Theoretical Computer Science 95 (1992) 75–95
Elsevier

Temporal logics need their clocks*

Ildikó Sain

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

Communicated by G. Mirkowska
Received July 1988
Revised January 1990

Abstract

Sain, I., Temporal logics need their clocks, Theoretical Computer Science 95 (1992) 75–95.

We investigate effective inference systems for first-order temporal logics from the point of view of completeness and soundness. Among others, the role of clocks in these issues will be somewhat clarified by our results. Some open problems from the literature of temporal logic will be solved.

1. Introduction

In this paper we solve some open problems raised in recent publications of the computer science temporal logic school represented by Manna–Pnueli [19, 20], Abadi–Manna [5], Abadi [1–4]. These problems concern the proof theoretic powers of the following inference systems:

- T_0 introduced in Manna–Pnueli [19, 20], and reformulated in [1–4] (the notation T_0 was introduced in the latter publications);
- the resolution system $\mathbb{R}$ of [5] with its final form in [3]; and
- T_1, T_2 of [1–4]. (T_1 is equivalent with $\mathbb{R}$, while the essence of T_2 is allowing recursive definitions "along time" in T_0.)

One of the main aims of the above quoted school is to find *adequate inference systems* for computer science temporal logics. The practical importance of this quest is explained in the introductions of e.g. [1–5]. An inference system is called adequate for a semantics iff it is both sound and complete for that semantics. To avoid misunderstandings, it is important to point out at this point that completeness issues in first-order philosophical logic, hence in particular in first-order temporal logic (FTL from now on) are of different character than those in classical first-order logic. Namely, in classical first-order logic one has an a priori fixed standard semantics, and all investigations are understood by definition w.r.t. that standard semantics.

* Research supported by Hungarian National Foundation for Scientific Research grant No. 1810.

In the FTL literature one usually investigates several different semantics. A semantics is usually given in the form of a class K of so called Kripke models. A semantics K is considered *natural* and useful if the definition of K is mathematically transparent, and mathematically familiar and natural. Usually, completeness investigations are done by looking at mathematically transparent semantics K_1, K_2, and comparing them with "proof theoretically attractive" inference systems $\vdash_1, \vdash_2$. (One of the main aims is to obtain theorems like saying that $\vdash_1$ is sound and complete for K_1.) See [13, p. $94^{5,6}$, § II.4.1, pp. 167-169, p. 290 § II.5.3.2] for more on this, and also for the reasons for this difference between the methods of classical- and philosophical logic.

Therefore, the quoted computer science FTL school (Abadi-Manna [5] etc.) starts out with two natural classes of Kripke models to be denoted below as $Mod(Ind + Tord)$ and $Mod(Ind + Tpa)$ on the semantic side[1], and with the most frequently used inference systems T_0 and $\mathbb{R}$ on the syntactic side. T_0 is a Hilbert-style system used in Manna-Pnueli [19, 20], in Kröger [17] to mention only a few sources. $\mathbb{R}$ is the machine implementation oriented "resolution" equivalent of T_0 (and/or of a slightly stronger version of T_0, cf. item (3) in Section 3). The above mentioned school discovered that T_0 is sound and incomplete for both semantics. They study the gap, and as is usual in the FTL literature, they search in both directions, namely they look both for natural semantical characterizations for T_0 and $\mathbb{R}$, *and* for reinforcements of T_0 that would be complete and sound for $Mod(Ind + Tord)$ and $Mod(Ind + Tpa)$ respectively. The candidates designed for these two model classes are the inference systems T_1 and T_2 respectively. Completeness was proved under the so called *clock condition*, and elimination (or clarification of the role) of this condition was raised as an *open problem* in several papers. Soundness of T_2 also needs some conditions, see Theorem 3 in Section 7 of the present paper. Here we prove theorems clarifying the role of the clock condition in the above mentioned inference systems. Actually, familiarity with these inference systems is not needed for an appreciation of our main results because we prove more general theorems which apply to arbitrary inference systems (satisfying some general conditions like recursive enumerability), and not only to the particular ones quoted above.

As indicated above, the project pursued by the quoted computer science FTL school is far from being finished (though many important results have been obtained). This is illustrated by the "Open questions" sections of [1-4]. The present paper is one in a series devoted to further advancing the quoted FTL project.

2. Syntax and semantics of FTL with modalities $\bigcirc$, $[F]$, U

Throughout, ω denotes the set of all natural numbers. We use first-order temporal logic (FTL) with modalities $\bigcirc$, $[F]$, and U denoting "nexttime", "always-in-the-

[1] The first one is based on the Time-frame being *ord*ered (this is abbreviated as *Tord*), while the second one on the Time-frame's being a model of *P*eano's *a*rithmetic (*Tpa*).

future", and "until" respectively. $\langle F \rangle$ abbreviates $\neg[F]\neg$, and reads "eventually". Given a first-order similarity type or language L, the usual predicate symbols etc. of L are considered to be *rigid*, i.e. their meanings do not change in time (cf. [13, p. 255]). Similarly, individual variables x_i ($i \in \omega$) are rigid. To this we add an infinity y_i ($i \in \omega$) of *flexible constants*. That is, the meaning of y_i is allowed to change in time. Other authors, see e.g. Abadi [1-4], add flexible predicates too, but we will not need them here though we will mention them occasionally. Our theorems remain true even if we allow flexible predicate and function symbols, as will be very easy to see. (This will be obvious from the proofs.) $Fm(FTL) = Fm_L(FTL)$ denotes the set of all FTL-formulas (of similarity type L) defined above. (Our "rigid-flexible" distinction coincides with the "global-local" distinction of Kröger [17].)

For semantic purposes, we use classical two-sorted models $\mathfrak{M} = \langle \mathbf{T}, \mathbf{D}, f_0, \ldots, f_i, \ldots \rangle_{i \in \omega}$ where $\mathbf{D}$ is a classical first-order structure of similarity type L, $\mathbf{T} = \langle T, 0, suc, \leq, +, \times \rangle$ is a structure similar to (of the same language as) the standard model $\mathbf{N} = \langle \omega, 0, suc, \leq, +, \times \rangle$ of arithmetic, and for $i \in \omega$, $f_i \in {}^T D$ (i.e. $f_i : T \to D$ is a function from T into D) serves to interpret the flexible constant y_i. $\mathbf{T}$ is called the time-frame of $\mathfrak{M}$, and, except for its language, is arbitrary. For simplicity, we often write y_i for f_i. *Mod* denotes the class of all models $\mathfrak{M}$ of the above kind. (To be precise, we should write Mod_L. The members of *Mod* are basically the same as Kripke models known from the traditional literature of FTL, cf. [13]. The next definition also agrees with the tradition of philosophical logic [13].)

To associate meanings to FTL-formulas in models from *Mod*, we follow the standard procedure of correspondence theory (cf. [13, § II.4.2.5, pp. 214–217]), and define a translation function

$$P : Fm(FTL) \to Fmcl(Mod),$$

where *Fmcl(Mod)* is the set of all *classical* (two-sorted) first-order formulas in the language of *Mod*. In *Fmcl(Mod)*, x_i ($i \in \omega$) are the variables of sort D (data), and t_i ($i \in \omega$) are variables of sort T (time). We may assume that all occurrences of the flexible constants y_i are of the form $y_i = x_j$ in the FTL-formulas (every formula is easily seen to be equivalent with one of this form as is well known, cf. [11]). For any $\varphi \in Fm(FTL)$, we let

$$P(\varphi) \stackrel{\text{def}}{=} \exists t_0 (t_0 = 0 \wedge P^*(\varphi, t_0)),$$

where $P^* : Fm(FTL) \times \{t_i : i \in \omega\} \to Fmcl(Mod)$ is defined as follows:

For every $t \in \{t_i : i \in \omega\}$ and $\varphi, \psi \in Fm(FTL)$,

- $P^*(y_i = x_j, t) \stackrel{\text{def}}{=} (f_i(t) = x_j)$ (here instead of $f_i(t)$ one could write $y_i(t)$),
- $P^*(\psi, t) \stackrel{\text{def}}{=} \psi$ whenever ψ is atomic and does not contain flexible symbols,
- P^* preserves classical connectives and quantifiers, i.e.,

$$P^*(\varphi \wedge \psi, t) \stackrel{\text{def}}{=} P^*(\varphi, t) \wedge P^*(\psi, t),$$

$$P^*(\neg\varphi, t) \stackrel{\text{def}}{=} \neg P^*(\varphi, t), \qquad P^*(\exists x_i \varphi, t) \stackrel{\text{def}}{=} \exists x_i P^*(\varphi, t)$$

and

- $P^*(\bigcirc\varphi, t) \stackrel{\text{def}}{=} \exists t_1(t_1 = suc(t) \wedge P^*(\varphi, t_1))$,
- $P^*([F]\varphi, t) \stackrel{\text{def}}{=} (\forall t_1 \geq t)P^*(\varphi, t_1)$,
- $P^*(\varphi U\psi, t) \stackrel{\text{def}}{=} (\forall t_1 \geq t)(P^*(\varphi, t_1) \vee \exists t_2(t \leq t_2 \leq t_1 \wedge P^*(\psi, t_2)))$.

This completes the definition (by recursion) of the translation functions P and P^*. We let

$$\mathfrak{M} \models \varphi \stackrel{\text{def}}{\Leftrightarrow} \mathfrak{M} \models P(\varphi), \quad \text{for any } \varphi \in Fm(FTL).$$

Here $\mathfrak{M} \models P(\varphi)$ is understood in the usual classical sense.

