A sequel to EWD859

by C.S. Scholten and Edsger W. Dijkstra.

A notational comment

The formulation of (13) and (14) in Theorem 0 of EWD859 is in terms of two functions p and q; the first one is predicate-valued, the value of the second one is an m-tuple of predicates, and both are defined on two arguments, viz. a predicate and an m-tuple of predicates. In retrospect this was a mistake. In the sequel we shall replace them by a single function, pq say, of which both value and argument are a pair (predicate, m-tuple of predicates). In the new notation, (13) and (14) become

$$(X,Y): ([r\ Y \equiv \mathcal{R}]\ \wedge \\ (\underline{A}\ U,V: (U,V)\ \underline{sub}\ (X,Y): \\ [(r\ U,\ rs\ V) \equiv pq\ (rV,\ rs\ U)])) \qquad (0)$$

$$h: (\underline{A}\,\mathcal{R} :: (\underline{\underline{E}}\ Z :: [(h\,\mathcal{R}, Z) \equiv pq\ (\mathcal{R}, h\,Z)])) \qquad (1)$$

We thus achieve several simplifications. There is the notational advantage that the arguments need not be repeated —once for p and once for q—; there is the conceptual simplification that, pq being defined on a single argument, it suffices to require for pq just monotonicity.

(End of notational comment.)

Formulation and proof of Lemma 0, EWD859-4, can be improved as follows.

<u>Lemma 0</u>. Let X and Y range over predicate structures of given shapes; let b be a boolean function such that $b\,X\,Y$ is defined for all X, Y. Consider the equations

$$(X,Y):\; b\,X\,Y \qquad (2)$$

and

$$X:\; (\underline{E}Y :: b\,X\,Y) \quad ; \qquad (3)$$

then there exists a (many to one) correspondence between the solutions of (2) and those of (3) such that a solution of (3) is the X-component of all corresponding solutions of (2) .

<u>Proof</u>. For all X we observe

$$\begin{aligned}
& (\underline{E}Y :: (X,Y) \text{ is a solution of } (2)) \\
= & \{(2)\} \\
& (\underline{E}Y :: b\,X\,Y) \\
= & \{(3)\} \\
& X \text{ is a solution of } (3) .
\end{aligned}$$

(End of Proof.)

<u>Corollary 0</u>. If (2) has an extreme solution (Xe, Ye) , Xe is (3)'s extreme solution of the same kind.

(Proof omitted.)

Re Lemma 1, EWD859-5, we remark that the corresponding lemma for weakest solutions is also valid; the proof is best conducted via the conjugate and is left to the reader.

Similarly, from Theorem 0, EWD859-10, the corresponding theorem for weakest solutions can be derived. Since this requires a bit more care, we now show how this can be done.

The weakest solution of (0) would be the negation of the strongest solution of (0) with (X,Y) replaced by $(\neg X, \neg Y)$, i.e.

$$\begin{aligned}&(X,Y):([r(\neg Y)\equiv \mathcal{R}]\ \wedge\\ &\qquad(\underline{A}\ U,V:(U,V)\ \underline{\text{sub}}\ (\neg X,\neg Y):\\ &\qquad\qquad[(r\,U,\ rs\,V)\equiv pq\,(r\,V,\ rs\,U)]))\end{aligned}$$

To begin with, we replace the dummies U,V by $\neg U, \neg V$; this yields

$$\begin{aligned}&(X,Y):([r(\neg Y)\equiv \mathcal{R}]\ \wedge\\ &\qquad(\underline{A}\ U,V:(\neg U,\neg V)\ \underline{\text{sub}}\ (\neg X,\neg Y):\\ &\qquad\qquad[(r(\neg U),\ rs(\neg V))\equiv pq\,(r(\neg V),\ rs(\neg U))]))\end{aligned}$$

With r, rs, and structure forming commuting with negation and in view of the definition of the conjugate, this yields

$$\begin{aligned}&(X,Y):([r\,Y\equiv \neg\mathcal{R}]\ \wedge &&(4)\\ &\qquad(\underline{A}\ U,V:(U,V)\ \underline{\text{sub}}\ (X,Y):\\ &\qquad\qquad[(r\,U,\ rs\,V)\equiv pq^{*}(r\,V,\ rs\,U)]))\quad.\end{aligned}$$

Since pq^{*} is monotonic, we deduce on account of Theorem 0, that (4) has a strongest solution, and, hence (0) has a weakest one.

