Notre Dame Journal of Formal Logic
Volume 30, Number 4, Fall 1989

An Elementary Proof for Some Semantic Characterizations of Nondeterministic Floyd–Hoare Logic

ILDIKÓ SAIN*

Abstract We give a relatively simple and direct proof for Csirmaz's characterization of Floyd–Hoare logic for nondeterministic programs [5]. (This also yields a very simple proof for Leivant's characterization [13].) We also establish a direct connection between "relational traces" and "time-models" for nondeterministic programs.

Introduction In this paper we investigate semantic characterizations of the program verifying power of Floyd-Hoare logic of *nondeterministic* programs. Our main aim is to obtain a relatively simple and direct proof for Csirmaz's model-theoretic characterization (this is the main theorem of [5]). Furthermore, as a byproduct of Makowsky–Sain [14] and our direct proof for Csirmaz's characterization herein, we get a self-contained and straightforward proof for Leivant's Proposition 9 of [13] (which is a characterization of Floyd–Hoare logic in terms of Henkin-type (or nonstandard) second-order logic): it was shown in [14] that our Corollary 2.1 immediately yields Leivant's characterization, hence our rather easy proof of Corollary 2.1 herein provides an equally easy proof for Leivant's result by [14].

To find simpler proofs (and direct constructions) for Csirmaz's important characterization is a problem which goes back to 1980. A characterization for deterministic programs was found in early 1980 (see [7]) and a *stronger* char-

*This project has been supported by the Hungarian National Foundation for Scientific Research, grant no. 1810. The final version of the present paper was completed when I was visiting at Iowa State University, Department of Mathematics, in September 1987.

I am grateful to L. Csirmaz for suggestions that considerably improved the mathematical content of this paper. I also wish to express my thanks to A. Pasztor for carefully reading this paper and for her valuable remarks.

Received November 20, 1985; revised October 15, 1987

acterization for nondeterministic ones was found somewhat later in 1980 (see [5]) that extended a result of Andréka and Németi from 1977 (see [2] and [3]). These are among the central results of the Nonstandard Logics of Programs (NLP) approach, and so it was considered important to simplify the proofs of these rather deep and hard theorems (cf. [17], [19], and [8]). For the result of [7], a short proof was obtained in [22]. The proofs of our Theorem 1.1 and Corollary 2.1 together provide a relatively simple proof for the sharper result of [5].

Another problem was to clarify the connection between [7] and [5]. Because [7] uses "relational traces" (see Theorem 1.1 herein) while [5] uses "time-models" like the ones in temporal logics or in [4] and [8] (see Corollary 2.2 herein), the connection between the two semantics was not quite obvious for *nondeterministic* programs. Here we show how to construct a time-model from any relational trace (in the nondeterministic case too). The other direction is easy (to construct relational traces from time-models). Another aim of this paper is to provide a direct, elementary construction (of a time-model to any unprovable program) for the main theorem of [5]. As a byproduct, we obtain various construction methods for (traces and) models of programs; see the proofs of Corollary 2.2 and Proposition 2.3. We also obtain some (simpler) equivalent versions and generalizations of the semantical characterization of Floyd–Hoare logic for nondeterministic programs (cf. Theorem 1.1, Corollary 2.2, and Remark 2.2).

To keep the formalism simple and short, we use Csirmaz's rather general notion of a program. Motivation for this notion may be found in [5] or [7] where it is also shown that block-diagram programs, regular programs, and programs are all special cases of this notion. A detailed proof of the latter fact can be found also in Chapter 1.7 of [8]. Recursive programs were treated within the NLP approach in a rather natural and elegant manner in [17], which therefore gives rise to the problem of extending the results of the present paper to those kinds of programs too. We will leave this problem unsettled. However, the form of NLP used in [17] is very close to that found in [14] and [15]. Hence one might ask the more concrete question whether the characterization in [14] and [15] (first-order parameter-free comprehension) also works for Floyd-provability of recursive programs.

To avoid the many-sorted logic formalism of [4], [8], [16], [21], [25], etc., we shall use an equivalent version called *time-traces* instead of the original, more natural and more flexible, notion of time-models. The reason for this is that time-traces are shorter to define.

1 Relational trace semantics

Notation Throughout, let d be an arbitrary similarity type (i.e., signature, i.e., ranked alphabet). By a (first-order) *d-formula* we understand a *first-order* formula of similarity type d, and by a *d-model* we understand a first-order model of similarity type d. The universe of a d-model $\mathbf{D}$ will always be denoted by D. By a *d-theory* we understand a set of d-formulas; the set of all d-formulas is denoted by F_d. Let ω denote the *set of all natural numbers*. For every $n \in \omega$, let F_d^n denote the set of all d-formulas which have their free variables among $\{x_i : i < n\}$. Throughout, we write $\phi \wedge \psi \to \gamma$ for $(\phi \wedge \psi) \to \gamma$.

Definition 1.1 If $\pi \in \mathrm{F}_d^{2k}$ for some $k \in \omega$ then we call π a (nondeterministic, k-ary, d-)*program*. The number k is fixed throughout (and will not always be explicitly indicated). That is, whenever we say that π is a program, we mean that π is a k-ary d-program.

We shall use the conventional infix notation $\bar{x}\pi\bar{y}$ for $\pi(\bar{x},\bar{y})$.

Remark 1.1 (i) Intuitively, $\pi(\bar{x},\bar{y})$ defines the *state transition relation of our program* (and *not its input-output relation*). Sometimes π is called a state-transducer. Roughly speaking, the input-output relation of π is the transitive closure of the relation defined by π.

