On different notions of termination

A repetition terminates for a given initial state means that after some number of iterations its guards are false. In the presence of unbounded nondeterminacy an upper bound for this number of iterations need not exist, the canonical example being

$$\underline{\text{do}}\ x > 0 \rightarrow x := x - 1$$
$$[\!]\ x < 0 \rightarrow x := \text{any natural number}$$
$$\underline{\text{od}}\ .$$

So-called <u>strong termination</u> means that such an upper bound exists. (The above program terminates for all initial states, but only strongly for $x \geq 0$.)

<u>Note</u>. In the absence of unbounded nondeterminacy termination is always strong. (End of Note.)

We would like to relate the above rather operational notion of termination to semantics defined by predicate transformation. To this end we have to capture first the notion of machine states in terms of predicates.

* * *

Point complements

In the following p and q will be used to denote so-called "point complements". For each point in state space there exists one point complement, i.e. a predicate that is false in that point and true everywhere else. We postulate for point complements

Axiom 0: $[(\underline{E}\, p :: \neg p)]$

Axiom 1: $[p \vee Q] \not\equiv [p \vee \neg Q]$ for all Q and point complement p .

For a person with an intuitive appreciation of point complements, these axioms express "obvious" properties of point complements. Point complements enjoy more equally "obvious" properties. These, however, we shall prove from the above two, thus justifying their being called "Axioms".

Lemma 0. $[p \equiv q] \not\equiv [p \vee q]$

Proof of Lemma 0.

$[p \equiv q]$
$= \{\text{predicate calculus}\}$
$[(p \vee \neg q) \wedge (q \vee \neg p)]$
$= \{\text{predicate calculus}\}$
$[p \vee \neg q] \wedge [q \vee \neg p]$
$= \{\text{Axiom 1, applied to both terms}\}$
$\neg[p \vee q] \wedge \neg[q \vee p]$
$= \{\text{predicate calculus}\}$
$\neg[p \vee q]$
$\neq \{\text{predicate calculus}\}$
$[p \vee q]$ (End of Proof of Lemma 0.)

Lemma 1. $[Q \equiv (\underline{E}p : [p \vee Q] : \neg p)]$ for all Q.

Proof of Lemma 1. We have for all Q

true
$= \{\text{Axiom 0}\}$
$[Q \equiv Q \wedge (\underline{E}p :: \neg p)]$
$= \{\text{predicate calculus}\}$
$[Q \equiv (\underline{E}p :: Q \wedge \neg p)]$
$= \{\text{Axiom 1}\}$
$[Q \equiv (\underline{E}p : [p \vee Q] \vee [p \vee \neg Q] : Q \wedge \neg p)]$
$= \{\text{predicate calculus}\}$
$[Q \equiv (\underline{E}p : [p \vee Q] : Q \wedge \neg p)]$

$= \{[P \vee Q] \equiv [\neg P \equiv Q \wedge \neg P]$ for all P and $Q\}$
$[Q \equiv (\underline{E}p : [p \vee Q] : \neg p)]$

(End of Proof of Lemma 1.)

Note. The rôle of the above Axioms and Lemmata can be interchanged: Axiom 0 can be proved from Lemma 1, Axiom 1 can be proved from Lemmata 0 and 1. (End of Note.)

Substituting in Lemma 1 $\neg Q$ for Q yields, by virtue of Axiom 1

Corollary 0 $\quad [Q \equiv (\underline{A}p :: [p \vee Q] \vee p)]$ for all Q .

For later purposes we need Lemma 2, which deals with a situation in which existential and universal quantification can be interchanged; its proof relies on Axiom 1 only.