Let us define $\tilde{g}$ by denoting the root of the X-component of the strongest solution of (4) by $\tilde{g}(\neg\mathcal{R})$.

With $\tilde{g}^*R$ short for $\neg\tilde{g}(\neg R)$ our first conclusion is that

$$[\tilde{g}^*R \equiv (\text{the root of the X-component of the weakest solution of (0)})]$$.

Our second conclusion from the definition of $\tilde{g}$, (4) and Theorem 0 is, that $\tilde{g}$ is the strongest solution of

$$h: (\underline{A}R :: (\underline{E}Z :: [(hR, Z) \equiv pq^*(R, hZ)]))$$;

this is equivalent to the conclusion that $\tilde{g}^*$ is the weakest solution of

$$h: (\underline{A}R :: (\underline{E}Z :: [(h^*R, Z) \equiv pq^*(R, h^*Z)]))$$.

Negating the dummies, we derive

$$h: (\underline{A}R :: (\underline{E}Z :: [(h^*(\neg R), \neg Z) \equiv pq^*(\neg R, h^*(\neg Z))]))$$

and, by applying the definition of the conjugate

$$h: (\underline{A}R :: (\underline{E}Z :: [(hR, Z) \equiv pq(R, hZ)]))$$,

i.e. $\tilde{g}^*$ is the weakest solution of (1). And this concludes our demonstration that Theorem 0 holds for weakest solutions as well. (The above book-keeping is more elaborate than we had hoped.)

* * *

We shall define, for a recursively defined procedure REC, the predicate transformer wlp(REC,?) as the weakest solution of an equation of type (1) and the predicate transformer wp(REC,?) as the

strongest solution of a very similar (possibly identical) equation. The ultimate goal of this note will be to prove at least
(i) that wp(REC,?) satisfies the Law of the Excluded Miracle
(ii) that wlp(REC,?) is universally conjunctive
(iii) that $[wp(REC, R) \equiv wlp(REC, R) \wedge wp(REC, true)]$.

To this end we have to establish first the relevant conjunctivity properties, etc. for functions pq —in (1)— as derived from the body of REC.

For the time being, we consider the body in isolation, i.e. we temporarily ignore that later the body will be used for a recursive definition. In other words, we consider a body D, built by means of concatenation and the alternative construct from known statements and one "parameter statement" denoted by REC.

Of the known statements S we use
(i) $[wp(S, false) \equiv false]$
(ii) wlp(S,?) is universally conjunctive
(iii) $[wp(S,R) \equiv wlp(S,R) \wedge wp(S, true)]$ for all R.

The parameter statement REC enters the game via two predicate transformers, h and lh respectively. They will be used to play the rôles of wp(REC,?) and wlp(REC,?) respectively; here h and lh will be independent parameters for which assumptions (i),(ii), and (iii) will <u>not</u> be made.

Lemma 1. Let D be a statement, built by concatenation and the alternative construct from known statements and a statement REC for which h and lh play the role of $wp(REC, ?)$ and $wlp(REC, ?)$ respectively. Then two known functions, pq and lpq, of which both value and argument are a pair (predicate, m-tuple of predicates), a predicate P, and an m-tuple of predicates Q can be defined that have the following properties

(i) $[pq\ false \equiv false]$ (Note that argument, value, and quantification refer to a pair (predicate, m-tuple of predicates).)

(ii) lpq is universally conjunctive

(iii) $[pq\ (X,Y) \equiv lpq\ (X,Y) \wedge (P,Q)]$ for all (X,Y)

(iv) $wp(D,R)$ is for all R the solution of

$$U: (\underline{\mathrm{E}}\, Z :: [(U,Z) \equiv pq\,(R, hZ)])$$

(v) $wlp(D,R)$ is for all R the solution of

$$U: (\underline{\mathrm{E}}\, Z :: [(U,Z) \equiv lpq\ (R, lh\, Z)]) \quad .$$

(In (iv) and (v), the existing Z is also unique, but this will not be proved.)

