Notre Dame Journal of Formal Logic
Volume 26, Number 1, January 1985

A Completeness Theorem for Dynamic Logic

LÁSZLÓ CSIRMAZ

Introduction Let t be a similarity type and denote by F_t^n the set of first-order formulas of type t which have their free variables among $\{x_i : i < n\}$. Let $\theta \subset F_t^0$ be a fixed consistent theory. A program (or rather a program scheme as defined in [11]) is a prescription which defines the possible next moment states from the present state, i.e., the program is a state transducer. (A state can be imagined as the collection of the contents of the memory registers used by the program.) If this prescription is not unique, i.e., if the program executor may choose more than one possibility, then the program is said to be nondeterministic. We are interested only in programs which can be represented by a formula $\phi \in F_t^{2n}$ with $n > 0$ and $\theta \vdash \forall x \exists y \phi(x,y)$. The states are the n-tuples of the elements of the underlying set A of some t-type structure $\mathbf{A}$ for which $\mathbf{A} \models \theta$ holds. The state $y \in A^n$ is a possible successor of the state $x \in A^n$ iff $\mathbf{A} \models \phi(x,y)$. The constraints $\mathbf{A} \models \theta$ and $\theta \vdash \forall x \exists y \phi(x,y)$ ensure that for every state there exists at least one successor state.

Particularly, the so-called *while*-programs with random assignments of the form $x := ?$ (meaning: set x to any value in the domain; cf. [9]) are of this kind, provided there are infinitely many definable elements in θ (cf. [1], [2], [12]).

The function $R : \omega \to A^n$ is a *standard run* of the program ϕ, if $\mathbf{A} \models \phi(R(i), R(i+1))$ for every $i \in \omega$. The run *halts* at the i-th step if $R(i) = R(i+1)$. A run, of course, may have several different halting configurations. Detailed intuitive motivations for these definitions can be found in [3], [5], and [12].

Given two formulas, ϕ_{in} and ϕ_{out} of F_t^n (called the input and output assertion, respectively), the program ϕ is partially correct with respect to ϕ_{in} and ϕ_{out} if for every t-type model $\mathbf{A}$ of θ and for every run $R : \omega \to A^n$, $\mathbf{A} \models \phi_{in}(R(0))$ and $R(i) = R(i+1)$ imply $\mathbf{A} \models \phi_{out}(R(i))$.

The inductive assertion method introduced by Floyd [7] and reformulated later by Hoare [10] is the most commonly used method for proving partial

Received June 6, 1982; revised January 9, 1984

correctness of programs. In our case this method can be restated as follows: Suppose there is a formula $\Phi \in F_t^n$ such that (i)–(iii) below are satisfied. Then the program ϕ is partially correct with respect to ϕ_{in} and ϕ_{out}.

(i) $\theta \vdash \phi_{in}(x) \to \Phi(x)$
(ii) $\theta \vdash \Phi(x) \wedge \phi(x,y) \to \Phi(y)$
(iii) $\phi \vdash \Phi(x) \wedge \phi(x,x) \to \phi_{out}(x)$.

In general the converse implication fails (see, e.g., [1]). One of the possible explanations of the fact is that the "time-structure" ω in the definition of the run is first-order undefinable (cf. [2], [8]). The aim of this paper is to give an alternative definition for the "run" of a program, essentially by allowing other time-structures, and to prove that under the new definition a completeness theorem holds, i.e., the new partially correct programs are exactly those which are Floyd-Hoare derivable. These results as well as the method are natural extensions of those in [5], and the theorems have an extensive application in the dynamic logic of programs in [3] and [12]. These two papers make heavy use of our results. In [6] a somewhat stronger result was stated for deterministic programs allowing an ordering in the time-structure. The proof, however, contains an error.

