SEMANTICS AND THE FOUNDATIONS OF PROGRAM PROVING

J. W. DE BAKKER
Mathematical Centre & Free University
Amsterdam, The Netherlands
(INVITED PAPER)

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 the associated proof theory which is rather economic in the structure 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.

1. INTRODUCTION

We see as a major task for theoretical computer science 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 improvement of the quality of their applications. In our paper we will 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 modal 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 universe 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 — for example, 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 universe 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 60. [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 will make extensive use of these ideas in the technical development below, we will not go into details now. The third group of techniques used in the study of languages in 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 an 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 Bisselstra's work on weakest preconditions. [12]

In our opinion, care should be taken not to view these three methodologies as competitive ones, but, on the contrary, as complementary in that no single one of them is appropriate for all possible applications. The remainder of our paper 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 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 for example by Donahue, [11] Liger, [17, 18] and Pratt. [26] (Cf. also Nilmar [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 the starting point in the formation of integer expressions we take the classes of integer variables \( \text{Var} = \{x, y, \ldots\} \) and of integer constants \( \text{Const} = \{0, 1, \ldots\} \). Using a syntactic definition formalism which should be self-explanatory, we then introduce:

The class of states \( \text{Stat} \) with elements \( S, \ldots \):

\[ S := x_1 \ldots s_1 \ldots \text{if } b \text{ then } S_1 \text{ else } S_2 \text{ fi while } b \text{ do } S \text{ od} \]

The class of integer expressions \( \text{IExp} \) with elements \( s, t, \ldots \):

\[ s := x_1 \ldots s_1 \ldots \text{if } b \text{ then } s_1 \text{ else } s_2 \text{ fi \ldots} \]

The class of boolean expressions \( \text{BExp} \) with elements \( b, \ldots \):

\[ b := \text{true} | \text{false} | s_1 \ldots s_2 \text{ if } b \text{ then } s_1 \text{ else } s_2 \text{ fi \ldots} \]

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 \( x := x \) 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 \( I = \{u, v, \ldots\} \) be the set of integers (note that in our programming language we use integer constants in \( \text{Const} \) to denote these), and let \( \Sigma = \text{Var} \cup I \) be the set of states, with elements \( \sigma, \tau, \ldots \). We now introduce mappings \( H, V \) and \( T \), defining the meaning of the elements in \( \text{Stat} \), \( \text{IExp} \) and \( \text{BExp} \), respectively, all with respect to a given state:

\[ H : \text{Stat} \rightarrow (I \rightarrow \Sigma) \]
\[ V : \text{IExp} \rightarrow (I \rightarrow \Sigma) \]
\[ T : \text{BExp} \rightarrow (I \rightarrow \{T, F\}) \]

These definitions should be read as follows: For each statement \( S, H(S) \) yields a (partial) function from states to states (thus, it is meaningful to write \( H(S)(\sigma) = \tau \)). Similarly, for each \( x, V(S) \) 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., \( T(b)(\sigma) \) might hold).

Before presenting the semantic definitions, we present one further piece of notation: For \( \sigma \in \Sigma \), \( x \in \text{Var} \), and \( u, v \in I \), we define \( \sigma(x/u) \) as a new state given by: \( \sigma(x/u)(x) = u \), and for each \( y \notin x \)\): \( \sigma(x/y)(y) = \sigma(y) \).

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

\[ \sigma(x := x) = \sigma(V(x)(\sigma)/x) \]
\[ H(S_1; S_2)(\sigma) = H(S_2)(H(S_1)(\sigma)) \]

\[ H(\text{if } b \text{ then } S_1 \text{ else } S_2 \text{ fi})(\sigma) = \begin{cases} H(S_1)(\sigma) & \text{if } T(b)(\sigma) = T \\ H(S_2)(\sigma) & \text{if } T(b)(\sigma) = F \end{cases} \]

\[ V(x)(\sigma) = \sigma(x) \]
\[ V(\text{true})(\sigma) = \mu \text{ (the integer denoted by the constant m) X} \]
\[ V(S_1; S_2)(\sigma) = \text{plus}(V(S_1)(\sigma), V(S_2)(\sigma)) \] (where we assume known the meaning of the mathematical function \( \text{plus} : I \times I \rightarrow I \))

\[ V(\text{if } b \text{ then } S_1 \text{ else } S_2 \text{ fi})(\sigma) = \begin{cases} V(S_1)(\sigma) & \text{if } T(b)(\sigma) = T \\ V(S_2)(\sigma) & \text{if } T(b)(\sigma) = F \end{cases} \]

