p.5 does not exist.

The repetition (Draft Ch. 6)

This chapter deals with the statement called "the repetitive construct" or "the repetition" for short. We shall use DO to denote statements of the form

$\underline{do}\ B0 \rightarrow S0\ \underline{od}$
$\underline{do}\ B0 \rightarrow S0\ [\!]\ B1 \rightarrow S1\ \underline{od}$
$\underline{do}\ B0 \rightarrow S0\ [\!]\ B1 \rightarrow S1\ [\!]\ B2 \rightarrow S2\ \underline{od}$

in general

$\underline{do}\ (\underline{[\!]}i : 0 \le i < n : B.i \rightarrow S.i)\ \underline{od}$.

Syntactically it is very similar to the corresponding alternative statement IF:

$\underline{if}\ (\underline{[\!]}i : 0 \le i < n : B.i \rightarrow S.i)\ \underline{fi}$.

Semantically, DO and IF are related by

(0) $\quad DO\ =\ \underline{do}\ BB \rightarrow IF\ \underline{od}$

where BB is again given by $[BB \equiv (\underline{E}i : 0 \le i < n : B.i)]$.

<u>Legenda</u> The equality sign between two statements expresses that they are semantically equivalent, i.e. have the same predicate transformers:

$$S0 = S1 \;\equiv (\underline{A}X :: [wlp(S0,X) \equiv wlp(S1,X)] \wedge [wp(S0,X) \equiv wp(S1,X)])\ .$$

(End of Legenda.)

<u>Remark</u> There are more such equivalences, such as

(1) $\quad IF = \underline{\text{if}}\ BB \rightarrow IF\ \underline{\text{fi}}$,

which can be proved using the definition of IF in Chapter 4 "The semantics of straight-line programs" and

(2) $\quad DO = \underline{\text{do}}\ BB \rightarrow DO\ \underline{\text{od}}$

which cannot be proved before we have defined DO. (End of Remark.)

Equality (0) is a postulate. It reduces the repetition with possibly many guards to a repetition with a single guard. It allows us to confine our further definition of the semantics of the repetition to the specially simple statement DO given by

(3) $\quad DO = \underline{\text{do}}\ B \rightarrow S\ \underline{\text{od}}$

and for brevity's sake we shall do so in the sequel.

For DO, B, and S, as connected by (3) we insist on the semantic equivalence

(4) $\quad DO = \underline{\text{if}}\ B \rightarrow S; DO\ [\!]\ \neg B \rightarrow skip\ \underline{\text{fi}}$,

i.e. we insist that both sides have the same wlp and the same wp. Using the semantics of skip, the semicolon, and the alternative construct this leads to the requirements

(5) $[wlp(DO,X) \equiv (\neg B \vee wlp(S,wlp(DO,X))) \wedge (B \vee X)]$

(6) $[wp(DO,X) \equiv (\neg B \vee wp(S, wp(DO,X))) \wedge (B \vee X)]$.

We shall show that these two requirements are met by defining

(7) $[wp(DO,true) \equiv$ the strongest solution of
$Y: [Y \equiv (\neg B \vee wp(S,Y))]$ $]$

(8) $[wlp(DO,X) \equiv$ the weakest solution of
$Y: [Y \equiv (\neg B \vee wlp(S,Y)) \wedge (B \vee X)]$ $]$,

from which we shall derive

(9) $[wp(DO,X) \equiv$ the strongest solution of
$Y: [Y \equiv (\neg B \vee wp(S,Y)) \wedge (B \vee X)]$ $]$.

That requirements (5) and (6) are met is a direct consequence of (8) and (9) respectively, so that is fine. We have to show, however

(i) that (7), (8), and (9) make sense in the sense that the postulated extreme solutions exist

(ii) that (9) follows from (7) and (8)

(iii) that wlp(DO,?) is universally conjunctive (i.e. Theorem 4.0)

(iv) that wp(DO,?) satisfies the Law of the Excluded Miracle (i.e. Theorem 4.1)

To begin with, we rewrite (7) and (9) using $[wp(S,Y) \equiv wlp(S,Y) \wedge wp(S, true)]$:

(7') $[wp(DO, true) \equiv$ the strongest solution of
$Y: [Y \equiv (\neg B \vee wlp(S,Y)) \wedge (\neg B \vee wp(S, true))]]$

(9') $[wp(DO, X) \equiv$ the strongest solution of
$Y: [Y \equiv (\neg B \vee wlp(S,Y)) \wedge (\neg B \vee wp(S, true)) \wedge (B \vee X)]]$

thus achieving that in all three defining equations – i.e. in (7'), (8), and (9') – the dependence of the right-hand side on Y is confined to the term $wlp(S,Y)$. In particular, all three equations are now of the form – each with its own Z –

(10) $\quad Y: [Y \equiv f.(Y,Z)]$

with f given by

(11) $\quad [f.(Y,Z) \equiv (\neg B \vee wlp(S,Y)) \wedge Z]$.