1 Notation, definitions The structure $\mathbf{I}$ with underlying set I is a *time-structure* if it is of similarity type $\langle s, 0\rangle$ where 0 is a constant symbol and s is the successor function and if the following (infinitely many) sentences are valid in $\mathbf{I}$:

$sx = sy \to x + y$
$sx \neq 0$
$x \neq 0 \to \exists y(sy = x)$
$x \neq s^k x$ for $k = 1, 2, \ldots$.

Every time-structure is an elementary extension of the standard time structure $\mathbf{I}_0 = \langle \omega, ', 0\rangle$ where the prime denotes the usual successor function. The elements of the underlying set of the time-structures are denoted by the letter i.

If t_1 and t_2 are similarity types, $t_1 < t_2$ means that t_1 and t_2 have the same function and relation symbols with the same arities, and every constant symbol of t_1 is a constant symbol of t_2.

In the sequel we fix the similarity type τ, the consistent theory $\theta \subset F_\tau^0$, the natural number $n > 0$, and the formulas ϕ_{in}, $\phi_{out} \in F_\tau^n$, and $\phi \in F_\tau^{2n}$. We assume that ϕ is a nondeterministic program in θ, i.e.,

$$\theta \vdash \forall x \exists y \phi(x,y) \ .$$

Definition 1.1 The program ϕ is Floyd-Hoare derivable with respect to ϕ_{in} and ϕ_{out} (in symbols $\theta \vdash (\phi_{in}, \phi, \phi_{out})$) if there is a formula $\Phi \in F_\tau^n$ such that

$\theta \vdash \phi_{in}(x) \to \Phi(x)$
$\theta \vdash \Phi(x) \wedge \phi(x,y) \to \Phi(y)$
$\theta \vdash \Phi(x) \wedge \phi(x,x) \to \phi_{out}(x)$.

Definition 1.2 Let $\mathbf{A}$ be a τ-type model of the theory θ, and $\mathbf{I}$ be a time-structure. The function $R: I \to A^n$ is a run of the program ϕ, if the following conditions hold:

(i) R describes a step-by-step execution of ϕ, i.e., for every $i \in I$ we have $\mathbf{A} \models \phi(R(i), R(si))$.

(ii) for every $\Phi \in F^{n+m}$ and $u \in A^m$, if $\mathbf{A} \models \Phi(R(0), u)$ and $\mathbf{A} \models \bigwedge_{i \in I} [\Phi(R(i), u) \to \Phi(R(si, u)]$ then $\mathbf{A} \models \bigwedge_{i \in I} \Phi(R(i), u)$.

The time structure $\mathbf{I}$ should not be connected, i.e., there can be time points $i, j \in I$ such that $i \neq s^k j$ and $j \neq s^k i$ for every $k \in \omega$. To connect the states $R(i)$ and $R(j)$ we have to make other constraints beyond (i). The most natural and, so far, the most successful one is requiring the induction principle: if some formula holds at the beginning, and for each $i \in I$ it inherits from i to the successor time point si then the formula should always hold. In (ii) this principle is stated, u is the parameter of the induction. The theorem below holds also if parameters are not allowed. In the other direction, the theorem can be strengthened slightly. If we merge the structures $\mathbf{I}$ and $\mathbf{A}$ and the function R into a 2-sorted structure then we could speak about induction over 2-sorted formulas. As a corollary not proved here, the theorem remains valid if we require the induction principle to hold for every 2-sorted formula containing no quantifier on time variables (possibly with parameters), but no longer valid if either the Σ_1^I or the Π_1^I formulas are in the scope of the induction.

Definition 1.3 The program ϕ is partially correct with respect to ϕ_{in} and ϕ_{out} (in symbols $\theta \models (\phi_{in}, \phi, \phi_{out})$) if for every τ-type model $\mathbf{A}$ of θ, for every time-structure $\mathbf{I}$, and for every run $R: I \to A^n$ of ϕ, if $\mathbf{A} \models \phi_{in}(R(0))$ then

$$\mathbf{A} \models \bigwedge_{i \in I} [R(i) = R(si) \to \phi_{out}(R(i))] \ .$$

2 The result In the remainder of the paper we prove the following:

Theorem $\theta \models (\phi_{in}, \phi, \phi_{out})$ *if and only if* $\theta \vdash (\phi_{in}, \phi, \phi_{out})$.