If $t \in T$ and $\varphi \in Fm(FTL)$ then, following the tradition (cf. [13, p. 466]), we let

$$\mathfrak{M}, t \Vdash \varphi \text{ iff } t \Vdash \varphi \text{ iff } (\mathfrak{M}, t) \models P^*(\varphi, t).$$

Intuitively, $t \models \varphi$ means that φ is true at time t in $\mathfrak{M}$. At this point it might be useful to observe that $\mathfrak{M} \models \varphi \Leftrightarrow \mathfrak{M}, 0 \Vdash \varphi$.

For any $K \subseteq Mod$, we let

$$K \models \varphi \stackrel{\text{def}}{\Leftrightarrow} (\forall \mathfrak{M} \in K)\mathfrak{M} \models \varphi.$$

A model $\mathfrak{M} = \langle \mathbf{T}, \ldots \rangle$ is called a *standard-time model* iff $\mathbf{T} = \mathbf{N}$, i.e. iff $\mathbf{T}$ is the standard model of arithmetic.

For any $\varphi \in Fm(FTL)$, $\models^{\omega} \varphi$ is defined to hold iff φ is valid in every standard-time model.

The semantics $\models^{\omega} \varphi$ is too restrictive, while $Mod \models \varphi$ is too general. Therefore, as usual in modal- and temporal logic, we introduce first-order axiomatizable subclasses of *Mod*, and will use *these* for semantic purposes. To this end, we recall three sets *Ind*, *Tord*, $Tpa \subseteq Fmcl(Mod)$ of postulates called "induction", "ordering of time", and "Peano's arithmetic for time" respectively. These are used in the literature for singling out workable model classes (i.e. semantics) for FTL.[2]

$$Ind \stackrel{\text{def}}{=} \{\varphi(0) \wedge \forall t(\varphi(t) \to \varphi(suc(t))) \to \forall t\varphi(t) \colon \varphi \in Fmcl(Mod)\},$$

where $\varphi(0)$ is obtained from φ by replacing the free occurrences of t in φ with 0, and similarly for $\varphi(suc(t))$. Since $\varphi(t)$ may contain free variables other than t, this induction allows the use of parameters.

Tpa denotes the usual set of Peano's axioms for the sort (or structure) $\mathbf{T}$.

Tord postulates the consequences of *Tpa* for the reduct $\langle T, 0, suc, \leq \rangle$ of $\mathbf{T}$. So, the main difference between *Tord* and *Tpa* is that *Tord* ignores $+$ and $\times$. Thus when using $(Ind + Tord)$ as semantics, we will pretend that $+$ and $\times$ are not there. See the 1977 version of [7] or [8] for more detail, where the present approach (including P and P^*) to FTL was first introduced (adapting the standard methodology of philosophical logic to computer science temporal logics). Later

[2] These postulate systems were first proposed for the present purpose by the NLP school, see e.g. Sain [23], Németi [21, 8, 7], Hájek [16].

Abadi [1-4] adopted the same definitions from [7] etc. with some notational differences to be indicated soon.

For any $Th \subseteq Fmcl(Mod)$ and $\varphi \in Fm(FTL)$, we let

$$Mod(Th) \stackrel{\text{def}}{=} \{\mathfrak{M} \in Mod : \mathfrak{M} \models Th\}, \quad \text{and}$$

$$Th \models \varphi \stackrel{\text{def}}{\Leftrightarrow} Mod(Th) \models \varphi.$$

Now, the two most frequently used semantics for FTL-formulas φ are

$$(Ind + Tord) \models \varphi \quad \text{and} \quad (Ind + Tpa) \models \varphi.$$

Abadi [1-4] writes $\vdash_0 P(\varphi)$ and $\vdash_P P(\varphi)$ for $(Ind + Tord) \models \varphi$ and $(Ind + Tpa) \models \varphi$ respectively. (In $\vdash_0$ the subscript can be thought of as the abbreviation of "ordering on time", while P in $\vdash_P$ abbreviates "Peano's arithmetic".) Further, Abadi writes $\models \varphi$ for our $\models^\omega \varphi$. (See e.g. [3, bottom of p. 9].)

The notation $Ind \models \varphi$ might seem confusing, since Ind is in one language, $Fmcl(Mod)$, while φ is in another, namely in $Fm(FTL)$. However, these two languages have the same class Mod of models, thus our notation makes sense.

3. Inference systems for FTL

Next we will consider inference systems for FTL. Our theorems will be about arbitrary inference systems satisfying certain general conditions (see conditions (a), (a*), (b) in Theorem 1 in Section 4). However, as special cases of these, we will consider four concrete inference systems, $T_0, \mathbb{R}, T_1$, and T_2 introduced in Manna-Pnueli [19, 20], Abadi-Manna [5], and Abadi [1-4]. Our theorems solve, among others, open problems raised about these inference systems in the quoted papers.

Let $\vdash$ be an inference system for FTL. Let $K \subseteq Mod$. Following the tradition, we say that $\vdash$ is *complete* for $(K \models)$ iff

$$(\forall \varphi \in Fm(FTL))(K \models \varphi \;\Rightarrow\; \vdash \varphi).$$

Soundness of $\vdash$ for $(K \models)$ means the opposite: we say that $\vdash$ is *sound* for $(K \models)$ iff

$$(\forall \varphi \in Fm(FTL))(K \models \varphi \;\Leftarrow\; \vdash \varphi).$$

If $\Sigma \subseteq Fmcl(Mod)$ then, instead of "$(Mod(\Sigma) \models)$", we sometimes write "$(\Sigma \models)$". That is, "$\vdash$ is complete (sound) for $(\Sigma \models)$" means that $\vdash$ is complete (sound) for $(Mod(\Sigma) \models)$. For brevity, we often write "K" and "Σ" for the semantics $(K \models)$ and $(\Sigma \models)$ respectively.

In the rest of this section we say a little more about the (concrete) inference systems $T_0, \mathbb{R}, T_1, T_2$. However, for obtaining our results concerning them, all we need to know about them is that they satisfy conditions (a), (a*), (b) in Theorem 1 in Section 4. Thus, the reader not interested in these particular inference systems may safely ignore the rest of this section. $\vdash_{Ti}$ and $\vdash_{\mathbb{R}}$ denote provability in T_i and $\mathbb{R}$ respectively ($i \in \{0, 1, 2\}$).

(1) $T_0 \leq \mathbb{R} \leq T_1 \leq T_2$, where $\leq$ denotes proof theoretic comparison, that is

$$T_i \leq T_j \text{ iff } (\vdash_{T_i} \varphi \Rightarrow \vdash_{T_j} \varphi) \text{ for all } \varphi \in Fm(FTL).$$

(2) T_0 is a very natural "basic" inference system. Roughly, T_0 is equivalent with the following (A1)+(A2):

(A1) is a Hilbert-style complete axiomatization of *Mod.*

(A2) contains all first-order instances of all $\vDash^{\omega}$-valid propositional FTL-schemes. It is known that (A2) is decidable, and many finite axiomatizations are known for (A2), cf. e.g. [14, 15]. T_0 is often investigated in the literature, see Manna–Pnueli [19, 20], Kröger [17, cf. Σ_{TP} in § III.9, and "Table of Laws and Rules"]; it is the natural first-order extension of the system in [14], or of that in [15, § 9, p. 73].

(3) $\mathbb{R}$ is a resolution system equivalent with T_0 or T_1, depending on which paper we quote.

(4) T_1 and T_2 are extensions of T_0. If R is a new rigid predicate symbol not occurring in any of $\varphi, \psi \in Fm(FTL)$, then

$$\vdash((R(\bar{x}) \leftrightarrow \psi(\bar{x})) \to \varphi) \Rightarrow \vdash \varphi$$

is the new rule which, when added to T_0, yields T_1. T_2 is obtained from T_1 by adding a similar new rule allowing "definitions of" new flexible symbols (by temporal recursion).

The new rule distinguishing T_1 and T_0 can, basically, be simulated by adding a "real always" (i.e. S5) modality $\Box$ in addition to the present always-in-the-future $[F]$ to FTL as in Goldblatt [15, p. 30] or Sain [25]. To simulate exactly the new rule of T_1, the modality J (for jetzt i.e. "now" introduced by Kamp in 1971) seems to be the most widely used tool in the literature of temporal logics, see [13, § II.2.4.10, p. 121]. $J\varphi$ is denoted as *First* φ in the NLP literature, e.g. in [21, 22, 24, 25].

The new rule in T_2 is very close to the comprehension schema *Ex* introduced in the 1979 version of Andréka–Németi–Sain [8] for computer science temporal logics. (Makowsky–Sain [18] reviews some of the "metamorphoses" or disguises *Ex* went through in the computer science literature since 1979.)

(5) T_1 is sound for $(Ind + Tord)$, T_2 was designed to be sound for $(Ind + Tpa)$ but it is not[3] (see Theorem 3 in Section 7). For more information on T_2 see Section 7.

It would be nice to know if some of T_0, T_1, T_2 is complete for *Ind* or $(Ind + Tord)$. As will follow from Theorem 2, none of them is complete for $(Ind + Tpa)$. If U

[3] There is a mistake in the soundness proof for T_2 in [2] etc., but for our present purposes, until we reach Theorem 3, we may pretend that T_2 is sound for $(Ind + Tpa)$. See also the footnote at the end of the proof of Claim 2.2 in Section 5.

(until) is omitted then T_0 and T_1 become incomplete for *Ind* and (*Ind* + *Tord*) respectively. (For proofs see [9, Theorems 17, 21].)

4. Clocks and arithmetical formulas

Let $\gamma(\bar{x}) \in Fm(FTL)$ with $\bar{x} = \langle x_0, \ldots, x_n \rangle$ as free variables. Recall from [1-4] that the *clock condition* $C(\gamma)$ for γ is the FTL-formula

$$C(\gamma) \stackrel{\text{def}}{=} [F]\exists\bar{x}\gamma(\bar{x}) \wedge [F]\forall\bar{x}(\gamma(\bar{x}) \rightarrow \bigcirc[F]\neg\gamma(\bar{x})).$$

Intuitively, $C(\gamma)$ says that γ "behaves like a clock", that is, it distinguishes different time instances from each other. If $C(\gamma)$ holds, γ is called a clock.

