About predicate transformers in general

by Edsger W. Dijkstra and C.S. Scholten

Considerations about the relation between "weakest liberal preconditions" and "strongest postconditions" lead to some very general theory about predicate transformers.

In the following P and Q will stand for total predicates defined on a possibly infinite state space; the predicate T is defined to be true in all states, and the predicate F is defined to be false in all states. Universal quantification of a predicate over all states will be denoted by surrounding that predicate by square brackets. This convention allows us to use the logical connectives ($\neg, \wedge, \vee, \Rightarrow, =, \neq$) to construct predicates from predicates, e.g. $P=Q$ is a predicate —true in those and only those states in which P and Q have equal values—, whereas $[P=Q]$ is a boolean —true if and only if in each state P and Q have equal values— .

Furthermore, f and g will stand for predicate transformers, i.e. total functions from predicates to predicates. Application of a predicate transformer will be denoted by juxtaposition, e.g. fP ; functional application has the highest priority.

Let f and g be two predicate transformers such that

(0) $[P \vee fQ] = [Q \vee gP]$ for all P and Q .

Such predicate transformers exist, e.g both equal to the identity transformation, or $[fQ = T]$ and $[gP = T]$ for all P and Q. Note that equation (0) is symmetric in f and g.

<u>Lemma 0</u>. Equation (0) defines a pairing for (some) predicate transformers, i.e. for any f equation (0) admits of at most 1 solution g.

<u>Proof</u>. Let the pairs $(f, g0)$ and $(f, g1)$ both satisfy equation (0), i.e.

$$[P \vee fQ] = [Q \vee g0\,P] \quad \text{for all } P \text{ and } Q$$
$$[P \vee fQ] = [Q \vee g1\,P] \quad \text{for all } P \text{ and } Q \; .$$

Hence

$$[Q \vee g0\,P] = [Q \vee g1\,P] \quad \text{for all } P \text{ and } Q \; .$$

On account of Lemma 1 we conclude $[g0\,P = g1\,P]$ for all P. (End of Proof.)

<u>Lemma 1</u>. From $[Q \vee P0] = [Q \vee P1]$ for all Q follows $[P0 = P1]$.

<u>Proof</u>. Substitution of $\neg P0$ for Q yields $[\neg P0 \vee P1]$; substitution of $\neg P1$ for Q yields $[\neg P1 \vee P0]$. Hence $[P0 = P1]$. (End of Proof.)

Before proceeding we introduce some terminology. A predicate transformer f satisfying

$$(1) \qquad [f(\underline{A}Q: Q \in S: Q) = (\underline{A}Q: Q \in S: fQ)]$$

for all finite and non-empty sets S of predicates is called "conjunctive". Note that, in order to prove that f is conjunctive, it suffices to prove that f satisfies

$$[f(Q0 \wedge Q1) = (fQ0 \wedge fQ1)] \quad \text{for all } Q0, Q1 .$$

A predicate transformer f satisfying (1) for <u>all</u> sets S is called "universally conjunctive", which is therefore a stronger property than just conjunctive. Note that for a universally conjunctive f the property $[fT]$ holds.

<u>Lemma 2.</u> A conjunctive predicate transformer f is monotonic, i.e. satisfies

$$[P \vee Q] \Rightarrow [\neg f(\neg P) \vee fQ] \quad \text{for all } P \text{ and } Q .$$

(A more usual formulation of monotonicity is

$$[P \Rightarrow Q] \Rightarrow [fP \Rightarrow fQ] \quad \text{for all } P \text{ and } Q .)$$

<u>Proof</u> $\quad [P \vee Q]$

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

$\quad [(\neg P \wedge Q) = \neg P]$

$\Rightarrow \{f \text{ is a function}\}$

$$[f(\neg P \wedge Q) = f(\neg P)]$$
$$= \{f \text{ is conjunctive}\}$$
$$[(f(\neg P) \wedge f\,Q) = f(\neg P)]$$
$$= \{\text{predicate calculus}\}$$
$$[\neg f(\neg P) \vee f\,Q] \quad .$$

(End of Proof.)

In the formulation of Lemma 0 we said "some" and "at most"; these were no idle precautions, as the next Lemma shows.

<u>Lemma 3</u> Predicate transformers that satisfy (0) are universally conjunctive.

<u>Proof</u>. Let (f, g) satisfy (0); for reasons of symmetry it suffices to show that f is universally conjunctive. For all P and all S we have

$$[P \vee f(\underline{A}\,Q : Q \in S : Q)]$$
$$= \{\text{on account of } (0)\}$$
$$[(\underline{A}\,Q : Q \in S : Q) \vee g\,P]$$
$$= \{\text{predicate calculus}\}$$
$$[(\underline{A}\,Q : Q \in S : Q \vee g\,P)]$$
$$= \{\text{predicate calculus}\}$$
$$(\underline{A}\,Q : Q \in S : [Q \vee g\,P])$$
$$= \{\text{on account of } (0)\}$$
$$(\underline{A}\,Q : Q \in S : [P \vee f\,Q])$$
$$= \{\text{predicate calculus}\}$$
$$[(\underline{A}\,Q : Q \in S : P \vee f\,Q)]$$

$= \{\text{predicate calculus}\}$
$[P \vee (\underline{A}\, Q : Q \in S : f Q)]$

The first and last lines being equal for all P and all S, application of Lemma 1 completes the proof. (End of Proof.)

