Extreme solutions of equations

In the previous chapter we have encountered a number of statements S, for which the predicate transformers $wlp(S,?)$ and $wp(S,?)$ were given in closed form. In the next chapter we shall encounter a statement for which the predicates $wlp(S,X)$ and $wp(S,X)$ are given as solutions of equations of the form

$$(0) \qquad Y: [b.(X,Y)] \quad .$$

Here, b is a function from predicate pairs to predicates, i.e. $b.(X,Y)$ is a boolean structure, $[b.(X,Y)]$ is a boolean expression in X and Y, which for given X and Y is either *true* or *false*.

In (0) we have followed our convention of notationally distinguishing between boolean expressions and equations: by prefixing the boolean expression $[b.(X,Y)]$ by "Y:" we indicate that the boolean expression should be viewed as equation in the unknown Y.

Remark We found the convention of explicitly identifying the unknown(s) preferable to the convention of using reserved letters for the unknowns. It enables us to distinguish between the quadratic equation $x: (x^2 + a \cdot x + b = 0)$ and the linear equation $b: (x^2 + a \cdot x + b = 0)$. (End of Remark.)

Which predicates Y are solutions of (0)

-if any- depends in general on which predicate we have chosen for X . A thing we would like to show -and we shall do so- is that the b's we shall encounter when defining semantics are such that (0) is solvable for any predicate X .

A minor problem is that -for a single X- (0) has often many solutions. Fortunately, we can strengthen (0) into equations that have at most one solution, viz.

$$(1)\quad Y{:}\left([b.(X,Y)] \wedge (\underline{A}Z{:}[b.(X,Z)]{:}[Y \Rightarrow Z])\right)$$

$$(2)\quad Y{:}\left([b.(X,Y)] \wedge (\underline{A}Z{:}[b.(X,Z)]{:}[Z \Rightarrow Y])\right) .$$

The solution of (1) is called "the strongest solution of (0)" since it implies all solutions of (0); the solution of (2) is called "the weakest solution of (0)" since it follows from all solutions of (0). Together they are referred to as "the extreme solutions of (0)". In due time we shall show that the b's we shall encounter in the definition of semantics are such that for any predicate X equations (1) and (2) are solvable, i.e. that the extreme solutions of (0) exist for any predicate X .

Before proceeding to do so, however, we shall demonstrate that extreme solutions are unique, i.e. that (1) and (2) each have at most one solution.

<u>Proof</u>. We prove the uniqueness of the solution of (1); for (2), the proof is very similar.

To this end we observe -for fixed X-

$(P$ and Q solve $(1))$

$=$ { def. of (1) and rearrangement of terms }

$[b.(X,P)] \wedge (\underline{A}Z: [b.(X,Z)]: [Q \Rightarrow Z]) \wedge$

$[b.(X,Q)] \wedge (\underline{A}Z: [b.(X,Z)]: [P \Rightarrow Z])$

$\Rightarrow$ { instantiate $Z:=P$ and $Z:=Q$ respectively }

$[Q \Rightarrow P] \wedge [P \Rightarrow Q]$

$=$ { predicate calculus }

$[P \equiv Q]$

(End of Proof.)

Thus we have established that the extreme solutions are each unique, provided that they exist. Instead of showing the existence of strongest solutions separately from the existence of weakest solutions, we shall first establish a duality theorem by means of which we can halve the length of the existence proof.

Two introductory remarks first. Let b be such that (1) has a solution for any X, or -equivalently- that (0) has a strongest solution for any X. Since that strongest solution depends in general on the predicate X, which occurs as parameter in the equation, it is a function of X; accordingly we denote it by $g.X$, thus indicating explicitly its dependence on X. Furthermore we shall formulate and prove the duality theorem only for a special form of the function b, viz. the form that allows the most elegant formulation of the duality (and, not surprisingly, is the only form in which we shall need it). After these preliminaries we can present

<u>Theorem 5.0</u> (Duality Theorem.)

universal quantification [illegible]

$$\begin{array}{l}(g.X \text{ is the strongest solution of} \\ \qquad Y{:}\ [p.(X,Y) \Rightarrow q.(X,Y)]\ ) \quad \equiv \\ (g^{*}.X \text{ is the weakest solution of} \\ \qquad Y{:}\ [p^{*}.(X,Y) \Leftarrow q^{*}.(X,Y)]\ )\end{array}$$

.