Proof. The proof is by induction over the grammar of D. For the base we take skip for D; for the induction step it suffices to consider for D the forms $S; D'$, $REC; D'$, and
$\underline{\mathbf{if}}\ B0 \rightarrow D0' \,[\!]\, B1 \rightarrow D1'\ \underline{\mathbf{fi}}$.

$\underline{D \equiv skip}$

In this case we have $[wp(D,R) \equiv R]$ and $[wlp(D,R) \equiv R]$. With the unique 0-tuple, $wp(D,R)$ and $wlp(D,R)$ are the solution of

$$U: (\underline{E}\, Z :: [(U,Z) \equiv (R, \text{0-tuple})]) \qquad ;$$

consequently it suffices to define, with $m=0$,

$[\, pq(X,Y) \equiv (X, \text{0-tuple})]$ for all X,Y *)
$[\, lpq\,(X,Y) \equiv (X, \text{0-tuple})]$ for all X,Y *)
$[(P,Q) \equiv (true, \text{0-tuple})]$

*) X,Y have to be taken from the appropriate range, i.e. X is any predicate and Y "any" 0-tuple of predicates.

The verification of (i) through (v) is left to the reader.

For each of the three cases of the induction step we need the following lemma, that we therefore formulate and prove first.

<u>Lemma 2</u>. Consider the conditions on V and U

$$(\underline{E}\, Z :: [V \equiv f\,Z] \wedge [Z \equiv g\,Z]) \qquad (5)$$
$$(\underline{E}\, Z :: [U \equiv k(f\,Z)] \wedge [Z \equiv g\,Z]) \quad . \qquad (6)$$

Then we have
$(U \text{ satisfies } (6)) \equiv$
$\quad (\underline{E}\, V :: [U \equiv k\,V] \wedge (V \text{ satisfies } (5)))$.

<u>Proof</u>. $(\underline{E}V :: [U \equiv kV] \wedge (V \text{ satisfies } (5)))$

$= \{(5)\}$

$(\underline{E}V :: [U \equiv kV] \wedge (\underline{E}Z :: [V \equiv fZ] \wedge [Z \equiv gZ]))$

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

$(\underline{E}Z :: (\underline{E}V :: [U \equiv kV] \wedge [V \equiv fZ] \wedge [Z \equiv gZ]))$

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

$(\underline{E}Z :: [U \equiv k(fZ)] \wedge [Z \equiv gZ])$

$= \{(6)\}$

$(U \text{ satisfies } (6))$ (End of Proof of Lemma 2)

<u>Corollary 1</u>. If Vu is the only solution of (5), k Vu is the only solution of (6).

<u>D = S; D'</u>

true

$= \{\text{definition of } ;\}$

$[wp(D,R) \equiv wp(S, wp(D',R))]$

$= \{\text{induction hypothesis (iv)}\}$

$[wp(D,R) \equiv wp(S, \text{the solution of}$
$\quad U{:}(\underline{E}Z :: [(U,Z) \equiv pq'(R,hZ)]))]$

$\Rightarrow \{\text{Corollary 1}\}$

$[wp(D,R) \equiv (\text{the solution of}$
$\quad U{:}(\underline{E}Z :: [U \equiv wp(S, p'(R,hZ))] \wedge [Z \equiv q'(R,hZ)])))]$

Hence we define pq by

$$[pq(X,Y) \equiv (wp(S, p'(X,Y)), q'(X,Y))] \quad ,$$

thus catering for (iv). We cater for (v) by the similar definition of lpq :

$[lpq(X,Y) \equiv (wlp(S, lp'(X,Y)), lq'(X,Y))]$.

Furthermore we observe

$[p(X,Y) \equiv wp(S, p'(X,Y))]$

$=$ {induction hypothesis (iii)}

$[p(X,Y) \equiv wp(S, lp'(X,Y) \wedge P')]$

$=$ {properties of $wp(S,?)$ and $wlp(S,?)$}

$[p(X,Y) \equiv wlp(S, lp'(X,Y)) \wedge wp(S,P')]$.

