COMPUTER SCIENCE TEMPORAL LOGICS
NEED THEIR CLOCKS

In this paper we solve some open problems raised in recent publications of the Computer Science Temporal Logic school represented by Manna-Pnueli [11], [12], Abadi-Manna [5], Abadi [1]-[4]. These problems concern the proof theoretic powers of the following inference systems: $T_0$ introduced in [11], [12] and reformulated in [1]-[4]; the resolution system $R$ of [5]; and $T_1, T_2$ of [1]-[4].

We use first-order temporal logic (FTL) with modalities $\Box$, $[F]$, and $U$ denoting “nexttime”, “always-in-the-future”, and “until” respectively. Given a first-order similarity type or language $L$, the usual predicate etc. symbols of $L$ are considered to be rigid, i.e. their meanings do not change in time. 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 it will be very easy to see. $Fm(FTL)$ denotes the set of all FTL-formulas (of some fixed similarity type $L$) defined above.

For semantic purposes, we use classical two-sorted models $M = < T, D, f_0, \ldots, f_i, \ldots >_{i \in \omega}$ where $D$ is a classical first-order structure of similarity type $L$, $T = < T, 0, suc, \leq, +, \times >$ is a structure of the same similarity type as the standard model $N = < \omega, 0, suc, \leq, +, \times >$ of arithmetic, and for $i \in \omega$, $f_i$, a function from $T$ into $D$, serves to interpret the flexible constant $y_i$. $T$ is called the time-frame of $M$, and, except for its language, is arbitrary. $Mod$ denotes the class of all models $M$ of the above kind. (The members of $Mod$ are basically the same as Kripke models known from the
To associate meanings to FTL-formulas in models from $\text{Mod}$, we define a translation function

$$P : Fm(FTL) \rightarrow Fmc(\text{Mod}),$$

where $Fmc(\text{Mod})$ is the set of all classical (two-sorted) first-order formulas in the language of $\text{mod}$. In $Fmc(\text{Mod})$, $x_i (i \in \omega)$ 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 it is well known, cf. [8]). For any $\varphi \in Fm(FTL)$, we let

$$P(\varphi) \overset{df}{=} \exists t_0 [t_0 = 0 \land P^*(\varphi, t_0)],$$

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

- For every $t \in \{t_i : i \in \omega\}$ and $\varphi, \psi \in Fm(FTL)$,
  $$P^*(y_i = x_j, t) \overset{df}{=} (f_i(t) = x_j),$$
  $$P^*(\psi, t) \overset{df}{=} \psi$$ whenever $\psi$ is atomic and does not contain flexible symbols,
  $$P^*$$ preserves classical connectives and quantifiers (i.e.: $P^*(\exists x_i \varphi, t) \overset{df}{=} \exists x_i P^*(\varphi, t)$ etc.), and
  $$P^*([\varphi], t) \overset{df}{=} (\forall t_1 \geq t) P^*(\varphi, t_1),$$
  $$P^*(\varphi U \psi, t) \overset{df}{=} (\forall t_1 \geq t) (P^*(\varphi, t_1) \lor \exists t_2 | t \leq t_2 \leq t_1 \land P^*(\psi, t_2))$$.

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

$$M \models \varphi \overset{df}{=} M \models P(\varphi),$$

for any $\varphi \in Fm(FTL)$.

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

For any $K \subseteq \text{Mod}$, we let $K \models \varphi \overset{df}{=} (\forall M \in K) M \models \varphi$.

A model $M = < T, \ldots >$ is called a standard-time model iff $T$ is the standard model $\mathbf{N}$ of arithmetic.

