Lecture notes "Predicate transformers" (Draft)

Introduction

The purpose of this course is manifold. A main target is the development of a number of theorems about predicate transformers, which have proved themselves to be a viable means for the definition of programming language semantics. It is our goal that this development be as self-contained as possible; as a consequence, we shall not hesitate to derive results for which no novelty is claimed. With the statement of our intention to give a "self-contained development" we mean that we intend to build on little more than the predicate calculus.

We have a secondary target, however. We have strong indications that the predicate calculus can serve as much more than just a basis to build upon and that, when properly used, it can be a very useful tool lending itself to intensive usage. Hence our secondary target: showing how the predicate calculus can be used at good advantage.

So we shall use the predicate calculus intensively. In doing so we hope to discover —and in this respect our development can be viewed as gathering experience— how to separate the many, many formulae from the predicate calculus into those to be known and those to be derived when needed. This (as yet absent) body of experience is needed when we wish to learn and then to teach how to use the predicate calculus sufficiently effectively, i.e. several orders of magnitude more effectively than its untrained user applies it. The inspiration for this last desire is very simple. On

the one hand -as some reflexion shows- the predicate calculus is the most promising carrier for convincing arguments about specific programs and for the derivation of programs meeting given specifications. On the other hand the viability of the predicate calculus as tool for programming methodology has been doubted on account of the experience that, in situations more ambitious than toy examples, formulae quickly tended to get unwieldy. We have reasons to believe that this disappointing experience is less due to some intrinsic inadequacy of the predicate calculus than to lack of knowledge how to use the predicate calculus well. Hence our desire to learn how to do the latter.

As said above, we intend to build on the predicate calculus. That means that we assume our readers able to convince themselves of the correctness of all its formulae we use and that we leave its definition and foundation gladly to the logicians, who are the experts in that field.

In contrast, we shall be fairly explicit about our notational conventions -conventions to which we intend to stick religiously-. We have to, not only because the world that agrees what the predicate calculus is about does not display a similar consensus on what notational conventions to adopt, but also because -after much hesitation and careful consideration- I have adopted a few conventions of my own that, to the best of my knowledge and foresight, made my formulae better suited to my manipulative needs. (Adoption of a notational convention of one's own is a very grave step; I found the courage to take it in the observation that it enabled me to ma-

nipulate my formulae much more simply and systematically than I could have done otherwise. I am perfectly willing to discuss the merits of my conventions with those of alternatives; the freedom to shed the notational shackles with which others are trying to live and to work I consider, however, the scientist's inalienable right, not withstanding the fact that I know full well the difficulty of making good use of it.)

General concepts and notational conventions

We consider predicates to be two-valued total functions defined on the Cartesian product of the spaces belonging to zero or more named coordinates, in this context also often referred to as variables. The spaces belonging to the individual coordinates are non-empty and well-understood —say, as well-understood as the integers or the natural numbers—.

Note that the trivial space of zero dimensions is deemed to consist of a single anonymous point. Hence, only two different predicates can be defined on the trivial space; they are denoted by true and false respectively.

A predicate in x and y is also a predicate in x, y, and z; its value not depending on z, it enjoys in this three-dimensional space the special property of being constant along lines in the z-direction. In other words, a predicate on a given space is also a predicate on any space of more dimensions of which the given space is a "Cartesian factor". The trivial space being a factor of any space, aforementioned predicates are defined on any space.

As a result, two predicates, each with its own space, can always be regarded as predicates in the same space, viz. "the least common Cartesian multiple" of their individual spaces; when two predicates on possibly different spaces are connected to form a new predicate, the latter is a predicate on that "least common Cartesian multiple," e.g. if P is a predicate in x and y, and Q is a predicate in y and z, connecting P and Q yields a predicate in x, y, and z.

Note that from a predicate in at least two variables we can always form without loss of information a predicate in one variable less: for a predicate in x and y we can construct a predicate in a new variable instead that ranges over all ordered pairs (x,y). We shall only consider predicates depending on a finite number of variables, and the moral of the previous remark is that their precise number is a bit arbitrary. (This need not disturb us too much: the system of two equations P and Q is also the system of the one equation $P \wedge Q$.) Since a variable may be of a type with an infinite range - e.g. of type integer - the number of points of a predicate's space need not be finite.

Side remark. Variables ranging over a class of predicates will not be excluded. We shall - in order to avoid all sorts of difficulties - never introduce a predicate whose value depends on a variable of which the predicate itself is a possible value. As far as I can see this constraint will not prevent me from introducing all the recursive predicate definitions I need. (End of Side remark.)

From predicates we shall construct new predicates using the well-known operators -given in order of decreasing binding power-

$\neg$	negation
$\wedge$	conjunction
$\vee$	disjunction
$\Rightarrow$	implication
$\equiv$	equivalence
$\not\equiv$	difference

Note. Since it does not matter whether we write

$$(P \equiv Q) \not\equiv R \quad \text{or} \quad P \equiv (Q \not\equiv R)$$

the suggested greater binding power of $\equiv$ over $\not\equiv$ is spurious. I could have given them in the same line, or the other way round. (End of Note.)

Negation is a unary operator and is point-wise defined: P and $\neg P$ are defined on the same space, in each point of which the one of them is true and the other is false.

The others are binary operators, and are point-wise defined on the smallest common Cartesian multiple of the spaces of their arguments.

Conjunction is symmetric and associative: it is true where all its arguments are true, and false elsewhere.

Disjunction is symmetric and associative: it is false where all its arguments are false, and true elsewhere.

Implication is neither symmetric nor associative; the distinction between $P \Rightarrow Q$ and $\neg P \vee Q$ is only textual. We shall use implication only where its asym-

metry can be exploited to advantage.

Note. Together with universal quantification - see below- implication can be used for the definition of a partial order among predicates which enables us to link the predicate calculus to lattice theory. This fact is of fundamental significance; its lack of symmetry and of associativity, however, make it cumbersome to manipulate. Universal quantification often being left implicit, it has led to endless confusions —vide the rather scholastic flavour of the distinction between the "logical implication" and the "material implication"—. We shall not hesitate to use implication in the trivial space in which universal quantification - whether hidden or not— is the identity function. (End of Note.)

Equivalence is symmetric and associative: it is true where an even number of its arguments are false, and is false elsewhere.

Difference is symmetric and associative: it is false where an even number of its arguments are true, and is true elsewhere.

Equivalence and difference usually occur with two arguments, and rarely with more than three (which is not amazing in view of the rôle of the notion "even").

There is one drastic way of deriving from a predicate P on some space a predicate on the trivial space: universal quantification over all points of the space on which P is defined. Since in many of our manipulations that space will be left anonymous —we have already seen that its actual dimension is not of overwhelming relevance— and we need that universal quantification

quite frequently denoted, we introduce a special notation for it, viz. surrounding P by a pair of square brackets: $[P]$. Axioms, theorems, "facts", definitions, etc. will frequently be expressed in terms of such universally quantified predicates, e.g. defining for given Q the predicate P by

$$[P \equiv Q]$$

means that the distinction between "P" and "Q" is only textual – as is the distinction between "$[P \equiv Q]$" and "true" – . Thus we can express the following rewrite rules, applicable to any P , Q , and R . (For a start we give both the fully parenthesized form and the form in which parenthesis pairs that our binding conventions have made redundant have been omitted.)

$[(\neg(\neg P)) \equiv P]$	$[\neg\neg P \equiv P]$
$[(\neg(P \wedge Q)) \equiv ((\neg P) \vee (\neg Q))]$	$[\neg(P \wedge Q) \equiv \neg P \vee \neg Q]$
$[(P \Rightarrow Q) \equiv ((\neg P) \vee Q)]$	$[P \Rightarrow Q \equiv \neg P \vee Q]$

Remarks. A comparison of the above two columns strongly suggests that the writing of the fully parenthesized form is a pain in the neck. So we had better appeal to the binding conventions to eliminate a number of parenthesis pairs.

In general I cannot recommend the exploitation of the convention that gives the conjunction a greater binding power than the disjunction, since this convention introduces the syntactic destruction of a semantic symmetry.

In the case of long formulae it is recommended to surround the connective with the lowest binding

power by some additional blank space.