Combining the above, we can cater for (iii) by defining (P,Q) by

$[(P,Q) \equiv (wp(S,P'), Q')]$.

The verification of (i) and (ii) is left to the reader.

$\underline{D = REC;D'}$

true

$=$ {definition of ; and of h}

$[wp(D,R) \equiv h\ wp(D',R)]$

$=$ {induction hypothesis (iv)}

$[wp(D,R) \equiv h$ (the solution of

$U: (\underline{E} Z :: [(U,Z) \equiv pq'(R, hZ)]))]$

$\Rightarrow$ {Corollary 1}

$[wp(D,R) \equiv$ (the solution of

$U: (\underline{E} Z :: [U \equiv h(p'(R,hZ))] \wedge [Z \equiv q'(R,hZ)]))]$

$=$ {pred.calc.; this transformation is necessary, since U should be expressed as a known function of (R,hZ); to this end we extend Z with the predicate $\tilde{Z}$ to $(\tilde{Z},Z)$}

$[wp(D,R) \equiv ($the solution of
$\quad U\!:\!(\underline{E}\,\tilde{Z},Z :: [U \equiv h\tilde{Z}] \wedge [(\tilde{Z},Z) \equiv pq'(R,hZ)]))]$.

Hence we cater for (iv) by defining pq by

$[pq(X,(\tilde{Y},Y)) \equiv (\tilde{Y}, pq'(X,Y))]$.

We cater for (v) by the similar definition of lpq

$[lpq(X,(\tilde{Y},Y)) \equiv (\tilde{Y}, lpq'(X,Y))]$.

In view of induction hypothesis (iii) we cater for (iii) by defining (P,Q) by

$[(P,Q) \equiv (true,(P',Q'))]$.

Verification of (i) and (ii) is left to the reader. Note that in this case the value of m has been increased by 1 .

$\underline{D = \underline{\text{if}}\ B0 \rightarrow D0'\ []\ B1 \rightarrow D1'\ \underline{\text{fi}}}$

true
$=$ {definition of $\underline{\text{if}} \ldots \underline{\text{fi}}$}
$[wp(D,R) \equiv (\underline{A}\,i :: BB \wedge (\neg Bi \vee wp(Di',R)))]$
$=$ {induction hypothesis (iv)}
$[wp(D,R) \equiv (\underline{A}\,i :: BB \wedge (\neg Bi \vee ($the solution of
$\qquad U\!:\!(\underline{E}\,Z :: [(U,Z) \equiv pqi'(R,hZ)])))))]$
$\Rightarrow$ {Corollary 1}
$[wp(D,R) \equiv (\underline{A}\,i :: ($the solution of
$\qquad U\!:\!(\underline{E}\,Z :: [U \equiv BB \wedge (\neg Bi \vee pi'(R,hZ))] \wedge [Z \equiv qi'(R,hZ)]))))]$
$=$ {pred. calc.}

$$[wp(D,R) \equiv (\text{the solution of } U : (\underline{E}\ Z0, Z1 :: \\ [U \equiv BB \wedge (\neg B0 \vee p0'(R, h\,Z0)) \wedge (\neg B1 \vee p1'(R, h\,Z1))] \\ \wedge [(Z0, Z1) \equiv (q0'(R, h\,Z0), q1'(R, h\,Z1))]))] \quad .$$

Hence we cater for (iv) by defining pq by

$$[pq(X,(Y0,Y1)) \equiv (BB \wedge (\neg B0 \vee p0'(X,Y0)) \wedge (\neg B1 \vee p1'(X,Y1)), \\ (q0'(X,Y0), q1'(X,Y1)))]$$

Similarly we cater for (v) by defining lpq by

$$[lpq(X,(Y0,Y1)) \equiv ((\neg B0 \vee lp0'(X,Y0)) \wedge (\neg B1 \vee lp1'(X,Y1)), \\ (lq0'(X,Y0), lq1'(X,Y1)))] \quad .$$

Again we can cater for (iii), this time by defining (P, Q) by

$$[(P,Q) \equiv (BB \wedge (\neg B0 \vee P0') \wedge (\neg B1 \vee P1'), (Q0', Q1'))] .$$

Verification of (i) and (ii) is again left to the reader. Note that the new m is m0+m1 . In view of the base and the three forms of the step, m equals the number of calls of REC in the body.