From the universal conjunctivity of $wlp(S,?)$ we conclude with Lemma 3.13 that $\neg B \vee wlp(S,?)$ is universally conjunctive; with – Lemma 3.11 – the identity function being universally conjunctive as well, we conclude from Lemma 3.18 that f is universally conjunctive (in its complete argument). Hence – Lemma 3.19 – f is monotonic in its first component and – Lemma 5.4: Knaster-Tarski – the extreme solutions of (10) exist. (This conclusion deals with (i).)

Let $g.Z$ be (10)'s strongest solution, and h.Z its weakest. Hence — (10), (11) —

$(7') \equiv [wp(DO, true) \equiv g.(\neg B \vee wp(S, true))]$

$(8) \equiv [wlp(DO, X) \equiv h.(B \vee X)]$

$(9') \equiv [wp(DO, X) \equiv g.((\neg B \vee wp(S, true)) \wedge (B \vee X))]$.

To show that (9') follows from (7') and (8) we observe

$$\begin{aligned}
& wp(DO, X) \\
= \ & \{\text{def. of } wp(S, X)\} \\
& wp(DO, true) \wedge wlp(DO, X) \\
= \ & \{(7') \text{ and } (8)\} \\
& g.(\neg B \vee wp(S, true)) \wedge h.(B \vee X) \\
= \ & \{f \text{ is finitely conjunctive; Corollary 5.5}\} \\
& g.((\neg B \vee wp(S, true)) \wedge (B \vee X))
\end{aligned}$$

and thus we have dealt with (ii) .

From f's universal conjunctivity we conclude — Theorem 5.0 — that h is universally conjunctive; so is — Lemma 3.13 — $(B \vee ?)$; (8) defines $wlp(DO, ?)$ as the functional composition of two universally conjunctive functions, and from Lemma 3.14 we conclude that $wlp(DO, ?)$ is universally conjunctive; thus we have dealt with (iii) .

To establish $[wp(DO, false) \equiv false]$ we observe that for $[X \equiv false]$ and $[wp(S, false) \equiv false]$, false is a solution of the defining equation in (9); and hence by definition its strongest; thus we have dealt with (iv).

And this concludes for the repetition our proof obligations as regards Theorem 4.0 and Theorem 4.1. For the repetition we want, however, to prove more, viz. the main theorem we use when reasoning about programs in which a repetition occurs. Before formulating the main theorem, however, some notational preliminaries first.

Let x and y range over some set D of which C is a subset; in that case $x \in D$, $y \in D$, $x \in C$, and $y \in C$ are domain constants of which the first two are by definition true. Let t be a D-valued function on the state space; then $t = y$ is a predicate and so is

$$(\underline{E}\, y : y \in C : t = y)$$

for which we introduce the abbreviation $t \in C$, i.e.

(12) $[t \in C \equiv (\underline{E}\, y : y \in C : t = y)]$.

The fact that t is a D-valued function on the state space is expressed by

(13) $[t \in D]$

or, in view of (12) —with $C := D$— equivalently by

(13') $[(\underline{E}\, y : y \in D : t = y)]$.

But for the fact that we have not explained yet what it means for a subset of a partially ordered set to be "well-founded" — which shall be explained after the theorem — we are now ready for the formulation of

<u>Theorem 6.0</u> Let $(D,<)$ be a partially ordered set; let C be a subset of D, such that $(C,<)$ is well-founded; let statement S, predicates B and P, and function t on the state space satisfy:

predicate transformer $wp(S,?)$ is monotonic;

(13) $[t \in D]$;

(14) $[P \wedge B \Rightarrow t \in C]$

(15) $[P \wedge B \wedge t=x \Rightarrow wp(S, P \wedge t<x)]$ for all x ;

then

(16) $[P \Rightarrow wp(\text{"}\underline{\text{do}}\ B \rightarrow S\ \underline{\text{od}}\text{"}, \neg B \wedge P]$.