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

The semantics $\models^\omega \varphi$ is too restrictive, while $\text{Mod} \models \varphi$ 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 ⊆ Fmc(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.

\[
\text{Ind} \overset{\text{def}}{=} \{ \varphi(0) \land \forall t[\varphi(t) \rightarrow \varphi(\text{suc}(t))] \rightarrow \forall t\varphi(t) : \varphi \in \text{Fmc}(\text{Mod}) \},
\]

where \( \varphi(0) \) is obtained from \( \varphi \) by replacing the free occurrences of \( t \) in \( \varphi \) with 0, and similarly for \( \varphi(\text{suc}(t)) \). 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) \( T \). Tord postulates the consequences of Tpa for the reduct \( < T, 0, \text{suc}, \leq > \) of \( T \). So, the main difference between Tord and Tpa is that Tord ignores + and \( \times \). Thus when using \((\text{Ind} + \text{Tord})\) as semantics, we will pretend that + and \( \times \) are not there. See the 1977 version of [6] or [7] 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 Abadi [1]-[4] adopted the same definitions from [6] etc. with some notational differences to be indicated soon.

For any \( Th \subseteq \text{Fmc}(\text{Mod}) \) and \( \varphi \in \text{Fm}(\text{FTL}) \), we let

\[
\text{Mod}(Th) \overset{\text{def}}{=} \{ M \in \text{Mod} : M \models Th \}, \text{ and } Th \models \varphi \overset{\text{def}}{=} \text{Mod}(Th) \models \varphi.
\]

Now, the two most frequently used semantics for FTL-formulas \( \varphi \) are \((\text{Ind} + \text{Tord}) \models \varphi \) and \((\text{Ind} + \text{Tpa}) \models \varphi \). Abadi [1]-[4] writes \( \vdash_0 P(\varphi) \) and \( \vdash P(\varphi) \) for \((\text{Ind} + \text{Tord}) \models \varphi \) and \((\text{Ind} + \text{Tpa}) \models \varphi \) respectively. Further, he writes \( \models_\omega \varphi \) for our \( \models_\omega \varphi \).

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 below). However, as special cases of these, we will consider four concrete inference systems, \( T_0, R, T_1, \) and \( T_2 \) introduced in Manna-Pluener [11], [12], Abadi-Manna [5], Abadi [1]-[4]. Our theorems solve, among others, open problems raised about these in the quoted papers.

Let \( \vdash \) be an inference system for FTL. Let \( K \subseteq \text{Mod} \). We say that \( \vdash \) is
complete for \((K \models)\) iff \(\forall \varphi \in Fm(FTL)(K \models \varphi \implies \vdash \varphi)\). We say that \(\vdash\) is sound for \((K \models)\) iff \(\forall \varphi \in Fm(FTL)(K \models \varphi \iff \vdash \varphi)\). If \(\Sigma \subseteq Fmc(Mod)\) then, instead of “\((\text{Mod}\!(\Sigma) \models)\)” we sometimes write “\((\Sigma \models)\)” \(\text{That is, (}\vdash\text{) is complete (sound) for (K |-) and (Sigma |-) respectively.}\)

Let \(\gamma(\mathbf{x}) \in Fm(FTL)\) with \(\mathbf{x} = \langle x_0, \ldots, x_n \rangle\) as free variables. Recall from Parikh [13] and Abadi [1]-[4] that the clock condition \(C(\gamma)\) for \(\gamma\) is the FTL-formula

\[
C(\gamma) \overset{df}{=} ([F] \exists \mathbf{x} \gamma(\mathbf{x}) \land [F] \forall \mathbf{x} [\gamma(\mathbf{x}) \rightarrow \bigcirc [F] \neg \gamma(\mathbf{x})]).
\]

Intuitively, \(C(\gamma)\) says that \(\gamma\) distinguishes different time instances from each other.

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

Thus there are many arithmetical formulas: if \(\vdash \varphi\) or if \(\not\vdash (C(\gamma) \rightarrow \varphi)\) for some \(\gamma\) then \(\varphi\) 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 non-arithmetical formula is \(\exists x \exists x_1 (x \not= x_1)\). But this formula is not valid. It is much harder to find a non-arithmetical \(\varphi\) such that \(\models \neg \varphi\). Indeed: §6 “Clocks and arithmetical formulas” of [2] contains a question asking for “more subtle examples” of non-arithmetical formulas.