<u>Proof 5.0</u>

$$\begin{array}{l}\quad (g.X \text{ is the strongest solution of} \\ \qquad Y{:}\ [p.(X,Y) \Rightarrow q.(X,Y)]\ ) \\ = \quad \{\text{definition of strongest solution, see (1)}\} \\ \quad (\underline{A}X{::}\ [p.(X,g.X) \Rightarrow q.(X,g.X)] \ \wedge \\ \qquad (\underline{A}Z{:}\ [p.(X,Z) \Rightarrow q.(X,Z)]{:}\ [g.X \Rightarrow Z])) \\ = \quad \{\text{transforming the dummies: } X := \neg X\ ,\ Z := \neg Z\} \\ \quad (\underline{A}X{::}\ [p.(\neg X, g.(\neg X)) \Rightarrow q.(\neg X, g.(\neg X))] \ \wedge \\ \qquad (\underline{A}Z{:}\ [p.(\neg X,\neg Z) \Rightarrow q.(\neg X,\neg Z)]{:}\ [g.(\neg X) \Rightarrow \neg Z])) \\ = \quad \{\text{definition of conjugate, property of } \Rightarrow \text{ and } \Leftarrow\} \\ \quad (\underline{A}X{::}\ [p^{*}.(X,g^{*}.X) \Leftarrow q^{*}.(X,g^{*}.X)] \ \wedge \\ \qquad (\underline{A}Z{:}\ [p^{*}.(X,Z) \Leftarrow q^{*}.(X,Z)]{:}\ [g^{*}.X \Leftarrow Z])) \\ = \quad \{\text{definition of weakest solution, see (2)}\} \\ \quad (g^{*}.X \text{ is the weakest solution of} \\ \qquad Y{:}\ [p^{*}.(X,Y) \Leftarrow q^{*}.(X,Y)]\ )\ .\end{array}$$

(End of Proof 5.0)

The previous theorem is about extreme solutions provided that they exist. We now turn to existence of extreme solutions; in view of Theorem 5.0, we only need to define and prove them for strongest solutions; sometimes we shall formulate the dual theorem as well. Since in this context nothing is gained by dragging the parameter X around —all the time we would be quantifying universally over it— we leave it out.

The first (general) step of coming to grips with the existence of a strongest solution is the consideration that the only candidate for a strongest solution is the conjunction of all solutions. Indeed we have

<u>Theorem 5.1</u> Consider equation

(3) $\qquad Y: [b.Y] \qquad ; \qquad$ then

$\qquad$ (equation (3) has a strongest solution) $\equiv$
$\qquad$ ($(\underline{A}Z: [b.Z]: Z)$ solves (3)) .

<u>Proof 5.1</u>

$\qquad$ (equation (3) has a strongest solution)

$=\qquad$ { see (1) }

$\qquad (\underline{E}Y:: [b.Y] \wedge (\underline{A}Z: [b.Z]: [Y \Rightarrow Z]))$

$=\qquad$ {in order to get Y outside the universal quantification we first interchange quantifications}

$\qquad (\underline{E}Y:: [b.Y] \wedge [(\underline{A}Z: [b.Z]: Y \Rightarrow Z)])$

$=\qquad$ {and use that the antecedent distributes over universal quantification}

$\qquad (\underline{E}Y:: [b.Y] \wedge [Y \Rightarrow (\underline{A}Z: [b.Z]: Z)])$

= {now we have $(\underline{A}Z: [b.Z]: Z)$ as subexpression; but note that the inverse implication follows from $[b.Y]$}

$(\underline{E}Y:: [b.Y] \wedge [Y \Leftarrow (\underline{A}Z: [b.Z]: Z)]$
$\wedge [Y \Rightarrow (\underline{A}Z: [b.Z]: Z)]\ )$

= {predicate calculus}

$(\underline{E}Y:: [b.Y] \wedge [Y \equiv (\underline{A}Z: [b.Z]: Z)])$

= {one-point rule}

$[b.(\underline{A}Z: [b.Z]: Z)]$

= {(3)}

($(\underline{A}Z: [b.Z]: Z)$ solves (3)) .

(End of Proof 5.1)

Note that in the above proof, until the application of the one-point rule, we have only massaged the existentially quantified term, which is nothing else but the body of the equation for the strongest solution of (3). Consequently, if $(\underline{A}Z: [b.Z]: Z)$ solves (3), it is also (3)'s strongest solution.

Remark The dual of Theorem 5.1 is

(equation (3) has a weakest solution) $\equiv$
($(\underline{E}Z: [b.Z]: Z)$ solves (3)) .

(End of Remark.)

Our next theorem states the existence of the strongest solution for a special b, viz. such that we can show that the equation is solved by the conjunction of its solutions.

Theorem 5.2 Let equation (4) be given by

(4) $\quad Y: [p.Y \Rightarrow q.Y]$,

let p be monotonic, and let q be conjunctive over the set of solutions of (4). Then equation (4) has a strongest solution. (The dual theorem states that for monotonic q, and for p disjunctive over the set of solutions of (4), equation (4) has a weakest solution.)

Proof 5.2 Thanks to Theorem 5.1, it suffices to show that the conjunction of (4)'s solutions solves (4). The calculation is straightforward

$$
\begin{array}{ll}
 & p.(\underline{A}Z : [p.Z \Rightarrow q.Z] : Z) \\
\Rightarrow & \quad \{p \text{ is monotonic}\} \\
 & (\underline{A}Z : [p.Z \Rightarrow q.Z] : p.Z) \\
\Rightarrow & \quad \{\text{predicate calculus}\} \\
 & (\underline{A}Z : [p.Z \Rightarrow q.Z] : q.Z) \\
= & \quad \{q \text{ is conjunctive over the solution set of } (4)\} \\
 & q.(\underline{A}Z : [p.Z \Rightarrow q.Z] : Z) \quad .
\end{array}
$$

(End of Proof 5.2)

And now we are ready for the famous

Theorem 5.3 (In the oral tradition known as the "Theorem of Knaster-Tarski.") For monotonic f

(5) $\quad Y: [f.Y \equiv Y]$

has the same strongest solution as

(6) $\quad Y: [f.Y \Rightarrow Y]$

and has the same weakest solution as

(7) $Y: [f.Y \Leftarrow Y]$.