Comment. This is a suggestion very similar to the well-known "rules of indentation" that have established themselves —almost by natural selection— for many a programming language. Impressed by indentation's "aid to readability", some language designers have gone a step further and have given indentation a rôle in the definition of the nesting structure of the text. In my experience the convention leads to consequences that are in conflict with other purposes of layout, and hence I cannot recommend it. (End of Comment.)

In order to avoid confusion with the Roman v and V and with the Greek $\wedge$, I recommend striving for a right angle when writing $\vee$ or $\wedge$.
(End of Remarks.)

With P and Q "of type Boolean" — i.e. predicates on the trivial space — many theorems are expressed in terms of $P \equiv Q$ or of $P \Rightarrow Q$. When this is not an obvious instance of a known formula, we prove it in two or more steps by the introduction of one or more intermediate predicates.

So may the computation that $P \equiv Q$ has the value true take the form of establishing that for some properly chosen R, $P \equiv R$ and $R \equiv Q$ both have the value true.

So may the computation that $P \Rightarrow Q$ has the value true take the form of establishing that for some properly chosen R, $P \equiv R$ and $R \Rightarrow Q$ both have the value true.

Remark. In view of the use made of $P \equiv R$ in the last example, it would have "sufficed" to compute that

$P \Rrightarrow R$ has the value true. For the sake of clarity, we shall not use the implication where the equivalence applies. (End of Remark.)

For very fundamental reasons we need a notational convention that allows us to render the structure of such a proof in a way such that the intermediate predicate R needs to be written down only once.

The above computation that $P \equiv Q$ has the value true will be represented as follows:

$$\begin{array}{ll} & P \\ = & \{\text{hint why } P \equiv R \text{ has the value true}\} \\ & R \\ = & \{\text{hint why } R \equiv Q \text{ has the value true}\} \\ & Q \quad . \end{array}$$

The above computation that $P \Rrightarrow Q$ has the value true will be represented as follows:

$$\begin{array}{ll} & P \\ = & \{\text{hint why } P \equiv R \text{ has the value true}\} \\ & R \\ \Rrightarrow & \{\text{hint why } R \Rrightarrow Q \text{ has the value true}\} \\ & Q \quad . \end{array}$$

Legenda. In the above "why" can be read (four times) as "how the reader can convince himself that". Whether the hint suffices depends at least as much on the reader as on the writer: if the reader is to convince himself —whatever that may mean!— he is the one to do that. (End of Legenda.)

The reasons for selecting a notation that mentions the intermediate predicate R only once are the following. In non-trivial proofs, such an R is often a formula of some length. Writing it out twice

would not only be a burden on the writer (which would not matter if it helped the reader) but also a burden on the reader, who would have to perform a string comparison in order to establish the (for the argument essential) sameness of the two occurrences. This, of course, could be circumvented by giving the formula a name, R say.

But we should not burden our texts with names if we can avoid them. Naming something which is referred to by name only once is obviously pointless; two references is therefore the most meagre justification for the introduction of a new name. This justification is insufficient when the duplication can be avoided by placing the "something" in some sort of infix position, provided the notational convention thus introduced is used sufficiently frequently.

Note. Since the scaling up of discrete reasoning is one of the central challenges of computing science, seemingly minor details like the size of the nomenclature to be introduced need our attention. (End of Note.)

Syntactic remark. When thus representing demonstrations, we give the separators "$=\{hint\}$" and "$\Rightarrow\{hint\}$" the lowest binding power of all. (End of Syntactic remark.)

Occasionally we shall compute that $P \equiv Q$ has the value true by computing that both $P \Rightarrow Q$ and $Q \Rightarrow P$ have the value true. Omitting intermediate steps, we can render the structure of that computation by

```
    P
⇒ { hint 1 }
    Q
⇒ { hint 2 }
    P
```

Here the use of the ⇒ could have been avoided: with the same hints we could have written

```
    P                          P
= { hint 1 }               = { hint 2 }
    P ∧ Q        or            P ∨ Q
= { hint 2 }               = { hint 1 }
    Q                          Q
```

Our earlier version, however, is shorter.

For $[P \Rightarrow Q]$ we also read "P is as strong as Q" or "Q is as weak as P"; for $[P \Rightarrow Q] \wedge \neg[P \equiv Q]$ we also read "P is stronger than Q" or "Q is weaker than P". The nature of our game is now clear: from one line to the next we shall massage predicate expressions either hinting why equivalence holds or why in the transition to the next line we have not strengthened the predicate.

As said before, this is not the moment to give an exhaustive catalogue which hints to admit. I expect to give the not very descriptive hint "{predicate calculus}" wherever it seems obvious to me which by then familiar rewriting rule has been applied. Some of them I shall take for granted right at the start, such as the following

$$[P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)]$$
$$[P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)]$$

expressing the mutual distributivity of conjunction and disjunction. Since also

(0) $\quad [P \equiv Q] \Rightarrow ([P] \equiv [Q])$

has the value true for any P and Q, we compute that also

$$[P \wedge (Q \vee R)] \equiv [(P \wedge Q) \vee (P \wedge R)]$$

has the value true for any P, Q, and R.

Reasonably well-known is the formula

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

(and so is its companion $[P \Rightarrow Q] \equiv [Q \equiv P \vee Q]$); the abominable Venn-diagrams have seen to that. It is, however, with the aid of (0) a direct consequence of the also valid

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

-easily settled by the point-wise argument substituting for P true and false respectively, and computing that both

$$[\, Q \equiv \text{true} \equiv Q \,] \quad \text{and} \quad [\text{true} \equiv \text{false} \equiv \text{false}]$$

have the value true — . Remembering that $\equiv$ is symmetric and associative, we see two other ways of applying (0), yielding that both

$$[P \Rightarrow Q \equiv P] \equiv [P \wedge Q] \qquad \text{and}$$
$$[P \Rightarrow Q \equiv P \wedge Q] \equiv [P]$$

have the value true. (Neither of the last two formulae seems worth remembering. They were derived by way of illustration.)

* * *

Formulae specially related to the fact that square brackets denote universal quantification (over a non-empty space) are

$$[P] \vee [Q] \Rightarrow [P \vee Q]$$

$$[P] \wedge [Q] \equiv [P \wedge Q]$$

$$[P] \vee [Q] \equiv [P \vee [Q]]$$

$$[P] \wedge [Q] \equiv [P \wedge [Q]]$$

– the last formula only being valid because the space is not empty – (Well, not really!)

* * *

Besides (universal) quantification over the points of the space of a predicate, we need quantification over predicates from a bag $\mathcal{B}$ of predicates defined on the same space. Universal quantification is expressed by

$$(\underline{A}\, X: X \underline{in}\, \mathcal{B}: X)$$

In the case of a finite bag $\mathcal{B}$, this expression denotes the conjunction of the elements of $\mathcal{B}$. It then satisfies

(1) $$(\underline{A}\, X: X \underline{in}\, \mathcal{B}: [X]) \equiv [(\underline{A}\, X: X \underline{in}\, \mathcal{B}: X)]$$

– i.e. universal quantifications commute –

(2) $$[(\underline{A}\, X: X \underline{in}\, \mathcal{B}: Q \vee X) \equiv Q \vee (\underline{A}\, X: X \underline{in}\, \mathcal{B}: X)]$$

– i.e. disjunction distributes over universal quantification –

(3) $$(\underline{A}\, Y: Y \underline{in}\, \mathcal{B}: [(\underline{A}\, X: X \underline{in}\, \mathcal{B}: X) \Rightarrow Y])$$

Formula (1), (2), and (3) are postulated to apply as well in the case of an infinite bag $\mathcal{B}$; $\mathcal{B}$ need

not even be denumerable.

From (3) it follows that $(\underline{A}X: X \underline{in} B: X)$ is a solution of

(4) $\quad Z: (\underline{A}Y: Y \underline{in} B: [Z \Rightarrow Y])$.

Note on notation. For given Z and Y, $[Z \Rightarrow Y]$ is a predicate on the trivial space. For given Z and B, $(\underline{A}Y: Y \underline{in} B: [Z \Rightarrow Y])$ is again a predicate on the trivial space. By prefixing it with "$Z:$" we form the equation whose roots are those predicates that, (when substituted for Z) make the prefixed predicate coincide with true . (End of Note on notation.)

