On the completeness of proving partial correctness

By L. CSIRMAZ

We give here a proof for the completeness of the Floyd—Hoare program verification method in a case which has remained open in [1]. The method used here is basically the same as in [5]. For the motivation behind our concepts see [1, 3, 10]. Applications of our results in dynamic logic can be found in [10].

1. Introduction

Structures will be denoted by bold-faced type letters, their underlying sets by the corresponding capital letters. If A is a set and $n\in\omega$ then A^n denotes the set of n-tuples of the elements of A. Throughout the paper d denotes an arbitrary, but fixed similarity type, and T denotes an arbitrary but fixed consistent theory of that type. For $n\in\omega$, F_d^n denotes the set of first order formulas of type d with free variables among $\{y_i\colon i<n\}$, and we let $F_d=\bigcup\{F_d^n\colon n\in\omega\}$. In particular, T is a proper subset of F_d^0. For the sake of simplicity we make no typographical distinction between single symbols and sequences of symbols.

A program (or rather a program scheme) can be regarded as a prescription which defines uniquely the next moment contents of the registers from their present moment contents. Therefore we adapt

Definition 1. Let $T\subset F_d^0$ be arbitrary. A d-type *program* (in T) is a formula $\varphi\in F_d^2$ such that

$$T\vdash\forall x\exists!\, y\varphi(x, y).\quad\square$$

Let $\mathbf{D}$ be a d-type structure, and $\mathbf{D}\models T$. Then, by this definition, the program φ defines a function from D to D which we denote by $p_{\varphi,\mathbf{D}}$. More precisely, for every $q\in D$ there is exactly one element of D, denoted by $p_{\varphi,\mathbf{D}}(q)$ for which $\mathbf{D}\models\varphi(q, p_{\varphi,\mathbf{D}}(q))$. To avoid long and unreadable formulas we omit the indices φ, $\mathbf{D}$ everywhere and use the letter p as a new function symbol denoting $p_{\varphi,\mathbf{D}}$ in every model $\mathbf{D}$ of the theory T. For example, if $\psi\in F_d^1$ then the formula

$$\forall y(\varphi(x, y)\to\psi(y))\in F_d^1$$

is abbreviated as $\psi(p(x))$.

To define semantics of programs we need the notion of the time-model [1, 3, 10].

Definition 2. The triplet $\mathfrak{M}=\langle \mathbf{I}, \mathbf{D}, f\rangle$ is a *time-model* if $\mathbf{I}$ is a structure of similarity type t, $\mathbf{D}$ is a structure of similarity type d, and $f\colon I\to D$ is a function, where the type t consists of the constant symbol 0, the one placed function symbol "+1", and the two placed relation symbol "$\leqq$". □

We say that $\mathbf{I}$ is the time structure, and $\mathbf{D}$ is the data structure of $\mathfrak{M}=\langle \mathbf{I}, \mathbf{D}, f\rangle$. Time-models can be regarded as a special 2-sorted models with sorts $\mathbf{t}$ and $\mathbf{d}$ (called time and data), and with operation symbols of t and d and the extra operation symbol f, see [9, 10]. Let TF denote the set of 2-sorted formulas of this type. By a little abuse of notation, we assume that F_t and F_d are disjoint, and $F_t\cup F_d\subset TF$.

Now we can give the strict definition of the program run. Note that by our agreement on the type t, we may write $i+1$ $(i\in I)$.

Definition 3. Let $\mathfrak{M}=\langle \mathbf{I}, \mathbf{D}, f\rangle$ be a time-model and let $p\colon D\to D$ be a program. The function f constitutes a *trace* of the program p in $\mathfrak{M}$ if for every $i\in I$, $f(i+1)=p(f(i))$. We say that the (trace of the) program *halts* at the timepoint $i\in I$ if $f(i+1)=f(i)$. □

Definition 4. Let φ_{in} and $\varphi_{\text{out}}\in F_d^1$ be two formulas. The program p is *partially correct* with respect to φ_{in} and φ_{out} in the time-model $\mathfrak{M}$ if whenever f is a trace of p, and $\mathbf{D}\models\varphi_{\text{in}}(f(0))$ (i.e. the input satisfies φ_{in}) then for every $i\in I$ such that $f(i+1)=f(i)$ (i.e. the program halts at the timepoint i), $\mathbf{D}\models\varphi_{\text{out}}(f(i))$. This assertion is denoted by $\mathfrak{M}\models(\varphi_{\text{in}}, p, \varphi_{\text{out}})$.

Let $S\subset TF$ be arbitrary. If for every time-model $\mathfrak{M}$, $\mathfrak{M}\models S$ implies $\mathfrak{M}\models(\varphi_{\text{in}}, p, \varphi_{\text{out}})$ then this fact is denoted by $S\models(\varphi_{\text{in}}, p, \varphi_{\text{out}})$. □

So far we have completed the definition of the partial correctness. The following definition is a reformulation of the well-known Floyd—Hoare partial correctness proof rule [7, 8, 10].