Let $\vdash$ be an arbitrary inference system for FTL. An FTL-formula φ is said to be *arithmetical in* $\vdash$ iff there is $\gamma \in Fm(FTL)$ with $(\vdash(C(\gamma) \rightarrow \varphi) \Rightarrow \vdash\varphi)$, see [1-4]. That is, φ is *not* arithmetical in $\vdash$ if $C(\gamma)$ is really useful in proving φ, i.e. if $\vdash(C(\gamma) \rightarrow \varphi)$ for all γ but $\nvdash\varphi$.

Thus there are many arithmetical formulas: if $\vdash\varphi$ or if $\nvdash(C(\gamma) \rightarrow \varphi)$ for some γ then φ is arithmetical in $\vdash$. Also, any formula of the form $(C(\gamma) \rightarrow \varphi)$ is arithmetical (under very mild assumptions on $\vdash$). A natural example for a nonarithmetical formula is $\exists x \exists x_1(x \neq x_1)$. But this formula is not valid. It is much harder to find a nonarithmetical φ such that $\models^{\omega} \varphi$. Indeed, [2, § 6 "Clocks and arithmetical formulas"] contains a question asking for "more subtle examples" (than $\exists x \exists x_1(x \neq x_1)$) of nonarithmetical formulas. In Theorem 1 we will answer this question by exhibiting a nonarithmetical (in any of $T_0, \ldots, T_2$) temporal formula which is valid in all standard-time models. (We note, however, that among rigid formulas, i.e. ones not containing flexible symbols, there are no "more subtle" examples in the sense that for any rigid formula φ, φ is not arithmetical in $\vdash$ iff $Mod \models \exists x_0 \ldots \exists x_n(\bigwedge\{x_i \neq x_j : i < j \leq n\}) \rightarrow \varphi$ for some natural number n but $Mod \not\models \varphi$. This is easy to see, we only have to assume $T_0 \leq \vdash$.)

This quest for a more subtle nonarithmetical formula seems to be implicit in all of [1-4]. Namely, each of these papers contains a theorem[4] stating that every FTL formula valid in all standard-time models is arithmetical in T_2. Unfortunately, this theorem turns out to be *false* below. Probably, it was the lack of a timely answer to the above quoted open problem which had led to the belief in the truth of the above theorem. Unfortunately, the new discovery influences the status of the strongest available (by now) temporal inference system[5] which was designed to be equivalent with Peano's arithmetic. Namely, as will be indicated in Section 6, by our method elaborated in the proof below, one can also prove that this strongest available temporal inference system is not complete for (*Ind* + *Tpa*).

[4] See Theorem 6.2. p. 60_8 in [2], the theorem on p. 127 of [1], Theorem 5.16 on p. 75 of [3], the second theorem in § 6 of [4], p. 12.

[5] Cf. e.g. the "Abstract" of [2] (and "Capsule review" in the preprint form of [2]), as well as Theorem 7.2 therein, the proof of which essentially uses the above Theorem 6.2.

The "more subtle" example for a nonarithmetical temporal formula in Theorem 1 below is valid in standard-time models, but it is not valid in $(Ind + Tpa)$. Also, in [1, 2], Abadi asks if T_1 is complete for $(Ind + Tord)$. This, by a theorem of Abadi, is equivalent with asking whether there is a formula not arithmetical in T_1 but valid in $(Ind + Tord)$. The latter problem remains open.

Theorem 1.

(i) *There is an FTL-sentence* ψ *such that* $\models^{\omega} \psi$, *and* ψ *is* not arithmetical *in any of* $T_0, \mathbb{R}, T_1$, *or* T_2.

(ii) *There is an FTL-sentence* ψ *such that* $\models^{\omega} \psi$, *and* ψ *is* not arithmetical *in* any *proof system* $\vdash$ *satisfying* (a) *and* (b) *below.*

  (a) $\vdash$ *is sound for* $(Ind + Tpa)$.

  (b) (1) $\vdash$ *is complete for Mod,*

    (2) $\vdash(\varphi \wedge [F](\varphi \to \bigcirc\varphi)) \to [F]\varphi$ *(induction), and* $\vdash [F]\varphi \to (\varphi \wedge \bigcirc[F]\varphi)$, *for any* $\varphi \in Fm(FTL)$, *further*

    (3) $\vdash$ *is closed under the rules of modus ponens and necessitation, i.e.* $\vdash\varphi$ *implies both* $\vdash[F]\varphi$ *and* $\vdash\bigcirc\varphi$.

(iii) *In* (ii) *above,* (a) *can be replaced with the following condition:*

  (a*) *The "$\vdash$-provable" formulas form a recursively enumerable set, and* $\vdash$ *is sound for* $\models^{\omega}$.

Proof. Will be given in Section 5. □

We recall from [1-4] (see the "Open questions" sections), that *adding a clock to* $\vdash$ is defined as introducing a rule

$$(\vdash(C(c(\bar{x})) \to \varphi) \Rightarrow \vdash\varphi),$$

where c is a flexible predicate symbol not occurring in $\varphi \in Fm(FTL)$. We call such a rule a *clock rule.* The reason we did not allow flexible predicate symbols in our language was only to keep things simple: It is straightforward how to introduce flexible predicate symbols, and give meanings to them. The reader not wanting to change the language introduced so far may replace $c(\bar{x})$, in the definition of a clock rule, with $y_i = x_0$ where y_i does not occur in φ. Theorem 2 below is true for both versions.

As pointed out in the quoted papers, a clock rule can be sound for models having infinite data domains ($|D| \geq \omega$) only. Hence, whenever clock rules are considered, we automatically restrict the semantical considerations to models with infinite data domains. So when considering clock rules we will use the semantics $(Ind + Tpa +$ "$|D| \geq \omega$") instead of the original $(Ind + Tpa)$, and similarly for *Tord.*

It is proved in [1-4] that T_1 and T_2 are complete for $(Ind + Tord)$ and $(Ind + Tpa)$ respectively, *if* we consider arithmetical formulas only. Hence, if we add clocks to T_1 and T_2, then the new systems become complete for $(Ind + Tord)$ and $(Ind + Tpa)$ respectively. However, we have to pay an unexpected price for this: we will prove in Theorem 2 (iii) below that the new systems are not sound for $(Ind + Tpa + \text{"}|D| \geqslant \omega\text{"})$. This seems to contradict a sentence in Section 9 "Open questions" of [1, 2], where Abadi writes that adding a clock to T_1 is harmless. The last sentence in the "Open questions" sections of [1–4] asks if a clock adds power to T_1 or $\mathbb{R}$. (The question is understood modulo infinite data domains, of course.) Theorem 2 below answers this question in the affirmative. In particular, the suggested clock rule turns out to be *not sound* for $(Ind + Tord)$, or even for $(Ind + Tpa)$ modulo infinite domains.

Recall that $\vdash_{\mathbb{R}}$ and $\vdash_{T_1}$ denote provability in $\mathbb{R}$ and T_1 respectively.

Theorem 2.

(i) *The inference systems $\mathbb{R}$ and T_1 become stronger if we add clocks to them. That is, for $\vdash \in \{\vdash_{\mathbb{R}}, \vdash_{T_1}\}$,*

$$\textit{there is a } \varphi \in Fm(FTL) \textit{ with } \models^{\omega} \varphi, \nvdash \varphi, \textit{ but } \vdash (C(c(\bar{x})) \to \varphi). \tag{$\dagger$}$$

(ii) *Adding a clock adds power to any proof system $\vdash$ satisfying* (a*) *and* (b) *of Theorem* 1. I.e., ($\dagger$) *above holds for any $\vdash$ satisfying* (a*) *and* (b).

(iii) *If we add a clock rule to any $\vdash$ satisfying* (b) *in Theorem* 1, *then the so reinforced system is not sound for $(Ind + Tpa + \text{"}|D| \geqslant \omega\text{"})$. In particular, if we add clocks to $\vdash_{\mathbb{R}}$ or $\vdash_{T_1}$ then the so reinforced system is not sound for the semantics denoted by $\vdash_0$ or for the one denoted by $\vdash_P$ in Abadi* [1–4] (*even if $\vdash_0$ and $\vdash_P$ are restricted to infinite data domains*).

Proof. Will be given in Section 5. □

5. Proof of Theorems 1 and 2

In set theory, therefore also in Peano arithmetic, there are many nonequivalent notions of finiteness. Examples of these are Dedekind-finiteness, and being isomorphic to a natural number. Our *idea* of proving ($\dagger$) of Theorem 2 above is the following: We consider two different notions of finiteness, call them *FINITE*1 and *FINITE*2. We define φ to be the equivalence of these two notions, more precisely, φ states that "the data domain **D** is finite according to *FINITE*1" is equivalent to "the data domain **D** is finite according to *FINITE*2". Shortly,

$$\varphi \stackrel{\text{def}}{=} ((\mathbf{D} \text{ is } \mathit{FINITE}1) \Leftrightarrow (\mathbf{D} \text{ is } \mathit{FINITE}2)).$$

Then φ holds in standard time models (because both *FINITE*1 and *FINITE*2 mean "real finiteness" there). This gives us $\models^{\omega} \varphi$. But φ is not valid logically (e.g. in Peano arithmetic) since we chose two *different* notions of finiteness. ("Different" means exactly that they are not equivalent *logically*.) From this $\nvdash \varphi$ will follow. The notion of a clock is a very strong notion of infinity. Therefore, if the choices of *FINITE*1 and *FINITE*2 are "clever enough", then both $\neg FINITE1$ and $\neg FINITE2$ will follow from a clock. Thus we will have $\vdash (C(\ldots) \to \varphi)$.