Furthermore we have for any P

$$
\begin{array}{ll}
 & (\underline{A}Y: Y \underline{in} B: [P \Rightarrow Y]) \\
= & \{\text{predicate calculus, (1) in particular}\} \\
 & [(\underline{A}Y: Y \underline{in} B: P \Rightarrow Y)] \\
= & \{\text{predicate calculus}\} \\
 & [(\underline{A}Y: Y \underline{in} B: \neg P \vee Y)] \\
= & \{\text{predicate calculus, i.e. (2) with } \neg P \text{ for } Q\} \\
 & [\neg P \vee (\underline{A}Y: Y \underline{in} B: Y)] \\
= & \{\text{predicate calculus and renaming}\} \\
 & [P \Rightarrow (\underline{A}X: X \underline{in} B: X)]
\end{array}
$$

Comparing the first line of the above deduction with (4) we see that any solution of (4) is as strong as $(\underline{A}X: X \underline{in} B: X)$, which is therefore the weakest solution of (4).

Conversely we could have <u>defined</u> $(\underline{A}X: X \underline{in} B: X)$ as the weakest solution of (4); in that case the existence of the weakest solution should have been postulated.

Defining $(\underline{E}X: X \underline{in} \mathcal{B}: X)$ – existential quantification – by $[(\underline{E}X: X \underline{in} \mathcal{B}: X) \equiv \neg(\underline{A}X: X \underline{in} \mathcal{B}: \neg X)]$ – which very much looks like a generalization of de Morgan's Law –, this expression denotes in the case of a finite bag $\mathcal{B}$ the disjunction of its elements. Analogously to (2) and (3) we have

(5) $[(\underline{E}X: X \underline{in} \mathcal{B}: Q \wedge X) \equiv Q \wedge (\underline{E}X: X \underline{in} \mathcal{B}: X)]$

– i.e. conjunction distributes over existential quantification – and

(6) $(\underline{A}Y: Y \underline{in} \mathcal{B}: [Y \Rightarrow (\underline{E}X: X \underline{in} \mathcal{B}: X)])$.

Conversely we could have <u>defined</u> $(\underline{E}X: X \underline{in} \mathcal{B}: X)$ as the strongest solution of

(7) $Z: (\underline{A}Y: Y \underline{in} \mathcal{B}: [Y \Rightarrow Z])$

together with the postulate that that solution exists.

Between the colons we had "$X \underline{in} \mathcal{B}$" or "$Y \underline{in} \mathcal{B}$"; this is referred to as the range of the dummy. The indication is omitted – what is indicated by placing the colons in immediate succession – when the range is understood, e.g. to be the set of all predicates on the space under consideration, as is the case in the formulation of

(8) $(\underline{A}X:: [X \vee P] \equiv [X \vee Q]) \equiv [P \equiv Q]$

To compute that the above coïncides with true we use the elementary

$$[(P \vee \neg Q) \wedge (Q \vee \neg P) \equiv P \equiv Q]$$

and proceed as follows:

$$
\begin{array}{ll}
 & [P \equiv Q] \\
\Rightarrow & \{\text{pred. calc., viz. (0)}\} \\
 & (\underline{A}X :: [X \vee P] \equiv [X \vee Q]) \\
\Rightarrow & \{\text{choose } \neg P \text{ and } \neg Q \text{ respectively}\} \\
 & ([\neg P \vee P] \equiv [\neg P \vee Q]) \wedge ([\neg Q \vee P] \equiv [\neg Q \vee Q]) \\
= & \{\text{pred. calc.}\} \\
 & [\neg P \vee Q] \wedge [\neg Q \vee P] \\
= & \{\text{pred. calc.}\} \\
 & [(\neg P \vee Q) \wedge (\neg Q \vee P)] \\
\Rightarrow & \{\text{pred. calc. and (0)}\} \\
 & [P \equiv Q]
\end{array}
$$

Predicate transformers and programming languages.

Semantics of programming languages have been defined in terms of so-called "predicate transformers", in particular wp (="weakest precondition") and wlp (="weakest liberal precondition").

For a given program S and a postcondition R the operational interpretation of wp(S,R) is the weakest condition on the initial state such that firing S is guaranteed to lead to a terminating computation ending in a final state where R coincides with true.

In the case of unbounded nondeterminacy - as we shall see later - two different notions of termination present themselves. They correspond to two different definitions for wp that we shall denote differently. The distinction will be postponed until relevant.

The definition in terms of wp has the practical advantage that it fully captures what we are usually interested in when designing a program: in that situation

we are usually not too interested in initial states for which termination is not guaranteed. For such initial states the concept of wp alone leaves the semantics of the program undefined. This is no longer the case when we define the weakest liberal precondition as well.

For a given program S and a postcondition R the operational interpretation of $wlp(S,R)$ is the weakest condition on the initial state such that firing S is guaranteed to lead to a computation that either fails to terminate or ends in a final state where R coincides with true.

We shall give one further consequence of this operational interpretation: $\neg\, wlp(S,\neg R)$ characterizes those initial states for which firing S may lead to a computation ending in a final state where R coincides with true. (It expresses the possibility of R being finally valid. It pairs each final state to those initial states "from which it can be reached via S"; it thus opens the way of dealing with program semantics in terms of the relational calculus.)

These predicate transformers will be defined in the usual way, i.e. inductively over the syntax of the little programming language fragment. At the same time we would like to prove a number theorems, such as

Theorem 0. $[\neg\, wp(S,false)]$ for any program S.

Theorem 1. $[wlp(S,true)]$ for any program S.

Theorem 2. $[wp(S,R) \equiv wlp(S,R) \wedge wp(S,true)]$ for any program S and any R.

Theorem 3. $[wp(S,(\underline{A}P:P \underline{in} \mathcal{B}:P)) \equiv (\underline{A}P:P \underline{in} \mathcal{B}: wp(S,P))]$ for any program S and any non-empty bag $\mathcal{B}$ of predicates.

Theorem 4. $[wlp(S,(\underline{A}P:P \underline{in} \mathcal{B}:P)) \equiv (\underline{A}P:P \underline{in} \mathcal{B}: wlp(S,P))]$ for any program S and any bag $\mathcal{B}$ of predicates.

Theorem 3 follows from Theorems 2 and 4.

Proof For any X and any non-empty bag $\mathcal{B}$ of predicates

$$
\begin{array}{ll}
 & [X \equiv wp(S,(\underline{A}P:P \underline{in} \mathcal{B}:P))] \\
= & \{\text{Theorem 2}\} \\
 & [X \equiv wlp(S,(\underline{A}P:P \underline{in} \mathcal{B}:P)) \wedge wp(S,true)] \\
= & \{\text{Theorem 4}\} \\
 & [X \equiv (\underline{A}P:P \underline{in} \mathcal{B}: wlp(S,P)) \wedge wp(S,true)] \\
= & \{\mathcal{B} \text{ is non-empty}\} \\
 & [X \equiv (\underline{A}P:P \underline{in} \mathcal{B}: wlp(S,P) \wedge wp(S,true))] \\
= & \{\text{Theorem 2}\} \\
 & [X \equiv (\underline{A}P:P \underline{in} \mathcal{B}: wp(S,P))]
\end{array}
$$

(End of Proof.)

Remark. At the very end we have omitted explicit reference to $(\underline{A}X:: [X \equiv P] \equiv [X \equiv Q]) \equiv [P \equiv Q]$. We shall also do so in the sequel. (End of Remark.)

By now we have had two hints that of wp and wlp, the latter one has the nicer properties. The one is that $\neg wp(S,\neg R)$ —try to interpret it!— is not half as useful as $\neg wlp(S,\neg R)$; the other one is that, as a result of the added constraint "non-empty", Theorem 3 is not as beautiful as Theorem 4. (The added constraint "non-empty" is essential; without it, Theorem 3 would be wrong.)

In order to prove such theorems smoothly, we can make good use of a number of concepts and theorems about predicate transformers in general.

Let f be a predicate transformer, i.e. some function from predicates to predicates. Functional application will be denoted by juxtaposition, eg "f P", and will be given the highest binding power of all, i.e.

$$fP \wedge Q \quad \text{is short for} \quad (fP) \wedge Q \quad .$$

Note. For the time being we can postpone the decision whether functional application will be regarded as left-associative or right-associative. When the time comes I expect us to prefer left-associativity. (End of Note.)

Until further notice we shall confine ourselves to predicate transformers for which argument and value are predicates on the same space.