\[ T(\text{true})(\sigma) = T \]
\[ T(\text{false})(\sigma) = F \]
\[ V(S_1; S_2)(\sigma) = \text{equal } (V(S_1)(\sigma), V(S_2)(\sigma)) \] (where we assume known the meaning of the mathematical function \( \text{equal} : I \times I \rightarrow \{T, F\} \))

\[ T(b)(\sigma) = \begin{cases} F & \text{if } T(b)(\sigma) = T \\ T & \text{if } T(b)(\sigma) = F \end{cases} \]

\[ T(b; b_2)(\sigma) = T(b_1)(\sigma) = T(b_2)(\sigma) \] (where we assume known the meaning of the logical operation "\( \& \)" between truth-values).

Examples. First we determine \( H(x := x)(\sigma) = \sigma(V(x)(\sigma)/x) = \sigma(x)/x = \sigma \). (Below, we shall use \( \Delta \) as the abbreviation for the "dummy statement" \( x := x \). Next, we evaluate \( H(x := y; x := y)(\sigma) \), where \( \sigma \) satisfies \( \sigma(y) = 0 \). We obtain successively - neglecting for the moment the distinction between integer constants and integers:

\[ H(x := y; x := y)(\sigma) = H(y := y)(H(x := y)(\sigma)) \]

\[ H(y := y)(H(x := y)(\sigma)) = \sigma(x)/x \]

\[ H(x := y; x := y)(\sigma) = \sigma(x)/x \]

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
equivocalness. The class of assertions \( p,q \ldots \) is an extension of the class of boolean expressions \( \text{Bexp} \) of section 2:

\[
p := \text{true} \mid \text{false} \mid s_1 \mid s_2 \mid p \mid p \circ p \mid S_i \mid \text{Bexp}(p)
\]

An equivalence is a construct of the form \( S_1 \equiv S_2 \).

We now extend the function \( T \) to assertions and equivalences. Thus, its definition for the first five syntactic clauses in the syntax for \( p \) is just as before, and therefore is not repeated. Furthermore, we define, for each \( a \),

\[
T(S;p)(a) =
\begin{cases}
T, & \text{if there exists } o' \text{ such that } o' = H(S)(o) \\
& \text{and } T(p)(o') = T
\end{cases}
\]

\[= F, \text{otherwise.} \]

\[
T(\text{Bexp}(p))(a) =
\begin{cases}
T, & \text{if there exists } u \text{ such that } T(p)(o(u/x)) = T
\end{cases}
\]

\[= F, \text{otherwise.} \]

Thus, it should be noted that the \( p \)'s are assertions about programs, and not themselves programming constructs. E.g., a boolean procedure \( p \) with the declaration (in ALGOL 60 notation) boolean procedure \( p ; b p ; b ; \text{begin } S ; \text{end} \); \( b p = \text{true} \), will result in an infinite computation when called in a state \( c \) for which \( S \) does not terminate, whereas \( T(S;\text{true})(o) \) yields \( F \).

Next, we introduce the following abbreviations:

\[
p \circ q, \quad \neg p, \quad p \land q, \quad p \lor q, \quad p \Rightarrow q, \quad p \Leftarrow q, \quad (p \land q), \quad (p \lor q), \quad (p \Rightarrow q), \quad (p \Leftarrow q)
\]

\[
\text{if } p \text{ then } q, \quad \text{if } p \text{ else } q, \quad \text{if } p \text{ and } q, \quad \text{if } p \text{ or } q
\]

\[
S \Rightarrow p, \quad S \Leftarrow p, \quad S \iff p
\]

\[
(p)S(q), \quad p = S = q, \quad p = S
\]

At the end of the present subsection, we consider the two cases for \( o \) and \( o' \), and define the function \( T \) as follows:

\[
T(S;p)(a) =
\begin{cases}
T, & \text{if there exists } o' \text{ such that } o' = H(S)(o) \\
& \text{and } T(p)(o') = T
\end{cases}
\]

\[= F, \text{otherwise.} \]

\[
T(\text{Bexp}(p))(a) =
\begin{cases}
T, & \text{if there exists } u \text{ such that } T(p)(o(u/x)) = T
\end{cases}
\]

\[= F, \text{otherwise.} \]

\[
T(\text{Bexp}(p))(a) =
\begin{cases}
T, & \text{if there exists } o' \text{ such that } o' = H(S)(o) \\
& \text{and } T(p)(o') = T
\end{cases}
\]

\[= F, \text{otherwise.} \]

A deduction is a construct of the form \( S_1 \Rightarrow S_2 \), where \( S_1 \) and \( S_2 \) 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 if the validity of its premises \( (\gamma) \) implies validity of its conclusion \( (\phi) \), i.e., \( (\gamma) \Rightarrow (\phi) \).