We implement the above idea as follows:

(a) Instead of $FINITE1 \Leftrightarrow FINITE2$, it will be enough to postulate $FINITE1 \Rightarrow FINITE2$ in φ.

(b) "**D** is *FINITE*1" will be chosen to be "$\mathbf{D} \cong$ (an initial segment of **T**)", while "**D** is *FINITE*2" will be chosen to be "$\mathbf{D} \models Con(PA)$", where $Con(PA)$ denotes the usual formula in the language of Peano arithmetic stating that PA (the set of Peano's axioms) is consistent.

*FINITE*2 is a very weak notion of finiteness since all what we know about it is the fact that it is true in every finite model (but not vice versa). But this helps us in choosing φ according to (a) above (using $\Rightarrow$ only, instead of $\Leftrightarrow$).

To see (†), we must check the following two things:

(A) The two notions of finiteness were chosen "well enough" for having $\vdash (C(\ldots) \to \varphi)$ (the "clock-part of (†)").

(B) $FINITE1 \not\equiv FINITE2$.

(B) will be proved in Claim 2.2 below (by constructing a model). To see (A), it is enough to prove that $C(\ldots) \to \neg FINITE1$. This will be done in Claim 2.3, by induction.

Now we come to the details of the proof.

Let PA_0 denote a sufficiently strong finite part of Peano's axioms (PA) for $\mathbf{N} = \langle \omega, 0, suc, \leqslant, +, \times \rangle$. For instance, PA_0 states that $\leqslant$ is a linear discrete ordering, its usual relationship with *suc*, 0, and +, further PA_0 states the recursive definitions of + and × from *suc*. Let $(PA \restriction b)$ be obtained from PA_0 by replacing the axiom stating that there is no greatest element by the axioms $\forall x (x \leqslant b)$, $suc(b) = b$.[6] So, $(PA \restriction b)$ states that b is the greatest element, but arithmetic (+, ×, etc.) between 0 and b is the usual.

A typical model for $(PA \restriction b)$ is

$$(N \restriction n) \stackrel{\text{def}}{=} \langle \{0, 1, \ldots, n\}, 0, (suc \restriction n), (\leqslant \restriction n), (+ \restriction n), (\times \restriction n) \rangle$$

for any $n \in \omega$, where $(suc \restriction n)(n) = n$, and for $x < n$, $(suc \restriction n)(x) = x + 1$, and similarly for + and ×. Since $(PA \restriction b)$ is finite, we will identify it with the *sentence* $\forall \bar{x} (\bigwedge (PA \restriction b))$. We draw $(\mathbf{N} \restriction n)$ as

$$\underset{0}{\bullet} \to \underset{1}{\bullet} \to \bullet \cdots \bullet \to \underset{n-1}{\bullet} \to \underset{n}{\bullet}\!\circlearrowleft$$

So the horizontal $\to$ denotes successor, the point to the right is the bigger one, and we do not draw + and ×.

An infinite model for $(PA \restriction b)$ is

$$\underset{0}{\bullet} \to \underset{1}{\bullet} \to \underset{2}{\bullet} \to \bullet \cdots \bullet \to \underset{n}{\bullet} \to \cdots \underset{\infty}{\bullet}\!\circlearrowleft$$

[6] We note that we still require that $(\forall x < b)$ (*suc* is one-one).

where for all $n, m \in \omega$, ($n+m$, $n \times m$ are the usual, and if $n = \infty$ then $n+x = n \times x = \infty = b$ for all x). This is a fairly trivial model, and it satisfies $(PA \upharpoonright b)$ only because induction is *not* postulated in $(PA \upharpoonright b)$ (or in PA_0 for that matter).

Let φ_0 be the following temporal sentence:

$$(PA \upharpoonright b) \wedge y_0 = 0 \wedge [F]\exists x(y_0 = x \wedge \bigcirc y_0 = suc(x)) \wedge \langle F\rangle y_0 = b.$$

Let us recall from e.g. [10, pp. 828, 1136] that $Con(PA)$ is of the form $\forall x\sigma(x)$ with $\sigma(x)$ a Σ_0-formula. Intuitively, $\sigma(x)$ states that the sequence coded by x is not a derivation of *FALSE* from *PA*. Let φ_1 be the temporal sentence $\varphi_0 \wedge (\exists x < b)\neg\sigma(x)$. We define

(0) $\quad \chi \stackrel{\text{def}}{=} (\neg\varphi_1)$.

χ will play the role of φ in (†) in the formulation of Theorem 2. Referring back to our plan at the beginning of this section, we note that χ is equivalent with $\varphi_0 \rightarrow (\forall x < b)\sigma(x)$. φ_0 plays the role of "**D** is *FINITE*1", while $(\forall x < b)\sigma(x)$ plays the role of "**D** is *FINITE*2". Here note that this formula indeed says that $Con(PA)$ holds in **D**.

Claim 2.1. $\models^{\omega} \chi$.

We will return to the (easy) proof of this later.

Recall that Abadi's T_1 and T_2 are extensions of T_0, hence if some ψ is T_0-provable then it is automatically T_1- and T_2-provable.

Claim 2.2. $\nvdash_{T_2} \chi$, *and* $\nvdash \chi$ *if* $\vdash$ *satisfies* (a) *of Theorem* 1.

We will return to the proof later (Claim 2.2 will easily follow from Gödel's stronger incompleteness theorem and Abadi's soundness (for Peano's arithmetic) proof for T_2 i.e. [3, Theorem 5.17, p. 77]).

The following claim says that χ is provable from the assumption that a clock exists.

Claim 2.3. *Let* $\psi(\bar{x})$ *be any temporal formula. Then*

(i) $\vdash C(\psi) \rightarrow \chi$ *if* $\vdash$ *satisfies* (b) *of Theorem* 1, *and in particular*

(ii) $\vdash_{T_0} C(\psi) \rightarrow \chi$.

Proof of Claim 2.3. Assume $\vdash$ satisfies (b). Then

(6) for every propositional temporal formula π containing only $\bigcirc$ and $[F]$ as modalities, if $\models^{\omega} \pi$ then every FTL instance of π is provable by $\vdash$.

(6) follows from the propositional completeness theorem in Goldblatt [15, § 9, p. 73] (or equivalently from a similar theorem in [14]) because the axioms therein are $\vdash$-provable by (b). For completeness, we note that of (6) above, we will use only its special case (7), our proof of (7), and relatively easy consequences of these.

(7) $\quad \vdash \langle F\rangle[F]\varphi \rightarrow \bigcirc\langle F\rangle[F]\varphi$.

This can be derived from (b) directly, as follows: By (b) we have $\vdash \bigcirc[F]\langle F\rangle\varphi \to \langle F\rangle\varphi$ because $Mod \models \bigcirc(\varphi \to \psi) \to (\bigcirc\varphi \to \bigcirc\psi)$, and then the rest of the axioms and rules in (b) imply $\vdash [F]\varphi \to \varphi$, $\vdash \bigcirc[F]\varphi \to \bigcirc\varphi$, $\vdash \bigcirc\varphi \to \langle F\rangle\varphi$, $\vdash \langle F\rangle\langle F\rangle\varphi \to \langle F\rangle\varphi$, $\vdash \bigcirc[F]\langle F\rangle\varphi \to \langle F\rangle\varphi$ as was desired. To complete the proof of (7), assume now $\neg\bigcirc\langle F\rangle[F]\varphi$. Then $\bigcirc[F]\langle F\rangle\neg\varphi$. Let ψ be $\bigcirc[F]\langle F\rangle\neg\varphi$. By $\vdash$"$[F] \to \bigcirc[F]$", then $\psi \to \bigcirc\psi$. Thus, by induction, $[F]\bigcirc[F]\langle F\rangle\neg\varphi$ which, by $\vdash$"$\bigcirc[F]\langle F\rangle \to \langle F\rangle$", implies $[F]\langle F\rangle\neg\varphi$. We proved $\neg\bigcirc\langle F\rangle[F]\varphi \to \neg\langle F\rangle[F]\varphi$ proving (7).

Assume $\nvdash C(\psi) \to \chi$ and that $\vdash$ satisfies (b). Then, by (b), there exist a nonstandard model $\mathfrak{M} \in Mod$ of $\vdash$ and some time instance t_0 of $\mathfrak{M}$ such that $t_0 \Vdash C(\psi)$ and $t_0 \Vdash \varphi_1$, hence $t_0 \Vdash \varphi_0$. Let this $\mathfrak{M}$ and t_0 be fixed. Let $\bar{x} = \langle x_0, \ldots, x_n\rangle$ be the sequence of free variables of the temporal formula $\psi(\bar{x})$ in $C(\psi)$.

In the following lemma, n and t_0 are as above.

Lemma 2.3.1. *Let $i \leq n$ and $\rho(x_i, x_{i+1}, \ldots, x_n)$ be a temporal formula. Assume*

(7.1) $t_0 \Vdash \forall\bar{x}\langle F\rangle[F]\neg\rho(x_i, \ldots, x_n)$.

Then $t_0 \Vdash \forall\bar{x}\langle F\rangle[F]\neg\exists x_i\rho(x_i, \ldots, x_n)$.

Proof of Lemma 2.3.1. Let i and ρ be as in the lemma. As in the lemma, assume (7.1). We let the temporal formulas $clb_i(x, \rho)$ be $[F]\forall x_i(\rho(x_i, \ldots, x_n) \to x_i \geq x)$, and $tail_i$ be $\exists x(x = y_0 \wedge \langle F\rangle clb_i(x, \rho))$. From (7.1), we will prove by temporal induction that

(7.2) $t_0 \Vdash [F]tail_i$ for any fixed $\bar{x} \in {}^{(n+1)}D$.

Proof of (7.2): Let $\bar{x} \in {}^{(n+1)}D$ be arbitrary but fixed.