For a predicate transformer f and a bag B of predicates on the same space we define — inspired by the formulae in Theorems 3 and 4 — the notion of conjunctivity by

$$(f \text{ is conjunctive over } B) \equiv$$
$$[f(\underline{A}P: P \underline{in} B: P) \equiv (\underline{A}P: P \underline{in} B: fP)] \quad ,$$

and different degrees of conjunctivity by specifying over bags of which type f is conjunctive, in particular:

$$(f \text{ is universally conjunctive}) \equiv$$
$$(f \text{ is conjunctive over any bag})$$

(f is unboundedly conjunctive) ≡
(f is conjunctive over any non-empty bag)

(f is infinitely conjunctive) ≡
(f is conjunctive over any non-empty denumerable bag)

(f is conjunctive) ≡
(f is conjunctive over any non-empty finite bag) .

Note that as the class of bags over which conjunctivity is required gets smaller, the type of conjunctivity becomes a weaker property:
a universally conjunctive f is unboundedly conjunctive;
an unboundedly conjunctive f is infinitely conjunctive;
an infinitely conjunctive f is conjunctive (sec).

In our new jargon, we can summarize Theorems 3 and 4 by stating that wlp is universally conjunctive, whereas wp is only unboundedly conjunctive.

Note that, since universal quantification ∀ by definition coïncides with [f true] over the empty bag, for any f

(f is unboundedly conjunctive) ∧ [f true]
≡ (f is universally conjunctive) .

The importance of the various degrees of conjunctivity is probably to be found in the circumstance that the functional composition of two predicate transformers of the same degree of conjunctivity enjoys that same degree of conjunctivity. Let us define functional composition of predicate transformers first.

For any two predicate transformers f and g

the functional composition $f \circ g$ is defined by

$$[f \circ g\ X \equiv f(g\ X)] \text{ for any } X .$$

Note. Here the binding power of $\circ$ is deemed to be even higher than functional application. At the same time we have placed the parenthesis in $f\ (g\ X)$ as if we have already decided that functional application is left-associative. Were functional application chosen to be right-associative $f\ g\ X$ would be interpreted "automatically" as $f(g\ X)$, what we denote as $f \circ g\ X$. Right-associativity would make the character $\circ$ therefore rather superfluous. But Curry would not like its omission. We wish to be able to denote the functional composition e.g. by $f \circ g$; omission of the $\circ$ would then lead to $f\ g$, but this juxtaposition would then not be functional application. The decision to choose functional application to be left-associative —at least: not right-associative— came sooner than expected! (End of Note.)

Remark on notation. We have defined universal quantification for any bag $\mathcal{B}$ of predicates: $(\underline{A}X: X \underline{in} \mathcal{B}: X)$. We have, however, already used $(\underline{A}X: X \underline{in} \mathcal{B}: Q \vee X)$, which is a special case of $(\underline{A}X: X \underline{in} \mathcal{B}: fX)$.

For any bag $\mathcal{B}$ of predicates and any predicate transformer f we can define a new bag, denoted by

$$(\underline{\mathcal{B}}\ X: X \underline{in} \mathcal{B}: fX) ,$$

i.e. the bag $\mathcal{B}$ in which each element is replaced by fX. (This is standard usage of the bag formator $\underline{\mathcal{B}}$).

The more general universal quantification can then be defined by

$$[(\underline{A}X: X \underline{in} \mathcal{B}: fX) \equiv (\underline{A}Y: Y \underline{in} (\underline{B}X: X \underline{in} \mathcal{B}: fX): Y)] .$$

The same can be done for existential quantification.

The construction of $(\underline{B}X: X \underline{in} \mathcal{B}: fX)$ implies that $(\underline{B}X: X \underline{in} \mathcal{B}: fX)$ has "as many elements" as $\mathcal{B}$: they are both empty or both non-empty, they are both finite or both infinite, they are both denumerable or both nondenumerable. (End of Remark on notation.)

We now return to the conservation of degree of conjunctivity. Reading for BAG "bag", "non-empty bag", "non-empty denumerable bag" or "non-empty finite bag", we have the four theorems

$$(f \text{ and } g \text{ are both conjunctive over any BAG}) \Rightarrow (f \circ g \text{ is conjunctive over any BAG})$$

Four proofs. Let f and g be both conjunctive over any BAG and let $\mathcal{B}$ be a BAG. Then, for any Z

$$\begin{aligned}
&[Z \equiv f \circ g\ (\underline{A}X: X \underline{in} \mathcal{B}: X)] \\
&= \{\text{definition of functional composition}\} \\
&\quad [Z \equiv f\ (g(\underline{A}X: X \underline{in} \mathcal{B}: X))] \\
&= \{g \text{ is conjunctive over any BAG}\} \\
&\quad [Z \equiv f\ (\underline{A}X: X \underline{in} \mathcal{B}: gX)] \\
&= \{f \text{ is conjunctive over any BAG}\} \\
&\quad [Z \equiv (\underline{A}X: X \underline{in} \mathcal{B}: f\ (gX))] \\
&= \{\text{definition of functional composition}\} \\
&\quad [Z \equiv (\underline{A}X: X \underline{in} \mathcal{B}: f \circ g\ X)] \quad ,
\end{aligned}$$

hence $[f \circ g\ (\underline{A}X: X \underline{in} \mathcal{B}: X) \equiv (\underline{A}X: X \underline{in} \mathcal{B}: f \circ g\ X)]$
i.e. $f \circ g$ is conjunctive over any BAG.

(End of Four proofs.)

A predicate transformer is said to be monotonic if it preserves the partial order of universally quantified implication, more precisely

$$(f \text{ is monotonic}) \equiv (\text{for any } X \text{ and } Y \quad [X \Rightarrow Y] \Rightarrow [fX \Rightarrow fY]) .$$

Theorem. A conjunctive predicate transformer is monotonic.

Proof. For any conjunctive predicate transformer f and any two predicates X and Y

$$\begin{aligned}
& [X \Rightarrow Y] \\
= \ & \{ \text{pred. calc} \} \\
& [X \wedge Y \equiv X] \\
\Rightarrow \ & \{ \text{functional application} \} \\
& [f(X \wedge Y) \equiv fX] \\
= \ & \{ f \text{ is conjunctive} \} \\
& [fX \wedge fY \equiv fX] \\
= \ & \{ \text{pred. calc} \} \\
& [fX \Rightarrow fY]
\end{aligned}$$

(End of Proof).

* * *

Intermezzo. While lecturing last week I realized that I should probably have used the "bagifier": given a bag B containing x's on which a function f is defined, we can form a new bag

$$C = (\underline{B}x: x \underline{\text{in}} B: fx)$$

where B and C are both emply or not, etc. The one essential property of bagification is that with f the identity function, $C = B$, i.e.

$$C = (\underline{B}y: y \underline{\text{in}} C: y) .$$

The other essential property of bagification is

$$(\underline{B}\, x : x \underline{in} (\underline{B}\, y : y \underline{in} C : g\, y) : f\, x) =$$
$$(\underline{B}\, y : y \underline{in} C : f(g\, y)) \ .$$

(End of Intermezzo.)

* * *

With "P is a fixed point of f" meaning $[f\, P \equiv P]$ we can formulate the theorem:

> A common fixed point of f and g is also a fixed point of $f \circ g$, i.e. "functional composition is fixed-point preserving".

Proof. Let P be a fixed point of both f and g. Then for any Z

$$\begin{aligned}
&[Z \equiv f \circ g\ P] \\
&= \{\text{definition of functional composition}\} \\
&\quad [Z \equiv f\,(g\, P)] \\
&= \{P \text{ is a fixed point of } g\} \\
&\quad [Z \equiv f\, P] \\
&= \{P \text{ is a fixed point of } f\} \\
&\quad [Z \equiv P]
\end{aligned}$$

(End of Proof.)

The simple fact that fixed points are preserved by functional composition is our first indication that the notion of a fixed point might be an important concept.

* * *

We now proceed to define our little programming language, proving the Theorems 0, 1, 2, and 4 as we go along. Note that theorems 0 and 1 could have been formulated as

$$[wp(S, false) \equiv false] \text{ and } [wlp(S, true) \equiv true],$$

in other words: false is a fixed point of wp, and true is a fixed point of wlp.

The semantics of skip are defined by

$$[wp(skip, R) \equiv R] \text{ and } [wlp(skip, R) \equiv R]$$

for any R. Since any predicate is a fixed point of both wp and wlp, all five (or four) theorems are trivially correct.