(End of Proof of Lemma 1.)

* * *

After the above explorations of the body D and its associated functions pq and lpq —as defined in the proof of Lemma 1— we are now ready to explore the recursive definition

$$REC = D \quad .$$

In view of Lemma 1 (iv) we now define wp(REC,?)

as the strongest solution of (1), and, in view of Lemma 1 (v), wlp(REC, ?) as the weakest solution of

$$\mathrm{lh}: (\underline{A}\, R :: (\underline{E}\, Z :: [(\mathrm{lh}\, R, Z) \equiv \mathrm{lpq}\, (R, \mathrm{lh}\, Z)])) \qquad . \quad (1')$$

According to Theorem 0, EWD859, wp(REC, R) is the root of the X-component of the strongest solution of (0), and – see EWD860-2 – wlp(REC, R) is the root of the X-component of the weakest solution of the corresponding

$$\begin{aligned}&(X, Y): ([r\, Y \equiv R]\ \wedge \qquad\qquad (0')\\ &\qquad (\underline{A}\, U, V : (U, V)\ \underline{\mathrm{sub}}\ (X, Y) :\\ &\qquad\qquad [(r\, U, rs\, V) \equiv \mathrm{lpq}\, (r\, V, rs\, U)])) \quad .\end{aligned}$$

Note that Theorem 0 is applicable since from Lemma 1, (ii) and (iii), it follows that lpq and hence pq are monotonic.

Since we would like to apply the results of EWD849a "Junctivity of extreme solutions", we shall rewrite (0) and (0') in the forms

$$(X, Y) : [f(R, X, Y) \equiv (X, Y)] \qquad (7)$$

$$(X, Y) : [(X, Y) \equiv \mathrm{l}f(R, X, Y)] \qquad (8)$$

respectively. The possibility of such a rewriting has been argued on EWD859-11. The relevant properties of these functions are given by

<u>Lemma 3.</u> The functions f – from (7) –, lf – from (8) – satisfy

(i) [f false ≡ false] (Note that the argument refers to a triple (predicate, pair of m-trees of predicates) and that the value and the quantification refer to a pair of m-trees of predicates.)

(ii) $\mathrm{l}f$ is universally conjunctive

(iii) a pair (PP, QQ) of m-trees of predicates exists such that

$$[f(X,Y) \equiv \mathrm{l}f(X,Y) \wedge (PP,QQ)] \quad .$$

<u>Proof.</u>

From (0) and (7) we deduce that f is defined by

$$\begin{array}{l} [(\tilde{X},\tilde{Y}) \equiv f(R,X,Y)] = \quad (\text{for all } \tilde{X},\tilde{Y},X,Y) \qquad (9) \\ [r\tilde{Y} \equiv R] \wedge \\ \quad (\underline{A}\, \tilde{U},\tilde{V},U,V : (\tilde{U},\tilde{V},U,V)\ \underline{\text{sub}}\ (\tilde{X},\tilde{Y},X,Y) : \\ \qquad [(r\,\tilde{U},\ rs\,\tilde{V}) \equiv pq\ (r\,V,\ rs\,U)]) \end{array}$$

From (0') and (8) we deduce that $\mathrm{l}f$ is defined by

$$\begin{array}{l} [(\tilde{X},\tilde{Y}) \equiv \mathrm{l}f(R,X,Y)] = \quad (\text{for all } \tilde{X},\tilde{Y},X,Y) \qquad (10) \\ [r\,\tilde{Y} \equiv R] \wedge \\ \quad (\underline{A}\, \tilde{U},\tilde{V},U,V : (\tilde{U},\tilde{V},U,V)\ \underline{\text{sub}}\ (\tilde{X},\tilde{Y},X,Y) : \\ \qquad [(r\,\tilde{U},\ rs\,\tilde{V}) \equiv \mathrm{l}pq\ (r\,V,\ rs\,U)]) \end{array}$$

The above can be verified by observing that the equation (7) with f defined by (9) yields (0).

