MIT/LCS/TM-97

COMPUTABILITY AND COMPLETENESS IN LOGICS OF PROGRAMS

David Harel
Albert R. Meyer
Vaughan R. Pratt

February 1978

Computability and Completeness in Logics of Programs

D. Harel, A. R. Meyer and V. R. Pratt
Massachusetts Institute of Technology
Cambridge, Mass. 02139
June 17, 1977

Abstract

Dynamic logic is a generalization of first order logic in which quantifiers of the form "for all X..." are replaced by phrases of the form "after executing program α...". This logic subsumes most existing first-order logics of programs that manipulate their environment, including Floyd's and Hoare's logics of partial correctness and Manna and Waldinger's logic of total correctness, yet is more closely related to classical first-order logic than any other proposed logic of programs. We consider two issues: how hard is the validity problem for the formulae of dynamic logic, and how might one axiomatize dynamic logic? We give bounds on the validity problem for some special cases, including a Π_2^0-completeness result for the partial correctness theories of uninterpreted flowchart programs and a Π_1^1-completeness result for unrestricted dynamic logic. We also demonstrate the completeness of an axiomatization of dynamic logic relative to arithmetic.

Key words: Arithmetic hierarchy
Dynamic logic
R.e. programs
Regular programs
Relative completeness
Validity problem

Computability and Completeness in Logics of Programs

D. Harel, A. R. Meyer and V. R. Pratt
Massachusetts Institute of Technology
Cambridge, Mass. 02139

Introduction

In this paper we continue the development of a proof theory and semantics of a formal logical language for making assertions about programs. This language, which was introduced in [13], will be called "dynamic logic" in this paper. It is based on the language of first order logic, with the quantifier "for all X ..." generalized to "after executing the program α ... ." Just as "for all X ..." is abbreviated to "$\forall X$...," so shall we abbreviate "after executing α ..." to "$[\alpha]$...". Just as $\exists X$ is the dual of $\forall X$, so is $\langle\alpha\rangle$ the dual of $[\alpha]$, and indeed $\langle\alpha\rangle P$ is equivalent to $\neg[\alpha]\neg P$. Informally, the truth of $[\alpha]P$ in a state (interpretation) $\mathcal{I}$ amounts to the claim that, if α is started in state $\mathcal{I}$, P will be true if and when α halts, no matter which state α halted in (α may be non-deterministic). Likewise, the truth of $\langle\alpha\rangle P$ in a state $\mathcal{I}$ affirms that, starting from state $\mathcal{I}$, some computation of α leads to a state in which P is true. A formal definition of $[\alpha]$ and $\langle\alpha\rangle$ is outlined below in terms of the notion of a modality in formal logic. Using this language, $\forall X$ could equivalently be expressed as $[X:=?]$ where $X:=?$ is a nondeterministic program which sets X to a random individual. This is the sense in which $[\alpha]$ generalizes ordinary logical quantification. (Our notation is motivated by the box and diamond notations of modal logic [10]; in conversation we have found it convenient to pronounce $[\alpha]$ as "box α" and $\langle\alpha\rangle$ as "diamond α.")

Many of the basic assertions one might like to make about programs are directly expressible as formulae involving $[\alpha]$ and $\langle\alpha\rangle$. For example, to assert that program α never halts on any input, one can write $[\alpha]$*false* (or $[\alpha]X\neq X$). Literally, this asserts that *false* holds in any final state reached by α, which of course is only possible if α never reaches such a final state. Dually, to assert that program α halts on all inputs, one need only write $\langle\alpha\rangle$*true*. Hoare's partial correctness assertion $P\{\alpha\}Q$ [8] may be expressed as $\models(P\supset[\alpha]Q)$, which suggests the analogous $\models(P\supset\langle\alpha\rangle Q)$ for a general termination assertion. Two programs each using a single variable for output (respectively Y and Z) may be asserted to be equivalent with $\forall X((\langle\alpha\rangle Y=X)\equiv(\langle\beta\rangle Z=X))$, where X does not appear in α or β. This asserts that if X is a possible output of the program α, then X is also a possible output value of β, and conversely. We may also assert that α is determinate by saying that the value it yields in some computation is the value it yields in every computation, using $\forall X(\langle\alpha\rangle Y=X\supset[\alpha]Y=X)$.

For convenience we refer to classical first-order logic as *first-order logic*. By *loop-free logic* we mean first-order logic augmented with modalities restricted to programs in the closure, under union and composition, of tests and assignments. By *regular logic* we mean loop-free logic together with transitive closure, denoted by *. By *dynamic logic* we permit $[\alpha]$ and $\langle\alpha\rangle$ modalities where α may be any r.e. program (defined below).

The first part of the paper deals with the problem of how hard it is to decide validity of formulae of dynamic logic. Validity is a recursively enumerable predicate on formulae of first-order logic. It was shown in [13] that validity is no harder for loop-free logic than for first-order logic, but harder for regular logic. In this paper we further widen this gap between loop-free and regular logic; in particular, we strengthen an incompleteness result obtained in [13] for the partial correctness theory of a trivial one-loop program with one instruction in its body. On the other hand, we show that at least for partial correctness assertions (formulae $P \supset [\alpha]Q$ for first-order P,Q), the validity problem is no harder for dynamic logic than it is for regular logic; thus if one considers enriching one's programming language with progressively more powerful control structures, the only change in the difficulty of the validity problem for partial correctness comes at the point where loops are introduced.