Lemma 2. For all point complements p and all sets S of predicates we have

$$[p \vee (\underline{E}Q : Q \ \underline{in}\ S : Q)] \equiv (\underline{E}Q : Q \ \underline{in}\ S : [p \vee Q])$$

Proof of Lemma 2. We have for all p and S

$[p \vee (\underline{E}Q : Q \ \underline{in}\ S : Q)]$
$\not\equiv \{$Axiom 1$\}$
$[p \vee \neg(\underline{E}Q : Q \ \underline{in}\ S : Q)]$
$= \{$predicate calculus$\}$
$[p \vee (\underline{A}Q : Q \ \underline{in}\ S : \neg Q)]$
$= \{$predicate calculus$\}$
$[(\underline{A}Q : Q \ \underline{in}\ S : p \vee \neg Q)]$
$= \{$predicate calculus$\}$
$(\underline{A}Q : Q \ \underline{in}\ S : [p \vee \neg Q])$
$= \{$Axiom 1$\}$
$(\underline{A}Q : Q \ \underline{in}\ S : \neg [p \vee Q])$
$\not\equiv \{$predicate calculus$\}$

$(\underline{E}Q: Q \text{ } \underline{in} \text{ } S: [p \vee Q])$.
(End of Proof of Lemma 2.)

* * *

Let —for the time being without further qualification of the notion of termination— $wp(S,R)$ stand, as usual, for the weakest condition on the initial state such that S is guaranteed to establish R. In order to familiarize ourselves a bit more with point complements, we explore the meanings of $[p \vee wp(S,q)]$ and $[p \vee \neg wp(S,q)]$.

Let sp and sq denote the single states in which p and q, respectively, are false. Then, $wp(S,q)$ characterizes all initial states guaranteed to lead to a final state different from sq . Hence $[p \vee wp(S,q)]$ is the assertion that an execution of S, started in sp, will terminate in a state different from sq. Conversely, $\neg wp(S,q)$ characterizes all initial states for which termination outside sq cannot be guaranteed; hence $[p \vee \neg wp(S,q)]$ is the assertion that the class of executions possible when S is started in sp contains at least one execution that either fails to terminate or ends in sq .

On account of Axiom 1 we have

$$[p \vee wp(S,T)] \not\equiv [p \vee \neg wp(S,T)]$$

and we investigate the 2 exclusive cases.

$[p \vee wp(S,T)]$: in this case termination of S when started in sp is guaranteed and $[p \vee \neg wp(S,q)]$ then means sq is a possible final state.

$[p \vee \neg wp(S,T)]$: in this case termination of S when started in sp is <u>not</u> guaranteed and, on account of the monotinicity of $wp(S,?)$, we have $[p \vee \neg wp(S,q)]$ for all q.

With some poetic license we shall describe the situation $[p \vee \neg wp(S,q)]$, regardless of the value of $[p \vee wp(S,T)]$, as "q is a successor of p".

We are interested in termination, that is in repetitions. With

DO: <u>do</u> $B \rightarrow S$ <u>od</u> and IF: <u>if</u> $B \rightarrow S$ <u>fi</u>

our interest in the equivalence of

DO and <u>if</u> $B \rightarrow$ IF; DO $[\!]$ $\neg B \rightarrow$ skip <u>fi</u>

can be translated into interest in the equivalence of

$$wp(DO,T) \quad \text{and} \quad wp(IF, wp(DO,T)) \vee \neg B \quad ,$$

i.e. the question whether $wp(DO,T)$ is a solution of

$$X: [X \equiv f X] \quad \text{with} \quad [f X \equiv wp(IF,X) \vee \neg B] \text{ for all } X.$$

The predicate transformer f cannot be interpreted as a weakest precondition — it violates the Law of the Excluded Miracle —, yet, stretching the notion of "successor" still further, we shall also describe the situation $[p \vee \neg f q]$ as "q is a successor of p". (Strictly speaking we should have added "with respect to $wp(S,?)$" and "with respect to f" respectively.) For a further interpretation of $[p \vee \neg f q]$ we consider again 2 exclusive cases.