(7.I) $t_0 \Vdash tail_i$

follows from (7.1) and from $t_0 \Vdash \varphi_0$, the latter of which implies $t_0 \Vdash y_0 = 0$ and $\forall x_i(x_i \geq 0)$, hence $t_0 \Vdash clb_i(0, \rho)$, implying $t_0 \Vdash \langle F\rangle clb_i(0, \rho)$ since $\vdash \varphi \to \langle F\rangle\varphi$, for any φ, by (6) or the proof of (7). Assume

(7.II) $t' \geq t_0$ and $t' \Vdash tail_i$.

Then

(8) $t_0 \leq t' \Vdash (\langle F\rangle clb_i(x, \rho) \wedge x = y_0)$ for some x.

Fix this x. We will prove

(8.1) $t' \models \bigcirc\langle F\rangle clb_i(x+1, \rho)$.

An equivalent form of (7.1) is

(7.1⁺) $t_0 \Vdash \forall\bar{x}\forall x\langle F\rangle[F]\forall x_i(\rho(x_i, \ldots, x_n) \to x_i \neq x)$.

By (7.1⁺), $t' \Vdash \langle F\rangle[F]\forall x_i(\rho(x_i, \ldots, x_n) \to x_i \neq x)$. Then, using (8), the definition of $clb_i(x, \rho)$, and that $\vdash (\langle F\rangle[F]\alpha \wedge \langle F\rangle[F]\beta) \to \langle F\rangle([F]\alpha \wedge [F]\beta)$ for every α and β, we get $t' \Vdash \langle F\rangle([F]\forall x_i(\rho(x_i, \ldots, x_n) \to x_i \neq x) \wedge clb_i(x, \rho))$, hence

$$t' \Vdash \langle F\rangle[F]\forall x_i(\rho(x_i, \ldots, x_n) \to x \neq x_i \geq x).$$

That is, $t' \Vdash \langle F\rangle clb_i(x+1, \rho)$. Since $clb_i(\ldots)$ is of the form $[F]\varphi$, by (6) or by the proof of (7), (8.1) is proved. Since by (8) $t' \Vdash x = y_0$, by φ_0 we have $t' \Vdash \bigcirc(x+1 = y_0)$. Then, by $\mathfrak{M} \in Mod$, $t' \Vdash \bigcirc(x+1 = y_0 \wedge \langle F\rangle clb_i(x+1, \rho))$ that is $t' \Vdash \bigcirc tail_i$. Since at the beginning of the present item (7.II) the choice of $t' \geq t_0$ was arbitrary, we proved

$$t_0 \Vdash [F](tail_i \to \bigcirc tail_i).$$

From this and (7.I), temporal induction (i.e. (b)(2)) yields (7.2).

We now finish the proof of Lemma 2.3.1.

Let $\bar{x} \in {}^{(n+1)}D$ be arbitrary. By $t_0 \Vdash \varphi_0$ we have $t_0 \Vdash \langle F\rangle(y_0 = b)$. Then by (7.2) and by $[F] = \neg\langle F\rangle\neg$, $t_0 \Vdash \langle F\rangle(y_0 = b \wedge tail_i)$ which, by

$$(y_0 = b \wedge tail_i) \Rightarrow (y_0 = b \wedge \langle F\rangle clb_i(b, \rho))$$

implies $t_0 \Vdash \langle F\rangle clb_i(b, \rho)$. This by definition is $t_0 \Vdash \langle F\rangle[F]\forall x_i(\rho(x_i, \ldots, x_n) \to x_i \geq b)$.

At the same time, (7.1^+) implies $t_0 \Vdash \langle F\rangle[F]\forall x_i(\rho(x_i, \ldots, x_n) \to x_i \neq b)$. These two formulas yield, by (6) or by the proof of (7),

$$t_0 \Vdash \langle F\rangle[F](\forall x_i(\rho(x_i, \ldots, x_n) \to x_i \neq b) \wedge \forall x_i(\rho(x_i, \ldots, x_n) \to x_i \geq b)).$$

But by the $(PA \restriction b)$ part of φ_0 we have $\forall x_i(x_i \geq b \to x_i = b)$. Thus

$$t_0 \Vdash \langle F\rangle[F]\forall x_i \neg\rho(x_i, \ldots, x_n).$$

That is $t_0 \Vdash \langle F\rangle[F]\neg\exists x_i(\rho(x_i, \ldots, x_n)$. Since the choice of $\bar{x} \in {}^{(n+1)}D$ above was arbitrary, we proved $t_0 \Vdash \forall\bar{x}\langle F\rangle[F]\neg\exists x_i\rho(x_i, \ldots, x_n)$ $\square$.

Proof of Claim 2.3 (*continued*). From $C(\psi)$ one easily proves

(9) $\quad t_0 \Vdash \forall\bar{x}\langle F\rangle[F]\neg\psi(\bar{x})$,

where $\bar{x} = \langle x_0, \ldots, x_n\rangle$; as follows.

Let $\bar{x} \in {}^{(n+1)}D$ be arbitrary but fixed. If $t_0 \Vdash [F]\neg\psi(\bar{x})$, then we are done. Assume therefore $(\exists t_1 \geq t_0)t_1 \Vdash \psi(\bar{x})$. Then, by $t_0 \Vdash C(\psi)$, $t_1 \Vdash \bigcirc[F]\neg\psi(\bar{x})$, Hence, by the proof of (7), $t_0 \Vdash \langle F\rangle[F]\neg\psi(\bar{x})$. By the choice of $\bar{x} \in {}^{(n+1)}D$ we proved (9).

Let now $i \in \omega$ be arbitrary. Assume

(9.1) $\quad t_0 \Vdash \forall\bar{x}\langle F\rangle[F]\neg\exists x_0 \ldots x_{i-1}\psi(\bar{x})$.

Choosing $\rho(x_i, \ldots, x_n)$ to be $\exists x_0 \ldots x_{i-1}\psi(\bar{x})$, Lemma 2.3.1 implies that (9.1) holds for $i+1$ instead of i. (9) postulates (9.1) for $i = 0$. Therefore by a trivial induction on i, we obtain (9.1) for $i = n+1$. But this is exactly

(9.2) $\quad t_0 \Vdash \langle F\rangle[F]\neg\exists\bar{x}\psi(\bar{x})$.

By $t_0 \Vdash C(\psi)$ stated in the first part of the (present) proof of Claim 2.3 (a few lines below item (7)) we have $t_0 \Vdash [F]\exists\bar{x}\psi(\bar{x})$. This yields from (9.2), by the proof of (7), $t_0 \Vdash \langle F\rangle[F](\exists\bar{x}\psi(\bar{x}) \wedge \neg\exists\bar{x}\psi(\bar{x}))$. That is $t_0 \Vdash \langle F\rangle[F]FALSE$. By the proof of (7) this is impossible.

We derived a contradiction from assuming $\nvdash C(\psi) \to \chi$. Therefore Claim 2.3(i) is proved. T_0 satisfies condition (b) both by item (2) in Remark 1 above and also by [3, Theorem 5.7, p. 61] or [1, Theorem on top of p. 126]). Now both (i) and (ii) of Claim 2.3 are proved. $\square$

Proof of Claim 2.2. We want to prove $\nvdash_{T_2} \chi$, and $\nvdash \chi$ for any $\vdash$ satisfying (a).

Let $\mathbf{A} \models (PA + \neg Con(PA))$. (Exists by Gödel's incompleteness theorem.) Then for our formulation $\forall x \sigma(x)$ of $Con(PA)$, there is $d \in A$ with $\mathbf{A} \models \neg\sigma(d)$. Let $2^d < b \in A$ be fixed. (Though exponentiation is not in the language of Peano arithmetic, it is well known from the literature that exponentiation is definable in *PA*, and there is a unique generally accepted way of doing it.)

Let

$$\mathbf{A} \upharpoonright b = \langle \{a \in A\colon a \leq b\}, 0, (suc \upharpoonright b), (\leq \upharpoonright b), (+ \upharpoonright b), (\times \upharpoonright b)\rangle$$

be the usual "initial segment" of $\mathbf{A}$ with b as its greatest element. Let $(Id \upharpoonright b)\colon A \to (A \upharpoonright b)$ be defined by $(Id \upharpoonright b)(x) = min(x, b)$ as usual. Let $\mathfrak{M} = (\mathbf{A}, (\mathbf{A} \upharpoonright \mathrm{b}), (Id \upharpoonright b), \ldots, (Id \upharpoonright b), \ldots) \in Mod$ with $(Id \upharpoonright b)$ interpreting all the flexible constants y_i $(i \in \omega)$. Clearly,

$$\mathfrak{M} \models \varphi_1 \quad \text{and} \quad \mathfrak{M} \models (Ind + Tpa + \text{“}|D| \geq \omega\text{”}).$$

Of the latter, $\mathfrak{M} \models Ind$ is true because $\mathfrak{M}$ is definable in $\mathbf{A}$, and induction was true in $\mathbf{A}$. Thus $(Ind + Tpa + \text{“}|D| \geq \omega\text{”}) \nvDash \chi$. Therefore, if $\vdash$ satisfies (a) then $\nvdash \chi$. It remains to check that T_2 satisfies (a).

