FIXPOINT APPROACH TO THE THEORY OF COMPUTATION

BY

ZOHAR MANNA

JEAN **VUILLEMIN**

COMPUTER SCIENCE DEPARTMENT

School of Humanities and Sciences

STANFORD UN **IVERS** ITY

FIXPOINTAPPROACHTO THETHEORYOFCOMPUTATION

by . .

Zohar Manna and Jean Vuillemin

Computer Science Department

Stanford University

Abstract

Following the fixpoint theory of Scott, we propose to define the
semantics of computer programs in terms of the least fixpoints of
recursive programs. This allows one not only to justify all existing
verification techniques, but also to extend them to handle various
properties of computer programs, including correctness, termination
and equivalence, in a uniform manner.

Keywords and Phrases: Verification techniques, semantics of programming
languages, least fixpoints, recursive programs,
computational induction

CR categories: 5.23, 5.24

Introduction

Substantial progress has recently been made in understanding the mathematical semantics of programming languages as a result of Scott's fixpoint theory. Our main purpose in this paper is to introduce the reader to some applications of this theory as a practical tool for proving properties of programs.

The paper consists of two parts.

In Part 1 we first introduce the notion of a recursive program and its (unique) least fixpoint. We describe the computational induction method, a powerful tool for proving properties of the least fixpoint of a recursive program. We then illustrate how one could describe the semantics of an Algol-like program P by "translating" it into a recursive program P' such that the partial function computed by P is identical to the least fixpoint of P'. Works in this area include those of McCarthy [1963a, 1963b], Landin [1964], Strachey [1966], Morris [1968], Bekić [1969], Park [1969], deBakker and Scott [1969], Scott [1970], Scott and Strachey [1971], Manna, Ness and Vuillemin [1972], Milner [1972], Weyhrauch and Milner [1972].

In Part 2 of the paper we illustrate some of the advantages of the fixpoint approach to program semantics. First, we justify the inductive assertion methods of Floyd [1967] and Hoare [1969, 1971]. Other verification methods such as recursion induction (McCarthy [1963a], [1963b]), structural induction (Burstall [1969]), fixpoint induction (Park [1969], Cooper [1971]), and the predicate calculus approach (Manna [1969], Manna and Pnueli [1970]) can be justified in much the same way. Secondly, we emphasize that the fixpoint approach suggests a natural method for proving properties of programs: given a

1

program P , we can translate it into the corresponding recursive

program **P'** , and then prove the desired properties for the least

fixpoint of **P'** by computational induction. In contrast to other

existing methods, this approach gives a <u>uniform</u> way of expressing

and proving different properties, including correctness, termination

and equivalence. This makes it very convenient for machine implementa-

tion (Milner [1972]).

Warning: The reader should be aware that some of the results

presented in this paper hold only under certain restrictions which are

ignored in this informal presentation.

PART 1.   THE FIXPOINT APPROACH TO PROGRAM SEMANTICS

1.1 Recursive Programs

A recursive program is a LISP-like definition of the form

$$F(\bar{x}) \Leftarrow \tau[F](\bar{x}) \; ,$$

where $\tau[F](\bar{x})$ is a composition of base functions and the function
variable F , applied to the individual variables $\bar{x} = (x,y,z,\ldots)$.
The following, for example, is a recursive program over the integers

$$P_0: \quad F(x,y) \Leftarrow \underline{if} \; x = y \; \underline{then} \; y+1 \; \underline{else} \; F(x,F(x-1,y+1)) \; .$$

We allow our base functions to be partial, i.e., they may be
undefined for some arguments. This is quite natural, since they
represent the result of *some* computation which may in general give
results for some inputs and run indefinitely for others. We include
as limiting cases the partial functions defined for all arguments,
called total functions, as well as the partial function undefined for
all arguments

Let us consider now the following partial functions:

$f_1(x,y):$ x+1

$f_2(x,y):$ $\underline{if} \; x \geq y \; \underline{then} \; x+1 \; \underline{else} \; y-1$, and

$f_3(x,y):$ $\underline{if} \; (x > y) \wedge (x-y \; even) \; \underline{then} \; x+1 \; else \; \underline{undefined}$.

These functions have an interesting common property: For each i
$(1 \leq i \leq 3)$, if we replace all occurrences of F in the program P_0
by f_i , the lefthand side and the righthand side of the symbol $\Leftarrow$
yield identical partial functions, i.e.,$\overset{*/}{}$

$\overset{*/}{}$ $\equiv$ is an extension of the regular = relation for handling underlined undefined
values. a $\equiv$ b is true if both a and b are undefined, but it is
false if only one of them is undefined.

3

$$f_i(x,y) \equiv \underline{\text{if}} \ x = y \ \underline{\text{then}} \ y{+}1 \ \underline{\text{else}} \ f_i(x,f_i(x{-}1,y{+}1)).$$

We say that the functions f_1 , f_2 and f_3 are <u>fixpoints</u> of the recursive program P_0 . ..

Among the three functions, f_3 has one important special property: for any (x,y) such that $f_3(x,y)$ is defined, i.e., $(x \geq y) \wedge (x{-}y \text{ even})$, both $f_1(x,y)$ and $f_2(x,y)$ are also defined and have the same value as $f_3(x,y)$. We say that f_3 is "less defined than or equal to" f_1 and f_2 , and denote this by $f_3 \sqsubseteq f_1$ and $f_3 \sqsubseteq f_2$. It can be shown that f_3 has this property not only with respect to f_1 and f_2 but with respect to all fixpoints of the recursive program P_0 . Moreover, $f_3(x,y)$ is the <u>only</u> function having this property; f_3 is therefore said to be the <u>least (defined) **fixpoint** of P_0</u> .

One of the most important results related to this topic is due to Kleene [1952], who showed that <u>every recursive program P has a unique least **fixpoint**</u> (denoted by f_P).

In discussing our recursive programs, the key problem is: <u>What is the partial function f defined by a recursive program P ?</u> There are two viewpoints.

.(a) **Fixpoint** approach: Let it be the unique least **fixpoint** f_P .

(b) **Computational** approach: Let it be the computed function C_P for some given **computation** rule C (such as "**call** by **name**" or "call by value").

We now come to an interesting point: all the theory for proving properties of recursive programs is based on the assumption that the

function defined by a recursive program is exactly the least fixpoint f_P .
That is, the fixpoint approach is adopted. Unfortunately, many programming
languages use implementations of recursion (such as "call by value" !)
which do not necessarily lead to the least fixpoint (Morris [1968]).*/

Let us consider, for example, the following recursive program over
the integers

$$P_1 \; : \; F(x,y) \; \Leftarrow \; \underline{if} \; x = 0 \; \underline{then} \; 1 \; else \; F(x-1, F(x,y))$$

The least fixpoint f_{P_1} can be shown to be

$$f_{P_1}(x,y) \; : \; \underline{if} \; x \geq 0 \; \underline{then} \; 1 \; \underline{else} \; \underline{undefined} \; .$$

However, the computed function C_{P_1} , where C is "call by value", turns
out to be

$$C_{P_1}(x,y) \; : \; \underline{if} \; x = 0 \; \underline{then} \; 1 \; else \; \underline{undefined} \; .$$

Thus, C_{P_1} is properly less defined than f_{P_1} -- e.g., $C_{P_1}(1,0)$ is
$\underline{undefined}$ while $f_{P_1}(1,0) = 1$.

There are two alternative ways to view this problem: (a) Existing
computer languages should be modified, and language designers and
implementors should seek computation rules which always lead to the least
fixpoint. "Call by name" is one such computation rule, but unfortunately
it often leads to very inefficient computations. An efficient computation
rule which always leads to the least fixpoint can be obtained by modifying

---

*/ It can be shown in general that for every recursive program P and
any computation rule C , C_P must be less defined than or equal to
f_P , i.e., $C_P \sqsubseteq f_P$ (Cadiou [1972]).

"call by value" so that the evaluation of the arguments of a procedure is delayed as long as possible (Vuillemin [1972]).   (b) Theoreticians are wasting their time by developing fixpoint methods for proving properties of programs which do not compute fixpoints. They should instead concentrate their efforts on developing direct methods for proving properties of programs as they are actually executed.

We shall indicate in Part 2 of this paper how the apparent conflict between these views can be resolved by a suitable choice of the semantic definition of the programming language.

1.2 The Computational Induction Method

The main practical reason for suggesting the fixpoint approach is the existence of a very powerful tool, the computational induction method, for proving properties of recursive programs. The idea of the method is essentially to prove properties of the least fixpoint f_P of a given recursive program P by induction on the level of recursion.

Let us consider, for example, the recursive program

P_2 : $F(x) \Leftarrow$ if $x = 0$ then 1 else $x \cdot F(x-1)$,

over the natural numbers. The least fixpoint $f_{P_2}(x)$ of this recursive program is the factorial function x! .

Let us denote by $f^i(x)$ the partial function indicating the "information" we have after the i-th level of recursion. That is,

6

$f^0(x)$ is <u>undefined</u> (for all x);

$f^1(x)$ is <u>if</u> x = 0 <u>then</u> 1 else $x \cdot f^0(x-1)$,

        i.e.,   <u>if</u> x = 0 <u>then</u> 1 else <u>undefined</u> ;

$f^2(x)$ is <u>if</u> x = 0 <u>then</u> 1 <u>else</u> $x \cdot f^1(x-1)$,

        i.e.,   <u>if</u> x = 0 <u>then</u> 1 else $x \cdot (\underline{if}$ x-1 = 0 <u>then</u> 1 <u>else undefined)</u> ,

        or in short,   <u>if</u> x = 0 $\vee$ x = 1 <u>then</u> 1 else <u>undefined</u> ;

    etc.

In general, for every i , $i \geq 1$,

        $f^i(x)$ is <u>if</u> x = 0 $x \cdot \underline{fn}$ 1 <u>else</u> $^{i-1}(x-1)$,

which is

        <u>if</u> x < i <u>then</u> x! <u>else undefined</u> .

This sequence of functions has a limit which is exactly the least fixpoint
of the recursive program; that is,

        $\lim_{i \to \infty} \{f^i(x)\} \equiv x!$.

    This will in fact be the case for any recursive program P : if P
is a recursive program of the form $F(\bar{x}) \Leftarrow \tau[F](\bar{x})$, and $f^i(\bar{x})$ is
defined by

        $f^0(\bar{x})$ is Ω (<u>undefined</u> for all $\bar{x}$), and

        $f^i(\bar{x})$ is $\tau[f^{i-1}](\bar{x})$ f o r   i ≥ 1 ,$\underline{*/}$

then

        $\lim_{i \to \infty} \{f^i(\bar{x})\} \equiv f_P(\bar{x})$.

$\underline{*/}$ $\tau[f^{i-1}]$ is the result of replacing all occurrences of F in $\tau[F]$
    byf $^{i-1}$.

This suggests an induction rule for proving properties of f_P : To show that some property φ holds for f_P , i.e., $\varphi(f_P)$, we show that $\varphi(f^i)$ holds for all $i \geq 0$, and that φ remains true in the limit; therefore we may conclude that $\varphi(\lim_{i \to \infty}\{f^i\})$, i.e., $\varphi(f_P)$, holds.

Note that it is not true in general that φ remains true in the limit. For example, for the recursive program P_2 introduced above, $f^i(x)$ is the non-total function if $x < i$ then x! else undefined , while $\lim_{i \to \infty}\{f^i\}$, i.e., f_{P_2} , is the total function x! . Thus for $\varphi(f)$ being " f is not total", we have that $\varphi(f^i)$ holds for all $i \geq 0$, while $\varphi(\lim_{i \to \infty} \{f^i\})$ does not hold. However, the limit property holds of a rather large class of φ (called "admissible predicates" -- see Manna, Ness and Vuillemin [1972]); in particular, all the predicates that we shall use later have this property.

There are two well-known ways to prove that $\varphi(f^i)$ holds for all $i \geq 0$, the rules for simple and complete induction on the level of recursion.

(a) Simple induction:

$$\text{if } \varphi(f^0) \text{ holds and } \forall i[\varphi(f^i) \Rightarrow \varphi(f^{i+1})] \text{ holds,}$$

$$\text{then } \varphi(f_P) \text{ holds .}$$

(b) Complete induction:

$$\text{if } \forall i\{[\forall j \text{ such that } j < i)\varphi(f^j)] \Rightarrow \varphi(f^i)\} \text{ holds ,}^{*/}$$

$$\text{then } \varphi(f_P) \text{ holds .}$$

---

*/ Note that this includes implicitly the need to prove $\varphi(f^0)$, since for i = 0 there is no j such that j < i .

8

The simple induction rule is essentially the "μ-rule" suggested by deBakker and Scott [1969], while the complete induction rule is the "truncation induction rule" of Morris [1971]. Scott actually suggested the more elegant rule

$$\text{if } \varphi(\Omega) \text{ holds and } \forall f[\varphi(f) \Rightarrow \varphi(\tau[f])] \text{ holds,}$$

$$\text{then } \varphi(f_P) \text{ holds,}$$

which does not assume any knowledge of the integers in its formulation. These rules generalize easily to systems of mutually recursive definitions.

Example: Consider the recursive programs

$$P_3 : \quad F(x,y,z) \Leftarrow \text{if } x = 0 \text{ then } y \text{ else } F(x\text{-}1,y\text{+}z,z)$$

and

$$P_4 : \quad G(x,y) \Leftarrow \text{if } x = 0 \text{ then } y \text{ else } G(x\text{-}1,y\text{+}2x\text{-}1) .$$

We would like to prove, using computational induction, that

$$f_{P_3}(x,0,x) \equiv g_{P_4}(x,0) \quad \text{for any natural number } x .$$

(Both functions compute the square of x .)

For this purpose, we shall prove a stronger result than the desired one by simple computational induction. Proving a stronger result often simplifies proofs by induction, since it allows the use of a stronger induction hypothesis. So, using

$$\varphi(f,g) : \quad \forall x \forall y [f(y,x(x\text{-}y),x) \equiv g(y,x^2\text{-}y^2) \; 1 \; ,$$

we try to show that

$$\varphi(f_{\blacksquare},g_{\blacksquare}) : \quad \forall x \forall y [f'_{\blacksquare} \blacksquare \equiv \blacksquare^2 \blacksquare^2) 1$$

■

holds. The desired result then follows by choosing $x = y$. The induction proceeds in two steps:

(a) $\varphi(f^0, g^0)$, i.e., $\forall x \forall y [f^0(y,x(x-y),x) \equiv g^0(y,x^2-y^2)\ 1$.

Trivial, since $\forall x \forall y[\underline{\text{undefined}} \equiv \underline{\text{undefined}}]$.

(b) $\forall i [\varphi(f^i,g^i) \Rightarrow \varphi(f^{i+1},g^{i+1})]$.

We assume
$$\forall x \forall y [f^i(y,x(x-y),x) \equiv g^i(y,x^2-y^2)\ 1$$

and prove
$$\forall x \forall y [\ f^{i+1}(y,x(x-y),x) \equiv g^{i+1}(y,x^2-y^2)]\quad .$$

$f^{i+1}(y,x(x-y),x) \equiv \text{if } Y = 0\ \underline{\text{then }} x(x-0)\ \text{else } f^i(y-1,x(x-y)+x,x)$

$\equiv \underline{\text{if }} y = 0\ \underline{\text{then }} x^2\ \text{else } f^i(y-1,x(x-(y-1)),x)$

$\equiv \underline{\text{if }} y = 0\ \underline{\text{then }} x2\ \underline{\text{else }} g^i(y-1,x^2-(y-1)^2)$

by the induction hypothesis

$\equiv \underline{\text{if }} y = 0\ \underline{\text{then }} x^2-0^2\ \text{else } g^i(y-1,(x^2-y^2)+2y-1)$

$\equiv g^{i+1}(y,x^2-y^2)\quad .$

1.3 Semantics of Algal-like Programs

Our purpose in this section is to illustrate how one can describe the semantics of an Algol-like program P by translating it into a recursive program **P'** such that the partial function computed by P is identical to the least **fixpoint** of **P'** . The features of Algol we consider are very simple indeed, but there is no theoretical difficulty in extending them,

The translation is defined blockwise: to each block B (or elementary statement) we associate a partial function f_B describing the effect of the block (or statement) on the values of the variables. For example,

$$\underline{begin}\ x\ :=\ x{+}1;\ y\ :=\ y{+}1\ \underline{end}\ ,$$

will be represented by the function

$$f(x,y) \equiv (x{+}1, y{+}1)\ .$$

Functions are then combined to represent the whole program using the rule:

$$f_{B_1 \bullet_2}(\bar{x}) \equiv f_{B_2}(f_{B_1}(\bar{x}))\ .$$

This definition is unambiguous, since composition of partial functions is associative, i.e.,

$$f_{B_3}(f_{B_1;B_2}(\bar{x})) \equiv f_{B_1;B_2;B_3}(\bar{x}) \equiv f_{B_2;B_3}(f_{B_1}(\bar{x}))\ .$$

All that remains to be done is to describe the partial function associated with each elementary statement of the language. For simplicity, we shall first consider only a "flowchartable" subset of a language, with no goto statements or procedure calls. We shall also ignore the problem of declarations.

1) Assignment statements

   if B is $x_i := E(\bar{x})$ where E is an expression,

   $f_B(\bar{x})$ is $(x_1, \ldots, x_{i-1}, E(\bar{x}), x_{i+1}, \ldots, x_n)$.

2) Conditional statements

   if B is if $p(\bar{x})$ then B_1 ,

   $f_B(\bar{x})$ is if $p(G)$ then $f_{B_1}(\bar{x})$ else $\bar{x}$,

11

and

if B is   <u>if</u> p(x) <u>then</u> B_1 <u>else</u> B_2,

$f_B(\bar{x})$ is <u>if</u> $p(\bar{x})$ <u>then</u> $f_{B_1}(\bar{x})$ else $f_{B_2}(\bar{x})$.

3)   Iterative statements

if B is <u>while</u> $p(\bar{x})$ <u>do</u> B_1 ·, .

$f_B(\bar{x})$ is the least fixpoint of the recursive program

$$F(\bar{x}) \Leftarrow \text{if } p(\bar{x}) \; t(\bar{x})) \; F(f_{B_1} \text{else} \quad \bar{x} \quad .$$

Example: Let us consider the following program for computing in x the greatest natural number smaller than or equal to $\sqrt{a}$, i.e., $x^2 \leq a < (x+1)^2$, where a is any natural number. (The computation method is based on the fact that $1 + 3 + 5 + \ldots + (2n-1) = n^2$ for every $n > 0$.)

P_5 : <u>begin</u> <u>integer</u> x,y,z;

        x := 0; y := z := 1;

        <u>w</u>hile y_ < a d<u>o</u>

            <u>begin</u> x := x+1;

                z := z+2;

                Y := y+z;

            <u>end</u>;

    <u>end</u>.

The partial function computed by P_5 is identical to the least fixpoint of P_5' , where

P_5' : $F_0(a) \Leftarrow F(a,0,1,1)$

    $F(a,x,y,z) \Leftarrow$ <u>if</u> $y \leq a$ <u>then</u> $F(a,x+1,y+z+2,z+2)$

                    <u>else</u> (a,x,y,z)

4) <u>got0 statements</u>

There has been much discussion (see, for example, Dijkstra [1968], Knuth and Floyd [1971], Ashcroft and Manna [1971]) about the usefulness of got0 statements: they tend to make programs difficult to understand and debug, and one might prefer to use while or for statements instead. Without entering further into this controversy, we shall see that the semantics of got0 statements is quite complex. In particular, it may lead to systems of mutually recursive definitions, and (not too surprisingly) it is indeed harder to prove properties of programs with goto statements. We consider two simple cases.

If we have a block of the form

$$\underline{begin} \ldots ; L: B_1 ; \ldots ; B_{i-1} ; \underline{goto} \; L ; B_{i+1} ; \ldots ; B_n \; \underline{end} \; ,$$

then we define

$f_{\underline{goto} \; L;B_{i+1};\ldots;B_n}(\bar{x})$ to be the least fixpoint of the recursive program

$$F_L(\bar{x}) \Leftarrow f_{B_1;\ldots;\bullet}(\bar{x})_{Bnx} .$$

If we have a block of the form

$$\underline{begin} \ldots ; \underline{goto} \; L ; B_1 ; \ldots ; B_{i-1} ; L: B_i ; B_{i+1} ; \ldots B_n \; \underline{end} \; ,$$

then we define

$f_{\underline{goto} \; L;B_1;\ldots;B_n}(\bar{x})$ to be the least fixpoint of the recursive program

$$F_L(\bar{x}) \Leftarrow f_{B \ldots ;B_n}(\bar{x}) \quad .$$

Note that we have revised our rule of composition, since $f_{B;B'}(\bar{x}) \equiv f_{B'}(f_B(\bar{x}))$ is not valid when B is a goto statement. Similarly, if we wish to allow goto's which jump out of

13

iterative statements or branches of conditional statements, then we must change their semantic definition accordingly.

Example: Let us consider anotherversion of P_5 , using only the operations <u>successor</u> and <u>predecessor</u> .

P_6 : <u>begin</u> <u>integer</u> x,y,z;

  x := 0; y:= z := l;

  L: <u>if</u> y $\leq$ a <u>then</u>

      <u>begin</u> integer t;

          x := x+l;

          z := z+l;

          t := z+l;

          M: <u>if</u> t > 0 <u>then</u>

          <u>begin</u> y := y+l;

              t := t-1;

              <u>goto</u> M;

          <u>end</u>;

          z := z+l; <u>gotO</u> L;

      <u>end</u>;

  <u>end</u>.

The partial function computed by P_6 is identical to the least fixpoint of P'_6 where

P'_6 : $F_0(a) \Leftarrow F_L(a,0,1,1)$

  $F_L(a,x,y,z) \Leftarrow$ <u>if</u> y $\leq$ a <u>then</u> $F_M(a,x+1,y,z+1,z+2)$

                              (<u>else</u> x, y, z)

  $F_M(a,x,y,z,t) \Leftarrow$ <u>if</u> t > 0 <u>then</u> $F_M(a,x,y+1,z,t-1)$

                              <u>else</u> $F_L(a,x,y,z+1)$

14

Let us now define the semantics of simple procedures without parameters. We shall not discuss problems such as "side effects", parameter passing or the procedure copy-rule for call by name.

5) <u>procedures</u>

  (a) For the non-recursive procedure

  <u>procedure</u> P;B

  (where P is the procedure name and B is its body), we define

  $$f_{\underline{call}\ P}(\bar{x}) \text{ to be } f_B(\bar{x}) \ .$$

  (b) For the recursive procedure

  <u>procedure</u> P; B[P] ,

  we define

  $$f_{\underline{call}\ P}(x) \text{ to be the least \textbf{fixpoint} of the recursive}$$
  $$\text{program } F(\bar{x}) <= f_{B[P]}(\bar{x})$$

  where occurrences of <u>call</u> P will be replaced by F in the semantic definition of $f_{B[P]}$.

6) <u>An answer to the problem of "call by value"</u>

Cur semantic definition of recursive procedures assumes that the implementation of recursion in the language always leads to the least fixpoint. If this is not the case, we must change our semantic definition: to every program P we associate a recursive program **P'** such that the least **fixpoint** of **P'** <u>will always be identical</u> to the partial function computed by P . Consider, for example, the program

  <u>integer procedure</u> P(<u>integer</u> x,y);

  P := <u>if</u> x = 0 <u>then</u> 1 <u>else</u> P(x-1,P(x,y));

15

If the implementation is "call by name", its semantics will be

$$f_{\underset{\sim}{call}\ P}(x,y) \quad \text{is the least fixpoint of}$$

$$F(x,y) \Leftarrow \underline{if}\ x = 0\ \underline{then}\ 1\ else\ F(x\text{-}1,F(x,y))\ .$$

However, if the implementation is "call by value", its semantics will be

$$f_{\underset{\sim}{call}\ P}(x,y) \quad \text{is the least fixpoint of}$$

$$F(x,y) \Leftarrow if\ (x = 0)\ \wedge\ def(y)\ \underline{then}\ 1\ else\ F(x\text{-}1,F(x,y))\ ,$$
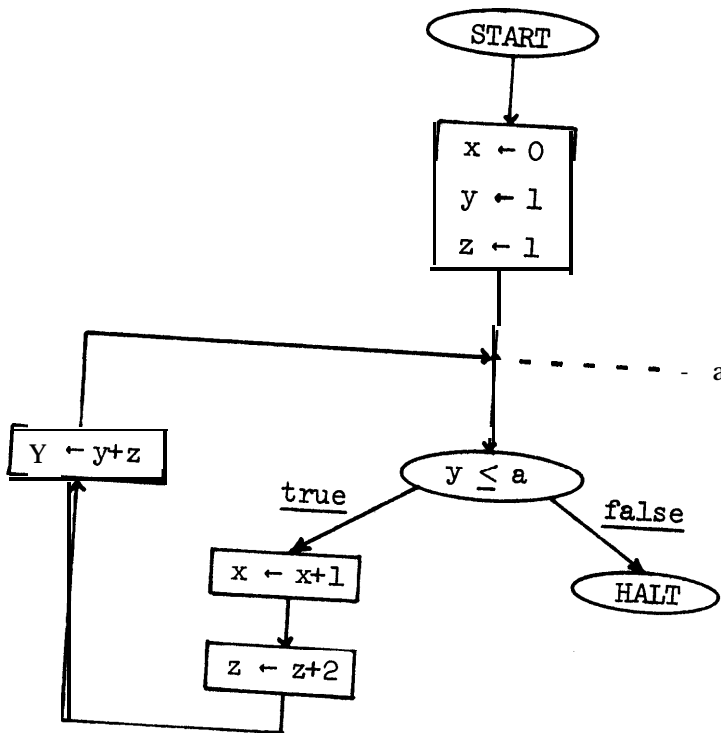
where the (computable) predicate $def(y)$ is true whenever y is

defined, and undefined otherwise.

PART 2. APPLICATION TO THE VERIFICATION PROBLEM

Our purpose in the second part of the paper is to illustrate some of the advantages or the fixpoint approach to program semantics.

2.1 Justification of the Inductive Assertions Method

The most widely used method for proving properties of "flowchart programs" is presently the inductive assertions method, suggested by Floyd [1967] and Naur [1966]. We shall illustrate the method on the simple program P_5 above. To clarify our discussion we shall describe the program as a flowchart:

```
                         ┌──────────┐
                         │  START   │
                         └────┬─────┘
                              │
                         ┌────▼─────┐
                         │  x ← 0   │
                         │  y ← 1   │
                         │  z ← 1   │
                         └────┬─────┘
                              │
         ┌────────────────────┼ ─ ─ ─ ─ ─ ─ ─ a
         │                    │
         │                ┌───▼────┐
  ┌──────────┐       true  │  y ≤ a │  false
  │  Y ← y+z │ ◄───────────┤        ├──────────┐
  └──────────┘             └────────┘          │
         ▲                                 ┌───▼────┐
         │              ┌──────────┐       │  HALT  │
         │              │ x ← x+1  │       └────────┘
         │              └────┬─────┘
         │              ┌────▼─────┐
         └──────────────┤  z ← z+2 │
                        └──────────┘
```

We wish to show that this flowchart program, whenever it terminates, computes the greatest natural number smaller than or equal to $\sqrt{a}$, i.e., that $x^2 \leq a < (x+1)^2$, for any natural number a .

17

To do this we associate a predicate $Q(a,x,y,z)$, called an
inductive assertion, with the point labelled α in the program, and
show that Q must be true for the values of the variables (a,x,y,z)
whenever execution of the program reaches point α . Thus, we must
show: (a) that if we start execution with $a > 0$, then the assertion
holds when point α is first reached, i.e., that $Q(a,0,1,1)$ holds;
and   (b) that the assertion remains true when one goes around the
loop from α to α , i.e., that $(y \leq a)$ A $Q(a,x,y,z)$ implies
$Q(a,x+1,y+z+2,z+2)$. To prove the desired result we finally show
(c) that $x^2 \leq a < (x+1)^2$ follows from the assertion $Q(a,x,y,z)$
when the program terminates, i.e., that $(y > a)$ A $Q(a,x,y,z)$ implies
$x^2 \leq a < (x+1)^2$.

To verify the program, we take

$$Q(a,x,y,z) \text{ to be } (x^2 \leq a) \text{ A } (y = (x+1)^2) \text{ A } (z = 2x+1) .$$

One can then verify easily that conditions (a), (b) and (c) above,
called the verification conditions, hold.

Hoare's inductive assertion method is actually a generalization of
Floyd's method; Hoare [1969, 1971] realized that if we wish to apply the
method of inductive assertions to prove properties of a large program, we
shall undoubtedly have to break the program into smaller parts, prove
what we need about the parts, and then combine everything together. We
will clearly break the program into pieces in the most convenient way
for the proof, and, since composition of statements is associative, the
way in which we group the statements of the program is irrelevant. For
example, if the given program is of the form

P: $B_1; B_2;\ B_3; B_4$,

18

we can associate the statements in several different ways, e.g.,

$$((B_1; B_2); B_2); B_3 \quad ,$$

$$(B_1; (B_2; B_3)) ; B_4 \quad ,$$

$$(B_1; B_2); (B_3; B_4) \quad ,$$

or

$$B_1; (B_2; (B_3; B_4)) \quad .$$

Although the programs do not look the same, all of them yield the same least fixpoint, and therefore they are equivalent. If we express other verification techniques using this notation, we find that Floyd and Naur consider only the first possibility, i.e., grouping statements to the left, while McCarthy [1963b] and Manna and Pnueli [1970] only consider the last possibility, i.e., grouping statements to the right.

Following Hoare, we express this idea by writing $\{R\}B\{T\}$ [*] to mean that if $R(\bar{x})$ holds before executing the piece of program B and if B terminates, then $T(\bar{x})$ will hold after executing B .

We first apply <u>verification rules</u> to each statement of the program. Examples of such rules are:

(a) assignment statement rule:

$$R \supset S_{x_i}^{E(\bar{x})} \text{ implies } \{R\} \ x_i := E(\bar{x}) \ \{S\}$$

where $S_{x_i}^{E(\bar{x})}$ stands for the result of replacing all occurrences of x_i in S by $E(\bar{x})$;

---

[*] We prefer this notation to Hoare's $R\{B\}T$.

19

(b)   conditional statement rule:

$$\frac{\{R_1\}B_1\{T\} \ \text{ and } \ \{R_2\}B_2\{T\} \ \text{ implies}}{\{\text{if } p(\bar{x}) \text{ then } R_1 \text{ else } R_2\} \ \underset{\sim}{\text{if }} p(\bar{x}) \ \underset{\sim}{\text{then }} B_1 \ \underset{\sim}{\text{else }} B_2 \ \{T\}} \ , \ ^{*/}$$

(c)   iterative statement rule:

$$\{R \wedge p(\bar{x})\} \ B \ \{R\} \ \text{implies} \quad \{R\} \ \underset{\sim}{\text{while }} p(\bar{x}) \ \underset{\sim}{\text{do }} B \ \{R \wedge \sim p(\bar{x})\} \ .$$

We then compose pieces of the program until we get the entire program, using the following

(d)   composition rule:

$$\frac{\{R\}B_1\{S\} \quad \text{and} \quad \{S\}B_2\{T\} \quad \text{implies} \quad \{R\}B_1;B_2\{T\}}{} \ ,$$

(e)   consequence rules:

$$\frac{R \supset S \text{ and } \{S\}B\{T\} \quad \text{implies} \quad \{R\}B\{T\}}{} \ , \ \text{and}$$

$$\frac{\{R\}B\{S\} \text{ and } S \supset T \quad \text{implies} \quad \{R\}B\{T\}}{} \ .$$

Example.   A proof of the correctness of the program P_5 , given above, could be sketched as follows.