In Theorem 1 below we will answer this question by exhibiting a non-arithmetical (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 there are no “more subtle” examples in the sense that for any rigid formula \(\varphi\), \(\varphi\) is not arithmetical in \(\vdash\) iff \(Mod \models \exists x_0 \ldots \exists x_n (\Lambda\{x_i \not= x_j : i < j \leq n\} \rightarrow \varphi)\) for some \(n \in \omega\) but \(Mod \not\models \varphi\).) This quest for a more subtle non-arithmetical formula seems to be implicit in all of [1]-[4]. Namely, each of these papers contains a theorem stating that

\[
\forall \varphi \in Fm(FTL)((\models \neg \varphi) \implies (\varphi \text{ is arithmetical in } T_2)).
\]

(See Thm. 6.2. somewhere around p. 60 in [2], the theorem on p. 127 of [1], Thm. 5.16 on p. 75 of [3], the second theorem in §6 of [4], p. 12.)
Unfortunately, (\(\ast\)) turns out to be false below. Probably, it was the lack of a timely answer to the above quoted open problem which had lead to the belief in the truth of (\(\ast\)) above. Unfortunately, the new discovery influences the status of the strongest available (by now) temporal inference system which was designed to be equivalent with Peano’s arithmetic (cf. e.g. the “Author’s abstract” and “Capsule review” at the beginning of the preprint version of [2], as well as Thm. 7.2 therein), but which turns out to be not yet strong enough for this purpose in Remark 3 way below.

The “more subtle” example for a non-arithmetical temporal formula in Theorem 1 below is a formula valid in standard-time models, but not valid in (\(Ind + Tpa\)). Also, in [1], [2], Abadi asks if \(T_1\) is complete for \((Ind+Tord)\). This, by using 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 \(\psi\) such that \(\models^{\omega} \psi\), and \(\psi\) is not arithmetical in any of \(T_0\), \(T_1\), or \(T_2\).

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

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

(b) \(\vdash\) is complete for \(\text{Mod}\), for any \(\varphi \in \text{Fm}(FTL)\), \(\vdash [\varphi \land [F](\varphi \rightarrow O\varphi)] \rightarrow [F]\varphi\), and \(\vdash [F]\varphi \rightarrow (\varphi \land O[F]\varphi)\), further \(\vdash\) is closed under the rules of modus ponens and necessitation, i.e. \(\vdash \varphi\) implies both \(\vdash [F]\varphi\) and \(\vdash O\varphi\).

(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 \(\models^{\omega}\).

**Outline of proof:** Let \(PA_0\) denote a sufficiently strong finite part of Peano’s axioms \((PA)\) for \(\mathbb{N} = (\omega, 0, \text{suc}, \leq, +, \times)\). E.g.: \(PA_0\) states that \(\leq\) is a linear discrete ordering, its usual relationship with \(\text{suc}\), 0, and +, further the recursive definition of + and \(\times\) from \(\text{suc}\). Let \((PA \mid b)\) be obtained from \(PA_0\) by replacing the axiom stating that there is no greatest element by \(\{\forall x (x \leq b)\}, \text{suc}(b) = b\). So, \((PA \mid b)\) states that \(b\) is the greatest element, but arithmetic (+, \(\times\), etc.) between 0 and \(b\) is the usual.