A deduction is a construct of the form \( S_1 \Rightarrow S_2 \), where \( S_1 \) and \( S_2 \) 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 if the validity of its premises \( (\gamma) \) implies validity of its conclusion \( (\phi) \), i.e., \( (\gamma) \Rightarrow (\phi) \).

A deduction is a construct of the form \( S_1 \Rightarrow S_2 \), where \( S_1 \) and \( S_2 \) 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 if the validity of its premises \( (\gamma) \) implies validity of its conclusion \( (\phi) \), i.e., \( (\gamma) \Rightarrow (\phi) \).

A deduction is a construct of the form \( S_1 \Rightarrow S_2 \), where \( S_1 \) and \( S_2 \) 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 if the validity of its premises \( (\gamma) \) implies validity of its conclusion \( (\phi) \), i.e., \( (\gamma) \Rightarrow (\phi) \).
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 same sense as investigated by a 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 \( x \leftarrow 1 \). Clearly, \( \text{true} x \leftarrow 1 (x = 1) \) is a desirable property of it, which is easily seen to be both valid, and derivable by Hoare's assignment axiom. Indeed, \( (x = 1) \leftarrow 1 \) reduces to \( 1 = 1 \), which is equivalent with 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., \( \text{true} a[2] = 1 \) (since \( \text{true} a[2] = 1 \)) (since \( \text{true} a[2] = 1 \)). Similarly we would then obtain

\[
\text{true} a[2] = 1 \quad \{ a[a[2]] = 1 \} \quad \text{(4.1)}
\]

(assuming that \( \text{true} a[2] = 1 \) \( \{ a[a[2]] = 1 \} \)) but this formula can be shown to be \( \text{true} a[2] = 1 \) in the following way: it is not difficult to verify the validity of

\[
a[1] \leftarrow 2 \quad a[a[2]] = 1 \quad \{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \text{(4.2)}
\]

Since, obviously, \( a[1] \leftarrow 2 \quad a[a[2]] = 1 \) is valid, from (4.1) we obtain

\[
a[1] \leftarrow 2 \quad a[a[2]] = 1 \quad \text{(4.3)}
\]

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

\[
(p_1 \circ p_2)[t/v] = p_1[t/v] \circ p_2[t/v], \quad \{ s_1 \leftarrow s_2 \} = \{ s_2 \leftarrow s_2[t/v] \} = \{ s_2 \leftarrow s_2[t/v] \} \text{, where we arrive at the treatment of } s_2 \text{, for } v \text{ and } a[s].
\]

We also omit the cases where \( v \) and/or \( v \) are simple variables.

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

\[
\text{Example.} \quad \{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \text{(4.4)}
\]

By a few (omitted) simplifications, we reduce this to:

\[
\{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \{ a[a[2]] = 1 \} \quad \text{(4.5)}
\]

thus correcting (4.1).

4.2 Weakest preconditions and the while statement

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

\[
\begin{align*}
\text{p.a.b} & \Rightarrow \text{Sip} \\
\text{p}(\text{while } b \text{ do } s \text{ od;true}) & \Rightarrow \text{p}(\text{while } b \text{ do } s \text{ od;true} \circ \text{true}) \\
\text{p.a.b} & \Rightarrow \text{Sip}
\end{align*}
\]

It will be shown that this is nothing but a weaker version of (3.14) (this was first noted in [3]).