By the soundness proof of [2] (i.e., the *proof* of Theorem 7.1 in [2]) for our specially constructed χ, the fact that $(Ind + Tpa) \nvDash \chi$ implies that $\nvdash_{T_2} \chi$.[7] □

Proof of Claim 2.1. Let $\mathfrak{M} = \langle\langle \omega, 0, suc, \leq\rangle, \mathbf{D}, y_0, \ldots\rangle$ be a standard-time model ($\mathbf{D}$ is arbitrary of course), and assume $\mathfrak{M} \models \varphi_1$. Then

$$y_0\colon \langle \omega, 0, suc\rangle \twoheadrightarrow \langle D, 0^{\mathbf{D}}, suc^{\mathbf{D}}\rangle$$

is a homomorphism onto $\mathbf{D}$ that is $Rng(y_0) = D$. Further $\mathbf{D} \models (PA_0 \upharpoonright b)$. In particular $\mathbf{D}$ has a greatest element b and $b = y_0(n)$ for some $n \in \omega$. Then D must be finite. But then $\mathbf{D} = \langle D, 0^{\mathbf{D}}, suc^{\mathbf{D}}, +, \times, b\rangle \models \forall x \sigma(x)$ since $Con(PA)$ holds in the standard model of arithmetic. This contradicts our assumption $\mathfrak{M} \models \varphi_1$ proving $\mathfrak{M} \models \chi$ for any standard-time model $\mathfrak{M}$. □

We continue proving Theorems 1 and 2. Claim 2.3 proves that χ is provable *from* assuming the existence of *any clock* in any proof system $\vdash$ satisfying (b) of Theorem 1. This applies, in particular, to Abadi's $\vdash_{T_0}, \vdash_{T_1}, \vdash_{T_2}$. Therefore, by Claim 2.2

(10) χ is *not arithmetical* in T_2, T_1, T_0, or $\mathbb{R}$, nor in any $\vdash$ satisfying (a)+(b) of Theorem 1.

Thus χ is the "more subtle example of a nonarithmetical formula" Abadi is asking for at the end of the item in [2, "Examples", § 6.1]. Namely χ is not arithmetical

[7] There is a mistake in the soundness proof in [2], i.e. in the proof of the T_2 part of Theorem 7.1 in [2]. However, this mistake disappears if we assume that $y_i\colon T \twoheadrightarrow D$ is *onto* D for some $i \in \omega$ in every model we are considering. Since this *is* the case in our present example, we may ignore the mistake. See also Theorem 3 below, and the remark following its proof.

in T_2, T_1, T_0 but it is valid in standard-time models by our Claim 2.1. Abadi's question is motivated by the fact that at that time the only known examples of nonarithmetical formulas were like $\exists x \exists x_1(x \neq x_1)$ which were of course not valid (even in $\models^\omega$). Therefore also: Claims 2.1-2.3 answer the last Open question in [2, § 9] also the last one in [1, § 9, p. 129], and the last one in [3, § 5.9, (p. 92)] the following way:

(11) A clock does add power to T_1, namely $\models^\omega \chi$, indeed χ is T_1-provable under assuming a clock, but $\nvdash_{T_1} \chi$. Here, T_1 can be replaced with *any* $\vdash$ satisfying (a)+(b) of Theorem 1, hence in particular with the resolution system $\mathbb{R}$ of Abadi–Manna [5] which answers a question in [3, § 5.9]. (All this is valid when the data domains are restricted to be infinite.)

The second sentence of the second problem in [3, § 5.9 ("Open questions"), p. 92], and [2, § 9] introduces a new proof rule to T_1 which permits us to assume the existence of a clock formula $c(x)$ (and use $C(c(\bar{x}))$ as an axiom) with c a *new* flexible predicate symbol not occurring in the formula we want to prove. Then it is written in the quoted papers that this new rule (in particular "T_1+the new rule") is harmless as long as the domain of discourse is infinite. Since the semantics used for T_1 in the quoted papers is "$(Ind + Tord \models)$" denoted by $\vdash_0$ therein[8], it is useful to point out that

(12) *(T_1 + the new clock rule) is not sound for the semantics ($Ind + Tord$ + "$|D| \geq \omega$" $\models$) or equivalently for "$\vdash_0 + (|D| \geq \omega)$". Nor is it sound for the semantics ($Ind + Tpa$ + "$|D| \geq \omega$").*

Proof of (12). By the proof of Claim 2.2, $(Ind + Tpa + \text{"}|D| \geq \omega\text{"}) \not\models \chi$. Actually this was stated in that proof. However, Claim 2.3 implies $\vdash C(c(\bar{x})) \rightarrow \chi$ for any $\vdash$ satisfying (b), hence the above new rule does prove χ. Thus the new rule is not sound for infinite domains when added to $T_0, \mathbb{R}, T_1$, or any $\vdash$ satisfying (b). □

Recall that Abadi writes $\models \varphi$ for what we denote as $\models^\omega \varphi$ (validity in standard-time models). Therefore in Abadi's notation, we have $\models \chi$ by Claim 2.1. Now, (10) completes the proof of (i) and (ii) of Theorem 1. (11) proves (i), and (12) proves (iii) of Theorem 2.

It remains to prove Theorem 1(iii) and Theorem 2(ii). They differ from Theorem 1 (ii) and its corollary in Theorem 2 only in that they assume (a*) instead of (a). We used (a) in proving Claim 2.2. Let us assume now, on $\vdash$, (a*) instead of (a).

Let

$$H \stackrel{\text{def}}{=} \{e(\bar{x}) : \vdash (\varphi_0 \rightarrow \forall \bar{x} \neg e(\bar{x})) \text{ where } e(\bar{x}) \text{ is a Diophantine equation}\}.$$

[8] One might have the impression that in the above quotation "harmless" is understood w.r.t. the semantics $\vdash_0$ because of the note at the end (in brackets) of the first sentence of Abadi's presently quoted second problem. Namely there it is mentioned that T_1 and $\mathbb{R}$ are complete for arithmetical formulas. Now, this is stated as a theorem (in the quoted papers) w.r.t. $\vdash_0$ as a semantics.

By (a*), H is recursively enumerable, and $\mathbf{N}\models\neg e(\bar{x})$ for all $e(\bar{x})\in H$, because of the following: Assume $e(\bar{x})\in H$. Let $\bar{u}\in {}^k\mathbf{N}$ be arbitrary. Let $b\in\mathbf{N}$ be an upper bound of $\bar{u}$. Then $\mathfrak{M}=\langle\mathbf{N},\mathbf{N}\upharpoonright b,\text{“}Id\text{”}\rangle\models\varphi_0$, and $\mathfrak{M}$ is a model of $\vdash$ by (a*). Hence, by $e\in H$, we have $\mathfrak{M}\models\forall\bar{x}\neg e(\bar{x})$. Thus $\mathbf{N}\models\neg e(\bar{u})$. Therefore by Matiasevitch's solution of Hilbert's tenth problem, there is a Diophantine equation $e(\bar{x})\notin H$ such that $\mathbf{N}\models\forall x\neg e(\bar{x})$.

Now, let us use this $e(\bar{x})$ in place of $\neg\sigma(x)$ in defining φ_1. That is let φ^+ be the formula $(\varphi_0\wedge\exists\bar{x}e(\bar{x}))$. We claim that we can reprove Claims 2.1–2.3 with φ^+ in place of φ_1 and using (a*), along the following lines.

By the definition of H and by $e\notin H$ we have $\nvdash(\varphi_0\to\forall\bar{x}\neg e(\bar{x}))$, hence $\nvdash(\neg\varphi^+)$ (this is the new version of Claim 2.2). Now, $\models^\omega(\neg\varphi^+)$ and $\vdash C(\psi)\to(\neg\varphi^+)$ are proved exactly as in Claims 2.1, 2.3 (in those parts we did not use the difference between $(\neg\sigma)$ and e). Let us choose $\chi^+\stackrel{\text{def}}{=}(\neg\sigma^+)$. Then χ^+ satisfies the conclusion of Theorem 1(iii). Theorem 1(iii) implies Theorem 2(ii).

This completes the proof of Theorem 1(iii) and Theorem 2(ii). $\square$

Remark. Let χ be as fixed in item (0) in the proof of Theorems 1, 2 above. The proof of Claim 2.2 establishes also that

(13) $(Ind+Tpa)\nvDash\chi$.

By [26, § V.1],

(14) $(Ind+Tpa+Ex)\models\chi$.

Looking into the lattice of logics of programs at the end of [24, 25] or [21], (13) and (14) give information about the proof theoretic powers of other computer science temporal logics. It appears that $(Ind+Ex)\nvDash\chi$, and repeating the same argument with $Con(PA_0+(Ind\upharpoonright\Sigma_1))$ in place of $Con(PA)$, as in [12] or [26, § V.1] one could probably prove $(Ind+Ex)<_\square(Ind+Tpa+Ex)$ (this notation means that strictly more *partial correctness assertions* can be proved from $(Ind+Ex)$ than from $(Ind+Tpa+Ex)$). However, we do not know if $(Ind+Tsuc+Ex)$ or $(Ind+Tord+Ex)$ imply χ (i.e. if one of these is strictly weaker than $(Ind+Tpa+Ex)$, cf. (14)).

6. On the incompleteness of T_2

Theorem 1(i) above proves that Abadi's theorem saying that

(15) $(\models^\omega\varphi)\Rightarrow(\varphi$ is arithmetical in $T_2)$, for any $\varphi\in Fm(FTL)$

is not true. (See also Abadi [28].) This is the theorem on page 127 of [1] which is basically the same as [3, Theorem 5.16] or [2, Theorem 6.2]. The main result of these works, completeness of the inference system $\vdash_{T_2}$ for Abadi's semantics $\vdash_P$ (which is our $(Ind+Tpa\models)$) is based on (15) disproved above. In more detail, (15) is used in all three papers to prove the main completeness theorem (for T_2) which is the second statement of [2, Theorem 7.2]. The proof of this completeness theorem heavily uses (15), see e.g. the first sentence of the proof either in [2] or in [3]. Unfortunately, this application of (15) turns out to be essential for proving completeness of T_2. Namely, a modified version of our counterexample $\chi = (\neg\varphi_1)$ constructed in item (0) in the above proof can be used to show that T_2 is indeed *not* complete for Abadi's $\vdash_P$ that is for $(Ind + Tpa\models)$. The modification consists of replacing $Con(PA)$, which was denoted as $\forall x\sigma(x)$, in our φ_1 with a slightly weaker statement $\forall x\sigma_1(x)$ such that $PA \models \forall x\sigma_1(x)$ becomes true but "barely". Here "barely" means that $\forall x\sigma_1(x)$ does not follow from slightly weaker versions of PA. E.g., as in [12], one could choose $\forall x\sigma_1(x)$ to be $Con(I\Sigma_n)$ for a suitable $n \in \omega$, where $I\Sigma_n$ is obtained from PA by restricting the induction schema of PA to Σ_n-formulas. For the new χ we will have $\vdash_P \chi$ but $\nvdash_{T_2} \chi$.