The results of the second part of the paper strike a more positive note by generalizing a relative completeness theorem of Cook [4]. We show that an economical set of Hoare-like axioms (first described in [13]), taken together with those formulae of logic that are valid in the "natural number universe," form a complete set of axioms for the formulae of regular logic valid in this universe.

Dynamic Logic

To keep this paper self-contained, we now give a brief account of dynamic logic as developed in [13]. The central concept here is the *symbol*. We envisage four kinds of symbols: *function symbols*, *predicate symbols*, symbols called *logical connectives*, and symbols called *modalities*, all of various arities ≥ 0 except that modalities are required to be unary. Modalities fall into two classes, "boxes" and "diamonds;" the distinction, discussed informally above, is explained formally in the paragraph below on expressions. We refer to a set of such symbols as a language; logicians may prefer the term "similarity type." Although we do not have any particular set of symbols in mind here, the reader will not go far astray if he assumes that the symbol set is fixed and consists of a countable supply of function and predicate symbols of each arity (including such standard symbols as +, x, >, and =), all standard unary and binary

boolean logical connectives, and whatever modalities we permit explicitly in the sequel.

The four concepts dependent on the concept of symbol are state, universe, expression, and evaluation.

A *state* (interpretation, world, environment) of a language specifies a non-empty *domain* D (carrier, underlying set) and assigns a *value* to every symbol in the language except the modalities; it assigns as values k-ary functions on D to k-ary function symbols, k-ary predicates on D to k-ary predicate symbols, and k-ary boolean functions to k-ary logical connectives. All logical connectives receive their standard values, as does equality.

A *universe* (Kripke structure [10]) specifies a set U of states having a common domain D, subject to the foregoing constraint that = and all logical connectives have their standard values. A universe assigns to every modality in the language a value which is a binary relation on U. (Note that modalities differ from the other symbols in that their values are assigned per universe rather than per state.) A binary relation α on a universe U determines the net behavior of a (nondeterministic) program, i.e. a multi-valued function from start states to final states. For our purposes it is appropriate to regard programs as *being* such binary relations [1]. We consider only modalities whose value is "standard", in the sense that for each modality considered explicitly or implicitly in this paper and for each universe we have in mind a specific value for that modality in that universe. We shall write $[\alpha]$ (resp. $\langle\alpha\rangle$) to denote a box (resp. diamond) modality whose value in the universe is determined by α, where α is a syntactic object such as the deterministic assignment "X:=X+1", the non-deterministic assignment "X:=?", or the test "X>0?". Informally, the test P? in the universe U is the restriction of the identity relation on U to those states of U that satisfy P, while the assignment X:=T in universe U is the function (i.e. deterministic relation) that maps state $\mathcal{I}$ of U to a state differing from $\mathcal{I}$ only in the value it assigns to the zeroary function symbol X; this value is that of the term T in $\mathcal{I}$. The equation (T) (resp. (A)) of [13] gives the precise rule for determining the binary relation from the test (resp. assignment) and the universe. While we do not explicitly consider array assignment in this paper, the results of [13] indicate that none of the results of this paper depend on whether array assignments are permitted.

An *expression* over a language L consists of an ordered pair whose first component (its *operator*) is a k-ary symbol of L and whose second component (its *operand*) is a k-tuple consisting of certain expressions (called the *arguments* of the expression). (This is equivalent to the definition given in [13] in terms of trees.) The simplest expressions have a 0-ary operator and the (unique) 0-tuple for an operand. Expressions are

classified according to their operators as either *terms* (if the operator is a function symbol) or *formulae* (the rest). Formulae with predicate-symbol operators are called *atomic* while formulae with modal operators are called *modal*. The arguments of function and predicate symbols must be terms; arguments of modal symbols and logical connectives must be formulae. These remarks suffice to characterize the expressions of dynamic logic.

Like symbols, expressions are assigned values by states; the values of terms are individuals in D and the values of formulae are truth values. Expressions other than modal formulae are assigned values, or *evaluated*, by the standard Tarskian method [15]: the value in state $\mathcal{I}$ of an expression is the result of applying the value in $\mathcal{I}$ of the operator to the values in $\mathcal{I}$ of the arguments. Given a universe U (which assigns a value to α) and a state $\mathcal{I}$ in U, the value in $\mathcal{I}$ of the modal formula $[\alpha]P$ is *true* when P is true in every $\mathcal{J}$ of U satisfying $\mathcal{I}\alpha\mathcal{J}$, and *false* otherwise. The value of $\langle\alpha\rangle P$ in $\mathcal{I}$ is *true* when P is true in some $\mathcal{J}$ of U satisfying $\mathcal{I}\alpha\mathcal{J}$, and *false* otherwise.

Our previous remarks about first-order quantifiers can now be formalized as follows. Define a k-ary function (resp. predicate) symbol S to be *uninterpreted* in U if for every k-ary function (resp. predicate) V on D and for every state $\mathcal{I}$ of U, there is a state $\mathcal{I}'$ in U such that $\mathcal{I}'$ is identical to $\mathcal{I}$ except that $\mathcal{I}'$ assigns the value V to S. Let X be a zeroary function symbol uninterpreted in U and let X:=? denote that binary relation on U that relates pairs of states differing at most in their value of X. (This is an equivalence relation. As we noted, this program may be regarded as the non-deterministic assignment statement that assigns an arbitrary element of the domain D to X; the ? can be taken in the spirit of APL's symbol for a random number.) Then it should be evident that we may take $\forall X$ to be the modality $[X:=?]$ and $\exists X$ to be $\langle X:=?\rangle$.

In [13] attention was focused on loop-free and regular programs. In the first part of this paper, on computability, we shall consider an even larger class of programs called r.e. programs. An *execution sequence* is a string over an alphabet whose elements denote tests and assignments of the kind considered in [13]. An execution sequence denotes the composition of the binary relations on states denoted by successive elements of the sequence. A set of execution sequences denotes the union of the denotations of the elements of the set. Then the above class of regular programs is just the class of programs denoted by regular sets (in the sense of automata theory) of execution sequences. The r.e. programs are precisely those denoted by recursively enumerable execution sequence sets. (Note that execution sequence sets are precisely the level (ii) programs of section 3.1 of [13].)

The only modalities we shall consider in this paper are first-order quantifiers and *program modalities* (defined by execution sequence sets, excluding the instruction X:=?).

We classify formulae of dynamic logic into four successively larger categories according to the kinds of program modalities which appear:

first-order	no program modalities
loop-free	loop-free program modalities permitted
regular	regular program modalities permitted
dynamic	r.e. program modalities permitted

We independently classify formulae according to the kinds of non-zeroary predicate and function symbols which appear:

arithmetic	only +,x,=
logic	any except +,x
augmented arithmetic	no restriction

A formula P is *valid in a universe* U, or *U-valid*, (notation: $\models_U P$) when it is true in every state of U. P is *valid* (notation: $\models P$) when it is valid in every non-empty universe in which function and predicate symbols (except =) are uninterpreted and modalities and logical connectives are interpreted as described in the above paragraph on universes. (For first-order formulae this usage coincides with the standard definition of validity.) The *natural number universe* ***N*** has as domain the natural numbers, and in every state assigns the standard values to + and x (and any other symbols the reader recognizes as standard symbols of arithmetic). All function and predicate symbols other than the standard ones are uninterpreted in N. P is ***N****-valid* (notation: $\models_N P$) when it is valid in the natural number universe.

We use the word *theory* to refer to valid formulae. Thus the valid formulae of dynamic logic constitute *dynamic theory.* The ***N***-valid formulae of first-order arithmetic will be called *first-order number theory*, the ***N***-valid formulae of dynamic augmented arithmetic will be called *dynamic augmented number theory*, etc. Deciding ***N***-validity of first-order augmented arithmetic is known to be much harder than for first-order arithmetic because predicates not in the arithmetic hierarchy are implicitly definable in first-order augmented arithmetic. Similar remarks apply to dynamic augmented number theory versus dynamic number theory.

Two observations of [13] are relevant to this paper.

(1) The partial correctness theory of X:=FX* (i.e. the set of valid formulae $P \supset [X:=FX^*]Q$ where P,Q are formulae of first-order logic) is not r.e. (This is Theorem 16 of [13], and was proved in essence by showing that any set in the class Π_1^0 is reducible to this partial correctness theory.

(2) The axiom system of section 3.2 [13] for loop-free theory is sound, complete and effective.

In this paper we improve the Π_1^0 reduction in (1) to Π_2^0, still for the partial correctness theory of the same simple program. This implies the incompleteness of any axiom system in which theoremhood is not at least as hard to decide as membership in Π_2^0-complete sets. However, we also show that the partial correctness theory of all r.e. programs (the set of valid formulae $P \supset [\alpha]Q$ where α may be any r.e. program) is in Π_2^0, so no r.e. program has a more intractable partial correctness theory than $X:=FX^*$.

It follows from (1) that a sound, complete, effective axiom system for the valid formulae of dynamic (or even regular) logic is impossible. However, as we show in this paper, by taking all of first-order number theory as axioms, the extension of the axiom system to handle loops (also given in [13]) is sound and complete for regular number theory. The result also holds for regular augmented number theory when we take first-order augmented number theory as axioms. Along with [6], this is the first time a completeness result has been obtained for systems that treat termination, let alone for one with the generality of dynamic logic.

Computability

We can abbreviate the four theorems of this section as follows. The notation should be self-explanatory when read in conjunction with the following expanded statements of the theorems.

(1) $\{\vDash \langle\alpha\rangle P\} \equiv \Sigma_1^0$ $(\{\alpha\} \leqslant \text{r.e.})$

(2) $\{\vDash [\alpha]U\} \equiv \Pi_1^0$ $(\text{regular} \leqslant \{\alpha\} \leqslant \text{r.e.})$

(3) $\{\vDash [\alpha]P\} \equiv \Pi_2^0$ $(\text{regular} \leqslant \{\alpha\} \leqslant \text{r.e.})$

(4) $\{\vDash \exists Z[\alpha]P\} \equiv \Pi_1^1$ $(\text{regular} \leqslant \{\alpha\} \leqslant \text{r.e.})$

$\{\vDash D.\} \equiv \Pi_1^1$ $(\text{regular} \leqslant \{\alpha\} \leqslant \text{r.e.})$

$\{\vDash \langle\beta\rangle[\alpha]P\} \equiv \Pi_1^1$ $(\text{regular} \leqslant \{\alpha\},\{\beta\} \leqslant \text{r.e.})$

$\{\vDash \exists Z_1 Z_2[\alpha]F\} \equiv \Pi_1^1$ $(\text{regular} \leqslant \{\alpha\} \leqslant \text{r.e.})$

$\{\vDash \langle\beta\rangle[\alpha]F\} \equiv \Pi_1^1$ $(\text{regular} \leqslant \{\alpha\},\{\beta\} \leqslant \text{r.e.})$

Theorem 1. The valid formulae of dynamic logic of the form $\langle\alpha\rangle P$, where α is any r.e. program and P is a formula of first-order logic, form a complete r.e. set.

Proof. Note that just the valid formulae of first-order logic already form a complete r.e. set, that is, $\{\models P\} \equiv \Sigma_1^0$. So to prove the Σ_1^0-completeness of the set of valid formulae of the more general form $\langle\alpha\rangle P$, we need only prove that this set of valid formulae is r.e.

The validity of $\langle\alpha\rangle P$ amounts to the validity of an infinite disjunction of formulae $\langle\beta\rangle P$ where the β's are the denotations of the individual execution sequences of α. Each of these formulae may be expanded by Theorems 3 and 4 of [13] as formulae of first-order logic. Then the infinite disjunction is valid if and only if some finite subset of the disjunction is valid, by compactness of first-order logic. Since the disjunction is of an r.e. set of formulae, validity can be decided by enumerating elements of the disjunction until sufficiently many elements are present that their disjunction is valid. ∎

Theorem 2. The valid formulae of dynamic logic of the form $[\alpha]U$, where α is any r.e. program (alternatively α may be restricted to be any regular program) and U is any universally quantified formula of first-order logic, form a complete co-r.e. set.

Proof. The validity of $[\alpha]U$ amounts to the validity of an infinite conjunction of formulae $[\beta]U$, which as in Theorem 1 may be expanded as universally quantified formulae of first-order logic. Then to check their validity it suffices to check the validity of each of the conjuncts, a decidable question since the conjuncts are universally quantified. The set of conjuncts being r.e., this problem is in Π_1^0 and so the valid formulae form a co-r.e. set.

To see that the set is complete in Π_1^0, it suffices to choose U to be *false*, and allow α to range merely over regular programs. $[\alpha]$*false* is valid iff the uninterpreted flowchart scheme corresponding to α never halts. This problem for flowchart schemes is known to be Π_1^0-complete [11], and so $\{\models[\alpha]U\}$ is complete in Π_1^0 even when U is the fixed formula *false*. ∎

Theorem 3. The valid formulae of dynamic logic of the form $[\alpha]P$, where α is any r.e. program and P is a formula of first-order logic, form a Π_2^0-complete set. This result holds even if the class of programs permitted is taken to be as small as regular programs; in fact, just the single regular program X:=Y;X:=FX* will suffice to obtain the result.

Proof. (Sketch). The upper bound is proved exactly as for Theorem 2, with the remark that the validity of each conjunct is now only partially decidable since each conjunct is an arbitrary formula of first-order logic including existential quantifiers. This boosts the problem from Π_1^0 to Π_2^0.

For the lower bound, our strategy will be to reduce the totality problem for Turing machines whose inputs are given in unary notation to the validity problem for sentences $[\alpha](C \supset H)$ where α is the fixed program $X:=Y;X:=FX^*$. States satisfying C will be forced to represent a computation of the Turing machine, while H will assert that the computation halts.

Clearly $[\alpha]$ amounts to a universal quantifier "for all X in the set $S = \{Y, FY, F(FY), \ldots\}$," which if thought of as natural numbers has Y for 0 and F for successor. Let W be the formula $\forall Z(G(FZ)=Z \wedge FZ \neq Y)$; it should be evident that in every model of W, the set S is infinite.

Now consider the following more or less standard approach to showing that the validity problem for first-order logic is complete in Σ_1^0. Let R be a binary predicate symbol. Confine attention to the values of R on SxS, which we may think of as the positive quadrant of the two dimensional integer lattice. Take the rows of the lattice to be Turing machine i.d.'s (instantaneous descriptions) coded in binary in some way. (For definiteness, take R(i,j) to assert that cell (i,j) contains a 1.) It is tedious but straightforward to give a formula of first-order logic which forces adjacent rows of the lattice to describe i.d.'s the second of which is the result of running a given Turing machine for one step on the first. We can also say that a halting state appears on some row. Similarly we can give a formula that says that the beginning of the first row codes the start state of the Turing machine (indicating that at the start of a computation the Turing machine's head is at the beginning of the tape). And we can say that everywhere outside the head, consecutive pairs of bits in the first row have only the configurations 11, 00 and 10, and furthermore that 10 occurs exactly once, namely at position X. If X is in S, this means that the first row represents the initial i.d. on input X given in unary. Let H denote the statement that a halting state occurs on some row, and let C denote the conjunction of all the other statements we discussed, which will be a function of which Turing machine we had in mind. Then we claim that $[\alpha](C \supset H)$ is valid if and only if that Turing machine we had in mind halts on all inputs. If it is valid then it is valid in the universe in which S exhausts the domain; hence, H is true in a those states of the universe in which R represents computations starting at any X in S; this implies that the machine always halts. Now suppose that the machine always halts. Then there always exists a halting state when C is true and X is in S, whence $[\alpha](C \supset H)$ is always true, i.e. it is valid. ∎

Our use of nondeterminism in this proof was not essential. Let β be the deterministic program $X:=Y;(X \neq Z?;X:=FX)^*;X=Z$. Then for any formula P having no free occurrences of W, $[\alpha]P$ is equivalent to $\forall W[\beta]P$, whence $[\alpha]P$ is valid if and only if $[\beta]P$ is valid.