(ii) Our definition of a program is slightly more general than that found in [5] and [7], for in [5] and [7] programs are defined relative only to theories $\mathrm{Th} \subseteq \mathrm{F}_d^0$ with the constraint that $\mathrm{Th} \models \forall\bar{x}\exists\bar{y}(\bar{x}\pi\bar{y})$. So the relation defined by π must be everywhere defined in [5] and [7] while we allow partial state-transducers too. In our Corollary 2.2 we show that the main theorem of [5] remains true for our more general notion of a program.

Definition 1.2 Let d be a similarity type.

(i) By a *d-partial correctness assertion* (d-p.c.a.) we understand any formula of the form $\phi \to \Box(\pi,\psi)$ where $\phi,\psi \in \mathrm{F}_d^k$ and π is a k-ary d-program for some $k \in \omega$.

(ii) Let ϕ,π,ψ,k be as in (i) and Th be a d-theory. We say that $\phi \to \Box(\pi,\psi)$ *is provable in Floyd–Hoare logic from (data) theory* Th, in symbols $\mathrm{Th} \overset{\mathrm{FH}}{\vdash} \phi \to \Box(\pi,\psi)$, iff there is a d-formula $\Phi \in \mathrm{F}_d^k$ such that

$$\mathrm{Th} \vdash \phi(\bar{x}) \to \Phi(\bar{x}),$$
$$\mathrm{Th} \vdash \Phi(\bar{x}) \wedge \bar{x}\pi\bar{y} \to \Phi(\bar{y}), \text{ and}$$
$$\mathrm{Th} \vdash \Phi(\bar{x}) \wedge \bar{x}\pi\bar{x} \to \psi(\bar{x}),$$

where $\vdash$ is first-order derivability, and $\bar{x}$, $\bar{y}$ stand for sequences of variables of length k.

Definition 1.3 Let d be a similarity type and $k \in \omega$, and let π be a k-ary d-program.

(i) Let $\mathbf{D}$ be a d-model, $R \subseteq {}^kD$, and $\bar{a} \in {}^kD$.

(a) Let χ be a d-formula. Then $\mathrm{indr}_a(\chi,\bar{x})$, or $\mathrm{indr}(\chi)$ for short, is defined to be the induction formula

$$(\chi(\bar{a}) \wedge (\forall\bar{x},\bar{y} \in R)[\chi(\bar{x}) \wedge \bar{x}\pi\bar{y} \to \chi(\bar{y})]) \to (\forall\bar{x} \in R)\chi(\bar{x})$$

where $\chi(\bar{a})$ is obtained from χ by substituting $\bar{a}$ for $\bar{x}$ in χ. (Notice that the formula $\mathrm{indr}(\chi)$ is not a d-formula because a new constant symbol $\bar{a}$ and a new k-ary relation symbol R occur in it, which are not symbols of d.) Now $\mathrm{Iar}_{R,a} = \{\mathrm{indr}_a(\chi,\bar{x}) : \chi \text{ is a } d\text{-formula and } \bar{x} \text{ is a sequence of variables of length } k\}$. We call $\mathrm{Iar}_{R,a}$ the set of *relational induction* formulas (with respect to the input $\bar{a}$ and the set of states R in $\mathbf{D}$, for program π). Whenever there is no danger of confusion, we shall omit the subscript R,a from $\mathrm{Iar}_{R,a}$.

(b) We say that R is *closed* under π if $\forall \bar{x}, \bar{y}[R(\bar{x}) \wedge \bar{x}\pi\bar{y} \rightarrow R(\bar{y})]$, that is, if $\bar{x}$ is in R then every possible next state $\bar{y}$ (allowed by program π) is also in R.

(c) We say that R is a *relational trace* of π in $\mathbf{D}$ with input $\bar{a}$, in symbols $\mathbf{D} \overset{r}{\models} \pi[R, \bar{a}]$, iff $\bar{a} \in R$, R is closed under π, and $\langle \mathbf{D}, R, \bar{a} \rangle \models \mathrm{Iar}$.

(ii) Let $\phi, \psi \in \mathrm{F}_d^k$ and let Th be a d-theory. We say that $\phi \rightarrow \Box(\pi, \psi)$ *follows from* Th *in relational trace semantics*, in symbols $\mathrm{Th} \overset{r}{\models} \phi \rightarrow \Box(\pi, \psi)$, if for every model $\mathbf{D}$ of Th, for every $R \subseteq {}^kD$ and $\bar{a} \in R$ we have that $\mathbf{D} \overset{r}{\models} \pi[R, \bar{a}]$ implies $\mathbf{D} \models (\phi(\bar{a}) \wedge b\pi b) \rightarrow \psi(b)$, for every $b \in R$.

We note that the relational trace semantics $\overset{r}{\models}$ defined above is a straightforward generalization of the relational trace semantics given in [7] and [23] for nondeterministic programs.

Theorem 1.1 *Let $\phi \rightarrow \Box(\pi, \psi)$ be a d-partial correctness assertion and let* Th *be a d-theory. Then*

$$\mathrm{Th} \overset{\mathrm{FH}}{\vdash} \phi \rightarrow \Box(\pi, \psi) \textit{ iff } \mathrm{Th} \overset{r}{\models} \phi \rightarrow \Box(\pi, \psi).$$

Proof: The proof is exactly the same as that of the Theorem in [22] except the *trivial* change that, instead of $R(\bar{x}) \rightarrow R(\pi(\bar{x}))$, we always have to write $\forall \bar{y}[R(\bar{x}) \wedge \bar{x}\pi\bar{y} \rightarrow R(\bar{y})]$.

