The operational interpretation of extreme solutions

Edsger W. Dijkstra and C.S. Scholten.

For the repetitive construct DO: <u>do</u> B → S <u>od</u>, wp(DO,R) has been defined as the strongest solution of

$$X: [X \equiv (B \vee R) \wedge (\neg B \vee wp(S,X))]$$

and wlp(DO,R) as the weakest solution of

$$X: [X \equiv (B \vee R) \wedge (\neg B \vee wlp(S,X))] \quad ,$$

the two equations being related by

$$[wp(S,X) \equiv wp(S,true) \wedge wlp(S,X)] \quad .$$

From an operational point of view we "know" that an activation of the repetition leads to one of four mutually exclusive courses of events (with respect to some postcondition R)

- the repetition terminates in a final state satisfying R
- the repetition terminates in a final state satisfying ¬R
- the repetition "continues", i.e. leads to an infinite sequence of activations of S
- the repetition "gets stuck", i.e. leads to a non-terminating activation of S.

The purpose of this note is to characterize for each of these four courses of events the initial condition under which it may occur. As a by-product we shall obtain an operational justification of the above definitions of wp(DO,R) and wlp(DO,R) .

* * *

We begin by observing that the postulated dichotomy of final states into those satisfying R and those satisfying ¬R presupposes the existence of what we call "point predicates".

In the sequel p, q, and r are variables of type "point predicate". Their properties are captured by the axioms

$[Q \equiv (\underline{E}p : [p \Rightarrow Q] : p)]$ for any Q (0)

$[p \Rightarrow \neg Q] \equiv \neg[p \Rightarrow Q]$ for any p, Q . (1)

By substituting true for Q, we obtain

from (0) $[(\underline{E}p :: p)]$ (2)
from (1) $\neg[\neg p]$ for any p . (3)

<u>Lemma 0</u> For any bag V of predicates and any point predicate p we have

$$[p \Rightarrow (\underline{E}X : X \ \underline{in}\ V : X)] \equiv (\underline{E}X : X \ \underline{in}\ V : [p \Rightarrow X]) \ .$$

<u>Proof</u>

$\neg[p \Rightarrow (\underline{E}X : X \ \underline{in}\ V : X)]$

$= \{$ (1) and de Morgan $\}$

$[p \Rightarrow (\underline{A}X :: \neg X)]$

$= \{$ pred.calc. $\}$

$$(\underline{A}X:: [p \Rrightarrow \neg X])$$
$$= \{(1) \text{ and de Morgan}\}$$
$$\neg(\underline{E}X: X \underline{\text{in}} V: [p \Rrightarrow X])$$

(End of Proof.)

<u>Lemma 1</u> For any bag V of point predicates we have

$$[(\underline{E}p: p \underline{\text{in}} V: p) \equiv (\underline{A}q: \neg(q \underline{\text{in}} V): \neg q)] \quad .$$

<u>Proof</u>

$$\text{true}$$
$$= \{(2) \text{ and pred. calc}\}$$
$$[(\underline{E}q: \neg(q \underline{\text{in}} V): q) \vee (\underline{E}p: p \underline{\text{in}} V: p)]$$
$$= \{\text{pred. calc. and de Morgan}\}$$
$$[(\underline{A}q: \neg(q \underline{\text{in}} V): \neg q) \Rrightarrow (\underline{E}p: p \underline{\text{in}} V: p)] \quad .$$

$$\text{true}$$
$$= \{\text{pred. calc}\}$$
$$(\underline{A}p,q: p \underline{\text{in}} V \wedge \neg(q \underline{\text{in}} V): \neg[p \equiv q])$$
$$= \{\text{pred. calc.}\}$$
$$(\underline{A}p,q: p \underline{\text{in}} V \wedge \neg(q \underline{\text{in}} V): \neg[p \Rrightarrow q] \vee \neg[q \Rrightarrow p])$$
$$= \{(1)\}$$
$$(\underline{A}p,q: p \underline{\text{in}} V \wedge \neg(q \underline{\text{in}} V): [p \Rrightarrow \neg q] \vee [q \Rrightarrow \neg p])$$
$$= \{\text{pred. calc.; note that } [Q \Rrightarrow \neg P] \equiv [P \Rrightarrow \neg Q]\}$$
$$[(\underline{E}p: p \underline{\text{in}} V: p) \Rrightarrow (\underline{A}q: \neg(q \underline{\text{in}} V): \neg q)] \quad .$$

(End of Proof.)

So much for the point predicates.

* * *

In order to show our heuristics we start by investigating under what circumstances a single execution of S, started in state p, may lead to state q. By virtue of the standard operational interpretation of wlp, we have

$[p \Rightarrow wlp(S, \neg q)] \equiv$ "no execution of S, started in p, leads to q".