(The well-informed reader will recognize in the above P an "invariant" of the repetition and in t a "variant function", which is the vehicle of the termination argument.)

From a strictly logical point of view, it would suffice to mention of well-founded sets only the property that is needed to prove Theorem 6.0, something that can be done in a single line. But in order to apply Theorem 6.0, one has at least to recognize a well-founded set when encountering it (if one has not to construct a well-founded set oneself as part of the correctness argument about a program). For that reason, we now insert, in view of the very central position of Theorem 6.0, an intermezzo on well-founded sets.

Intermezzo on well-founded sets

The standard definition of $(D, \leq)$ as a partially ordered set is the combination of a set D and a relation $\leq$ (pronounced "at most") such that for all x, y, z elements of D

(i) $x \leq x$ (Reflexivity)
(ii) $x \leq y \wedge y \leq x \Rightarrow x = y$ (Antisymmetry)
(iii) $x \leq y \wedge y \leq z \Rightarrow x \leq z$ (Transitivity).

Its most common model is a directed graph with the elements of D as its nodes and an arrow from y to x as a coding for $x \leq y$. From the reflexivity it follows that each x has a socalled "autoloop", i.e. an arrow leading from it to itself. From the antisymmetry it follows that the autoloops are the only directed cyclic paths. The transitivity means that we can interpret $x \leq y$ as "x is reachable from y".

Removing the autoloops —which don't carry any information— we get the partially ordered set $(D, <)$

with the non-reflexive relation $<$ (pronounced "less than") given in terms of $\leq$ by

$$x<y \equiv x\leq y \wedge x\neq y \quad .$$

Alternatively we have

$$x\leq y \equiv x<y \vee x=y \quad .$$

Also relation $<$ is transitive. (It is not completely fair to call $(D,<)$ also a partially ordered set, $<$ not being reflexive; yet it is not uncommon. If $x<y$, it makes, for instance, sense to state that all directed paths from y to x in $(D,<)$ are of finite length: if in $(D,\leq)$ there is a directed path from y to x, there are also such paths of infinite lengths.)

Next we have the definition of "minimal element":

$$(x \text{ is a minimal element of } C) \equiv$$
$$x\in C \wedge (\underline{A}\, y: y<x: \neg\, y\in C) \quad .$$

Note that a minimal element need not be unique. Take for C the natural numbers; with the standard interpretation of $<$, 0 is the only minimal element of C, but with $<$ defined as

$$x<y \equiv (\underline{E}\, p: p \text{ is positive integer}: x+2\cdot p=y)$$

both 0 and 1 are minimal elements of C. Note also that a subset may have no minimal elements: take for C the integers and for $<$ the usual interpretation.

For a partially ordered set to be well-founded is given by the definition

$$(C \text{ is well-founded}) \equiv (\text{each non-empty subset of } C \text{ contains a minimal element}) \quad .$$

For a sequence of elements $x.i \ (i \geq 0)$ of C to be a descending chain is given by

$$(\text{sequence } x.i \ (i \geq 0) \text{ is a descending chain}) \equiv (\underline{A}\, i, j :\ 0 \leq i < j :\ x.j < x.i) \quad ;$$

the number of elements in the sequence is called its length.

For mathematical induction over C to be valid, it should suffice to demonstrate

$$P.x \ \vee \ (\underline{E}\, y :\ y \in C \wedge y < x :\ \neg P.y) \qquad \text{for any } x \in C$$

in order to prove $\quad (\underline{A}\, x :\ x \in C :\ P.x) \quad .$

After the above definitions we can formulate

<u>Theorem 6.1</u> For a partially ordered set $(C, <)$ the following three statements are equivalent

(i) C is well-founded
(ii) mathematical induction over C is valid
(iii) all descending chains in C are of finite length.

<u>Proof Th. 6.1</u> In the following proof of the equivalence of (i) and (ii), V ranges over the subsets of C and P over the predicates over the elements of C.
on ?

Between the subsets V and the predicates P we establish a one-to-one correspondence by

(17) $\quad (\underline{A}x: x \in C: P.x \equiv \neg\, x \in V)$

with the special consequence

(18) $\quad (\underline{A}x: x \in C: P.x) \equiv V = \emptyset$.