Proof: The "if" part of this theorem is trivial. Assume now that the program is partially correct. We look for a derivation, and distinguish two cases. Let

$$H = \{\Phi \in F^n : \theta \vdash \phi_{in}(x) \to \Phi(x), \text{ and } \theta \vdash \Phi(x) \wedge \phi(x, y) \to \Phi(y)\} \ ,$$

the set of candidates for a Floyd-Hoare derivation. Let c and d each denote n new different constant symbols not in τ. Note that H is closed under conjunction, i.e., if Φ_1 and $\Phi_2 \in H$ then $\Phi_1 \wedge \Phi_2 \in H$.

Case I. In every model of the theory

$$\{\theta, \phi_{in}(c), H(d), \phi(d, d)\}$$

the formula $\phi_{out}(d)$ is valid. Then, by Gödel's Completeness Theorem and by the fact that H is closed under conjunction, there is a $\psi \in H$ such that

$$\theta \vdash [\phi_{in}(c) \wedge \psi(d) \wedge \phi(d,d)] \rightarrow \phi_{out}(d) \ .$$

The constants c and d do not occur in θ so introducing $\Phi(x) \equiv \exists y\ \phi_{in}(y) \wedge \psi(x)$, we get

$$\theta \vdash [\Phi(x) \wedge \phi(x,x)] \rightarrow \phi_{out}(x) \ .$$

This and the obvious $\Phi \in H$ show the derivability of $(\phi_{in}, \phi, \phi_{out})$.

Case II. Not the case above, i.e.,

$$Con\{\theta, \phi_{in}(c),\ H(d),\ \phi(d,d),\ \neg\phi_{out}(d)\} \ .$$

Our aim is to construct a model of θ and a run of ϕ in this model which show that ϕ is not partially correct. To achieve this goal, first we define the syntactical notion of *prerun* instead of the semantical notion of run. We do not require the induction principle to hold, instead we list a set of formulas that should be valid at every time point, and we claim their consistency. Then we pick new constant symbols to denote the first ω states of the wanted run, and show that they, together with the halting configuration d, form a prerun. The crucial part of the proof is Lemma 2.4. Here we show how to extend a prerun to satisfy all parameterless induction with basic formula from the old signature. Finally, we build up an ω-high tower of preruns the union of which is the desired run. For the undefined notions consult [4].

Definition 2.1 Let t be a similarity type and $T \subset F_t^0$ be a theory. The pair $R = \langle \mathbf{I}_R, f_R \rangle$ is a (t,T)-prerun, if $\mathbf{I}_R \succ \mathbf{I}_0$ is a time-structure with the underlying set $I_R \supseteq \omega$, and f_R is a function which assigns to every $i \in I_R$ an n-tuple of constants of t in such a way that (i) and (ii) below are satisfied. A bit loosely, but not ambiguously, we write $R(i)$ everywhere instead of $f_R(i)$. Let

$$B_T^t = \left\{ \Phi \in F_t^n : \text{there exists } k \in \omega - \{0\} \text{ such that } T \vdash \bigwedge_{i<k} \Phi(R(i)), \text{ and } T \vdash \left[\bigwedge_{i<k} \Phi(x_i) \wedge \phi(x_i, x_{i+1}) \right] \rightarrow \Phi(x_k) \right\} \ ,$$

and $B_T^t(x) = \{\Phi(x) : \Phi \in B_T^t\}$. The conditions are:

(i) $T \vdash \phi(R(i), R(si))$ for every $i \in I_R$

(ii) $Con\left(T \cup \bigcup \{B_T^t(R(i)) : i \in I_R\}\right)$.

