Weakest preconditions, liberal and not

by Edsger W. Dijkstra and C. S. Scholten

The purpose of this note is to show how for the weakest liberal precondition a predicate transformer wlp can be defined such that

(0) $\qquad [(wlp(S,Q) \wedge wp(S,T)) = wp(S,Q)]$ for all Q .

Since wlp will be defined recursively over the syntax, the validity of (0) will be proved by induction over the syntax. For the syntax we take the one of the language fragment from "A Discipline of Programming". The reader is supposed to be familiar with EWD813.

* * *

By way of preparation we shall prove some simple theorems about predicate transformer pairs (f, g), satisfying

(1) $\qquad [P \Rightarrow fQ] = [gP \Rightarrow Q]$ for all P and Q .

(Equation (6) of EWD813.) The theorems deal with new solutions of (1) constructed from previous ones; we need them in view of the recursive definitions of wlp .

<u>Lemma 0</u>. Let $(f0, g0)$ and $(f1, g1)$ be solutions of (1); then $(f0 \circ f1, g1 \circ g0)$ is also a solution of (1). (Here "$\circ$" is used to denote functional composition.)

<u>Proof</u>. For all P and Q we have

$$[P \Rightarrow (f0 \circ f1)\, Q]$$
$= \{\text{definition of } "\circ"\}$
$$[P \Rightarrow f0\, (f1\, Q)]$$
$= \{ (f0, g0) \text{ satisfies } (1)\}$
$$[g0\, P \Rightarrow f1\, Q]$$
$= \{ (f1, g1) \text{ satisfies } (1)\}$
$$[g1\, (g0\, P) \Rightarrow Q]$$
$= \{\text{definition of } "\circ"\}$
$$[(g1 \circ g0)\, P \Rightarrow Q]$$. (End of Proof.)

<u>Lemma 1</u>. Let (fi, gi) be solutions of (1) for all i from a set of natural numbers; then (f, g) is a solution of (1) with f and g defined by

$$[f\,Q = (\underline{A}i :: fi\; Q)] \quad \text{for all } Q$$
$$[g\,P = (\underline{E}i :: gi\; P)] \quad \text{for all } P \quad .$$

<u>Proof</u>. For all P and Q we have

$$[P \Rightarrow f\,Q]$$
$= \{\text{definition of } f\}$
$$[P \Rightarrow (\underline{A}i :: fi\; Q)]$$
$= \{\text{predicate calculus}\}$
$$[(\underline{A}i :: P \Rightarrow fi\; Q)]$$
$= \{\text{predicate calculus}\}$
$$(\underline{A}i :: [P \Rightarrow fi\; Q])$$
$= \{ (fi, gi) \text{ satisfies } (1)\}$
$$(\underline{A}i :: [gi\; P \Rightarrow Q])$$
$= \{\text{predicate calculus}\}$
$$[(\underline{A}i :: gi\; P \Rightarrow Q)]$$
$= \{\text{predicate calculus}\}$
$$[(\underline{E}i :: gi\; P) \Rightarrow Q]$$

$= \{\text{definition of } g\}$
$[gP \Rightarrow Q]$ (End of Proof.)

<u>Lemma 2</u>. Let (f,g) satisfy (1); then (fb, gb) satisfies (1) with fb and gb defined by

$$[fb\ Q = (\neg B \vee fQ)] \text{ for all } Q$$
$$[gb\ P = g(B \wedge P)] \text{ for all } P$$

where B is an arbitrary predicate.

<u>Proof</u>. For all P and Q we have

$[P \Rightarrow fb\ Q]$
$= \{\text{definition of } fb\}$
$[P \Rightarrow (\neg B \vee fQ)]$
$= \{\text{predicate calculus}\}$
$[(B \wedge P) \Rightarrow f\,Q]$
$= \{(f,g) \text{ satisfies } (1)\}$
$[g(B \wedge P) \Rightarrow Q]$
$= \{\text{definition of } gb\}$
$[gb\ P \Rightarrow Q]$ (End of Proof.)

<u>Lemma 3</u>. Let (f,g) satisfy (1); then (fb, gb) satisfies (1) with fb and gb defined by

$$[fb\ Q = f(B \vee Q)] \text{ for all } Q$$
$$[gb\ P = (\neg B \wedge gP)] \text{ for all } P$$

where B is an arbitrary predicate.

The proof of Lemma 3 is so similar to that of Lemma 2 that it is left to the reader.

We introduce for an arbitrary predicate transformer f the notation f^n defined by

f^0 is the identity and $f^{n+1} = f \circ f^n$ for $n \geq 0$.