Definition 5. The program p is *Floyd—Hoare derivable* from the theory $T\subset F_d^0$ with respect to φ_{in} and $\varphi_{\text{out}}\in F_d^1$, in symbols $T\vdash(\varphi_{\text{in}}, p, \varphi_{\text{out}})$, if there is a formula $\Phi\in F_d^1$ such that

$$T\vdash \varphi_{\text{in}}(x)\to\Phi(x)$$

$$T\vdash \Phi(x)\to\Phi(p(x))$$

$$T\vdash \Phi(x)\wedge p(x)=x\to\varphi_{\text{out}}(x).\quad\square$$

Let TI denote the set of axioms of the discrete linear ordering with initial element for the type t. That is, TI states that the relation "$\leqq$" is a linear ordering, 0 is the least element, every element i has an immediate successor denoted by $i+1$, and every element except for the 0 has an immediate predecessor. We remark that TI is finite and its theory is complete, see [4] pp. 159—162.

If in the time-model $\mathfrak{M}=\langle \mathbf{I}, \mathbf{D}, f\rangle$ the time structure $\mathbf{I}$ is isomorphic to the ordering of the natural numbers (the time-model is *standard*) then $\mathbf{D}\models T$ and $T\vdash(\varphi_{\text{in}}, p, \varphi_{\text{out}})$ implies $\mathfrak{M}\models(\varphi_{\text{in}}, p, \varphi_{\text{out}})$. By the upward Lövenheim—Skolem theorem, there is no $S\subset TF$ for which $\mathfrak{M}\models S$ would force $\mathfrak{M}$ to be standard.

But we may require $\mathfrak{M}$ to satisfy the most important feature of standard time-models, namely that they admit induction on the time. Let $\varphi(x)\in TF$ be such that x is a variable of sort $\mathbf{t}$ (i.e. x is a time-variable). Then φ^* denotes the following formula of TF:

$$[\varphi(0)\wedge\forall x(\varphi(x)\rightarrow\varphi(x+1))]\rightarrow\forall x\varphi(x).$$

The set of induction axioms are

$$IA=\{\varphi^*\colon\ \varphi(x)\in TF \text{ and } x \text{ is of sort } \mathbf{t}\}.$$

Moreover we introduce a proper subset of IA, the induction axioms of restricted form:

$IR=\{\varphi^*\colon\ \varphi(x)\in TF$ and there is no quantifier for any variable of sort $\mathbf{t}$ in $\varphi(x)\}$.

It is important to remark here that $\varphi(x)$ may contain other free variables. All these free variables are also free in φ^* except for x, they are the parameters of the induction.

Of course $IR\subset IA\subset TF$, and one can easily prove the following theorem.

Theorem 1. Suppose $T\subset F_d^0$ and p is a d-type program. Then $T\vdash(\varphi_{in}, p, \varphi_{out})$ implies $(TI\cup IR\cup T)\models(\varphi_{in}, p, \varphi_{out})$. □

The aim of this paper is to prove the inverse of this theorem.

Theorem 2. With the notation of Theorem 1, $(TI\cup IR\cup T)\models(\varphi_{in}, p, \varphi_{out})$ implies $T\vdash(\varphi_{in}, p, \varphi_{out})$. □

These theorems state the completeness of the Floyd—Hoare program verification method in the case when the time-models satisfy the axioms $TI\cup IR$. In Theorem 2 the fact that induction axioms of restricted form are required only is essential as it is shown by the following theorem [1].

Theorem 3. There is a type d, a theory $T\subset F_d^0$ and a d-type program p such that $(TI\cup IA\cup T)\models(\varphi_{in}, p, \varphi_{out})$ while $T\nvdash(\varphi_{in}, p, \varphi_{out})$. □

2. Strongly continuous traces

We start to prove Theorem 2. From now on we fix the similarity type d, the theory $T\subset F_d^0$, the d-type program p and the formulas $\varphi_{in}, \varphi_{out}\in F_d^1$. In this section for every time-model $\mathfrak{M}=\langle\mathbf{I}, \mathbf{D}, f\rangle$ we assume $\mathfrak{M}\models TI$. The explicit declaration of this fact will be omitted everywhere.

First we need a definition.

Definition 6. Let $\mathfrak{M}=\langle\mathbf{I}, \mathbf{D}, f\rangle$ be a time-model, $\mathbf{D}\models T$. The function f constitutes a *strongly continuous trace* of p if

(i) $f(i+1)=p(f(i))$ for every $i\in I$;
(ii) let $i, j\in I, i\leqq j, u\in D^n$ and $\Phi\in F_d^{1+n}$ be arbitrary. If $\mathbf{D}\models\Phi(f(i), u)\wedge\neg\Phi(f(j), u)$ then there is a $k\in I$, $i\leqq k\leqq j$ such that $\mathbf{D}\models\Phi(f(k), u)\wedge\neg\Phi(f(k+1), u)$. □

Strongly continuous traces (sct in the sequel) are traces, cf. Definition 3. In other words, an sct satisfies the induction principle in every time interval. Obviously, if $\mathfrak{M}\models IR$ and f is a trace then f is an sct, too. Properties of continuous traces are discussed in [2, 6, 10].

Lemma 1. Let f be a trace of the program p in $\mathfrak{M}$. Then $\mathfrak{M}\models IR$ iff f is strongly continuous.