<u>Proof 5.3</u> We can confine ourselves to demonstrating the existence and equality of the strongest solutions of (5) and (6), as existence and equality of the weakest solutions of (5) and (7) is merely the dual.

Choosing in Theorem 5.2 f for p, and for q the identity function (which is universally conjunctive), we conclude that (6) has a strongest solution, i.e. calling it Q , we have

(8) $[f.Q \Rightarrow Q]$

(9) $(\underline{A}Z: [f.Z \Rightarrow Z]: [Q \Rightarrow Z])$.

In order to show that Q solves (5) we observe

$[f.Q \equiv Q]$

= { predicate calculus; rewriting the equivalence as mutual implication is suggested by (8)}

$[f.Q \Rightarrow Q] \wedge [Q \Rightarrow f.Q]$

= {(8)}

$[Q \Rightarrow f.Q]$

⇐ {(9) tells us what Q implies, hence instantiate (9) with $Z := f.Q$}

$[f.(f.Q) \Rightarrow f.Q]$

⇐ { now we can use f's monotonicity}

$[f.Q \Rightarrow Q]$

= {(8) again}

true

In order to show that Q implies all solutions of

(5) we observe

$(\underline{A}Z: [f.Z \equiv Z]: [Q \Rightarrow Z])$

$\Leftarrow$ { fortunately $[f.Z \equiv Z] \Rightarrow [f.Z \Rightarrow Z]$, i.e. (5) is the least tolerant equation }

$(\underline{A}Z: [f.Z \Rightarrow Z]: [Q \Rightarrow Z])$

$=$ {(9)}

true .

(End of Proof 5.3)

The Theorem of Knaster-Tarski is of profound methodological significance. It allows us to characterize the common strongest solution of (5) and (6) for monotonic f as the unique solution of

(10) $Y: ([f.Y \equiv Y] \wedge (\underline{A}Z: [f.Z \Rightarrow Z]: [Y \Rightarrow Z]))$

or as the unique solution of

(11) $Y: ([f.Y \Rightarrow Y] \wedge (\underline{A}Z: [f.Z \equiv Z]: [Y \Rightarrow Z]))$.

Note that both conjuncts in the body of (11) are weaker than the corresponding conjuncts in the body of (10). Yet, for monotonic f, these two equations have the same unique solution!

Hence, in a proof in which a predicate has been given to be such a strongest solution, we tend to <u>use</u> that it solves (10); in an argument in which we have to show that a predicate is such a strongest solution, it suffices to show that it solves (11).

The usefulness of the above device is enhanced by the fact that f only needs to be monotonic, i.e. only needs to enjoy the weakest junctivity property.

We have seen that if $Y:[f.Y \Rightarrow Y]$ has a strongest solution, $(\underline{A}Z:[f.Z \Rightarrow Z]:Z)$ gives that solution in closed form. This closed form, however, is not one with which we can do very much. It is therefore good to know that for $\underline{\text{or}}$-continuous f there exists a closed expression for the strongest solution which is more easily manipulated. The next two theorems deal with that; the first one is a stepping-stone.

<u>Theorem 5.4</u> For monotonic f and any Y

$$[f.Y \Rightarrow Y] \Rightarrow [(\underline{E}i:: i \geq 0: f^i.\text{false}) \Rightarrow Y)] \quad .$$

<u>Proof 5.4</u> The dummy i ranging over the natural numbers and functional iteration being defined recursively, a proof by mathematical induction over the natural numbers seems indicated. Hence we try to massage the consequent so as to make it amenable to an inductive proof:

$$
\begin{array}{ll}
 & [(\underline{E}i: i \geq 0: f^i.\text{false}) \Rightarrow Y\,] \\
= & \quad \{\text{quasi-distribution of the consequent}\} \\
 & [(\underline{A}i: i \geq 0: f^i.\text{false} \Rightarrow Y)] \\
= & \quad \{\text{interchange of quantifications}\} \\
 & (\underline{A}i: i \geq 0: [f^i.\text{false} \Rightarrow Y]) \quad .
\end{array}
$$

This we shall demonstrate by mathematical induction over i under the assumptions that f is monotonic and $[f.Y \Rightarrow Y]$. The base is easy; neither assumption is needed.

<u>Base</u> $[f^0.\mathit{false} \Rightarrow Y]$

$=$ {definition of functional iteration}

$[\mathit{false} \Rightarrow Y]$

$=$ {predicate calculus}

true .

