \underline{in}\ C \wedge y<x: P \wedge t=y \Rightarrow X)] \\
= & \{\text{predicate calculus}\} \\
 & [(\underline{A}y: t=y: y\ \underline{in}\ C \wedge y<x \wedge P \Rightarrow X)] \\
= & \{\text{predicate calculus}\} \\
 & [t\ \underline{in}\ C \wedge t<x \wedge P \Rightarrow X] \\
= & \{(0)\} \\
 & [P \wedge t<x \Rightarrow X] \quad . \quad (6)
\end{array}
$$

Next we observe for that x and any Z

$$
\begin{array}{ll}
 & [Z \equiv B \wedge P \wedge t=x] \\
\Rightarrow & \{(1)\} \\
 & [Z \Rightarrow wp(\text{"}y:=t\text{"}, wp(S, P \wedge t<y)) \wedge t=x] \\
= & \{\text{Axiom of Assignment; conjunctivity of } wp\} \\
 & [Z \Rightarrow wp(\text{"}y:=t\text{"}, wp(S, P \wedge t<y) \wedge y=x)] \\
= & \{\text{thought variables } x \text{ and } y \text{ don't occur in } S\}
\end{array}
$$

$[Z \Rrightarrow wp(\text{"}y{:=}t\text{"}, wp(S, P \wedge t < y \wedge y = x))]$

$\Rightarrow$ {monotonicity of wp}

$[Z \Rrightarrow wp(\text{"}y{:=}t\text{"}, wp(S, P \wedge t < x))]$

$=$ {thought variable y does not occur in $wp(S, P \wedge t<x)$}

$[Z \Rrightarrow wp(S, P \wedge t < x)]$

$\Rightarrow$ {(6) and monotonicity of wp}

$[Z \Rrightarrow wp(S, X)]$.

Eliminating Z, we conclude

true

$=$ {see above}

$[B \wedge P \wedge t = x \Rrightarrow wp(S,X)]$

$=$ {predicate calculus}

$[P \wedge t=x \Rrightarrow wp(S,X) \vee \neg B]$

$=$ { X is a solution of (3)}

$[P \wedge t=x \Rrightarrow X]$.

(End of Proof.)

* * *

The theorem is well-known for or-continuous $wp(S,?)$ and natural t . The continuity permits us to write the strongest solution of (3) as the limit of a weakening chain. EWD used this expression a decade ago to prove the restricted theorem, but that proof was no 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

29 February 1984

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