Proof. We prove the "if" part only. Let $\varphi(x_0)\in TF$ be such that $\varphi(x_0)$ does not contain quantifiers on variables of sort **t**. Let $x_0, x_1, \ldots, x_{m-1}$ be the free variables of φ of sort **t**, and $y_0, \ldots, y_{n-1}$ be that of sort **d**. Because there are finitely many applications of the function "+1" only in φ, we may assume that there is none, simply replace these applications by a new parameter of sort t or use the identity $f(x+1)=p(f(x))$. We may assume also that every $f(x_j)$ is denoted by some of the parameters among $y_0, \ldots, y_{n-1}$, i.e. the function f is applied to x_0 only. Thereafter for every $\varphi(x_0)\in TF$ with fixed parameters from I and D, there are elements $i_1\leqq i_2\leqq\ldots\leqq i_m$ from I, elements $u_0, u_1, \ldots, u_{n-1}$ from D, and formulas $\Phi_0, \Phi_1, \ldots, \Phi_m\in F_d^{1+n}$ such that

$$\begin{aligned}\mathfrak{M}\models\varphi(x)\leftrightarrow\{[\quad & x<i_1\rightarrow\Phi_0(f(x),u)]\wedge\\ \wedge[i_1\leqq{} & x<i_2\rightarrow\Phi_1(f(x),u)]\wedge\\ & \ldots\\ \wedge[i_{m-1}\leqq{} & x<i_m\rightarrow\Phi_{m-1}(f(x),u)]\wedge\\ \wedge[i_m\leqq{} & x\qquad\rightarrow\Phi_m(f(x),u)]\}\end{aligned}$$

which can be got, for example, by induction on the complexity of φ. Now if $\mathfrak{M}\models\varphi(0)\wedge\forall x(\varphi(x)\rightarrow\varphi(x+1))$ then, applying the strongly continuity in the intervals $[0, i_1]$, $[i_1, i_2]$, etc. we get $\mathfrak{M}\models\forall x\varphi(x)$ which was to be proved. □

By this lemma it is enough to show that either the triplet $(\varphi_{in}, p, \varphi_{out})$ is Floyd—Hoare derivable, or there is a strongly continuous trace which shows that p is not partially correct.

Let us make a step forward.

Definition 7. Let $H\subset F_d^1$ consist of the formulas $\Phi\in F_d^1$ for which

$$T\vdash\varphi_{in}(x)\rightarrow\Phi(x)$$

and

$$T\vdash\Phi(x)\rightarrow\Phi(p(x)).\quad\square$$

Note that H is closed under conjunction, i.e. if Φ_1 and Φ_2 are in H then $\Phi_1\wedge\Phi_2\in H$. Now let c_0 and c_ω denote two new constant symbols not occuring previously. We distinguish two cases.

Case I. In every model of the theory

$$\{T, \varphi_{in}(c_0), H(c_\omega), p(c_\omega)=c_\omega\}$$

the formula $\varphi_{out}(c_\omega)$ is valid. Here $H(c_\omega)=\{\Phi(c_\omega)\colon\Phi\in H\}$. Then by the compactness theorem and by the fact that H is closed under conjunction, there is a $\Psi \in H$ such that

$$T \vdash [\varphi_{\text{in}}(c_0) \wedge \Psi(c_\omega) \wedge p(c_\omega) = c_\omega] \to \varphi_{\text{out}}(c_\omega).$$

The constants c_0 and c_ω do not occur in T, so introducing $\Phi(x) = (\exists y \varphi_{\text{in}}(y)) \wedge \Psi(x)$, we get

$$T \vdash \Phi(x) \wedge p(x) = x \to \varphi_{\text{out}}(x).$$

This and the obvious $\Phi \in H$ shows the Floyd—Hoare derivability of $(\varphi_{\text{in}}, p, \varphi_{\text{out}})$.

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

$$\text{Con}\,\{T, \varphi_{\text{in}}(c_0), H(c_\omega), p(c_\omega) = c_\omega, \neg\varphi_{\text{out}}(c_\omega)\}.$$

By Theorem 4 of the following section, in this case we have a time-model $\mathfrak{M} = \langle \mathbf{I}, \mathbf{D}, f \rangle \models T$ such that f is an sct of p, $\mathbf{D} \models \varphi_{\text{in}}(f(0))$ and for some $i \in I$, $\mathbf{D} \models f(i) = p(f(i)) \wedge \neg\varphi_{\text{out}}(f(i))$. This means $\mathfrak{M} \not\models (\varphi_{\text{in}}, p, \varphi_{\text{out}})$, i.e. p is not partially correct. This proves Theorem 2, because $\mathfrak{M} \models TI \cup IR \cup T$ by Lemma 1.

3. The proof of the crucial theorem

In the remaining part of this paper we prove the following theorem.