As a corollary of Lemmata 0, 1, and 3 we formulate

Corollary 0. Let (f, g) satisfy (1); then (fb, gb) satisfies (1) with fb and gb defined by

$$[fb\ Q = (\underline{A}i: i \geq 0: f^i(B \vee Q))] \quad \text{for all } Q$$
$$[gb\ P = (\neg B \wedge (\underline{E}i: i \geq 0: g^i P))] \quad \text{for all } P$$

where B is an arbitrary predicate.

* * *

For the language fragment from "A Discipline of Programming" we shall define a weakest liberal precondition wlp . As we go along, we shall show the validity of (0) and, in view of EWD813, that $wlp(S, ?)$ is universally conjunctive, so that a strongest postcondition $sp(?, S)$ corresponds to it. For the sake of completeness we repeat their relation

(2) $[P \Rightarrow wlp(S, Q)] = [sp(P, S) \Rightarrow Q]$ for all P, Q and all S.

abort. $[wlp(abort, Q)]$ for all Q . In view of $[\neg\ wp(abort, Q)]$, for all Q, (0) is satisfied. With the strongest postcondition defined by $[\neg sp(P, abort)]$ for all P, (2) is satisfied. By EWD813, Lemma 11, we conclude that $wlp(abort, ?)$ is universally conjunctive (and $sp(?, abort)$ is universally disjunctive).

skip. $[wlp(skip, Q) = Q]$ and $[sp(P, skip) = P]$ for all P and Q. Relations (0) and (2) are obviously satisfied.

assignment. Confining ourselves, as in "A Discipline of Programming" to total expressions E, we define $[wlp(\text{"}x := E\text{"}, Q) = Q^x_E]$ for all Q. From predicate calculus we know that $wlp(\text{"}x := E\text{"}, ?)$ is universally conjunctive, so that $sp(?, \text{"}x := E\text{"})$ exists; by EWD813, Lemma 12,

for all P: $sp(P, \text{"}x := E\text{"})$ is the strongest solution of
$[P \Rightarrow X^x_E]$.

In this case we abstain from a more explicit formulation.

concatenation. We define
$$[wlp(\text{"}S0; S1\text{"}, Q) = wlp(S0, wlp(S1, Q))] \quad \text{for all } Q .$$

In order to prove that (0) is satisfied, we remark that we have (for all S0 and S1 and) for all X and Q:

$$[X = (wlp(\text{"}S0; S1\text{"}, Q) \wedge wp(\text{"}S0; S1\text{"}, T))]$$
$$= \{\text{definitions of concatenation}\}$$
$$[X = (wlp(S0, wlp(S1, Q)) \wedge wp(S0, wp(S1, T)))]$$
$$= \{S0 \text{ is assumed to satisfy (0)}\}$$
$$[X = (wlp(S0, wlp(S1, Q)) \wedge wlp(S0, wp(S1, T)) \wedge wp(S0, T))]$$
$$= \{wlp(S0, ?) \text{ is assumed to be conjunctive}\}$$
$$[X = (wlp(S0, wlp(S1, Q) \wedge wp(S1, T)) \wedge wp(S0, T))]$$
$$= \{S1 \text{ is assumed to satisfy (0)}\}$$

$$[X = (wlp(S0, wp(S1, Q)) \wedge wp(S0, T))]$$
$$= \{S0 \text{ is assumed to satisfy } (0)\}$$
$$[X = wp(S0, wp(S1, Q))]$$
$$= \{\text{definition of concatenation}\}$$
$$[X = wp(\text{"}S0; S1\text{"}, Q)]$$

From the equality of the first and the last line we conclude that (0) is satisfied. From Lemma 0 we conclude that the strongest postcondition defined by

$$[sp(P, \text{"}S0; S1\text{"}) = sp(sp(P, S0), S1)]$$

satisfies (2). Hence $wlp(\text{"}S0;S1\text{"}, ?)$ is universally conjunctive.

alternative construct. For the statement IF of the form

$$IF: \quad \mathbf{if}\ B0 \rightarrow S0\ [] \ldots []\ Bn \rightarrow Sn\ \mathbf{fi}$$

we define

$$[wlp(IF, Q) = (\underline{A}i : 0 \le i \le n : \neg Bi \vee wlp(Si, Q))] \quad \text{for all } Q\,.$$

In order to prove that (0) is satisfied, we observe for all X, etc. — with, as usual, $[BB = (\underline{E}i : 0 \le i \le n : Bi)]$ — under omission of i's range

$$[X = (wlp(IF, Q) \wedge wp(IF, T))]$$
$$= \{\text{definitions of the alternative constructs}\}$$
$$[X = ((\underline{A}i :: \neg Bi \vee wlp(Si, Q)) \wedge BB \wedge (\underline{A}i :: \neg Bi \vee wp(Si, T)))]$$
$$= \{\text{predicate calculus}\}$$
$$[X = (BB \wedge (\underline{A}i :: \neg Bi \vee (wlp(Si, Q) \wedge wp(Si, T))))]$$
$$= \{\text{the } Si \text{ are assumed to satisfy } (0)\}$$
$$[X = (BB \wedge (\underline{A}i :: \neg Bi \vee wp(Si, Q)))]$$
$$= \{\text{definition of the alternative construct}\}$$
$$[X = wp(IF, Q)] \quad .$$

Hence, (0) is satisfied. From Lemmata 1 and 2 it follows that the strongest postcondition satisfying (2) exists and is given by

$[sp(P, IF) = (\underline{E}i : 0 \leq i \leq n : sp(Bi \wedge P, Si))]$.