Assume (3.14) and the premise \( a \Rightarrow b \Rightarrow \text{Sip} \). We show that the conclusion of (4.3) is then derivable: Since \( a \Rightarrow b \Rightarrow \text{Sip} \), clearly, also \( a \Rightarrow b \Rightarrow \text{Sip} \), or, by simple propositional logic, \( a \Rightarrow b \Rightarrow \text{Sip} \), i.e., \( a \Rightarrow b \Rightarrow \text{Sip} \), or, in the partial correctness notation \( \langle p \Rightarrow \text{Sip} \rangle \). Thus, the premise of (3.14) holds, and we infer the conclusion of (3.14): \( p \) while \( b \) do \( s \) od; \( \text{true} \circ \text{true} \), which, in the same way, can be shown to be nothing but an 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, 3]. 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 \( P \rightarrow \langle \text{val} x, \text{var} y \rangle \text{Sip} \), where to the right of "\text{Sip}" 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 \( S \) in \( S \)). For this purpose we first of all need the construct of a block: \( \text{begin new z:S end} \), 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 for example to [1, 2, 15]. We use the precise definition of substitution in a statement, written as \( \text{S}[x/v] \), apart from mentioning that the new \( z \) construct has the same variable binding effect as \( v \) ... or \( f \) ... \( d \) has elsewhere in mathematics.

Assuming these definitions, we introduce the following notation:

\[
\text{def.} \quad \begin{align*}
\text{S}[x/v] & \rightarrow \text{S}[x/v] \\
\text{S}[x/v] & \rightarrow \text{S}[x/v] \quad \text{if } a[x/v] = a & \text{then else } a[x/v] & \text{fi.}
\end{align*}
\]
\text{\textit{Semantics and the Foundations of Program Proving}}

\textit{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 of the proof theory. There is currently a vigorous activity in this area, and our paper 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 for example 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, for example 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].}

\textit{We consider it interesting work for future work to justify the proof theory as proposed for example in Owckl & 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.}

\textit{By way of conclusion, let us recall the aims of a mathematical theory of programming languages as stated in the introduction, namely 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.}

\textbf{APPENDIX}

\textit{In this appendix we give the semantics of the while statement, and present a new type of assertion which provides an alternative to the while \texttt{b do S od} construct.}

\textit{Let us assume the usual partial ordering on the elements \( \phi, \psi \in E \), \( \texttt{if} \phi \leq \psi \texttt{if} \), for all \( \alpha \), either \( \phi(\alpha) \) is undefined, or \( \phi(\alpha) \) and \( \psi(\alpha) \) are both defined and yield the same value. Let, for a chain \( \phi_0 \leq \phi_1 \leq \cdots \leq \phi_\ell \leq \cdots \), \( \ell(A) \) denotes its least upper bound. We put}

\[ M(\text{while } b \text{ do } S \text{ od}) = \bigcup_{\ell=0}^{\infty} \phi_\ell \]

\textit{where, for each \( \alpha \),}

\[ \phi_0(\alpha) = \text{undefined} \]

\[ \phi_(1)(\alpha) = \begin{cases} 
\phi_{(\ell)}(M(S)\alpha) & \text{if } T(b)\alpha = T \\
\alpha & \text{if } T(b)\alpha = F
\end{cases} \]

\textit{Furthermore, let us extend the definition of the class of assertions with the clause}

\[ \texttt{p := \_ | rep b S per p} \]

\textit{for which we define the function \texttt{T} in the following manner: For each \( \gamma, \gamma' \in E = \{T,F\} \), we put \( \gamma \leq \gamma' \texttt{if} \), for each \( \alpha \), \( \gamma(\alpha) \rightarrow \gamma'(\alpha) \). Again, \( \bigcup_{\ell=0}^{\infty} \gamma_\ell \) denotes the lub of the chain \( \gamma_0 \leq \gamma_1 \leq \cdots \leq \gamma_\ell \leq \cdots \). We now put}
\[ T(\text{rep } b; S \text{ per } p) = \gamma \]

where, for each \( \alpha \),
\[ \gamma(\alpha) = \begin{cases} 
\gamma_{i}(N(S)(), \text{ if } T(b)() = T) \\
\gamma_{i}(P(S)(), \text{ if } T(b)() = F)
\end{cases} 
\]

On the basis of these definitions we can then show the validity of assertions such as
\[
\text{while } b \text{ do } S \text{ op } p = \text{rep } b; S \text{ per } p \\
\text{rep } b; S \text{ per } p = \begin{cases} 
\text{if } b \text{ then } S \text{ rep } b; S \text{ per } p & \text{if } P \text{ fi} \\
\text{else } & 
\end{cases} 
\]

and the soundness of a deduction such as
\[
qu = \text{if } b \text{ then } S \text{ else } q \text{ per } p \\
\text{rep } b; S \text{ per } p = q
\]

(Observe that (A.1 - A.3) together yield a least-fixed-point characterization of while \( b \) do \( S \) op \( p \).

REFERENCES