<u>Step</u> $[f^{i+1}.\mathit{false} \Rightarrow Y]$

$=$ {definition of functional iteration}

$[f.(f^i.\mathit{false}) \Rightarrow Y]$

$\Leftarrow$ {let us use $[f.Y \Rightarrow Y]$ to get f in the consequent}

$[f.(f^i.\mathit{false}) \Rightarrow f.Y]$

$\Leftarrow$ { f is monotonic }

$[f^i.\mathit{false} \Rightarrow Y]$.

(End of Proof 5.4)

Theorem 5.4 states that, for monotonic f, $(\underline{E}i : i \geq 0 : f^i.\mathit{false})$ implies any solution of $Y: [f.Y \Rightarrow Y]$, just as its strongest solution does. And this raises the question whether $(\underline{E}i : i \geq 0 : f^i.\mathit{false})$ could itself be that strongest solution. This question is answered in

<u>Theorem 5.5</u> For <u>or</u>-continuous f

$$(\underline{E}i : i \geq 0 : f^i.\mathit{false})$$

is the strongest solution of

(6) $Y: [f.Y \Rightarrow Y]$.

(The dual is that, for <u>and</u>-continuous f, the weakest solution of $Y: [f.Y \Leftarrow Y]$ is $(\underline{A}i : i \geq 0 : f^i.\mathit{true})$.)

<u>Proof 5.5</u> Since an <u>or</u>-continuous f is monotonic, (6) has a strongest solution. In view of Theorem 5.4 it suffices to show that $(\underline{E}i : i \geq 0 : f^i.\mathit{false})$ solves (6) . To this end we shall first show that

its terms form a weakening sequence, i.e.

$$(\underline{A}i: i \geq 0: [f^i.\mathit{false} \Rightarrow f^{i+1}.\mathit{false}]) \quad .$$

This is done by mathematical induction:

Base
$$\begin{array}{ll} & [f^0.\mathit{false} \Rightarrow f^1.\mathit{false}] \\ = & \quad \{\text{definition of functional iteration}\} \\ & [\mathit{false} \Rightarrow f.\mathit{false}] \\ = & \quad \{\text{predicate calculus}\} \\ & \mathit{true} \quad . \end{array}$$

Step
$$\begin{array}{ll} & [f^{i+1}.\mathit{false} \Rightarrow f^{i+2}.\mathit{false}] \\ = & \quad \{\text{definition of functional iteration}\} \\ & [f.(f^i.\mathit{false}) \Rightarrow f.(f^{i+1}.\mathit{false})] \\ \Leftarrow & \quad \{f \text{ is monotonic}\} \\ & [f^i.\mathit{false} \Rightarrow f^{i+1}.\mathit{false}] \quad . \end{array}$$

Finally we observe

$$\begin{array}{ll} & f.(\underline{E}i: i \geq 0: f^i.\mathit{false}) \\ = & \quad \{f \text{ is } \underline{\text{or}}\text{-continuous, sequence is weakening}\} \\ & (\underline{E}i: i \geq 0 : f^{i+1}.\mathit{false}) \\ = & \quad \{\text{renaming the dummy } i := j-1 \text{ ; } [f^0.\mathit{false} \equiv \mathit{false}]\} \\ & (\underline{E}j: j \geq 1: f^j.\mathit{false}) \vee f^0.\mathit{false} \\ = & \quad \{\text{predicate calculus}\} \\ & (\underline{E}i: i \geq 0: f^i.\mathit{false}) \end{array}$$

(End of Proof 5.5)

Continuity derives a lot of its significance from the above theorem; it enables us to prove properties of an extreme solution by means of mathematical induction over the natural numbers. It is, however, possible that the importance of this possibility has been overrated

* * *

We now reintroduce our parameter X in the equation and turn our attention to equation

(12) $\quad Y: [f.(X,Y) \equiv Y]$

for monotonic f. Such an f being also monotonic in the individual components of its argument, in particular in the second component, Theorem 5.3 (Knaster-Tarski) asserts that its extreme solutions exist.

In what follows, $g.X$ denotes the strongest solution of (12) and $h.X$ denotes the weakest solution of (12). In analogy with (10), we capture our knowledge about g and h in the formally strongest way: we have for all X and Z

(13) $\quad [f.(X,g.X) \equiv g.X]$

(14) $\quad [f.(X,Z) \Rightarrow Z] \Rightarrow [g.X \Rightarrow Z]$

(15) $\quad [f.(X,h.X) \equiv h.X]$

(16) $\quad [f.(X,Z) \Leftarrow Z] \Rightarrow [h.X \Leftarrow Z]$.

The ultimate goal of this section is to prove junctivity properties of g and h, given the junctivity properties of f. As we go along, we shall see that the proofs can be smoothly derived with a minimum of invention or trial and error by each time realizing which of the formulae (13) through (16) is the appropriate one to appeal to.

Let in the demonstrandum an application of g occur in the consequent. For that g, an appeal to (14) is of no interest: (14) allows us to conclude that an application of g implies something and not what it is implied by. Therefore, for such an application, <u>only</u> (13) can be of interest (and in all probability has to be used).