Let x be one of the coordinates of the state space; let def E be the predicate that coincides with true wherever the expression E is defined, and false everywhere else.

Remark. The predicate def E is assumed to be a total function. Evaluation of E where def E is assumed to lead to a unique value of E, where $\neg$ def E, however, it is assumed to lead to a non-terminating computation. (End of Remark.)

The semantics of the assignment statement $x := E$ is given by

$$[wp(x := E, R) \equiv \text{def } E \text{ cand } R(E/x)] \quad \text{for any } R$$

$$[wlp(x := E, R) \equiv \neg \text{def } E \text{ cor } R(E/x)] \quad \text{for any } R$$

Here cand and cor are the socalled conditional and and or respectively: [false cand $X \equiv$ false]

$[\text{true } \underline{\text{cor}}\ X \equiv \text{true}]$ without assumptions that X is a total predicate. Note that $\underline{\text{cand}}$ and $\underline{\text{cor}}$ are not symmetric, but satisfy together de Morgans Law $[\neg(P\ \underline{\text{cand}}\ Q) \equiv (\neg P)\ \underline{\text{cor}}\ (\neg Q)]$. These connectives have been used to make the right-hand sides also total predicates if $\neg[\text{def } E]$.

The expression $R(E/x)$ is usually described as "the predicate R in which each occurrence of the variable x is replaced by E". We shall define it by

$$[R(E/x) \equiv R(x'/x)(E/x')]$$

where $R(x'/x)$ is a predicate defined on the same space as R, except that the coordinate x has been renamed x' — the name of a "fresh variable" —

$$R(x'/x) = (\underline{A}\, x :: x \neq x' \vee R)$$

and $$Q(E/x') = (\underline{A}\, x' :: x' \neq E \vee Q)\ .$$

Combining all this, we find

$$[R(E/x) \equiv (\underline{A}\, x' :: x' \neq E \vee (\underline{A}\, x :: x \neq x' \vee R))]\ .$$

Remark. The temporary shift to a predicate in which x has been renamed x' is necessary because E might depend on x. (End of Remark.)

Since in our usage of $R(E/x)$ — also denoted by R^x_E — it is either prefixed by "def E $\underline{\text{cand}}$" or by "$\neg$ def E $\underline{\text{cor}}$" the value of $x' \neq E$ is irrelevant where def E coincides with false.

Since $[\text{true}(E/x) \equiv \text{true}]$ and $[\text{false}(E/x) \equiv \text{false}]$, Theorems 0 and 1 are also valid for the assignment

statement. In order to prove Theorem 2, we observe for any Z and R

$$
\begin{array}{l}
\quad [Z \equiv wlp(x:=E, R) \wedge wp(x:=E, true)] \\
= \{\text{definition of semantics of } x:=E\} \\
\quad [Z \equiv (\neg\, def\, E \ \underline{cor}\ R(E/x)) \wedge (def\, E \ \underline{cand}\ true(E/x))] \\
= \{\text{since } [true(E/x) \equiv true] \text{ and pred. calc.}\} \\
\quad [Z \equiv (\neg\, def\, E \ \underline{cor}\ R(E/x)) \wedge def\, E) \\
= \{\text{pred. calc}\} \\
\quad [Z \equiv def\, E \ \underline{cand}\ R(E/x)] \ .
\end{array}
$$

In order to prove Theorem 4, we have to show that for any E and any bag of predicates B

$$
\begin{array}{l}
[\neg\, def\, E \ \underline{cor}\ (\underline{A}P : P \ \underline{in}\ B : P)(E/x) \equiv \\
\qquad (\underline{A}P : P \ \underline{in}\ B : \neg\, def\, E \ \underline{cor}\ P(E/x))\ ]
\end{array}
$$

Omitting the range B, we observe for any Z

$$
\begin{array}{l}
\quad [Z \equiv (\underline{A}P :: \neg\, def\, E \ \underline{cor}\ P(E/x))] \\
= \{\text{pred. calc}\} \\
\quad [Z \equiv \neg\, def\, E \ \underline{cor}\ (\underline{A}P :: P(E/x))] \\
= \{\text{definition of } P(E/x)\} \\
\quad [Z \equiv \neg\, def\, E \ \underline{cor}\ (\underline{A}P :: (\underline{A}\, x' :: x' \neq E \vee (\underline{A}x :: x \neq x' \vee P)))] \\
= \{\text{pred. calc., viz interchanging of universal quantifications}\} \\
\quad [Z \equiv \neg\, def\, E \ \underline{cor}\ (\underline{A}\, x' :: (\underline{A}P :: x' \neq E \vee (\underline{A}x :: x \neq x' \vee P)))] \\
= \{\text{pred. calc., since } x' \neq E \text{ does not depend on dummy } P\} \\
\quad [Z \equiv \neg\, def\, E \ \underline{cor}\ (\underline{A}\, x' :: x' \neq E \vee (\underline{A}P :: (\underline{A}x :: x \neq x' \vee P)))] \\
= \{\text{two similar steps combined into one}\} \\
\quad [Z \equiv \neg\, def\, E \ \underline{cor}\ (\underline{A}\, x' :: x' \neq E \vee (\underline{A}x :: x \neq x' \vee (\underline{A}P :: P)))] \\
= \{\text{definition of } (\underline{A}P :: P)(E/x)\} \\
\quad [Z \equiv \neg\, def\, E \ \underline{cor}\ (AP :: P)(E/x)]
\end{array}
$$

This ends the proof of Theorem 4. (In including def E in the definitions of both wp and wlp I followed a suggestion from J.L.A. van de Snepscheut, in proving Theorem 4 I followed a suggestion from A.J.M. van Gasteren.)

Concatenation is simple. The semantics of $S0;S1$ is defined in terms of that of $S0$ and $S1$ by

$$[wp("S0;S1",R) \equiv wp(S0, wp(S1,R))] \text{ for any } R$$

$$[wlp("S0;S1",R) \equiv wlp(S0, wlp(S1,R))] \text{ for any } R$$

The right-hand sides have the form of functional composition, say $f0 \circ f1\ R$ and $g0 \circ g1\ R$ respectively. From the validity of Theorems 0 through 4 for the f's and the g's we have to derive the validity for their functional compositions. Since – see EWD835-23 – functional composition is fixed point preserving, Theorems 0 and 1 are valid for the concatenation; since functional composition preserves the common degree of conjunctivity of the components, also Theorems 3 and 4 are valid for the concatenation. For Theorem 2 we have to do some work: for any Z and any R we observe

$$\begin{aligned}
&[Z \equiv f0 \circ f1\ R] \\
=&\ \{\text{definition of functional composition}\} \\
&[Z \equiv f0\ (f1\ R)] \\
=&\ \{\text{Theorem 2 valid for } f1, g1\} \\
&[Z \equiv f0\ (g1\ R \wedge f1\ true)] \\
=&\ \{f0 \text{ is conjunctive}\} \\
&[Z \equiv f0(g1\ R) \wedge f0(f1\ true)] \\
=&\ \{\text{Theorem 2 valid for } f0, g0\} \\
&[Z \equiv g0(g1\ R) \wedge f0\ true \wedge f0(f1\ true)] \\
=&\ \{f0 \text{ is conjunctive}\} \\
&[Z \equiv g0\ (g1\ R) \wedge f0(f1\ true)] \\
=&\ \{\text{definition of functional composition}\} \\
&[Z \equiv g0 \circ g1\ R \wedge f0 \circ f1\ true]
\end{aligned}$$

Next the alternative statement. For brevity's sake we use the [] as "guarded command set former". Let, as usual, IF denote if ([]i :: Bi → Si) fi and let BB be given by [BB ≡ (∃i :: Bi)].

The semantics of IF is given by

[wp(IF, R) ≡ BB ∧ (∀i :: ¬Bi ∨ wp(Si, R))]

[wlp(IF, R) ≡ (∀i :: ¬Bi ∨ wlp(Si, R))]

Again we have to prove Theorems 0 through 4 for IF, assuming they hold for all the Si.

To prove Theorem 0, we observe for any Z

```
  [Z ≡ wp(IF, false)]
= {definition of semantics}
  [Z ≡ BB ∧ (∀i :: ¬Bi ∨ wp(Si, false))]
= {Theorem 0 holds for all Si}
  [Z ≡ BB ∧ (∀i :: ¬Bi)]
= {definition of BB and de Morgan}
  [Z ≡ false].
```

We don't need to prove Theorem 1, since it follows from Theorem 4, the universal conjunctivity. To prove Theorem 4, we formulate two little lemmata.

