stichting
mathematisch
centrum

AFDELING INFORMATICA IW 62/76 DECEMBER
(DEPARTMENT OF COMPUTER SCIENCE)

J.W. DE BAKKER

SEMANTICS AND THE FOUNDATIONS OF PROGRAM PROVING

Prepublication

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

AMS(MOS) subject classification scheme (1970): 68A05

ACM-Computing Reviews-categories: 5.24

Semantics and the foundations of program proving [*)]

by

J.W. de Bakker

ABSTRACT

A discussion is presented of some of the applications of mathematical (also called denotational) semantics in the justification of a proof theory for program correctness. Syntax and (denotational) semantics of a simple example language are given, together with a sketch of its assertions. The system is applied to three case studies in program proving: Assignment to a subscripted variable, weakest preconditions and the while statement, and the parameter mechanisms of PASCAL. An Appendix contains further details on the while statement.

KEY WORDS & PHRASES: *denotational semantics, program correctness, assignment, subscripted variables, weakest preconditions, parameter mechanisms, while statement.*

[*)] This report has been submitted for publication elsewhere.

1. INTRODUCTION

As a major task for theoretical computer science we see the development of a mathematical theory of programming languages, aimed at a better understanding of the fundamental notions in programming, and, hopefully, resulting in an improved quality of their applications. In our lecture we shall present a review of some of the current issues in this area, with the main emphasis on the interface between semantics and program correctness proofs.

Let us first briefly indicate in which sense we want to take these terms. As usual in language theory, we distinguish between problems of *form* and *content*, the former corresponding to the study of *syntax* - how to specify and analyse well-formed programs -, the latter leading us into the realm of *semantics*, where we study ways of attributing *meaning* to programs.

Unfortunately, there is no agreement at all on what constitutes a proper methodology for semantic specification. On the contrary, we find ourselves confronted with an embarrassingly rich choice of approaches, ranging from the simple view that a language is best defined through its compiler, via intriguing applications of various forms of model logic, to the use of sophisticated techniques rooted in category theory or universal algebra.

We find it advantageous to distinguish three main trends in the field of semantic description of programming languages. Two of these are what one might call model-theoretic, in the sense that meaning is attributed to programs by relating them to a model, i.e., some universum which is not the same as the linguistic world of the program texts. Of course, the same idea applies to natural languages: A linguistic object - e.g. the word "table" which happens to consist of five letters - is assigned meaning through its correspondence to the external world - where we might observe a table as an object with four legs. For many years, the only universum used in the specification of the meaning of programs was that of a - real or abstract - *machine*. In this point of view, each program instruction determines a *state-transforming* action of the machine, and execution of a complete program leads to a sequence of states, starting from an initial state and, normally, terminating in some final state. It has become customary to refer to this as *operational semantics*. Important examples of it are the definition of PL/I with the so-called Vienna method [19], and the definition of ALGOL 68 [32]. In recent years, a second model-theoretic approach has gained increasing acceptance, namely the method of *mathematical* (or *denotational*) *semantics* advocated by the Oxford school of Dana Scott and the late Christopher Strachey [29] (see also, e.g., [21,31]). The qualification "mathematical" is here not to be taken as implying that the methods of operational semantics would not necessarily satisfy mathematical standards. Rather, it reflects the nature of the model used, which is completely machine-independent and relies solely on certain basic mathematical notions such as sets, functions and operators. Since we shall make extensive use of these ideas in the technical development below, we won't go into details now. The third group of techniques used in the study of languages is *proof-theoretic* - as opposed to the model-theoretic nature of the first two. As an implicit way of assigning meaning to programs, one proposes certain axioms and proof rules which are used in the (formal) proofs of program properties. As outstanding representative of this approach we mention the inductive assertion method, originally proposed by Floyd [13], embedded in a formal system by Hoare [14], and reappearing in somewhat modified form in Dijkstra's work on weakest preconditions [12].

In our opinion, care should be taken not to view these three methodologies as competetive ones, but, on the contrary, as complementary in that no single one of them is appropriate for all possible applications. The remainder of our lecture will be devoted to an illustration of how mathematical semantics can help in clarifying proof theory. However, let us emphasize that operational semantics has just as well an important role in that it is closest to the actual problems of the compiler writer.

Let us now outline how the rest of the paper is organized. We first present a very simple language and define its mathematical semantics. Next, we state the sort of formal assertions one might be interested to make on this language, and sketch the structure of a possible proof theory for it. We then proceed with three applications dealing with

- assignment, in particular to subscripted variables
- weakest preconditions and the while statement
- the parameter mechanisms call-by-value and call-by-variable, as occurring in the language PASCAL.

We hope to show what challenges are offered to mathematical semantics by this sample of problems in the area of program proving. Though the examples treated are simple, we find that they are not always well-understood. It has been our experience that the foundations of program proving are in danger of being somewhat shaky, when established without the support of semantic justification.

(Related investigations of the connections between semantics and proof theory have been reported e.g. by Donahue [11], Ligler [17,18], and Pratt [26]. Cf. also Milner [22].)