Conversely, if the demonstrandum has an application of g as its antecedent, an appeal to (14) is almost certainly required as (13), all by itself, fails to express how strong g really is.

For the choice between (15) and (16), similar considerations apply.

A major decision is often whether to start massaging the antecedent so as to show that it implies the consequent, or to start massaging the consequent so as to show that it follows from the antecedent. It may surprise the reader that we call this decision "major", since the two proofs are each other's reverse and, hence, logically identical. The point is that steps that in the one direction are almost dictated by what has been written down, may in the other direction require clairvoyance for their justification. The general advice is to start at the most complicated side (if there is one): usually the more complicated expression shows more explicitly which transformation is appropriate.

We have also minor decisions to take, such as the order in which to apply different transformations. We call them minor because as a rule they do not influence our ability to prove the theorem; they may influence the length of our proofs and are therefore preferably taken wisely.

Just to show how well these heuristics work, let us prove

<u>Theorem 5.6</u> Let p and q be monotonic functions from predicate pairs to predicates;
let (P, Q) be the strongest solution of

$$(X,Y): [(p.(X,Y), q.(X,Y)) \equiv (X,Y)] \quad ;$$

let $g.X$ be the strongest solution of

$$Y: [q.(X,Y) \equiv Y] \quad .$$

Then we have $[g.P \equiv Q]$.

<u>Proof 5.6</u> For the sake of completeness we observe that both strongest solutions exist — $(p.(X,Y), q.(X,Y))$ being a monotonic function of (X,Y) for monotonic p and q — .

Our formal knowledge about P and Q is — expressed in the separate components — (analogously to (13) or the first conjunct of (10)) :

(17) $[p.(P,Q) \equiv P]$

(18) $[q.(P,Q) \equiv Q]$

and analogously to (14) or the second conjunct of (10):

(19) $[p.(X,Y) \Rightarrow X] \wedge [q.(X,Y) \Rightarrow Y] \Rightarrow [(P,Q) \Rightarrow (X,Y)]$

Our formal knowledge about g is similarly captured by

(20) $[q.(X, g.X) \equiv g.X]$

(21) $[q.(X,Y) \Rightarrow Y] \Rightarrow [g.X \Rightarrow Y]$.

So much for what has been given. Not surprisingly in this context, we shall prove the equivalence by mutual implication. Let us tackle $[Q \Rightarrow g.P]$ first. (That is one of those "minor decisions".)

$[Q \Rightarrow g.P]$

$=$ { we can tackle $g.P$ via (20) or try to tackle Q via (19); let us take the minor decision to do the latter; in view of (19) we rewrite }

$[(P, Q) \Rightarrow (P, g.P)]$

$\Leftarrow$ { (19) with $X, Y := P, g.P$ }

$[p.(P, g.P) \Rightarrow P] \;\wedge\; [q.(P, g.P) \Rightarrow g.P]$

$=$ { for the consequent $g.P$ of the second conjunct, only (20) can be of interest, so (20) with $X := P$ }

$[p.(P, g.P) \Rightarrow P] \;\wedge\; [q.(P, g.P) \Rightarrow q.(P, g.P)]$

$=$ { predicate calculus }

$[p.(P, g.P) \Rightarrow P]$

$=$ { for the consequent P, only (17) can be of interest }

$[p.(P, g.P) \Rightarrow p.(P, Q)]$

$\Leftarrow$ { fortunately, p is monotonic }

$[g.P \Rightarrow Q]$

$\Leftarrow$ { we can tackle the consequent Q via (18) or the antecedent $g.P$ via (21); let us take the minor decision to do the latter; (21) with $X, Y := P, Q$ }

$[q.(P, Q) \Rightarrow Q]$

$=$ { now we tackle consequent Q with (18) }

$[q.(P, Q) \Rightarrow q.(P, Q)]$

$=$ { predicate calculus }

true

Notice that in the mean time we have proved the other implication as well and that, hence, our proof obligation has been met. Notice also that we have appealed to each of the given formulae (17) through (21) precisely once, and since we need all of them, our proof is in that sense the shortest possible one.

<u>Remark</u> Trusting that the reader has read the above proof very carefully and has absorbed the heuristics, we shall in future abbreviate the heuristics. We shall also combine steps, such as omitting the two intermediate results preceding "{predicate calculus}". (End of Remark.)

(End of Proof 5.6)

After this interlude we return to the junctivity properties of g and h, given the junctivity properties of f. As a starter we establish Theorem 5.7. (It will be subsumed in later theorems, for whose proofs it will be used.)

<u>Theorem 5.7</u> For monotonic f, g and h are monotonic.

<u>Proof 5.7</u> To prove the monotonicity of g, we have to show for arbitrary predicates P and Q

$$[P \Rightarrow Q] \Rightarrow [g.P \Rightarrow g.Q] \quad ,$$

using that g is given by

(13) $[f.(X, g.X) \equiv g.X]$ and

(14) $[f.(X,Z) \Rightarrow Z] \Rightarrow [g.X \Rightarrow Z]$.