(i) By (9), f false is the solution of

$$\begin{array}{l} (\tilde{X},\tilde{Y}) : ([r\,\tilde{Y} \equiv \text{false}] \wedge \\ \quad (\underline{A}\, \tilde{U},\tilde{V},U,V : (\tilde{U},\tilde{V},U,V)\ \underline{\text{sub}}\ (\tilde{X},\tilde{Y},\text{false},\text{false}) : \\ \qquad [(r\,\tilde{U},\ rs\,\tilde{V}) \equiv pq\ (r\,V,\ rs\,U)])) \quad . \end{array}$$

Since all subtrees of false have that same value, this equation is, on account of Lemma 1, (i), equivalent to the equation

$$(\tilde{X},\tilde{Y}) : ([r\,\tilde{Y} \equiv false] \wedge (\underline{A}\,\tilde{U},\tilde{V} : (\tilde{U},\tilde{V})\ \underline{sub}\ (\tilde{X},\tilde{Y}) : [(r\,\tilde{U}, rs\,\tilde{V}) \equiv false])) \quad ,$$

which has false as its only solution.

(ii) By (10), all elements of $(\tilde{X},\tilde{Y})$ are defined as universally conjunctive functions of (R,X,Y): for $r\,\tilde{Y}$ this is obvious, for the remaining elements we rely on Lemma 1, (ii). Hence $\mathbb{f}$ is universally conjunctive.

(iii) With P and Q as they occur in Lemma 1, with the pair (PP, QQ) of m-trees of predicates defined by

$$(\underline{A}\,\tilde{U} : \tilde{U}\ \underline{sub}\ PP : [r\,\tilde{U} \equiv P]) \qquad \text{– i.e. the m-tree with all its elements equal to P –}$$

$$[r\,QQ \equiv true] \wedge (\underline{A}\,\tilde{V} : \tilde{V}\ \underline{sub}\ QQ : [rs\,\tilde{V} \equiv Q]) \quad ,$$

the conclusion follows from (9), (10), and Lemma 1, (iii). (End of Proof.)

<u>Theorem 0</u>.

(i) $[wp(REC, false) \equiv false]$

(ii) $wlp(REC, ?)$ is universally conjunctive

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

<u>Proof</u>. (i) $wp(REC, false)$ is by (7) the root of

the strongest solution of $(X,Y)\colon [f(\mathit{false},X,Y) \equiv (X,Y)]$. By Lemma 3, (i), this solution is *false* .

(ii) Since —Lemma 3, (ii)— If is universally conjunctive, the weakest solution of (8) —EWD849a, Theorem 2— is a universally conjunctive function of R, hence so is the root of its X-component.

(iii) Consider, with Z standing for a pair of m-trees of predicates, the equation

$$(X,Y)\colon [\,(X,Y) \equiv \mathit{If}(R,X,Y) \wedge Z\,] \qquad . \quad (11)$$

By Lemma 3,(iii), (11) becomes (7) with (PP,QQ) for Z ; if we substitute *true* for Z, (11) becomes (8). The right-hand side of (11) is universally conjunctive —Lemma 3, (ii)— in the quadruple (R,X,Y,Z) .

Let $G(R,Z)$ be the strongest solution of (11) and let $H(R,Z)$ be its weakest solution. The right-hand side of (11) being conjunctive, we have —EWD849a, Theorem 4—

$$[G(R,Z) \equiv H(R,\mathit{true}) \wedge G(\mathit{true},Z)]$$

With the special choice of (PP,QQ) for Z and confining our attention to the roots of the X-components, the conclusion (iii) follows.

(End of Proof.)

Remark. Along the lines of the proof of Lemma 1, it can be shown that pq is or-continuous in

case non-determinacy is bounded. Along
lines of the proof of Lemma 3 it can be
own that then the corresponding f is *or*-
ntinuous. From Theorem 2* of EWD849a-16
then follows that wp(REC,?) is *or*-continu-
s as well. (End of Remark.)

5 December 1983

s. C.S.Scholten
cientific Adviser
hilips Research Laboratories
600 JA EINDHOVEN
he Netherlands

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