We regard Theorem 3 as significant because it indicates the extent of the difficulty of supplying complete axiomatizations for the true partial correctness assertions of the form $P\{\alpha\}Q$ even when P is just *true*. We

remark that the Π_2^0 upper bound of Theorem 3 can obviously be applied to partial correctness asertions of the general form $P \supset [\alpha]Q$.

Theorem 4. The set of valid formulae of dynamic logic of the form $\exists Z[\alpha]P$, where α may simply be the fixed program $X:=Y;X:=FX^*$ and P is any formula of first-order logic, is complete in Π_1^1. Further the set of valid formulae of dynamic logic is in Π_1^1.

The sudden jump in the complexity of validity is attributable to being able to state that the model is "standard", by allowing us to state as an hypothesis that for every element there exists a "standard" element equal to it. We may write this hypothesis as "$\forall Z\langle X:=Y;X:=FX^*\rangle X=Z$". Alternatively, to avoid non-deterministic programs we may write it as "$\forall Z\langle X:=Y;(X\neq Z?;X:=FX)^*;X=Z\rangle$ *true*", which says that every element can be found by searching from 0 deterministically. The upper bound of Π_1^1 is due in essence to the validity problem for "constructive" $L\omega_1\omega$ being in Π_1^1. ($L\omega_1\omega$ is first-order logic with infinite conjunctions and disjunctions permitted. By "constructive" $L\omega_1\omega$ we mean in this case that each set of infinite conjunctions or disjunctions is either a set of formulae of first order logic that is in Π_1^1 or a set of representations of formulae of constructive $L\omega_1\omega$ that is in Π_1^1.)

Some variations of this theorem are possible. For example, "$\exists Z$" can be replaced by "$\langle\beta\rangle$" for an appropriate choice of nondeterministic β. Alternatively, P (a general first-order formula) can be replaced by a quantifier-free formula provided two existentially quantified variables Z_1 and Z_2 are used. These variations can be applied simultaneously. We do not know whether "$\exists Z$" can be replaced by "$\langle\beta\rangle$" where β is deterministic. We leave the detailed proof of Theorem 4 and its variations to a later paper.

Completeness

In this section we prove that an axiomatization of regular number theory (that is, an axiom system whose theorems are among the N-valid formulae of dynamic logic with no non-zeroary function or predicate symbols save +, x, and =, and restricted to modalities with regular programs) that was given in [13] can be made complete simply by taking the formulae of number theory as further axioms. The same proof shows that the same axiom system completely axiomatizes regular augmented number theory (permitting other function and predicate symbols besides +, x and =) provided the formulae of augmented number theory are taken as axioms.

Cook [4] has used the notion of expressiveness to prove the completeness of what is essentially Hoare's axiom system, and not surprisingly our proof does so too. We say that a language L is as *U-expressive* as a language M when for every formula P of M there exists a formula Q of L such that $\vdash_U (P \equiv Q)$. We argue briefly here that (augmented) number theory is as N-expressive as regular (augmented) number theory. (We could of course replace "regular" by "r.e.", or even more, but since we only exhibit axioms for regular programs there is little point in our so doing.) For the purposes of this section, we take α^N to be the program that maps state $\mathcal{I}$ to the states that $\alpha \circ \alpha \circ \ldots \circ \alpha$ would map $\mathcal{I}$ to, where the number of α's is given by the value of N in $\mathcal{I}$. (N must be a zeroary function symbol which is not changed by α, nor does α depend on N.) The main point is that from Cook's expressiveness observation we can infer that if P is N-expressible in (augmented) arithmetic and α is a regular program then $[\alpha^N]P$ is N-expressible in (augmented) arithmetic, say as Q. Hence $\forall N Q$ N-expresses $[\alpha^*]P$ provided N does not occur free in P. Further, if Q' N-expresses $\langle \alpha^N \rangle P$ then $\exists N Q'$ N-expresses $\langle \alpha^* \rangle P$.

We reproduce here the axiom system that appears in section 3.2 of [13] and refer to it henceforth as P. It is of interest inasmuch as it is the appropriate generalization of conventional axiom systems for pure first-order logic.

Logical Axioms

All tautologies of Propositional Calculus.

$[\alpha](P \supset Q) \supset ([\alpha]P \supset [\alpha]Q)$.

Logical Inference Rules

$P, P \supset Q \vdash Q$.

$P \vdash [\alpha]P$ (subsumes $P \vdash \forall x P$).

Non-logical Axioms

$\forall X P \supset P_X^T$ any term T — $\forall$ Performance Axiom.

$P \supset \forall X P$ (P has no free occ. of X) — $\forall$ Invariance Axiom.

$[P]Q \equiv P \supset Q$ — Test Axiom.

$[F(\underline{S}) := T]P \equiv P'$ (See [13] for details) — Assignment Axiom.

$[\alpha \cup \beta]P \equiv [\alpha]P \wedge [\beta]P$ — Union Axiom.

$[\alpha \circ \beta]P \equiv [\alpha][\beta]P$ — Composition Axiom.

Rules for $*$

$P \supset [\alpha]P \vdash P \supset [\alpha^*]P$ — Rule of Invariance.

$P_N^{N+1} \supset \langle \alpha \rangle P \vdash P \supset \langle \alpha^* \rangle P_N^0$ — Rule of Convergence.

A detailed discussion of these axioms appears in [13]. Here it suffices to observe that the first six axioms and rules, down to $P \supset \forall XP$, constitute a complete axiom system for classical pure predicate calculus. Together with the next four equivalences, they constitute a complete axiomatization of loop-free theory. Our objective now is to show that the whole system above, together with all the N-valid formulae of arithmetic as axioms, is a complete axiom system for regular number theory. The same proof will serve to show that when the N-valid formulae of augmented arithmetic are taken as axioms, the axiom system is complete for regular augmented number theory. We will not further consider the augmented case; however we note here that the augmented case falls much higher in the hierarchy of degrees of unsolvability and so it is interesting that the same proof applies.

The main result of this section is proved by a variant of the Star Interpolation Theorem (Theorem 24 of [13]). That theorem stated in essence that $[\alpha^*]P$ and $\langle\alpha^{*-}\rangle P$ (where for a program β, β^- is the converse relation: $\mathcal{I}\beta\mathcal{J}$ iff $\mathcal{J}\beta^-\mathcal{I}$) were both invariants of α, which is obvious when one writes $[\alpha^*]P \supset [\alpha][\alpha^*]P$, and (not quite so obviously)

$$\langle\alpha^{*-}\rangle P \supset [\alpha]\langle\alpha^-\rangle\langle\alpha^{*-}\rangle P \supset [\alpha]\langle\alpha^{*-}\rangle P$$

We prove another Star Interpolation Theorem in this paper which interpolates, not invariants, but rather what we call convergents, which are to termination (and in the case of deterministic programs, to total correctness) what invariants are to partial correctness.

In the following we redefine some concepts from [13] in such a way as to make clear the relationship between Cook's completeness result for partial correctness alone and our completeness result for regular number theory, of which partial correctness and termination assertions are very special cases.

Note that $\models(P \supset [\alpha]Q)$ expresses the same thing as Hoare's $P\{\alpha\}Q$. Whenever $P\{\alpha\}Q$ holds, we may call P a *box antecedent* of Q via α, and Q a *box consequent* of P via α. Since $\models([\alpha]Q \supset [\alpha]Q)$, it follows that $[\alpha]Q$ must be the *weakest* box antecedent of Q via α (since for any antecedent P, $P \supset [\alpha]Q$ is valid).

Analogous to the partial correctness assertion $P \supset [\alpha]Q$ is the formula $P \supset \langle\alpha\rangle Q$, which asserts that if P holds α can terminate and satisfy Q (if α is deterministic, i.e. is a function, this asserts the total correctness of α). We can call $\langle\alpha\rangle Q$ a *weakest diamond antecedent* of Q via α.

We define an *invariant* of α to be any formula P such that $P \supset [\alpha]P$ is N-valid.

Weakest Invariant Lemma. $[\alpha^*]P$ (the weakest box antecedent of P via α^*) is the weakest invariant of α that implies P.

Proof. Since $\alpha \circ \alpha^* \subseteq \alpha^*$, $[\alpha^*]P \supset [\alpha][\alpha^*]P$ is valid, $[\alpha^*]P$ is an invariant of α. Further, since $I \subseteq \alpha^*$, $[\alpha^*]P \supset P$ (I is the identity relation) so it implies P. Finally, suppose $Q \supset [\alpha]Q$ and $Q \supset P$. Then $Q \supset [\alpha^*]Q \supset [\alpha^*]P$, so $[\alpha^*]P$ is the weakest such. ∎

We say that an invariant Q of α is an *invariant interpolate* of two formulae P and R via α, when $P \supset Q \supset R$ is valid.

Invariant Interpolation Lemma. If $P \supset [\alpha^*]R$ then $[\alpha^*]R$ is an invariant interpolate of P and R via α.

Proof. It is an invariant of α by the above lemma. Further, $P \supset [\alpha^*]R$ (hypothesis), and $[\alpha^*]R \supset R$ ($I \subseteq \alpha^*$). ∎

Just as the diamond antecedent was the analogue of the box antecedent, so do we have an analogue of the notion of invariant. We call Q a *convergent* of α when $Q' \supset \langle\alpha\rangle Q$ is valid, (where Q' is Q_N^{N+1}, which substitutes N+1 for all free occurrences of N in Q) and say that the convergent Q of α is a *convergent interpolate* of P and R when $P \supset \exists N(Q)$ and $Q_N^0 \supset R$. The interest in convergents is that they allow us to prove that a loop can eventually terminate with the right answer, just as invariants allow us to prove that a terminating loop always yields the right answer. In the case of deterministic programs, convergents subsume invariants, since for deterministic α, $\langle\alpha\rangle P \supset [\alpha]P$. Note that convergents and convergent interpolates are defined differently from invariants and invariant interpolates to permit the following lemmas, though when Q has no free occurrences of N these differences vanish except for the use of $\langle\rangle$ for $[]$.

Convergent Lemma. $\langle\alpha^N\rangle P$ is a convergent of α.

Proof. $\langle\alpha^{N+1}\rangle P \supset \langle\alpha\rangle\langle\alpha^N\rangle P$. ∎

Convergent Interpolation Lemma. If $P \supset \langle\alpha^*\rangle R$ then $\langle\alpha^N\rangle R$ is a convergent interpolate of P and R.

Proof. $P \supset \exists N \langle\alpha^N\rangle R$ and $\langle\alpha^0\rangle R \supset R$. ∎

We now prove that the axiom system P for regular number theory given at the beginning of this section is sound and complete when number theory is taken as additional axioms. We leave to the reader the task of

showing that P is sound. The proofs of the following three theorems deal with the completeness of P. They depend on our notion of expressiveness discussed at the beginning of this section.

Write P without the Rule of Invariance as $P\langle\rangle$, and without the Rule of Convergence as $P[]$.