To this end we observe

$$\begin{array}{ll}
 & [g.P \Rightarrow g.Q] \\
\Leftarrow & \quad \{\text{tackle } g.P \text{ via (14) with } X, Z := P, g.Q\} \\
 & [f.(P, g.Q) \Rightarrow g.Q] \\
= & \quad \{\text{tackle } g.Q \text{ via (13) with } X := Q\} \\
 & [f.(P, g.Q) \Rightarrow f.(Q, g.Q)] \\
\Leftarrow & \quad \{f \text{ is monotonic, hence monotonic in } 1^{st} \text{ comp.}\} \\
 & [P \Rightarrow Q] \quad .
\end{array}$$

The monotonicty of h is merely the dual of the above.

(End of Proof 5.7)

And now we are ready to demonstrate the beautiful

<u>Theorem 5.8</u> Any type of conjunctivity enjoyed by f is enjoyed by h as well.

(Its dual is: Any type of disjunctivity enjoyed by f is enjoyed by g as well.)

<u>Proof 5.8</u> With f enjoying some type of conjunctivity, f is monotonic; hence -Theorem 5.7- h is monotonic.

In order to show that h is conjunctive over some V, i.e.

$$[h.(\underline{A}X : X \in V : X) \equiv (\underline{A}X : X \in V : h.X)] \quad ,$$

we show that either side implies the other.

(i) Because h is monotonic we have

$$[h.(\underline{A}X : X \in V : X) \Rightarrow (\underline{A}X : X \in V : h.X)] \quad .$$

(Here we see what good use we can make of Theorem 5.7 when showing a junctivity property of extreme solutions; the latter being monotonic, we get the implication in the one direction for free.)

(ii) To show the implication in the other direction we begin by observing that $X\in$

$$[h.(\underline{A}X{:}\ X\in V{:}\ X) \Leftarrow (\underline{A}X{:}\ X\in V{:}\ h.X)]$$

$\Leftarrow$ { the h. in the consequent is to be tackled via (16) with $X, Z := (\underline{A}X{:}\ X\in V{:}\ X), (\underline{A}X{:}\ X\in V{:}\ h.X)$ }

$$[f.((\underline{A}X{:}\ X\in V{:}\ X), (\underline{A}X{:}\ X\in V{:}\ h.X)) \Leftarrow (\underline{A}X{:}\ X\in V{:}\ h.X)]$$

$=$ { simplification of f's argument: quantification distributes over pair forming }

$$[f.(\underline{A}X{:}\ X\in V{:}\ (X, h.X)) \Leftarrow (\underline{A}X{:}\ X\in V{:}\ h.X)]$$

$=$ { the h. in the antecedent is to be tackled via (15) }

$$[f.(\underline{A}X{:}\ X\in V{:}\ (X, h.X)) \Leftarrow (\underline{A}X{:}\ X\in V{:}\ f.(X, h.X))]$$

Now the -minor- complication is that whereas h's conjunctivity is related to a bag of predicates, f's conjunctivity is related to a bag of predicate pairs. To be formally precise, we construct a bag W of predicate pairs by

(22) $\quad (X, Y)\in W \ \equiv\ X\in V \ \wedge\ [Y \equiv h.X]$

and observe that, thanks to the monotonicity of h, V and W are of the same junctivity type. Hence it suffices to show the above implication under the assumption that f is conjunctive over W. The formal demonstration proceeds as follows

$$f.(\underline{A}X{:}\ X\in V{:}\ (X, h.X))$$

$=\quad \{\text{one-point rule to introduce } Y\}$

$\quad f.(\underline{A}X: X\in V: (\underline{A}Y: [Y\equiv h.X]: (X,Y)))$

$=\quad \{\text{unnesting and (22) to introduce } W\}$

$\quad f.(\underline{A}X,Y: (X,Y)\in W: (X,Y))$

$=\quad \{f \text{ conjunctive over } W\}$

$\quad (\underline{A}X,Y: (X,Y)\in W: f.(X,Y))$

$=\quad \{\text{elimination of } W \text{ with (22) and nesting}\}$

$\quad (\underline{A}X: X\in V: (\underline{A}Y: [Y\equiv h.X]: f.(X,Y)))$

$=\quad \{\text{one-point rule to eliminate } Y\}$

$\quad (\underline{A}X: X\in V: f.(X,h.X))$.

<u>Remark</u> The last 5 steps of the above proof are not very exciting. Note that a number of them were needed to introduce Y and to get rid of it again, obligations caused by the way in which we defined W. Had we used the "bagifier" $\underline{B}$, we could have defined W by

$$W = (\underline{B}X: X\in V: (X,h.X))$$

and with rules how to manipulate expressions for such bags, there would have been no need to refer explicitly to the one-point rule. (End of Remark.)

(End of Proof 5.8)

Whereas Theorem 5.8 dealt with the conjunctivity properties of the weakest solution of

(12) $\qquad Y: [f.(X,Y)\equiv Y]$,

Theorem 5.10 will do so for its strongest solution. But first we state and prove Theorem 5.9 — $g.X$ and $h.X$ denoting, as before, the strongest and the weakest solution of (12) — .