Negating both sides, we find

$\neg[p \Rightarrow wlp(S, \neg q)] \equiv$ "there exists an execution of S, started in p, that leads to q".

On account of (1) and the definition of the conjugate, the left-hand side can be rewritten as

$$[p \Rightarrow wlp^*(S, q)] \quad .$$

So much for the relation between p and q for S considered in isolation. In the repetition we have

$[p \Rightarrow B] \equiv$ "in state p, S is started another time".

Combining those two, we get

$[p \Rightarrow B \wedge wlp^*(S, q)] \equiv$ "in $\underline{do}\ B \rightarrow S\ \underline{od}$, state q is a possible successor of state p".

With f defined by $[f X \equiv \neg B \vee wlp(S, X)]$, the left-hand side is $[p \Rightarrow f^* q]$. Note that this f is universally conjunctive.

So much for our heuristics. Our next section explores in abstracto the relation $[p \Rightarrow f^* q]$ for universally conjunctive f.

* * *

With respect to predicate transformer f the relation $\underline{suc}$ (for "successor") between point predicates is defined by

$$q \ \underline{suc} \ p \ \equiv [p \Rightarrow f^*q] \quad \text{for all } p, q \ .$$

Relation $\underline{des}$ (for "descendant") is defined as the reflexive transitive closure of $\underline{suc}$, i.e. the strongest transitive relation satisfying

$$p \ \underline{des} \ p \quad \text{for all } p$$
$$q \ \underline{suc} \ p \Rightarrow q \ \underline{des} \ p \quad \text{for all } p, q \ .$$

(We have refrained from denoting $\underline{des}$ by $\underline{suc}^*$ because the star is already used to denote the conjugate.)

A "descending chain on p" is a sequence of point predicates $q\,i$ $(0 \leq i)$ satisfying

$$[q\,0 \equiv p] \qquad \text{and}$$

$$(\underline{A}\, i :: q\,(i+1) \ \underline{suc} \ q\,i) \ .$$

Note that descending chains may be of finite length; in the last formula the range of i is understood to be such as to encompass all elements of the chain.

We now turn our attention to the equation

$$X: [X \equiv Y \wedge f X] \qquad (4)$$

with universally conjunctive f. (Parameter Y has been introduced for the sake of brevity: our results will only be used with a few very specific choices for Y.)

In the following, gY is defined as the strongest solution of (4) and hY as its weakest. We recall — from EWD849a-4 —

g is unboundedly conjunctive ;
h is universally conjunctive;
$[g(Y \wedge Z) \equiv gY \wedge hZ]$ for all Y, Z . (5)

Our relevant results are captured by the following two theorems:

<u>Theorem 0</u>. For any point predicate p

$$[p \Rightarrow g\ true] \equiv \text{"all descending chains on } p \text{ are finite"} \quad .$$

<u>Theorem 1</u>. For any point predicate p and any predicate Y

$$[p \Rightarrow hY] \equiv (\underline{A}q : q\ \underline{des}\ p : [q \Rightarrow Y]) \quad .$$

<u>Proof of Theorem 0</u> The proof is by showing that in

$$\neg[p \Rightarrow g\ true] \equiv \text{"there exists an infinite descending chain on } p\text{"}$$

each side implies the other.

$\underline{L \Rightarrow R}$

$\neg[p \Rightarrow g\ true]$
$= \{(1)\}$
$[p \Rightarrow \neg g\ true]$
$= \{g\ true \text{ is a solution of (4) with } true \text{ for } Y\}$
$[p \Rightarrow \neg f(g\ true)]$
$= \{\text{definition of conjugate}\}$
$[p \Rightarrow f^*(\neg g\ true)]$
$= \{(0)\}$
$[p \Rightarrow f^*(\underline{E}q : [q \Rightarrow \neg g\ true] : q)]$
$= \{f^* \text{ is universally disjunctive}\}$
$[p \Rightarrow (\underline{E}q : [q \Rightarrow \neg g\ true] : f^* q)]$
$= \{\text{Lemma 0}\}$
$(\underline{E}q : [q \Rightarrow \neg g\ true] : [p \Rightarrow f^* q])$
$= \{(1), \text{definition of } \underline{suc} \text{ and pred.calc.}\}$
$(\underline{E}q : q\ \underline{suc}\ p : \neg[q \Rightarrow g\ true])$.

We conclude that any point predicate solving the equation $x : (\neg[x \Rightarrow g\ true])$ has a successor solving that equation, from which the existence of the infinite descending chain follows.