We now observe

$$\begin{aligned}
&(i) \\
= &\{\text{definition of well-foundedness of } C\} \\
&(\underline{A}V:: V \neq \emptyset \equiv (\underline{E}x: x \in C: x \in V \wedge (\underline{A}y: y \in C \wedge y < x: \neg\, y \in V))) \\
= &\{\text{negating both sides; de Morgan}\} \\
&(\underline{A}V:: V = \emptyset \equiv (\underline{A}x: x \in C: \neg\, x \in V \vee (\underline{E}y: y \in C \wedge y < x: y \in V))) \\
= &\{\text{from dummy } V \text{ to dummy } P;\ (17) \text{ and } (18)\} \\
&(\underline{A}P:: (\underline{A}x: x \in C: P.x) \equiv \\
&\qquad (\underline{A}x: x \in C: P.x \vee (\underline{E}y: y \in C \wedge y < x: \neg P.y))) \\
= &\{\text{definition of mathematical induction over } C\} \\
&(ii)
\end{aligned}$$

In order to prove $(i) \equiv (iii)$, we shall show that either side implies the other.

$\underline{(i) \Rightarrow (iii)}$ Defining the predicate DCF by

$\quad$ DCF.x $\equiv$ (all descending chains in C with x as leading element are of finite length)

we observe

$$DCF.x \not\equiv (\underline{E}y: y \text{ in } C \wedge y < x: \neg DCF.y)$$

and further

$$
\begin{array}{l}
\quad (i) \\
\Rightarrow \{\text{mathematical induction over } C \text{ valid}\} \\
\quad (\underline{A}x{:}\, x \in C{:}\, DCF.x) \equiv \\
\quad (\underline{A}x{:}\, x \in C{:}\, DCF.x \;\vee\; (\underline{E}y{:}\, y \;\underline{in}\; C \wedge y<x{:}\, \neg DCF.y)) \\
= \{\text{right-hand side} \equiv true\} \\
\quad (\underline{A}x{:}\, x \in C{:}\, DCF.x) \\
= \{\text{def. of } DCF\} \\
\quad (iii)
\end{array}
$$

$\neg(i) \Rrightarrow \neg(iii)$ Let C be not well-founded, i.e. there exists a non-empty V without minimal element, i.e. such that

$$(\underline{A}x{:}\, x \in V{:}\, (\underline{E}y{:}\, y<x{:}\, y \in V)) \quad ;$$

but this expresses that each x in V is the leading element of an infinite descending chain in V, from which, V being non-empty, $\neg(iii)$ follows.

(End of Proof Th. 6.1.)

Needless to say, a theorem as beautiful as Theorem 6.1 is of profound significance. The equivalence of (i) and (iii) is nice when we are interested in the existence of minimal elements of subsets, the equivalence between (ii) and (iii) is of particular interest for computing: associating terminating computations with descending chains of finite length, we see some sort of link between finite computations on the one hand and the validity of an inductive argument on the other: computation and mathematical induction go somehow hand in hand.

A well-known example of a well-founded set is presented by the natural numbers with $<$ with its standard meaning; we appeal to its well-foundedness whenever we prove something by mathematical induction over the natural numbers.

Another well-known example is provided by the sentences of a programming language —or any formalism with a similar grammar—; here "$<$" should be read as "occurs as subsentence in" —clearly a transitive relation!—. It leads to "induction over the grammar" as we have encountered in Chapter 4, "Semantics of straight-line programs".

Well-founded sets being the indispensable ingredient of all termination arguments, computing scientists are regularly invited to invent the proper well-founded set that will carry the termination argument. In this connection, what is known as "The Lexical Ordering" is particularly relevant, as it allows us to construct new well-founded sets from given ones.

Consider two sequences $x.i$ $(0 \le i < n)$ and $y.i$ $(0 \le i < n)$ —note that the sequences are of finite length!—, called x and y respectively; let for each i the elements $x.i$ and $y.i$ belong to the same well-founded set, so that $x.i < y.i$ is defined (i.e. to refer to the ordering relation corresponding to that well-founded set). We now define on the sequences x and y

an order by defining $x<y$ by

$$x<y \equiv$$
$$(\underline{E}i: 0\leq i<n: (\underline{A}j: 0\leq j<i: x.j=y.j) \wedge x.i<y.i) \quad .$$

This is called "The Lexical Order"; it is well-founded if, for all i, $x.i$ and $y.i$ are taken from a well-founded set and vice versa; the proof is left to the reader. (Sometimes one finds the lexical order only defined for $n=2$, i.e. as a - often barely visible - infix operator; this infix operator is as associative as juxtaposition. We leave the proof to the interested reader.)