<u>Theorem 5.9</u> For finitely conjunctive f and predicates X and Y satisfying

$$[f.(X,Y) \equiv Y]$$

we have

$$[g.X \equiv g.true \wedge Y] \quad .$$

(The dual states that for finitely disjunctive f and such X and Y we have

$$[h.X \equiv h.false \vee Y] \quad .)$$

In other words: the strongest solution of (12) is for finitely conjunctive f the conjunction of an arbitrary solution of (12) and the constant predicate - i.e. independent of X - $g.true$.

<u>Proof 5.9</u> Given are

(23) $\quad [f.(X,Y) \equiv Y]$

(13) $\quad [f.(X', g.X') \equiv g.X']$

(14) $\quad [f.(X',Z) \Rightarrow Z] \Rightarrow [g.X' \Rightarrow Z]$.

We shall prove the equivalence by proving that either side implies the other.

(i) $\quad [g.X \Rightarrow g.true \wedge Y]$

$=$ $\quad$ { predicate calculus }

$\quad [g.X \Rightarrow g.true] \wedge [g.X \Rightarrow Y]$

$\Leftarrow$ $\quad$ { g is monotonic; (14) with $Z := Y$ }

$\quad [X \Rightarrow true] \wedge [f.(X,Y) \Rightarrow Y]$

$=$ $\quad$ { predicate calculus; (23) }

$\quad true$

(ii) $[g.\mathrm{true} \wedge Y \Rightarrow g.X]$

$=$ {predicate calculus, so as to tackle $g.\mathrm{true}$ via (14)}

$[g.\mathrm{true} \Rightarrow g.X \vee \neg Y]$

$\Leftarrow$ {(14) with $X', Z := \mathrm{true}\ ,\ g.X \vee \neg Y$}

$[f.(\mathrm{true}, g.X \vee \neg Y) \Rightarrow g.X \vee \neg Y]$

$=$ {predicate calculus, preparing for f's conjunctivity}

$[f.(\mathrm{true}, g.X \vee \neg Y) \wedge Y \Rightarrow g.X]$

$=$ {(23), the only thing given about Y!}

$[f.(\mathrm{true}, g.X \vee \neg Y) \wedge f.(X,Y) \Rightarrow g.X]$

$=$ {f is finitely conjunctive; predicate calculus}

$[f.(X, g.X \wedge Y) \Rightarrow g.X]$

$=$ {(23) and (14) with $X', Z := X, Y$}

$[f.(X, g.X) \Rightarrow g.X]$

$=$ {(13) with $X' := X$}

true .

(End of Proof 5.9)

Theorem 5.9 is most interesting for the weakest possible choice for Y , viz. $h.X$. And so we get as first corollary

<u>Theorem 5.9.0</u> For finitely conjunctive f

$$[g.X \equiv g.\mathrm{true} \wedge h.X] \quad .$$

The second corollary is

<u>Theorem 5.9.1</u> For finitely conjunctive f

$$[g.(X \wedge Y) \equiv g.X \wedge h.Y] \quad .$$

<u>Proof 5.9.1</u>

$g.(X \wedge Y)$

$=$ {Theorem 5.9.0 with $X := X \wedge Y$}

$g.\mathrm{true} \wedge h.(X \wedge Y)$

$=$ {f conjunctive, hence h conjunctive, Theorem 5.8}

$$\begin{array}{ll} & g.true \wedge h.X \wedge h.Y \\ = & \quad \{\text{Theorem 5.9.0}\} \\ & g.X \wedge h.Y \end{array}$$.

(End of Proof 5.9.1)

Remark. The last two corollaries capture the important outcome of Theorem 5.9. We could have proved Theorem 5.9.1 directly – Theorem 5.9.0 then follows – instead of Theorem 5.9. We have not done so, firstly because Theorem 5.9.1 is more specific (in its mentioning of h) and, secondly, because the formulae of the proof would have been quite a bit longer. (End of Remark.)

Having expressed – Theorem 5.9.0 – $g.X$ in terms of (a constant predicate and) $h.X$, and having established – Theorem 5.8 – that h inherits the conjunctivity of f, we are ready for

Theorem 5.10 With the exception of universal conjunctivity and and-continuity, the conjunctivity of f is enjoyed by g as well.

(Its dual states that with the exception of universal disjunctivity and or-continuity, the disjunctivity of f is enjoyed by h as well.)

Proof 5.10 For monotonic f, the monotonicity of g is asserted in Theorem 5.7. For the remaining types of conjunctivity (i.e. unbounded, denumerable or finite), f is finitely conjunctive and hence – Theorem 5.9.0 – we have

$$[g.X \equiv g.true \wedge h.X]$$.

Theorem 5.8 states that h enjoys the conjunctivity of f , and √ states that g inherits the conjunctivity of h , universal conjunctivity excepted.

