IBM SEMINAR
VIENNA
AUGUST 1969

A THEORY OF PROGRAMS

AN OUTLINE OF JOINT WORK BY
J.W. DE BAKKER AND
DANA SCOTT

MACHINES

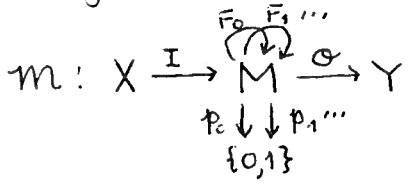
A <u>machine</u> is a structure

$$\mathcal{M} = (I, \mathcal{O}, F_0, p_0, F_1, p_1, \dots)$$

of <u>partial</u> functions for which there exist (uniquely determined) sets X, M, Y such that:

$I : X \to M$ (the <u>input</u> function),
$\mathcal{O} : M \to Y$ (the <u>output</u> function),
$F_i : M \to M$ (the <u>operations</u>),
$p_j : M \to \{0,1\}$ (the <u>tests</u>).

As a diagram we can write:



COMPUTATIONS

A <u>computation</u> (from $x \in X$ to $y \in Y$) is a finite sequence

$$\xi_0 \, F_{i_0} \, \xi_1 \, F_{i_1} \, \xi_2 \cdots \xi_{k-1} \, F_{i_{k-1}} \, \xi_k$$

where each $\xi_\ell \in M$ and $\xi_{\ell+1} = F_{i_\ell}(\xi_\ell)$ for $\ell < k$

(and where $I(x) = \xi_0$ and $\mathcal{O}(\xi_k) = y$.)

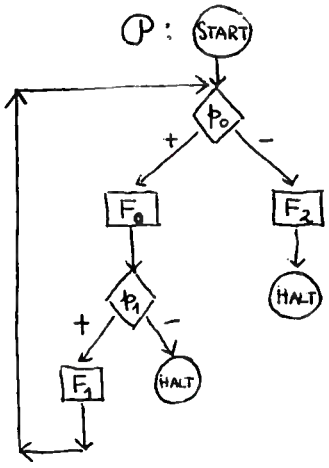
PROGRAMS

Informally a program is a "method" of selecting at most one computation starting from each $x \in X$. Thus a program $\mathcal{P}$ associates to the machine $\mathcal{M}$ a partial function

$$\mathcal{P}(\mathcal{M}) : X \to Y$$

Programs must be defined "independently" of particular machines, and indeed we can identify the program with this mapping from machines to functions. A program as a mapping must satisfy some general conditions to be mentioned later. First we give some examples.

FLOW DIAGRAMS



It is intuitively clear that, given an arbitrary machine $\mathcal{M}$, this diagram allows us to generate for each $x \in X$ at most one computation, obtained by following the "flow" of the diagram. We say that the diagram (a "syntactical" object) defines a program (a mathematical object.)

PROCEDURES

$$\mathcal{P}: \begin{cases} P_0 \Rightarrow (p_0 \to F_0 ; P_1 , F_2) \\ P_1 \Rightarrow (p_1 \to F_1 ; P_0 , E) \end{cases}$$

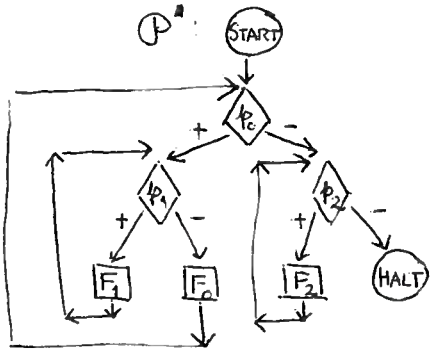
Here we have a system of procedure declarations (where by convention P_0 is the "principal" one.) $(p \to P, P')$ is the conditional expression; $P;P'$ is composition (P followed by P'); and E is the symbol for the identity function. The above system defines the same program as the flow diagram on p. 2.

WHILE STATEMENTS

$$\mathcal{P}'': (p_0 * (p_1 * F_1) ; F_0) ; (p_2 * F_2)$$

Read "$(p * P)$" as "while p do P." The same program can be defined by flow diagrams or by procedures:

$\mathcal{P}''$:



$$\mathcal{P}': \begin{cases} P_0 \Rightarrow (p_0 \to P_1 ; P_0 , E_2) \\ P_1 \Rightarrow (p_1 \to F_1 ; P_1 , E_0) \\ P_2 \Rightarrow (p_2 \to F_2 ; P_2 , E) \end{cases}$$

EQUIVALENCES

Two programs P and P' are *equivalent on* a machine M iff $P(M) = P'(M)$. They are *(strongly) equivalent* iff they are equivalent on *all* machines; that is, iff $P = P'$. Two flow diagrams (systems of procedures, *while* statements) are equivalent iff they define equivalent programs.

THEOREM. Every program defined by a *while* statement is (effectively) equivalent to one defined by a flow diagram, *but* there is a flow diagram that defines a program *not* defined by any *while* statement.

THEOREM. (The same for flow diagrams and procedures.)

THEOREM. It is (effectively) decidable whether two flow diagrams are equivalent.

THEOREM. It is (effectively) decidable whether a system of procedures defines the null program Ω.

PROBLEMS. Is it (effectively) decidable whether two procedures are equivalent? Is it decidable when a procedure is equivalent to some flow diagram? a flow diagram to a *while* statement?

General Properties

We write $M \subseteq M'$ iff M and M' have the same sets X, M, Y and have operations and tests $F_i \subseteq F_i'$ and $p_j \subseteq p_j'$ for all i, j. (That is, F_i' is consistent with, but more defined than F_i.)

(I) $M \subseteq M'$ implies $\mathcal{P}(M) \subseteq \mathcal{P}(M')$

(Property (I) can be generalized by defining the notion of morphism $\varphi : M \to M'$ between machines. See below.)

(II) If $M_n \subseteq M_{n+1}$ for $n = 0, 1, 2, \ldots$, then

$$\mathcal{P}\left(\bigcup_{n=0}^{\infty} M_n\right) = \bigcup_{n=0}^{\infty} \mathcal{P}(M_n)$$

(Property (II) can be generalized to directed unions (and, no doubt, to direct limits).) Write $M^{(n,m)}$ for the result of modifying M by replacing F_i and p_j by the totally undefined functions for $i \geq n$ and $j \geq m$.

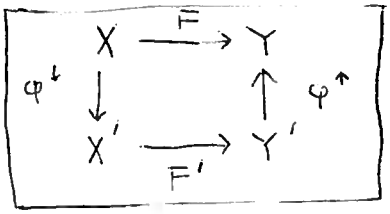
(III) For each program $\mathcal{P}$ there exist n, m such that for all machines M:

$$\mathcal{P}(M) = \mathcal{P}(M^{(n,m)}).$$

The above are clear for procedures and (suitably generalized) ought to be taken as "axiomatic" for the notion of program.

CATEGORIES

Let $\mathbb{F}$ be the category whose objects are partial functions $F : X \to Y$ and whose morphisms $\varphi : F \to F'$ are pairs $\varphi = (\varphi^{\downarrow}, \varphi^{\uparrow})$ where



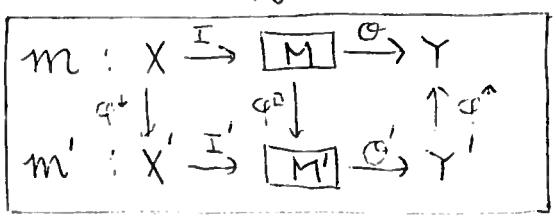
$\varphi^{\downarrow} : X \to X'$ and
$\varphi^{\uparrow} : Y' \to Y$ and
$F \subseteq \varphi^{\downarrow}; F'; \varphi^{\uparrow}$.

(Here ";" denotes composition of relations so that $(F;G)(x) = G(F(x))$ in the case of functions.)

Let $\mathbb{M}$ be the category whose objects are machines and whose morphisms $\varphi : M \to M'$ are triples $\varphi = (\varphi^{\downarrow}, \varphi^{\square}, \varphi^{\uparrow})$ where $\varphi^{\downarrow} : X \to X'$ and $\varphi^{\square} : M \to M'$ and $\varphi^{\uparrow} : Y' \to Y$ and where for all i, j :

$I \subseteq \varphi^{\downarrow}; I'; (\varphi^{\square})^{-1}$
$O \subseteq \varphi^{\square}; O'; \varphi^{\uparrow}$
$F_i \subseteq \varphi^{\square}; F_i'; (\varphi^{\square})^{-1}$
$p_j \subseteq \varphi^{\square}; p_j'$

(Here "-1" denotes converse of a relation.)



CATEGORIES (CONT)

Let P be a program and let $\varphi: M \to M'$.
Define $P(\varphi) = (\varphi^{\downarrow}, \varphi^{\uparrow})$ where $\varphi = (\varphi^{*}, \varphi^{\square}, \varphi^{\uparrow})$

"THEOREM" If $\varphi: M \to M'$ in the category $\mathbb{M}$, then

$P(\varphi): P(M) \to P(M')$ in the category $\mathbb{F}$.

This is at least clear for programs defined by procedures; it should be taken as "axiomatic" in general. Thus it follows that $P: \mathbb{M} \to \mathbb{F}$ is a functor between categories. This is the proper generalization of property (I) above. As a functor P ought to be rather "continuous" in some suitable sense.

If $M: X \xrightarrow{I} \boxed{M} \xrightarrow{O} Y$, define $[M]: M \xrightarrow{E} \boxed{M} \xrightarrow{E} M$ to be the machine with the same operations and tests but with I, O, X, Y replaced by E, E, M, M, where E is the identity on M. Then we have the result:

$$(I, E, O): M \to [M] \quad \text{in } \mathbb{M}$$

It was the "obvious correctness" of this relationship that motivated the above definitions. The categories $\mathbb{M}$ and $\mathbb{F}$ require much more study, however, before their usefulness can be determined.

CONTROL DEVICES

By a control device we shall understand a "Boolean" machine:

$$\Gamma : \{0\} \xrightarrow{S} C \xrightarrow{H} \{0,1\}$$

C: $c_0, c_1, \dots$ (arrows $\gamma_1, \gamma_2, \dots$)

$q_0 \downarrow \downarrow q_1 \cdots$

$\{0,1\}$

"ABSTRACT" PROGRAMS

Let $N = \{0,1,2,\dots\}$ and let $\{0,1\}^\infty$ be the set of all partially defined infinite sequences of 0's and 1's. If M is a machine and $\xi \in M$, define

$$p(\xi) = (p_0(\xi), p_1(\xi), \dots, p_n(\xi), \dots) \in \{0,1\}^\infty.$$

An "abstract" program $P^\Gamma_{f,g}$ is defined by giving a control device Γ (generally fixed so that a definite class of programs is considered) and two functions

$$f, g : \{0,1\}^\infty \times \{0,1\}^\infty \to N$$

such that the selected computations of $P^\Gamma_{f,g}$ on a machine M (in the notation of p. 1) are those for which there exist (uniquely determined) computations

$$\gamma_{i_0} c_{j_0} \gamma_1 c_{j_1} \gamma_2 \cdots \gamma_{k-1} c_{j_{k-1}} \gamma_k$$

on the machine Γ where for $l < k$

"ABSTRACT" PROGRAMS (CONT.)

$$i_\ell = f(p(\xi_\ell), q(\gamma_\ell)), \text{ and}$$
$$j_\ell = g(p(\xi_\ell), q(\gamma_\ell)), \text{ and}$$

$$\gamma_0 = S(0), \quad H(\gamma_\ell) = 0, \text{ for } \ell < k, \text{ and}$$
$$H(\gamma_k) = 1.$$

Thus S and H control <u>start</u> and <u>halt</u> and f and g tell where to look for the next operation to execute. We need Γ as a "memory" to keep track of where we are in the intermediate stages of "reading" the text of the program definition. Assuming that f and g are "finitely given" (i.e. depend on a fixed bounded number of coordinates of $p(\xi)$ and $q(\xi)$), we can then prove that $P^{\Gamma}_{f,g}$ is a functor with basic properties (I), (II), (III). (We need some slight <u>consistency</u> conditions on f and g.)

CONJECTURE. There are a few more "nice" properties (like (I), (II), (III)) such that any functor $P: \mathbb{M} \to \mathbb{F}$ having these properties is of the form $P^{\Gamma}_{f,g}$.

NOTE: In this abstract setting it is convenient to make the harmless convention that on all machines M we have $F_\ell = E = \text{identity on } M$

EXAMPLES

The "abstract" version of the flowdiagram uses the control device where

$$C = \{-1, 0, 1, 2, \dots\}$$
$$S(0) = 0$$
$$G_j(\gamma) = j-1$$
$$q_j(\gamma) = \begin{cases} 1 & \text{if } \gamma = j \\ 0 & \text{otherwise} \end{cases}$$
$$H(\gamma) = \begin{cases} 1 & \text{if } \gamma = -1 \\ 0 & \text{otherwise} \end{cases}$$

The "abstract" version of the procedure uses the more general control device where

$$C = \{0, 1, 2, \dots\}^* = \{\sigma_0, \sigma_1, \sigma_2, \dots\}$$
$$S(0) = 0$$
$$G_j(n\gamma) = \sigma_j \gamma$$
$$q_j(n\gamma) = \begin{cases} 1 & \text{if } n = j \\ 0 & \text{otherwise} \end{cases}$$
$$H(\gamma) = \begin{cases} 1 & \text{if } \gamma = \Lambda \\ 0 & \text{otherwise} \end{cases}$$

where Λ is the null sequence and the σ_n represent some (recursive!) enumeration of the finite sequences of integers. (In other words: the control of a procedure computation is in general a push-down store)

DEDUCTIONS

For the time being we restrict attention to procedures and ask how it can be established when two of them are equivalent. In one sense the question is answered because we have given a completely precise definition of the program defined by a procedure with the aid of a certain control device. That answer is not too helpful, because no simple "methods" of proof for proving equivalence are provided by the bare definition. Two different (though related) deductive systems are presented below which might be called the "algebraic" and the "second-order relational" theories. The algebraic method is more efficient for proving equivalences; while the relational method is better for problems of correctness. It is not known whether an algebraic theory can be complete — because if it is, and if its theorems are recursively enumerable, then we would have a recursive decision method for equivalence. The relational theory is complete — because we use second-order logic — but the theorems are not enumerable.

THE ALGEBRAIC THEORY

LANGUAGE

Lower-case letters are Boolean variables (mostly we use $p\ q\ r$) Upper-case are procedure variables, except we use E and Ω as constants. Compound terms are constructed from upper-case letters by these three operations:

$$(p \to \tau, \sigma) \qquad \tau;\sigma \qquad \mu X[\tau]$$

where in place of p we can have any Boolean and in place of X any procedure variable. The first is the conditional expression; the second, a composition; and the third has a variable-binding operator μ whose meaning is explained below. Atomic formulas are either equations $\tau = \sigma$ or inclusions $\tau \subseteq \sigma$. Lists $\Phi_0, \Phi_1, \ldots, \Phi_{n-1}$ of atomic formulas are used as a short-hand for the conjunction $[\Phi_0 \wedge \Phi_1 \wedge \cdots \wedge \Phi_{n-1}]$. Theorems are of the form of implications $\Phi \vdash \Phi'$ between lists. We use for simplicity in these notes the usual notation $\tau(X,Y)$, $\Phi(X,Z)$, $\Psi(X, \tau(X))$ to indicate (roughly!) free variables and the results of substitutions

A.T (CONT.)

VALIDITY

Consider an implication $\Phi \vdash \Psi$ Suppose the free variables are $p_0, p_1, p_2, \ldots$ and $F_0, F_1, F_2, \ldots$ The implication is valid just in case for all sets M and all systems $F_i : M \to M$ and $p_j : M \to \{0,1\}$ of partial functions and predicates on M, if Φ is true for these, then so is Ψ. Now a list is true iff all terms are. An atomic $\tau = \sigma$ is true iff τ and σ denote the same function on M into M. An atomic $\tau \subseteq \sigma$ is true iff τ denotes a function included in that denoted by σ. Thus, given the values of the free variables we need still only define what is the function denoted by a term. E denotes the identity function. Ω denotes the empty ("undefined") function. Conditionals and compositions denote functions obtained from the denotations of the parts in the usual way. The special term $\mu X[\tau(X)]$ denotes the least function G such that $\tau(G) \subseteq G$ ("least" in the sense of the partial ordering $\subseteq$) We shall see below why it always exist, and why it is of interest in connection with procedures

A.T. (CONT.)

THEOREM. The set of valid implications is not recursively enumerable (sorry!)

PROBLEM. Is the set of valid $\vdash \Psi$ recursively enumerable (and hence recursive)?

AXIOMS AND RULES

The axioms and rules for conjunctions and equations are well-known. As for $; \subseteq E \Omega$ we give the axioms of a partially ordered semigroup with unit and zero. We give the usual axioms for conditional expressions and besides:

$$\vdash (p \to X, Y); Z = (p \to X; Z, Y; Z)$$

$$\vdash (p \to X, X) \subseteq X$$

$$X \subseteq X', Y \subseteq Y' \vdash (p \to X, Y) \subseteq (p \to X', Y')$$

$$(p \to X, \Omega) \subseteq Z, (p \to \Omega, Y) \subseteq Z \vdash (p \to X, Y) \subseteq Z$$

(Maybe some others are required?? This point about conditionals is not too clear and needs more study.) For μ we have:

$$Y = \mu X [\tau(X)] \vdash \tau(Y) \subseteq Y \qquad \text{(Axiom)}$$

$$\frac{\Phi \vdash \Psi(\Omega) \qquad \Phi, \Psi(X) \vdash \Psi(\tau(X))}{\Phi \vdash \Psi(\mu X [\tau(X)])} \qquad \text{(Rule)}$$

(In the rule X is not free in Φ.)

A.T. (CONT.)

APPLICATION

Consider the following system of procedures:

$$\mathcal{P}'\ \begin{cases} P_0 \Rightarrow \tau_0(P_0, P_1) \\ P_1 \Rightarrow \tau_1(P_1, P_2) \\ P_2 \Rightarrow \tau_2(P_2, P_0) \end{cases}$$

where the τ_i are terms with the P_i and possibly other free variables. The P_i variables, of course, play a special rôle, and the above "rewrite" rules mean that the P_i should be computed as the "least" functions that result from replacing a procedure "call" by the corresponding procedure "body". Hence,

$$P_2 = \mu Z\,[\tau_2(Z, P_0)]\ ,$$

and then

$$P_1 = \mu Y\,[\tau_1(Y, \mu Z\,[\tau_2(Z, P_0)])]\ ,$$

and finally

$$P_0 = \mu X\,[\tau_0(X, \mu Y\,[\tau_1(Y, \mu Z\,[\tau_2(Z, X)])])]\ .$$

Thus the whole program can be defined by the algebraic expression on the right-hand side. Proving equations between expressions, then, is proving equivalence of programs.

A.T. (CONT.)

JUSTIFICATION

With a combination of results proved within the system and remarks outside the theory, we will see that the axioms are valid and that the rules preserve validity. Later we give some examples of particular equivalence proofs.

(1) MONOTONICITY

$$X \subseteq X' \vdash \tau(X) \subseteq \tau(X')$$

Proof: The theorem must first be generalized to any number of variables and then proved by induction on the complexity of the term τ. The cases of conditionals and compositions are already assumed as (obviously valid) axioms. For the μ-operator we do a representative special case. Thus assume $\sigma(X, Y)$ monotone in both variables, and consider $\tau(X)$ to be $\mu Y[\sigma(X, Y)]$. By the first μ-axioms:

$$\vdash \sigma(X', \tau(X')) \subseteq \tau(X'),$$

hence by assumption on σ:

$$X \subseteq X' \vdash \sigma(X, \tau(X')) \subseteq \tau(X')$$

We can again apply the monotonicity of the term σ to derive:

$$X \subseteq X', \; Y \subseteq \tau(X') \vdash \sigma(X, Y) \subseteq \tau(X').$$

A.T. (CONT.)

Note that $X \subseteq X' \vdash \Omega \subseteq \tau(X')$ is trivial; thus by the rule for the μ-operator we have:

$$X \subseteq X' \vdash \mu Y [\sigma(X, Y)] \subseteq \tau(X') \quad ,$$

which is the desired result for τ.

Discussion. We proved monotonicity by the axioms and rules for μ, but this proof also helps (in part) to establish the validity of these principles. In our calculus the expressions represent monotonic operations on partial functions. It is well-known that such operations have minimal fixed points. Speaking informally:

$$\mu X [\tau(X)] = \bigcap \{X : \tau(X) \subseteq X\}$$

$$= \bigcup_{n=0}^{\infty} \tau^n(\Omega)$$

where $\tau^n(\Omega) = \overbrace{\tau(\tau(\cdots \tau}^{n\text{-times}}(\Omega)\cdots))$. The second equation, which justifies the special case of the rule used in the proof of (1), is correct because the operations are also continuous in this sense (speaking outside the theory):

$$\tau\left(\bigcup_{n=0}^{\infty} X_n\right) = \bigcup_{n=0}^{\infty} \tau(X_n)$$

whenever $X_0 \subseteq X_1 \subseteq \cdots \subseteq X_n \subseteq \cdots$. This is clear for conditionals and compositions, but again must be established for μ-s. Once

A.T. (CONT.)

continuity is understood, the validity of the full rule for μ (which we may call the induction principle) follows easily.

(2) FIXED POINT PROPERTIES

$$Y = \mu X[\tau(X)] \vdash \tau(Y) = Y \quad \text{and}$$

$$\tau(Y) \subseteq Y \vdash \mu X[\tau(X)] \subseteq Y$$

The proof uses monotonicity and induction as in the proof of (1).

(3) SYSTEMS OF FIXED POINTS

$$X = \mu X[\tau(X, \mu Y[\sigma(X,Y)])],$$

$$Y = \mu Y[\sigma(X,Y)],$$

$$\tau(X',Y') \subseteq X',\ \sigma(X',Y') \subseteq Y' \vdash$$

$$\tau(X,Y) \subseteq X \subseteq X',\ \sigma(X,Y) \subseteq Y \subseteq Y'$$

Proof: "assume" the four hypotheses. Then $\tau(X, \mu Y[\sigma(X,Y)]) \subseteq X$ and so $\tau(X,Y) \subseteq X$. Also $\sigma(X,Y) \subseteq Y$. Let $Y'' = \mu Y[\sigma(X',Y)]$. Then $Y'' \subseteq Y'$ and so $\tau(X',Y'') \subseteq X'$. But then $X \subseteq X'$ and so $\sigma(X,Y') \subseteq Y'$. Finally $Y \subseteq Y'$.

Discussion. The above theorems on minimal fixed points can be extended to systems with any number of procedure declarations.

A.T (CONT.)

EXAMPLES

We define *while* as $(p * F) = \mu X[(p \to F; X, E)]$

(i) $(p * F); G = \mu Y[(p \to F; Y, G)]$

Proof By definition $(p*F) = (p \to F; (p*F), E)$

Hence $(p*F); G = (p \to F; (p*F); G, G)$

Therefore $\mu Y[(p \to F; Y, G)] \subseteq (p*F); G$.

To prove the opposite inclusion, first let $Y = \mu Y[(p \to F; Y, G)]$. By induction it is enough to show $\Omega; G \subseteq Y$ (obvious!) and $X; G \subseteq Y \vdash (p \to F; X, E); G \subseteq Y$. So assume $X; G \subseteq Y$. But $(p \to F; Y, G) \subseteq Y$. Thus $(p \to F; X, E); G = (p \to F; X; G, G) \subseteq Y$

(ii) $p * (p * F) = p * (F; p * F)$

Proof Let L be the left-hand side and R the right.

Then $L = (p \to (p * F); L, E)$

$= (p \to (p \to F; (p*F), E); L, E)$

$= (p \to F; (p*F); L, E)$

Thus $R \subseteq L$

Next $R = (p \to F; (p*F); R, E)$

$= (p \to (p \to F; (p*F), E); R, E)$

$= (p \to (p*F); R, E)$

Thus $L \subseteq R$ and $L = R$ follows.

A.T. (CONT)

EXAMPLES (CONT)

(iii) $(p * F); (p \to G, H) = (p * F); H$

(iv) $(p * F); (p * G) = p * F$

(v) $p * (p * F) = p * F$

All of these follow easily from (i) and the method shown for (ii).

THE RELATIONAL THEORY

Functions are, after all, <u>relations</u>. Thus it must be possible to axiomatize the functions defined by program expressions, hopefully without the minute detail of the definitions involving control devices which are closer to the ideas of implimentation. We do this for procedures.

LANGUAGE

We use simply a standard second-order predicate calculus with equality and notational conventions corresponding to our language of procedure declarations. In particular we employ the following styles of variables and non-logical constants:

R. T. (CONT.)

Individual variables $\xi, \eta, \zeta, \xi', \eta', \ldots$

1-place predicate constants:

$$p, \bar{p}, q, \bar{q}, r, \bar{r}, \ldots$$

Binary relation variables: $R, S, T, X, Y, Z, \ldots$

Binary relation constants:

$$E, \Omega, P_0, P_1, P_2, \ldots$$

Relational operations: $(R;S)$ $(p \to R,S)$

Atomic formulas: equations plus

$$R \subseteq S \qquad p(\xi) \qquad \xi R \eta$$

(where in place of R and S we can have relational terms and in place of p the other $\bar{p}, q, \bar{q}, \ldots$ and in place of ξ, η any individual variables.)

VALIDITY AND DEDUCTION

Thus as the usual notion from second-order logic; we do, however, have a few non-logical axioms to suit the application to procedures. Remember that the valid formulas are not recursively enumerable in second-order logic

R. T. (CONT.)

GENERAL AXIOMS

We assume once and for all the following definitions and axioms:

(1) $\neg \exists \xi [p(\xi) \wedge \bar{p}(\xi)]$ (sim. for $q, r, \ldots$)

(2) $\forall \xi, \eta [\xi E \eta \leftrightarrow \xi = \eta]$

(3) $\neg \exists \xi, \eta [\xi \Omega \eta]$

(4) $\forall \xi, \eta [\xi (R;S) \eta \leftrightarrow \exists \zeta [\xi R \zeta \wedge \zeta S \eta]]$

(5) $\forall \xi, \eta [\xi (p \to R, S) \eta \leftrightarrow$
$[[p(\xi) \wedge \xi R \eta] \vee [\bar{p}(\xi) \wedge \xi S \eta]]]$

(6) $R \subseteq S \leftrightarrow \forall \xi, \eta [\xi R \eta \to \xi S \eta]$

(where the R, S should be universally quantified)

The meaning of the axioms is clear except maybe for (1). Here the pair $p, \bar{p}$ is to represent a partial predicate (by convention all predicates in logic are total.) The p is the true part and the $\bar{p}$ the false part. They must be disjoint – but that is the only requirement. We do not need any similar tricks for partial functions since they are just relations in a straight-forward way.

R. T. (CONT.)

SPECIAL AXIOMS

Consider a program P defined by a system of declarations:

$$P \begin{cases} P_0 \Rightarrow \tau_0(P_0, \ldots, P_n) \\ \vdots \\ P_n \Rightarrow \tau_n(P_0, \ldots, P_n) \end{cases}$$

Corresponding to this system we have:

(i_P) $[\tau_0(P_0, \ldots, P_n) \subseteq P_0 \wedge$
$\tau_1(P_0, \ldots, P_n) \subseteq P_1 \wedge \cdots$
$\cdots \wedge \tau_n(P_0, \ldots, P_n) \subseteq P_n]$

(ii_P) $\forall R [\overset{n}{\underset{i=0}{\curlywedge}} [\tau_i(R_0, \ldots, R_n) \subseteq R_i] \rightarrow \overset{n}{\underset{i=0}{\curlywedge}} [P_i \subseteq R_i]]$

JUSTIFICATION

Given a system of procedures, we have merely assumed - in second-order language - that the P_i are the least relations where $\tau_i(P_0, \ldots, P_n) \subseteq P_i$, $i = 0, 1, \ldots, n$. This was the same idea as for the algebraic theory - except here we do not have the μ-operator. We could introduce it, and then all the algebraic principles could be proved from the second-order axioms.

R. T. (CONT.)

REMARK.

Assuming that the free variables of the procedures are $F_0, F_1, F_2, \ldots$ (our usual convention) we might want to assume that they are partial functions (our usual convention). We should have, then, as general axioms:

(1') $\forall \xi, \eta, \eta' [\xi F_i \eta \wedge \xi F_i \eta' \rightarrow \eta = \eta']$

These axioms do not seem to make too much difference, however.

APPLICATIONS

Suppose P and P' are two programs defined by procedures (where, say, in the second system we use constants $P_0', P_1', \ldots$) The equivalence problem is to deduce, therefore, the statement $P_0 = P_0'$ from all the axioms combined. The use of second-order deductions does not seem, however, any more convenient than the algebraic method for such equivalence. The point of the second-order system lies, rather, in the fact that more and different kinds of problems can be expressed within it.

R.T. (CONT.)

WHILE STATEMENTS

For the sake of illustration we restrict attention to *while* statements. These are special procedures, and we may as well introduce them by an additional operation on relations into the language: $(p * R)$. Our axioms (i_2) and (ii_2) then become:

$$(i_*) \quad (p \to F; (p * F), E) \subseteq (p * F)$$

$$(ii_*) \quad \forall R [(p \to F; R, E) \subseteq R \to (p * F) \subseteq R]$$

(where F is to be taken as a variable.)

EXAMPLE

Axiom (ii_*) seems to be a special case of our algebraic induction axiom — but it is much stronger in view of the quantifier $\forall R$. The reason is that we may specialize R to any relation, not just those that can be defined by terms using the operations we have given a notation for. As an illustration we prove

$$(p \to F; R, G) \subseteq R \to (p * F); G \subseteq R$$

(compare example (1) on p. 19.)

R.T. (cont.)

EXAMPLE (cont.)

Proof: With individual variables the conclusion requires:

$$\forall \xi, \eta, \zeta \, [\, \xi (p * F) \eta \wedge \eta G \zeta \rightarrow \xi R \zeta \,] ;$$

equivalently:

$$\forall \xi, \eta \, [\, \xi (p * F) \eta \rightarrow \forall \zeta \, [\eta G \zeta \rightarrow \xi R \zeta \,]\,] .$$

This suggests we introduce the relation S such that (and here we use second-order logic to know the S exists):

$$\forall \xi, \eta \, [\, \xi S \eta \leftrightarrow \forall \zeta \, [\eta G \zeta \rightarrow \xi R \zeta \,]\,] .$$

Now the problem is to show:

$$(p * F) \subseteq S .$$

In view of axiom (ii_*) it is sufficient to prove:

$$(p \rightarrow F ; S, E) \subseteq S .$$

This requires two cases:

(a) $p(\xi) \wedge \xi (F ; S) \eta \rightarrow \xi S \eta$

(b) $\bar{p}(\xi) \rightarrow \xi S \xi$.

For (a) assume $p(\xi)$ and $\xi F \zeta$ and $\zeta S \eta$. We want to show $\xi S \eta$. So assume in addition $\eta G \zeta'$ and show $\xi R \zeta'$. But we know by hypothesis $(p \rightarrow F ; R, G) \subseteq R$.

R.T. (cont)

EXAMPLE (cont.)

Also, since $\eta \, G \, \zeta'$ holds and $\zeta S \eta$, we have $\zeta R \zeta'$ Hence $\xi (F; R) \zeta'$. But then $\xi R \zeta'$ follows at once. Case (b) is even easier.

REMARK

From the work of Hoare we can find a simplification of axiom (ii_*); namely, it can be replaced by the combination of these two axioms:

(ii'_*) $\forall \xi, \eta \, [\xi (p * F) \eta \to \bar{p}(\eta)]$

(ii''_*) $\forall u \, [\forall \xi, \eta \, [u(\xi) \wedge p(\xi) \wedge \xi F \eta \to u(\eta)] \to$
$\forall \xi, \eta \, [u(\xi) \wedge \xi (p * F) \eta \to u(\eta)]]$

In particular (ii''_*) reads more like the arithmetic induction axiom. (Here u is a unary predicate <u>variable</u> and thus second-order form with $\forall u$ is equivalent to the earlier form with $\forall R$.) A similar simplification of the axiom (ii_p) for procedures is not yet apparent.

R.T. (cont.)

CORRECTNESS

In order to prove programs "correct", Floyd, and later Hoare, have been working with the idea of taking (a part of) a program (relation) P and thinking of desirable properties u and v such that if you enter P in u, you exit P in v. Hoare writes (more or less).

$$u\{P\}v$$

In our second-order logical notation we would write more fully:

$$\forall \xi, \eta\, [\, u(\xi) \wedge \xi P \eta \rightarrow v(\eta)\,]$$

This point of view has several advantages:

1) It is part of a well-known logical system.
2) $u\{P\}v$ becomes an ordinary proposition that can be negated, etc., etc.
3) Floyd's "logical" rules become obvious
4) Floyd's incorrect existential rule is avoided.

CONCLUSIONS

Starting from an intuitively correct idea of a machine, we explained and developed a theory of programming concepts (mainly procedures). This work could be extended by investigating more powerful control devices. But that is probably not a good idea at this level of abstraction. What is needed is a more refined model of a machine. In the work above we have treated each "state vector" $\xi \in M$ as a whole — and it is remarkable how many sensible things there are say even so. But in "real life" a vector ξ has components, and these are generally modified more or less independently during computation. This idea should be introduced into the model; then in the programs we will want to use assignment statements to modify the coordinates. This means that the operations on M, the various F_i and p_j, are being analized instead of being treated as "atoles". Along with

CONCLUSIONS (cont.)

these problems, we will also want to treat scope of "variables". One way to do this is to make the components of a state vector into push-down stores. But there are so many problems of "reference" that we might want to use Strachey's method of L- and R-values and LUP's. If we can do this, we will then want to isolate general properties of the programs (defined already with the aid of the machine model) in order to organize our deductions more clearly (the so-called "axiomatic" method.) At one level of abstraction this has all been illustrated above. To really carry out the proposal for the "real life" situation is a big, big "program". The outlines seem clear, however, and we should be able to do it in such a way that it actually refines the present theory and keeps all the "abstract" results intact.