<u>Example</u> Given a finite bag of natural numbers; a move consists of replacing an x from the bag by a finite bag of natural numbers all $<x$. Show that the game terminates (because the bag has become empty).

Let all numbers in the bag be $<n$; characterize the contents of the bag by listing for $n>j\geq 0$ in the order of decreasing j the frequency with which j occurs in the bag. Each frequency being a natural number, the lexical order induces well-foundedness on the frequency listings; furthermore the frequency listing is lexically decreased by each move. (End of Example.)

(End of Intermezzo on well-founded sets.)

After the above intermezzo we return to Theorem 6.0, which we still have to prove.

<u>Proof Th. 6.0</u> On account of (9) — the definition of $wp(DO, ?)$ — we can prove (16) by showing

$$[P \Rightarrow Q]$$

for any Q that satisfies

$$[Q \equiv (\neg B \vee wp(S,Q)) \wedge (B \vee P)] ,$$

an equation, from which we derive by predicate calculus (because we shall need them in a moment) the implications

(19) $\quad [\neg B \wedge P \Rightarrow Q]$

(20) $\quad [P \Rightarrow (\neg B \vee wp(S,Q) \equiv Q)]$.

We shall show $[P \Rightarrow Q]$ by showing separately

(i) $\quad [P \wedge \neg\, t \in C \Rightarrow Q]$ and subsequently

(ii) $\quad [P \wedge t \in C \Rightarrow Q]$.

<u>Proof of (i)</u>

$$\begin{array}{l} \quad \mathit{true} \\ = \{(14) \text{ and predicate calculus}\} \\ \quad [P \wedge \neg\, t \in C \Rightarrow \neg B \wedge P] \\ \Rightarrow \{(19)\} \\ \quad [P \wedge \neg\, t \in C \Rightarrow Q] \end{array}$$.

(End of Proof of (i).)

Proof of (ii).

This part of the proof relies on the fact that C is well-founded. In order to exploit this fact, we first manipulate our demonstrandum so as to make it amenable to a proof by mathematical induction over C.

$[P \wedge t \in C \Rightarrow Q]$
$= \{(12)\}$
$[P \wedge (\underline{E}x : x \in C : t = x) \Rightarrow Q]$
$= \{$distribution of $\wedge$ over existential quantification$\}$
$[(\underline{E}x : x \in C : P \wedge t = x) \Rightarrow Q]$
$= \{$predicate calculus; interchange of univ. quantification$\}$
$(\underline{A}x : x \in C : [P \wedge t = x \Rightarrow Q])$.

In view of C's well-foundedness, the latter is proved by deriving —for any x in C—

(21) $[P \wedge t = x \Rightarrow Q]$

from

(22) $(\underline{A}y : y \in C \wedge y < x : [P \wedge t = y \Rightarrow Q])$.

To this end we observe

(22)
$= \{$interchange of quantifications; predicate calculus$\}$
$[(\underline{E}y : y \in C \wedge y < x : P \wedge t = y) \Rightarrow Q]$
$= \{ [t = y \wedge y < x \equiv t = y \wedge t < x] \}$
$[(\underline{E}y : y \in C : P \wedge t = y \wedge t < x) \Rightarrow Q]$
$= \{$distribution of $\wedge$ over existential quantification$\}$

$$
\begin{aligned}
& [P \wedge (\underline{E}y : y \in C : t = y) \wedge t < x \Rrightarrow Q] \\
= & \{(12)\} \\
& [P \wedge t \in C \wedge t < x \Rrightarrow Q] \\
= & \{[P \wedge \neg t \in C \wedge t < x \Rrightarrow Q] \text{ on account of (i)}\} \\
& [P \wedge t < x \Rrightarrow Q] \\
\Rightarrow & \{ wp(S, ?) \text{ is monotonic}\} \\
& [wp(S, P \wedge t < x) \Rrightarrow wp(S, Q)] \\
\Rightarrow & \{(15)\} \\
& [P \wedge B \wedge t = x \Rrightarrow wp(S, Q)] \\
= & \{\text{predicate calculus}\} \\
& [P \wedge t = x \Rrightarrow \neg B \vee wp(S, Q)] \\
= & \{(20)\} \\
& [P \wedge t = x \Rrightarrow Q] \\
= & \{\text{definition}\} \\
& (21)
\end{aligned}
$$

(End of Proof of (ii).)
(End of Proof Th.6.0.)