(End of Proof 5.10)

* * *

Theorems 5.9 and 5.10 are less beautiful than Theorem 5.8 , which states that h inherits without constraint or exception the conjunctivity enjoyed by f . To show that these constraints and exceptions are not void - i.e. have not entered the picture merely as a result of our weakness as theorem provers - we shall construct counter-examples.

Theorem 5.9 is restricted to finitely conjunctive f . All other forms of conjunctivity imply monotonicity, and, for a really convincing counter-example, it therefore suffices to come up with a monotonic - but not finitely conjunctive! - f such that the conclusion of 5.9 or 5.9.0 or 5.9.1 does <u>not</u> hold.

Let us look for the simplest example we can come up with that is monotonic but not finitely conjunctive; $[f.(X,Y) \equiv X]$, $[f.(X,Y) \equiv Y]$, and $[f.(X,Y) \equiv X \wedge Y]$ won't do, because they are finitely conjunctive, but

$$[f.(X,Y) \equiv X \vee Y]$$

is monotonic and passes the test of non-conjunctivity. (In general we have $\neg[(X \wedge X') \vee (Y \wedge Y') \equiv (X \vee Y) \wedge (X' \vee Y')]$.) With this choice for f , equation

(12) $Y: [f.(X,Y) \equiv Y]$

becomes $Y: [X \Rightarrow Y]$

with the obvious extreme solutions $[g.X \equiv X]$ and $[h.X \equiv true]$. Substituting these in the conclusion of Theorem 5.9.0 , viz. $[g.X \equiv g.true \wedge h.X]$ would yield $[X]$ which does not hold for any X . We have been fortunate: the simplest proposal for f that we could think of provided the counter-example. So much for the constraint of Theorem 5.9 to conjunctive f .

In order to show that Theorem 5.10's exception of universal conjunctivity is justified, we should look for a universally conjunctive f such that $\neg[g.true]$. Here the simple choice $[f.(X,Y) \equiv Y]$ does the job. With this choice, (12) becomes

$$Y: [Y \equiv Y]$$

with the obvious extreme solutions $[g.X \equiv false]$ and $[h.X \equiv true]$; g is not universally conjunctive.

In order to show, finally, that also Theorem 5.10's exception of and-continuity is justified, we look for an f that is and-continuous, but is not finitely conjunctive. In our first counter-example we found the simple f, given by $[f.(X,Y) \equiv X \vee Y]$, that was not finitely conjunctive, but we cannot use that because the corresponding strongest solution is the identity function, which is and-continuous. But we can use that f by using it as a source of inspiration, and by complicating it a little: replacing Y by $p.Y$ for a carefully chosen p .

We look for a p that is and-continuous, so that – Lemma 3.25, EWD908-27 – f is and-continuous. We look for a p that is also or-continuous so that – Theorem 5.5 – we have a closed form for g.X . And we would like p so simple that there is hope of tackling that closed form analytically. In a state space that has z as one of its integer coordinates, we suggest wp("z:=z+1, Y) for p.Y , i.e. we consider f given by

$$[f.(X,Y) \equiv X \vee Y^{z}_{z+1}] \quad .$$

According to Theorem 5.5 and the fact that f is or-continuous in its second argument, g.X is given by

$$[g.X \equiv (\underline{E}i : i \geq 0 : k^{i}.false)]$$

where k is given by $[k.U \equiv X \vee U^{z}_{z+1}]$, which – via induction over i – leads to

$$[g.X \equiv (\underline{E}i : i \geq 0 : X^{z}_{z+i})] \quad .$$

Consider now the strengthening sequence of predicates C.j given by $[C.j \equiv z \geq j]$ for $j \geq 0$. Then

$$\neg[g.(\underline{A}j : j \geq 0 : C.j) \equiv (\underline{A}j : j \geq 0 : g.(C.j))] \quad .$$

for:

$$
\begin{aligned}
& g.(\underline{A}j : j \geq 0 : C.j) \\
= & \quad \{\text{def. of } C\} \\
& g.(\underline{A}j : j \geq 0 : z \geq j) \\
= & \quad \{\text{predicate and integer calculus}\} \\
& g.\,false \\
= & \quad \{\text{last expression for } g.X\} \\
& false
\end{aligned}
$$

and

$(\underline{A}j: j \geq 0: g.(C.j))$

$= \quad \{\text{def. of } C\}$

$(\underline{A}j: j \geq 0: g.(z \geq j))$

$= \quad \{\text{last expression for } g.X\}$

$(\underline{A}j: j \geq 0: (\underline{E}i: i \geq 0: z+i \geq j))$

$= \quad \{\text{predicate and integer calculus}\}$

$(\underline{A}j: j \geq 0: true)$

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

$true$.

And this concludes the construction of the third and last counter-example. We would like to add that the sequence $C.j$ used above is a standard ingredient for showing non-*and*-monotonicity. (Similarly, the weakening sequence $z \leq j$ is used to show that *or*-continuity has been lost.) This knowledge makes the choice of our last f less surprising.

8 September 1986

prof. dr. Edsger W. Dijkstra
Department of Computer Science
The University of Texas at Austin
Austin, TX 78712-1188
USA