The next Lemma can be viewed as the inverse of the previous one.

<u>Lemma</u> 4: For universally conjunctive f the pair (f, g) satisfies (0) with g defined by

for all P: $\quad [g P = (\underline{E}\, X : [P \vee f X] : \neg X)]$.

<u>Proof</u>. $[Q \vee g P]$
$= \{\text{because } [([P \vee f Q] \wedge \neg Q) \Rightarrow g P]\}$
$[Q \vee g P \vee ([P \vee f Q] \wedge \neg Q)]$
$= \{\text{predicate calculus}\}$
$[Q \vee g P \vee [P \vee f Q]]$
$= \{\text{predicate calculus}\}$
$[Q \vee g P] \vee [P \vee f Q]$, hence

(2) $\quad [P \vee f Q] \Rightarrow [Q \vee g P] \quad$ for all P and Q .

$[Q \vee g P]$
$\Rightarrow \{\text{on account of Lemma 2}\}$
$[f Q \vee \neg f(\neg g P)]$
$= \{\text{definition of } g \text{ and de Morgan}\}$

$$
\begin{aligned}
& [f\,Q \vee \neg f(\underline{A}\,X : [P \vee fX] : X)] \\
= \; & \{f \text{ is universally conjunctive and de Morgan}\} \\
& [f\,Q \vee (\underline{E}\,X : [P \vee fX] : \neg fX)] \\
\Rightarrow \; & \{\text{predicate calculus}\} \\
& [f\,Q \vee (\underline{E}\,X : [P \vee fX] : \neg fX \wedge \neg P) \vee P] \\
= \; & \{\text{predicate calculus, de Morgan in particular}\} \\
& [f\,Q \vee P] \quad , \text{ hence}
\end{aligned}
$$

(3) $[Q \vee gP] \Rightarrow [P \vee fQ]$ for all P and Q.

From (2) and (3) follows that the pair (f,g) satisfies (0).
(End of Proof.)

Besides the above we derive directly

<u>Lemma 5.</u> For a pair (f,g) satisfying (0), we have for all P: gP is the weakest solution of $[P \vee f(\neg X)]$, i.e.:
(i) $[P \vee f(\neg gP)]$
(ii) $[P \vee f(\neg Q)] \Rightarrow [Q \Rightarrow gP]$ for all Q.

<u>Proof</u> (i) Substitution of $\neg gP$ for Q in (0) yields $[P \vee f(\neg gP)] = [T]$.
(ii) Substituting $\neg Q$ for Q in (0) suffices on account of $[(Q \Rightarrow gP) = (\neg Q \vee gP)]$.
(End of Proof.)

Combining the last two lemmata we conclude that for universally conjunctive f the equation $[P \vee fX]$ in

X has a strongest solution.

* * *

For predicate transformer f its "conjugate" f^* is defined by

$$[f^*P = \neg f(\neg P)] \quad \text{for all } P \quad .$$

Obviously, the conjugate of f^* is f.

A predicate transformer f satisfying

$$(4) \quad [f\,(\underline{E}\,Q: Q \in S: Q) = (\underline{E}\,Q: Q \in S: f\,Q)]$$

for all finite and non-empty sets S of predicates is called "disjunctive". Note that, in order to prove that f is disjunctive, it suffices to prove that f satisfies

$$[f\,(Q0 \vee Q1) = (f\,Q0 \vee f\,Q1)] \quad \text{for all } Q0, Q1 \quad .$$

A predicate transformer f satisfying (4) for all sets S is called "universally disjunctive", which is therefore a stronger property than just disjunctive. Note that for a universally disjunctive f the property $[f\,F = F]$ holds.

We observe for any predicate transformer f and any set S of predicates

$$[f\,(\underline{A}\,Q: Q \in S: Q) = (\underline{A}\,Q: Q \in S: f\,Q)]$$

$$
\begin{array}{l}
= \{\text{definition of } f^* \text{ and de Morgan}\} \\
\quad [\neg f^*(\underline{E}Q : Q \in S : \neg Q) = (\underline{A}Q : Q \in S : \neg f^*(\neg Q))] \\
= \{\text{negation of both sides and de Morgan}\} \\
\quad [f^*(\underline{E}Q : Q \in S : \neg Q) = (\underline{E}Q : Q \in S : f^*(\neg Q))] \\
= \{\text{introducing } S^* \text{ defined by } (\underline{A}X :: (\neg X) \in S^* = X \in S)\} \\
\quad [f^*(\underline{E}Q : Q \in S^* : Q) = (\underline{E}Q : Q \in S^* : f^* Q)]
\end{array}
$$

where S and S^* are of equal cardinality. From the equality of the first and the last line in the above and the equal cardinalities of S and S^* we conclude