* * *

We recall for our next discussion

(4) $\quad DO = \underline{\text{if}}\ B \rightarrow S; DO\ [\!]\ \neg B \rightarrow skip\ \underline{\text{fi}}$.

The intended equivalence of these two statements led us to considering extreme solutions of equations of the form

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

with f of the form

(24) $\quad [f.(X,Y) \equiv (\neg B \vee k.Y) \wedge (B \vee X)]$

According to (8), wlp(DO,X) is the weakest solution of (23) with wlp(S,?) for k ; according to (9), wp(DO,X) is the strongest solution of (23) with wp(S,?) for k .

Since the semantics of a program should not be changed if we replace one of its constituent statements by a semantically equivalent one we derive from (4)

(25) DO = <u>if</u> $B \rightarrow$ S;
<u>if</u> $B \rightarrow$ S; DO ▯ $\neg B \rightarrow$ skip <u>fi</u>
▯ $\neg B \rightarrow$ skip
<u>fi</u> .

<u>Remark</u> The right-hand side of (4) is sometimes referred to as "the first unfolding of DO"; the right-hand side of (25) is similarly called "the second unfolding of DO". Unfolding —and the inverse transformation, called "folding"— are standard program transformations, which may be used to transform one program into another semantically equivalent one (for instance with the aim of proving their equivalence). (End of Remark.)

Equation (25) immediately raises the question what equation we would have got instead of (23), had we started from (25) instead of from (4), and also: would we get the same extreme solutions?

Taking the wlp or the wp from both sides of (25) yields instead of (23)

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

with for k the same choices wlp(S,?) and wp(S,?) respectively. Had we "Curried" f. i.e. had we defined the function $\tilde{f}$ of two arguments by

$$[\tilde{f}.X.Y \equiv f.(X, Y)] \quad ,$$

we could write the above equation

$$Y: [Y \equiv (\tilde{f}.X)^2.Y] \quad ;$$

from Lemma 5.13 we learn that it has the <u>same</u> extreme solutions as (23), for the occasion —functional application being left-associative— rewritten as

$$Y: [Y \equiv (\tilde{f}.X).Y] \quad .$$

This is very comforting. (It were, in fact, considerations like the above that led us to Lemma 5,13. The following "obviously correct" Theorem led similarly to Lemma 5.14.)

<u>Theorem 6.2</u> DO = DO;DO

<u>Proof Th. 6.2</u> Since equivalence of programs means equality of their predicate transformers, we have to show that wlp(DO,?) and wp(DO,?) are idempotent. Since $\neg B \vee k.Y$ is monotonic in Y for

both choices for k , and $B \vee X$ is monotonic, weakening, and idempotent in X , we conclude on account of (24) that equation (23) meets the requirements of Lemma 5.14 and, hence, has idempotent extreme solutions.

(End of Proof Th. 6.2)

<u>Theorem 6.3</u> $DO = $ <u>do</u> $B \rightarrow DO$ <u>od</u> .

<u>Proof Th. 6.3</u> Let $e.X$ be an extreme solution of (23) with the appropriate choice for k (i.e. $wlp(S,?)$ if $e.X$ is the weakest solution and $wp(S,?)$ if $e.X$ is the strongest solution). From (23) and (24) we then deduce

(26) $$[e.X \equiv (\neg B \vee k.(e.X)) \wedge (B \vee X)]$$.

The predicate transformers of <u>do</u> $B \rightarrow DO$ <u>od</u> are then the corresponding extreme solutions of

(27) $$Y{:}[Y \equiv (\neg B \vee e.Y) \wedge (B \vee X)]$$

We observe

$\neg B \vee e.Y$

$=$ { (26) with $X := Y$ }

$\neg B \vee ((\neg B \vee k.(e.Y)) \wedge (B \vee Y))$

$=$ { $\vee$ distributes over $\wedge$ }

$(\neg B \vee \neg B \vee k.(e.Y)) \wedge (\neg B \vee B \vee Y)$

$=$ { predicate calculus }

$\neg B \vee k.(e.Y)$

Hence (27) is the same equation as

$$Y\colon [Y \equiv (\neg B \vee k.(e.Y)) \wedge (B \vee X)]$$

i.e. - see (24)

(27') $\quad Y\colon [Y \equiv f.(X, e.Y)]$.

On account of (24) and Lemma 5.14, our f satisfies the requirement of Lemma 5.15 - even for any monotonic ip - , hence the corresponding extreme solution of (27') is again e .

(End of Proof Th. 6.3)

Austin, 15 April 1985

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
United States of America