$\underline{R \Rightarrow L}$ Let $q\,i$ $(i \geq 0)$ be an infinite descending chain on p.

$true$
$= \{\text{definitions of } q\,i \text{ and of } \underline{suc}\}$
$(\underline{A}i : 0 \leq i : [q\,i \Rightarrow f^*(q(i+1))])$
$= \{\text{pred.calc. and definition of conjugate}\}$
$(\underline{A}i : 0 \leq i : [f(\neg q(i+1)) \Rightarrow \neg q\,i])$
$\Rightarrow \{\text{pred.calc.}\}$

$[(\underline{A}i: 0\le i: f(\neg q(i+1))) \Rightarrow (\underline{A}i: 0\le i: \neg qi)]$

$\Rightarrow$ { strengthening the antecedent by "$f(\neg q0)\wedge$" }

$[(\underline{A}i: 0\le i: f(\neg qi)) \Rightarrow (\underline{A}i: 0\le i: \neg qi)]$

$=$ { f is universally conjunctive }

$[f(\underline{A}i:: \neg qi) \Rightarrow (\underline{A}i:: \neg qi)]$

$\Rightarrow$ { g true is the strongest solution of (4) with true for Y ; Knaster-Tarski }

$[g \text{ true} \Rightarrow (\underline{A}i:: \neg qi)]$

$\Rightarrow$ { weakening the consequent and $[q0 \equiv p]$ }

$[g \text{ true} \Rightarrow \neg p]$

$=$ { predicate calculus }

$[p \Rightarrow \neg g \text{ true}]$

$=$ { (1) }

$\neg [p \Rightarrow g \text{ true}]$.

(End of Proof of Theorem 0.)

Proof of Theorem 1

L ⇒ R In view of the definition of des it suffices to prove

$$[p \Rightarrow hY] \Rightarrow [p \Rightarrow Y] \quad \text{and}$$

$$[p \Rightarrow hY] \Rightarrow (\underline{A}q: q \,\underline{\text{suc}}\, p: [q \Rightarrow hY])$$

Since hY is a solution of (4), we have $[hY \Rightarrow Y]$, from which the first one follows. For the second one, let q be a successor of p. We observe

$[p \Rightarrow hY] \wedge \neg [q \Rightarrow hY]$

$=$ { (1) }

$[p \Rightarrow hY] \wedge [q \Rightarrow \neg hY]$

$\Rightarrow$ { hY is a solution of (4), hence $[hY \Rightarrow f(hY)]$ }

$[p \Rightarrow f(hY)] \wedge [q \Rightarrow \neg hY]$
$\Rightarrow$ {$[p \Rightarrow f^* q]$ and f^* is monotonic}
$[p \Rightarrow f(hY)] \wedge [p \Rightarrow f^*(\neg hY)]$
$=$ {definition of conjugate and predicate calculus}
$[\neg p]$
$=$ {(3)}
false.

Hence $[p \Rightarrow hY] \Rightarrow [q \Rightarrow hY]$.

R⇒L. To begin with we define predicate P by

$$[P \equiv (\underline{E}q : q \ \underline{des}\ p : q)] \qquad (6)$$

or

$$[P \equiv (\underline{A}q : \neg(q \ \underline{des}\ p) : \neg q)] \quad , \qquad (7)$$

(6) and (7) being equivalent on account of Lemma 1. Since $p \ \underline{des}\ p$ we conclude from (6)

$$[p \Rightarrow P] \quad . \qquad (8)$$

We shall first prove about P that $[P \Rightarrow fP]$. To this end we observe

true
$=$ {transitivity and definition of des}
$(\underline{A}q,r : r \ \underline{suc}\ q \wedge q \ \underline{des}\ p : r \ \underline{des}\ p)$
$=$ {pred. calc.}
$(\underline{A}q,r : q \ \underline{des}\ p \wedge \neg(r \ \underline{des}\ p) : \neg(r \ \underline{suc}\ q))$
$=$ {definition of suc}
$(\underline{A}q,r : q \ \underline{des}\ p \wedge \neg(r \ \underline{des}\ p) : \neg[q \Rightarrow f^* r])$
$=$ {(1) and definition of conjugate}
$(\underline{A}q,r : q \ \underline{des}\ p \wedge \neg(r \ \underline{des}\ p) : [q \Rightarrow f(\neg r)])$

$= \{$ pred. calc. $\}$

$[(\underline{E}q : q \ \underline{des}\ p : q) \Rightarrow (\underline{A}r : \neg(r \ \underline{des}\ p) : f(\neg r))]$