(The Theorem in [22] states our Theorem 1.1 for deterministic programs only. The change indicated above follows from this difference: if we want to say that

(1.1) R is closed under π

then, instead of the functional formulation $\forall \bar{x}[R(\bar{x}) \rightarrow R(\pi\bar{x})]$, we have to say the relational (or nondeterministic) version $\forall \bar{x}, \bar{y}[R(\bar{x}) \wedge \bar{x}\pi\bar{y} \rightarrow R(\bar{y})]$. The same applies, of course, if (1.1) is formulated for some set other than R. E.g., $\mathrm{cl}(\psi)$ is defined to be $\psi(\bar{q}) \wedge \forall \bar{x}, \bar{y}[\psi(\bar{x}) \wedge \bar{x}\pi\bar{y} \rightarrow \psi(\bar{y})]$.)

Remark 1.2 Csirmaz and Pasztor independently suggested the following correction and simplification of the proof in [22]:

1. There is a misprint on p. 346: the definition of $\Phi_{\bar{q}}$ should be $\wedge\{\mathrm{cl}(\psi) \rightarrow \psi(\bar{x}) : \psi \in \Pi\}$.
2. The same proof goes through if we use the much simpler set $\{\wedge \Pi_0 : \Pi_0 \subseteq \{\phi_i : i \leq m\}\}$ instead of the set Π of all Boolean combinations of $\phi_0, \ldots, \phi_m$.

2 Nonstandard-time semantics In this section we first recall the so-called nonstandard-time semantics $\overset{N}{\models}$ for programs (or for p.c.a.'s) as it was formulated in [5]. This is the semantics developed in Nonstandard Logics of Programs (see e.g., [1]–[4], [8]–[10], [12], [16], [17], [19]–[21], [23], [25]). Then we shall recall Csirmaz's characterization (in terms of $\overset{N}{\models}$) of nondeterministic Floyd–Hoare logic from [5] as Corollary 2.1 herein, and we shall show that it is a consequence of our Theorem 1.1. Finally we shall give some generalizations and simple equivalent versions of Corollary 2.1 (i.e., Csirmaz's theorem).

Definition 2.1 (see [5], Definitions 1.1 and 1.2)

(i) Let **T** denote an arbitrary model of successor arithmetic, with universe denoted by T. That is, **T** is elementarily equivalent to $\langle \omega, 0, \text{suc} \rangle$. We call **T** a *time-structure.*

(ii) Let **D** be a d-model, **T** a time-structure, π a k-ary d-program, and $Q: T \to {}^{k}D$.

(a) We say that the function Q is a *π-homomorphism* iff $\mathbf{D} \models \bigwedge_{i \in T} Q(i) \pi Q(\text{suc } i)$.

(b) For every d-formula χ, the *time-induction* $\text{ind}_Q(\chi)$ is defined to be $(\chi(Q(0)) \wedge \bigwedge_{i \in T} [\chi(Q(i)) \to \chi(Q(\text{suc } i))]) \to \bigwedge_{i \in T} \chi(Q(i))$. Let $\text{ind}_Q =_{def} \{\text{ind}_Q(\chi) : \chi \text{ is a } d\text{-formula}\}$.

(c) Q is called a *time-trace* of π in **D** iff it is a π-homomorphism and $\mathbf{D} \models \text{Ind}_Q$.

(iii) Let $\phi \to \Box(\pi, \psi)$ be a d-p.c.a. and Th a d-theory. We say that $\phi \to \Box(\pi, \psi)$ *follows from* Th *in nonstandard-time semantics*, in symbols $\text{Th} \overset{\text{N}}{\models} \phi \to \Box(\pi, \psi)$, iff for every model **D** of Th, for every time-structure **T**, and for every time-trace $Q: T \to {}^{k}D$ of π, if $\mathbf{D} \models \phi(Q(0))$ then $\mathbf{D} \models \bigwedge_{i \in T} [Q(i) = Q(\text{suc } i) \to \psi(Q(i))]$.

Corollary 2.1 (Csirmaz [5]) *Let $\phi \to \Box(\pi, \psi)$ be a d-partial correctness assertion and* Th *a d-theory. Assume that* $\text{Th} \models \forall \bar{x} \exists \bar{y} (\bar{x} \pi \bar{y})$. *Then (i) and (ii) below are equivalent:*

(i) $\text{Th} \overset{\text{FH}}{\vdash} \phi \to \Box(\pi, \psi)$

(ii) $\text{Th} \overset{\text{N}}{\models} \phi \to \Box(\pi, \psi)$.

Proof: (i) $\Rightarrow$ (ii) is easy to prove, therefore we prove here only (ii) $\Rightarrow$ (i). Let $\text{Th}, \phi, \psi, \pi$ be as in the formulation of Corollary 2.1. Let d^+ denote the following expansion of the similarity type d. For every $i \in \omega$, we add to d a new k-ary relation symbol R_i and k new constant symbols $c_1^i, c_2^i, \ldots, c_k^i$, and k more new constant symbols $e_1, e_2, \ldots, e_k$. Let $c_i = \langle c_1^i, c_2^i, \ldots, c_k^i \rangle$ and $e = \langle e_1, e_2, \ldots, e_k \rangle$. Roughly speaking, our expanded similarity type is $d^+ = d \cup \{R_i, c_i, e : i \in \omega\}$. Let Th^+ denote the following set of formulas of similarity type d^+:

$\text{Th} \cup \{\phi(\bar{x}/c_0),\ e \pi e,\ c_i \pi c_{i+1},\ \text{Iar}_{R_i, c_i},\ R_i(e),\ R_i(c_i),\ R_i \supseteq R_{i+1},\ (\forall \bar{x} \in R_i)(\exists \bar{y} \in R_i) \bar{x} \pi \bar{y} : i \in \omega,\ \bar{x} \text{ and } \bar{y} \text{ are sequences of variables of length } k\}$.