Let \(\varphi_0\) be the following temporal sentence:
\[(PA \mid b) \land y_0 = 0 \land [F\exists x = y_0 \land \Box y_0 = suc(x)] \land \langle F \rangle y_0 = b.\]

Let \(\delta(x)\) be a \(\Sigma_0\)-formula in the language of \(PA\), such that \(\forall x \delta(x)\) is the usual formalization of \(\text{Con}(PA)\) in \(PA\). We define \(\psi\) to be the temporal sentence \(\varphi_0 \rightarrow (\forall x < b)\delta(x)\). We claim that \(\psi\) satisfies the conclusion of (ii). Of this, \(|=\psi\) and \(\not\models\psi\) are not hard to prove. The proof of \(\vdash C(\gamma) \rightarrow \psi\) goes by temporal induction. The inductive hypothesis is

\[\exists x (x = y_0 \land \langle F \rangle [\exists x \geq x] \gamma(\pi)).\]

Now, (i) follows from (ii). In the proof of (iii) we choose \(\delta\) differently. □

We recall from Abadi [1]-[4] (see the “Open questions” sections), that adding a clock to \(\vdash\) is defined as introducing a new rule \(\vdash (C(c(x)) \rightarrow \varphi) \Rightarrow \vdash \varphi\), where \(c\) is a flexible predicate symbol not occurring in \(\varphi \in \text{Fm}(FTL)\). 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, in the definition of a clock rule, \(c(x)\) with \(y_i = x_0\) where \(y_i\) does not occur in \(\varphi\). 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 \(\mid D \mid \geq \omega\) 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 \(\text{Ind} + Tord\) instead of the original \(\text{Ind} + Tpa\), and similarly for \(Tord\).

It is proved in Abadi [1]-[4] that \(T_1\) and \(T_2\) are complete for \(\text{Ind} + Tord\) and \(\text{Ind} + Tpa\) 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 \(\text{Ind} + Tord\) and \(\text{Ind} + Tpa\) respectively. However, we have to pay an unexpected price for this: by Theorem 2 (iii) below, the new systems are not sound for \(\text{Ind} + Tpa + \text{~}D = \omega\)), while the original ones were sound. This seems to contradict §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 \(R\). (The question is understood modulo infinite data domains, of course.)

Theorem 2 below answers this question in the affirmative.

\(\vdash_{T_i}\) and \(\vdash_{R}\) denote provability in \(T_i\) and \(R\) respectively \((i \in \{0, 1, 2\})\).
Theorem 2.

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

there is a $\varphi \in Fm(FTL)$ with $\models^{\omega}, \forall \varphi$, but $\vdash (C(c(\overline{x})) \rightarrow \varphi)$.

(ii) Adding a clock adds power to any proof system $\vdash$ satisfying (a*) and (b) of Theorem 1. I.e.: (i) 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 $(\text{Ind} + Tpa + "|D| \geq \omega")$. In particular, if we add clocks to $\vdash_R$ 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).

Remark 3. Theorem 1 (i) above proves that Thm. 6.2 of Abadi [2] and the theorem on p. 127 of [1] which is basically the same as Thm. 5.16 on p. 75 of [3] saying that:

\[(\models^{\omega} \varphi) \implies (\varphi \text{ is arithmetical in } T_2)\]

are not true. The main result of these works, completeness of the inference system $\vdash_{T_2}$ for Abadi’s semantics $\vdash_P$ (which is our "$(\text{Ind} + Tpa \models^=)"$) is based on the above disproved theorem. In more detail, (a) is used in all three papers to prove the main completeness theorem (for $T_2$) which is the second statement of Thm. 7.2 in Abadi [2]. Unfortunately, this application of (a) turns out to be essential for proving completeness of $T_2$. Namely, a modified version of our counterexample $\psi$ constructed in the proof of Theorem 1 (i), (ii) can be used to show that $T_2$ is indeed not complete for Abadi’s $\vdash_P$ that is for $(\text{Ind} + Tpa \models^=)$. This modified version of $\psi$ is analogous to the counterexample in Biró-Sain [9].

Open Problem. Find a nice, Hilbert-style inference system $\vdash$ for FTL which is sound and complete for $(\text{Ind} + Tpa \models^=) \text{ i.e. for Abadi’s } \vdash_P$.

References


This work has been supported by the Hungarian National Foundation for Scientific Research Grant No 1810.

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