A summary of formulae (and of some theory).

The following contains nothing new and nothing deep. It is written in reaction to my exposure to recent work of C.A.R.Hoare and of C.S.Scholten, in which I needed all kinds of formulae of which I was, until recently, only vaguely aware. Some formulae I knew longer have been included for the sake of completeness. As we have done lately, universal quantification over all states will be denoted by enclosure within square brackets. The boolean operators are in the order of decreasing priority: $\neg \ \wedge \ \vee \ \Rightarrow \ =$. Following a suggestion of Jan L.A. van de Snepscheut's, I shall not rely on conjunction's priority over disjunction: the omission of brackets would destroy too much symmetry. The letters B, P, Q, R, X, Y, and Z will only be used to denote predicates. Functional application has the highest priority of all.

(0) $[P \Rightarrow Q \ = \ (P \wedge Q = P)]$ for all P, Q

(1) $[P \Rightarrow Q \ = \ (P \vee Q = Q)]$ for all P, Q .

(2) $[(\neg B \vee P) \wedge (B \vee Q) = (B \wedge P) \vee (\neg B \wedge Q)]$ for all P, Q, B

A predicate transformer f that distributes over conjunction, i.e. that satisfies

(3) $[f(P \wedge Q) = fP \wedge fQ]$ for all P, Q

is called "conjunctive". Similarly, a predicate transformer f that distributes over disjunction, i.e. that satisfies

(4) $[f(P \vee Q) = fP \vee fQ]$ for all P, Q

is called "disjunctive". A predicate transformer f that is conjunctive or disjunctive is monotonic, i.e. satisfies

(5) $[P \Rightarrow Q] \Rightarrow [fP \Rightarrow fQ]$ for all P, Q .

For conjunctive f, (5) follows from (0), for disjunctive f, (5) follows from (1) — more precisely from their consequences $[P \Rightarrow Q] = [P \wedge Q = P]$ and $[P \Rightarrow Q] = [P \vee Q = Q]$ respectively — . Since being conjunctive or disjunctive is not uncommon, monotonic predicate transformers are not uncommon.

An infinite sequence of predicates $P\,i$ $(i \geq 0)$ such that $(\underline{A}\,i : i \geq 0 : [P\,i \Rightarrow P\,(i+1)])$ is called "weakening"; one such that $(\underline{A}\,i : i \geq 0 : [P\,(i+1) \Rightarrow P\,i])$ is called "strengthening". A sequence that is weakening or strengthening is called monotonic, and monotonic sequences are not uncommon since for monotonic f the sequence $f^i F$ is weakening and the sequence $f^i T$ is strengthening — as can be proved by mathematical induction.

A monotonic sequence of predicates $P\,i$ has a limit, for which we have the two alternative expressions

$$(\underline{A}\,i : i \geq 0 : (\underline{E}\,j : j \geq i : P\,j))$$

and

$$(\underline{E}\,i : i \geq 0 : (\underline{A}\,j : j \geq i : P\,j)) \quad .$$

For a weakening sequence of predicates $P\,i$ we have a third expression for the limit, viz. $(\underline{E}\,i : i \geq 0 : P\,i)$; similarly for the limit of a strengthening sequence of predicates $P\,i$, viz. $(\underline{A}i : i \geq 0 : P\,i)$.

A predicate transformer f that satisfies for any sequence of predicates $P\,i$ $(i \geq 0)$

$$(6) \quad [f(\underline{A}i : i \geq 0 : P\,i) = (\underline{A}i : i \geq 0 : f(P\,i))]$$

is called "infinitely conjunctive"; an infinitely conjunctive predicate transformer is conjunctive. A predicate transformer f that satisfies (6) for any strengthening sequence of predicates $P\,i$ $(i \geq 0)$ is called "and-continuous". A predicate transformer may be and-continuous without being conjunctive.

A predicate transformer f that satisfies for any sequence of predicates $P\,i$ $(i \geq 0)$

$$(7) \quad [f(\underline{E}i : i \geq 0 : P\,i) = (\underline{E}i : i \geq 0 : f(P\,i))]$$

is called "infinitely disjunctive"; an infinitely disjunctive predicate transformer is disjunctive. A predicate transformer f that satisfies (7) for any weakening sequence of predicates $P\,i$ $(i \geq 0)$ is called "or-continuous". A predicate transformer may be or-continuous without being disjunctive.

For the language fragment from "A Discipline of Programming" the predicate transformer $wp(S, ?)$ is infinitely conjunctive, hence conjunctive and and-continuous. As a result of its nondeterminacy it is not disjunctive, hence not infinitely disjunctive; as a result of its nondeterminacy being bounded, $wp(S, ?)$ is, however, or-continuous.