Lemma For any universally conjunctive f and predicate Q, predicate g, defined by [g.X ≡ Q ∨ f.X] for any X, is universally conjunctive.

This is proved by observing for any bag C of predicates and any Z

```
  [Z ≡ g.(∀P: P in C: P)]
= {definition of g}
  [Z ≡ Q ∨ f.(∀P: P in C: P)]
= {f is universally conjunctive}
```

$$
\begin{array}{ll}
 & [Z \equiv Q \vee (\underline{A}P : P \underline{in} C : fP)] \\
= & \{\text{pred. calc}\} \\
 & [Z \equiv (\underline{A}P : P \underline{in} C : Q \vee fP)] \\
= & \{\text{definition of } g\} \\
 & [Z \equiv (\underline{A}P : P \underline{in} C : gP)] \quad .
\end{array}
$$

Lemma For a bag of universally conjunctive $f.i$, g, defined by $[gX \equiv (\underline{A}i :: f.i\ X)]$ for all X, is universally conjunctive.

This is proved by observing for any bag C of predicates and any Z

$$
\begin{array}{ll}
 & [Z \equiv g(\underline{A}P : P \underline{in} C : P)] \\
= & \{\text{definition of } g\} \\
 & [Z \equiv (\underline{A}i :: f.i\ (\underline{A}P : P \underline{in} C : P))] \\
= & \{f.i \text{ are universally conjunctive}\} \\
 & [Z \equiv (\underline{A}i :: (\underline{A}P : P \underline{in} C : f.i\ P))] \\
= & \{\text{interchange of universal quantifications}\} \\
 & [Z \equiv (\underline{A}P : P \underline{in} C : (\underline{A}i :: f.i\ P))] \\
= & \{\text{definition of } g\} \\
 & [Z \equiv (\underline{A}P : P \underline{in} C : gP)]
\end{array}
$$

From these two lemmata it follows immediately that IF is universally conjunctive.

To prove Theorem 2, we observe for any R and Z

$$
\begin{array}{ll}
 & [Z \equiv wlp(IF, R) \wedge wp(IF, true)] \\
= & \{\text{definition of semantics}\} \\
 & [Z \equiv (\underline{A}i :: \neg Bi \vee wlp(Si, R)) \wedge \\
 & \qquad BB \wedge (\underline{A}i :: \neg Bi \vee wp(Si, true))] \\
= & \{\text{pred. calc}\} \\
 & [Z \equiv BB \wedge (\underline{A}i :: \neg Bi \vee (wlp(Si, R) \wedge wp(Si, true)))] \\
= & \{\text{Theorem 2 valid for all } Si\} \\
 & [Z \equiv BB \wedge (\underline{A}i :: \neg Bi \vee wp(Si, R))
\end{array}
$$

$= \{$definition of semantics$\}$
$[Z \equiv wp(IF, R)]$.

So far our proofs have mostly been very boring. They were also effective. But the element of surprise was usually lacking.

* * *

To prepare the road for our treatment of repetition we shall first prove our version of the

Theorem of Knaster-Tarski. For monotonic f the equations $X: [fX \Rrightarrow X]$ and $X: [fX \equiv X]$ have the same strongest solution Q given by
$[Q \equiv (\underline{A}\, X: [fX \Rrightarrow X]: X)]$.

Corollary. For monotonic f, $X: [fX \Rrightarrow X]$ and $X: [fX \equiv X]$ each have a strongest solution.

Proof of Theorem of Knaster-Tarski.

$$
\begin{array}{l}
\quad true \\
= \{\text{definition of } Q\} \\
\quad [Q \equiv (\underline{A}\, X: [fX \Rrightarrow X]: X)] \\
\Rrightarrow \{\text{pred. calc}\} \\
\quad [Q \Rrightarrow (\underline{A}\, X: [fX \Rrightarrow X]: X)] \\
= \{\text{pred. calc.}\} \\
\quad [(\underline{A}\, X: [fX \Rrightarrow X]: Q \Rrightarrow X)] \\
= \{\text{pred. calc.}\} \\
\quad (\underline{A}\, X: [fX \Rrightarrow X]: [Q \Rrightarrow X]) \qquad * \\
\Rrightarrow \{f \text{ is monotonic}\} \\
\quad (\underline{A}\, X: [fX \Rrightarrow X]: [fQ \Rrightarrow fX]) \\
= \{\text{pred. calc.}\} \\
\quad [fQ \Rrightarrow (\underline{A}\, X: [fX \Rrightarrow X]: fX)] \\
\Rrightarrow \{\text{pred. calc.}\}
\end{array}
$$

$$
\begin{array}{ll}
 & [fQ \Rrightarrow (\underline{A}X: [fX \Rrightarrow X]: X)] \\
= & \{\text{definition of } Q\} \\
 & [fQ \Rrightarrow Q]
\end{array}
$$

Now it has been established that Q is a solution of $X: [fX \Rrightarrow X]$, whereas the line * states that it is as strong as any solution; hence Q is the strongest solution of $X: [fX \Rrightarrow X]$.

We continue

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

Hence $[fQ \equiv Q]$.

(End of Proof of Theorem of Knaster-Tarski.)

Though the steps in the above proof are as simple as those in our earlier proofs, this one is not boring; on the contrary, it is surprising to see what we can prove about fQ when, firstly, we remember how Q has been defined and, secondly, we realize that for f no conjunctivity of any form has been assumed. The Theorem of Knaster-Tarski clearly captures something nontrivial. It is also worth noting that, again, we see fixed points emerging.

Another theorem that only requires monotonicity of f is the

Limit Theorem. For monotonic f and P any solution of $X: [fX \equiv X]$ or of $X: [fX \Rrightarrow X]$, $[(\underline{E}i: i \geq 0: f^i \text{false}) \Rrightarrow P]$.

Here the exponent indicates iterated functional composition, more precisely

$[f^0 X \equiv X]$ for any X

$[f^{i+1} X \equiv f \circ f^i X]$ for any X

(or $[f^{i+1} X \equiv f(f^i X)]$ for any X).

Proof of the Limit Theorem. Since any solution of $X: [fX \equiv X]$ is also a solution of $X: [fX \Rightarrow X]$, it suffices to prove the theorem for a solution P of the latter equation.

We observe firstly

```
    true
=  { predicate calculus }
    [¬ false ∨ P]
=  { definition of iterated functional composition }
    [¬ f^0 false ∨ P]
```

and secondly

```
    [¬ f^i false ∨ P]
⇒  { f is monotonic }
    [¬ f(f^i false) ∨ f P]
=  { definition of iterated functional composition }
    [¬ f^(i+1) false ∨ f P]
⇒  { P is a solution of X: [fX ⇒ X] }
    [¬ f^(i+1) false ∨ P].
```

Hence

```
 true
= { mathematical induction } (A i: i≥0: [¬ f^i false ∨ P])
= { pred. calc. } [(A i: i≥0: ¬ f^i false ∨ P)]
= { pred. calc. } [(A i: i≥0: ¬ f^i false) ∨ P]
= { pred. calc. } [(E i: i≥0: f^i false) ⇒ P].
```

(End of Proof of Limit Theorem.)

For the sake of brevity we observe that we can write the statement IF with a number of alternatives **if** $(\llbracket i :: B_i \to S_i)$ **fi** also as

$$\textbf{if } BB \to IF \textbf{ fi}$$

i.e. an alternative construct with in the first instance only 1 guarded command. Similarly, the repetitive construct **do** $(\llbracket i :: B_i \to S_i)$ **od** can be written as

$$\textbf{do } BB \to IF \textbf{ od} \quad .$$

The above observation is exploited to study the repetition

$$DO: \quad \textbf{do } B \to S \textbf{ od}$$

in relation to the corresponding

$$IF: \quad \textbf{if } B \to S \textbf{ fi} \quad .$$

The generalization to the general repetition with more guarded commands is left to the reader.