Hence $wlp(IF, ?)$ is universally conjunctive.

repetitive construct. For the statement DO of the form

DO: $\quad$ do $B0 \rightarrow S0 \, [] \ldots [] \, Bn \rightarrow Sn$ od

we define, in terms of the corresponding IF,

$$[wlp(DO, Q) = (\underline{A}i : i \geq 0 : kq^i \, T)]$$

where the predicate transformer kq is defined by

$$[kq\,X = (BB \vee Q) \wedge wlp(IF, X)] \quad \text{for all } Q \text{ and } X .$$

Note that, in view of $[BB \vee wlp(IF, X)]$ for all X, predicate transformer kq satisfies

$$[kq\,X = (\neg BB \wedge Q) \vee (BB \wedge wlp(IF, X))] \quad \text{for all } X.$$

Analogously to the above we rewrite the traditional definition of wp

$$[wp(DO, Q) = (\underline{E}i : i \geq 0 : hq^i \, F)]$$
$$[wp(DO, T) = (\underline{E}i : i \geq 0 : ht^i \, F)]$$

where the predicate transformers hq and ht are defined by

$[hq\ X = (\neg BB \wedge Q) \vee wp(IF, X)]$ for all Q and X
$[ht\ X = \neg BB \vee wp(IF, X)]$ for all X .

We derive for all X, Y, and Z

$[Z = kq\ X \wedge ht\ Y]$
$=$ {definitions of kq and ht}
$[Z = ((\neg BB \wedge Q) \vee (BB \wedge wlp(IF, X))) \wedge (\neg BB \vee wp(IF, Y))]$
$=$ {predicate calculus}
$[Z = (\neg BB \wedge Q) \vee (BB \wedge wlp(IF, X) \wedge wp(IF, Y))]$
$=$ {since $[wp(IF, Y) \Rightarrow BB]$}
$[Z = (\neg BB \wedge Q) \vee (wlp(IF, X) \wedge wp(IF, Y))]$
$=$ {$[wp(IF, Y) \Rightarrow wp(IF, T)]$}
$[Z = (\neg BB \wedge Q) \vee (wlp(IF, X) \wedge wp(IF, T) \wedge wp(IF, Y))]$
$=$ {(0) is satisfied for $S = IF$}
$[Z = (\neg BB \wedge Q) \vee (wp(IF, X) \wedge wp(IF, Y))]$
$=$ {wp is conjunctive}
$[Z = (\neg BB \wedge Q) \vee (wp(IF, X \wedge Y))]$
$=$ {definition of hq}
$[Z = hq\ (X \wedge Y)]$, hence

(3) $[kq\ X \wedge ht\ Y = hq\ (X \wedge Y)]$ for all X, Y .

We can now prove

<u>Lemma 4</u>. For all natural i

$$[kq^i\ X \wedge ht^i\ Y = hq^i\ (X \wedge Y)] \quad \text{for all } X, Y .$$

<u>Proof</u>. The Lemma being correct for $i = 0$, we proceed with a proof by mathematical induction by observing for all X, Y, and Z

$[Z = kq^{i+1} X \wedge ht^{i+1} Y]$
= {definition of iterated functional composition}
$[Z = kq(kq^i X) \wedge ht(ht^i Y)]$
= {(3)}
$[Z = hq(kq^i X \wedge ht^i Y)]$
= {induction hypothesis}
$[Z = hq(hq^i(X \wedge Y))]$
= {definition of iterated functional composition}
$[Z = hq^{i+1}(X \wedge Y)]$. (End of Proof.)

Applying Lemma 4 to the case $[X] \wedge [\neg Y]$ we obtain

(4) $[kq^i T \wedge ht^i F = hq^i F]$ for all natural i ,

from which we immediately derive

true
= {(4)}
$[(\underline{E}j : j \geq 0 : (\underline{A}i : i \geq j : kq^i T \wedge ht^i F)) = (\underline{E}j : j \geq 0 : (\underline{A}i : i \geq j : hq^i F))]$
= {predicate calculus}
$[(\underline{E}j : j \geq 0 : (\underline{A}i : i \geq j : kq^i T)) \wedge (\underline{E}j : j \geq 0 : (\underline{A}i : i \geq j : ht^i F)) =$
$(\underline{E}j : j \geq 0 : (\underline{A}i : i \geq j : hq^i F))]$
= {see below *)}
$[(\underline{A}i : i \geq 0 : kq^i T) \wedge (\underline{E}i : i \geq 0 : ht^i F) = (\underline{E}i : i \geq 0 : hq^i F)]$
= {definitions of wlp(DO, Q), wp(DO, T), and wp(DO, Q)}
$[wlp(DO, Q) \wedge wp(DO, T) = wp(DO, Q)]$.