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

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

Relevant properties are

(8) $[f^{**} P = f\, P]$ for all P, i.e. the conjugate of f^* is f.

(9) (f is monotonic) = (f^* is monotonic)

(10) (f is (infinitely) conjunctive)
= (f^* is (infinitely) disjunctive)

(11) (f is <u>and</u>-continuous) = (f^* is <u>or</u>-continuous)

(12) $[(f \circ g)^* P = (f^* \circ g^*)\, P]$ for all P, i.e. the conjugate of a functional composition is the functional composition of the conjugates.

As a corollary we mention $[f^{i*} P = f^{*i} P]$.

(13) For a predicate transformer f defined by

$$[f\, P = (\underline{A}\, i : i \geq 0 : f_i\, P)] \text{ for all } P$$

we have

$$[f^* P = (\underline{E}\, i : i \geq 0 : f_i^* P)] \text{ for all } P .$$

* * *

For monotonic f the equations

(14) $X : [f\, X = X]$ and $X : [f\, X \Rightarrow X]$ have strongest solutions

that are equal, and

(15) $X:[X=fX]$ and $X:[X\Rightarrow fX]$ have weakest solutions that are equal.

Property (15) follows from (14) with f replaced by f^* -see 9-. For (14) I include C.S. Scholten's proof.

<u>Proof</u> With Q defined by $[Q=(\underline{A}X:[fX\Rightarrow X]:X)]$ we shall first show that Q is the strongest solution of $X:[fX\Rightarrow X]$.

$\underline{true}$

$=$ {definition of Q}

$[Q=(\underline{A}X:[fX\Rightarrow X]:X)]$

$\Rightarrow$ {predicate calculus}

$[Q\Rightarrow(\underline{A}X:[fX\Rightarrow X]:X)]$

$=$ {predicate calculus}

$[(\underline{A}X:[fX\Rightarrow X]:Q\Rightarrow X)]$

$=$ {predicate calculus}

$(\underline{A}X:[fX\Rightarrow X]:[Q\Rightarrow X])$ *

$\Rightarrow$ {f is monotonic}

$(\underline{A}X:[fX\Rightarrow X]:[fQ\Rightarrow fX])$

$=$ {predicate calculus}

$[(\underline{A}X:[fX\Rightarrow X]:fQ\Rightarrow fX)]$

$=$ {predicate calculus}

$[fQ\Rightarrow(\underline{A}X:[fX\Rightarrow X]:fX)]$

$\Rightarrow$ {predicate calculus}

$[fQ\Rightarrow(\underline{A}X:[fX\Rightarrow X]:X)]$

$=$ {definition of Q}

$[fQ\Rightarrow Q]$

From the truth of the last line we conclude that Q is a solution of $X:[fX\Rightarrow X]$; the line marked with an asterisk then shows that Q is its strongest solution .

Continuing the above we have

$$\begin{array}{ll}
 & [fQ \Rightarrow Q] \\
\Rightarrow & \{f \text{ is monotonic}\} \\
 & [f(fQ) \Rightarrow fQ] \\
\Rightarrow & \{Q \text{ is the strongest solution of } X{:}[fX \Rightarrow X]\} \\
 & [Q \Rightarrow fQ]
\end{array}$$

From the truths of first and last lines we see $[fQ = Q]$, showing Q to be a solution of $X: [fX = X]$. The line marked with an asterisk implies $(\underline{A}X: [fX = X]: [Q \Rightarrow X])$, showing Q to be the strongest solution. (End of Proof.)

For a while we continue our study of the equation $X: [X = fX]$ with monotonic f. Let Y be a solution. Then we have

(16) $\quad [(\underline{E}i: i \geq 0: f^i F) \Rightarrow Y]$

(17) $\quad [Y \Rightarrow (\underline{A}i: i \geq 0: f^i T)]$

We shall give the proof of (16).

<u>Proof</u>. Having untrained my usage of the implication, I have to observe first

$$\begin{array}{ll}
 & [(\underline{E}i: i \geq 0: f^i F) \Rightarrow Y] \\
= & \{\text{definition of implication and de Morgan}\} \\
 & [(\underline{A}i: i \geq 0: \neg f^i F) \vee Y] \\
= & \{\text{predicate calculus}\}
\end{array}$$

$[(\underline{A}i: i \geq 0: \neg f^i F \vee Y)]$
$=$ {definition of implication}
$[(\underline{A}i: i \geq 0: f^i F \Rightarrow Y)]$
$=$ {predicate calculus}
$(\underline{A}i: i \geq 0: [f^i F \Rightarrow Y])$.

We proceed by mathematical induction over i .

Base. $[f^0 F \Rightarrow Y]$
$=$ {definition of iterated functional composition}
$[F \Rightarrow Y]$
$=$ {predicate calculus}
$\underline{true}$.