We take the position that the semantics of DO is not changed by unfolding it once, i.e. is equivalent to that of

$$DO': \quad \textbf{if } B \to S\,;DO \llbracket \neg B \to \text{skip } \textbf{fi} \quad .$$

In other words, we require

$$[wp(DO,R) \equiv wp(DO',R)] \quad \text{for all } R \text{ , and}$$

$$[wlp(DO,R) \equiv wlp(DO',R)] \quad \text{for all } R \text{ ,}$$

i.e. $wp(DO,R)$ is a solution of $X : [X \equiv fX]$ with

$$[fX \equiv (\neg B \vee wp(S,X)) \wedge (B \vee R)]$$

and $wlp(DO,R)$ is a solution of $X : [X \equiv hX]$ with

$$[hX \equiv (\neg B \vee wlp(S,X)) \wedge (B \vee R)] \quad .$$

Since we have for any B, P, and Q

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

we could also have defined

$$[fX \equiv (B \wedge wp(S,X)) \vee (\neg B \wedge R)] \quad \text{for all } X$$
$$[hX \equiv (B \wedge wlp(S,X)) \vee (\neg B \wedge R)] \quad \text{for all } X.$$

We now define $wp(DO,R)$ as the strongest solution of $X:[X \equiv fX]$ and $wlp(DO,R)$ as the weakest solution of $X:[X \equiv hX]$.

Remembering that Theorem 2 states in this case

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

we see that we also need to consider the strongest solution of $X:[X \equiv gX]$ with g defined by

$$[gX \equiv (B \wedge wp(S,X)) \vee \neg B],$$

in short, we have to establish a relation between extreme solutions of three different equations.

In order to cope with that problem we devise a notation in which we strictly separate what these equations have in common from where they differ. Since we study the equations with an S satisfying Theorem 2, we may replace $wp(S,X)$ in f and g by $wlp(S,X) \wedge wp(S,true)$, or, since the last term is a constant predicate for fixed S, by $wlp(S,X) \wedge K$. Our notation introduces a predicate transformer c which operates on three arguments instead of the usual one; it is defined by

$$[cXYZ \equiv (B \wedge wlp(S,X) \wedge Y) \vee (\neg B \wedge Z)]$$
for all X, Y, and Z.

In terms of c, the equations $X:[X \equiv fX]$, $X:[X \equiv gX]$, and $X:[X \equiv hX]$ become in order

$X: [X \equiv c\ X\ K\ R]$
$X: [X \equiv c\ X\ K\ true]$
$X: [X \equiv c\ X\ true\ R]$.

There is hope because c is <u>multiply conjunctive</u>, i.e.

$$[c\ (X \wedge X')\ (Y \wedge Y')\ (Z \wedge Z') \equiv (c\ X\ Y\ Z) \wedge (c\ X'\ Y'\ Z')]$$

for any predicates X, X', Y, Y', Z, and Z' .

<u>Proof</u>. The proof depends primarily on the special structure of c and the general formula from predicate calculus

$$[(B \wedge P \wedge P') \vee (\neg B \wedge Q \wedge Q') \equiv ((B \wedge P) \vee (\neg B \wedge Q)) \wedge ((B \wedge P') \vee (\neg B \wedge Q'))]$$

—which is most readily proved by substituting for B, true and false respectively (the latter substitution being superfluous on account of symmetry considerations)— .

For any H, etc.

$[H \equiv (c\ X\ Y\ Z) \wedge (c\ X'\ Y'\ Z')]$
$= \{$definition of c$\}$
$[H \equiv ((B \wedge wlp(S, X) \wedge Y) \vee (\neg B \wedge Z)) \wedge ((B \wedge wlp(S, X') \wedge Y') \vee (\neg B \wedge Z'))]$
$= \{$predicate calculus, see above$\}$
$[H \equiv (B \wedge wlp(S, X) \wedge wlp(S, X') \wedge Y \wedge Y') \vee (\neg B \wedge Z \wedge Z')]$
$= \{$conjunctivity of wlp$\}$
$[H \equiv (B \wedge wlp(S, X \wedge X') \wedge (Y \wedge Y')) \vee (\neg B \wedge (Z \wedge Z'))]$
$= \{$definition of c$\}$
$[H \equiv c\ (X \wedge X')\ (Y \wedge Y')\ (Z \wedge Z')]$.

(End of Proof)

A pleasant consequence of c's multiple conjunctivity is the

Multiple Conjunctivity Lemma 0. With P a solution of $X:[X \equiv c\ X\ Y\ Z]$ and P' one of $X:[X \equiv c\ X\ Y'\ Z']$, $P \wedge P'$ is a solution of $X:[X \equiv c\ X\ (Y \wedge Y')\ (Z \wedge Z')]$.

Proof.

$$
\begin{array}{ll}
 & \text{true} \\
= & \{\text{definitions of } P \text{ and } P'\} \\
 & [P \equiv c\ P\ Y\ Z] \wedge [P' \equiv c\ P'\ Y'\ Z'] \\
\Rightarrow & \{\text{predicate calculus}\} \\
 & [P \wedge P' \equiv c\ P\ Y\ Z \wedge c\ P'\ Y'\ Z'] \\
= & \{c \text{ is multiply conjunctive}\} \\
 & [P \wedge P' \equiv c\ (P \wedge P')\ (Y \wedge Y')\ (Z \wedge Z')]
\end{array}
$$

(End of Proof)

Before proceeding it is correct to establish that our definitions of wp and wlp make sense, i.e. that weakest and strongest solutions of $X:[X \equiv c\ X\ Y\ Z]$ exist for any Y and Z. Because c is multiply conjunctive, it is conjunctive, and hence monotonic, in its first argument. The strongest solution exists on account of Knaster-Tarski as formulated, the weakest solution exists on account of its equivalent formulation

Theorem of Knaster-Tarski. For monotonic f^* the equations $Y:[Y \Rightarrow f^*Y]$ and $Y:[Y \equiv f^*Y]$ have the same weakest solution R given by $[R \equiv (\underline{E}Y:[Y \Rightarrow f^*Y]:Y]$.

Sketch of Proof. Relating firstly f and f^* by

$$[f\,X \equiv \neg f^*(\neg X)] \quad \text{for any } X$$

-i.e. f and f^* are each other's so-called conjugate- one establishes first

$$(f \text{ is monotonic}) \equiv (f^* \text{ is monotonic})$$

Relating furthermore $[\neg X \equiv Y]$ and $[\neg Q \equiv R]$, one can transform the one formulation into the other. (End of Sketch of Proof)

Having established the existence of the extreme solutions, we show two further lemmata about them (since we shall need them in the near future).

Multiple Conjunctivity Lemma 1

For multiply conjunctive c
P the weakest solution of $X: [X \equiv c\ X\ Y\ Z]$,
P' the weakest solution of $X: [X \equiv c\ X\ Y'\ Z']$,
H the weakest solution of $X: [X \equiv c\ X\ (Y \wedge Y')(Z \wedge Z')]$,
we have $[H \equiv P \wedge P']$

Proof. Multiple Conjunctivity Lemma 0 tells us that $P \wedge P'$ is a solution of the equation of which H is the weakest solution, hence $[P \wedge P' \Rrightarrow H]$.

In order to show $[H \Rrightarrow P \wedge P']$, we show $[H \Rrightarrow P] \wedge [H \Rrightarrow P']$. To show $[H \Rrightarrow P]$, we show that H is a solution of $X: [X \Rrightarrow c\ X\ Y\ Z]$, of which P is the weakest solution.

$$\begin{array}{ll} & \text{true} \\ = & \{ \text{definition of } H \} \\ & [H \equiv c\ H\ (Y \wedge Y')(Z \wedge Z')] \\ \Rrightarrow & \{ \text{being multiply conjunctive, } c \text{ is a monotonic function} \} \\ & [H \Rrightarrow c\ H\ Y\ Z], \end{array}$$

hence $[H \Rrightarrow P]$; $[H \Rrightarrow P']$ similarly. (End of Proof)

Remark The above Lemma 1 also holds for multiply conjunctive c with 2 or more than 3 arguments. (End of Remark.)

Multiple Conjunctivity Lemma 2 For doubly conjunctive b,
P the strongest solution of $X:[X \equiv b\,X\,R]$,
Q any solution of $X:[X \equiv b\,X\,R]$, and
H the strongest solution of $X:[X \equiv b\,X\,true]$,
we have $[P \equiv Q \wedge H]$.