$[p \vee B]$: in this case, DO, when started in sp, does not immediately terminate and $[p \vee \neg f q]$ means that the class of possible executions of S when started in sp contains at least one execution that either fails to terminate or ends in sq.

$[p \vee \neg B]$: in this case DO, when started in sp, immediately terminates and, as will be shown, sp has no successor.

<u>Proof.</u> $[p \vee \neg B]$
$$= \{\text{Axiom 1}\}$$
$$\neg[p \vee B]$$
$$\Rightarrow \{\text{by predicate calculus for any } q\}$$
$$\neg[p \vee (B \wedge \neg wp(IF, q))]$$
$$= \{\text{definition of } f\}$$
$$\neg[p \vee \neg fq]$$
(End of Proof.)

In the case of nested repetitions an infinite computation obviously implies that at least one repetition fails to terminate; stronger, in any infinite computation precisely one repetition displays infinite repetition: its interior repetitions obviously terminate and its embracing repetitions don't make progress. Therefore, investigations about termination or infinite repetition of <u>do</u> $B \rightarrow S$ <u>od</u> can be carried out in isolation, i.e. under the assumption that each activation of S terminates. Under this assumption, $[p \vee \neg fq]$ means that, operationally speaking, sq is a genuine possible successor of sp.

A "decreasing chain" is defined to be a non-empty sequence of point complements such that of any two consecutive predicates in this sequence the second one is a successor of the first one; a decreasing chain is said "to start at" its first predicate. A maximal decreasing chain is a decreasing chain that cannot be extended, i.e. does not end at a predicate with one or more successors. A maximal decreasing chain of finite length therefore ends at a predicate with no successor. The length of a decreasing chain is defined as the number of predicates in the chain.

After the above we can now formulate the two main results of this note, viz.

<u>Theorem 0</u>. For unboundedly conjunctive f and any point complement p

$[p \vee (\underline{E}i : i \geq 0 : f^i F)] \equiv$
(there exists an upper bound for the lengths of the decreasing chains starting at p) .

<u>Theorem 1</u>. For unboundedly conjunctive f, let Q be the strongest solution of $X: [fX \equiv X]$; then for any point complement p

$[p \vee Q] \equiv$
(all decreasing chains starting at p are of finite length) .

<u>Remark on nomenclature</u>. Predicate transformer f is unboundedly conjunctive means

$$[f(\underline{A}X : X \underline{in} S : X) \equiv (\underline{A}X : X \underline{in} S : fX)]$$

for any non-empty set S of predicates. (End of Remark on nomenclature.)

Note that Theorem 1 could have stated that Q is the weakest predicate such that the solutions of $p : [p \vee Q]$ are well-founded with respect to the successor relation.

We have shown earlier - see EWD822 - that for monotonic f - and hence for unboundedly conjunctive f - $(\underline{E}i : i \geq 0 : f^i F)$ is at least as strong as any solution of $X : [fX \equiv X]$. Fortunately, this is compatible with "of bounded length" being a stronger property than "of finite length".

In EWD822 we have also shown that for <u>or</u>-continuous f — i.e. in the absence of unbounded nondeterminacy — $[Q \equiv (\underline{E} i: i \geq 0: f^i F)]$. In that case it is irrelevant whether we define $wp(DO, T)$ as Q or as $(\underline{E} i: i \geq 0: f^i F)$. Otherwise we have to distinguish between wpb and wpf — for "bounded" and "finite" respectively — , the general formulae being

$$[wpb(DO, R) \equiv (\underline{E} i: i \geq 0: f^i F)]$$

$$[wpf(DO, R) \equiv Q] \text{ with } Q \text{ the strongest solution of } X: [fX = X]$$

where f is defined by $[fX \equiv wp(IF, X) \vee \neg B \wedge R]$.