2. SYNTAX AND SEMANTICS OF A SIMPLE LANGUAGE

Our example language has three kinds of constructs, viz. *statements*, *integer expressions*, and *boolean expressions*. As starting point in the formation of integer expressions we take the classes of *integer variables* $\mathit{Var} = \{x,y,\ldots\}$ and of *integer constants* $\mathit{Const} = \{m,n,\ldots\}$. Using a syntactic definition formalism which should be self-explanatory, we then introduce:

The class of statements *Stat* with elements S,...

$$S ::= x{:=}s \mid S_1;S_2 \mid \underline{\text{if}}\ b\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2\ \underline{\text{fi}} \mid \underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}}$$

The class of integer expressions *Iexp* with elements s,t,...

$$s ::= x \mid m \mid s_1+s_2 \mid \underline{\text{if}}\ b\ \underline{\text{then}}\ s_1\ \underline{\text{else}}\ s_2\ \underline{\text{fi}}$$

The class of boolean expressions *Bexp* with elements b,...

$$b ::= \underline{\text{true}} \mid \underline{\text{false}} \mid s_1 = s_2 \mid \neg b \mid b_1 \supset b_2$$

Meaning is attributed to the constructs of this language with respect to a *state*, i.e., a mapping from variables to values. E.g., the meaning of the assignment statement x:= x+1 in a state where x has the value 0 is a new state in which x now has the value 1 (and all other variables have maintained their old values).

Let $I = \{\mu, \nu, \ldots\}$ be the set of integers (note that in our programming language we use integer constants in *Const* to denote these), and let $\Sigma = Var \to I$ be the set of states, with elements $\sigma, \sigma', \ldots$. We now introduce mappings M, V and T, defining the meaning of the elements in *Stat*, *Iexp* and *Bexp*, respectively, all with respect to a given state:

$$M\colon Stat \to (\Sigma \xrightarrow[\text{part}]{} \Sigma)$$

$$V\colon Iexp \to (\Sigma \longrightarrow I)$$

$$T\colon Bexp \to (\Sigma \longrightarrow \{T,F\}) \ .$$

These definitions should be read as follows: For each statement S, $M(S)$ yields a (partial) function from states to states (thus, it is meaningful to write $M(S)(\sigma) = \sigma'$). Similarly, for each s, $V(s)$ yields a function from states to integers (we can write $V(s)(\sigma) = \mu$), and $T(b)$ yields a function from states to the set consisting of the two truth-values T and F (e.g., $T(b)(\sigma) = T$ might hold).

Before presenting the semantic definitions, we present one further piece of notation: For $\sigma \in \Sigma$, $x \in Var$ and $\mu \in I$, we define $\sigma\{\mu/x\}$ as a new state given by: $\sigma\{\mu/x\}(x) = \mu$, and for each $y \not\equiv x$: $\sigma\{\mu/x\}(y) = \sigma(y)$.

This formalism enables us to give a succinct definition of the concepts in our simple language. For each σ:

$$M(x{:=}s)(\sigma) = \sigma\{V(s)(\sigma)/x\}$$

$$M(S_1;S_2)(\sigma) = M(S_2)(M(S_1)(\sigma))$$

$$M(\underline{\text{if}}\ b\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2\ \underline{\text{fi}})(\sigma) = \begin{cases} M(S_1)(\sigma) & \text{if } T(b)(\sigma) = T \\ M(S_2)(\sigma) & \text{if } T(b)(\sigma) = F \end{cases}$$

$M(\underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}})(\sigma)$ = (this case is somewhat more complex than the other ones, and relegated to the Appendix)

$V(x)(\sigma) = \sigma(x)$

$V(m)(\sigma) = \mu$ (the integer denoted by the constant m)

$V(s_1+s_2)(\sigma) = \mathit{plus}\ (V(s_1)(\sigma), V(s_2)(\sigma))$ (where we assume known the meaning of the mathematical function $\mathit{plus}\colon I \times I \to I$)

$$V(\underline{\text{if}}\ b\ \underline{\text{then}}\ s_1\ \underline{\text{else}}\ s_2\ \underline{\text{fi}})(\sigma) = \begin{cases} V(s_1)(\sigma) \text{ if } T(b)(\sigma) = \mathrm{T} \\ V(s_2)(\sigma) \text{ if } T(b)(\sigma) = \mathrm{F} \end{cases}$$

$T(\underline{\text{true}}\ )(\sigma) = \mathrm{T}$

$T(\underline{\text{false}})(\sigma) = \mathrm{F}$

$T(s_1=s_2)(\sigma) = \mathit{equal}\ (V(s_1)(\sigma), V(s_2)(\sigma))$ (where we assume known the meaning of the mathematical function $\mathit{equal}\colon I \times I \to \{\mathrm{T},\mathrm{F}\}$)

$$T(\neg b)(\sigma) = \begin{cases} \mathrm{F}, \text{ if } T(b)(\sigma) = \mathrm{T} \\ \mathrm{T}, \text{ if } T(b)(\sigma) = \mathrm{F} \end{cases}$$

$T(b_1 \supset b_2)(\sigma) = (T(b_1)(\sigma) \Rightarrow T(b_2)(\sigma))$ (where we assume known the meaning of the logical operation "$\Rightarrow$" between truth-values).

Examples. First we determine $M(x:=x)(\sigma)$ as follows: $M(x:=x)(\sigma) = \sigma\{V(x)(\sigma)/x\} = \sigma\{\sigma(x)/x\} = \sigma$. (Below, we shall use Δ as abbreviation for the "dummy statement" x:=x.) Next, we evaluate $M(x:=2;y:=x+y)(\sigma)$, where σ satisfies $\sigma(y) = 1$. We obtain successively - neglecting for the moment the distinction between integer constants and integers:

$M(x:=2;y:=x+y)(\sigma) =$
$M(y:=x+y)(M(x:=2)(\sigma)) =$
$M(y:=x+y)(\sigma\{2/x\}) =$
$\sigma\{2/x\}\{\mathit{plus}\ (V(x)(\sigma\{2/x\}), V(y)(\sigma\{2/x\}))/y\} =$
$\sigma\{2/x\}\{\mathit{plus}(2,1)/y\} =$
$\sigma\{2/x\}\{3/y\}$.

Once having acquired some familiarity with the notation, the reader will easily convince himself that the definitions indeed capture the usual meaning of the concepts in our language. Of course, the definitions become considerably more complex for more interesting languages, but, still, the basic approach remains essentially the same as the one described here.

3. PROOF THEORY

Proofs about programs are usually concerned with three types of program properties:

- *correctness*: Program S is correct if and only if it transforms input satisfying condition p_1 to output satisfying condition p_2, for suitably chosen conditions p_1,p_2.
- *termination*: The computation specified by program S terminates for all input satisfying a suitable condition p.
- *equivalence*: Programs S_1 and S_2 determine the same state transformation.

We shall outline a formal system in which these properties can be formulated for our simple language, together with a definition of the notion of justifying the system using the semantics as given in section 2.

The *formulae* of the system are either *assertions* or *equivalences*. The class of assertions p,q,... is an extension of the class of boolean expressions $\mathcal{B}exp$ of section 2:

$$p ::= \underline{\text{true}} \mid \underline{\text{false}} \mid s_1 = s_2 \mid \neg p \mid p_1 \supset p_2 \mid S;p \mid \exists x[p]$$

An equivalence is a construct of the form $S_1=S_2$. We now extend the function $\mathcal{T}$ to assertions and equivalences. Thus, its definition for the first five syntactic clauses in the syntax for p is just as before, and omitted. Furthermore, we define, for each σ,

$$\mathcal{T}(S;p)(\sigma) = \begin{cases} \mathcal{T}, \text{ if there exists } \sigma' \text{ such that } \sigma' = \mathcal{M}(S)(\sigma) \\ \quad \text{and } \mathcal{T}(p)(\sigma') = T \\ \\ F, \text{ otherwise.} \end{cases}$$

$$\mathcal{T}(\exists x[p])(\sigma) = \begin{cases} \mathrm{T}, & \text{if there exists } \mu \text{ such that } \mathcal{T}(p)(\sigma\{\mu/x\}) = \mathrm{T} \\ \mathrm{F}, & \text{otherwise.} \end{cases}$$

$$\mathcal{T}(S_1{=}S_2)(\sigma) = \mathit{equal}(\mathcal{M}(S_1)(\sigma),\mathcal{M}(S_2)(\sigma)) \text{ (here } \mathit{equal}\colon \Sigma\times\Sigma \to \{\mathrm{T},\mathrm{F}\}).$$

(It should be noted that the p's are assertions *about* programs, and not themselves programming constructs. E.g., a boolean procedure bp with the declaration (in ALGOL 60 notation) boolean procedure bp; begin S; bp:= true end, will result in an infinite computation when called in a state σ for which S does not terminate, whereas $\mathcal{T}(S;\underline{\mathrm{true}})(\sigma)$ yields F.)

Next, we introduce the following abbreviations:

$$\begin{array}{ll}
p \vee q & \equiv (\neg p) \supset q \\
p \wedge q & \equiv \neg(p \supset \neg q) \\
p = q & \equiv (p\supset q)\wedge(q\supset p) \\
\underline{\mathrm{if}}\ p\ \underline{\mathrm{then}}\ q_1\ \underline{\mathrm{else}}\ q_2\ \underline{\mathrm{fi}} & \equiv (p\wedge q_1)\vee(\neg p\wedge q_2) \\
S \to p & \equiv (S;\underline{\mathrm{true}}) \supset (S;p) \\
\{p\}S\{q\} & \equiv p \supset (S\to q) \\
[p]S[q] & \equiv p \supset (S;q)\ .
\end{array}$$

(Below we apply the usual conventions on the priority of the logical operators ¬ , ∧ , ∨ , ⊃ , =.)

Let us now see what we obtain from these definitions in the last two cases: For each σ

$$\mathcal{T}(\{p\}S\{q\})(\sigma) = \begin{cases} \mathrm{T}, & \text{if, for all } \sigma'\text{, whenever } \mathcal{T}(p)(\sigma) = \mathrm{T} \\ & \quad \text{and } \sigma' = \mathcal{M}(S)(\sigma)\text{, then } \mathcal{T}(q)(\sigma') = \mathrm{T} \\ \mathrm{F}, & \text{otherwise.} \end{cases}$$

$$\mathcal{T}([p]S[q])(\sigma) = \begin{cases} \mathrm{T}, & \text{if, whenever } \mathcal{T}(p)(\sigma) = \mathrm{T}\text{, then there exists} \\ & \quad \sigma' \text{ such that } \sigma' = \mathcal{M}(S)(\sigma) \text{ and } \mathcal{T}(q)(\sigma') = \mathrm{T} \\ \mathrm{F}, & \text{otherwise.} \end{cases}$$

Thus, we encounter here the usual notions of *partial correctness* (in the formulation of Hoare [14]) and *total correctness* (see e.g. Manna [20]). Let us moreover point out that the meaning of our construct S;p (also appearing in Mirkowska & Salwicki [23]) is nothing but Dijkstra's weakest precondition wp(S,p) (provided that we restrict ourselves - as we do here - to deterministic programs; the nondeterministic case is investigated e.g. in De Bakker [6] and De Roever [27]).

A formula is called *valid* if, for *all* σ, $T(p)(\sigma) = T$, or $T(S_1{=}S_2)(\sigma) = T$, respectively. Examples of valid assertions are

$$S;\underline{\text{false}} = \underline{\text{false}} \tag{3.1}$$

$$S;(p\wedge q) = (S;p) \wedge (S;q) \tag{3.2}$$

$$S;(p\vee q) = (S;p) \vee (S;q) \tag{3.3}$$

Using p[s/x] to denote the result of replacing all occurrences of x in p by s, we also have the validity of

$$(x{:=}s);p = p[s/x] \tag{3.4}$$

provided that p *contains no subexpressions of the form* S;p'

$$(S_1;S_2);p = S_1;(S_2;p) \tag{3.5}$$

$$\underline{\text{if}}\ b\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2\ \underline{\text{fi}};p = \underline{\text{if}}\ b\ \underline{\text{then}}\ S_1;p\ \underline{\text{else}}\ S_2;p\ \underline{\text{fi}} \tag{3.6}$$

Valid assertions expressing partial correctness are

$$\{p[s/x]\}\ x{:=}s\ \{p\} \tag{3.7}$$

provided that p *contains no subexpressions of the form* S;p'

$$\{p\}\ x{:=}s\ \{\exists y[p[y/x] \wedge x{=}s[y/x]]\}\quad \text{(Floyd [13])} \tag{3.8}$$

$$\{p\wedge b\}S_1\{r\} \wedge \{p\wedge \neg b\}S_2\{r\} \supset \{p\}\ \underline{\text{if}}\ b\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2\ \underline{\text{fi}}\ \{r\} \tag{3.9}$$

As examples of valid equivalences we mention

$$\underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}} = \underline{\text{if}}\ b\ \underline{\text{then}}\ S;\underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}}\ \underline{\text{else}}\ \Delta\ \underline{\text{fi}} \tag{3.10}$$

$$\underline{\text{if}}\ b\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2\ \underline{\text{fi}};S = \underline{\text{if}}\ b\ \underline{\text{then}}\ S_1;S\ \underline{\text{else}}\ S_2;S\ \underline{\text{fi}} \tag{3.11}$$

A *deduction* is a construct of the form $\frac{\pi_1}{\pi_2}$, where π_1 and π_2 are formulae. In the formal proof theory, it will serve as a means for deriving new theorems from old ones (which are either axioms or previously derived theorems). Therefore, we are interested in the notion of a *sound* deduction: A deduction is called sound iff validity of its premise (π_1) implies validity of its conclusion (π_2). Examples of sound deductions are

$$\frac{p}{p[y/x]}\text{, } \textit{provided that } y \textit{ does not occur free in } p \tag{3.12}$$

$$\frac{\{p\}S_1\{q\} \wedge \{q\}S_2\{r\}}{\{p\}S_1;S_2\{r\}} \tag{3.13}$$

$$\frac{\{p\wedge b\}S\{p\}}{\{p\}\ \underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}}\ \{p\wedge\neg b\}} \tag{3.14}$$

$$\frac{p\supset q}{S;p\supset S;q} \qquad \frac{S_1=S_2}{S;S_1=S;S_2} \qquad \frac{S_1=S_2}{S_1;p=S_2;p} \tag{3.15 a,b.c}$$

An example of an invalid assertion is: $(p\supset q) \supset ((S;p)\supset(S;q))$. An unsound deduction is the following $\frac{\{\underline{\text{true}}\}x:=1;y:=2\{x=1\wedge y=2\}}{\{\underline{\text{true}}\}y:=1;y:=2\{y=1\wedge y=2\}}$.

In a proof theory one selects certain valid formulae as axioms, and sound deductions as proof rules. E.g., in Hoare's proof theory we encounter assertion (3.7) as an axiom, and assertion (3.9) and deductions (3.13) and (3.14) as proof rules, whereas in Dijkstra's system we find (3.1 - 3.6) and (3.15a). One then hopes to be able to derive a class of interesting program properties on the base of these axioms and rules. The development of a formal proof theory is in particular motivated by two considerations:

- a judicious selection of axioms and rules may lead to a system which is *complete* for a certain class of properties - thus enabling the programmer in that case to base all his proofs on the selected axioms and rules, without any appeal to facts outside the formal theory. (E.g., Hoare's system is incomplete, since the equivalence (3.10) is not derivable in it (see [4]). Addition of (3.10) yields a theory which fully characterizes the while statement in the sense as investigated in a much more general setting in De Bakker & Meertens [9].) Moreover, an appropriate choice of the axioms and rules may sometimes lead to a natural (implicit) definition of the meaning of the concepts concerned.

- Any system for computer verification of program correctness has to rely on some formalized proof theory which informs the computer as to what are the legal inferences of the system.

4. APPLICATIONS AND EXTENSIONS

In this section we present three case studies which illustrate the interface between semantics and proof theory. They are concerned with
- assignment to a subscripted variable
- weakest preconditions and the while statement
- parameter mechanisms for procedures.

In each case we hope to shed some light on a point which, simple as it may be, seems to be not yet fully understood in the literature.

4.1. *Assignment to a subscripted variable*

Consider the assignment statement $x:=1$. Clearly, $\{\underline{\text{true}}\}x:=1\{x=1\}$ is a desirable property of it, which is easily seen to be both valid, and derivable by Hoare's assignment axiom. Indeed, $(x=1)[1/x]$ reduces to $1=1$, which is equivalent with $\underline{\text{true}}$. Now let us assume that our language has been extended with subscripted variables. We first of all have to give the semantics of this extension. This is rather straightforward, and omitted here (see [8]). What to do, however, with the proof theory? First we try to treat a subscripted variable $a[s]$ in the same manner as a simple variable, allowing us to derive, e.g., $\{\underline{\text{true}}\}a[2]=1\{a[2]=1\}$ (since $\underline{\text{true}}$ is equivalent with $(a[2]=1)[1/a[2]]$). Similarly we would then obtain

$$\{\underline{\text{true}}\}a[a[2]]:=1\{a[a[2]]=1\}, \qquad (4.1)$$

(assuming that $\underline{\text{true}}$ is also equivalent with $(a[a[2]]=1)\ [1/a[a[2]]]$) but this formula can be shown to be *invalid* in the following way: It is not difficult to verify the validity of

$$\{a[1]=2 \wedge a[2]=2\}\ a[a[2]]:=1\ \{a[a[2]]=2\}. \qquad (4.2)$$

Since, obviously, $a[1]=2 \wedge a[2]=2 \supset \underline{\text{true}}$ is valid, from (4.1) we obtain

$$\{a[1]=2 \wedge a[2]=2\}\ a[a[2]]:=1\ \{a[a[2]]=1\}$$

contradicting (4.2).

The solution to the invalidity of Hoare's axiom, when carried over directly to the subscripted variable case, is provided by refining the definition of substitution $p[t/v]$, where v now ranges over both simple variables x and subscripted variables $a[s]$. By obvious reductions such as $(p_1 \supset p_2)[t/v] \equiv p_1[t/v] \supset p_2[t/v]$, or $(s_1 = s_2)[t/v] \equiv (s_1[t/v] = (s_2[t/v])$, we arrive at the treatment of $w[t/v]$, for v,w arbitrary variables. The cases where w and/or v are simple variables are rather straightforward and omitted here (see [8]). The heart of the definition consists of

$$\begin{array}{ll} b[s'][t/a[s]] \overset{\text{df.}}{\equiv} b[s'[t/a[s]]] & (a \not\equiv b) \\ a[s'][t/a[s]] \overset{\text{df.}}{\equiv} \underline{\text{if}}\ s'[t/a[s]] = s\ \underline{\text{then}}\ t\ \underline{\text{else}}\ a[s'[t/a[s]]]\ \underline{\text{fi}}. & \end{array}$$

It can be shown that (3.7), taken with the new substitution definition, is valid ([8]).

Example. $(a[a[2]] = 1)[1/a[a[2]]] \equiv$
$(\underline{\text{if}}\ a[2][1/a[a[2]]] = a[2]\ \underline{\text{then}}\ 1\ \underline{\text{else}}\ a[a[2][1/a[a[2]]]]\ \underline{\text{fi}} = 1)$.
By a few (omitted) simplifications, we reduce this to:
$\underline{\text{if}}\ a[2] = 2\ \underline{\text{then}}\ a[1] = 1\ \underline{\text{else}}\ \underline{\text{true}}\ \underline{\text{fi}}$. Thus, we obtain as instance of (3.7):

$$\{\underline{\text{if}}\ a[2] = 2\ \underline{\text{then}}\ a[1] = 1\ \underline{\text{else}}\ \underline{\text{true}}\ \underline{\text{fi}}\}$$
$$a[a[2]] := 1\{a[a[2]] = 1\},$$

thus correcting (4.1).

4.2. *Weakest preconditions and the while statement*

Let us consider Theorem 4 of [12]. When stripped to its essentials (the presence of nondeterminacy is irrelevant here), the theorem can be phrased in our notation in the following way:

$$\frac{p \wedge b \supset S;p}{p \wedge (\underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}};\underline{\text{true}}) \supset (\underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}};(p \wedge \neg b))} \qquad (4.3)$$

It will be shown that this is nothing but a weaker version of (3.14) (this remark was first made in [5]).

Assume (3.14) and the premise $p \wedge b \supset S;p$. We show that the conclusion of (4.3) is then derivable: Since $p \wedge b \supset S;p$, clearly, also $p \wedge b \wedge (S;\underline{\text{true}}) \supset S;p$, or, by simple propositional logic, $p \wedge b \supset (S;\underline{\text{true}} \supset S;p)$, i.e., $p \wedge b \supset (S \rightarrow p)$, or, in the partial correctness notation $\{p \wedge b\}S\{p\}$. Thus, the premise of (3.14) holds, and we infer the conclusion of (3.14): $\{p\}$ <u>while</u> b <u>do</u> S <u>od</u> $\{p \wedge \neg b\}$, which, in the same way, can be shown to be nothing butan abbreviation for the conclusion of (4.3). □

We here observe the advantages of an approach in which it is possible to formally compare notions such as partial correctness and weakest preconditions, thus clarifying the relationship between the various techniques.

4.3. *Parameter mechanisms*

By way of example we consider the parameter mechanisms of call-by-value and call-by-variable as occurring in the programming language PASCAL (this subsection is based on [1,2]). We extend the syntax as given in section 2 by introducing a class of procedure variables P, together with the constructs of procedure declaration and call. For the sake of simplifying the presentation here, we assume some restrictions: We have one procedure declaration $P \Leftarrow$ <<u>val</u> x, <u>var</u> y | S>, where to the right of "$\Leftarrow$" we find a construct which has a formal value parameter x, a formal variable parameter y, and body S. A procedure call has the form P(t,v), with as actual parameters the integer expression t (for the formal x) and variable v (for the formal y).

We now outline how to provide a meaning to P(t,v) in the non-recursive case (no occurrences of P in S). For this purpose we first of all need the construct of a *block*: <u>begin</u> <u>new</u> z;S <u>end</u>, where z is any simple variable and S any statement. We assume that the reader has an intuitive understanding of this concept, and omit formal specification of its semantics (and corresponding proof rule). For this we refer to e.g. [1,2,15]. We also omit the precise definition of substitution in a statement, written as S[v/x], apart from mentioning that the new z... construct has the same variable binding effect as $\forall z \ldots$ or $\int \ldots dz$ has elsewhere in mathematics. Assuming these definitions available, we introduce the following notation:

$$\langle \underline{\text{val}}\ x, \underline{\text{var}}\ y \mid S\rangle\ (t,z) \overset{\text{df.}}{\equiv}$$

$$\underline{\text{begin}}\ \underline{\text{new}}\ u;\ u:=t; S[u/x][z/y]\ \underline{\text{end}}$$

$$\langle \underline{\text{val}}\ x, \underline{\text{var}}\ y \mid S\rangle\ (t,a[s]) \overset{\text{df.}}{\equiv}$$

$$\underline{\text{begin}}\ \underline{\text{new}}\ u_1,u_2;\ u_1:=t; u_2:=s; S[u_1/x][a[u_2]/y]\ \underline{\text{end}}\ .$$

Writing B as shorthand for $\langle \underline{\text{val}}\ x, \underline{\text{var}}\ y \mid S\rangle$, we can now give concise rules for meaning and proofs for a procedure call P(t,v). Assume the declaration $P \Leftarrow B$. Then, for all σ,

$$\mathcal{M}(P(t,v))(\sigma) = \mathcal{M}(B(t,v))(\sigma),$$

and in the proof theory we might incorporate, e.g.,

$$P(t,v) = B(t,v)$$

$$P(t,v);p = B(t,v);p,$$

or

$$\frac{\{p\}\quad B(t,v)\quad \{q\}}{\{p\}\quad P(t,v)\quad \{q\}}$$

depending on whether this proof theory favors equivalences, weakest preconditions, or a partial correctness approach.

Various approaches in the literature (e.g. [15,16]) tend to confuse procedure calls with substitution. Let us give an example of this: Consider the declaration $P_1 \Leftarrow \langle \underline{\text{var}}\ y1,y2 \mid y1:=2;y2:=3\rangle$ (with a slight deviation from our previous syntactic convention). The treatment of procedure calls as proposed in [16] would, through inappropriate use of substitution, result in deductions such as

$$\frac{\{\underline{\text{true}}\}\quad y1:=2;\quad y2:=3\quad \{y1=2 \wedge y2=3\}}{\{\underline{\text{true}}\}\qquad P_1(z,z)\qquad \{z=2 \wedge z=3\}}\ ,$$

and, rightly considering this undesirable, its authors remedy this by forbidding calls such as $P_1(z,z)$. We find our definition advantageous, since there is no contradiction in the inference

$$\frac{\{\underline{\text{true}}\}\quad \langle\underline{\text{var}}\ y1, y2 \mid y1 := 2;\ y2 := 3\rangle\ (z,z)\ \{z=3\}}{\{\underline{\text{true}}\}\qquad\qquad P_1(z,z)\qquad\qquad \{z=3\}}$$

because, by the $B(t,v)$ definition, this reduces to the sound deduction

$$\frac{\{\underline{\text{true}}\}\ z:=2;\ z:=3\ \{z=3\}}{\{\underline{\text{true}}\}\quad P_1(z,z)\quad \{z=3\}}\ .$$

Remark. Observe that from (3.12) we obtain that

$$\frac{\{p\}S\{q\}}{\{p[y/x]\}S[y/x]\{q[y/x]\}}, \quad \textit{provided that } y \textit{ does not occur free in } p, S \textit{ or } q \qquad (4.4)$$

is a sound proof rule. However, this rule does *not* allow the deduction

$$\frac{\{\underline{\text{true}}\}\ y1:=2;\ y2:=3\ \{y1=2 \wedge y2=3\}}{\{\underline{\text{true}}\}\quad z:=2;\quad z:=3\ \{\ z=2 \wedge\ \ z=3\}},$$

since the proviso of (4.4) is violated after substitution of z for either y1 or y2.

5. CONCLUSIONS

We have illustrated the connections between semantics and the foundations of program proving by an analysis of a few basic programming concepts and a fragment of the associated proof theory. We are convinced that the development of firm foundations for program proving has to rely heavily on a thorough study of the semantics of the concepts concerned, together with a careful application of it in the justification and the proof theory. There is currently a vigorous activity in this area, and our lecture has touched only on a modest selection of the work in progress. For example, we have omitted all treatment of the investigations dealing with concepts such as recursion, nondeterministic and parallel programming, or (abstract) data types. *Recursion* is well-understood both as to its semantics, where the so-called least fixed point characterization is used (described e.g. in[4]), and as to its proof theory, which centers around an induction rule due to Scott ([28]). (It may be of some interest to mention here that the discovery of this rule formed part of the motivation for Scott's recent Turing award.) Certain doubts shed on the validity of the least fixed point approach in the presence of, e.g., the call-by-value parameter mechanism, were clarified in our [7]. For *parallel* programming, we have good hopes for the development of appropriate semantics on the basis of the mathematical constructions of Plotkin [25] and Smyth [30]. We consider it an interesting challenge for future work to justify the proof theory as proposed e.g. in Owicki & Gries [24] on the basis of these semantics. As to the study of abstract data types, we feel that it is as yet too early to single out any definitive developments in this field.

By way of conclusion, let us recall the aims of a mathematical theory of programming languages as stated in the introduction, viz. an improved insight into the fundamental programming concepts, and application of this in the methodology of program design and verification. When we compare the present situation with that of say ten years ago (cf. [3]), we may well be proud of the achievements in semantics during this period. Though still in a state of intense development, there are now some major results and techniques in semantics which are here to stay, allowing the programmer a better understanding of his most precious tool.

APPENDIX

In this appendix we give the semantics of the while statement, and present a new type of assertion which provides an alternative to the <u>while</u> b <u>do</u> S <u>od</u>;p construct.

Let us assume the usual partial ordering on the elements ϕ,ϕ' in $\Sigma \xrightarrow[\text{part}]{} \Sigma$ ($\phi \subseteq \phi'$ iff, for all σ, either $\phi(\sigma)$ is undefined, or $\phi(\sigma)$ and $\phi(\sigma')$ are both defined and yield the same value). Let, for a chain $\phi_0 \subseteq \phi_1 \subseteq \ldots \subseteq \phi_i \subseteq \ldots$, $\bigcup_{i=0}^{\infty} \phi_i$ denote its least upper bound. We put

$$M(\underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}}) = \bigcup_{i=0}^{\infty} \phi_i$$

where, for each σ,

$$\begin{aligned} \phi_0(\sigma) &= \text{undefined} \\ \phi_{i+1}(\sigma) &= \begin{cases} \phi_i(M(S)(\sigma)), & \text{if } T(b)(\sigma) = \mathrm{T} \\ \sigma & \text{, if } T(b)(\sigma) = \mathrm{F}. \end{cases} \end{aligned}$$

Furthermore, let us extend the definition of the class of assertions with the clause

$$p ::= \ \ldots \mid \underline{\text{rep}}\ b;S\ \underline{\text{per}}\ q$$

for which we define the function T in the following manner: For each $\gamma,\gamma' \in \Sigma \to \{\mathrm{T},\mathrm{F}\}$, we put $\gamma \subseteq \gamma'$ iff, for each σ, $\gamma(\sigma) \Rightarrow \gamma'(\sigma)$. Again, $\bigcup_{i=0}^{\infty} \gamma_i$ denotes the lub of the chain $\gamma_0 \subseteq \gamma_1 \subseteq \ldots \subseteq \gamma_i \subseteq \ldots$. We now put

$$T(\underline{\text{rep}}\ b;S\ \underline{\text{per}}\ p) = \bigcup_{i=0}^{\infty} \gamma_i$$

where, for each σ,

$$\begin{aligned} \gamma_0(\sigma) &= \mathrm{F} \\ \gamma_{i+1}(\sigma) &= \begin{cases} \gamma_i(M(S)(\sigma)), & \text{if } T(b)(\sigma) = \mathrm{T} \\ T(p)(\sigma) & \text{, if } T(b)(\sigma) = \mathrm{F}. \end{cases} \end{aligned}$$

On the basis of these definitions we can then show the validity of assertions such as

$$\underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}};p = \underline{\text{rep}}\ b;S\ \underline{\text{per}}\ p \tag{A.1}$$

$$\underline{\text{rep}}\ b;S\ \underline{\text{per}}\ p = \underline{\text{if}}\ b\ \underline{\text{then}}\ S;\underline{\text{rep}}\ b;S\ \underline{\text{per}}\ p\ \underline{\text{else}}\ p\ \underline{\text{fi}} \tag{A.2}$$

and the soundness of a deduction such as

$$\frac{q = \underline{\text{if}}\ b\ \underline{\text{then}}\ S;q\ \underline{\text{else}}\ p\ \underline{\text{fi}}}{\underline{\text{rep}}\ b;S\ \underline{\text{per}}\ p \supset q}\ . \tag{A.3}$$

(Observe that (A.1 - A.3) together yield a least-fixed-point characterization of $\underline{\text{while}}\ b\ \underline{\text{do}}\ S\ \underline{\text{od}};p$. Cf. De Bakker & De Roever [10], p.187.)

REFERENCES

[1] Apt, K.R. & J.W. de Bakker, *Exercises in denotational semantics,* in Proc. 5th Symp. Mathematical Foundations of Computer Science (A. Mazurkiewicz, ed.), pp.1-11, Lecture Notes in Computer Science 45, Springer (1976).

[2] Apt, K.R. & J.W. de Bakker, *On the semantics of PASCAL procedures,* to appear.

[3] De Bakker, J.W., *Semantics of programming languages,* in Advances in Information Systems Science (J.T. Tou, ed.), Vol. 2, pp. 173-227, Plenum Press (1969).

[4] De Bakker, J.W., *The fixed point approach in semantics: theory and applications,* in Foundations of Computer Science (J.W. de Bakker, ed.), pp.3-53, Mathematical Centre Tracts 63 (1975).

[5] De Bakker, J.W., *Flow of control in the proof theory of structured programming,* in Proc. 16th IEEE Symp. Foundations of Computer Science, Berkeley, pp.29-33 (1975).

[6] De Bakker, J.W., *Semantics and termination of nondeterministic recursive programs,* in Proc. 3d Coll. Automata, Languages and Programming (S. Michaelson & R. Milner, eds.), pp. 435-477, Edinburgh University Press (1976).

[7] De Bakker, J.W., *Least fixed points revisited,* Theoretical Computer Science, 2 , pp. 155-181 (1976).

[8] De Bakker, J.W., *Correctness proofs for assignment statements,* Report IW 55/76, Mathematical Centre (1976).

[9] De Bakker, J.W. & L.G.L.T. Meertens, *On the completeness of the inductive assertion method,* Journal of Computer and System Sciences, 11, pp.323-357 (1975).

[10] De Bakker, J.W. & W.P. de Roever, *A calculus for recursive program schemes,* in Proc. 1st Coll. Automata, Languages and Programming (M. Nivat, ed.), pp.167-196, North-Holland (1973).

[11] Donahue, J.E., *Complementary Definitions of Programming Language Semantics*, Lecture Notes in Computer Science 42, Springer (1976).

[12] Dijkstra, E.W., *Guarded commands, nondeterminacy and formal derivation of programs,* Comm. ACM, 18, pp.453-457 (1975).

[13] Floyd, R.W., *Assigning meanings to programs*, in Proc. Symp. in Applied Mathematics Vol. 19 - Math. Aspects of Computer Science (J.T. Schwartz, ed.), pp.19-32, AMS (1967).

[14] Hoare, C.A.R., *An axiomatic basis for computer programming*, Comm. ACM, 12, pp.576-580 (1969).

[15] Hoare, C.A.R., *Procedures and parameters, an axiomatic approach,* in Symp. on Semantics Algorithmic Languages (E. Engeler, ed.), pp. 102-116, Lecture Notes in Mathematics 188, Springer (1971).

[16] Igarashi, S., R.L. London & D.C. Luckham, *Automatic program verification I: A logical basis and its implementation*, Acta Informatica 4, pp.145-182 (1975).

[17] Ligler, G., *A mathematical approach to language design,* Conf. Record Second ACM Symp. on Principles of Programming Languages, Palo Alto, pp.41-53 (1975).

[18] Ligler, G., *Surface properties of programming language constructs*, Int. Symp. on Proving and Improving Programs, Arc-et-Senans, pp.299-323, IRIA (1975).

[19] Lucas, P. & K. Walk, *On the formal description of PL/I*, Annual Review in Automatic Programming, <u>6</u>, pp.105-182 (1969).

[20] Manna, Z., *Mathematical Theory of Computation*, McGraw-Hill (1974).

[21] Milne, R. & C. Strachey, *A View of Programming Language Semantics*, Chapman & Hall (1976).

[22] Milner, R., *Program semantics and mechanized proof*, <u>in</u> Foundations of Computer Science (J.W. de Bakker, ed.), Vol. II, Mathematical Centre Tracts <u>82</u> (1976).

[23] Mirkowska, G. & A. Salwicki, *A complete axiomatic characterization of algorithmic properties of block-structured programs with procedures*, <u>in</u> Proc. 5th Symp. Mathematical Foundations of Computer Science (A. Mazurkiewicz, ed.), pp.602-606, Lecture Notes in Computer Science <u>45</u>, Springer (1976).

[24] Owicki, S. & D. Gries, *Verifying properties of parallel programs: an axiomatic approach*, Comm. ACM, <u>19</u>, pp. 279-285 (1976).

[25] Plotkin, G., *A powerdomain construction*, SIAM J. on Computing, to appear.

[26] Pratt, V.R., *Semantical considerations on Floyd-Hoare logic*, Proc. 17th IEEE Symp. on Foundations of Computer Science, Houston (1976).

[27] De Roever, W.P., *Dijkstra's predicate transformer, nondeterminism, recursion and termination*, <u>in</u> Proc. 5th Symp. Mathematical Foundations of Computer Science (A. Mazurkiewicz, ed.), pp.472-481, Lecture Notes in Computer Science <u>45</u>, Springer (1976).

[28] Scott, D. & J.W. de Bakker, *A theory of programs*, unpublished memo (1969).

[29] Scott, D. & C. Strachey, *Towards a mathematical semantics for computer languages*, <u>in</u> Proc. Symp. Computers and Automata (J. Fox, ed.), pp.19-46, Polytechnic Institute of Brooklyn (1971).

[30] Smyth, M.B., *Powerdomains*, in Proc. 5th Symp. Mathematical Foundations of Computer Science (A. Mazurkieweicz, ed.), pp.537-543, Lecture Notes in Computer Science 45, Springer (1976).

[31] Tennent, R.D., *The denotational semantics of programming languages*, Comm. ACM, 19, pp.437-453 (1976).

[32] Van Wijngaarden, A. et al. (eds.), *Revised Report on the Algorithmic Language ALGOL 68*, Mathematical Centre Tracts 50 (1976).