Proof. We first show $[P \Rrightarrow Q \wedge H]$ by demonstrating that $Q \wedge H$ satisfies the equation of which P is the strongest solution. We have for any Z

$$
\begin{array}{ll}
 & [Z \equiv b\ (Q \wedge H)\ R] \\
= & \{\ b \text{ is multiply conjunctive}\ \} \\
 & [Z \equiv b\ Q\ R \ \wedge\ b\ H\ true] \\
= & \{\ \text{definitions of } Q \text{ and } H\ \} \\
 & [Z \equiv Q \wedge H]
\end{array}
$$

Hence $[P \Rrightarrow Q \wedge H]$. We now show $[Q \wedge H \Rrightarrow P]$, i.e. $[H \Rrightarrow \neg Q \vee P]$ by demonstrating that $\neg Q \vee P$ satisfies $X:[b\,X\,true \Rrightarrow X]$ of which — Knaster-Tarski — H is the strongest solution:

$$
\begin{array}{ll}
 & true \\
= & \{\ \text{trivially}\ \} \\
 & [b\ (P \wedge Q)\ R \ \equiv\ b\ (P \wedge Q)\ R] \\
= & \{\ \text{predicate calculus}\ \} \\
 & [b\ ((P \vee \neg Q) \wedge Q)\ R \ \equiv\ b\ (P \wedge Q)\ R] \\
\Rightarrow & \{\ b \text{ is doubly conjunctive and monotonic}\ \} \\
 & [b\ (P \vee \neg Q)\ true \ \wedge\ b\ Q\ R \Rrightarrow b\ P\ R] \\
= & \{\ \text{definitions of } P \text{ and } Q\ \} \\
 & [b\ (P \vee \neg Q)\ true \ \wedge\ Q \Rrightarrow P] \\
= & \{\ \text{predicate calculus}\ \} \\
 & [b\ (P \vee \neg Q)\ true \Rrightarrow P \vee \neg Q]
\end{array}
$$

(End of Proof.)

And now we are ready to prove that, provided Theorem 2 holds for S, it holds for DO. For any Z, etc.

$$
\begin{array}{l}
\quad [Z \equiv wp(DO, R)] \\
= \{ \text{definition of } wp \} \\
\quad [Z \equiv (\text{strongest solution of } X: [X \equiv c\, X \,K\, R])] \\
= \{ \text{Lemma 2 applied with "weakest" for "any";} \\
\quad\ c \text{ is doubly conjunctive in the pair } X\ R \} \\
\quad [Z \equiv (\text{weakest solution of } X: [X \equiv c\, X \,K\, R]) \wedge \\
\qquad (\text{strongest solution of } X: [X \equiv c\, X \,K\, \text{true}])] \\
= \{ \text{Lemma 1} \} \\
\quad [Z \equiv (\text{weakest solution of } X: [X \equiv c\, X\, \text{true}\ R]) \wedge \\
\qquad (\text{weakest solution of } X: [X \equiv c\, X \,K\, \text{true}]) \wedge \\
\qquad (\text{strongest solution of } X: [X \equiv c\, X \,K\, \text{true}])\ ] \\
= \{ \text{predicate calculus} \} \\
\quad [Z \equiv (\text{weakest solution of } X: [X \equiv c\, X\, \text{true}\ R]) \wedge \\
\qquad (\text{strongest solution of } X: [X \equiv c\, X \,K\, \text{true}])\ ] \\
= \{ \text{definitions of } wp \text{ and } wlp \} \\
\quad [Z \equiv wlp(DO, R) \wedge wp(DO, \text{true})]
\end{array}
$$

Thus Theorem 2 has been proved for DO.

Theorem 0 follows for DO from the fact that if Theorem 0 holds for S $[\text{false} \equiv c\, \text{false}\ K\ \text{false}]$, i.e. false is the strongest solution of $X: [X \equiv c\, X\, K\, \text{false}]$.

Finally we have to show the validity of Theorem 4, i.e. that $wlp(DO, ?)$ is universally conjunctive if $wlp(S, ?)$ is. We shall not prove that here. We should have observed 4 pages ago that c is multiply universally conjunctive and Lemmata 0 and 1 should have been generalized from 2 (primed and unprimed) to any bag. The generalization is straightforward.

* * *

Concluding Remarks.

These draft lecture notes are now concluded, not because all theory developed in the preceding eight months has been presented, but because the semester draws to a close and – together with, say, EWD830 and EWD844 – I think we have collected enough material for our secondary target, viz. the discovery how to use the predicate calculus effectively.

After I had lectured for a few weeks, J.T. Udding suggested a generalization of one of my notational conventions which I have not adopted since one of my purposes was to experiment with the conventions I had chosen. The result of the experiment is that Udding's suggestion is, indeed, an improvement, and that I shall adopt it.

On p. EWD835-8 I have proposed to render the computation via an intermediate predicate R that $P \equiv Q$ has the value true – coincides with true – as follows

$$\begin{array}{l} \quad P \\ = \{ \text{hint why } P \equiv R \text{ has the value true} \} \\ \quad R \\ = \{ \text{hint why } R \equiv Q \text{ has the value true} \} \\ \quad Q \quad , \end{array}$$

and I have religiously adhered to the constraint that in such proofs P, Q, and R were predicates on the trivial space. In that case $P \equiv Q$, $P \equiv R$, and $R \equiv P$ are predicates on the trivial space as well, and without change of meaning we could have written:

$$
\begin{array}{l}
\quad P \\
= \{ \text{hint why } [P \equiv R] \} \\
\quad R \\
= \{ \text{hint why } [R \equiv Q] \} \\
\quad Q
\end{array}
$$

as structure of a computation of the truth of $[P \equiv Q]$. But in the latter interpretation there is no need anymore for P, Q, and R to be elementary predicates. Removing that constraint does away with the need for the "dummy" as in

$$
\begin{array}{l}
\quad [Z \equiv P] \\
= \{ \text{hint why } [P \equiv R] \} \\
\quad [Z \equiv R] \\
= \{ \text{hint why } [R \equiv Q] \} \\
\quad [Z \equiv Q]
\end{array}
\qquad \text{for any } Z .
$$

We had lots of such proofs in which we observed such equivalences "for any Z". Udding's suggestion eliminates the need for such a dummy. In the case of a proof of $[P \Rightarrow Q]$ the improvement is even more marked.

* * *

EWD844 is a definite improvement compared to this draft's introduction of universal quantification.

Nomenclature. In $(\underline{A} X : X \underline{\text{in}} \mathcal{B} : fX)$ I need a name for "fX"; I propose "the term". I also need a name for $\mathcal{B}$; I propose to call it "the range" over which the term is quantified. (End of Nomenclature.)

* * *

In connection with EWD842 I have replaced

during a number of lectures the phrasing "has the value true" by "coincides with black". The introduction of the verb "to coincide" and of the identifier "black" were both experienced as an improvement. The verb "to coincide" can be introduced noiselessly, just by using it; abolishing "true" by replacing it by "black" will cause a greater shock. In my current estimation the latter change of terminology is the more essential one.

* * *

Re EWD842 and EWD843 the following remarks.

In EWD842 I have omitted to state that when P, Q, and R stand for predicate variables they may be systematically replaced by any predicate expression.

Furthermore, EWD843 has to be rewritten – or to be made superfluous by rewriting EWD842 –. The remark is the following. In the presence of a formula of the form

$$(P \equiv Q) \vee R$$

we may generate from F the formula $F' \vee R$ in which F' is obtained from F by replacing in F some (but not necessarily all) occurrences of P by Q. Unless I am profoundly mistaken, this does away with all the magic and philosophy associated with the turnstile. (Disjunction – and probably also equivalence – has in any case to be defined as well on a bag containing a single argument.)

* * *

Finally one observation, the full significance of which I have not fathomed yet. Nowhere in EWD835 have I used the fact that the space consists of points!

We can introduce them by postulating the existence of "elementary predicates" – denoted by p – such that

Axiom 0: $[(\underline{E}p :: p)]$

Axiom 1: $[p \Rrightarrow Q] \equiv \neg[p \Rrightarrow \neg Q]$ for any Q.

In the theory developed so far we did <u>not</u> need those two axioms. For the time being I regard this as another indication that set theory does not deserve the primacy usually given to it.

The remark that "a space without points" is a bit hard to "imagine" is beside the point since "imagining" could very well be a habit not to be universally encouraged.

The elementary predicates – be it, by mistake, their complements – have been introduced in EWD830 that deals with termination in the light of unbounded non-determinacy (as announced op p. EWD835-15). The contents of EWD830 belong to this lecture course as well.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

22 November 1982

prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow