stichting
mathematisch
centrum

MC

AFDELING INFORMATICA
(DEPARTMENT OF COMPUTER SCIENCE)

IW 236/83 SEPTEMBER

J.A. BERGSTRA & J.V. TUCKER

THE AXIOMATIC SEMANTICS OF PROGRAMS BASED ON HOARE'S LOGIC

Preprint

kruislaan 413 1098 SJ amsterdam

Printed at the Mathematical Centre, Kruislaan 413, Amsterdam, The Netherlands.

The Mathematical Centre, founded 11 February 1946, is a non-profit institution for the promotion of pure and applied mathematics and computer science. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

69F31, 69D24

1980 Mathematics subject classification: 035D35, 03D75, 68D10

1982 CR. Categories: D.2.4., F.3.1.

Copyright © 1983, Mathematisch Centrum, Amsterdam

The axiomatic semantics of programs based on Hoare's logic*

by

J.A. Bergstra & J.V. Tucker**

ABSTRACT

This paper is about the Floyd-Hoare Principle which says that the semantics of a programming language can be formally specified by axioms and rules of inference for proving the correctness of programs written in the language. We study the simple language WP of while-programs and Hoare's system for partial correctness and we *calculate* the semantics of WP as this is determined by Hoare's logic. This calculation is possible by using relational semantics to build a completeness theorem for the logic. The resulting semantics AX we call the *axiomatic semantics* for WP. This AX is *not* the conventional semantics for WP : it need not be effectively computable or deterministic, for example. A large number of elegant properties of AS are proved and the Floyd-Hoare Principle is reconsidered.

KEY WORDS & PHRASES : *Programming language definition; program specification; program verification; Hoare's logic; non-deterministic semantics*

---

* This report is not for review as it will be published elsewhere.

** Department of Computer Studies, University of Leeds, Leeds, LS2 9JT, United Kingdom.

BIBLIOTHEEK MATHEMATISCH CENTRUM
——AMSTERDAM——

INTRODUCTION

BACKGROUND The idea that a programming language L can be defined by the axioms and rules of inference involved in proving properties of programs written in L originates in R.W. FLOYD [19] and C.A.R. HOARE [32]. The beauty, and utility, of this *Floyd-Hoare Principle* are derived from the observation that, on taking a formal axiomatic system to be the ultimate source for the specification of language behaviour, the system provides

(1) formal criteria for the correctness of implementations of the language L; and

(2) a set of properties for each program S of L which may be formally verified and, if verified, apply in all implementations of the language L.

The application of the Floyd-Hoare Principle to the language L is commonly described as defining L by means of *axiomatic semantics*.

Among early and significant writings on the axiomatic method of language specification are HOARE [23], HOARE & LAUER [24], LAUER [27], MANNA [29], DIJKSTRA [17,18]. In particular, in HOARE & WIRTH [25] there is an axiomatic semantics for a part of Pascal. Subsequently, axiomatic semantics have been invented for older languages, such as Algol 68 (SCHWARTZ [36]), and have been used in the design of new languages, such as Euclid (LONDON [28]). Popular and useful introductory accounts of axiomatic semantics are included in MC GETTRICK [31] and PAGAN [34].

OBJECTIVE In this paper we present a thorough theoretical analysis of the Floyd-Hoare Principle in the original setting of HOARE [22]. We consider the simple language WP of *while*-programs and the axiomatic system now known as *Hoare's logic* which proves input-output specifications of the form {p}S{q}, where p and q are first-order statements and S is a program. *Without any preconceived idea as to the semantics of* WP, *we carefully calculate the semantics of* WP *when all that is known about* while*-program computation is what can be proved in Hoare's logic.* Such a calculation is possible using the general framework of relational semantics for programs and the following idea about completeness theorems in logic :

COMPLETENESS PRINCIPLE *Let L be a formal logical system analysing a property P. A completeness theorem for L with respect to a formal semantics S for P is a statement confirming that semantics S characterises the property P, as P is determined by L.*

Thus, we will construct a relational semantics AX for WP based on Hoare's logic and prove that Hoare's logic is complete with respect to partial correctness under the semantics AX; this confirms that AX characterises the meaning of WP as far as Hoare's logic is concerned. Then we will study AX in detail and catalogue some of its intriguing properties; for example, AX is not a conventional semantics of WP for it is not computable and not deterministic! In consequence, the Floyd-Hoare Principle does not accomplish the task of defining this programming language in a natural way, as originally intended. We reconsider the Floyd-Hoare Principle in the wake of our results in Section 9.

OVERVIEW It will be helpful if we prolong this introduction by summarising what we do in the paper. First, here are some words about Hoare's logic :

Hoare's logic consists of axioms and rules for manipulating specified programs $\{p\}S\{q\}$; and a first-order axiomatic specification (Σ,T) for the data types on which the programs compute. Each structure A of signature Σ that is a model of (Σ,T) represents an implementation of (Σ,T). The data type specification (Σ,T) and the specified programs $\{p\}S\{q\}$ cooperate in the logic via the Rule of Consequence which is applied to first-order statements provable from T. The set of all specified programs provable in Hoare's logic we denote $HL(\Sigma,T)$. This essential material, including many derived rules and metamathematical results for the system, is documented in Sections 1 and 2.

In Section 3, we define a relational semantics $AX(\Sigma,T)$ for WP based on $HL(\Sigma,T)$ and we refer to it as the *axiomatic semantics of* WP. This axiomatic semantics determines a new partial correctness semantics for specified programs. In Section 4, we prove :

COMPLETENESS THEOREM *Let (Σ,T) be any first-order data type specification. Let $\{p\}S\{q\}$ be any first-order specified program. Then*

$$HL(\Sigma,T) \vdash \{p\}S\{q\} \text{ if, and only if, } AX(\Sigma,T) \models \{p\}S\{q\}$$

The proof of this theorem is relatively complicated and we give it in detail because *the semantical definition of* AX(Σ,T) *and the demonstration of completeness may be generalised to any logical system for partial correctness for any programming language, provided the system satisfies the generalised derived rules and metamathematical statements involved in the proof.*

Such a completeness theorem is impossible using the standard partial correctness semantics based on, say, the operational semantics OP(Σ,T) of WP : see [7].

We study computation on a single structure A using the axiomatic semantics AX(A) of the Hoare's logic HL(A) made by allowing the set Th(A) of all true first-order statements about A as data type specification. Of especial interest is the relationship between AX(A) and the standard semantics of WP on A. Among the many results of Sections 5 and 6 are :

THEOREM *The operational semantics* OP(A) *of* WP *on* A *is faithfully embedded in the axiomatic semantics* AX(A).

If the first-order assertion language is expressive for WP *with respect to its operational semantics* OP(A) *on* A *then* OP(A)=AX(A). *In particular, for the standard model of arithmetic* $\mathbb{N}$, OP($\mathbb{N}$) = AX($\mathbb{N}$).

THEOREM *For any program* S *of WP the operational semantics* OP(A)(S) *of* S *on* A *is recursively enumerable in* Th(A) *while the axiomatic semantics* AX(A)(S) *of* S *on* A *is co-recursively enumerable in* Th(A).

There is a program S *of* WP *on Presburger Arithmetic* P *such that* OP(P)(S) $\subsetneq$ AX(P)(S).

In Section 7, we consider the completeness of HL(A) with respect to AX(A) in greater detail. And in Section 8 we construct a structure A and a program S such that AX(A)(S) is nondeterministic. We conclude the paper with further discussion of the project in Section 9.

PREREQUISITES Our interest in axiomatic semantics began with our [6] written in collaboration with J. Tiuryn (see also A.R. MEYER & J.Y. HALPERN [32,33]). However, this paper owes more to our series of articles on the role of the data type specification in Hoare's logic [7-13]. There we found a paucity of significant completeness theorems for the logic which is the

clue to the present project : it is a consequence of the Completeness Principle that *if a logical system is not complete for a semantics then the system is not talking about that semantics*. These issues are discussed in detail in [10]. In addition to HOARE [22], the reader must be familiar with the basic results of COOK [14], for which APT[1] may be consulted. To master all the arguments that follow acquaintence with the entire series [7-13] is recommended, and may be necessary.

ACKNOWLEDGEMENT We are grateful to Peter Lauer for his encouraging reception and detailed criticism of a first draft of this paper. And we thank Ms. Judith Thursby for typing this manuscript.

1. SPECIFICATIONS AND PROGRAMS

1.1 SYNTAX The first-order language $L(\Sigma)$ of some signature Σ is based upon a set Var of variables $x_1, x_2, \ldots$ and its constant, function and relational symbols are those of Σ, together with the equality relation. We assume $L(\Sigma)$ possesses the usual logical connectives and quantifiers; and the set of algebraic expressions of terms over Σ we denote $T(\Sigma)$.

If T is a set of assertions of $L(\Sigma)$ and $p \in L(\Sigma)$ is formally provable from T then we write $T \vdash p$. Such a set T of formulae is usually called a theory over Σ, but more appropriate for our purposes is to call the pair (Σ, T) a *first-order data type specification.*

Using the syntax of $L(\Sigma)$, the set $WP(\Sigma)$ of all while-programs over Σ is defined in the customary way.

By a *specified* or *asserted program* we mean a triple of the form $\{p\}S\{q\}$ where $S \in WP(\Sigma)$ and $p, q \in L(\Sigma)$.

Thus, here first-order languages are used as program specification languages and data type specification languages.

1.2 SPECIFICATION SEMANTICS The semantics of $L(\Sigma)$ is the standard satisfaction semantics of model theory. A *state* over a structure A is a map

$$\sigma : \text{Var} \to A$$

assigning a value $\sigma(x)$ in A to each and every variable x of $L(\Sigma)$; let State(A) denote the set of all states over A. The validity of $p \in L(\Sigma)$ at a state σ we write $A \models p(\sigma)$; and if $A \models p(\sigma)$ for every state $\sigma \in \text{State}(A)$ then we write $A \models p$. The set of all sentences of $L(\Sigma)$ which are valid in A is called the first-order theory of A and is denoted Th(A).

The class of all models of a specification (Σ, T) is denoted $\text{Mod}(\Sigma, T)$. If $p \in L(\Sigma)$ and $A \models p$ for each $A \in \text{Mod}(\Sigma, T)$ then we write $\text{Mod}(\Sigma, T) \models p$. According to our Completeness Principle in the Introduction the semantics of the first-order data type specification (Σ, T) is $\text{Mod}(\Sigma, T)$:

1.3 GÖDEL COMPLETENESS THEOREM. *Let* (Σ, T) *be a specification. For each* $p \in L(\Sigma)$,

$$T \vdash p \quad \textit{if, and only if,} \quad \text{Mod}(\Sigma, T) \models p$$

Of course, the Completeness Principle was first understood in the contrasting of Theorem 1.3 with the Gödel Incompleteness Theorem.

1.4 PROGRAM SEMANTICS Since the purpose of this paper is to investigate a new and non-standard semantics for WP(Σ) it is wise to comment on the familiar and standard semantics for WP(Σ). For the semantics of WP(Σ) on a structure A the reader is free to choose any "conventional" account of while-program computation to make comparisons with the new axiomatic semantics. Informally, of course, we expect all semantics for WP(Σ) defined elsewhere, in normal circumstances, to be essentially equivalent.

However, since there is, as yet, no single framework for studying semantics in an unified way, there is no formal and general criterion for the equivalence or isomorphism of any two semantic definitions of program behaviour. In consequence, there is no way of refining the idea of a "conventional" semantics for while-programs by means of a formal definition that identifies the standard semantics uniquely up to isomorphism. A notable attempt at the problem of *rigorously* comparing the disparate methods of defining the semantics of while-programs is made in I.GREIF and A.R. MEYER [21].

Among the existing treatments of while-programs, our preference is the operational semantics defined in DE BAKKER [5], generalised from the natural numbers $\mathbb{N}$ to an abstract structure A. The meaning of $S \in WP(\Sigma)$ on A is defined, by induction on the structure of S, to be a *state transformation map*

$$O_A(S) : State(A) \to State(A) .$$

The map $O_A(S)$ is a partial function and we write $O_A(S)(\sigma)\downarrow\tau$, if $O_A(S)(\sigma)$ is defined and has the value τ, and $O_A(S)(\sigma)\uparrow$ if $O_A(S)(\sigma)$ is not defined. Let us note that if S has n variables then, for the purpose of analysing S, we may faithfully represent State(A) by A^n and faithfully represent $O_A(A)$ by a map

$$\hat{O}_A(S) : A^n \to A^n$$

in an obvious way.

1.5 PARTIAL CORRECTNESS Putting together the semantics of L(Σ) and WP(Σ), we define the (*standard*) *partial correctness semantics* of the specified programs : the specified program $\{p\}S\{q\}$ is *valid* on A, written $A \models \{p\}S\{q\}$, if for each initial state $\sigma \in State(A)$, $A \models p(\sigma)$ implies either $O_A(S)(\sigma)\downarrow\tau$ and $A \models q(\tau)$ or $O_A(S)(\sigma)\uparrow$. In particular, if $A \models \{p\}S\{q\}$ then we

say that S is *partially correct with respect to the precondition* p *and postcondition* q *under its standard operational semantics*. The specified program {p}S{q} is *valid* for the data type specification (Σ,T) if $A\models\{p\}S\{q\}$ for each $A\in Mod(\Sigma,T)$; in symbols, $Mod(\Sigma,T)\models\{p\}S\{q\}$.

We define the (*standard*) *partial correctness theory of a structure* A as the set

$$PC(A) = \{\{p\}S\{q\} \ : \ A\models\{p\}S\{q\}\}$$

and the (*standard*) *partial correctness theory of a specification* (Σ,T) as the set

$$PC(\Sigma,T) = \{\{p\}S\{q\} \ : \ Mod(\Sigma,T)\models\{p\}S\{q\}\}$$

1.6 COMPUTABILITY Foremost among the properties common to the several "conventional" semantics for while-programs is the property that while-programs can compute all and only partial recursive functions on the standard model of arithmetic

$$\mathbb{N} = (\{0,1,\ldots\} : 0,\ x+1, x+y, x\times y) \ .$$

In particular, with reference to our operational semantics, we note that the representation

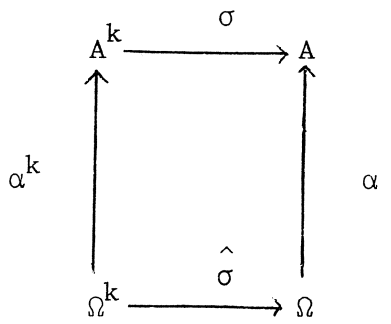
$$\hat{O}_{\mathbb{N}}(S) : \mathbb{N}^n \to \mathbb{N}^n$$

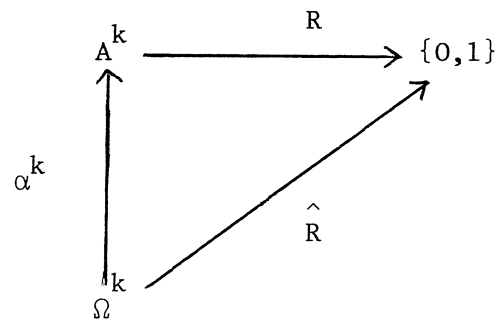
is partial recursive for every $S\in WP(\Sigma_{\mathbb{N}})$. These remarks are true of the simpler structure Presburger Arithmetic

$$P = (\{0,1,\ldots\} : 0,\ x+1).$$

Later, in Section 6, we will contrast these familiar results with theorems about the effective computabiltiy of the axiomatic semantics and thereby show that the semantics is indeed nonstandard. We consider computability issues in a general setting using the ideas of RABIN [35] and MAL'CEV [30].

A structure A has an *effective enumeration* when there is a recursive set Ω of natural numbers and a surjection $\alpha : \Omega \to A$ such that for each k-ary operation σ and k-ary relation R of A there exist recursive functions $\hat{o}$ and $\hat{R}$ which commute the following diagrams :





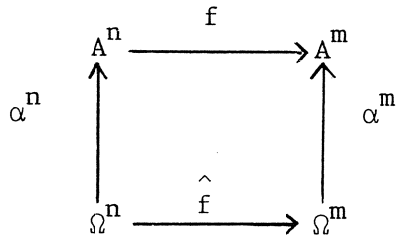
wherein $\alpha^k(n_1,\ldots,n_k) = (\alpha n_1,\ldots,\alpha n_k)$ and R is identified with its characteristic function.

A structure A is *computable* when there is an effective enumeration α such that the relation $\equiv_\alpha$ defined by

$$n \equiv_\alpha m \quad \text{if, and only if, } \alpha n = \alpha m \text{ in A}$$

is recursive.

Let A be a structure computable under enumeration α. Then the partial function $f : A^n \to A^m$ is *computable under* α if there is a partial recursive function $\hat{f} : \Omega^n \to \Omega^m$ that commutes the following diagram :



With these concepts we may formulate a partial generalisation of our opening remarks.

1.7 LEMMA *Let A be a computable structure with signature* Σ. *Then for every* $S \in WP(\Sigma)$ *the partial function*

$$\hat{O}_A(S) : A^n \to A^n$$

is computable.

Thus, while-programs equipped with their standard semantics define computable partial functions on a computable structure. However, in general, not every computable function on a computable structure is definable by a while-program. This is because one can computably search all of a computable structure A via its enumeration, but the possibility that a while-program can search A depends on the constants named in the signature of A.

2. HOARE'S LOGIC

Hoare's logic for $WP(\Sigma)$ with data type specification (Σ,T) and assertion language $L(\Sigma)$ has the following axioms and proof rules for proving specified programs : let $S,S_1,S_2 \in WP(\Sigma)$; $p,q,p_1,q_1,r \in L(\Sigma)$; $b \in L(\Sigma)$, a quantifier-free formula.

Assignment axiom scheme : For $e \in T(\Sigma)$ and $x \in Var$ and $p \in L(\Sigma)$ the specified program

$$\{p[e/x]\}\ x := e\{p\}$$

is an axiom, where $p[e/x]$ stands for the result of substituting e for free occurrences of x in p.

Composition rule :

$$\frac{\{p\}S_1\{r\}\ ,\ \{r\}S_2\{q\}}{\{p\}S_1;S_2\ \{q\}}$$

Conditional rule :

$$\frac{\{p \wedge b\}S_1\{q\}\ ,\ \{p \wedge \neg b\}S_2\{q\}}{\{p\}\ \underline{\text{if}}\ b\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2\ \underline{\text{fi}}\ \{q\}}$$

Iteration rule :

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

Consequence rule :

$$\frac{p \rightarrow p_1,\ \{p_1\}S\{q_1\},\ q_1 \rightarrow q}{\{p\}\ S\ \{q\}}$$

Specification axiom scheme : Each $p \in L(\Sigma)$ such that $T \vdash p$ is an axiom.

The set of specified programs derivable from these axioms by the proof rules we denote $HL(\Sigma,T)$ and we write $HL(\Sigma,T) \vdash \{p\}S\{q\}$ in place of $\{p\}S\{q\} \in HL(\Sigma,T)$.

In the thorough examination of this system that follows we will employ a number of simple derived rules and proof-theoretic results; most of these we have established in our series [7-13] and are recalled here; first the derived rules :

2.1 DISJUNCTION RULE $$\frac{\{p\}S\{q\} \ , \ \{r\}S\{t\}}{\{p \vee r\}S\{q \vee t\}}$$

2.2 CONJUNCTION RULE $$\frac{\{p\}S\{q\} \ , \ \{r\}S\{t\}}{\{p \wedge r\}S\{q \wedge t\}}$$

2.3 INVARIANT RULE *If* S *and* p *have no free variables in common then*

$$HL(\Sigma,T) \vdash \{p\}S\{p\}$$

2.4 $\forall$-RULE *If* x *is not a free variable of* S *or* p *then*

$$\frac{\{p\}S\{q\}}{\{p\}S\{\forall x q\}}$$

2.5 $\exists$-RULE *If* x *is not a free variable of* S *or* q *then*

$$\frac{\{p\}S\{q\}}{\{\exists x \, p\}S\{q\}}$$

Next we record the following metamathematical results taken from [8,9].

2.6 FINITENESS LEMMA *If* $HL(\Sigma,T) \vdash \{p\}S\{q\}$ *then for some closed* $\phi \in L(\Sigma)$ *we have*

$$T \vdash \phi \quad \textit{and} \quad HL(\Sigma,\{\phi\}) \vdash \{p\}S\{q\}.$$

2.7 DEDUCTION LEMMA *Let* $\phi \in L(\Sigma)$ *be closed and suppose that*

$$HL(\Sigma, T \cup \{\phi\}) \vdash \{p\}S\{q\}$$

then

$$HL(\Sigma,T) \vdash \{\phi \wedge p\}S\{q\}$$

2.8 CONSTANTS LEMMA *Let* $\Sigma_c = \Sigma \cup \{c\}$ *where* c *is a new constant symbol and suppose that*

$$HL(\Sigma_c,T) \vdash \{p\}S\{q\}$$

where $T \subset L(\Sigma)$ *and* $p,q \in L(\Sigma_c)$. *Then for any variable* x *not in* S, p *or* q

$$HL(\Sigma,T) \vdash \{p[x/c]\}S\{q[x/c]\}.$$

In addition, we recall the basic results of COOK [14] about the soundness and completeness of Hoare's logic with respect to its standard semantics :

2.9 SOUNDNESS THEOREM $HL(\Sigma,T) \subset PC(\Sigma,T)$

A specification (Σ,T) is *complete* if for any sentence $p \in L(\Sigma)$ either $T \vdash p$ or $T \vdash \neg p$. For any structure A, Th(A) is complete.

The assertion language $L(\Sigma)$ is *expressive* for $WP(\Sigma)$ on Σ-structure A if for every $p \in L(\Sigma)$ and every $S \in WP(\Sigma)$ the strongest postcondition

$$sp_A(p,S) = \{\sigma \in State(A) : \exists \tau [Q_A(S)(\tau) \downarrow \sigma \ \& \ A \models p(\tau)]\}$$

is definable by a formula of $L(\Sigma)$.

2.10 COOK'S COMPLETENESS THEOREM *Let* (Σ,T) *be a complete specification and let* $A \in Mod(\Sigma,T)$. *If* $L(\Sigma)$ *is expressive for* $WP(\Sigma)$ *on* A *then*

$$HL(\Sigma,T) = PC(A)$$

Observe that $HL(A) = HL(\Sigma,Th(A))$ is the strongest Hoare logic for analysing program correctness on A because it is equipped with all first-order facts about A; and HL(A) is complete whenever $L(\Sigma)$ is expressive.

2.11 COROLLARY *For the standard model of arithmetic* $\mathbb{N}$

$$HL(\mathbb{N}) = PC(\mathbb{N})$$

We conclude with a fact from [7] we will use in Section 5.

2.12 LEMMA *Let* A *be any structure of signature* Σ *and let* ϕ *and* ψ *be any state formulae of the form*

$$\phi(x) \equiv \bigwedge_{i=1}^{n} x_i = t_i \quad \text{and} \quad \psi(x) \equiv x_i = r_i$$

where $x_i \in Var$ *and* $t_i, r_i \in T(\Sigma)$. *Let* $S \in WP(\Sigma)$ *have the same variables* $x = (x_1,\ldots,x_n)$. *If* $A \models \phi(\sigma)$ *implies* $OP(A)(S)(\sigma)\downarrow$, *and* $OP(A) \models \{\phi\}S\{\psi\}$, *then* $HL(A) \vdash \{\phi\}S\{\psi\}$.

3. AXIOMATIC SEMANTICS

Using Hoare's logic $HL(\Sigma,T)$ for the data type specification (Σ,T) we will define a semantics $AX(\Sigma,T)$ for $WP(\Sigma)$ over the class $Mod(\Sigma,T)$ of implementations of (Σ,T). Before defining this axiomatic semantics we describe a general scheme for formulating a relational semantics over any class of interpretations.

3.1 PROGRAM SEMANTICS FOR A CLASS Let K be a class of structures of signature Σ. A *relational semantics* M_K for the set $WP(\Sigma)$ over K is a family

$$M_K = \{M_A : A \in K\}$$

wherein each M_A is a mapping which assigns to each $S \in WP(\Sigma)$ a relation

$$M_A(S) \subset State(A) \times State(A).$$

3.2 PARTIAL CORRECTNESS Let $M_K = \{M_A : A \in K\}$ be a relational semantics over a class K. A specified program $\{p\}S\{q\}$ is *partially correct on* A *with respect to* M_A if for each $(\sigma,\tau) \in M_A(S)$, $A \models p(\sigma)$ implies $A \models q(\tau)$; and we write $M_A \models \{p\}S\{q\}$ in such circumstances. Furthermore, the specified program $\{p\}S\{q\}$ is *partially correct over* K *with respect to* M_K if it is partially correct on A with respect to M_A for each $A \in K$; and we write $M_K \models \{p\}S\{q\}$ in such circumstances. Thus :

$$M_K \models \{p\}S\{q\} \text{ if and only if for each } A \in K,\ M_A \models \{p\}S\{q\}.$$

3.3 CORRECTNESS THEORIES The *partial correctness theory* of $WP(\Sigma)$ on A with respect to M_A is the set

$$PC(M_A) = \{\{p\}S\{q\} : M_A \models \{p\}S\{q\}\}$$

The partial correctness theory of $WP(\Sigma)$ over K with respect to M_K is the set

$$PC(M_K) = \{\{p\}S\{q\} : M_K \models \{p\}S\{q\}\}$$

Clearly

$$PC(M_K) = \bigcap_{A \in K} PC(M_A)$$

3.4 OPERATIONAL SEMANTICS Recalling 1.4, we redefine the operational semantics of $WP(\Sigma)$ and a class K to be the family

$$OP(K) = \{OP(A) : A \in K\}$$

wherein for $S \in WP(\Sigma)$

$$(\sigma,\tau) \in OP(A)(S) \text{ if and only if } O_A(S)(\sigma) \downarrow \tau$$

Thus, the notations

$$A \models \{p\}S\{q\} \text{ and } OP(A) \models \{p\}S\{q\}$$
$$K \models \{p\}S\{q\} \text{ and } OP(K) \models \{p\}S\{q\}$$

are equivalent; and

$$PC(A) = PC(OP(A)) \text{ and } PC(K) = PC(OP(K))$$

3.5 AXIOMATIC SEMANTICS Let (Σ,T) be a data type specification. The axiomatic semantics of $WP(\Sigma)$ over $Mod(\Sigma,T)$ determined by $HL(\Sigma,T)$ is the family

$$AX(\Sigma,T) = \{AX(\Sigma,T)_A : A \in Mod(\Sigma,T)\}$$

wherein the meaning function $AX(\Sigma,T)_A$ assigns to each $S \in WP(\Sigma)$ the relation

$$AX(\Sigma,T)_A(S) = \{(\sigma,\tau) \in State(A) \times State(A) : \text{for any } p,q \in L(\Sigma),$$
$$\text{if } HL(\Sigma,T) \vdash \{p\}S\{q\} \text{ then } A \models p(\sigma) \text{ implies } A \models q(\tau)\}.$$

Thus, informally, we say that $(\sigma,\tau) \in AX(\Sigma,T)_A(S)$ *if and only if the input state* σ *and output state* τ *are* consistent *with every provably correct specification of the program* S *given the data type axiomatisation* (Σ,T) *for* A.

Applying the notations of Definitions 3.2 and 3.3 we write :

$AX(\Sigma,T) \models \{p\}S\{q\}$ if, and only if, for each $A \in K$, $AX(\Sigma,T)_A \models \{p\}S\{q\}$;

and

$$PC(AX(\Sigma,T)) = \cap\{PC(AX(\Sigma,T)_A) : A \in Mod(\Sigma,T)\}.$$

For the remainder of this section we examine the axiomatic semantics on a single interpretation A.

To compute on the structure A using <u>while</u>-programs under axiomatic semantics it is necessary to choose a data type specification (Σ,T) for A and then apply $AX(\Sigma,T)_A$ as described in Definition 3.5. It *appears* that the axiomatic semantics of $WP(\Sigma)$ on A is not uniquely determined by A (as is the case for operational semantics, of course), but that the axiomatic semantics depends on A and (Σ,T) : *Can different data type specifications allow different relations to be computed?* We show that the answer to this question is : No.

Consider the complete first-order specification of the structure A, namely the full first-order theory Th(A) of A. Recall from Section 2,

$$HL(A) = HL(\Sigma,Th(A))$$

which maximises the set of provable information about <u>while</u>-program behaviour obtainable from Hoare's proof system.

<u>3.6 DEFINITION</u> The *full axiomatic semantics* of $WP(\Sigma)$ on A is $AX(A)=AX(\Sigma,Th(A))_A$. Thus, for $S \in WP(\Sigma)$,

$$AX(A)(S) = \{(\sigma,\tau) : \text{for all } p,q \in L(\Sigma) \text{ if } HL(A) \vdash \{p\}S\{q\} \text{ then } A \models p(\sigma)$$
$$\text{implies } A \models q(\sigma)\}.$$

<u>3.7 UNIQUENESS THEOREM</u> *Let* (Σ,T) *be a specification. For each* $S \in WP(\Sigma)$ *and* $A \in Mod(\Sigma,T)$ *it is the case that*

$$AX(\Sigma,T)_A(S) = AX(A)(S) .$$

PROOF First, we show that $AX(A)(S) \subset AX(\Sigma,T)_A(S)$; this is straight-forward. Let $(\sigma,\tau) \in AX(A)(S)$ and suppose that for every $p,q \in L(\Sigma)$, $HL(\Sigma,T) \vdash \{p\}S\{q\}$. Then, trivially, $HL(A) \vdash \{p\}S\{q\}$ for every $p,q \in L(\Sigma)$. Since $(\sigma,\tau) \in AX(A)(S)$ by assumption, we know that $A \models p(\sigma)$ implies $A \models q(\tau)$. We have deduced that $(\sigma,\tau) \in AX(\Sigma,T)(S)$.

Consider now the converse : let $(\sigma,\tau) \in AX(\Sigma,T)(S)$ and suppose that for every $p,q \in L(\Sigma)$, $HL(A) \vdash \{p\}S\{q\}$; we must prove that $A \models p(\sigma)$ implies $A \models q(\tau)$.

By the Finiteness Lemma 2.6, there is a closed first-order assertion $\phi \in L(\Sigma)$ such that $A \models \phi$ and

$$HL(\Sigma,T \cup \{\phi\}) \vdash \{p\}S\{q\}.$$

By the Deduction Lemma 2.7,

$$HL(\Sigma,T) \vdash \{p \wedge \phi\}S\{q\}$$

Since $(\sigma,\tau) \in AX(\Sigma,T)_A(S)$ we may deduce that

$$A \models (p \wedge \phi)(\sigma) \text{ implies } A \models q(\tau)$$

and because $A \models \phi$ we know that

$$A \models p(\sigma) \text{ implies } A \models q(\tau). \qquad \square$$

Thus, *the axiomatic semantics of* $WP(\Sigma)$ *on a structure* A *defined by* $HL(\Sigma,T)$ *is independent of the data type specification* (Σ,T) *for* A. And the importance of $AX(A)$ is assured by the following observation :

3.8 COROLLARY *Let* (Σ,T) *be a specification. Let* $S \in WP(\Sigma)$ *and* $p,q \in L(\Sigma)$. *For each* $A \in Mod(\Sigma,T)$

$$AX(\Sigma,T)_A \models \{p\}S\{q\} \text{ } \textit{if, and only if,} \text{ } AX(A) \models \{p\}S\{q\}.$$

Furthermore:

$AX(\Sigma,T) \models \{p\}S\{q\}$ *if, and only if, for each* $A \in Mod(\Sigma,T)$, $AX(A) \models \{p\}S\{q\}$.

Finally, we record a technical fact of use in the next section.

Let B be an expansion of a structure A of signature Σ, namely B is A augmented with new constants, operations and relations and so $A = B|_\Sigma$.

3.9 LEMMA *If* B *is an expansion of* A *then for every* $S \in WP(\Sigma)$

$$AX(B)(S) \subset AX(A)(S)$$

and this entails that

$$AX(A) \models \{p\}S\{q\} \text{ } \textit{implies} \text{ } AX(B) \models \{p\}S\{q\}$$

for every $p,q \in L(\Sigma)$.

4. SOUNDNESS AND COMPLETENESS OF HOARE'S LOGIC

We will now prove that Hoare's logic is sound and complete with respect to the axiomatic semantics of Definition 3.5 :

4.1 THEOREM *Let* (Σ,T) *be a data type specification. For each program* $S\in WP(\Sigma)$ *and any assertions* $p,q\in L(\Sigma)$,

$$HL(\Sigma,T)\vdash\{p\}S\{q\} \quad \textit{if, and only if,} \quad AX(\Sigma,T)\models\{p\}S\{q\}.$$

Using the Completeness Principle, we interpret the theorem as a statement that *confirms* that the formulae of Definition 3.5 define the semantics of while-programs according to Hoare's logic. The proof of the soundness of $HL(\Sigma,T)$ with respect to $AX(\Sigma,T)$ is trivial, but completeness requires a longish proof which uses some standard techniques of first-order logic and information about $HL(\Sigma,T)$.

PROOF First, we consider soundness : suppose that $HL(\Sigma,T)\vdash\{p\}S\{q\}$. Let $A\in Mod(\Sigma,T)$ and let $(\sigma,\tau)\in AX(\Sigma,T)_A(S)$; we must show that $A\models p(\sigma)$ implies $A\models q(\tau)$. Now this follows immediately from the definition of $AX(\Sigma,T)_A(S)$ and our assumption that $HL(\Sigma,T)\vdash\{p\}S\{q\}$.

For completeness we assume, contrapositvely, that $HL(\Sigma,T)\nvdash\{p\}S\{q\}$ and show that $AX(\Sigma,T)\not\models\{p\}S\{q\}$; the latter means that there exists $A\in Mod(\Sigma,T)$ and $(\sigma,\tau)\in AX(\Sigma,T)_A(S)$ for which $A\models p(\sigma)$ does *not* imply $A\models q(\tau)$. The construction of this interpretation A and input-output pair (σ,τ) is a lengthy exercise in logic and is organised by Lemmas 4.2 and 4.3 below.

Let $x=x_1,\ldots,x_k$ be a list of all free variables in p,q and all variables of S. We choose a list $c=c_1,\ldots,c_k$ of new constant symbols and add it to Σ to make $\Sigma_c=\Sigma\cup\{c_1,\ldots,c_k\}$. Let p(c) be the sentence of $L(\Sigma_c)$ obtained by substituting each c_i for x_i in p $(1\le i\le k)$; and set $T_p=T\cup\{p(c)\}$. A structure $A_o\in Mod(\Sigma_c,T_p)$ consists of a structure $A\in Mod(\Sigma,T)$ augmented by an input $a=a_1,\ldots,a_k\in A$ that satisfies p. We write $A_o=(A,a)$ and $A=A_o|_\Sigma$ in conventional reduct notation. Notice that $State(A)=State(A_o)$.

Let x=c abbreviate $\bigwedge_{i=1}^{k} x_i=c_i$.

4.2 LEMMA $HL(\Sigma_c,T_p)\nvdash\{x=c\}S\{q\}$.

4.3 LEMMA *There is* $A_o\in Mod(\Sigma_c,T_p)$ *such that* $AX(A_o)\not\models\{x=c\}S\{q\}$.

Using these lemmas we can finish the proof of Theorem 4.1 as follows :

Let A be the Σ-reduct $A_o|_\Sigma$ so that $A \in Mod(\Sigma,T)$. By Corollary 3.8, to show that $AX(\Sigma,T) \not\models \{p\}S\{q\}$ it is sufficient to show that $AX(A) \not\models \{p\}S\{q\}$.

By the description of A_o in Lemma 4.3, there exists $(\sigma,\tau) \in AX(A_o)(S)$ such that $A_o \models [x=c](\sigma)$ but $A_o \not\models q(\tau)$. Since $A_o \models p(c)$ we deduce that $A_o \models p(\sigma)$ and because $p \in L(\Sigma)$ this implies that $A \models p(\sigma)$. In addition, we note that $A_o \not\models q(\tau)$ implies that $A \not\models q(\tau)$ because $q \in L(\Sigma)$. Hence, we have demonstrated that :

$$A \models p(\sigma) \quad \text{does not imply } A \models q(\tau).$$

It remains to remark that $(\sigma,\tau) \in AX(A)(S)$ by Lemma 3.9 and hence that $\{p\}S\{q\}$ is not partially correct with respect to $AX(A)$.

PROOF OF LEMMA 4.2

Suppose for a contradiction that $HL(\Sigma_c,T_p) \vdash \{x=c\}S\{q\}$. By the Deduction Lemma 2.7,

$$HL(\Sigma_c,T) \vdash \{x=c \wedge p(c)\}S\{q\}$$

By Lemma 2.8, we may replace the constants $c=c_1,\ldots,c_k$ by new variables $y=y_1,\ldots,y_k$ not in p,q or S and obtain

$$HL(\Sigma,T) \vdash \{x=y \wedge p(y)\}S\{q\}.$$

By the $\exists$-Rule 2.4,

$$HL(\Sigma,T) \vdash \{\exists y(x=y \wedge p(y))\}S\{\exists y.q\}.$$

Applying the Rule of Consequence on this specified program using

$$T \vdash p(x) \to \exists y(x=y \wedge p(y)) \text{ and } T \vdash \exists y.q \to q$$

we deduce that

$$HL(\Sigma,T) \vdash \{p\}S\{q\}$$

which is a contradiction. □

PROOF OF LEMMA 4.3

Let $\{(r_i,t_i) : i \in \omega\}$ be an enumeration of all assertions of $L(\Sigma)$ such that $HL(\Sigma_c,T_p) \vdash \{r_i\}S\{t_i\}$. Let us write $r_i = r_i(x,z_i)$ and $t_i = t_i(x,z_i)$ where z_i lists all free variables in r_i and t_i distinct from those in the list x.

Define $\phi_i(x) = \forall z_i[r_i(c,z_i) \to t_i(x,z_i)]$ wherein $r(c,z_i)$ is $r(x,z_i)$ with c_i replacing x_i $(1 \le i \le k)$.

4.4 LEMMA *For no* $n \in \omega$ *is it the case that*

$$T_p \vdash \bigwedge_{i=1}^{n} \phi_i(x) \to q$$

PROOF Suppose for a contradiction that

$$T_p \vdash \bigwedge_{i=1}^{m} \phi_i(x) \to q \qquad (1)$$

for some $m\in\omega$. We will prove that for each $i\in\omega$

$$HL(\Sigma_c,T_p)\vdash\{x=c\}S\{\phi_i(x)\}. \tag{2}$$

Then by the Conjunction Rule Lemma 2.2,

$$HL(\Sigma_c,T_p)\vdash\{x=c\}S\{\bigwedge_{i=1}^{m}\phi_i(x)\}$$

and by the Rule of Consequence, using (1), we obtain

$$HL(\Sigma_c,T_p)\vdash\{x=c\}S\{q\}$$

which contradicts Lemma 4.2. Thus, it is sufficient to deduce (2) as a general fact.

From the enumeration we may assert that

$$HL(\Sigma_c,T_p)\vdash\{r_i(x,z_i)\}S\{t_i(x,z_i)\}$$

By the Invariant Rule 2.3, since the variables of z_i are distinct from those of S,

$$HL(\Sigma_c,T_p)\vdash\{\neg r_i(c,z_i)\}S\{\neg r_i(c,z_i)\}.$$

By the Disjunction Rule Lemma 2.1,

$$HL(\Sigma_c,T_p)\vdash\{r_i(x,z_i)\vee\neg r_i(c,z_i)\}S\{t_i(c,z_i)\vee\neg r_i(x,z_i)\}$$

By the Rule of Consequence

$$HL(\Sigma_c,T_p)\vdash\{x=c\wedge(r_i(x,z_i)\vee\neg r_i(c,z_i))\}S\{r_i(x,z_i)\rightarrow t_i(c,z_i)\}$$

and by a further application we can simplify the specified program to

$$HL(\Sigma_c,T_p)\vdash\{x=c\}S\{r_i(x,z_i)\rightarrow t_i(c,z_i)\}$$

By the $\forall$-Rule Lemma 2.4,

$$HL(\Sigma_c,T_p)\vdash\{x=c\}S\{\forall z_i[r_i(c,z_i)\ t_i(x,z_i)]\}$$

and by the definition of $\phi_i(x)$ this statement (2). □

4.5 LEMMA *There is* $B\in Mod(\Sigma_c,T_p)$ *such that for some* $b=b_1,\ldots,b_k\in B$ *and for each* $i\in\omega$

$$B\models\phi_i(b) \textit{ but } B\not\models q(b).$$

PROOF Suppose the lemma is false. Let $d=d_1,\ldots,d_k$ be a list of new constants and adjoin d to Σ_c to make $\Sigma_{c,d}$. Define the set

$$\Gamma=\{\phi_i(d)\ :\ i\in\omega\}\cup\{\neg q(d)\}$$

wherein $\phi_i(d)$ and $q(d)$ are ϕ_i and q with x_i replaced by d_i $(1\le i\le k)$. Our supposition asserts that the set of sentences $T_p\cup\Gamma$ has no model and is therefore inconsistent. By the Compactness Theorem, some finite subset

Γ_o of $T_p \cup \Gamma$ is inconsistent. This means that for some $n \in \omega$ dependent on Γ_o,

$$T_p \vdash \bigwedge_{i=1}^{m} \phi_i(d) \to q(d)$$

On replacing the constants d by the variables of x we obtain a contradiction with Lemma 4.4. □

We claim that the Structure B in Lemma 4.5 can serve as the structure A_o required in Lemma 4.3.

Let $\sigma, \tau \in State(B)$ such that

(i) $\sigma(v) = \tau(v)$ for each $v \notin x$;

(ii) $\sigma(x_i) = a_i$ where a_i is named by c_i

(iii) $\tau(x_i) = b_i$ where b_i is given in Lemma 4.5.

By Lemma 4.5, $B \models p(\sigma)$ does not imply $B \models q(\tau)$; and so we have to show that $(\sigma,\tau) \in AX(B)(S)$.

By Theorem 3.7, $AX(B)(S) = AX(\Sigma_c, T_p)_B(S)$. Suppose $r,t \in L(\Sigma)$ are such that $HL(\Sigma_c, T_p) \vdash \{r\}S\{t\}$. Then for some $i \in \omega$, $r = r_i$ and $t = t_i$ in our enumeration. Because $B \models \phi_i(b)$ we know that

$$B \models \forall z_i (r(a,z_i) \to t(b,z_i))$$

By (i) we can take $\sigma(z_i) = \tau(z_i) = e$ for some list of elements e and write

$$B \models r(c,e) \to t(b,e)$$

Hence $B \models r(\sigma)$ implies $B \models t(\tau)$ and we may conlcude that $(\sigma,\tau) \in AX(\Sigma_c, T_p)_B(S)$.

This ends the proof of Lemma 4.3 and the argument for completeness. □

Finally, notice that Theorem 4.1 has this to say about computation on an individual structure :

4.6 COROLLARY *Let* A *be a structure of signature* Σ. *For each program* $S \in WP(\Sigma)$ *and any assertions* $p,q \in L(\Sigma)$, $HL(A) \vdash \{p\}S\{q\}$ *if, and only if, for every structure* B *elementarily equivalent to* A *we have* $AX(B) \models \{p\}S\{q\}$.

The corollary is proved by simply taking T = Th(A) in Theorem 4.1. Notice, in particular, that it does not answer the following

4.7 QUESTION *Given any structure* A, *is it the case that*

$$HL(A) \vdash \{p\}S\{q\} \text{ if, and only if, } AX(A) \models \{p\}S\{q\}$$

for any $p,q \in L(\Sigma)$ *and* $S \in WP(\Sigma)$?

This question will be answered in Section 7.

5. COMPARISON OF AXIOMATIC AND OPERATIONAL SEMANTICS

To contrast the axiomatic and operational semantics we prove some theorems about their effects on computation on an individual structure A.

5.1 THEOREM *For any structure* A *of signature* Σ *and any program* $S \in WP(\Sigma)$,

$$OP(A)(S) \subseteq AX(A)(S) .$$

PROOF Suppose $(\sigma,\tau) \in OP(A)(S)$. Now to show that $(\sigma,\tau) \in AX(A)(S)$ is to show for any assertions $p,q \in L(\Sigma)$ if $HL(A) \vdash \{p\}S\{q\}$ then $A \models p(\sigma)$ implies $A \models q(\tau)$. But this is an immediate consequence of the soundness of Hoare's logic HL(A) for the operational semantics OP(A). □

Theorem 5.1 means that if τ can be computed as *the* output state from input state σ using S under its standard operational semantics then τ can be obtained as *an* output state from σ using S and its axiomatic semantics : whilst OP(A)(S) is deterministic, we do not know that AX(A)(S) is deterministic.

5.2 THEOREM *Let* A *be a structure of signature* Σ *and* $S \in WP(\Sigma)$. *If* $(\sigma,\tau) \in OP(A)(S)$ *and* $(\sigma,\tau') \in AX(A)(S)$ *then* $\tau = \tau'$.

PROOF Let $x = x_1,\ldots,x_k$ be the list of variables in S and let $z = z_1,\ldots,z_k$ be a list of new variables. Suppose that $(\sigma,\tau) \in OP(A)(S)$ and without loss of generality assume that $A \models [x=z](\sigma)$ (recall monotonicity in DE BAKKER [5], for instance).

We can represent the operational computation of τ from σ in a first-order formula :

5.3 LEMMA *There exists a formula* $\phi(x,z) \in L(\Sigma)$ *and a list of terms* $t(z) = t_1(z),\ldots,t_k(z)$ *such that*

(i) $A \models \phi(\sigma)$

(ii) $A \models [\phi(x,z) \wedge x=z](\delta)$ *implies* $OP(A)(S)(\delta)\downarrow$

(iii) $A \models [x=t(z)](\tau)$

By Lemma 2.12, we may now deduce

$$HL(A) \vdash \{\phi(x,z) \wedge x=z\}S\{x=t(z)\}$$

If $(\sigma,\tau') \in AX(A)(S)$ then, because HL(A) is sound for the axiomatic semantics AX(A), we know that

$$A \models [\phi(x,z) \wedge x=z](\sigma) \text{ implies } A \models [x=t(z)](\tau').$$

By Lemma 5.3, we have

$$A \models [x=t(z)](\tau') \quad \text{and} \quad A \models [x=t(z)](\tau)$$

and so τ,τ' coincide on variables x of S.

Thus, on the *operational domain* of S on A

$$DOM_A(S) = \{\sigma \in State(A) : \exists \tau \in State(A).(\sigma,\tau) \in OP(A)(S)\}$$

the axiomatic semantics is single-valued and coincides with the operational semantics; we record this fact as follows :

5.4 COROLLARY *For any structure* A *of signature* Σ *and any program* $S \in WP(\Sigma)$ *the operational semantics* $OP(A)(S)$ *is faithfully embedded in the axiomatic semantics* $AX(A)(S)$.

5.5 COROLLARY *For any structure* A *of signature* Σ *and any program* $S \in WP(\Sigma)$, *if* S *is everywhere convergent under its operational semantics then*

$$OP(A)(S) = AX(A)(S)$$

In particular, if there is a difference between the axiomatic and operational semantics of a program S it must arise at an input state where S fails to converge to an output state under its conventional operational semantics; furthermore, at such an input S may converge to many output states under its axiomatic semantics.

The next result recovers Cook's analysis of completeness : recall Theorem 2.10 :

5.6 THEOREM *Let* A *be a structure of signature* Σ *and suppose that the assertion language* $L(\Sigma)$ *is expressive for* $WP(\Sigma)$ *with respect to* $OP(A)$. *Then for every* $S \in WP(\Sigma)$

$$OP(A)(S) = AX(A)(S)$$

and the axiomatic semantics is deterministic. Moreover, HL(A) *is sound and complete for* AX(A) : *for any* $p,q \in L(\Sigma)$,

$$HL(A) \vdash \{p\}S\{q\} \text{ if, and only if, } AX(A) \models \{p\}S\{q\}.$$

PROOF Everything in the theorem follows from equality of the two semantics. By Theorem 5.1, it is sufficient to show that $AX(A)(S) \subseteq OP(A)(S)$.

Let $x=x_1,\ldots,x_k$ be the list of variables in S and let $z=z_1,\ldots,z_k$ be a list of new variables. Since A is an expressive structure, we can choose some $\phi(x,z) \in L(\Sigma)$ to define the strongest postcondition $sp_A(x=z,S)$. This formula $\phi(x,z)$ can represent the input-output behaviours of S under

operational semantics as follows : let $\delta \in State(A)$ and define state

$$\delta_*(v) = \begin{cases} \delta(v) & \text{if } v \notin x; \\ \delta(z_i) & \text{if } v = x_i \end{cases}$$

Then we note that

$$A \models \phi(\delta) \text{ if, and only if, } (\delta_*, \delta) \in OP(A)(S).$$

Now suppose that $(\sigma,\tau) \in AX(A)(S)$, and without loss of generality assume that $A \models [x=z](\sigma)$. Since ϕ is strongest postcondition,

$$OP(A) \models \{x=z\}S\{\phi\}$$

and by Cook's Completeness Theorem 2.10,

$$HL(A) \vdash \{x=z\}S\{\phi\}.$$

Since HL(A) is sound for the axiomatic semantics AX(A)

$$A \models [x=z](\sigma) \text{ implies } A \models \phi(\tau)$$

By our assumption on σ we can deduce that $A \models \phi(\tau)$ and hence that $(\tau_*, \tau) \in OP(A)(S)$. But $\tau_* = \sigma$ and hence $(\sigma,\tau) \in OP(A)(S)$. □

5.7 COROLLARY *Let* $\mathbb{N}$ *be the standard model of arithmetic with signature* Σ, *namely*

$$\mathbb{N} = (\{0,1,\ldots\} : 0,\ x+1, x+y,\ x.y) .$$

Then for every while*-program* $S \in WP(\Sigma)$

$$OP(\mathbb{N})(S) = AX(\mathbb{N})(S) .$$

Theorem 5.6 allows us to prove the following curious characterisation of the operational semantics.

5.8 THEOREM *For any structure of signature* Σ *and any program* $S \in WP(\Sigma)$,

$$OP(A)(S) = \cap\{AX(B)(S) : B \textit{ is an expansion of } A\}$$

PROOF If B is an expansion of A then for $S \in WP(\Sigma)$

$$OP(A)(S) = OP(B)(S) \subseteq AX(B)(S)$$

by Theorem 5.1; this proves one inclusion. For the reverse inclusion, choose a structure B which is an expansion of A and is expressive with respect to OP(B) : such B can be made by adding appropriate arithmetic coding functions following the methods in Section 3 of [12]. Then by Theorem 5.6 we have

$$AX(B)(S) = OP(B)(S) = OP(A)(S) .$$ □

6. AXIOMATIC SEMANTICS AND COMPUTABILITY

By Corollary 5.7, the functions and relations computable by the operational and axiomatic semantics coincide on the standard model of arithmetic $\mathbb{N}$; in particular, the class of partial functions on $\mathbb{N}$ definable by while-programs under their axiomatic semantics is the class of partial recursive functions. More generally, we may observe, using the definitions of 1.6, and Theorem 5.6, that

6.1 LEMMA *Let* A *be a computable structure of signature* Σ *and suppose that* $L(\Sigma)$ *is expressive for* $WP(\Sigma)$ *with respect to* $OP(A)$. *Then every partial function on* A *definable by a* while*-program under its axiomatic semantics is computable.*

The converse is not true because the remark following Lemma 1.7.

6.2 QUESTION *What sets of functions are definable by* while*-programs under axiomatic semantics on computable, but non-expressive, structures such as Presburger arithmetic*

$$P = (\{0,1,...\}: 0, x+1)?$$

The set of while-programs under operational semantics defines the set of partial recursive functions on Presburger arithmetic. The main task of this section is to show that the axiomatic semantics is able to define non-recursive functions (Corollary 6.5).

6.3 THEOREM *Let* A *be an effectively enumerated structure of signature* Σ *and let* $S \in WP(\Sigma)$. *Then*

(1) $OP(A)(S)$ *is recursively enumerable in* $Th(A)$; *and*

(2) $AX(A)(S)$ *is co-recursively enumerable in* $Th(A)$.

Therefore, if $AX(A)(S) = OP(A)(S)$ *then the set is decidable in* $Th(A)$.

PROOF The proof of statement (1) is left as an exercise. Consider the definition of $AX(A)(S) \subset States(A)$:

$$\begin{aligned}(\sigma,\tau) \in AX(A)(S) &\iff (\forall p,q \in L(\Sigma))[HL(A) \vdash \{p\}S\{q\} \Rightarrow A \models p(\sigma) \to q(\tau)] \\ &\iff (\forall p,q \in L(\Sigma))[\{p\}S\{q\} \in HL(A) \Rightarrow p(\sigma) \to q(\tau) \in Th(A)] \\ &\iff (\forall p,q \in L(\Sigma))[\{p\}S\{q\} \notin HL(A) \vee p(\sigma) \to q(\tau) \in Th(A)]\end{aligned}$$

With an enumeration of A, a derived codification of States (A), a gödel numbering of $L(\Sigma)$, and derived codifications of Th(A) and HL(A), we may formally express the fact that $\{p\}S\{q\} \notin HL(A)$ is co-recursively enumerable in Th(A), and hence deduce that AX(A)(S) is co-recursively enumerable in Th(A). □

6.4 COROLLARY *Let* A *be a computable structure and suppose* Th(A) *is decidable. If* AX(A)(S) = OP(A)(S) *then the set is decidable. In particular, if* A *is expressive then for every* S *the set* AX(A)(S) = OP(A)(S) *is decidable.*

6.5 COROLLARY *There is a* while*-program* S *over Presburger arithmetic* P *such that*

$$OP(P)(S) \subsetneq AX(P)(S)$$

PROOF P satisfies the hypotheses of Corollary 6.3. Each recursively enumerable set Ω may be represented as the graph of a partial recursive function : let S be a program such that

$$\Omega = OP(P)(S)$$

where Ω is an r.e. non-recursive set. □

7. COMPLETENESS FOR STRUCTURES

Question 4.7 asked if HL(A) is complete for the axiomatic semantics AX(A) for any structure A. Here is the answer :

7.1 THEOREM *There is a structure* A *and specified program* $\{p\}S\{q\}$ *such that*

$$AX(A) \models \{p\}S\{q\} \text{ but } HL(A) \not\vdash \{p\}S\{q\};$$

in particular, HL(A) *is not complete for* AX(A).

PROOF Let $A = (\{0,1,\ldots\}: 0, x+1, x\dot{-}1)$ and consider the program

S::=x:=0;
    while y≠0 do x:=x+1;y:=y$\dot{-}$1 od.

This S with p and q defined by

y=z and x=z

respectively forms the specified program required in the theorem. The valdity property that $AX(A) \models \{p\}S\{q\}$ follows from Corollary 5.5, because S is everywhere convergent under OP(A). The fact that $\{p\}S\{q\}$ cannot be derived in HL(A) is more complicated to prove. It begins with the observation that an invariant for the loop in S would define addition x+y on A. However one can prove that A admits quantifier elimination (since A is so close to Presburger Arithmetic P); and further that boolean or quantifier-free formulae over A cannot define the graph of addition on A. Thus no invariant for the loop can exist, and hence no deduction of $\{p\}S\{q\}$ in HL(A). □

The result should be compared with Theorem 5.6; we conclude this section with two further results on completeness.

7.2 LEMMA *For any structure* A, *if* HL(A) *is complete for the operational semantics* OP(A) *then it is complete for the axiomatic semantics* AX(A).

PROOF Suppose that HL(A) is complete for OP(A) and assume that $AX(A) \models \{p\}S\{q\}$. By Theorem 5.1, $OP(A) \models \{p\}S\{q\}$ and, therefore, $HL(A) \vdash \{p\}S\{q\}$. □

7.3 THEOREM *There is a structure* A *such that* HL(A) *is complete for* AX(A) *but* HL(A) *is not complete for* OP(A).

PROOF Again we outline the argument which is based on our earlier studies of Hoare's logic and arithmetic. The following result is rather interesting :

7.4 THEOREM *Let* A *be a model of Peano Arithmetic* PA. *Then* HL(A) *is complete for* AX(A). *Furthermore, for each* $S \in WP(\Sigma_{PA}), AX(A)(S)$ *is first-order definable over* A.

PROOF The proof is based upon the principal theorem in [12] which establishes a strongest postcondition calculus for Peano Arithmetic : for each precondition p and program S there is a first-order formula SP(p,S) such that for each postcondition q

$$HL(PA) \vdash \{p\}S\{q\} \text{ if, and only if, } PA \vdash SP(p,S) \rightarrow q$$

and, in particular,

$$HL(PA) \vdash \{p\}S\{SP(p,S)\}$$

We couple with Theorem 7.4 one of the main theorems in [10], namely : for a model A of Peano Arithmetic, HL(A) is complete for OP(A) if, and only if, A is elementary equivalent to the standard model $\mathbb{N}$. Thus, to prove Theorem 7.3 it is sufficient to choose A to be any model of Peano Arithmetic that is not elementary equivalent to $\mathbb{N}$. □

8. NON-DETERMINISM

The basic relationships existing between the axiomatic semantics and operational semantics were worked out in Sections 5 and 6. In this last section we examine in greater detail a principal semantic difference between the meanings : the axiomatic semantics need not be deterministic. We will construct a structure A and a program S such that AX(A)(S) is not a single-valued relation on A.
The program S has form

$$S ::= \underline{\text{while}}\ b\ \underline{\text{do}}\ S_o\ \underline{\text{od}}$$

where S_o contains no loops : let us refer to such a program as being in *simple form*. The following is routine :

8.1 LEMMA *Let* A *be a structure of signature* Σ *and let* $S \in WP(\Sigma)$ *be in simple form. Then a sufficient condition for* $(\sigma,\tau) \in AX(A)(S)$ *is the following : for each invariant* $I \in L(\Sigma)$ *where*

$$HL(A) \vdash \{I \wedge b\} S_o \{I\}$$

we have that

$$A \models I(\sigma) \text{ implies } A \models (I \wedge \neg b)(\tau)$$

In applying the lemma to two distinct pairs (σ,τ) and (σ,τ'), and thereby demonstrating nondeterminism, the sufficient condition can be verified by means of the following condition :

8.2 PATCHING LEMMA *A sufficient condition for* $(\sigma,\tau) \in AX(A)(S)$ *is that* $A \models \neg b(\tau)$ *and for each invariant* I *such that* $I(\sigma)$ *there is a pair of sequences of states*

$$\sigma = \sigma_0, \sigma_1, \ldots, \sigma_k \text{ and } \tau_0, \tau_1, \ldots, \tau_\ell = \tau$$

for which

(i) $(\sigma_i,\sigma_{i+1})\in OP(A)(S)$ *and* $(\tau_j,\tau_{j+1})\in OP(A)(S)$ *for* $0\le i\le k-1$ *and* $0\le j\le \ell-1$;

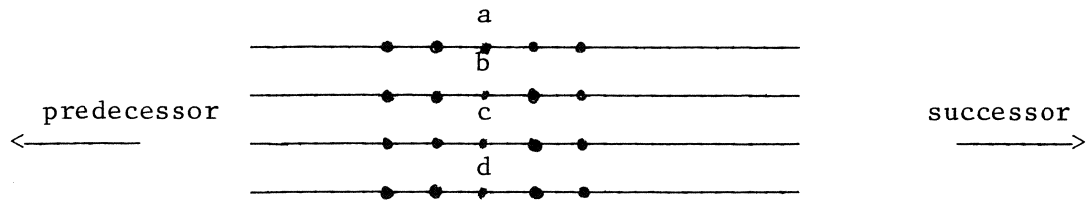
(ii) $A\models I(\sigma_k)$ *implies* $A\models I(\tau_0)$.

The condition describes how two operational computations can be "patched" by the formula I. We can now proceed with the example.

8.3 EXAMPLE Let Σ = {a,b,c,d,SUCC,PRED} where a,b,c,d are constant symbols and SUCC and PRED are unary operator symbols. Let E be the set containing the equations

$$SUCC(PRED(X)) = X$$
$$PRED(SUCC(X)) = X$$

We take A to be the initial algebra semantics of the algrebaic specification (Σ,E) : see ADJ[20]. The following picture may be helpful in understanding the structure A :



Next we define a program S by

S::= while $x\neq a$ do x:=PRED(x); y:=SUCC(y) od

And we define the states σ,τ,τ' by

$$\sigma(v) = \begin{cases} b & \text{if } v=x \\ a & \text{otherwise} \end{cases}$$

$$\tau(v) = \begin{cases} c & \text{if } v=y \\ a & \text{otherwise} \end{cases}$$

$$\tau'(v) = \begin{cases} d & \text{if } v=y \\ a & \text{otherwise} \end{cases}$$

8.4 CLAIM *Is is the case that* $(\sigma,\tau)\in AX(A)(S)$ *and* $(\sigma,\tau')\in AX(A)(S)$.

PROOF We show that $(\sigma,\tau)\in AX(A)(S)$; the other axiomatic computation is treated similarly.

With reference to the Patching Lemma 8.2, clearly

$$A \models \neg(x \neq a)(\tau)$$

Suppose that I is an invariant with

$$HL(A) \vdash \{I \wedge x \neq a\}\ x:=PRED(x);\ y:=SUCC(y)\ \{I\}$$

and $A \models I(\sigma)$; we must now construct appropriate sequences of states which serve as operational computations, of lengths k and ℓ, patched by I.

In our construction $k=\ell$ and, postponing the calculation of the value of k, we define the states for $i=1,\ldots,k$

$$\sigma_i(v) = \begin{cases} PRED^i(b) & \text{if } v=x \\ SUCC^i(a) & \text{if } v=y \\ a & \text{otherwise} \end{cases}$$

$$\tau_0^{(k)} = \begin{cases} SUCC^k(a) & \text{if } v=x \\ PRED^k(c) & \text{if } v=y \\ a & \text{otherwise} \end{cases}$$

$$\tau_i^{(k)} = \begin{cases} PRED^i SUCC^k(a) & \text{if } v=x \\ SUCC^i PRED^k(c) & \text{if } v=y \\ a & \text{otherwise} \end{cases}$$

We take $\sigma_0=\sigma$ and note that $\tau_k^{(k)}=\tau$.

What remains is for us to show there is a value of k that is sufficiently large to ensure that

$$A \models I(\sigma_k) \text{ implies } A \models I(\tau_0^{(k)})$$

The existence of a k_0 such that, for all $k>k_0$, the implication is true is demonstrated by a combinatorial argument based on the fact that A admits quantifier elimination.

9. CONCLUDING REMARKS

We have shown that the axiomatic semantics AX of while-programs is a non-standard semantics far removed from the standard semantics of WP. In general, AX is non-deterministic and it need not be computable : on the structure Presburger Arithmetic P it cannot be implemented, in principle. But there are structures (for example, the standard model of arithmetic $\mathbb{N}$)

on which the axiomatic semantics and the operational semantics coincide. In the light of these and the other results, what conclusions on axiomatic semantics, and the role of verification in language design, can be found?

The situation reminds us of the non-standard models of Peano Arithmetic PA. The system PA is a fundamental formal system that fails to capture the equally fundamental semantics $\mathbb{N}$ for which it was specifically designed. The system is no less important as a logical tool for the study of number theory and the non-standard models are now considered as indispensible tools for the analysis of the system. We consider the case of Hoare's logic to be the same : Hoare's logic is a basic tool for the study of program verification, and the study of the non-standard semantics for while-programs, the true semantics for the proof system, will be significant in understanding the system. Ultimately, the system's importance will be determined by its role in the theoretical and practical exploration of the following idea :

9.1 LOGICIST'S THESIS *What may be known about our computer programs is represented, and delimited, by what may be formally proved about programs in logical systems.*

In the case of proving program correctness, Hoare's logic, as we have defined it, maintains its eminence for three connected reasons. First, it is based on first-order logic which is the logical system known in greatest depth. Secondly, logical systems for total correctness are fraught with difficulties associated with the proof of termination; in addition, first-order logic cannot be used to specify termination (see APT[1]). Thus, partial correctness is the principal property for which we can make and study formal systems. Thirdly, the first-order Hoare's logic for while-programs serves as the prototype for the manufacture of partial correctness logics for most of our contemporary programming languages and in these logics specific programs can be verified : see APT[1] and MC GETTRICK[31].

If one is interested in the Logicist Thesis then the Floyd-Hoare Principle is fundamentally important.

Finally, we will make references to research relevant to the central concerns of this paper.

A rather different perspective on completeness theorems, and hence on axiomatic semantics, emerges from the work of the Hungarian School of I. Nemeti, H. Andreka, I. Sain and L. Csirmaz on the logical foundations of verification [2,3,4,15,16]. Among the subjects they have investigated in great depth is completeness for first-order systems involving axiomatic time. Technically, their time structure semantics provides an alternative route to the completeness theorem we prove, but further work is required to reconcile their results with the questions examined here. Perhaps it is worth examining the use of a time sort in pursuit of a substitute for a total correctness logic.

We note that Magidor and J. Stavi have made a completeness theorem for an iterative language and its first-order partial correctness logic using a semantics involving time (personal communication).

For relevant work on the completeness problem outside first-order Hoare's logic see F. KRÖGER [26] in which ω-rules are considered and the monograph [37] in many-sorted finite sequencing mechanism is allowed.

REFERENCES

[1] APT, K.R., Ten years of Hoare's logic. A Survey : Part 1, ACM - Transactions Programming Languages and Systems 3(4) (1981) 431-483.

[2] ANDREKA, H. and I. NEMETI, Completeness of Floyd Logic, Bulletin Section of Logic Wroclaw 7 (1978)(3) 115-121.

[3] ANDREKA, H., I. NEMETI and I. SAIN, A complete logic for reasoning about programs via non-standard model theory, Theoretical Computer Science 17 (1982) 193-212.

[4] _____ , A characterization of Floyd-provable programs, in : Mathematical Foundations of Computer Science '81, Lecture Notes in Computer Science 118, Springer-Verlag, Berlin, 1981, 162-171.

[5] DE BAKKER, J.W., *Mathematical theory of program correctness*, Prentice-Hall International, London, 1980.

[6] BERGSTRA, J.A., J. TIURYN and J.V. TUCKER, Floyd's Principle, correctness theories and program equivalence, Theoretical Computer Science 17 (1982) 113-149.

[7] BERGSTRA, J.A. and J.V. TUCKER, Some natural structures which fail to possess a sound and decidable Hoare-like logic for their while-programs, Theoretical Computer Science 17 (1982) 303-135.

[8] _____ , Algebraically specified programming systems and Hoare's logic, in : International Colloquium on Automata, Languages and Programming 1981, Lecture Notes in Computer Science 115, Springer-Verlag, Berlin, 1981, 348-362.

[9] _____ , The refinement of specifications and the stability of Hoare's logic, in : Logics of Programs, Lecture Notes in Computer Science 131, Springer-Verlag, 1981, 24-36.

[10] _____ , Expressiveness and the completeness of Hoare's logic, Journal Computer and System Sciences 25 (1982) 267-284.

[11] _____ , Two theorems about the completeness of Hoare's logic ,Information Processing letters 15 (1982) 143-149.

[12] _____ , Hoare's logic and Peano's Arithmetic, Theoretical Computer Science 22 (1983) 265-284.

[13] _____ , Hoare's logic for programming languages with two data types, Mathematical Centre Report IW 207 Amsterdam, 1982.

[14] COOK, S.A., Soundness and completeness of an axiomatic system for program verification, SIAM Journal Computing 7 (1978) 70-90; Corrigendum 10 (1981) 612.

[15] CSIRMAZ, L., On the completeness of proving partial correctness, Acta Cybernetica 5 (1981) 181-190.

[16] CSIRMAZ, L. and J.B. PARIS, A property of 2-sorted Peano models and program verification, Preprint, Math. Inst., Hungarian Academy, Budapest, 1981.

[17] DIJKSTRA E.W., Guarded commands, nondeterminacy and formal derivation of programs, Communications ACM, 18 (1975) 453-457.

[18] _____, *A discipline of programming*, Prentice-Hall, 1976.

[19] FLOYD, R.W., Assigning meaning to programs, in : J.T. Schwartz (ed) *Mathematical aspects of computer science*, AMS, 1967, 19-32.

[20] GOGUEN, J.A., J.W. THATCHER and E.G. WAGNER, An initial algebra approach to the specification, correctness and implementation of abstract data types, in : R.T. Yeh (ed.) *Current trends in programming methodology* IV, *Data structuring*, Prentice-Hall, Englewood Cliffs, New Jersey, 1978, 80-149.

[21] GREIF, I. and A.R. MEYER, Specifying the semantics of while programs: a tutorial and critique of a paper by Hoare and Lauer, ACM Transactions Programming Languages and Systems 3 (1981) 484-507.

[22] HOARE, C.A.R., An axiomatic basis for computer programming, Communications ACM 12 (1969) 576-580.

[23] _____, Procedures and parameters : an axiomatic approach, in E. Engeler (ed.) *Symposium on the semantics of algorithmic languages*, Springer-Verlag, Berlin, 1971, 102-116.

[24] HOARE, C.A.R. and P. LAUER, Consistent and complementary formal theories of the semantics of programming lnaguages, Acta Informatica 3 (1974) 135-155.

[25] HOARE, C.A.R. and N. WIRTH, An axiomatic definition of the programming language PASCAL, Acta Informatica, 2 (1973) 335-355.

[26] KRÖGER, F., Infinite proof rules for loops, Acta Informatica 14 (1980) 371-389.

[27] LAUER, P., Consistent and complementary formal theories of the semantics of programming languages, Ph.D. Thesis Queens University, Belfast, 1972.

[28] LONDON, R.L., J.V. GUTTAG, J.J. HORNING, B.W. LAMPSON, J.G. MITCHELL and G.L. POPEK, Proof rules for the programming language EUCLID, Acta Informatica 10 (1978) 1-26.

[29] MANNA, Z., The correctness of programs, Journal Computer and Systems Sciences 3 (1969) 119-127.

[30] MAL'CEV, A.I., Constructive algebras I, Russian Mathematical Surveys 16 (1961) 77-129.

[31] MCGETTRICK, A., *The definition of programming languages*, Cambridge University Press, 1980.

[32] MEYER, A.R. and J.Y. HALPERN, Axiomatic definitions of programming languages. A theoretical assessment. Journal ACM 29 (1982) 555-576.

[33] _____ , Axiomatic definitions of programming languages II, MIT Laboratory Computer Science, TM-179 (1980).

[34] PAGAN, F.G., *Formal specification of programming languages*, Prentice-Hall Inc., 1981.

[35] RABIN, M.O., Computable algebra, general theory and the theory of computable fields, Transactions AMS, 95 (1960) 341-360.

[36] SCHWARTZ, R., An axiomatic semantic definition of ALGOL 68, UCLA Computer Science Report 7838, 1978.

[37] TUCKER, J.V. and J.I. ZUCKER, *Program correctness over abstract data types, with error state semantics*, Monograph, in preparation.

ONTVANGEN 3 0 SEP. 1983