In order to prove Theorems 0 and 1 we need a lemma connecting fQ for general Q with the successor relation, which is one between point complements:

<u>Lemma 3</u> For unboundedly conjunctive f and any predicate Q satisfying $\neg[Q] \vee [fT]$ and any point complement p

$$[p \vee fQ] \equiv (\underline{A} q: [p \vee \neg fq]: [q \vee Q])$$.

<u>Proof</u>. The somewhat mysterious condition $\neg[Q] \vee [fT]$ occurs because, in combination with f's unbounded conjunctivity, it allows us to conclude

$$[f(\underline{A} q: [q \vee \neg Q]: q) \equiv (\underline{A} q: [q \vee \neg Q]: fq)]$$.*

In the case $\neg[Q]$ the above follows from f's unbounded conjunctivity and the fact that the range of q is not empty; in the case $[fT]$ the above follows because then f is universally conjunctive.

The remainder of the proof proceeds as follows. For any p

$$
\begin{array}{l}
\quad [p \vee fQ] \\
= \{\text{Corollary 0}\} \\
\quad [p \vee f(\underline{A}\, q :: [q \vee Q] \vee q)] \\
= \{\text{pred. calc. and Axiom 1}\} \\
\quad [p \vee f(\underline{A}\, q : [q \vee \neg Q] : q)] \\
= \{\text{see * above}\} \\
\quad [p \vee (\underline{A}\, q : [q \vee \neg Q] : fq)] \\
= \{\text{pred. calc.}\} \\
\quad [(\underline{A}\, q : [q \vee \neg Q] : p \vee fq)] \\
= \{\text{pred. calc.}\} \\
\quad (\underline{A}\, q : [q \vee \neg Q] : [p \vee fq]) \\
= \{\text{pred. calc. and Axiom 1}\} \\
\quad (\underline{A}\, q : [p \vee \neg fq] : [q \vee Q])
\end{array}
$$

(End of Proof.)

We shall first use Lemma 3 with $f^i F$ for Q, yielding —using the definition of functional composition—

<u>Lemma 4</u>. For unboundedly conjunctive f, natural i, and point complement p

$$[p \vee f^{i+1} F] \equiv (\underline{A}\, q : [p \vee \neg fq] : [q \vee f^i F])$$

<u>Proof</u>. In order to justify the appeal to Lemma 3, we have to demonstrate $[f^i F] \Rightarrow [fT]$. For $i=0$, this is trivial; for the remaining cases we observe

$$
\begin{array}{l}
\quad \text{true} \\
= \{\text{pred. calc.}\} \\
\quad [f^{i-1} F \Rightarrow T] \\
\Rightarrow \{f \text{ is monotonic}\} \\
\quad [f^i F \Rightarrow fT] \\
\Rightarrow \{\text{pred. calc.}\} \\
\quad [f^i F] \Rightarrow [fT]
\end{array}
$$

. (End of Proof.)

In order to prove Theorem 0, one further step is needed: using Lemma 4, we shall interpret $[p \vee f^i F]$

in terms of decreasing chains.

Lemma 5. For unboundedly conjunctive f, natural i, and point complement p

$$[p \vee f^i F] \equiv$$
(the length of any decreasing chain starting at p is at most i) .

Proof. For $i=0$ the above equivalence holds, both sides being false for all p. For the remainder we proceed by mathematical induction over i:

$[p \vee f^{i+1} F]$
= {Lemma 4}
$(\underline{A} q : [p \vee \neg f q] : [q \vee f^i F])$
= {definition of successor and induction hypothesis}
($\underline{A} q$: q is a successor of p: the length of any decreasing chain starting at q is at most i)
= {definition of decreasing chain starting at p}
(the length of any decreasing chain starting at p is at most $i+1$)

(End of Proof).

Proof of Theorem 0.

$[p \vee (\underline{E} i : i \geq 0 : f^i F)]$
= {Lemma 2}
$(\underline{E} i : i \geq 0 : [p \vee f^i F])$
= {Lemma 5}
($\underline{E} i : i \geq 0$: the length of any decreasing chain starting at p is at most i)
= {definition of upper bound}
(there exists an upper bound for the lengths of the decreasing chains starting at p) .