Hence, (0) is satisfied for $S = DO$.

*) The expression $(\underline{E}j : j \geq 0 : (\underline{A}i : i \geq j : X_i))$ equals

a) $(\underline{E}i : i \geq 0 : X_i)$ if $(\underline{A}i : i \geq 0 : [X_i \Rightarrow X_{i+1}])$ holds, in which case we might call the X_i "a weakening sequence",

b) $(\underline{A}i: i \geq 0: X_i)$ if $(\underline{A}i: i \geq 0: [X_{i+1} \Rightarrow X_i])$ holds, in which case we might call the X_i "a strengthening sequence".

In view of the monotonicity of the predicate transformer kq the predicates $kq^i T$ form a strengthening sequence; in view of the monotonicity of the predicate transformers ht and hq, the predicates $ht^i F$ and $hq^i F$ form weakening sequences. (End of *).)

<u>Remark</u> Had we so desired, we could have defined

$$[wlp(DO, Q) = (\underline{E}j: j \geq 0: (\underline{A}i: i \geq j: kq^i T))]$$

$$[wp(DO, Q) = (\underline{E}j: j \geq 0: (\underline{A}i: i \geq j: hq^i F))] \quad .$$

We leave it to the reader to decide whether he thinks these more symmetric definitions misleading or illuminating. (End of Remark.)

Remains to be shown that the predicate transformer wlp(DO,?) is universally conjunctive. This follows directly from Corollary 0 thanks to the following alternative expression for wlp(DO, Q)

$$[wlp(DO, Q) = (\underline{A}i: i \geq 0: wlp(IF^i, BB \vee Q))] \quad .$$

This follows from the fact that for all natural i

$$(5) \quad [kq^i T = (\underline{A}j: 0 \leq j < i: wlp(IF^j, BB \vee Q))] \quad .$$

<u>Proof</u> Relation (5) obviously holds for $i = 0$. We proceed by mathematical induction. We observe for all Z

$$[Z = kq^{i+1} T]$$

= {definition of iterated functional composition}
  $[Z = kq\,(kq^i T)]$
= {definition of kq}
  $[Z = (BB \vee Q) \wedge wlp(IF, kq^i T)]$
= {induction hypothesis (5)}
  $[Z = (BB \vee Q) \wedge wlp(IF, (\underline{A}j: 0 \le j < i: wlp(IF^j, BB \vee Q)))]$
= {$wlp(IF, ?)$ is conjunctive}
  $[Z = (BB \vee Q) \wedge (\underline{A}j: 1 \le j < i+1: wlp(IF^j, BB \vee Q))]$
= {$[BB \vee Q = wlp(IF^0, BB \vee Q)]$}
  $[Z = (\underline{A}j: 0 \le j < i+1: wlp(IF^j, BB \vee Q))]$. (End of Proof.)

Finally we conclude from Corollary 0

$$[sp(P,DO) = (\neg BB \wedge (\underline{E}i: i \ge 0: sp(P, IF^i)))] \quad \text{for all } P .$$

* * *

<u>Critical remarks</u>. We are not too satisfied with the large number of competing expressions for $wlp(DO, Q)$ that have been used in the above, a baroqueness, which makes this note unfit for publication.

Furthermore, its title is not entirely appropriate; the note deals with strongest postconditions and expressions for them as well. We could have confined ourselves to the definition of wlp ; the proof of (0) would be very much like the above, the proofs of wlp's universal conjunctivity would be given directly, and the existence of a strongest postcondition would, hence, have been settled. The expressions for the strongest postconditions could then have been delegated to an appendix. Though more disentangled, such a text would probably have been longer.

As a piece of positive criticism we note that the subsequent lines of our proofs are <u>all</u> connected by equality signs, thus giving rise to strong results. The experience is a further incentive to use equality instead of implication wherever possible. (End of Critical Remarks.)

* * *

In the past we have experimented with different concepts for the strongest postcondition, viz.

$sp'(P,S)$ is the strongest predicate X satisfying
$$[P \Rightarrow wp(S,X)]$$

$sp''(P,S)$ is the strongest predicate X satisfying
$$[P \wedge wp(S,T) \Rightarrow wp(S,X)] \quad .$$

The experiments failed: sp' is not a total function and for sp'' concatenation did not correspond to functional composition.

22 April 1982

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

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