If $(\forall \bar{x} \in R)(\exists \bar{y} \in R) \bar{x} \pi \bar{y}$ for some k-ary relation R, then we say that R is *weakly closed* under π. If R is weakly closed, and in addition $\text{Iar}_{R,a}$ holds for R and for some $a \in R$, then we say that R is a *weak relational trace* of π (with input "a"). Using this terminology, Th^+ claims, among other things, that for every $i \in \omega$, R_i is a weak relational trace of π with input c_i and terminating at e.

For proving (ii) $\Rightarrow$ (i), it is enough to prove Claims 2.1.1 and 2.1.2 below.

Claim 2.1.1 $\text{Th} \overset{\text{N}}{\models} \phi \to \Box(\pi, \psi) \Rightarrow \text{Th}^+ \models \psi(e)$.

Claim 2.1.2 $\text{Th}^+ \models \psi(e) \Rightarrow \text{Th} \overset{\text{FH}}{\vdash} \phi \to \Box(\pi, \psi)$.

Proof of Claim 2.1.1: Assume that $\mathrm{Th} \overset{\mathrm{N}}{\models} \phi \to \Box(\pi,\psi)$ and that $\mathfrak{M} \models \mathrm{Th}^+$ for some $\mathfrak{M} = \langle \mathbf{D}, e, c_i, R_i \rangle_{i\in\omega}$ with $\mathbf{D} \in \mathrm{Mod}_d$, and $e, c_i \in R_i \subseteq {}^kD$. We may assume that $\mathfrak{M}$ is ω^+-saturated.[1] We want to prove that $\mathfrak{M} \models \psi(e)$.

Let $R_\infty =_{def} \bigcap\{R_i : i \in \omega\}$, $C =_{def} \{c_i : i \in \omega\}$, and $S =_{def} R_\infty \cup C$. We now show that:

(2.1) S is a weak relational trace of π in $\mathbf{D}$ with input c_0 and terminating at e.

In the proof of (2.1) the only nontrivial thing is proving

(2.2) $\langle \mathbf{D}, S, c_0 \rangle \models \mathrm{Iar}$.

To show (2.2), assume that (2.2) fails. Then

(2.3) $\langle \mathbf{D}, S, c_0 \rangle \models \chi(c_0) \wedge (\forall \bar{x}, \bar{y} \in S)[\chi(\bar{x}) \wedge \bar{x}\pi\bar{y} \to \chi(\bar{y})] \wedge (\exists \bar{z} \in S)\, \neg\chi(\bar{z})$

for some $\chi \in \mathrm{F}_d$ with parameters from D. Let such a χ and $\bar{z}$ be fixed. Then $\bar{z} \in R_\infty$ and $\mathbf{D} \models \chi(c_i)$ for every $i \in \omega$. So, since $\mathfrak{M} \models \mathrm{Th}^+$, we have that $\mathfrak{M} \models \mathrm{Iar}_{R_i,c_i} \wedge R_i(c_i) \wedge R_i(\bar{z}) \wedge \chi(c_i) \wedge \neg\chi(\bar{z})$ for every $i \in \omega$. Thus, for every $i \in \omega$, there are $\bar{x}_i, \bar{y}_i \in R_i$ such that $\bar{x}_i \pi \bar{y}_i \wedge \chi(\bar{x}_i) \wedge \neg\chi(\bar{y}_i)$ holds. Then, since $R_i \supseteq R_{i+1}$ by Th^+ and since $\mathfrak{M}$ is ω-saturated, there are $\bar{x}_\infty, \bar{y}_\infty \in R_\infty \subseteq S$ with $\mathbf{D} \models \bar{x}_\infty \pi \bar{y}_\infty \wedge \chi(\bar{x}_\infty) \wedge \neg\chi(\bar{y}_\infty)$. This contradicts (2.3), thereby proving (2.2).

By (2.2), (2.1) is also true, i.e., S is really a weak relational trace. From *this particular* weak relational trace S it is easy to construct a time-trace of π starting at c_0 and terminating at e. Then, by our assumption that $\mathrm{Th} \overset{\mathrm{N}}{\models} \phi \to \Box(\pi,\psi)$, we have that $\mathbf{D} \models \psi(e)$, which proves Claim 2.1.1.

For the sake of completeness, we include here the straightforward construction of a time-trace Q from S:

If $e \in C$ then the desired time-trace is $\langle c_i : i \in \omega \rangle$. Assume that $e \notin C$. For constructing a time-trace in this case, we first show that

(2.4) every element of R_∞ has a π-predecessor in R_∞.

First observe that if $c_i \in R_\infty$ then c_i has a π-predecessor in R_∞, because if c_i has no π-predecessor in R_n then it has none in R_{n+1} either. Therefore by Ind_{R_n,c_n} and $\mathrm{Ind}_{R_{n+1},c_{n+1}}$, we have that both $c_i = c_n$ and $c_i = c_{n+1}$. Thus $c_i \pi c_i$, proving that c_i *does* have a π-predecessor in each R_n. Then, by compactness, it has one in R_∞ too. To prove (2.4), let $b \in R_\infty$. By the above we may assume that $b \notin C$. Then, by Ind_{R_i,c_i}, b has a π-predecessor in every R_i. Hence, by compactness, it has one in R_∞ too. We have proved (2.4).