First, we establish, using the assignment statement rule, the following results:

Since $a \geq 0 \supset R(a,0,1,1)$, where $R(a,x,y,z)$ is $(x^2 \leq a) \wedge (y = (x+1)^2) \wedge (z = 2x+1)$, we get

(1) $(a > 0\} \ x := 0; \ y := z := 1 \ \{R(a,x,y,z)\}$.

Since $R(a,x,y,z) \land y \leq a \supset R(a,x+1,y+z+2,z+2)$, we get

(2) $\{R(a,x,y,z) \land y \leq a\}$ x := x+1; z := z+2; y := y+z $\{R(a,x,y,z)\}$.

By using the iterative statement-rule, we get from (2)

(3) $\{R(a,x,y,z)\}$ <u>while</u> $y \leq a$ <u>do begin</u> x := x+1;

  z := z+2; y := y+z <u>end</u> $\{R(a,x,y,z) \land y > a\}$.

We now combine the results of (1) and (3) using the composition rule
to obtain

(4) $\{a \geq 0\}$ P_5 $\{R(a,x,y, z) \land \; > a\}$.

Since $[R(a,\bar{x},y,z) \land y > a] \supset x^2 \leq a < (x+1)^2$, we apply the consequence
rule and finally get

(5) $\{a \geq 0\}$ P_5 $\{x^2 \leq a < (x+1)^2\}$

It is quite important that all of **Hoare's** verification rules can in
fact be <u>proved</u> from the semantics we gave, just by using **computational**
induction. We shall illustrate this point by justifying two of the most
powerful verification rules: the rule for <u>while</u> statements, and the rule
for <u>call</u> of recursive procedures. For this purpose, we need to relate
the notation $\{R\}$ B $\{T\}$ to our $f_B(\bar{x})$, the partial function indicating
the change of the values of the variables during the execution of B .
$\{R\}$ B $\{T\}$ simply means that whenever $R(\bar{x})$ is <u>true</u>, $T(f_B(\bar{x}))$ is either
<u>true</u> (if B terminates) or <u>undefined</u>. We can express this by the relation

  $R(\bar{x}) \Rightarrow T(f_B(\bar{x}))$,

adopting here the convention that a ⇒ b is <u>true</u> whenever a or b

is <u>undefined</u>.

We are ready now to prove the following rules:

(a) <u>rule for while statements</u>

The verification rule for <u>while</u> statements indicates that if the

execution of the body of the <u>while</u> statement leaves the assertion R

invariant, R should hold upon termination of the <u>while</u> statement. More

precisely,

$$\{R(\bar{x}) \wedge p(\bar{x})\} \; B \; \{R(\bar{x})\} \quad \text{implies} \quad \{R(\bar{x})\} \; \underline{\text{while}} \; p(x) \; \underline{\text{do}} \; B \; \{R(\bar{x}) \wedge \sim p(\bar{x})\} \; .$$

We therefore-have to prove the following theorem:

$$\forall \bar{x}[R(\bar{x}) \; A \; p(\bar{x}) \Rightarrow R(f_B(\bar{x}))]$$

implies

$$\forall \bar{x}[R(\bar{x}) \Rightarrow R(f_p(\bar{x})) \wedge \sim p(f_p(\bar{x}))] \; \text{where}$$

$$\mathbf{P}: \quad F(\bar{x}) <= \underline{\text{if}} \; p(\bar{x}) \; \underline{\text{then}} \; F(f_B(\bar{x})) \; \underline{\text{else}} \; \bar{x} \; .$$

The proof is by computational induction.

1. $\forall \bar{x}[R(\bar{x}) \Rightarrow R(f^0(\bar{x})) \, A \sim p(f^0(\bar{x}))]$ is clearly true according to our

    convention, since $R(f^0(\bar{x}))$ and $\sim p(f^0(\bar{x}))$ are <u>undefined</u>.

2. We assume $\forall \bar{x}[R(\bar{x}) \Rightarrow R(f^i(\bar{x})) \wedge \sim p(f^i(\bar{x}))]$ and show

    $\forall \bar{x}[R(\bar{x}) \Rightarrow R(f^{i+1}(\bar{x})) A \sim p(f^{i+1}(\bar{x}))]$. By definition of f^{i+1}

    we have

    $$R(f^{i+1}(\bar{x})) . - \underline{\text{if}} \; p(\bar{x}) \; \underline{\text{then}} \; R(f^i(f_B(\bar{x}))) \; \text{else} \; R(\bar{x}) \; , \; \text{and}$$

    $$p(f^{i+1}(\bar{x})) \equiv \underline{\text{if}} \; p(\bar{x}) \; \underline{\text{then}} \; p(f^i(f_B(\bar{x}))) \; \underline{\text{else}} \; p(\bar{x})$$

We distinguish between two cases:

Case 2A: $p(\bar{x})$ is <u>false</u>. Then, $R(f^{i+1}(\bar{x})) \equiv R(\bar{x})$ and
$p(f^{i+1}(\bar{x})) \equiv p(\bar{x})$, so that $R(\bar{x}) \Rightarrow R(f^{i+1}(\bar{x})) \wedge \sim p(f^{i+1}(\bar{x}))$ is v&Lid.

Case 2B: $p(\bar{x})$ is <u>true</u>. Then $R(f^{i+1}(\bar{x})) \equiv R(f^i(f_B(\bar{x})))$ and
$p(f^{i+1}(\bar{x})) \equiv p(f^i(f_B(\bar{x})))$. By the assumption $R(\bar{x}) \wedge p(\bar{x}) \Rightarrow R(f_B(\bar{x}))$

holds, and since by the induction hypothesis

$R(f_B(\bar{x})) \Rightarrow R(f^i(f_B(\bar{x}))) \wedge \sim p(f^i(f_B(\bar{x})))$, we get

$R(\bar{x}) \Rightarrow R(f^i(f_B(\bar{x}))) \wedge \sim p(f^i(f_B(\bar{x})))$. Hence,

$R(\bar{x}) \Rightarrow R(f^{i+1}(\bar{x})) \wedge \sim p(f^{i+1}(\bar{x}))$ as desired.

(b) <u>Rule for recursive calls</u>

Let us consider a recursive procedure

<u>procedure</u> P; B[P] ,

where P is the name of the **procedure** and B[P] represents its body.
The verification rule for proving properties of P is quite similar to
computational induction, although its **formulation** might look rather
paradoxical: in order to prove a property of the recursive procedure P ,
one is permitted to assume that the desired property holds for the
body B[P] of the procedure! This can be stated as follows:

$\forall g$ [{R} g {T} implies {R} B[g] {T}] implies {R} <u>call</u> P {T} .