Of these claims, $\vdash_P \chi$ is immediate by $PA \models \sigma_1(x)$ and by the definitions of $\vdash_P$ and χ. Proving $\nvdash_{T_2} \chi$ is more tedious. However, it is not very hard to see the reason (on an intuitive level) for $\nvdash_{T_2} \chi$ as follows.

Our χ is equivalent with $\varphi_0 \to \forall x\sigma_1(x)$, see the material above item (0) for the definition of φ_0 and χ. Assume therefore that $\mathfrak{M} \models \varphi_0$ for some model $\mathfrak{M} = \langle \mathbf{T}, \mathbf{D}, f_i \rangle_{i\in\omega}$ of T_2. (See item (16) below for more on T_2 and on what its models look like. To be precise, for our present purposes, in (16) below, we should replace the text "$h: D \to D$ is a distinguished unary function" with "$h: D \to D$ is a first-order definable (in $\mathfrak{M}$) unary function".) Now, by the definition of φ_0, $\mathbf{D}$ is isomorphic to an initial segment of $\mathbf{T}$, that is $\mathbf{D} \cong (\mathbf{T} \restriction b)$, for some $b \in T$, and all the "recursively defined" f_i's act from T into D. From the mathematical point of view, we may identify $\mathbf{D}$ with $\mathbf{T} \restriction b$, therefore $\mathfrak{M}$ is equivalent with a structure $\mathbf{A} = \langle A, 0, suc, \leqslant, (+ \restriction b), (\times \restriction b), f_i \rangle_{i\in\omega}$ where $(\forall i \in \omega)\, f_i : A \to (A \restriction b)$, see the construction in the proof of Claim 2.2 for detail and notation. Here $\langle A, 0, suc, \leqslant \rangle = \mathbf{T}$ and $(\mathbf{A} \restriction b) = \mathbf{D}$. $\mathbf{A}$ looks like the following:

$$\underbrace{0 \to 1 \to 2 \to \cdots \to \bullet \to b}_{+\text{ and } \times \text{ are defined } \textit{only} \text{ here}} \to \bullet \to \cdots$$
$$\leqslant$$

From the "logical" point of view[9] $\mathbf{A} \restriction b$ behaves like a finite structure even if b is nonstandard. So from the point of view of "the logic", $\mathbf{A}$ is only a simple ordering with a partial arithmetic defined only on a finite part of $\mathbf{A}$. Thus the arithmetical part is negligible. On the other hand, it is well known that simple orderings have no "metamathematical power" e.g. they admit an elimination of quantifiers and are decidable. Therefore there is no hope for obtaining a truth definition for $I\Sigma_n$ (i.e. for Peano's arithmetic with restricted induction) in $\mathbf{A}$. Thus there is no hope for deriving $Con(I\Sigma_n)$ from the formal system T_2 a typical model of which is $\mathbf{A}$. We can sum up the reason for $\nvdash_{T_2} \chi$ in the following dialog:

Q: χ is a consistency statement about $I\Sigma_n$ (a weakened version of PA), why should T_2 prove such consistency statements? Surely, set theories or PA do prove

[9] This is sometimes called internal point of view in the literature of nonstandard models (of PA etc.) cf. e.g. pp. 199, 204, 265 of [10].

such consistency statements (but e.g. $I\Sigma_n$ in itself does not), but why would T_2 have the metamathematical" power of set theories or PA?

A: The power of T_2 comes from recursive definability of "new" functions $f: T \to D$ in T_2, as described in item (16) below. In particular, addition and multiplication can be defined recursively, so we have something similar to PA. This is where the "metamathematical" power comes from.

Q: The problem with this is that the new functions f_i go from T to D and *not* from T to T. This makes a difference. Namely, in our above constructed $\mathbf{A}$ (which was a merged version of T and D), all the f_i's map to elements below the bound b. In symbols, $f_i: A \to (A \upharpoonright b)$. So from the "logical" or "internal" point of view, all the f_i's map into a fixed *finite* segment of $\mathbf{A}$. In other words, the ranges of all the f_i's are bounded by an internally finite b. So in particular, we cannot define addition and multiplication of arbitrary large elements of $\mathbf{A}$ (or of $\mathbf{T}$ equivalently). Therefore we do not have a PA-like system. The same argument shows that we do not have any nontrivial "metamathematical" power, therefore we cannot prove $Con(I\Sigma_n)$ and hence we cannot prove χ.

A careful analysis reveals that, indeed, Q wins the argument. The above, of course, is only an intuitive explanation and not a carefully elaborated proof. A detailed proof and some further consequences are in [29]. In [30], Krajíček also gave a proof.

In [22], it is shown that no number of new axioms, but a single new modality can eliminate the incompleteness of T_2.

7. On the soundness of T_2

Next we turn to a somewhat closer inspection of the FTL inference system T_2 of [1-4]. We recall from [1-4] that T_2 contains an auxiliary axiom of a "second-order logic" character[10] saying that

(16) *If* $\mathfrak{M} = \langle \mathbf{T}, \mathbf{D}, f_i \rangle_{i \in \omega}$ is a model of T_2 with $\mathbf{D} = \langle D, \ldots, h, \ldots \rangle$ where $h: D \to D$ is a distinguished unary function of $\mathbf{D}$, *then* for any $d \in D$ there exists a function $g: T \to D$ such that $g(0) = d$ and $(\forall t \in T) g(suc(t)) = h(g(t))$, *and* $(\mathfrak{M}, g)$ is a model of T_2 again. (In $(\mathfrak{M}, g)$ g is added to $\{f_i : i \in \omega\}$.)

We note that g does not have to appear in $\mathfrak{M}$ anywhere, in particular $g \notin \{f_i : i \in \omega\}$ is allowed. We will use that T_2 is *complete* for its models [2, Prop. 5.3] or [3, Prop. 5.14].

As was already mentioned, T_2 satisfies condition (b) of Theorem 1 above. (At this point looking at Remark 1 might be useful for the reader, though is not absolutely indispensable.)

[10] It is this axiom (16) which we mentioned to be similar to the comprehension schema Ex of the NLP school.

Theorem 3. T_2 *is* not sound *for the semantics* $(Ind + Tpa \models)$ *i.e. for* $\vdash_P$ *of* [1-4].

Proof. Let PA_0 be the finite theory described at the beginning of the proof of Theorems 1, 2 above. Let $\mathbf{D}$ consist of two disjoint models $\mathbf{A}$ and $\mathbf{B}$ of PA_0. I.e. $\mathbf{A} \models PA_0$ and $\mathbf{B} \models PA_0$. Let the language of $\mathbf{A}$ be 0_A, suc_A, $\leqslant_A$, $+_A$, $\times_A$ and that of $\mathbf{B}$ be 0_B, suc_B, $\leqslant_B$, $+_B$, $\times_B$. (Of course, then the language of $\mathbf{D}$ is the union of these two languages.) Further, A and B are two unary predicates of $\mathbf{D}$ (with $A \cap B = 0$ and A the universe of $\mathbf{A}$ etc.).

Let $\mathbf{A} \models \neg Con(PA)$ and $\mathbf{B} \models Con(PA)$.

All what we said so far is expressible by a single classical first-order formula ψ_0 in the language of $\mathbf{D}$. Let ψ_1 be the FTL formula saying that y_0 is a homomorphism mapping the "0, *suc*, $\leqslant$"-reduct of $\mathbf{T}$ *onto* the "0 *suc*, $\leqslant$"-reduct of $\mathbf{A}$. I.e.

$$(y_0 = 0_A \wedge [F]\exists x(x = y_0 \wedge A(x) \wedge \bigcirc suc_A(x) = y_0)$$

$$\wedge \forall x(A(x) \to \langle F\rangle x = y_0) \text{ etc.})$$

is ψ_1. Let

$$\psi_2 \stackrel{\text{def}}{=} (\psi_0 \wedge \psi_1).$$

Claim 3.1. $(Ind + Tpa) \not\models (\neg\psi_2)$.