(End of Proof of Theorem 0.)

In order to prove Theorem 1, we use Lemma 3 a second time, viz. with for Q a solution of $X: [fX \equiv X]$.

Lemma 6. For unboundedly conjunctive f, Q a solution of $X: [fX \equiv X]$ and point complement p

$$[p \vee Q] \equiv (\underline{A} q : [p \vee \neg fq] : [q \vee Q]) \quad .$$

Proof. Since $[p \vee Q] \equiv [p \vee fQ]$, the above is nothing but the equivalence from Lemma 3. In order to justify the appeal to Lemma 3, we have to demonstrate $[Q] \Rightarrow [fT]$.

$$\begin{array}{ll} & \text{true} \\ = & \{\text{definition of } Q\} \\ & [Q \equiv fQ] \\ \Rightarrow & \{f \text{ is monotonic}\} \\ & [Q \Rightarrow fT] \\ \Rightarrow & \{\text{pred. calc.}\} \\ & [Q] \Rightarrow [fT] \end{array}$$

. (End of Proof.)

Proof of Theorem 1. We shall prove Theorem 1 in the form of

$\neg[p \vee Q] \equiv$
(there exists an infinite decreasing chain starting at p)

by showing that either side implies the other.

Applying de Morgan's Law to the conclusion of Lemma 6, we obtain

$$\begin{array}{ll} & \neg[p \vee Q] \equiv (\underline{E} q : [p \vee \neg fq] : \neg[q \vee Q]) \\ = & \{\text{definition of successor}\} \\ & \neg[p \vee Q] \equiv (\underline{E} q : q \text{ is a successor of } p : \neg[q \vee Q]) \end{array}$$

Hence

$\neg[p \vee Q] \Rightarrow$ (there exists an infinite decreasing chain starting at p) .

Conversely, let $q\,i$ for $i \geq 0$ and $[q\,0 \equiv p]$ be an infinite decreasing chain starting at p. We have for any Z

$$
\begin{array}{l}
\quad [Z \equiv f(\underline{A}\,i : i \geq 0 : q\,i)] \\
= \{f \text{ is unboundedly conjunctive and range } i \text{ non-empty}\} \\
\quad [Z \equiv (\underline{A}\,i : i \geq 0 : f(q\,i))] \\
\Rightarrow \{\text{pred. calc}\} \\
\quad [Z \Rightarrow (\underline{A}\,i : i \geq 1 : f(q\,i))] \\
= \{\text{renaming the dummy}\} \\
\quad [Z \Rightarrow (\underline{A}\,i : i \geq 0 : f(q(i+1)))] \\
\Rightarrow \{\text{since } [q\,i \vee \neg f(q(i+1))]\} \\
\quad [Z \Rightarrow (\underline{A}\,i : i \geq 0 : q\,i)]
\end{array}
$$

,

hence $(\underline{A}\,i : i \geq 0 : q\,i)$ is a solution of $X : [f X \Rightarrow X]$. Since Q, the strongest solution of $X : [f X \equiv X]$ is —see EWD822— also the strongest solution of $X : [f X \Rightarrow X]$,

$$
\begin{array}{l}
\quad true \\
= \{\text{previous remark}\} \\
\quad [Q \Rightarrow (\underline{A}\,i : i \geq 0 : q\,i)] \\
\Rightarrow \{\text{pred. calc. and } [q\,0 \equiv p]\} \\
\quad [Q \Rightarrow p] \\
= \{\text{pred. calc. and Axiom 1}\} \\
\quad \neg[p \vee Q]
\end{array}
$$

(End of Proof of Theorem 1.)

15 October 1982

drs. C. S. Scholten
Scientific Adviser
Philips Research Laboratories
5600 JA EINDHOVEN
The Netherlands

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