As Hoare [1971, p. 109] puts it, "this assumption of what we want to
prove before embarking on the proof **explains** well the aura of magic which
attends a programmer's first introduction to recursive programming".

---

*/ A more rigorous treatment would require checking also the case in
which $p(\bar{x})$ is <u>undefined</u>.

The rule.howeve.is easy to justify. We have to prove the
following theorem:

$$\forall g[\forall \bar{x}[R(\bar{x}) \Rightarrow T(g(\bar{x}))] \text{ implies } \forall \bar{x}[R(\bar{x}) \Rightarrow T(f_{B[g]}(\bar{x}))]]$$

implies

$$\forall \bar{x}[R(\bar{x}) \Rightarrow T(f(\bar{x}))] \text{ where}$$

$$\mathbf{P}: \quad F(\bar{x}) <= f_{B[F]}(\bar{x}) \quad .$$

The **proof** is again by computational induction.

1. $\forall x[R(\bar{x}) \Rightarrow T(f^0(\bar{x}))]$ is <u>true</u>,. since $T(f^0(\bar{x}))$ is <u>undefined</u>.

2. We assume $\forall \bar{x}[R(\bar{x}) \Rightarrow T(f^i(\bar{x}))]$ and show $\forall \bar{x}[R(\bar{x}) \Rightarrow T(f^{i+1}(\bar{x}))]$.
   By the induction hypothesis, $R(\bar{x}) \Rightarrow T(f^i(\bar{x}))$, therefore, by the
   assumption of the theorem $R(\bar{x}) \Rightarrow T(f_{B[f^i]}(\bar{x}))$. Thus, from the
   definition of f^{i+1} we get $R(\bar{x}) \Rightarrow T(f^{i+1}(\bar{x}))$, as desired.

2.2 Translation to Recursive Programs

In the present state of the art of verifying programs, Hoare's method
is presumably the most convenient for proving the correctness of programs.
However, its main drawback is that it can **handle** only "partial correctness"
of data ...e., we can only show that the **final** results of the programs,
... satisfy some given input-output relation. The method, does not
... ...that any means for proving termination, and seems rather ill-fitted
for proving equivalence between programs.

This is another case where our semantic definition of the programming
language pays off: properties like termination and equivalence can be

handled in exactly the same way as partial correctness. The idea is quite simple: To prove some property of a given program P , translate it to the corresponding recursive program **P'** , and then prove the desired property for $f_{P'}$, by computational induction. In this method we actually still benefit from all the advantages of **Hoare's** approach since we may associate the blocks **of the** program arbitrarily at our convenience.

To show, for example, that the partial function defined by the given program P is monotonic increasing, we prove

$$\forall x,y[\ (x < y) \Rightarrow (f_{P'}(x) \leq f_{P'}(y)]\ \ .$$

Note that it is rather hard to express such a property as an input-output relation.

(A) <u>Termination</u>

To show that f_P is total, or in general that $g \sqsubseteq f_P$ for some function g which is total on the desired domain, we cannot simply use computational induction choosing $\varphi(F)$ to be $g \sqsubseteq F$, as then $\varphi(f^0)$ will always be <u>false</u>. However, we can overcome this difficulty by considering the **domain** over which our data range as defined by a recursive program.

For example, the natural numbers can be characterize [*] by the least **fixpoint** <u>num</u>(x) of the recursive program

$$N(x) \Leftarrow \text{if } x = 0 \text{ then true else } N(x-1)\ .$$

We can now translate any program P over the natural numbers into the corresponding recursive program **P'** and show that **P'** terminates by simply proving the relation

---
[*] Given that 0 , 1 , - , + , = have their usual meaning.

$$\forall x[\underline{num}(x) \sqsubseteq \underline{num}(f_{P'}(x))] \quad .$$

In other words, $f_{P'}(x)$ is defined and its value is a natural number, whenever x is a natural number.

(B) Equivalence

It should be quite clear at this point that equivalence of two recursive programs is no more difficult to prove than the other properties. Consider, for example, the two recursive programs over the natural numbers

$$P_7: \quad F(x) <= \underline{if} \ x = 0 \ \underline{then} \ 1 \ \underline{else} \ x \cdot F(x-1) \quad ,$$

and

$$P_8: \quad G(x,y,z) <= \underline{if} \ x \quad y \ \underline{then} \ z \ \underline{else} \ G(x,y+1,(y+1) \cdot z) \quad .$$

We want to show that

$$\forall x[f_{P_7}(x) \equiv g_{P_8}(x,0,1) \ 1 \quad .$$

Note that both $f_{P_7}(x)$ and $g_{P_8}(x,0,1)$ computes x! , but quite differently: $f_{P_7}(x)$ is 'going down' from x to 0 , while $g_{P_8}(x,0,1)$ is 'going up' from 0 to x . This explains why a "direct" computational induction fails in this case.

However, if we consider the predicate x > y over the natural numbers to be characterized by the least fixpoint ge(x,y) of the recursive program

$$M(x,y) <= \underline{if} \ x = y \ \underline{then} \ true \ \underline{else} \ M(x,y+1)) \quad ,$$

we can show by computational induction that

$$\forall x,y[\underline{ge}(x,y) \sqsubseteq [f_{P_7}(x) = g_{P_8}(x,y,f_{P_7}(y))]] \quad .$$

Then, in particular, for y = 0 we get

26

$$\forall x[\underline{ge}(x,0) \sqsubseteq [f_{P_7}(x) = g_{P_8}(x,0,1)]] \quad ,$$

i.e., for every natural number x, either both $f_{P_7}(x)$ and $g_{P_8}(x,0,1)$ are defined and equal, or both are undefined.

The proof is by computational induction with

$$\varphi(F) : \forall x,y[F(x,y) \sqsubseteq [f_{P_7}(x) = g_{P_8}(x,y,f_{P_7}(y))]] \quad .$$

It is clear that $\varphi(f^0)$ holds. So, we assume that $\varphi(f^i)$ holds and show that $\varphi(f^{i+1})$ holds, i.e.,

$$\forall x,y[f^{i+1}(x,y) \sqsubseteq [f_{P_7}(x) = g_{P_8}(x,y,f_{P_7}(y))]] \quad ,$$

or in other words

$$\forall x,y[\text{ [if } x = y \text{ } \underline{\text{then true else }} f^i(x,y+1)) \text{] } \sqsubset [f_{P_7} = g_{P_8}(x,y,f_{P_7}(y))]] \quad .$$

The proof proceeds easily by distinguishing between the two cases where $x = y$ and $x \neq y$.

(a) If $x = y$ we get $\forall x[\underline{\text{true}} \sqsubseteq x f_{P_7}) = f_{P_7}(x)]$, which clearly holds.

(b) If $x \neq y$ we get $\forall x,y[f^i(x,y+1) \sqsubseteq [f_{P_7}(x) = g_{P_8}(x,y,f_{P_7}(y))]]$.

Using the definitions of f_{P_7} and g_{P_8} we get

$$\forall x,y[f^i(x,y+1) \sqsubseteq [f_{P_8}(x) = g_{P_8}(x,y+1,f_{P_7}(y+1))]] \text{ , which holds}$$

by the induction hypothesis.

References

ASHCROFT and MANNA [1971]. E. Ashcroft and Z. Manna, "The Translation of 'Goto' Programs to 'While' Programs", Proceedings of IFIP Congress 1971.

BEKIĆ [1969]. H. Bekić, *'Definable Operations in General Algebra and the Theory of Automata and Flowcharts'% Unpublished memo, IBM, Vienna (December 1969).

BURSTALL [1969]. R. M. Burstall, "Proving Properties of Programs by Structural Induction", Computer Journal, Vol. 12, No. 1 (February 1969), pp. 41-48.

CADIOU [1972]. J. M. Cadiou, "Recursive Definitions of Partial Functions and their Computations", Ph.D. Thesis, Computer Science Dept., Stanford University (to appear).

COOPER [1971]. D. C. Cooper, "Programs for Mechanical Program Verification", in Machine Intelligence 6 (B. Meltzer and D. Michie, Eds.), Edinburgh University Press, pp. 43-59.

DEBAKKER and SCOTT [1969]. J. W. deBakker and D. Scott, "A Theory of Programs", unpublished memo (August 1969).

DIJKSTRA [1968]. E. Dijkstra, "Goto Statements Considered Harmful", CACM, Vol. 11, No. 3 (March 1968), pp. 147-148.

FLOYD [1967]. R. W. Floyd, "Assigning Meanings to Programs', in Proceedings of a Symposium in Applied Mathematics, Vol. 19, Mathematical Aspects of Computer Science (Ed. J. T. Schwartz), pp. 19-32.

HOARE [1969]. C. A. R. Hoare, "An Axiomatic Approach to Computer Programming", CACM, Vol. 12, No. 10 (October 1969), pp. 576-580, 583.

HOARE [1971]. C. A. R. Hoare, "Procedures and Parameters: an Axiomatic Approach", in Symposium on Semantics of Algorithmic Languages, Lecture notes Mathematics, Vol. 188 (E. Engeler, Ed.), Berlin, Springer-Verlag, pp. 102-116

KLEENE [1952]. S. C. Kleene, Introduction to Meta-mathematics, Van Nostrand, Princeton, New Jersey.

KNUTH and FLOYD [1971]. D. E. Knuth and R. W. Floyd, "Notes on Avoiding 'Goto' Statements", Information Processing Letters 1 (January 1971), pp. 23-31.

LANDIN [1964]. P, J. Landin, "The Mechanical Evaluation of Expressions", Computer Journal, Vol. 6, No. 4 (January 1964), pp. 308-320.

MANNA [1969]. Z. Manna, "The Correctness of Programs", JCSS, Vol. 3,
   No. 2 (May 1969), pp. 119-127.

MANNA, NESS, and WILLEMIN [1972]. Z. Manna, S. Ness, and J. Vuillemin,
   "Inductive Methods for Proving Properties of Programs", in
   Proceedings of ACM Conference on Proving Assertions about Programs,
   ACM, New York (January 1972).

MANNA and PNUELI [1970]. Z. Manna and A. Pnueli, "Formalization of
   Properties of Functional Programs", JACM, Vol. 17, No. 3 (July 1970),
   pp. 555-569.

McCARTHY [1963a]. J. McCarthy, "A Basis for a Mathematical Theory of
   Computation". In Computer Programming and Formal Systems,
   (P. Braffort and D. Hirschberg, Eds.), pp. 33-70.

McCARTHY [1963b]. J. McCarthy, "Towards a Mathematical Science of
   Computation", in Information Processing: Proceedings of IFIP 62
   (C. M. Popplewell, Ed.), Amsterdam, North Holland, pp. 21-28.

MILNER [1972]. R. Milner, "Implementation and Applications of Scott's
   Logic for Computable Functions", in Proceedings of ACM Conference
   on Proving Assertions about Programs, ACM, New York (January 1972).

MORRIS [1968]. J. H. Morris, "Lambda-Calculus Models of Programming
   Languages", Ph.D. Thesis, Project MAC, M.I.T., MAC-TR-57 (December 1968).

MORRIS [1971]. J. H. Morris, "Another Recursion Induction Principle",
   CACM, Vol. 14, No. 5 (May 1971), pp. 351-354.

NAUR [1966]. P. Naur, "Proof of Algorithms by General Snaptshots",
   BIT, vol. 6 (1966), pp. 310-316.

PARK [1969]. D. Park, "Fixpoint Induction and Proofs of Program Properties",
   in Machine Intelligence 5 (B. Meltzer and D. Michie, Eds.), Edinburgh
   University Press, pp. 59-78.

SCOTT [1970]. D. Scott, "Outline of a Mathematical Theory of Computation",
   Oxford University Computing Lab., Programming Research Group,
   Technical Monograph PRG-2 (November 1970).

SCOTT and STRACHEY [1971]. D. Scott and C. Strachey, "Towards a Mathematical
   Semantics for Computer Languages", Technical Monograph PRC-6,
   Oxford University (August 1971).

STRACHEY [1966]. C. Strachey, "Towards a Formal Semantics", in Formal
   Languages Description Languages, (T. B. Steel, Ed.), Proc. IFIP
   Working Conf. 1964, Amsterdam, North-Holland, pp. 198-220.

WILLEMIN [1972]. J. Vuillemin, "Proof Techniques for Recursive Programs",
   Ph.D. Thesis, Computer Science Dept., Stanford University (to appear).

WEYHRAUCH and MILNER [1972]. R. Weyhrauch and R. Milner, "Program
   Semantics and Correctness in a Mechanized Logic", The USA-Japan
   Computer Conference, Tokyo (October 1972).