Proof. This is fairly easy to prove. There exists $\mathbf{A} \models PA + \neg Con(PA)$. Choose this $\mathbf{A}$ to be both $\mathbf{T}$ and $\mathbf{A}$, and let f_i be the *identity* function Id_A mapping $\mathbf{A}$ onto itself for all $i \in \omega$. Let $\mathbf{B}$ be the standard model $\mathbf{N}$ of arithmetic disjoint from $\mathbf{A}$. Then, roughly speaking, $\mathfrak{M} = \langle \mathbf{A}, (\mathbf{A} \cup \mathbf{N}), Id_A, \ldots, Id_A, \ldots\rangle$. Clearly $\mathfrak{M} \models (Ind + Tpa)$ but $\mathfrak{M} \not\models (\neg\psi_2)$. This proves Claim 3.1. □

Claim 3.2. $\vdash_{T_2} (\neg\psi_2)$. *I.e.* $(\neg\psi_2)$ *is* T_2*-provable.*

Proof. Since T_2 is complete for its models, it is enough to prove that $\mathfrak{M} \models (\neg\psi_2)$ for every model $\mathfrak{M}$ of T_2. Let $\mathfrak{M}$ be a model of T_2 and assume $\mathfrak{M} \models \psi_2$. We may assume that $\mathbf{T}$ of $\mathfrak{M}$ is in normal form (i.e. its undistinguishable elements are collapsed). Then $f_0 : T \rightarrowtail\!\!\!\!\twoheadrightarrow A$ interpreting y_0 is a surjective "0, *suc*, $\leqslant$" homomorphism (by $\mathfrak{M} \models \psi_2$), hence $f_0^{-1} : A \to T$ is a "0, *suc*, $\leqslant$" isomorphism, too. By axiom (16) of T_2, there is a "0, *suc*" homomorphism $g : \langle T, 0_T, suc_T\rangle \to \langle B, 0_B, suc_B\rangle$ mapping 0_T to 0_B and preserving *suc*. Since T_2 satisfies condition (b) of Theorem 1, induction along $\mathbf{T}$ is available. By this induction, one easily proves that $g : \langle T, 0, suc, \leqslant\rangle \rightarrowtail \langle B, 0_B\, suc_B, \leqslant_B\rangle$ embeds $\mathbf{T}$ into $\mathbf{B}$ as an initial segment (according to $\leqslant_B$), and that $\mathbf{A} \models PA$, moreover, that we have induction on $\mathbf{A}$ along 0_A, and suc_A for all two-sorted formulas of $(\mathfrak{M}, g)$. Therefore,

$$h \stackrel{\text{def}}{=} (g \circ f_0^{-1}) : \langle A, 0_A, suc_A, \leqslant_A\rangle \rightarrowtail \langle B, 0_B, suc_B, \leqslant_B\rangle$$

is an isomorphic embedding as an initial segment. Further by our above noted induction along **A** one easily proves that h preserves $+$ and $\times$, i.e. that $h: \mathbf{A} \rightarrowtail \mathbf{B}$ is an isomorphic embedding. Now $\mathbf{A} \models \neg Con(PA)$ and $\mathbf{B} \models Con(PA)$ contradict embeddability of **A** into **B** since $Con(PA)$ is a Π_1-formula i.e. $Con(PA)$ is of the form $\forall \bar{x} \sigma(\bar{x})$ as indicated in the proof of Theorems 1, 2 above. Thus $(\mathbf{A}, \bar{a}) \models \neg\sigma(\bar{a})$ for some $\bar{a} \in {}^nA$. Then $h(\bar{a})$ should satisfy $\neg\sigma(\bar{x})$ in **B** since $\sigma(\bar{x})$ is a Σ_0-formula and therefore its truth is preserved by h. But $\mathbf{B} \models \forall \bar{x} \sigma(\bar{x})$ follows from ψ_2. A contradiction, proving Claim 3.2. □

Summing up, $\vdash_{T_2} (\neg\psi_2)$ and $(Ind + Tpa) \not\models (\neg\psi_2)$ together prove that T_2 is not sound for $(Ind + Tpa \models)$. This completes the proof of Theorem 3. □

As a consequence of Theorem 3, the theorems stating that T_2 is sound for the semantics $(Ind + Tpa \models)$ in [1-4] are, apparently, not true. In particular, this applies to [2, Theorem 7.1], [3, Theorem 5.17 (the mistake in the proof is on p.81)], and the first theorem in [1, p. 128]. However, these theorems become true if we restrict the semantics to those models $\mathfrak{M} = \langle \mathbf{T}, \mathbf{D}, f_i \rangle_{i \in \omega}$ for which $(\exists i \in \omega)$ "$D \subseteq$ the range of f_i". For this case Abadi's original proof, e.g. that in [2] or [3, p. 81], goes through.

8. Open problems

Open problem 1. Find a nice, Hilbert-style inference system $\vdash$ for FTL which is sound and complete for $(Ind + Tpa \models)$ i.e. for Abadi's $\vdash_P$. Cf. Section 6 and Theorem 3 above.

Open problem 2. We note that T_2 is sound for $(Ind + Tpa + Ex \models)$ of the NLP school, see e.g. [8, 27]. Find a natural subset Ex_0 of Ex such that a variant of Abadi's T_2 would become both sound and complete for $(Ind + Tpa + Ex_0 \models)$.

Open problem 3. Is any of T_0, T_1, T_2 complete for *Ind* or $(Ind + Tord)$? (Cf. the last paragraph of Section 3 and the paragraph preceding Theorem 1 in Section 4.)

Acknowledgment

Thanks are due to Martín Abadi and Yde Venema for their careful reading of this paper, their valuable remarks, and suggestions. The author is especially grateful to Yde Venema for his improving the original proof of Claim 2.3.

References

[1] M. Abadi, The power of temporal proofs, in: *Proc. 2nd Ann. IEEE Symp. on Logic in Computer Science*, Ithaca, NY, USA (1987) 123-130.

[2] M. Abadi, The power of temporal proofs, *Theoret. Comput. Sci.* **64** (1989) 35-84.
[3] M. Abadi, Temporal-logic theorem proving, Dissertation, Dept. of Comp. Sci., Stanford Univ., 1987.
[4] M. Abadi, Temporal logic was incomplete only temporarily, preprint.
[5] M. Abadi and Z. Manna, A timely resolution, in: *Proc. 1st Ann. Symp. on Logic in Computer Science* (1986) 176-189.
[6] H. Andréka, L. Csirmaz, J. Krajíček and I. Sain, manuscript, in preparation.
[7] H. Andréka, I. Németi and I. Sain, Henkin-type semantics for program schemes to turn negative results to positive, in: L. Budach, ed., *Fundamentals of Computation Theory '79* (Akademie Verlag, Berlin, Band 2 1979) 18-24.
[8] H. Andréka, I. Németi and I. Sain, A complete logic for reasoning about programs via nonstandard model theory, Parts I-II, *Theoret. Comput. Sci.* **17** (2, 3) (1982) 193-212 and 259-278.
[9] H. Andréka, I. Németi and I. Sain, On the strength of temporal proofs, *Theoret. Comput. Sci.* **80** (1991) 125-151.
[10] J. Barwise (ed.), *Handbook of Mathematical Logic* (North-Holland, Amsterdam, 1977).
[11] J.L. Bell and M. Machower, *A course in mathematical logic* (North-Holland, Amsterdam, 1977).
[12] B. Biró and I. Sain, Peano arithmetic for the time scale of nonstandard models for logics of programs, *Ann. Pure Appl. Logic*, to appear.
[13] D. Gabbay and F. Guenther (eds.), *Handbook of Philosophical Logic Vol II* (Reidel, Dordrecht, 1984).
[14] D. Gabbay, A. Pnueli, S. Shelah, J. Stavi, On the temporal analysis of fairness, Preprint Weizman Institute of Science, Dept. of Applied Math. 1981.
[15] R. Goldblatt, Logics of time and computation, Center for the Study of Language and Information, Lecture Notes Number 7 (1987).
[16] P. Hájek, Some conservativeness results for nonstandard dynamic logic, in: *Proc. Conf. Győr Hungary* 1983 *Colloq. Math. Soc. János Bolyai* **42** (North-Holland, Amsterdam, 1986) 443-449.
[17] F. Kröger, *Temporal Logic of Programs*, EATCS Monogr. Theoret. Comput. Sci. (1988).
[18] J.A. Makowsky and I. Sain, Weak second order characterizations of various program verification systems, *Theoret. Comput. Sci.* **66** (1989) 229-321. Abstracted in: *Logic in Computer Science* (*Proc. Conf. Cambridge USA*) (1986) 293-300.
[19] Z. Manna and A. Pnueli, The modal logic of programs, in: *Proc. Internat. Colloq. on Automata, Languages and Programming '79, Graz*, Lecture Notes in Computer Science, Vol. 71 (Springer, Berlin, 1979) 385-409.
[20] Z. Manna and A. Pnueli, Verification of concurrent programs: A temporal proof system, Report No STAN-CS-83-967, Comp. Sci. Dept., Stanford Univ., June 1983.
[21] I. Németi, Nonstandard Dynamic Logic, in: D. Kozen ed., *Logics of Programs, Proc. Conf. New York 1981*, Lecture Notes in Computer Science, Vol. 131 (Springer, Berlin, 1982) 311-348.
[22] A. Pasztor and I. Sain, A streamlined temporal completeness theorem, in: *Proc. Conf. on Computer Science Logic*, Lecture Notes in Computer Science, Vol. 440 (Springer, Berlin, 1990).
[23] I. Sain, There are general rules for specifying semantics: Observations on Abstract Model Theory, *CL & CL* (*Comput. Linguistics and Comput. Languages*) **XIII** (1979) 195-250.
[24] I. Sain, Relative program verifying powers of the various temporal logics, Preprint No. 40/1985, Math. Inst. Hungar. Acad. Sci. An extended abstract of this is [25] (1985).
[25] I. Sain, The reasoning powers of Burstall's (model logic) and Pnueli's (temporal logic) program verification methods, in: R. Parikh, ed., *Logics of Programs, Proc. Conf. Brooklyn USA* 1985 Lecture Notes in Computer Science, Vol. 193 (Springer, Berlin, 1985) 302-319.
[26] I. Sain, Nonstandard Logics of Programs, Dissertation, Hungarian Academy of Sciences, Budapest (in Hungarian) (1986).
[27] I. Sain, Total correctness in nonstandard logics of programs, *Theoret. Comput. Sci.* **50** (1987) 285-321.

References added in proof

[28] M. Abadi, Corrigendum to "The power of temporal proofs", *Theoret. Comput. Sci.* **70** (1990) 275.
[29] L. Csirmaz, Induction and Peano models, DIMACS Tech. Report 90-28, Dept. of Computer Science, Rutgers Univ., 1990.
[30] J. Krajíček, Letter to H. Andréka, I. Némethi and I. Sain, 1989.