$= \{ f$ is universally conjunctive $\}$

$[(\underline{E}q : q \ \underline{des}\ p : q) \Rightarrow f(\underline{A}r : \neg(r \ \underline{des}\ p) : \neg r)]$

$= \{ (6)$ and $(7) \}$

$$[P \Rightarrow f P] \qquad . \qquad (9)$$

In order to prove $R \Rightarrow L$ we now observe

$(\underline{A}q : q \ \underline{des}\ p : [q \Rightarrow Y])$

$= \{$ pred. calc. $\}$

$[(\underline{E}q : q \ \underline{des}\ p : q) \Rightarrow Y]$

$= \{ (6) \}$

$[P \Rightarrow Y]$

$= \{ (9) \}$

$[P \Rightarrow Y \wedge f P]$

$\Rightarrow \{$ definition of h and Knaster-Tarski $\}$

$[P \Rightarrow h Y]$

$\Rightarrow \{ (8) \}$

$[p \Rightarrow h Y]$.

(End of Proof of Theorem 1.)

* * *

After the above exploration of the relation $q \ \underline{suc}\ p$ —i.e. $[p \Rightarrow f^* q]$— we shall apply our results to equation (4) with f given by

$$[f X \equiv \neg B \vee wlp(S, X)] \qquad ;$$

we recall that with this choice for f relation $q \ \underline{suc}\ p$ admits of the interpretation "in $\underline{\text{do}}\ B \rightarrow S\ \underline{\text{od}}$, state q is a possible successor of state p".

<u>Remark</u>. Note that with this choice for f, equation (4) with $[Y \equiv (B \vee R) \wedge (\neg B \vee wp(S, true))]$ yields our very first equation, of which $wp(DO, R)$ had been defined as the strongest solution; with $[Y \equiv B \vee R]$, equation (4) yields our second equation, of which $wlp(DO, R)$ had been defined as the weakest solution. (End of Remark.)

With the above operational interpretation of $\underline{suc}$, Theorem 0 enables us to give an operational interpretation of the predicate $g\ true$:

> $g\ true$ characterizes all (initial) states for which DO will not "continue" - i.e. will not lead to an infinite sequence of activations of S.

Theorem 1 enables us to give an operational interpretation to $h\ Y$ with $[Y \equiv \neg B \vee wp(S, true)]$. With this choice for Y, $[q \Rightarrow Y]$ means that in state q, either DO has terminated or the activation of S is guaranteed to terminate. From Theorem 1 we now see:

> $h\ (\neg B \vee wp(S, true))$ characterizes all (initial) states for which DO will not "get stuck", i.e. will not lead to a nonterminating activation of S.

Our next choice for Y is $[Y \equiv B \vee R]$. With this choice for Y, $[q \Rightarrow Y]$ means that in state q, DO has not terminated or has terminated with R holding. From Theorem 1 we now see:

> $h(B \vee R)$ characterizes all (initial) states for which DO will not terminate with $\neg R$.

This operational interpretation of $h(B \vee R)$ justifies its identification with $wlp(DO, R)$. (See earlier Remark.)

The joint exclusion of continuing, getting stuck, and termination with $\neg R$ equivales guaranteed termination with R. From the above we see that the corresponding initial states are characterized by

$$g\ true \ \wedge\ h(\neg B \vee wp(S, true)) \ \wedge\ h(B \vee R).$$

From (5) we conclude that the above equivales

$$g((B \vee R) \wedge (\neg B \vee wp(S, true))) \quad ;$$

its operational interpretation justifies its identification with $wp(DO, R)$. (See earlier Remark.)

For the sake of completeness we remark

- $h\,B$ characterizes all (initial) states for which DO will not terminate
- $g\,B$ characterizes all (initial) states for which DO will get stuck
- $h(B \wedge wp(S, true))$ characterizes all (initial)

states for which DO will continue.

The well-known relation

$$[wp(DO,R) \equiv wlp(DO,R) \wedge wp(DO,true)]$$

takes on account of the above the form

$$[g((B \vee R) \wedge (\neg B \vee wp(S,true))) \equiv h(B \vee R) \wedge g(\neg B \vee wp(S,true))] \quad ,$$

which is confirmed by (5).

Finally we check that it is impossible to guarantee nontermination and termination, i.e. that $[hB \wedge wp(DO,true) \equiv false]$, or, by the above and (5), that $[g(B \wedge wp(S,true)) \equiv false]$. Substitution of g's argument for Y in (4) yields

$$X: [X \equiv B \wedge wp(S,true) \wedge (\neg B \vee wlp(S,X))]$$

or

$$X: [X \equiv B \wedge wp(S,X)] \quad ,$$

which has indeed false as its strongest solution.

6 April 1984

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