In fact, the set B_T^t depends not only on t and T, but also on the first ω values of the function f_R. These values, however, are omitted from the denotation since they will be the same for every prerun occurring in the proof. Note that the set B_T^t is also closed under conjunction, a fact which will be used tacitly many times.

Lemma 2.2 *Let R be a (t,T)-prerun. Then there exists a complete theory S such that $T \subseteq S \subset F_t^0$ and R is a (t,S)-prerun.*

Proof: It suffices to show that for any $\beta \in F_t^0$, R is either a $(t, T \cup \{\beta\})$ or a $(t, T \cup \{\neg\beta\})$-prerun. If neither of these holds then in both cases (ii) of Definition 2.1 is violated. This means that there are formulas $\Phi_1 \in B^t_{T\cup\{\beta\}}$ and $\Phi_2 \in B^t_{T\cup\{\neg\beta\}}$ and a finite $J \subset I_R$ such that

$$T \cup \{\beta\} \vdash \neg \bigwedge_{i\in J} \Phi_1(R(i))$$

$$T \cup \{\neg\beta\} \vdash \neg \bigwedge_{i\in J} \Phi_2(R(i)) \ .$$

From these we get

$$T \vdash \neg \bigwedge_{i\in J} [\beta \to \Phi_1(R(i))] \wedge [\neg\beta \to \Phi_2(R(i))] \ .$$

But $\psi(x) \equiv [\beta \to \Phi_1(x)] \wedge [\neg\beta \to \Phi_2(x)] \in B^t_T$, therefore the assumption in the lemma gives $Con\left(T, \bigwedge_{i\in J} \psi(R(i))\right)$, a contradiction.

Lemma 2.3 *Let R be a (t, T)-prerun, and let T be complete. Then there exist a type $r > t$ and a theory $S \subset F_r^0$ such that*

(i) *$T \subseteq S$, S is complete*
(ii) *R is an (r, S)-prerun*
(iii) *for every $\Psi \in F_t^1$, if $T \vdash \exists x \Psi(x)$, then for some constant c from r we have $S \vdash \Psi(c)$.*

Proof: What we have to prove is the following: Suppose the type r contains the extra constant symbol c only, $\beta \in F_t^1$, and $Con(T, \beta(c))$. Then R is an $(r, T \cup \{\beta(c)\})$-prerun. If this is not the case, then there are $\Phi \in F_t^{n+1}$ and a finite $J \subset I_R$ such that

(1) $T \cup \{\beta(c)\} \vdash \neg \bigwedge_{i\in J} \Phi(R(i), c)$

and $\Phi(x, c) \in B^r_{T\cup\{\beta(c)\}}$. From this latter condition we get

$$\forall y(\beta(y) \to \Phi(x, y)) \in B^t_T \ .$$

On the other hand, T is complete, therefore $B^t_T(R(i)) \subset T$; i.e.,

$$T \vdash \bigwedge_{i\in J} \forall y(\beta(y) \to \Phi(R(i), y)) \ .$$

From this and from (1), $T \vdash \neg\beta(c)$, contradicting the assumption $Con(T, \beta(c))$.

In the next lemma we extend a prerun in such a way that in the extension the validity of the induction principle for each old formula is explicitly stated either by negating one of the premisses (cases a and b), or by putting all of the consequences into the new theory (case c).

Lemma 2.4 *Let R be a (t, T)-prerun and let T be complete. Then there exist a type $r > t$, a theory $T \subseteq S \subset F_r^0$, and an (r, S)-prerun Q such that*

(i) $\mathbf{l}_Q > \mathbf{l}_R$, and $Q \supseteq R$, i.e., $R(i) = Q(i)$ for every $i \in I_R \subseteq I_Q$

(ii) for every $\Phi \in F_t^n$ at least one of the following holds:
   a. $S \vdash \neg\Phi(Q(0))$
   b. $S \vdash \Phi(Q(i)) \wedge \neg\Phi(Q(si))$ for some $i \in I_Q$
   c. there exists $\chi \in B_T^t$ such that $T \vdash \forall x(\chi(x) \to \Phi(x))$ and $S \vdash \Phi(Q(i))$ for every $i \in I_Q$.

Proof: T is complete therefore $B_T^t(R(i)) \subset T$ for every $i \in I_R$. Let $\Delta \subset F_t^n$ be the set of formulas δ for which

(2) $T \vdash \delta(R(i))$ for every $i \in \omega \subset I_R$

(3) $T \nvdash \left[\bigwedge_{i<k} \Phi(x_i) \wedge \delta(x_i) \wedge \phi(x_i, x_{i+1})\right] \to \delta(x_k)$ for every $k \in \omega - \{0\}$ and $\Phi \in B_T^t$.

Let Z denote the set of integers, and let $I_Q = I_R \cup \Delta \times Z$. If we define the function s on $I_Q - I_R$ by $s(\delta, j) = (\delta, j+1)$, then we get a time-structure $\mathbf{I}_Q$ for which $\mathbf{I}_Q \succ \mathbf{I}_R$.

Let $c_{\delta,j}$ be n new constant symbols for every $\delta \in \Delta$ and $j \in Z$, and let the type r be the enlargement of t by these constants. Let the function Q be defined by

$$Q(i) = \begin{cases} R(i) & \text{if } i \in I_R \\ c_{\delta,j} & \text{if } i = (\delta, j) \in I_Q - I_R \end{cases},$$

and finally let the theory $S \subset F_r^0$ be

$$S = T \cup \bigcup \{B_T^t(c_{\delta,j}) \cup \{\delta(c_{\delta,0}),\ \neg\delta(c_{\delta,1}),\ \phi(c_{\delta,j},\ c_{\delta,j+1})\} : \delta \in \Delta, j \in Z\} \ .$$

We claim that S is consistent. It suffices to show that T is consistent with any finite part of the big union. Because T is complete, we may assume that there is only one $\delta \in \Delta$ which occurs as index in this finite part, and, because B_T^t is closed under conjunction, we may assume that only one $\Phi \in B_T^t$ occurs. Using the definition of B_T^t and the fact that $T \vdash \forall x \exists y\ \phi(x, y)$, it suffices to show

$$Con\left(T,\ \bigwedge_{i<k} [\Phi(c_{\delta,-i}) \wedge \phi(c_{\delta,-i}, c_{\delta,-i+1})],\ \delta(c_{\delta,0}),\ \neg\delta(c_{\delta,1})\right)$$

for every $k > 0$ and $\Phi \in B_T^t$. But T is complete, therefore from (3)

$$T \vdash \exists x_0 \ldots \exists x_k \left[\bigwedge_{i<k} \Phi(x_i) \wedge \delta(x_i) \wedge \phi(x_i, x_{i+1})\right] \wedge \neg\delta(x_k) \ ,$$

which gives the wanted consistency.

Next we prove that Q satisfies (i) and (ii). (i) is trivial from the construction. For (ii) let $\Phi \in F_t^n$ be arbitrary. If there is an $i \in \omega$ such that $T \nvdash \Phi(R(i))$ then, since T is complete, $T \subseteq S$ and $R(i) = Q(i)$, we have $S \vdash \neg\Phi(Q(i))$, i.e., either case a or case b holds. If not, then we have two cases. Either there are $k > 0$ and $\psi \in B_T^t$ such that

$$T \vdash \left[\bigwedge_{i<k} \psi(x_i) \wedge \Phi(x_i) \wedge \phi(x_i, x_{i+1})\right] \to \Phi(x_k)$$

or there is no such pair. In the first case $\chi(x) \equiv \psi(x) \wedge \Phi(x) \in B_T^t$ and case c holds. In the second case $\Phi \in \Delta$, therefore $\Phi(c_{\Phi,0}) \in S$ and $\neg\Phi(c_{\Phi,1}) \in S$, i.e., case b holds.

Finally we prove that Q is an (r,S)-prerun. Definition 2.1(i) is immediate, and (ii) follows from $B_S^r(Q(i)) \subset S$. To prove this inclusion, let $\Phi \in F_t^{n+m}$ and let $e = \langle e_1, \ldots, e_m \rangle$ be constants from $r - t$ such that $\Phi(x,e) \in B_S^r$, i.e., for some $k > 0$

$$S \vdash \bigwedge_{i<k} \Phi(Q(i),e)$$

$$S \vdash \left[\bigwedge_{i<k} \Phi(x_i,e) \wedge \phi(x_i,x_{i+1})\right] \to \Phi(x_k,e) \ .$$

We may assume that there is an $\alpha \in F_t^m$ with $S \vdash \alpha(e)$ such that the right-hand sides of these formulas can be derived from $T \cup \{\alpha(e)\}$ alone. Now let

$$\psi(x) \equiv \forall y(\alpha(y) \to \Phi(x,y)) \ .$$

Because $Q(i) = R(i)$ for $i \in \omega$ and the constants e do not occur in T, these formulas give $\psi \in B_T^t$; i.e., $\psi(Q(i)) \in S$ for every $i \in I_Q$. Now from this and from $S \vdash \alpha(e)$ we get $S \vdash \Phi(Q(i),e)$ for every $i \in I_Q$, as was required.

Returning to the proof of the theorem, Case II, we shall define three infinite increasing sequences of types, theories, and preruns. We start with the definition of t_0, T_0, and R_0. Recall that the type τ, the theory $\theta \in F_\tau^0$, and the formulas ϕ_{in}, $\phi_{out} \in F_\tau^n$ are such that

(4) $Con\{\theta, \phi_{in}(c), H(d), \phi(d,d), \neg\phi_{out}(d)\}$.

Let c_i for $i \in \omega$ and d be n-tuples of different constant symbols not occurring in τ, and let $t_0 > \tau$ be the smallest similarity type containing them. The time structure $\mathbf{I}_{R_0}$ consists of ω and a thread isomorphic to Z endowed with the usual successor function. The definition of the function R_0 goes as follows:

$$R_0(i) = \begin{cases} c_i & \text{if } i \in \omega \\ d & \text{otherwise} \ . \end{cases}$$

Finally, let

$$T_0 = \theta \cup \{\phi(c_i, c_{i+1}) : i \in \omega\} \cup \{\phi_{in}(c_0), \phi(d,d), \neg\phi_{out}(d)\} \ .$$

Lemma 2.5 *R_0 is a (t_0, T_0)-prerun.*

Proof: (i) of Definition 2.1 is immediate. By the definition of the program, $\theta \vdash \forall x \exists y \phi(x,y)$, therefore using the same model as in (4) we get

$$Con(T_0, \{B_{T_0}^{t_0}(R_0(i)) : i \in \omega\}) \ .$$

If the consistency stated in Definition 2.1(ii) does not hold, then there are a formula $\Phi \in F_\tau^{n+m\cdot n+n}$ and constants $e = \langle c_0, c_1, \ldots, c_{m-1} \rangle$ such that $\Phi(x,e,d) \in B_{T_0}^{t_0}$, i.e.,

(5) $T_0 \vdash \bigwedge_{i<k} \Phi(c_i,e,d)$

(6) $T_0 \vdash \left[\bigwedge_{i<k} \Phi(x_i,e,d) \wedge \phi(x_i,x_{i+1})\right] \to \Phi(x_k,e,d)$,

and for some $i_0 \in \omega$,

$$T_0 \cup \{\Phi(c_i,e,d) : i < i_0\} \vdash \neg\Phi(d,e,d) \ ,$$

or, by (5) and (6),

(7) $T_0 \vdash \neg\Phi(d,e,d)$.

We may assume $k < m$, too. Let $\alpha \in F_\tau^{n\cdot m}$ and $\beta \in F_\tau^n$ be the formulas for which

$$\alpha(e) \equiv \phi_{in}(c_0) \wedge \bigwedge_{i+1<m} \phi(c_i,c_{i+1}) \ ,$$
$$\beta(d) \equiv \phi(d,d) \wedge \neg\phi_{out}(d) \ .$$

The right-hand sides of (5), (6), and (7) can be derived even from $\theta \cup \{\alpha(e), \beta(d)\}$. Now let

$$\psi(x_0) \equiv \forall x_1 \ldots \forall x_k \forall y \exists z \left[\bigwedge_{i<k} \phi(x_i,x_{i+1}) \wedge \beta(y) \to \alpha(z) \wedge \bigwedge_{i<k} \Phi(x_i,z,y)\right] \ .$$

By (5), $\theta \vdash \phi_{in}(c_0) \to \psi(c_0)$, by (6), $\theta \vdash \psi(x_0) \wedge \phi(x_0,x_1) \to \psi(x_1)$, thus $\psi \in H$. Choosing $x_0 = x_1 = \ldots = x_k = y = d$, (4) gives

$$Con(\theta,\ \exists z(\beta(d) \to \alpha(z) \wedge \Phi(d,z,d)),\ \beta(d)) \ .$$

But by (7), $\theta \vdash \forall z[\alpha(z) \wedge \beta(d) \to \neg\Phi(d,z,d)]$, a contradiction.

Now we have the similarity type t_0, the theory $T_0 \subset F_{t_0}^0$, and the (t_0,T_0)-prerun R_0 such that $\tau < t_0$, $\theta \subseteq T_0$, $\phi_{in}(R_0(0)) \in T_0$, and for some $i \in I_{R_0}$

$$R_0(i) = R_0(si) \wedge \neg\phi_{out}(R_0(i)) \in T_0 \ .$$

Suppose we have defined t_k, T_k, and R_k for some $k \in \omega$. By Lemma 2.2 there exists a complete theory T_k' with $T_k \subseteq T_k' \subset F_{t_k}^0$ such that R_k is a (t_k,T_k')-prerun. By Lemma 2.3 we have a type $r_k > t_k$ and a complete theory S_k of type r_k such that $T_k' \subseteq S_k \subset F_{r_k}^0$ with every existential formula of T_k' satisfied by some constant of r_k. Finally, by Lemma 2.4 there is a type $t_{k+1} > r_k$, a theory T_{k+1} of type t_{k+1}, and a (t_{k+1},T_{k+1})-prerun R_{k+1} such that $S_k \subseteq T_{k+1}$ and $R_k \subseteq R_{k+1}$, and for every $\Phi \in F_{t_k}^n$ at least one of the following holds:

(a) $T_{k+1} \vdash \neg\Phi(R_{k+1}(0))$
(b) $T_{k+1} \vdash \Phi(R_{k+1}(i)) \wedge \neg\Phi(R_{k+1}(si))$ for some $i \in I_{R_{k+1}}$
(c) There exists $\chi \in B_{T_k}^{t_k}$ for which $T_k \vdash \forall x(\chi(x) \to \Phi(x))$.

Now let $t = \bigcup\{t_k : k \in \omega\}$, $T = \bigcup\{T_k : k \in \omega\}$, and $R = \bigcup\{R_k : k \in \omega\}$. Then $T \subset F_t^0$ is a complete theory and R is a (t,T)-prerun since T is a union of an increasing sequence of complete theories. The constants of the type t form a model for the theory T; this is ensured by the theories S_k. (Strictly speaking, certain equivalence classes of constants form this model; see [4].) Let this model be $\mathbf{A}$, its underlying set be A. We claim that $R : I_R \to A^n$ is a run of the program

ϕ. If this claim is true we are done. Indeed, $\mathbf{A}$ is a model of $\theta \subseteq T_0 \subset T$, $\mathbf{A} \models \phi_{in}(R(0))$, and for some $i \in I_{R_0} \subset I_R$ we have

$$\mathbf{A} \models R(i) = R(si) \wedge \neg\phi_{out}(R(i))$$

because these formulas are in T_0. Therefore the program ϕ is not partially correct with respect to ϕ_{in} and ϕ_{out}.

To see the claim, we remark that $\mathbf{I}_R$ is a time-structure and R is a (t, T)-prerun, so (i) of Definition 1.1 is obvious. To check (ii), let $\psi \in F^{n+m}$ and let $u \in A^m$ be arbitrary. Every element of A is named by a constant of t, so there is a $\Phi \in F_t^n$ such that

$$\mathbf{A} \models \psi(x, u) \leftrightarrow \Phi(x) \ .$$

But this Φ belongs to $F_{t_k}^n$ for some $k \in \omega$; i.e., one of (a), (b), or (c) above holds. In the case of (a) or (b)

$$\mathbf{A} \not\models \Phi(R(0)) \wedge \bigwedge_{i \in I_R} [\Phi(R(i)) \rightarrow \Phi(R(si))] \ ,$$

i.e., the premise does not hold. In the case of (c), $\chi \in B_{T_k}^{t_k} \subset B_T^t$, and $B_T^t(R(i)) \subset T$ because R is a prerun and T is complete. Therefore $\mathbf{A} \models \chi(R(i))$; i.e., $\mathbf{A} \models \Phi(R(i))$ for every $i \in I_R$.

REFERENCES

[1] Andréka, H. and I. Németi, "A characterization on Floyd provable programs," *Proceedings of Colloquia on the Mathematical Foundations of Computer Science 1981, Lecture Notes in Computer Science*, vol. 118 (1981), pp. 162–171.

[2] Andréka, H., I. Németi, and I. Sain, "Completeness problems in verification of programs," *Mathematical Foundations of Computer Science 1977, Lecture Notes in Computer Science*, vol. 74 (1979), pp. 208–218.

[3] Andréka, H., I. Németi, and I. Sain, "A complete logic for reasoning about programs via nonstandard model theory I-II," *Theoretical Computer Science*, vol. 17 (1982), pp. 193–212, 259–278.

[4] Chang, C. C. and H. J. Keisler, *Model Theory*, North Holland, Amsterdam, 1973.

[5] Csirmaz, L., "Programs and program verification in a general setting," *Theoretical Computer Science*, vol. 16 (1981), pp. 199–210.

[6] Csirmaz, L., "On the completeness of proving partial correctness," *Acta Cybernetica*, vol. 5 (1981), pp. 181–190.

[7] Floyd, R. W., "Assigning meanings to programs," pp. 19–32 in *Mathematical Aspects of Computer Science*, ed., J. T. Schwartz, American Mathematical Society, 1967.

[8] Gergely, T. and M. Szöts, "On the incompleteness of proving partial correctness," *Acta Cybernetica*, vol. 3 (1979), pp. 45–57.

[9] Harel, D., *First order dynamic logic*, *Lecture Notes in Computer Science*, vol. 68 (1979).

[10] Hoare, C. A. R., "An axiomatic basis for computer programming," *Communications of the Association for Computing Machinery*, vol. 12 (1969), pp. 576–580.

[11] Manna, Z., *Mathematical Theory of Computation*, McGraw-Hill, New York, 1974.

[12] Németi, I., "Nonstandard dynamic logic," *Proceedings of the Workshop on Logic of Programs 1981*, *Lecture Notes in Computer Science*, vol. 131 (1982), pp. 311–348.

Mathematical Institute of the Hungarian Academy of Sciences
Budapest, Reáltanoda u. 13-15, H-1053, Hungary