<u>Lemma 6</u>. For any predicate transformer f we have

$$(f \text{ is conjunctive}) = (f^* \text{ is disjunctive}) \quad .$$

<u>Lemma 7</u>. For any predicate transformer f we have

$$(f \text{ is universally conjunctive}) = (f^* \text{ is universally disjunctive}) \; .$$

Expressing in (0) f and g in terms of their conjugates we obtain

$$[P \vee \neg f^*(\neg Q)] = [Q \vee \neg g^*(\neg P)] \quad \text{for all } P \text{ and } Q$$

or, replacing P and Q by their negations and applying de Morgan

$$[(P \wedge f^* Q) = F] = [(Q \wedge g^* P) = F] \quad \text{for all } P \text{ and } Q \; .$$

Consider now a pair of predicate transformers (f, g) satisfying

(5) $[(P \wedge fQ) = F] = [(Q \wedge gP) = F]$ for all P and Q .

We derive from the above and Lemma 3

<u>Lemma 8</u>. Predicate transformers that satisfy (5) are universally disjunctive.

We derive from the above and Lemma 4

<u>Lemma 9</u>. For universally disjunctive f the pair (f, g) satisfies (5) with g defined by

for all P: $[gP = (\underline{A}X : [(P \wedge fX) = F] : \neg X)]$.

We derive from the above and Lemma 5

<u>Lemma 10</u>. For a pair (f, g) satisfying (5), we have for all P: gP is the strongest solution of

$[(P \wedge f(\neg X)) = F]$

i.e. (i) $[(P \wedge f(\neg gP)) = F]$

(ii) $[(P \wedge f(\neg Q)) = F] \Rightarrow [gP \Rightarrow Q]$ for all Q .

<u>Note</u>. Expression $[(P \wedge fQ) = F]$ can also be written as $[\neg(P \wedge fQ)]$. (End of Note.)

Expressing, finally, in (0) only g in terms of its conjugate, we are similarly led to the equation

$$(6) \quad [P \Rightarrow fQ] = [gP \Rightarrow Q] \quad \text{for all } P \text{ and } Q .$$

Note that, in contrast to (0) and (5), equation (6) is <u>not</u> symmetric in f and g. We summarize the results in Lemma 11, 12, and 13:

<u>Lemma 11</u>. Of any pair (f,g) of predicate transformers satisfying (6), f is universally conjunctive and g is universally disjunctive.

<u>Lemma 12</u>. For universally conjunctive f, the pair (f,g) satisfies (6) with g defined by

for all P: $[gP = (\underline{A}X : [P \Rightarrow fX] : X)]$;

for all P: gP is the strongest solution of $[P \Rightarrow fX]$.

<u>Lemma 13</u>. For universally disjunctive g, the pair (f,g) satisfies (6) with f defined by

for all Q: $[fQ = (\underline{E}X : [gX \Rightarrow Q] : X)]$;

for all Q: fQ is the weakest solution of $[gX \Rightarrow Q]$.

*　　*
*

Now it is time to tie in with our introductory remark, which referred to weakest liberal preconditions and strongest postconditions.

Let "$wlp(S,Q)$" denote the weakest condition on the initial state such that firing S is guaranteed not to establish $\neg Q$ (i.e. S establishes Q or fails to terminate). Note that $wlp(S,?)$ is a total predicate transformer and that $[wlp(S,T)]$ holds for all statements S.

Let "$sp(P,S)$" denote the strongest assertion guaranteed to be valid upon completion when S has been fired in an initial state satisfying P. Note that $sp(?,S)$ is a total predicate transformer and that $[\neg sp(F,S)]$ holds for all statements S.

With the above definitions

$$[P \Rightarrow wlp(S,Q)] = [sp(P,S) \Rightarrow Q] \quad \text{for all } P, Q$$

is sweetly reasonable: the truth of the left-hand side is the assertion that the firing of S in an initial state satisfying P will either establish Q or lead to nontermination, the truth of the right-hand side is the assertion that the firing of S in an initial state satisfying P will, upon completion, establish Q.

The above relation, however, is of form (6). As a result we conclude from Lemma 11 that $wlp(S,?)$ is universally conjunctive and sp(?, S) is universally disjunctive. From Lemma 12 we conclude

for all P: sp(P,S) is the strongest solution of $[P \Rightarrow wlp(S,X)]$.

From Lemma 13 we conclude

for all Q: wlp(S,Q) is the weakest solution of $[sp(X,S) \Rightarrow Q]$.

Reservation. Our uninhibited quantification "for all P and Q" is a reason for some concern. (End of Reservation.)

17 March 1982

drs. C.S. Scholten
Philips Research Laboratories
5600 MD EINDHOVEN
the Netherlands

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