Let $\mathbf{Z}$ denote the set of all integers. For every $b \in R_\infty$ there is a π-homomorphism $Q_b : \langle \mathbf{Z}, \mathrm{suc} \rangle \to R_\infty$ with $b \in \mathrm{Rng}(Q_b)$, since every $\bar{y} \in R_\infty$ has a π-predecessor by (2.4), and a π-successor since S is weakly closed. Let Q_b^+ be the same as Q_b with the only change that its domain is made disjoint from everything else (e.g., we may choose $\mathrm{Dom}(Q_b^+) = \mathbf{Z} \times \{b\}$). For every $b \in R_\infty$ let us fix such a Q_b^+. Now we let $Q =_{def} (\bigcup\{Q_b^+ : b \in R_\infty\}) \cup \langle c_i : i \in \omega \rangle$, and define 0 and suc on $T =_{def} \mathrm{Dom}(Q)$ in the obvious way.

It is easy to see that Q is a time-trace with the desired properties.

Proof of Claim 2.1.2: Assume that $\mathrm{Th}^+ \models \psi(e)$. Then, by compactness, there is a finite subset $\mathrm{Ax} \subseteq \mathrm{Th}^+$ such that $\mathrm{Ax} \models \psi(e)$. We may assume that there is an $n \in \omega$ such that

$$\mathrm{Ax} = \mathrm{Th} \cup \{\phi(\bar{x}/c_0),\ e\pi e,\ c_i\pi c_{i+1},\ \mathrm{Iar}_{R_i,c_i},\ R_i(e),\ R_i(c_i),\ R_i \supseteq R_{i+1},\ (\forall \bar{x} \in R_i)(\exists \bar{y} \in R_i)\ \bar{x}\pi\bar{y} : i \leq n,\ \bar{x} \text{ and } \bar{y} \text{ are sequences of variables of length } k\}.$$

Let this n be fixed, and let $\phi_m(\bar{x})$ be the formula

$$\exists \bar{z}_0 \ldots \exists \bar{z}_m [\phi(\bar{z}_0) \wedge \bar{z}_m = \bar{x} \wedge \bar{z}_0 \pi \bar{z}_1 \wedge \bar{z}_1 \pi \bar{z}_2 \wedge \ldots \wedge \bar{z}_{m-1} \pi \bar{z}_m].$$

Let $\eta(\bar{x})$ be $\phi_n(\bar{x})$. Now Claims 2.1.2.1 and 2.1.2.2 together prove Claim 2.1.2.

Claim 2.1.2.1 $\mathrm{Th} \overset{\mathrm{FH}}{\vdash} \eta \to \Box(\pi, \psi) \Rightarrow \mathrm{Th} \overset{\mathrm{FH}}{\vdash} \phi \to \Box(\pi, \psi)$.

Proof of Claim 2.1.2.1: Assume that $\mathrm{Th} \overset{\mathrm{FH}}{\vdash} \eta \to \Box(\pi, \psi)$. Then by the definition of $\overset{\mathrm{FH}}{\vdash}$, there is a formula $\Phi(\bar{x}) \in \mathrm{F}_d$ such that

(2.5) $\mathrm{Th} \models \eta(\bar{x}) \to \Phi(\bar{x})$

(2.6) $\mathrm{Th} \models \Phi(\bar{x}) \wedge \bar{x}\pi\bar{y} \to \Phi(\bar{y})$ and

(2.7) $\mathrm{Th} \models \Phi(\bar{x}) \wedge \bar{x}\pi\bar{x} \to \psi(\bar{x})$.

Let $\Phi^+(\bar{x})$ be $\Phi(\bar{x}) \vee (\vee\{\phi_m(\bar{x}) : m \leq n\})$. We now show that Φ^+ establishes $\mathrm{Th} \overset{\mathrm{FH}}{\vdash} \phi \to \Box(\pi, \psi)$. Indeed, the following holds

(2.8) $\mathrm{Th} \models \phi(\bar{x}) \to \Phi^+(\bar{x})$

since $\phi(\bar{x}) \Rightarrow \phi_0(\bar{x}) \Rightarrow \Phi^+(\bar{x})$. Next assume Th together with $\Phi^+(\bar{x}) \wedge \bar{x}\pi\bar{y}$. If $\Phi(\bar{x})$ then $\Phi(\bar{y})$ by (2.6). If $\neg\Phi(\bar{x})$ then $\neg\eta(\bar{x})$ by (2.5), so since $\Phi^+(\bar{x})$, there is an $m \not\leq n$ such that $\phi_m(\bar{x})$ holds (by the definition of Φ^+). By the definition of ϕ_{m+1}, $\mathrm{Th} \models \phi_m(\bar{x}) \wedge \bar{x}\pi\bar{y} \to \phi_{m+1}(\bar{y})$. Thus $\mathrm{Th} \models \Phi^+(\bar{y})$ since $m + 1 \leq n$. We have proved

(2.9) $\mathrm{Th} \models \Phi^+(\bar{x}) \wedge \bar{x}\pi\bar{y} \to \Phi^+(\bar{y})$.

Next we assume that $\Phi^+(\bar{x}) \wedge \bar{x}\pi\bar{x}$. This implies $\Phi(\bar{x})$, since by $\bar{x}\pi\bar{x}$ we have that $(\forall m \leq n)[\phi_m(\bar{x}) \Rightarrow \eta(\bar{x})]$ which, by (2.5), yields $\Phi(\bar{x})$. Thus, by (2.7), we have proved

(2.10) $\mathrm{Th} \models \Phi^+(\bar{x}) \wedge \bar{x}\pi\bar{x} \to \psi(\bar{x})$.

(2.8), (2.9), and (2.10) together prove that $\mathrm{Th} \overset{\mathrm{FH}}{\vdash} \phi \to \Box(\pi, \psi)$.

Claim 2.1.2.2 $\mathrm{Ax} \models \psi(e) \Rightarrow \mathrm{Th} \overset{\mathrm{FH}}{\vdash} \eta \to \Box(\pi, \psi)$.

Proof of Claim 2.1.2.2: Assume that $\mathrm{Ax} \models \psi(e)$ and $\mathrm{Th} \overset{\mathrm{FH}}{\not\vdash} \eta \to \Box(\pi, \psi)$. Then, by Theorem 1.1, there are $\mathbf{D}, e, a, R$ such that $\mathbf{D} \models \eta(a) \wedge \neg\psi(e) \wedge e\pi e$ and R is a relational trace, etc.

By $\eta(a)$ then there are $c_0, c_1, \ldots, c_n \in {}^k D$ such that $\phi(c_0) \wedge c_0\pi c_1\pi c_2 \ldots c_{n-1}\pi c_n = a$. Let $R_m =_{def} \{c_m, \ldots, c_n\} \cup R$ for all $m \leq n$, and let $\mathfrak{M} = \langle \mathbf{D}, e, c_0, \ldots, c_n, R_0, R_1, \ldots, R_n \rangle$. Then $\mathfrak{M} \models \mathrm{Ax}$ which imples $\mathfrak{M} \models \psi(e)$, i.e., $\mathbf{D} \models \psi(e)$ by our assumption. This contradicts the definition of $\mathbf{D}$, proving that $\mathrm{Th} \overset{\mathrm{FH}}{\vdash} \eta \to \Box(\pi, \psi)$.

Claims 2.1.2.1 and 2.1.2.2 together prove Claim 2.1.2. And since we have now proved both Claims 2.1.1 and 2.1.2, this completes the proof of Corollary 2.1.

Corollary 2.2 *Corollary 2.1 remains true without the assumption*

$$\mathrm{Th} \models \forall \bar{x} \exists \bar{y} (\bar{x}\pi\bar{y}).$$

Proof: In this proof we use the terminology and notation of the proof of Corollary 2.1. Do *not* assume that

(2.11) $\mathrm{Th} \models \forall \bar{x} \exists \bar{y} (\bar{x} \pi \bar{y})$.

The whole proof of Corollary 2.1 works for the present Corollary 2.2 as well, *except* the proof of Claim 2.1.2.2 therein. In the proof of Claim 2.1.2.2 we had an R which was a relational trace by Theorem 1.1. This R was also a *weak* relational trace there because Corollary 2.1 assumes (2.11). Assuming (2.11), every relational trace is a weak relational trace as well. Without (2.11) R is not necessarily a *weak* relational trace. To fill in this gap, it is sufficient to construct a weak relational trace from the relational trace R. This is what we are going to do now.

Let $\mathbf{D}, e, a, R$ be as at the beginning of the proof of Claim 2.1.2.2. We may assume that $\langle \mathbf{D}, R \rangle$ is ω^+-saturated. Let $R^+ \subseteq R$ be the largest subset of R with $(\forall \bar{x} \in R^+)(\exists \bar{y} \in R^+) \bar{x} \pi \bar{y}$, i.e., let $R_0^+ =_{def} R$, $R_{n+1}^+ =_{def} \{\bar{x} \in R_n^+ : (\exists \bar{y} \in R_n^+) \bar{x} \pi \bar{y}\}$, and $R^+ =_{def} \bigcap_{n \in \omega} R_n^+$. Clearly $e \in R^+$, and also $a \in R^+$ (since $\langle \mathbf{D}, R \rangle$ is ω^+-saturated). Also, $\langle \mathbf{D}, R^+ \rangle$ is clearly ω^+-saturated. We now prove

(2.12) $R^+ \models \mathrm{Iar}$.

Assume

(2.13) $R^+ \not\models \mathrm{indr}(\chi)$ for some d-formula χ.

Then χ is preserved in R^+ and $R^+ \not\models \chi$.

Claim 2.2.1 *There is an $n \in \omega$ such that χ is preserved in R_n^+.*

Proof: Assume that, for every $n \in \omega$, there are $b_n, c_n \in R_n^+$ such that $\chi(b_n) \wedge b_n \pi c_n \wedge \neg \chi(c_n)$. Then there are $b_\infty, c_\infty \in R^+$ such that $\chi(b_\infty) \wedge b_\infty \pi c_\infty \wedge \neg \chi(c_\infty)$, since $\langle \mathbf{D}, R^+ \rangle$ is ω^+-saturated, which is a contradiction.

Let this n be fixed, and let $\chi^+(\bar{x}) =_{def} [\bar{x} \in R_n^+ \to \chi(\bar{x})]$.

Claim 2.2.2 $R \not\models \mathrm{indr}(\chi^+)$.

Proof: It is easy to check that χ^+ is preserved in R (assume that $b \pi c$ and investigate the cases $b \in R_n^+$ and $b \notin R_n^+$; use Claim 2.2.1, and observe that $(\bar{x} \pi \bar{y} \wedge \bar{y} \in R_n^+) \to \bar{x} \in R_n^+$. It follows that $\chi^+(a)$ and $R \not\models \chi$ by $R^+ \subseteq R$ and (2.13).

But $R \not\models \mathrm{indr}(\chi^+)$ contradicts the definition of R, so we have proved (2.12). Now we can repeat the whole proof of Corollary 2.1 with R replaced by R^+ in the proof of Claim 2.1.2.2, thus establishing Corollary 2.2.

Remark 2.1 Corollary 2.2 has a shorter proof, too. We wrote down the long proof above because we wanted to show how one can construct the "total part" of such a trace of a program π in which π is only partially defined. The shorter proof goes as follows: Let $\pi^+(\bar{x}, \bar{y}) =_{def} (\bar{x} \pi \bar{y} \vee (\neg \exists \bar{y} (\bar{x} \pi \bar{y}) \wedge \bar{x} = \bar{y})$ and $\psi^+ =_{def} \bar{x} \pi \bar{x} \to \psi(\bar{x})$. Now $\phi \to \Box(\pi^+, \psi^+)$ has a Floyd-Hoare proof Φ by Corollary 2.1. It is not hard to show that Φ is a Floyd-Hoare proof for $\phi \to \Box(\pi, \psi)$ as well.

In the proof of Corollary 2.1 we have seen how to construct a time-trace from a relational trace. In the proof of Proposition 2.3 below, we show how to construct a relational trace from a time-trace. The main point in Proposition 2.3 is *not* its statement (i) $\leftrightarrow$ (ii), since this equivalence trivially follows from Corollary 2.2 and Theorem 1.1. Instead, the point is in the proof which provides a *transfer principle* between $\models^{r}$ and $\models^{N}$. This is a direct construction of a relational trace $\bar{a} \in R \subseteq {}^{k}D$ from any (nonstandard) time-trace $Q: T \to {}^{k}D$ and vice versa. (Note that we do not assume that Th $\models \exists \bar{y}(\bar{x}\pi\bar{y})$ in Proposition 2.3.)

Proposition 2.3 *Let $\phi \to \Box(\pi, \psi)$ be a d-p.c.a. and* Th *a d-theory. Then (i) and (ii) below are equivalent:*
(i) Th $\models^{r} \phi \to \Box(\pi, \psi)$
(ii) Th $\models^{N} \phi \to \Box(\pi, \psi)$.

Proof: Proposition 2.3 follows from Theorem 1.1 and Corollary 2.2. However, we include a constructive proof here, to reveal a direct connection between the two semantics $\models^{r}$ and $\models^{N}$.

The construction for (ii) $\Rightarrow$ (i): Let $\mathfrak{A} = \langle \mathbf{D}, R, \bar{a} \rangle$ be a relational trace witnessing Th $\not\models^{r} \phi \to \Box(\pi, \psi)$. Form any nontrivial ultrapower $\mathfrak{A}' = \langle \mathbf{D}', R', a' \rangle$ of $\mathfrak{A}$ with index set ω. Then $\mathfrak{A}'$ is ω-saturated. Now, the construction in the proofs of Corollaries 2.1, 2.2 gives us a time-trace $Q: T \to R' \subseteq D'$ witnessing Th $\models^{N} \phi \to \Box(\pi, \psi)$.

The construction for (i) $\Rightarrow$ (ii): Let $Q: T \to {}^{k}D$ be a time-trace of π in $\mathbf{D}$ witnessing Th $\not\models^{N} \phi \to \Box(\pi, \psi)$. We construct a relational trace R of π in $\mathbf{D}$ witnessing Th $\not\models^{r} \phi \to \Box(\pi, \psi)$ as follows.

Let R be the smallest set containing $\mathrm{Rng}(Q)$ and closed under π. It is not hard to see that $\mathbf{D} \models^{r} \pi[R, Q(0)]$, since, trivially, $Q(0) \in R$ and R is closed under π, and $\langle \mathbf{D}, R, Q(0) \rangle \models \mathrm{Iar}$ can be seen as follows. Assume that $K \subseteq R$ is definable by some d-formula χ, $Q(0) \in K$, and K is closed under π. Then $\chi(Q(0)) \wedge \bigwedge_{i \in T} [\chi(Q(i)) \to \chi(Q(\mathrm{suc}\, i))]$, since Q is a π-homomorphism. From this we conclude that $\bigwedge_{i \in T} \chi(Q(i))$ by Ind_Q. Thus $\mathrm{Rng}(Q) \subseteq K \subseteq R$, which proves $R = K$ (by the definition of R and by R being closed under π), and therefore $\langle \mathbf{D}, R, Q(0) \rangle \models \mathrm{Iar}$.

We have proved that R is a relational trace of π with input $Q(0)$. By the definition of Q, $Q(j) = Q(\mathrm{suc}\, j)$ and $\neg\psi(Q(j))$ for some $j \in T$. Since $Q(j)\pi Q(\mathrm{suc}\, j)$ and $Q(j) \in R$, R witnesses Th $\not\models^{r} \phi \to \Box(\pi, \psi)$.

Remark 2.2 At the end of the Introduction of [5] the problem is raised whether Theorem 2 in [6] is true or not (since the proof in [6] contains an error). Using the notation of [16] and [23], Theorem 2 of [6] says that $\vdash^{FH} \equiv_{\Box}$ ($\mathrm{Ind}_{tqf} \cup \mathrm{Tord} \models^{N}$), that is, for any p.c.a. ρ, $\vdash^{FH} \rho$ iff ($\mathrm{Ind}_{tqf} \cup \mathrm{Tord}$) $\models^{N} \rho$. In terms of our Definition 2.1, Tord means the assumption that the time-scale $\mathbf{T}$ is linearly ordered, say by $\leq$, and Ind_{tqf} is a strengthened version of our time-induction Ind_Q. To be more precise, Ind_{tqf} is a "time-induction principle" ranging over those formulas in the language of the two-sorted model $\langle \langle \mathbf{T}, \leq \rangle, \mathbf{D}, Q \rangle$ which do not quantify over the elements of $\mathbf{T}$. Parameters from both sorts are allowed in Ind_{tqf}.

It appears that the answer to Csirmaz's problem is affirmative. Namely,

Theorem 2 of [6] seems to be provable by a suitable modification of the proof method of our Corollary 2.1 herein. However, I have not checked the details carefully.

Remark 2.3 The results and methods in the present paper were applied in [8] to obtain an analogous characterization for Hoare's inference system in its original axiomatic form; see Theorem II.5.21 on p. 155 there. The point of that result is in its concrete and explicit formulation concerning the syntax (of both Hoare's logic and the programming language). We note that Hoare's inference system was also characterized in [11].

NOTE

1. This is so because all the properties we are investigating are first-order ones; hence if we replace the original $\mathfrak{M}$ with its ω^+-saturated ultrapower nothing will change.

REFERENCES

[1] Andréka, H., "Sharpening the characterization of the power of Floyd's method," pp. 1–26 in *Logics of Programs and their Applications*, edited by A. Salwicki, Lecture Notes in Computer Science 148, Springer Verlag, Berlin, 1983.

[2] Andréka, H. and I. Németi, "Completeness of Floyd logic," *Bulletin of the Section of Logic*, Wroclaw 7 (1978), pp. 115–120.

[3] Andréka, H. and I. Németi, "Completeness of the Floyd method with respect to nonstandard time models" (in Hungarian), Seminar Notes, Mathematical Institute of the Hungarian Academy of Sciences–SZKI, 1977.

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

[5] Csirmaz, L., "A completeness theorem for dynamic logic," *Notre Dame Journal of Formal Logic*, vol. 26 (1985), pp. 51–60.

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

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

[8] Gergely, T., "Nonstandard programming logic," Technical Report, SZÁMALK Applied Logic Laboratory, Budapest, 1987.

[9] Gergely, T. and L. Úry, "Time models for programming logics," pp. 359–427 in *Mathematical Logic in Computer Science*, Colloquia Mathematica Societatis J. Bolyai, Vol. 26, edited by B. Dömölki and T. Gergely, North Holland, 1978.

[10] Gonzalez, M. T. H. and M. R. Artalejo, "Hoare's logic for nondeterministic regular programs: A nonstandard approach," preprint Universidad de Madrid 84/85/cc-1, 1985.

[11] Gonzalez, M. T. H. and M. R. Artalejo, "Hoare's logic for nondeterministic regular programs: A nonstandard completeness theorem," pp. 270–280 in *Automata, Languages and Programming*, edited by W. Brauer, Lecture Notes in Computer Science 194, Springer Verlag, Berlin, 1985.

[12] Hájek, P., "Some conservativeness results for nonstandard dynamic logic," pp. 443–449 in *Algebra, Combinatorics, and Logic in Computer Science*, Colloquia Mathematica Societatis J. Bolyai, Vol. 42, edited by J. Demotrovics, G. Katona, and A. Salomaa, North Holland, 1986.

[13] Leivant, D., "Logical and mathematical reasoning about imperative programs," in *Proceedings of POPL '85*.

[14] Makowsky, J. A. and I. Sain, "On the equivalence of weak second-order and nonstandard time semantics for various program verification systems," pp. 293–300 in *Proceedings of the First Annual IEEE Symposium on Logic in Computer Science*, Cambridge, Massachusetts, June 1986.

[15] Makowsky, J. A. and I. Sain, "Weak second-order characterizations of various program verification systems," Technical Report #457, TECHNICON–Israel Institute of Technology, June 1987. To appear in *Theoretical Computer Science*.

[16] Németi, I., "Nonstandard dynamic logic," pp. 133–348 in *Logics of Programs*, edited by D. Kozen, Lecture Notes in Computer Science 131, Springer Verlag, Berlin, 1982.

[17] Pasztor, A., "Nonstandard algorithmic and dynamic logic," *Journal of Symbolic Computation*, Academic Press, vol. 2 (1986), pp. 59–81.

[18] Pasztor, A., "Recursive programs and denotational semantics in absolute or nonstandard logics of programs," Preprint, Florida International University, School of Computer Science, 1987.

[19] Richter, M. M. and M. E. Szabo, "Nonstandard computation theory," pp. 667–693 in *Algebra, Combinatorics, and Logic in Computer Science*, Colloquia Mathematica Societatis J. Bolyai, Vol. 42, edited by J. Demetrovics, G. Katona, and A. Salomaa, North Holland, 1986.

[20] Sain, I., "Total correctness in nonstandard dynamic logic," *Bulletin of the Section of Logic*, Wroclaw-Kódz 2 (1983), pp. 64–70.

[21] Sain, I., "Structured nonstandard dynamic logic," *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, vol. 30 (1984), pp. 481–497.

[22] Sain, I., "A simple proof for completeness of the Floyd method," *Theoretical Computer Science*, vol. 35 (1985), pp. 345–348.

[23] Sain, I., "Relative program verifying powers of the various temporal logics," Preprint No. 40/1985, Mathematical Institute of the Hungarian Academy of Sciences, Budapest, 1985.

[24] Sain, I.,"The reasoning powers of Burstall's (modal logic) and Puueli's (temporal logic) program verification methods," pp. 302–319 in *Logics of Programs*, edited by R. Parikh, Lecture Notes in Computer Science 193, Springer Verlag, Berlin, 1985.

[25] Sain, I., "Total correctness in nonstandard dynamic logic," *Theoretical Computer Science*, to appear.

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest 1364, PF. 127
Hungary