Box Completeness Theorem. For any first-order formulae P and R, and for any α, $\vdash_N P \supset [\alpha]R$ iff $\vdash_{P[]} P \supset [\alpha]R$.

Proof. The result follows by induction on the number of *'s in α together with the fact that for $\alpha = \beta^*$, $[\beta^*]R$ is an invariant interpolate of P and R via β (by the Invariant Interpolation Lemma). By expressiveness, $[\beta^*]R$ is equivalent to some formula F of arithmetic, and hence $\vdash_N F \supset [\beta]F$. By the inductive hypothesis $\vdash_{P[]} F \supset [\beta]F$, and so by the Rule of Invariance $\vdash_{P[]} F \supset [\alpha]F$, and using logical axioms, modus ponens and $P \supset F$ and $F \supset R$ (valid by the definition of F, and hence axioms of arithmetic), we can obtain $P \supset [\alpha]R$. ∎

Diamond Completeness Theorem. For any first-order formulae P and R, and for any α, $\vdash_N P \supset \langle\alpha\rangle R$ iff $\vdash_{P\langle\rangle} P \supset \langle\alpha\rangle R$.

Proof. Again induction may be used on the number of *'s in α together with the fact that for $\alpha = \beta^*$, $\langle\beta^N\rangle R$ is a convergent interpolate of P and R via β (by the Convergent Interpolation Lemma), which implies that the Rule of Convergence can be applied. Similarly, in this case $\langle\beta^N\rangle R$ is equivalent to a formula of arithmetic. We can now continue as in the previous proof using $P \supset \exists N \langle\beta^N\rangle R$ and $\langle\beta^0\rangle R \supset R$. ∎

Main Completeness Theorem. For any formula P of regular arithmetic, $\vDash_N P$ iff $\vdash_P P$.

Proof. Again we appeal to the expressiveness of arithmetic, this time with respect to formulae of dynamic logic by a trivial argument on the depth of nesting of modalities. This implies that for any formula P there exists a formula L(P) of arithmetic such that $\vDash_N P \equiv L(P)$. We say that P is in conjunctive normal form when the argument of each $\neg$ is an atomic formula and the arguments of each $\vee$ are not conjuncts. Appealing to the evident completeness of our system for Propositional Calculus, we may assume that P is given in conjunctive normal form with n modalities, such that $\vDash_N P$. We proceed by induction on the number n of modalities in P. The case n = 1 can easily be seen to follow from the previous two theorems. Now assume the theorem holds for any formula with n-1 or less modalities. Observing that if $\vDash_N P_1 \wedge P_2$ then $\vDash_N P_1$ and $\vDash_N P_2$, we can restrict our discussion to

a single disjunction. Without loss of generality we can assume P to be of the form $P_1 \vee m(\alpha)P_2$ where $m(\alpha)$ is $[\alpha]$ or $\langle\alpha\rangle$. We have $\vdash_N P_1 \vee m(\alpha)P_2$ and therefore $\vdash_N \neg L(P_1) \supset m(\alpha)L(P_2)$. Applying the appropriate of the two previous theorems we obtain $\vdash_P \neg L(P_1) \supset m(\alpha)L(P_2)$. Obviously by the definition of L(P) we have $\vdash_N \neg P_1 \supset \neg L(P_1)$ and $\vdash_N L(P_2) \supset P_2$. Both these last formula have less than n modalities, hence by the inductive hypothesis $\vdash_P \neg P_1 \supset \neg L(P_1)$ and $\vdash_P L(P_2) \supset P_2$. Applying the rule $P \vdash [\alpha]P$ we obtain $\vdash_P [\alpha](L(P_2) \supset P_2)$. We now apply modus ponens and either the axiom $[\alpha](P \supset Q) \supset ([\alpha]P \supset [\alpha]Q)$, if m(a) is [a], or the theorem $[\alpha](P \supset Q) \supset (\langle\alpha\rangle P \supset \langle\alpha\rangle Q)$, if m(a) is $\langle a\rangle$, to obtain $\vdash_P m(\alpha)L(P_2) \supset m(\alpha)P_2$. Easy applications of modus ponens now give $\vdash_P \neg P_1 \supset m(\alpha)P_2$ or equivalently $\vdash_P P_1 \vee m(\alpha)P_2$. ∎

The Diamond Completeness Theorem can be regarded as establishing the completeness of a system for proving total correctness of programs, if α is restricted to be deterministic. This provides a completeness proof for the Burstall-Manna-Waldinger technique [3,12], which essentially is an informal description of the method of proving $P \supset \langle\alpha\rangle R$, which is incorporated in *P*. Basu and Yeh [2] have the same notion for convergents; however they do not envisage the application for it that we have presented here. In a future paper, we hope to clarify in more detail the relationships between these and other techniques for proving total correctness of programs.

We conclude this section with the following observations which serve to formalize the dual notions of "weakest antecedents" and "strongest consequents" for box-formulae, which appear in the literature.

Duality Lemma. $P \wedge \langle\alpha\rangle Q$ and $\langle\alpha^-\rangle P \wedge Q$ are equally satisfiable.

Proof. $\exists \mathcal{I}\mathcal{J}(\mathcal{I} \models P \wedge \mathcal{I}\alpha\mathcal{J} \wedge \mathcal{J} \models Q)$ asserts the satisfiability of each of the two formulae. ∎

Duality Principle. $\models (P \vee [\alpha]Q) \equiv \models ([\alpha^-]P \vee Q)$.

Proof. Take the Boolean dual of satisfiability, $\wedge$, and $\langle\alpha\rangle$ in the duality lemma. ∎

Corollary. $\models (P \supset [\alpha]Q) \equiv \models (\langle\alpha^-\rangle P \supset Q)$.

Corollary. $\models (P \supset [\alpha]\langle\alpha^-\rangle P)$ (as remarked earlier).

Note now, that $\models (\langle\alpha^-\rangle P \supset Q)$, besides $\models (P \supset [\alpha]Q)$ expresses Hoare's $P\{\alpha\}Q$, and that $\langle\alpha^-\rangle P$ is the strongest box consequent of P

via α, which leads us to ask for a strongest diamond consequent. Unfortunately the Duality Principle does not hold for $\langle\alpha\rangle$ in place of $[\alpha]$, as can be checked with $P = \neg Q = true$, $\alpha = \varphi$ (the empty program), for which $\models(true \vee \langle\varphi\rangle false)$ holds but $\models(\langle\varphi^-\rangle true \vee false)$ does not. That is, $[\alpha^-]P$ is not even a diamond consequent of P via α (since the above is a counterexample to $P \supset \langle\alpha\rangle[\alpha^-]P$), let alone a strongest diamond consequent. The conclusion is that termination is not exactly the dual of partial correctness: weakest diamond antecedents are given by $\langle\alpha\rangle Q$ but strongest diamond consequents are not given by $[\alpha^-]P$. We do have however:

Strongest Invariant Lemma. $\langle\alpha^{*-}\rangle P$ (the strongest box consequent of P via α^*) is the strongest invariant of α implied by P.

Proof. Since $\alpha^- \circ \alpha^{*-} \subseteq \alpha^{*-}$, $\langle\alpha^-\rangle\langle\alpha^{*-}\rangle P \supset \langle\alpha^{*-}\rangle P$ is valid, so $\langle\alpha^{*-}\rangle P \supset [\alpha]\langle\alpha^{*-}\rangle P$ by the Duality Principle, so $\langle\alpha^{*-}\rangle P$ is an invariant of α. Further, $P \supset \langle\alpha^{*-}\rangle P$. Finally, if $Q \supset [\alpha]Q$ and $P \supset Q$ then $Q \supset [\alpha^*]Q$, so $\langle\alpha^{*-}\rangle Q \supset Q$, so $\langle\alpha^{*-}\rangle P \supset \langle\alpha^{*-}\rangle Q \supset Q$. ∎

We therefore conclude also that whenever $P \supset [\alpha^*]R$ holds, $\langle\alpha^{*-}\rangle P$ (besides $[\alpha^*]R$) is an invariant interpolate of P and R via α. This last fact implies that $\langle\alpha^{*-}\rangle P$ could have been used in the proof of the Box-Completeness Theorem, as in fact is done by Cook [4].

Acknowledgments

Jerry Schwarz pointed out the absence of an induction axiom in an earlier version of our axiom system, prompting us to include the Rule of Convergence, without which half of this paper would not have been written. We had valuable discussions with R. Burstall, M. Fischer, R. Ladner, S. Litvintchouk, R. Milner, G. Plotkin, and R. Rivest.

References

[1] de Bakker, J.W., and W.P. de Roever. A calculus for recursive program schemes. in *Automata, Languages and Programming* (ed. Nivat), 167-196. North Holland, 1972.

[2] Basu, S. K. and R. T. Yeh. Strong Verification of Programs. IEEE Trans. Software Engineering, SE-1, 3, 339-345. Sept. 75.

[3] Burstall, R.M. Program Proving as Hand Simulation with a Little Induction. IFIP 1974, Stockholm.

[4] Cook, S.A. Soundness and Completeness of an Axiom System for Program Verification. TR-95, Department of Computer Science, University of Toronto, 1976, 37pp. (Note: this is a revision of "Axiomatic and Interpretive Semantics for an Algol Fragment", TR-79, 1975)

[5] Dijkstra, E. *A Discipline of Programming.* Prentice-Hall, Englewood Cliffs, N.J. 1976.

[6] Harel, D., A. Pnueli and J. Stavi. A complete axiomatic system for proving deductions about recursive programs. Proc. Ninth Ann. ACM Symp. on Theory of Computing, Boulder, Col., May 1977.

[7] Hitchcock, P. and D. Park. Induction Rules and Termination Proofs. In *Automata, Languages and Programming* (ed. Nivat, M.), IRIA. North-Holland, 1973.

[8] Hoare, C.A.R. An Axiomatic Basis for Computer Programming. CACM *12*, 576-580, 1969.

[9] Hughes, G.E. and M.J. Cresswell. *An Introduction to Modal Logic.* London: Methuen and Co Ltd. 1972.

[10] Kripke, S. Semantical considerations on Modal Logic. Acta Philosophica Fennica, 83-94, 1963.

[11] Luckham, D., D. Park and M. Paterson. On Formalized Computer Programs. J.CSS *3*, 2, 119-127. May 1970.

[12] Manna, Z. and R. Waldinger. Is "sometime" sometimes better than "always"? Intermittent assertions in proving program correctness. Proc. 2nd Int. Conf. on Software Engineering, Oct. 1976.

[13] Pratt, V.R. Semantical Considerations on Floyd-Hoare Logic. 17th IEEE Symposium on Foundations of Computer Science, Oct. 1976.

[14] Rogers, H. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, 1967.

[15] Tarski, A. The semantic conception of truth and the foundations of semantics. Philos. and Phenom. Res, *4*, 341-376, 1944.