Theorem 4. With the notation of the previous section, suppose

$$\text{Con}\,\{T, \varphi_{\text{in}}(c_0), H(c_\omega), p(c_\omega) = c_\omega, \neg\varphi_{\text{out}}(c_\omega)\}.$$

Then there is a time-model $\mathfrak{M} = \langle \mathbf{I}, \mathbf{D}, f \rangle$ such that $\mathbf{I} \models TI$, $\mathbf{D} \models T$, f is a strongly continuous trace of p, $\mathbf{D} \models \varphi_{\text{in}}(f(0))$, and for some $i \in I$, $f(i+1) = f(i)$ and $\mathbf{D} \models \neg\varphi_{\text{out}}(f(i))$.

Proof. We need some more definitions. If d_1 and d_2 are similarity types then $d_1 < d_2$ means that d_1 and d_2 have the same function and relation symbols with the same arities and every constant symbol of d_1 is a constant symbol of d_2.

Definition 8 .Let d be a similarity type, $T \subset F_d^0$ be a theory. The pair $R = \langle \mathbf{I}_R, f_R \rangle$ is a *(d, T)-pretrace* if $\mathbf{I}_R$ is a time structure, $\mathbf{I}_R \models TI$, and f_R is a function which assigns to every $i \in I_R$ a constant symbol of d in such a way that (i) and (ii) below are satisfied. A bit loosely but not ambiguously, we write $R(i)$ or simply Ri instead of $f_R(i)$.

(i) $T \vdash R(i+1) = p(Ri)$ for every $i \in I_R$

(ii) $\text{Con}\,(T \cup \{\Phi(Rj)\colon j \in I_R,\ \Phi \in B_T^d$ and there exists $i \in I_R,\ i < j$ such that $T \vdash \Phi(Ri)\})$,

where

$$B_T^d = \{\Phi \in F_d^1\colon T \vdash \Phi(x) \to \Phi(px)\}. \quad \square$$

Note that the set B_T^d is closed under conjunction, this fact will be used many times.

Lemma 2. Let R be a (d, T)-pretrace. Then there exists a complete theory $T \subset S \subset F_d^0$ such that R is a (d, S)-pretrace.

Proof. It suffices to show that for any $\beta\in F_d^0$, R is either $(d, T\cup\{\beta\})$ or $(d, T\cup\{\neg\beta\})$-pretrace. If neither of them hold then in both cases (ii) of Definition 8 is violated. It means that there are finitely many $i_s, j_s\in I_R$, $i_s\leqq j_s$, and $\Phi_s\in B^d_{T\cup\{\beta\}}$, $\Phi_s^*\in B^d_{T\cup\{\neg\beta\}}$ such that

$$T\cup\{\beta\}\vdash\neg\bigwedge_s\Phi_s(Rj_s)\quad\text{and}\quad T\cup\{\beta\}\vdash\bigwedge_s\Phi_s(Ri_s)\tag{3.1}$$

$$T\cup\{\neg\beta\}\vdash\neg\bigwedge_s\Phi_s^*(Rj_s)\quad\text{and}\quad T\cup\{\neg\beta\}\vdash\bigwedge_s\Phi_s^*(Ri_s).\tag{3.2}$$

Now let $\Psi_s(x)=(\beta\to\Phi_s(x))\wedge(\neg\beta\to\Phi_s^*(x))$. Obviously, $\Psi_s\in B_T^d$ and $T\vdash\bigwedge_s\Psi_s(Ri_s)$. Elementary considerations show that (3.1) and (3.2) imply

$$T\vdash\neg\bigwedge_s\Psi_s(Rj_s)$$

which contradicts the assumption $\mathrm{Con}\,(T, \{\Psi_s(Rj_s)\})$. □

Lemma 3. Let R be a (d, T)-pretrace, and let T be complete. Then there exist a similarity type $e>d$ and a complete theory $T\subset S\subset F_e^0$ such that

(i) R is an (e, S)-pretrace,
(ii) for every $\psi\in F_d^1$, if $\exists x\psi(x)\in T$ then for some constant c from the type e, $\psi(c)\in S$,
(iii) the cardinality of the new constants in e does not exceed the cardinality of F_d, i.e.

$$|F_e|=|e|\leqq|F_d|=|d|\cdot\omega.$$

Proof. What we have to prove is the following. Suppose that the type e contains the extra constant symbol c only, $\beta\in F_d^1$ and $\mathrm{Con}\,\{T, \beta(c)\}$, then R is an $(e, T\cup\{\beta(c)\})$-pretrace. From this (i)—(iii) can be got by a standard argument, see, e.g. [4] pp. 62—66. Now suppose that this is not the case, i.e. there are finitely many $\Phi_s(x, c)\in B^e_{T\cup\{\beta(c)\}}$ and $i_s, j_s\in I_R$, $i_s<j_s$ such that

$$T\cup\{\beta(c)\}\vdash\neg\bigwedge_s\Phi_s(Rj_s, c)\tag{3.3}$$

$$T\cup\{\beta(c)\}\vdash\bigwedge_s\Phi_s(Ri_s, c).\tag{3.4}$$

The condition $\Phi_s(x, c)\in B^e_{T\cup\{\beta(c)\}}$ implies

$$\Psi_s(x)=\forall y(\beta(y)\to\Phi_s(x, y))\in B_T^d,$$

and by (3.4), $T\vdash\forall y(\beta(y)\to\Phi_s(Ri_s, y))$, i.e. $\Psi_s(Ri_s)\in T$. Now T is complete, therefore $j_s>i_s$ implies $T\vdash\Psi_s(Rj_s)$, from which

$$T\vdash\bigwedge_s(\beta(c)\to\Phi_s(Rj_s, c))\vdash\beta(c)\to\bigwedge_s\Phi_s(Rj_s, c).$$

This and (3.3) gives $T\vdash\neg\beta(c)$, a contradiction. □

Lemma 4. Let R be a (d, T)-pretrace, and let T be complete. Suppose $i_0, j_0\in I_R$, $i_0<j_0$ and $\chi\in F_d^1$ such that

$$T\vdash\chi(Ri_0)\wedge\neg\chi(Rj_0).$$

Then there exist a type $e>d$, a theory $T\subset S\subset F_e^0$ and an (e, S)-pretrace Q such that

(i) $\mathbf{I}_Q$ is an elementary extension of $\mathbf{I}_R$ and $Q\supset R$, i.e.

$$Q(i) = R(i) \quad \text{for} \quad i\in I_R$$

(ii) there is an $i\in I_Q$, $i_0\leqq i<j_0$ such that

$$S\vdash \chi(Q(i))\wedge\neg\chi(Q(i+1)).$$

Proof. Let $\alpha=\{i\in I_R\colon \text{for every } i_0\leqq i'\leqq i, T\vdash\chi(Ri')\}$. Obviously, α is an initial segment of I_R, we write $i<\alpha$ and $i>\alpha$ instead of $i\in\alpha$ and $i\notin\alpha$, respectively. The element $j_0>\alpha$, and we may assume that there is no largest element in α otherwise there is nothing to prove. It means that for every $j>\alpha$, there exists $\alpha<j'<j$ such that $T\vdash\neg\chi(Rj')$ .We shall insert a thread isomorphic to the set of integer numbers, denoted by Z, into the cut indicated by α.

Let $\{a_l\colon l\in Z\}$ be countably many new symbols and let $\{c_l\colon l\in Z\}$ be new constant symbols. Let $I_Q=I_R\cup\{a_l\colon l\in Z\}$ and define the ordering on I_Q by $a_l<a_{l+1}$, $i<a_l$ if $i\in I_R$, $i<\alpha$ and $a_l<i$ if $i\in I_R, i>\alpha$ for every $l\in Z$. Evidently, $\mathbf{I}_Q$ is an elementary extension of $\mathbf{I}_R$.

Define the function Q by $Q(i)=R(i)$ if $i\in I_R$ and $Q(a_l)=c_l$ otherwise. Let the type e be the enlargement of d by the constant symbols $\{c_l\colon l\in Z\}$, and finally let the theory $S\subset F_e^0$ be

$$\begin{aligned} S = T\cup\{p(c_l) = c_{l+1}\colon l\in Z\}\cup\{\chi(c_0), \neg\chi(c_1)\}\cup \\ \cup\{\Phi(c_l)\colon l\in Z, \Phi\in B_T^d \text{ and } T\vdash \Phi(Ri) \text{ for some } i<\alpha\}\cup \\ \cup\{\neg\Phi(c_l)\colon l\in Z, \Phi\in B_T^d \text{ and } T\vdash\neg\Phi(Rj) \text{ for some } j>\alpha\}. \end{aligned}$$

We claim that S is consistent. It suffices to show that T is consistent with any finite part of $S\setminus T$. Using the facts that T is complete, B_T^d is closed under conjunction, and the formulas $\Phi\in B_T^d$ are hereditary in $\mathbf{I}_R$, this reduces to

$$\operatorname{Con}\left(T\cup\{\Phi(c_{-l}), \chi(c_0), \neg\chi(c_1), \neg\Phi^*(c_l)\}\right)$$

where $l\in\omega$ is a natural number, $\Phi, \Phi^*\in B_T^d$, and $T\vdash\Phi(Ri_1)\wedge\neg\Phi^*(Rj_1)$ for some $i_0\leqq i_1<\alpha<j_1\leqq j_0$. Now if this consistency does not hold then, T being complete,

$$T\vdash \Phi(x)\wedge\chi(p^l(x))\wedge\neg\Phi^*(p^{2l}(x)) \rightarrow \chi(p^{l+1}(x)).$$

Now let $\Psi(x)=\Phi(x)\wedge[\chi(p^l(x))\vee\Phi^*(p^{2l-1}(x))]$. By the previous statement, $T\vdash\Psi(x)\rightarrow\Psi(px)$, i.e. $\Psi\in B_T^d$. Now, by the assumptions, $T\vdash\Phi(R(i))$ and $T\vdash\chi(R(i+l))$ for $i_1\leqq i<\alpha$, therefore $T\vdash\Psi(Ri)$. But R is a pretrace so for every $\alpha<j<j_1-2l, T\vdash\Psi(Rj)$, although for some $\alpha<j'<j_1-2l, T\vdash\neg\chi(Rj')$ and $T\vdash\neg\Phi^*(R(j'+l-1))$. This contradiction shows that S is consistent indeed.

We prove that Q is an (e, S)-pretrace, (i) and (ii) of the lemma are clear from the construction. First assume that $i\in I_R$, $\Psi\in B_S^e$ and $S\vdash\Psi(Ri)$. We are going to show that in this case $S\vdash\Psi(Qj)$ for every $j\in I_Q$, $j>i$. Indeed, we may suppose that Ψ contains the new constant symbol $c=c_{-l}$ only and that

$$T\cup\{\delta(c)\}\vdash\Psi(x, c) \rightarrow \Psi(px, c)$$

$$T\cup\{\delta(c)\}\vdash\Psi(Ri, c)$$

where $\delta(c)=\Phi(c)\wedge\chi(p^l(c))\wedge\neg\chi(p^{l+1}(c))\wedge\neg\Phi^*(p^{2l}(c))$. By the first derivability, $\Theta(x)=\forall y[\delta(y)\to\Psi(x,y)]\in B_T^d$, and by the second one, $T\vdash\Theta(Ri)$. R is a pretrace, and by the definition of S, $S\vdash\Theta(Qj)$ for every $j\in I_Q$, $j>i$. But $S\vdash\delta(c_{-l})$, i.e. $S\vdash\Psi(Qj,c_{-l})$ as was stated.

Now if Q is not an (e,S)-pretrace then (ii) of Definition 8 is violated, which means that there are finitely many $i_s\in I_Q\setminus I_R$, $j_s\in I_R$, $j_s>\alpha$ and $\Phi_s\in B_S^e$ such that $S\vdash\neg\bigwedge_s\Phi_s(Rj_s)$ while $S\vdash\bigwedge_s\Phi_s(Qi_s)$. The set B_S^e is closed under conjunction, therefore we may assume that all the i_s and Φ_s coincide, that this $\Phi_s=\Psi$ contains the new constant symbol $c=c_{-l}=Qi_s$ only, and that with $\delta(c)$ as above,

$$T\cup\{\delta(c)\}\vdash\Psi(x,c)\to\Psi(px,c)$$
$$T\cup\{\delta(c)\}\vdash\Psi(c,c)$$
$$T\cup\{\delta(c)\}\vdash\neg\bigwedge_s\Psi(Rj_s,c).$$

By the first derivability, $\Theta(x)=\exists y(\delta(y)\wedge\Psi(x,y))\in B_T^d$, and by the third one, $T\vdash\bigvee_s\neg\Theta(Rj_s)$. T is complete, which means $T\vdash\neg\Theta(Rj_s)$ for some $j_s>\alpha$, i.e. by the definition of S, $S\vdash\neg\Theta(c)$, which contradicts the second derivability. □

Returning to the proof of Theorem 4, we shall define three increasing sequences of similarity types, theories and pretraces. Recall that the type d, the theory $T\subset F_d^0$ and the formulas $\varphi_{\text{in}},\varphi_{\text{out}}\in F_d^1$ are such that

$$\text{Con}\,\{T,\varphi_{\text{in}}(c_0),H(c_\omega),p(c_\omega)=c_\omega,\neg\varphi_{\text{out}}(c_\omega)\}. \tag{3.5}$$

Let c_l be new constant symbols for $l\in\omega-\{0\}$, and let the similarity type $e>d$ be the smallest one containing them. Let the time structure $\mathbf{I}_R$ consist of a thread isomorphic to ω and another one isomorphic to Z. The definition of the function R goes as follows:

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

Finally let

$$S=T\cup\{p(c_l)=c_{l+1}\colon l\in\omega\}\cup\{\varphi_{\text{in}}(c_0),p(c_\omega)=c_\omega,\neg\varphi_{\text{out}}(c_\omega)\}.$$

Lemma 5. R is an (e,S)-pretrace.

Proof. For the sake of simplicity, let

$$\gamma(x)=(p(x)=x\wedge\neg\varphi_{\text{out}}(x)).$$

It is enough to prove that if $\Phi\in F_d^3$,

$$S\vdash\Phi(x,c_0,c_\omega)\to\Phi(px,c_0,c_\omega) \tag{3.6}$$

and

$$S\vdash\Phi(c_0,c_0,c_\omega) \tag{3.7}$$

then Con $\{S,\Phi(c_\omega,c_0,c_\omega)\}$. Suppose the contrary, i.e.

$$S\vdash\neg\Phi(c_\omega,c_0,c_\omega). \tag{3.8}$$

We may change S to $T\cup\{\varphi_{\text{in}}(c_0), \gamma(c_\omega)\}$ everywhere, so introducing

$$\Psi(x)=\forall z\,\exists y\,[\gamma(z)\to\varphi_{\text{in}}(y)\wedge\Phi(x,y,z)]\in F_d^1,$$

(3.6) says that $T\vdash\Psi(x)\to\Psi(px)$. From (3.7) we get $T\vdash\varphi_{\text{in}}(x)\to\Psi(x)$, therefore $\Psi\in H$. Choosing $x=z=c_\omega$ in Ψ, the condition (3.5) gives

$$\text{Con}\,\{T,\varphi_{\text{in}}(c_0),\gamma(c_\omega),\exists y\,[\gamma(c_\omega)\to\varphi_{\text{in}}(y)\wedge\Phi(c_\omega,y,c_\omega)]\}.$$

But by (3.8),

$$T\vdash\forall y[\gamma(c_\omega)\wedge\varphi_{\text{in}}(y)\to\neg\Phi(c_\omega,y,c_\omega)]$$

a contradiction. □

Let $d_0=e$, $R_0=R$. By Lemma 2 there is a complete theory $S\subset T_0\subset F_e^0=F_{d_0}^0$ such that R_0 is a (d_0, T_0)-pretrace. Let the cardinality of $F_{d_0}^0$ be $\varkappa$, and let $\varkappa^+$ denote the smallest cardinal exceeding $\varkappa$. Let $C=\{c_\xi:\ \xi<\varkappa^+\}$ be different constant symbols such that the constants of the type d_0 are among them, and let $J=\{a_\xi:\ \xi<\varkappa^+\}$ be symbols of time points such that $I_{R_0}\subset J$. (Note that I_{R_0} is countable.)

Arrange the triplets of $J\times J\times F_{d\cup C}^1$ in a sequence $\{\langle i_\xi, j_\xi, \Phi_\xi\rangle:\ \xi<\varkappa^+\}$ of length $\varkappa^+$ in such a way that every triplet occurs $\varkappa^+$ times in this sequence. Now we define three increasing sequences d_ξ, T_ξ, and R_ξ for $\xi<\varkappa^+$ such that

(i) d_ξ is a similarity type,
(ii) $T_\xi\subset F_{d_\xi}^0$ is a complete theory, and $|F_{d_\xi}^0|=\varkappa$,
(iii) R_ξ is a (d_ξ, T_ξ)-pretrace, and $I_{R_\xi}\subset J$, $|I_{R_\xi}|\le\varkappa$.

Suppose we have defined d_ξ, T_ξ, R_ξ for $\xi<\eta<\varkappa^+$, they have properties (i)—(iii) and we want to define d_η, T_η, R_η.

If η is a limit ordinal, simply put $d_\eta=\bigcup\{d_\xi:\ \xi<\eta\}$, $T_\eta=\bigcup\{T_\xi:\ \xi<\eta\}$, $R_\eta= =\bigcup\{R_\xi:\ \xi<\eta\}$. This definition is sound because $\mathbf{I}_{R_\eta}$ is the union of the increasing elementary chain $\langle\mathbf{I}_{R_\xi}:\ \xi<\eta\rangle$, therefore it is also a model of the axiom system TI. T_η is the union of an increasing sequence of complete theories, therefore itself is complete. Similarly for the other properties.

If η is a successor ordinal, say $\eta=\xi+1$, then work as follows. If either $i_\xi\notin I_{R_\xi}$, $j_\xi\notin I_{R_\xi}$, $\Phi_\xi\notin F_{d_\xi}^1$ or $i_\xi, j_\xi\in I_{R_\xi}$, $\Phi_\xi\in F_{d_\xi}^1$ but $i_\xi>j_\xi$ or $T_\xi\nvdash\Phi_\xi(R_\xi i_\xi)\wedge\neg\Phi_\xi(R_\xi j_\xi)$ then let $d_{\xi+1}=d_\xi$, $T_{\xi+1}=T_\xi$, $R_{\xi+1}=R_\xi$.

If not, i.e. $i_\xi\le j_\xi$ and $T_\xi\vdash\Phi_\xi(R_\xi i_\xi)\wedge\neg\Phi_\xi(R_\xi j_\xi)$ then, by Lemma 4, there is a type $d_\xi'>d_\xi$, a theory $T_\xi'\supset T_\xi$ and a (d_ξ', T_ξ')-pretrace $R_{\xi+1}\supset R_\xi$ such that $d_\xi'\setminus d_\xi$ and $I_{R_{\xi+1}}\setminus I_{R_\xi}$ are countable, so we may put $I_{R_{\xi+1}}\subset J$, $|I_{R_{\xi+1}}|\le|I_{R_\xi}|+\omega\le\varkappa$ and for some $k\in I_{R_{\xi+1}}$, $i_\xi\le k\le j_\xi$ and

$$T_\xi'\vdash\Phi_\xi(R_{\xi+1}(k))\wedge\neg\Phi_\xi(R_{\xi+1}(k+1)).$$

By Lemma 2, there is a complete theory $T_\xi'\subset T_\xi''\subset F_{d_\xi'}^0$ such that $R_{\xi+1}$ is a (d_ξ', T_ξ'')-pretrace, finally, by Lemma 3, $R_{\xi+1}$ is a $(d_{\xi+1}, T_{\xi+1})$-pretrace, where $d_{\xi+1}>d_\xi'$, $T_{\xi+1}\supset T_\xi''$, $T_{\xi+1}$ is complete, the cardinality of $d_{\xi+1}\setminus d_\xi$ is at most $\varkappa$, and every existential formula of T_ξ'' (and therefore of T_ξ) is satisfied by some constant of $d_{\xi+1}$. In this case the inductive assertions are trivially satisfied.

Now let $d^*=\bigcup\{d_\xi:\ \xi<\varkappa^+\}$, $T^*=\bigcup\{T_\xi:\ \xi<\varkappa^+\}$, and $R^*=\bigcup\{R_\xi:\ \lambda<\varkappa^+\}$. The theory T^* is complete and R^* is a (d^*, T^*)-pretrace. The constants of the type d^* form a model for the theory T^* because every existential formula of T^*

is satisfied by some constant, this was ensured by the applications of Lemma 3. (Strictly speaking, certain equivalence classes of these constants form this model, see [4], pp. 63—66). Let this model be $\mathbf{D}$, we claim that the time-model $\mathfrak{M}=\langle \mathbf{I}_{R^*}, \mathbf{D}, f_{R^*}\rangle$ satisfies the requirements of Theorem 4.

Indeed, $\mathbf{I}_{R^*}\models TI$, and $T\subset T_0\subset T^*$, therefore $\mathbf{D}\models T$. By the definition of the pretrace $R_0, f_{R^*}(0)=f_{R_0}(0)=c_0$, $T_0\vdash \varphi_{\rm in}(c_0)$. For some $i\in I_{R_0}\subset I_{R^*}, f_{R^*}(i)=f_{R_0}(i)=$ $=c_\omega$, and $T_0\vdash p(c_\omega)=c_\omega\wedge\neg\varphi_{\rm out}(c_\omega)$. Because $\mathbf{D}\models T_0$, these formulas are valid in $\mathbf{D}$. What have remained is to check that f_{R^*} is a strongly continuous trace of p.

Let $i\in I_{R^*}$ be arbitrary. Then $i\in I_{R_\xi}$ for some $\xi<\varkappa^+$, and because R_ξ is a (d_ξ, T_ξ)-pretrace, $T_\xi\vdash f_{R_\xi}(i+1)=p\big(f_{R_\xi}(i)\big)$, from which

$$\mathbf{D}\models f_{R^*}(i+1)=p\big(f_{R^*}(i)\big)$$

proving (i) of Definition 6. Finally, let i, $j\in I_{R^*}$, $i\leqq j$, $u\in D^n$ and $\Psi\in F_d^{1+n}$ be such that

$$\mathbf{D}\models \Psi\big(f_{R^*}(i),u\big)\wedge\neg\Psi\big(f_{R^*}(j),u\big).$$

Every element of D is named by some constant of the type d^*, so there is a formula $\Phi\in F_{d^*}^1$ such that $\mathbf{D}\models\Psi(x,u)\leftrightarrow\Phi(x)$. Now $\Phi\in F_{d\cup C}^1$ therefore the triplet $\langle i, j, \Phi\rangle$ occurs $\varkappa^+$ times in the sequence $\{\langle i_\xi, j_\xi, \Phi_\xi\rangle\colon \xi<\varkappa^+\}$. Consequently there exists an index $\xi<\varkappa^+$ such that i, $j\in I_{R_\xi}$, $\Phi\in F_{d_\xi}^1$, and $i=i_\xi$, $j=j_\xi$, $\Phi=\Phi_\xi$. Then, by the construction, there is a $k\in I_{R_{\xi+1}}\subset I_{R^*}$, $i\leqq k\leqq j$ such that

$$T_{\xi+1}\vdash\Phi\big(f_{R_{\xi+1}}(k)\big)\wedge\neg\Phi\big(f_{R_{\xi+1}}(k+1)\big),$$

that is,

$$\mathbf{D}\models\Phi\big(f_{R^*}(k)\big)\wedge\neg\Phi\big(f_{R^*}(k+1)\big)$$

which completes the proof of Theorem 4.

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
REÁLTANODA U. 13—15.
BUDAPEST, HUNGARY
H—1053

References

[1] ANDRÉKA, H., L. CSIRMAZ, I. NÉMETI, I. SAIN, More complete logics for reasoning about programs, to appear.

[2] ANDRÉKA, H., I. NÉMETI, Completeness of Floyd logic, *Bull. Section Logic,* v. 7, 1978, pp. 115—120.

[3] ANDRÉKA, H., I. NÉMETI, I. SAIN, Henkin type semantics for program schemes, *Fund. Comp. Theory '79,* Akademie-Verlag Berlin, 1979, pp. 18—24.

[4] CHANG, C. C., H. J. KEISLER, *Model theory,* North Holland, 1973.

[5] CSIRMAZ, L., Programs and program verifications in a general setting, *Theoret. Comput. Sci.* v. 16, 1981.

[6] CSIRMAZ, L., Structure of program runs of non-standard time, *Acta Cybernet.,* v. 4, 1980, pp. 325—331.

[7] GERGELY, T., M. SZŐTS, On the incompleteness of proving partial correctness, *Acta Cybernet.,* v. 3, 1979, pp. 45—57.

[8] MANNA, Z., *Mathematical theory of computation,* McGraw-Hill, 1974.

[9] MONK, J. D., *Mathematical logic,* Springer, 1976.

[10] NÉMETI, I., A complete first order dynamic logic, *Acta Cybernet.,* to appear; Math. Inst. Hung. Acad. Sci., Preprint, 1980.

(Received July 17, 1980)