Step. $[f^i F \Rightarrow Y]$
$\Rightarrow$ {f is monotonic}
$[f(f^i F) \Rightarrow f Y]$
$=$ {definition of iterated functional composition}
$[f^{i+1} F \Rightarrow f Y]$
$=$ {Y is a solution of $X: [X = fX]$}
$[f^{i+1} F \Rightarrow Y]$.
(End of Proof.)

If, besides being monotonic, f is <u>or</u>-continuous, $(\underline{E}i: i \geq 0: f^i F)$ is the strongest solution of $X: [X = fX]$.

If, besides being monotonic, f is <u>and</u>-continuous, $(\underline{A}i: i \geq 0: f^i T)$ is the weakest solution of $X: [X = fX]$.

We shall prove the first of the two above statements.

<u>Proof</u>. In view of (16) it suffices to show that $(\underline{E}i: i \geq 0: f^i F)$ is a solution of $X: [X = fX]$. We observe for any Z:

$[Z = f(\underline{E}i: i \geq 0: f^i F)]$

$=$ {f is $\underline{\text{or}}$-continuous and $f^i F$ is a weakening sequence}

$[Z = (\underline{E}i: i \geq 0: f(f^i F))]$

$=$ {definition of iterated functional composition}

$[Z = (\underline{E}i: i \geq 0: f^{i+1} F) \vee f^0 F]$

$=$ {predicate calculus}

$[Z = (\underline{E}i: i \geq 0: f^i F)]$.

(End of Proof.)

* * *

Our interest in the equation $X{:}\,[X = fX]$ is derived from our intention that the program segments

(18) $\underline{\text{do}}\ B \rightarrow S\ \underline{\text{od}}$ (called "DO") and

(19) $\underline{\text{if}}\ B \rightarrow S;\ \underline{\text{do}}\ B \rightarrow S\ \underline{\text{od}}\ [\!]\ \neg B \rightarrow \text{skip}\ \underline{\text{fi}}$

be equivalent. Constructing the wp's and the wlp's, respectively, for (18) and (19), we conclude that wp (DO,R) be a solution of

(20) $X{:}\,[X = (\neg B \vee wp(S,X)) \wedge (B \vee R)]$

and that wlp(DO, R) be a solution of

(21) $X{:}\,[X = (\neg B \vee wlp(S,X)) \wedge (B \vee R)]$.

<u>Note</u>. We observe that (20) and (21) are the same equation if $[\neg B \vee (wp(S,X) = wlp(S,X))]$ for all X. (End of Note.)

We can rewrite these two equations as

$X: [X = hX]$ and $X: [X = kX]$ with

$[hX = (\neg B \vee wp(S,X)) \wedge (B \vee R)]$ for all X, and

$[kX = (\neg B \vee wlp(S,X)) \wedge (B \vee R)]$ for all X .

With "IF" equal to "$\underline{\text{if}}\ B \rightarrow S\ \underline{\text{fi}}$" we have

$[wp(IF,X) = B \wedge wp(S,X)]$ and $[wlp(IF,X) = \neg B \vee wlp(S,X)]$,

and, thanks to (2), we can redefine h and k :

(22) $[hX = wp(IF,X) \vee (\neg B \wedge R)]$ for all X, and

(23) $[kX = wlp(IF,X) \wedge (B \vee R)]$ for all X .

Predicate transformers h and k are infinitely conjunctive, hence monotonic and _and_-continuous. As a result $wlp(DO,R)$ defined by

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

is the _weakest_ solution of (21) .

In the absence of unbounded nondeterminacy, predicate transformer h is also _or_-continuous, and as a result $wp(DO,R)$ defined by

$$[wp(DO,R) = (\underline{E}i: i \geq 0: h^i F)]$$

is the _strongest_ solution of (20) . We remind the reader that, with the above definition of wp, (18) and (19) are, indeed, to be regarded as not equivalent as soon as unbounded nondeterminacy, which destroys <u>or</u>-continuity, has been included.

*   *   *

At the beginning of this note I announced that it would contain nothing new and nothing deep. I wrote it because its contents seems insufficiently known. "Fundamental Structures of Computer Science" by William A. Wulf, Mary Shaw, Paul N. Hilfinger, and Lawrence Flon (Addison-Wesley Publishing Company, Inc. 1981), for instance, in spite of its ambitious title, its four authors, and its more than 600 pages, contains <u>nothing</u> of the above. (Some might consider the book's dedication embarrassing: "To the CMU Computer Science community: this couldn't have happened elsewhere.".)

Plataanstraat 5
5671 AL NUENEN
The Netherlands

2 May 1982
prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow.