P. Bouyer, F. Chevalier and
N. Markey

About the Expressiveness of TPTL and MTL

Research Report LSV-05-05
May 2005

Laboratoire
Spécification
et
Vérification

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Ecole Normale Supérieure de Cachan
61, avenue du Président Wilson
94235 Cachan Cedex France

On the Expressiveness of TPTL and MTL

Patricia Bouyer, Fabrice Chevalier and Nicolas Markey

LSV – CNRS UMR 8643 & ENS de Cachan
61, avenue du Président Wilson,
94230 Cachan, France
e-mails: {bouyer,chevalie,markey}@lsv.ens-cachan.fr

Abstract. TPTL and MTL are two classical timed extensions of LTL. In this paper, we answer a 15 year old conjecture that TPTL is strictly more expressive than MTL. But we show that, surprisingly, the TPTL formula proposed in [AH90] for witnessing this conjecture can be expressed in MTL. More generally, we show that TPTL formulae using only the **F** modality can be translated into MTL.

1 Introduction

Temporal logics. Temporal logics [Pnu77] are a widely used framework in the field of specification and verification of (models of) reactive systems. In particular, Linear-time Temporal Logic (LTL) allows to express properties about the executions of a model, such as the fact that *any occurrence of a problem eventually raises the alarm.* LTL has been extensively studied, both about its expressiveness [Kam68,GPSS80] and for model checking purposes [SC85,VW86, Var96].

Timed temporal logics. At the beginning of the 90s, real-time constraints have naturally been added to temporal logics [Koy90,ACD90], in order to add quantitative constraints to temporal logic specifications of timed models. The resulting logics allow to express, *e.g.*, that any occurrence of a problem in a system will raise the alarm *in at most 5 time units.*

When dealing with dense time, we may consider two different semantics for timed temporal logics, depending on whether the formulae are evaluated over *timed words* (*i.e.* over a discrete sequence of timed events; this is the *pointwise semantics*) or over *timed state sequences* (*i.e.*, roughly, over the continuous behavior of the system; this is the *interval-based semantics*). We refer to [AH92b, Hen98] for a survey on linear-time timed temporal logics and to [Ras99] for more recent developments on that subject.

Expressiveness of TPTL *and* MTL. Two interesting timed extensions of LTL are MTL (Metric Temporal Logic) [Koy90,AH93] and TPTL (Timed Propositional Temporal Logic) [AH94].

MTL extends LTL by adding subscripts to temporal operators: for instance, the above property can be written in MTL as

$$\mathbf{G}\,(\texttt{problem} \Rightarrow \mathbf{F}_{\leq 5}\,\texttt{alarm}).$$

TPTL is "more temporal" [AH94] in the sense that it uses real clocks in order to assert temporal constraints. A TPTL formula can "reset" a formula clock at some point, and later compare the value of that clock to some integer. The property above would then be written as

$$\mathbf{G}\,(\texttt{problem} \Rightarrow x.\mathbf{F}\,(\texttt{alarm} \wedge x \leq 5))$$

where "$x.\varphi$" means that x is reset at the current position, before evaluating φ. This logic also allows to easily express that, for instance, within 5 t.u. after any problem, the system rings the alarm and then enters a failsafe mode:

$$\mathbf{G}\,(\texttt{problem} \Rightarrow x.\mathbf{F}\,(\texttt{alarm} \wedge \mathbf{F}\,(\texttt{failsafe} \wedge x \leq 5))). \tag{1}$$

While it is clear that any MTL formula can be translated into an equivalent TPTL one, [AH92b,AH93] state that there is no intuitive MTL equivalent to formula (1). It has thus been conjectured that TPTL would be strictly more expressive than MTL [AH92b,AH93,Hen98], formula (1) being proposed as a possible witness not being expressible in MTL.

Our contributions. In this paper, we prove that the above-mentioned conjecture does hold for both pointwise and interval-based semantics. But we also prove that formula (1) *is not* a witness for that conjecture under the interval-based semantics, since we build an MTL formula that is equivalent to formula (1) under that semantics.

For the pointwise semantics, we prove that formula (1) cannot be expressed in MTL. In order to prove the conjecture for the interval-based semantics, we had to find another formula, namely $x.\mathbf{F}\,(a \wedge x \leq 1 \wedge \mathbf{G}\,(x \leq 1 \Rightarrow \neg b))$, stating that the last atomic proposition before time point 1 is an a, and prove that it cannot be expressed in MTL.

As side results, we get that, for both semantics, MTL+Past (where the past-time modality "Since" is used [AFH96]) is strictly more expressive than MTL, and we also get that the branching-time logic TCTL with explicit clock [HNSY94] is strictly more expressive than TCTL with subscripts [ACD93], which has been conjectured in [Alu91] and in [Yov93].

Finally, we prove that, under the interval-based semantics, the fragment of TPTL where only the $\mathbf{F}$ modality is allowed (we call it the *existential fragment* of TPTL) can be translated into MTL. This generalizes the fact that formula (1) can be expressed in MTL.

Related work. Over the last 15 years, many researches have focused on expressiveness questions for timed temporal logics (over both integer and real time). See [AH92a,AH93,AH94,AFH96,RSH98] for original works, and [Ost92,Hen98, Ras99] for a survey on that very topic.

MTL and TPTL have also been studied for the purpose of verification. If the underlying time domain is discrete, then MTL and TPTL have decidable verification problems [AH93,AH94]. When considering dense time, verification problems (satisfiability, model checking) become much harder: [AFH96] proves that the satisfiability problem for MTL is undecidable when considering the interval-based semantics. This result of course carries on for TPTL. It has recently been proved that MTL model checking and satisfiability *are* decidable over finite words under the pointwise semantics [OW05], while it is still undecidable for TPTL [AH94].

MTL and TPTL have also been studied in the scope of monitoring and path model checking. [TR04] proposes an (exponential) monitoring algorithm for MTL under the pointwise semantics. [MR05] shows that, in the interval-based semantics, MTL formulae can be verified on lasso-shaped timed state sequences in polynomial time, while TPTL formulae require at least polynomial space.

Plan of the paper. The paper is organized as follows: in Section 2, we define the logics TPTL and MTL together with their two possible semantics. In Section 3, we present our main result, namely that TPTL is strictly more expressive than MTL (for both semantics), whereas the last section (Section 4) focuses on the existential fragments of TPTL and MTL, where we prove that those two fragments are equally expressive under the interval-based semantics.

2 Linear-Time Timed Temporal Logics

In the sequel, AP represents a non-empty, countable set of atomic propositions.

Basic definitions. Let $\mathbb{R}$ denote the set of reals, $\mathbb{R}^+$ the set of nonnegative reals, $\mathbb{Q}$ the set of rationals and $\mathbb{N}$ the set of nonnegative integers. An *interval* is a convex subset of $\mathbb{R}$. Two intervals I and I' are said to be *adjacent* when $I \cap I' = \emptyset$ and $I \cup I'$ is an interval. We denote by $\mathcal{I}_\mathbb{R}$ the set of intervals, and by $\mathcal{I}_\mathbb{Q}$ the set of intervals whose bounds are in $\mathbb{Q}$.

Given a finite set X of variables called *clocks*, a *clock valuation* over X is a mapping $\alpha \colon X \to \mathbb{R}^+$ which assigns to each clock a time value in $\mathbb{R}^+$.

Timed state sequences and timed words. A *timed state sequence* over AP is a pair $\kappa = (\overline{\sigma}, \overline{I})$ where $\overline{\sigma} = \sigma_1\sigma_2\ldots$ is an infinite sequence of elements of 2^{AP} and $\overline{I} = I_1 I_2 \ldots$ is an infinite sequence of intervals satisfying the following properties:

- *(adjacency)* the intervals I_i and I_{i+1} are adjacent for all $i \geq 1$, and
- *(progress)* every time value $t \in \mathbb{R}^+$ belongs to some interval I_i.

A timed state sequence can equivalently be seen as an infinite sequence of elements of $2^{\mathsf{AP}} \times \mathcal{I}_\mathbb{R}$.

A *time sequence* over $\mathbb{R}^+$ is an infinite non-decreasing sequence $\tau = \tau_0\tau_1\ldots$ of nonnegative reals satisfying the following properties:

- *(initialization)* $\tau_0 = 0$,

– *(monotonicity)* the sequence is nondecreasing: $\forall\ i \in \mathbb{N}\ \tau_{i+1} \geq \tau_i$,
– *(progress)* every time value $t \in \mathbb{R}^+$ is eventually reached: $\forall t \in \mathbb{R}. \exists i.\ \tau_i > t$.

A *timed word* over AP is a pair $\rho = (\sigma, \tau)$, where $\sigma = \sigma_0\sigma_1\ldots$ is an infinite word over AP and $\tau = \tau_0\tau_1\ldots$ a time sequence over $\mathbb{R}^+$. It can equivalently be seen as an infinite sequence of elements $(\sigma_0, \tau_0)(\sigma_1, \tau_1)\ldots$ of $(\mathsf{AP} \times \mathbb{R})$.

We force timed words to satisfy $\tau_0 = 0$ in order to have a natural way to define initial satisfiability in the semantics of MTL. This is no loss of generality since it can be obtained by adding a special action to the alphabet.

Note that a timed word can be seen as a timed state sequence: for example the timed word $(a, 0)(a, 1.1)(b, 2)\ldots$ corresponds to the timed state sequence $(\{a\}, [0, 0])(\emptyset,]0, 1.1[)(\{a\}, [1.1, 1.1])(\emptyset, [1.1, 2[)(\{b\}, [2, 2])\ldots$

2.1 Clock Temporal Logic (TPTL)

The logic TPTL [AH94,Ras99] is a timed extension of LTL [Pnu77] which uses extra variables (clocks) explicitly in the formulae. Formulae of TPTL are built from atomic propositions, boolean connectives, "until" operators, clock constraints and clock resets:

$$\mathsf{TPTL} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \varphi_1 \mathbf{U}\, \varphi_2 \mid x \sim c \mid x.\varphi$$

where $p \in \mathsf{AP}$ is an atomic proposition, x is a clock variable, $c \in \mathbb{Q}$ is a rational number and $\sim\, \in \{\leq, <, =, >, \geq\}$.

There are two main semantics for TPTL, the *interval-based* semantics which interprets TPTL over timed state sequences, and the *pointwise* semantics, which interprets TPTL over timed words. This last semantics is less general as (as we will see below) formulae can only be interpreted at points in time when actions occur.

In the literature, these two semantics are used indifferently, but results highly depends on the underlying semantics. For example, a recent result by Ouaknine and Worrell [OW05] states that MTL (a subset of TPTL, see below) is decidable under the pointwise semantics, whereas it is known to be undecidable under the interval-based semantics [AFH96].

Interval-based semantics. In this semantics, models are time state sequences κ, and are evaluated at a date $t \in \mathbb{R}^+$ with a valuation $\alpha : X \to \mathbb{R}^+$ (where X is the set of clocks for formulae of TPTL). The satisfaction relation (denoted with $(\kappa, t, \alpha) \models_i \varphi$) is defined inductively as follows:

$$\begin{array}{rcl}
(\kappa, t, \alpha) \models_i p & \text{iff} & p \in \kappa(t) \\
(\kappa, t, \alpha) \models_i \varphi_1 \wedge \varphi_2 & \text{iff} & (\kappa, t, \alpha) \models_i \varphi_1 \text{ and } (\kappa, t, \alpha) \models_i \varphi_2 \\
(\kappa, t, \alpha) \models_i \neg\varphi & \text{iff} & \neg[(\kappa, t, \alpha) \models_i \varphi] \\
(\kappa, t, \alpha) \models_i \varphi_1 \mathbf{U}\, \varphi_2 & \text{iff} & \exists t' > t \text{ such that } (\kappa, t', \alpha) \models_i \varphi_2 \\
 & & \quad \text{and } \forall t < t'' < t',\ (\kappa, t'', \alpha) \models_i \varphi_1 \vee \varphi_2 \\
(\kappa, t, \alpha) \models_i x \sim c & \text{iff} & t - \alpha(x) \sim c \\
(\kappa, t, \alpha) \models_i x.\varphi & \text{iff} & (\kappa, t, \alpha[x \mapsto t]) \models_i \varphi
\end{array}$$

We write $\kappa \models_i \varphi$ when $(\kappa, 0, \mathbf{0}) \models_i \varphi$ where $\mathbf{0}$ is the valuation assigning 0 to all clocks.

Following [Ras99], we interpret "$x.\varphi$" as a reset operator. Note also that the semantics of $\mathbf{U}$ is strict in the sense that, in order to satisfy $\varphi_1 \mathbf{U} \varphi_2$, a time state sequence is not required to satisfy φ_1; this semantics is more expressive than the non-strict semantics (see section 2.4).

In the following, we use classical shorthands: $\top$ holds for $p \vee \neg p$, $\varphi_1 \Rightarrow \varphi_2$ holds for $\neg\varphi_1 \vee \varphi_2$, $\mathbf{F}\,\varphi$ holds for $\top \mathbf{U}\,\varphi$ (and means that φ eventually holds at a future time), and $\mathbf{G}\,\varphi$ holds for $\neg(\mathbf{F}\,\neg\varphi)$ (and means that φ always holds in the future).

Pointwise semantics. In this semantics, models are timed words ρ, and satisfiability is no longer interpreted at a date $t \in \mathbb{R}$ but at a position $i \in \mathbb{N}$ in the timed word. For a timed word $\rho = (\sigma, \tau)$ with $\sigma = (\sigma_i)_{i \geq 0}$ and $\tau = (\tau_i)_{i \geq 0}$, we define the satisfaction relation $(\rho, i, \alpha) \models_p \varphi$ inductively as follows (where α is a valuation for the set X of formula clocks):

$$\begin{array}{rcl}
(\rho, i, \alpha) \models_p p & \text{iff} & \sigma_i = p \\
(\rho, i, \alpha) \models_p \varphi_1 \wedge \varphi_2 & \text{iff} & (\rho, i, \alpha) \models_p \varphi_1 \text{ and } (\rho, i, \alpha) \models_p \varphi_2 \\
(\rho, i, \alpha) \models_p \neg\varphi & \text{iff} & \neg[(\rho, i, \alpha) \models_p \varphi] \\
(\rho, i, \alpha) \models_p \varphi_1 \mathbf{U}\, \varphi_2 & \text{iff} & \exists j > i \text{ s.t. } (\rho, j, \alpha) \models_p \varphi_2 \\
& & \quad \text{and } \forall i < k < j\ (\rho, k, \alpha) \models_p \varphi_1 \\
(\rho, i, \alpha) \models_p x \sim c & \text{iff} & \tau_i - \alpha(x) \sim c \\
(\rho, i, \alpha) \models_p x.\varphi & \text{iff} & (\rho, i, \alpha[x \mapsto \tau_i]) \models_p \varphi
\end{array}$$

We write $\rho \models_p \varphi$ whenever $(\rho, 0, \mathbf{0}) \models_p \varphi$.

Example 1. Consider the timed word $\rho = (a, 0)(a, 1.1)(b, 2)\ldots$ which, as already mentioned, can be viewed as the time state sequence

$$\kappa = (\{a\}, [0])(\emptyset, (0, 1.1))(\{a\}, [1.1, 1.1])(\emptyset, (1.1, 2))(\{b\}, [2, 2])\ldots$$

If $\varphi = x.\mathbf{F}\,(x = 1 \wedge y.\mathbf{F}\,(y = 1 \wedge b))$, then

$$\rho \not\models_p \varphi \quad \text{whereas} \quad \kappa \models_i \varphi$$

This is due to the fact that there is no action at date 1 along ρ.

2.2 Metric Temporal Logic (MTL)

The logic MTL [Koy90,AH93] extends the logic LTL with time restrictions on "until" modalities. Formulae of MTL are built from atomic propositions, boolean connectives and time-constrained "until":

$$\mathsf{MTL} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \varphi_1 \mathbf{U}_I\, \varphi_2$$

where p ranges over the set AP of atomic propositions, and I an interval in $\mathcal{I}_{\mathbb{Q}}$.

For defining the semantics of MTL, we better view MTL as a fragment of TPTL: $\varphi_1 \mathbf{U}_I \varphi_2$ is then interpreted as $x.(\varphi_1 \mathbf{U} (x \in I \wedge \varphi_2))$. As for TPTL, we will thus consider both the interval-based (interpreted over time state sequences) and the pointwise (interpreted over timed words) semantics.

We omit the constraint on modality $\mathbf{U}$ when $[0, \infty)$ is assumed. We write $\mathbf{U}_{\sim c}$ for $\mathbf{U}_I$ when $I = \{t \mid t \sim c\}$. As previously, we use classical shorthands such as $\mathbf{F}_I$ or $\mathbf{G}_I$.

Example 2. In MTL, the formula φ of Example 1 expresses as $\mathbf{F}_{=1}\mathbf{F}_{=1}b$. In the interval-based semantics, this formula is equivalent to $\mathbf{F}_{=2}b$, and this is **not** the case in the pointwise semantics.

2.3 Adding Past-Time Modalities

The logics defined above only allow to deal with future time points. As for LTL, we can define a symmetric version of the "Until" modality, named "Since", that deals with events that occurred in the past [Kam68,LPZ85]. The semantics of that modality is defined symmetrically:

– For the interval-based semantics:

$$\begin{aligned}(\kappa, t, \alpha) \models_i \varphi_1 \mathbf{S} \varphi_2 \quad \text{iff} \quad & \exists t' < t \text{ such that } (\kappa, t', \alpha) \models_i \varphi_2 \\ & \text{and } \forall t' < t'' < t,\ (\kappa, t'', \alpha) \models_i \varphi_1 \vee \varphi_2\end{aligned}$$

– For the pointwise semantics:

$$\begin{aligned}(\rho, i, \alpha) \models_p \varphi_1 \mathbf{S} \varphi_2 \quad \text{iff} \quad & \exists j < i \text{ s.t. } (\rho, j, \alpha) \models_p \varphi_2 \\ & \text{and } \forall j < k < i\ (\rho, k, \alpha) \models_p \varphi_1\end{aligned}$$

This way, formula $x.(p \mathbf{S} (q \wedge x = -2))$ expresses that q held 2 t.u. earlier, and that p held between that time point and the current one.

The corresponding MTL modality is defined in the obvious way. We note MTL+Past (resp. TPTL+Past) the logic MTL (resp. TPTL) extended with the "Since" modality. Such extensions have been defined and studied in [AH92a, AH93].

2.4 Relative Expressiveness

Let $\mathcal{S}$ be a set of models, and $\mathcal{L}$ and $\mathcal{L}'$ two logical languages interpreted over models in $\mathcal{S}$. We say that a formula $\varphi \in \mathcal{L}$ is *equivalent* to $\psi \in \mathcal{L}'$ if for every $\pi \in \mathcal{S}$, π satisfies φ iff π satisfies ψ. $\mathcal{L}'$ is strictly more expressive than $\mathcal{L}$ over $\mathcal{S}$ iff all formulae in $\mathcal{L}$ have an equivalent formula in $\mathcal{L}'$ and there exists a formula in $\mathcal{L}'$ which has no equivalent in $\mathcal{L}$. We say that $\mathcal{L}$ and $\mathcal{L}'$ are equally expressive whenever all formulae in $\mathcal{L}$ (resp. $\mathcal{L}'$) have an equivalent in $\mathcal{L}'$ (resp. $\mathcal{L}$).

Let us mention some classical results about expressiveness of linear-time temporal logics:

– first of all, it is quite obvious that the strict until is at least as expressive as the non-strict one. The converse inclusion does not hold in general (for example, it can be shown that formula $\neg a \wedge (a\,\mathbf{U}\,b)$, involving the strict until, cannot be expressed using only non-strict until).
– adding past-time modalities to LTL does not increase its expressive power: any LTL+Past formula can be expressed in LTL [Kam68,GPSS80]. But there are cases where the resulting LTL formula is exponentially larger [LMS02]. Those result don't carry on to timed temporal logics: [AH92a] shows that past-time modalities strictly increase the expressive power of MITL, a weak version of MTL where punctuality (*i.e.* singular intervals) are not allowed as timing constraints.

Proving expressiveness results is sometimes involved. In order to prove that a given formula φ cannot be expressed in a logic $\mathcal{L}$, the basic technique is to build two models M and N such that φ *distinguishes* between them (*i.e.* evaluates to true on one model and to false on the other one), and prove that no formula of $\mathcal{L}$ distinguishes between those two models. However, that technique is generally too "naive", and it is often needed to build two families of models (M_i) and (N_i) s.t. φ distinguishes between M_i and N_i for all i, and such that no formula in $\mathcal{L}$ with size less than i distinguishes between M_i and N_i. This technique is applied *e.g.* in [EH86,Eme91,Lar95,BCL05] as well as in this paper.

Other techniques involve translations of temporal logics to other formalisms, such as automata theory, language theory, algebraic structures or pebble games. Many examples can be found in the literature [Kam68,GPSS80,AH92a,TW96, LMS02].

3 TPTL is Strictly More Expressive Than MTL

3.1 Conjecture

It has been conjectured in [AH92b,AH93,Hen98] that TPTL is strictly more expressive than MTL, and in particular that a TPTL formula such as

$$\mathbf{G}\,(a \Rightarrow x.\mathbf{F}\,(b \wedge \mathbf{F}\,(c \wedge\ x \leq 2)))$$

can not be expressed in MTL. The following proposition states that this formula is not a good witness formula for proving that TPTL is strictly more expressive than MTL.

Proposition 1. *The* TPTL *formula* $x.\mathbf{F}\,(b \wedge \mathbf{F}\,(c \wedge\ x \leq 2))$ *can be expressed in* MTL *for the interval-based semantics.*

Proof. Let Φ be the TPTL formula $x.\mathbf{F}\,(b \wedge \mathbf{F}\,(c \wedge x \leq 2))$. This formula expresses that, along the time state sequence, from the current point on, there is a b followed by a c, and the delay before that c is less than 2 t.u. For proving the proposition, we write an MTL formula Φ' which is equivalent to Φ over time state sequences. Formula Φ' is defined as the disjunction of three formulae $\Phi' = \Phi'_1 \vee \Phi'_2 \vee \Phi'_3$ where:

$$\begin{cases} \Phi'_1 = \mathbf{F}_{\leq 1}\, b \wedge \mathbf{F}_{[1,2]}\, c \\ \Phi'_2 = \mathbf{F}_{\leq 1}\, (b \wedge \mathbf{F}_{\leq 1}\, c) \\ \Phi'_3 = \mathbf{F}_{\leq 1}\, (\mathbf{F}_{\leq 1}\, b \wedge \mathbf{F}_{=1}\, c) \end{cases}$$

Let κ be a time state sequence. If $\kappa \models_i \Phi'$, it is obvious that $\kappa \models_i \Phi$. Suppose now that $\kappa \models_i \Phi$, then there exists $0 < t_1 < t_2 \leq 2$ such that[1] $(\kappa, t_1) \models_i b$ and $(\kappa, t_2) \models_i c$. If $t_1 \leq 1$ then κ satisfies Φ'_1 or Φ'_2 (or both) depending on t_2 being smaller or greater than 1. If $t_1 \in]1,2]$ then there exists a date t' in $(0,1]$ such that $(\kappa, t') \models_i \mathbf{F}_{\leq 1}\, b \wedge \mathbf{F}_{=1}\, c$ which implies that $\kappa \models_i \Phi'_3$. We illustrate the three possible cases on Fig. 1. □

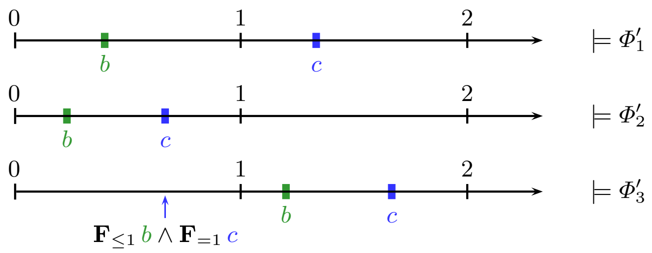


Fig. 1. Translation of TPTL formula Φ in MTL

From the proposition above we get that the TPTL formula $\mathbf{G}\,(a \Rightarrow \Phi)$ is equivalent over time state sequences to the MTL formula $\mathbf{G}\,(a \Rightarrow \Phi')$. However this does not imply that the conjecture is wrong, and we will now prove two results:

- $x.\mathbf{F}\,(b \wedge \mathbf{F}\,(c \wedge\ \ x \leq 2))$ can not be expressed in MTL for the pointwise semantics (thus over timed words)
- the more involved TPTL formula $x.\mathbf{F}\,(a \wedge x \leq 1 \wedge \mathbf{G}\,(x \leq 1 \Rightarrow \neg b))$ can not be expressed in MTL for the interval-based semantics.

This implies that TPTL is indeed strictly more expressive than MTL for both pointwise and interval-based semantics, which positively answers the conjecture of [AH92b,AH93,Hen98].

3.2 Pointwise Semantics

We now show that the formula $\Phi = x.(\mathbf{F}\,(b \wedge \mathbf{F}\,(c \wedge x \leq 2)))$ cannot be expressed in MTL for the pointwise semantics.

[1] In this reasoning we abstract away the value for clock x as it corresponds to the date.

We note $\mathsf{MTL}_{p,n}$ the set of MTL formulae whose constants are multiples of p and whose temporal height is less than n. We construct two families of timed words $(\mathcal{A}_{p,n})_{p\in\mathbb{Q},n\in\mathbb{N}}$ and $(\mathcal{B}_{p,n})_{p\in\mathbb{Q},n\in\mathbb{N}}$ such that:

- $\mathcal{A}_{p,n} \models_p \Phi$ whereas $\mathcal{B}_{p,n} \not\models_p \Phi$ for every $p \in \mathbb{Q}$ and $n \in \mathbb{N}$,
- for all $\varphi \in \mathsf{MTL}_{p,n-3}$, $\mathcal{A}_{p,n} \models_p \varphi \iff \mathcal{B}_{p,n} \models_p \varphi$.

The two families of models are presented in Fig. 2. Note that there is no action between dates 0 and $2-p$. In $\mathcal{A}_{p,n}$ (resp. $\mathcal{B}_{p,n}$) the first b occurs at time $2-\frac{5p}{4n}$ (resp. $2-\frac{p}{4n}$); in both models the first c occurs at time $2-p+\frac{p}{2n}$ and actions b and c are repeated with period $\frac{p}{n}$. It is obvious that $\mathcal{A}_{p,n} \models_p \Phi$ whereas $\mathcal{B}_{p,n} \not\models_p \Phi$.

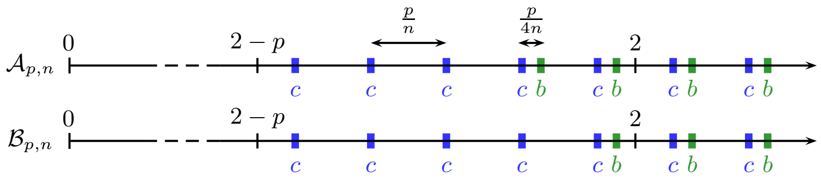


Fig. 2. Models $\mathcal{A}_{p,n}$ and $\mathcal{B}_{p,n}$

The expressiveness proof will be decomposed into several steps:

- we first prove that the two models $\mathcal{A}_{p,N+3}$ and $\mathcal{B}_{p,N+3}$ can not be distinguished by $\mathsf{MTL}_{p,N}$ formulae after date $2-p$ for the interval-based semantics
- we then show how we can use this result for the pointwise semantics
- we finally prove that the two models $\mathcal{A}_{p,N+3}$ and $\mathcal{B}_{p,N+3}$ can not be initially distinguished by an $\mathsf{MTL}_{p,N}$ formula in the pointwise semantics

We will prove two lemmas which show that $\mathcal{A}_{p,N+3}$ and $\mathcal{B}_{p,N+3}$ are indistinguishable at time $2-p$. For simplicity reason, we prove this two lemmas in the interval based semantics and then show that they can also be used for the pointwise semantics.

Lemma 2. *For all $\varphi \in \mathsf{MTL}$, for all $x > 2-\frac{5p}{4(N+3)}$,*

$$(\mathcal{A}_{p,N+3}, x) \models_i \varphi \iff (\mathcal{B}_{p,N+3}, x) \models_i \varphi$$

For all $\varphi \in \mathsf{MTL}$, for all $x \geq 2-p$,

$$(\mathcal{A}_{p,N+3}, x) \models_i \varphi \iff (\mathcal{B}_{p,N+3}, x + \frac{p}{N+3}) \models_i \varphi$$

Proof. The first property is due to the fact that for $x > 2-\frac{5p}{4(N+3)}$, the two models are the same. The second property is due to the fact that for $x > 2-\frac{5p}{4(N+3)}$, model $\mathcal{B}_{p,N+3}$ is a shift of model $\mathcal{A}_{p,N+3}$ of length $\frac{p}{N+3}$. $\square$

Lemma 3. *For all $\varphi \in \mathsf{MTL}_{p,k}$ with $0 \leq k \leq N$, for all $x \in [2-p, 2-\frac{(k+2)p}{N+3})$,*

$$\mathcal{A}_{p,N+3}, x \models_i \varphi \iff \mathcal{B}_{p,N+3}, x \models_i \varphi$$

The proof of this lemma is done by induction on k and φ and is given in appendix A.

We now want to use Lemmas 2 and 3 for the pointwise semantics, we thus show that the interval-based semantics is somehow “finer” than the pointwise semantics. We denote by action the formula $\bigvee_{a \in \mathsf{AP}} a$ which means that an action occurs, and for every formula $\varphi \in \mathsf{MTL}$, we construct a formula $\tilde{\varphi}$ inductively as follows:

- $\tilde{p} = p$ if p is a propositional variable
- $\widetilde{\varphi_1 \wedge \varphi_2} = \tilde{\varphi_1} \wedge \tilde{\varphi_2}$
- $\widetilde{\neg \varphi} = \neg \tilde{\varphi}$
- $\widetilde{\varphi_1 \, \mathbf{U}_I \, \varphi_2} = (\mathsf{action} \Rightarrow \tilde{\varphi_1}) \, \mathbf{U}_I \, (\mathsf{action} \wedge \tilde{\varphi_2})$

The following lemma relates both semantics and is then straightforward, by induction on the structure of formula φ:

Lemma 4. *If $\rho = (\sigma_i, \tau_i)_{i \geq 0}$ is a timed word, we note $\kappa(\rho)$ its corresponding time state sequence. Then for every $\varphi \in \mathsf{MTL}$, for every timed word ρ, $(\kappa(\rho), \tau_i) \models_i \tilde{\varphi} \iff (\rho, i) \models_p \varphi$.*

Note that if φ is in $\mathsf{MTL}_{p,N}$, then $\tilde{\varphi}$ is also in $\mathsf{MTL}_{p,N}$. Thus lemmas 2 and 3 also hold in the pointwise semantics, as if two models cannot be distinguished in MTL (resp. $\mathsf{MTL}_{p,N}$) in the interval-based semantics, neither can they in the pointwise semantics.

We can now prove the following lemma:

Lemma 5. *For every $\varphi \in \mathsf{MTL}_{p,N}$,*

$$(\mathcal{A}_{p,N+3}, 0) \models_p \varphi \iff (\mathcal{B}_{p,N+3}, 0) \models_p \varphi$$

The proof of this lemma is given in appendix A.

This concludes the expressiveness proof: we have constructed two families of timed words $(\mathcal{A}_{p,N+3})_{p \in \mathbb{Q}, N \in \mathbb{N}}$ and $(\mathcal{B}_{p,N+3})_{p \in \mathbb{Q}, N \in \mathbb{N}}$ such that $\mathcal{A}_{p,N+3} \models_p \Phi$, $\mathcal{B}_{p,N+3} \not\models \Phi$, but $\mathcal{A}_{p,N+3}$ and $\mathcal{B}_{p,N+3}$ can not initially be distinguished by formulae in $\mathsf{MTL}_{p,N}$ for the pointwise semantics. This implies that formula Φ has no equivalent formula in MTL (as every formula of MTL is in some $\mathsf{MTL}_{p,N}$ for some $p \in \mathbb{Q}$ and $N \in \mathbb{N}$). We can now state the following theorem:

Theorem 6. TPTL *is strictly more expressive than* MTL *for the pointwise semantics.*

Since the MTL+Past formula $\mathbf{F}_{\leq 2} \, (c \wedge \top \, \mathbf{S} \, b)$ also distinguishes between the families of models $(\mathcal{A}_{p,n})_{p \in \mathbb{Q}, n \in \mathbb{N}}$ and $(\mathcal{B}_{p,n})_{p \in \mathbb{Q}, n \in \mathbb{N}}$, we get the following corollary:

Corollary 7. MTL+Past *is strictly more expressive than* MTL *for the pointwise semantics.*

Note that the above result is a main difference between the timed and the untimed framework where it is well-known that past does not add any expressiveness to LTL [Kam68,GPSS80], but this is to be put together with the result of [AH92b] where it is proved that past adds expressive power to MITL, a subset of MTL where punctuality is not allowed.

3.3 Interval-Based Semantics

As we have seen, the formula which has been used for the pointwise semantics can not be used for the interval-based semantics. We will instead prove the following proposition:

Proposition 8. *The* TPTL *formula* $\Phi = x.\mathbf{F}\,(a \wedge x \leq 1 \wedge \mathbf{G}\,(x \leq 1 \Rightarrow \neg b))$ *has no equivalent* MTL *formula over time state sequences.*

Proof. Assume some formula $\Psi \in$ MTL is equivalent to Φ over time state sequences, and define its granularity p as follows:

$$p = \prod_{\frac{a}{b} \in \Psi} \frac{1}{b}.$$

W.l.o.g., we may assume that Ψ uses only constraints of the form $\sim p$, with $\sim \in \{<,=,>\}$. Let N be the temporal height of this formula, *i.e.* the maximum number of nested modalities. We write $\mathsf{MTL}^{-}_{p,n}$ for the fragment of MTL using only $\sim p$ constraints, and with temporal height at most n. Thus $\Psi \in \mathsf{MTL}^{-}_{p,n}$.

Now, we build two different time state sequences $\mathcal{A}_{p,n}$ and $\mathcal{B}_{p,n}$, such that Φ holds initially in the first one but not in the second one. We will then prove that they cannot be distinguished by any formula in $\mathsf{MTL}^{-}_{p,n-3}$.

Let us first define $\mathcal{A}_{p,n}$. Along that time state sequence, atomic proposition a will be set to true exactly at time points $\frac{p}{4n} + \alpha\frac{p}{2n}$, where α may be any nonnegative integer. Atomic proposition b will hold exactly at times $(\alpha+1)\cdot\frac{p}{2} - \frac{4p}{6n}$, with $\alpha \in \mathbb{N}$.

As for $\mathcal{B}_{p,n}$, it has exactly the same a's, and b holds exactly at time points $(\alpha+1)\cdot\frac{p}{2} - \frac{p}{6n}$, with $\alpha \in \mathbb{N}$.

The portion between 0 and $\frac{p}{2}$ of both time state sequences is represented on Fig. 3. Both time state sequences are in fact periodic, with period $\frac{p}{2}$.

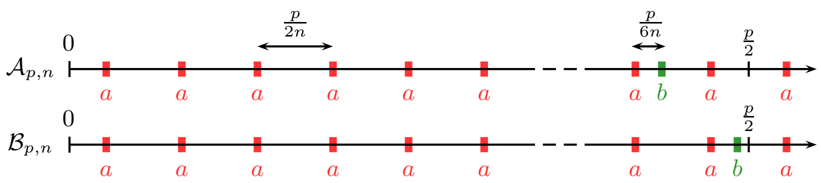


Fig. 3. Two timed paths $\mathcal{A}_{p,n}$ and $\mathcal{B}_{p,n}$

The following lemma is straightforward since, for each equivalence, the suffixes of the paths are the same.

Lemma 9. *For any positive p and n, for any nonnegative real x, and for any* MTL *formula φ,*

$$\mathcal{A}_{p,n}, x \models_i \varphi \iff \mathcal{B}_{p,n}, x + \frac{p}{2n} \models_i \varphi \tag{2}$$

$$\mathcal{A}_{p,n}, x \models_i \varphi \iff \mathcal{A}_{p,n}, x + \frac{p}{2} \models_i \varphi \tag{3}$$

$$\mathcal{B}_{p,n}, x \models_i \varphi \iff \mathcal{B}_{p,n}, x + \frac{p}{2} \models_i \varphi \tag{4}$$

We can now prove the following lemma:

Lemma 10. *For any $k \leq N$, for any $\varphi \in \mathsf{MTL}^-_{p,k}$, for any $x \in \left[0, \frac{p}{2} - \frac{(k+2)p}{2(N+3)}\right)$, for any nonnegative integer α, we have*

$$\mathcal{A}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi \iff \mathcal{B}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi$$

Proof. The proof is by induction on both k and the structure of the formula φ.

- The case where $k = 0$ is easy, since φ may only be a propositional formula, and all positions in the interval we consider are labeled with the same propositions.
- Assume the result holds for some $k < N$. We prove it for $k + 1$.
  - the case of atomic propositions and boolean combinations is still straightforward.
  - Assume $\varphi = \varphi_1 \mathbf{U}_{=p} \varphi_2$: Pick some value $x \in \left[0, \frac{p}{2} - \frac{(k+1+2)p}{2(N+3)}\right)$ and $\alpha \in \mathbb{N}$, and assume $\mathcal{A}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{=p} \varphi_2$. Then φ_2 holds at position $(\alpha + 2)\frac{p}{2} + x$, and φ_1 holds at all intermediate positions. Applying the induction hypothesis, we get that $\mathcal{B}_{p,N+3}, (\alpha + 2)\frac{p}{2} + x \models \varphi_2$. We also obtain that φ_1 holds along $\mathcal{B}_{p,N+3}$ at positions between $\alpha\frac{p}{2} + x$ and $\alpha\frac{p}{2} + x + \frac{p}{2(N+3)}$. It also holds at positions between $\alpha\frac{p}{2} + x + \frac{p}{2(N+3)}$ and $(\alpha+2)\frac{p}{2}+x$ thanks to equation (2). This entails that $\mathcal{B}_{p,N+3}, \alpha\frac{p}{2}+x \models \varphi$. Conversely, assume that $\mathcal{B}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{=p} \varphi_2$. With the induction hypothesis, we get that $\mathcal{A}_{p,N+3}, (\alpha + 2)\frac{p}{2} + x \models \varphi_2$. From equation (2), we know that φ_1 holds between $\alpha\frac{p}{2}+x$ and $(\alpha+2)\frac{p}{2}+x-\frac{p}{2(N+3)}$ along $\mathcal{B}_{p,N+3}$. Last, equation (3) ensures that it also holds between $(\alpha + 2)\frac{p}{2} + x - \frac{p}{2(N+3)}$ and $(\alpha + 2)\frac{p}{2} + x$, which completes the proof.
  - Assume $\varphi = \varphi_1 \mathbf{U}_{<p} \varphi_2$: Pick some value $x \in \left[0, \frac{p}{2} - \frac{(k+1+2)p}{2(N+3)}\right)$ and $\alpha \in \mathbb{N}$, and assume $\mathcal{A}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{<p} \varphi_2$.
    - ∗ If the witness for φ_2 lies between $\alpha\frac{p}{2}+x$ and $(\alpha+1)\frac{p}{2}+x$, then by applying equation (2), we get that $\mathcal{B}_{p,N+3}, (\alpha + 1)\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{<\frac{p}{2}} \varphi_2$. The induction hypothesis ensures that φ_1 holds on time state sequence $\mathcal{B}_{p,N+3}$ between $\alpha\frac{p}{2}+x$ and $(\alpha+1)\frac{p}{2}+x$, and we deduce that $\mathcal{B}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{<p} \varphi_2$.
    - ∗ Now, if the witness lies between $(\alpha+1)\frac{p}{2}+x$ and $(\alpha+2)\frac{p}{2}+x$, with equation (3), there is also a possible witness between $\alpha\frac{p}{2} + x$ and $(\alpha + 1)\frac{p}{2} + x$, and we apply the previous proof.

Conversely, assume $\mathcal{B}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{<p} \varphi_2$. We still consider two cases:

* If the witness for φ_2 lies between $\alpha\frac{p}{2}+x$ and $\alpha\frac{p}{2}+x+\frac{p}{2(N+3)}$, we can apply the induction hypothesis to φ_1 and φ_2, and we get the result.
* Otherwise, it suffices to apply equation (2).

- Last, assume that $\varphi = \varphi_1 \mathbf{U}_{>p} \varphi_2$: Pick some value x in the interval $\left[0, \frac{p}{2} - \frac{(k+1+2)p}{2(N+3)}\right)$ and $\alpha \in \mathbb{N}$, and assume $\mathcal{A}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{>p} \varphi_2$. By applying equation (2), and the induction hypothesis for φ_1, we get that $\mathcal{B}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{>p} \varphi_2$.
  Conversely, if $\mathcal{B}_{p,N+3}, \alpha\frac{p}{2} + x \models \varphi_1 \mathbf{U}_{>p} \varphi_2$, if the witnessing position for φ_2 lies after $\alpha\frac{p}{2} + x + \frac{p}{2(N+3)}$, it suffices to apply equation (2). Otherwise, equation (3) ensures that we can find another witness for φ_2 satisfying this condition. This completes the proof. □

As a corollary of the lemma, when $k = N$ and $\alpha = x = 0$, we get that any formula in $\mathsf{MTL}^-_{p,N}$ cannot distinguish between models $\mathcal{A}_{p,N+3}$ and $\mathcal{B}_{p,N+3}$. This is in contradiction with the fact that Ψ is equivalent to Φ, since Ψ holds initially along $\mathcal{A}_{p,k}$ but fails to hold initially along $\mathcal{B}_{p,k}$, for any k. This concludes the proof of Proposition 8. □

We can now state our main theorem:

Theorem 11. TPTL *is strictly more expressive than* MTL *for the interval-based semantics.*

Note that the formula $x.\mathbf{F}\,(a \wedge x \leq 1 \wedge \mathbf{G}\,(x \leq 1 \Rightarrow \neg b))$ does not use the $\mathbf{U}$ modality, so the fragment of TPTL using $\mathbf{F}$ and $\mathbf{G}$ modalities is also strictly more expressive than MTL for the interval-based semantics. This is not the case for the fragment of TPTL using only the $\mathbf{F}$ modality (see section 4).

Since the MTL+Past formula $\mathbf{F}_{=1}\,(\neg b\,\mathbf{S}\,a)$ distinguishes between the two families of models $(\mathcal{A}_{p,n})_{p\in\mathbb{Q},n\in\mathbb{N}}$ and $(\mathcal{B}_{p,n})_{p\in\mathbb{Q},n\in\mathbb{N}}$, we get the following corollary:

Corollary 12. MTL+Past *is strictly more expressive than* MTL *for the interval-based semantics.*

Up to our knowledge, this is the first expressiveness result for timed linear-time temporal logics using past modalities under the interval-based semantics.

4 On the Existential Fragments of MTL and TPTL

$\mathsf{TPTL}_\mathbf{F}$ is the fragment of TPTL which only uses the $\mathbf{F}$ modality (and not a general $\mathbf{U}$ modality) and which does not use the general negation but only negation of atomic propositions. Formally, $\mathsf{TPTL}_\mathbf{F}$ is defined by the following grammar:

$$\mathsf{TPTL}_\mathbf{F} \ni \varphi ::= p \mid \neg p \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mathbf{F}\,\varphi \mid x \sim c \mid x.\varphi.$$

An example of a $\mathsf{TPTL}_\mathbf{F}$ formula is $x.\mathbf{F}\,(b \wedge \mathbf{F}\,(c \wedge x \leq 2))$ (see Subsection 3.1). Similarly we define the fragment $\mathsf{MTL}_\mathbf{F}$ of MTL where only $\mathbf{F}$ modalities are allowed:

$$\mathsf{MTL}_\mathbf{F} \ni \varphi ::= p \mid \neg p \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mathbf{F}_I\,\varphi.$$

From Subsection 3.2, we know that, under the pointwise semantics, $\mathsf{TPTL}_\mathbf{F}$ is strictly more expressive than $\mathsf{MTL}_\mathbf{F}$, since formula $x.\mathbf{F}\,(b \wedge \mathbf{F}\,(c \wedge x \leq 2))$ has no equivalent in MTL (thus in $\mathsf{MTL}_\mathbf{F}$). On the contrary, when considering the interval-based semantics, we proved that this $\mathsf{TPTL}_\mathbf{F}$ formula can be expressed in $\mathsf{MTL}_\mathbf{F}$ (see Subsection 3.1). In this section, we generalize the construction of Subsection 3.1, and prove that $\mathsf{TPTL}_\mathbf{F}$ and $\mathsf{MTL}_\mathbf{F}$ are in fact equally expressive for the interval-based semantics.

Theorem 13. *$\mathsf{TPTL}_\mathbf{F}$ is not more expressive than $\mathsf{MTL}_\mathbf{F}$ for the interval-based semantics.*

Proof. We may assume w.l.o.g. that all constants appearing in formulae of $\mathsf{TPTL}_\mathbf{F}$ are integers.

Normal form of $\mathsf{TPTL}_\mathbf{F}$ formulae. For the sake of simplicity, we assume w.l.o.g. that all $\mathbf{F}$ modalities are directly embedded into some reset operator "$x.$", and that any clock x appearing in the formula is reset only once. Every $\mathsf{TPTL}_\mathbf{F}$ formula can be easily transformed into an equivalent formula of the following logic:

$$\varphi ::= p \mid \neg p \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid x \sim c \mid x.\mathbf{F}\,\varphi \tag{5}$$

where $p \in \mathsf{AP}$ is an atomic proposition, x is a clock variable, c is a rational and $\sim \in \{\leq, <, =, >, \geq\}$. We call *atom* an atomic proposition or its negation.

We now recursively build a normal form for $\mathsf{TPTL}_\mathbf{F}$ formulae, which is some kind of disjunctive normal form.

Definition 14. *A $\mathsf{TPTL}_\mathbf{F}$ formula is said* simple *if it is an atom, a clock constraint or if it is of the form:*

$$x.\mathbf{F}\left(\bigwedge_{k=1}^{l_1} a_k \wedge \left(\bigwedge_{k=1}^{l_2} x_k \sim_k c_k\right) \wedge \bigwedge_{k=1}^{l_3} \varphi_k\right)$$

where a_k are atoms, x_k are clocks, c_k are rationals, $\sim_k \in \{\leq, <, =, >, \geq\}$ and φ_k are simple $\mathsf{TPTL}_\mathbf{F}$ formulae.

The following lemma is straightforward, using the property that $x.\mathbf{F}\,(\varphi_1 \vee \varphi_2)$ is equivalent to $(x.\mathbf{F}\,\varphi_1) \vee (x.\mathbf{F}\,\varphi_2)$.

Lemma 15. *Every $\mathsf{TPTL}_\mathbf{F}$ formula is equivalent to some boolean combination of simple $\mathsf{TPTL}_\mathbf{F}$ formulae.*

From $\mathsf{TPTL}_\mathbf{F}$ *formulae to systems of difference inequations.* In this part, we recursively transform a $\mathsf{TPTL}_\mathbf{F}$ formula into a system of inequations, where a subformula $x.\mathbf{F}\ \varphi$ is represented by the date y at which φ holds. This yields extra conditions between y and the other clocks and variables that already appear in the transformation.

We first define the so-called *systems of difference inequations*, into which we want to transform $\mathsf{TPTL}_\mathbf{F}$ formulae.

Definition 16. *Let X be the set of formula clocks, and Y be a finite set of variables disjoint from X. A* system $\mathcal{S}$ *over Y is a pair $(V, \mathcal{J})$ where $V\colon Y \to \mathsf{MTL}_\mathbf{F}$ associates to every variable an $\mathsf{MTL}_\mathbf{F}$ formula, and $\mathcal{J}$ is a set of (difference) inequations of the form $x - x' \sim c$ or $x \sim c$ where x, x' are elements of $X \cup Y$.*

The conjunction of two systems $\mathcal{S} = (V, \mathcal{J})$ and $\mathcal{S}' = (V', \mathcal{J}')$, denoted by $\mathcal{S} \wedge \mathcal{S}'$, is the system $(V'', \mathcal{J} \cup \mathcal{J}')$ where $V''\colon y \mapsto V(y) \wedge V'(y)$. By abuse of notation, for any $y \in Y$, we will simply write $\mathcal{S}(y)$ instead of $V(y)$, and if e is an inequation of $\mathcal{J}$, we will note $e \in \mathcal{S}$.

Let $\mathcal{S}$ be a system over Y, κ be a time state sequence, $v\colon Y \to \mathbb{R}^+$ be a valuation, and $\alpha\colon X \to \mathbb{R}^+$ a context for clocks in X. We say that $(\kappa, v, \alpha) \vdash \mathcal{S}$ iff the context $\alpha'\colon X \cup Y \to \mathbb{R}^+$ that naturally extends v and α satisfies the following properties:

$$\forall e \in \mathcal{S}.\ \alpha' \models e \quad \text{and} \quad \forall y \in Y.\ (\kappa, v(y)) \models_i \mathcal{S}(y).$$

Now, the satisfaction relation is defined as follows:

$$(\kappa, t, \alpha) \models \mathcal{S} \quad \text{iff} \quad \exists v\colon Y \to \mathbb{R}^+ \text{ s.t. } (\kappa, v, \alpha) \vdash \mathcal{S} \text{ and } \forall\ y \in Y,\ v(y) \geq t.$$

Now, let φ be a simple $\mathsf{TPTL}_\mathbf{F}$ formula. We explain how to inductively build a system $\mathcal{S}_\varphi$ such that

$$(\kappa, 0, \alpha) \models_i \varphi \quad \text{iff} \quad (\kappa, 0, \alpha) \models \mathcal{S}_\varphi.$$

- If φ is an atom, the system has no constraint and only one variable y, and $\mathcal{S}(y) = \varphi$;
- If φ is a clock constraint $x \sim c$, the system has one constraint, $y \sim c$, and $\mathcal{S}(y) = \top$.
- The main case is now if φ is $x.\mathbf{F}\ \left(\bigwedge_{k=1}^{l_1} a_k \wedge \left(\bigwedge_{k=1}^{l_2} x_{i_k} \sim_k c_k\right) \wedge \bigwedge_{k=1}^{l_3} \varphi_k\right)$, where we assume that φ_k have the form $x_{j_k}.\mathbf{F}\ \psi_k$ and that we already computed a system $\mathcal{S}_{\varphi_k}$ over Y_k for each $1 \leq k \leq l_3$; The construction of the system is done inductively as follows: $\mathcal{S}_\varphi$ is the system over $Y = \bigcup_{k=1}^{l_3} Y_k \cup \{y\}$, where y is a fresh variable representing the current date, defined by the following conjunction:

$$\mathcal{S}_\varphi = \bigwedge_{1 \leq k \leq l_3} \mathcal{S}_{\varphi_k}[x_{j_k} \leftarrow y] \ \wedge\ \begin{cases} V : y \mapsto \bigwedge_{k=1}^{l_1} a_k \\ \mathcal{J} = \{y > x\} \cup \{y - x_{i_k} \sim_k c_k \mid 1 \leq k \leq l_2\} \end{cases}$$

where $\mathcal{S}_{\varphi_k}[x_{j_k} \leftarrow y]$ is the system $\mathcal{S}_{\varphi_k}$ in which variable x_{j_k} has been replaced by y. For the outer-most "$x.\mathbf{F}$" we replace x by 0 because we start evaluating the formula at date 0.

Example 3. For the formula $x_1.\mathbf{F}\,(a \wedge x_2.\mathbf{F}\,(b \wedge x_1 \leq 2))$, the system which is constructed is:

$$\mathcal{S} = \left\{ \begin{array}{l} V : y_1 \mapsto a \\ \qquad y_2 \mapsto b \\ \mathcal{J} = \left\{ \begin{array}{l} y_2 \leq 2 \\ y_2 > y_1 \\ y_1 > 0 \end{array} \right\} \end{array} \right.$$

It is just a technical matter to prove that:

$$(\kappa, t, \alpha[x \mapsto t]) \models_i \varphi \iff (\kappa, t, \alpha[x \mapsto t]) \models \mathcal{S}_\varphi.$$

The proof is by induction on the structure of φ, and is given in Appendix B.

Note that thanks to the above equivalence, the construction of the system gives a decidability procedure for the satisfiability of $\mathsf{TPTL}_\mathbf{F}$: to decide satisfiability of formula φ we roughly have to decide whether the system $\mathcal{S}_\varphi$ has a solution using simple linear programming and to ensure consistence of the solution, *i.e.* to check that whenever $V(y_i)$ is not consistent with $V(y_j)$, then $y_i \neq y_j$ (see corollary 20).

Properties of systems. Let $\mathcal{S}$ be a system and ψ be an $\mathsf{MTL}_\mathbf{F}$ formula. We say that $\mathcal{S}$ and ψ are *equivalent* if, for every time state sequence κ,

$$(\kappa, 0, \mathbf{0}) \models \mathcal{S} \quad \text{iff} \quad (\kappa, 0) \models_i \psi.$$

Our goal is thus to find a $\mathsf{MTL}_\mathbf{F}$ formula ψ equivalent to $\mathcal{S}_\varphi$.

We say that two systems $\mathcal{S} = (V, \mathcal{J})$ and $\mathcal{S}' = (V', \mathcal{J}')$ are *equivalent* whenever $V = V'$ and $\mathcal{J}$ and $\mathcal{J}'$ have the same solutions. Note that two equivalent systems represent $\mathsf{TPTL}_\mathbf{F}$ formulae that are equivalent over time state sequences.

The following lemma can easily be proved.

Lemma 17. *Let $\mathcal{S}_1 = (V, \mathcal{J}_1)$ and $\mathcal{S}_2 = (V, \mathcal{J}_2)$ be two systems, and $\mathcal{S}$ be a system equivalent to $(V, \mathcal{J}_1 \vee \mathcal{J}_2)$. Then*

$$(\kappa, t, \alpha) \models \mathcal{S} \iff (\kappa, t, \alpha) \models \mathcal{S}_1 \ \textit{or}\ (\kappa, t, \alpha) \models \mathcal{S}_2.$$

Thanks to this lemma, we have the following property: if φ_i is an $\mathsf{MTL}_\mathbf{F}$ formula equivalent to a system $\mathcal{S}_i$, then $\varphi_1 \vee \varphi_2$ is an $\mathsf{MTL}_\mathbf{F}$ formula equivalent to $\mathcal{S}$.

Reduction to bounded systems of difference inequations. We fix a system $\mathcal{S} = (V, \mathcal{J})$, assuming $\mathcal{J} = \{x_i - x_j \prec_{i,j} m_{i,j} \mid i,j = 0 \dots n\}$ is a set of constraints in normal form (*i.e.* all constraints are tightened. See how such sets of constraints or equivalently DBMs can be manipulated in [Bou04]). We assume in addition (even if it means adding constraints of the form $x_i \leq x_j$) that constraints in $\mathcal{J}$ imply that $x_{i-1} \leq x_i$ for every $0 < i \leq n$, and we let M be the maximal constant appearing in $\mathcal{J}$. For every $\mathsf{b}\colon \{1,\dots,n\} \to \{\leq, >\}$, we define a new set of constraints $\mathcal{J}^{\mathsf{b}}$ where constraints $\{x_i - x_{i-1}\ \mathsf{b}(i)\ M \mid 1 \leq i \leq n\}$ are added to $\mathcal{J}$. We claim the following two lemmas:

Lemma 18. $(a_i)_{0 \leq i \leq n}$ *is a solution of* $\mathcal{J}$ *iff it is a solution of* $\mathcal{J}^{\mathsf{b}}$ *for some* $\mathsf{b}\colon \{1,\dots,n\} \to \{\leq, >\}$.

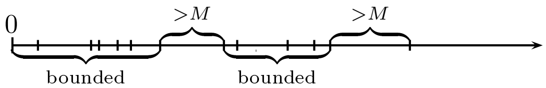
Lemma 19. *We pick some* $\mathsf{b}\colon \{1,\dots,n\} \to \{\leq, >\}$ *such that* $\mathcal{J}^{\mathsf{b}}$ *is consistent (*i.e. *$\mathcal{J}^{\mathsf{b}}$ has a solution), and write* $\equiv_{\mathsf{b}}$ *for the following equivalence on indices:*

$$i \equiv_{\mathsf{b}} j \quad \text{iff} \quad \text{for all } i \leq k < j,\ \mathsf{b}(k) = \leq.$$

Then $\mathcal{J}^{\mathsf{b}}$ *is equivalent to*

$$\{x_i - x_j \prec_{i,j} m_{i,j} \mid i \equiv_{\mathsf{b}}, j\} \cup \{x_i - x_{i-1}\ \mathsf{b}(i)\ M \mid 1 \leq i \leq n\}.$$

Lemma 19 can be depicted as follows:



On this picture, each point on the line represents a variable, and a part denoted "bounded" gathers variables whose differences are bounded by the system of inequations $\mathcal{J}^{\mathsf{b}}$. Two "bounded" parts are separated by at least M t.u.

From Lemma 18, if ψ^{b} is an $\mathsf{MTL}_{\mathbf{F}}$ formula equivalent to $\mathcal{S}^{\mathsf{b}}$, then the disjunction of all ψ^{b}'s, when b ranges in the whole set of functions $\{1,\dots,n\} \to \{\leq, >\}$, is equivalent to $\mathcal{S}$. It remains to explain how we construct a formula equivalent to a system $\mathcal{S}^{\mathsf{b}}$.

We fix a $\mathsf{b}\colon \{1,\dots,n\} \to \{\leq, >\}$, and denote by $(I_i)_{0 \leq i \leq p}$ the equivalence classes for $\equiv_{\mathsf{b}}$ (in increasing order). For each $0 \leq i \leq p$, we denote by n_i the largest index in I_i. We assume we have a procedure which computes $\mathsf{MTL}_{\mathbf{F}}$ formulae equivalent to a system $\mathcal{S} = (V, \mathcal{J})$ where $\mathcal{J}$ implies that all variables are bounded. We will describe such a procedure in the next paragraphs. We note the resulting $\mathsf{MTL}_{\mathbf{F}}$ formula $\Psi(\mathcal{S})$. By a decreasing induction we define systems $(\mathcal{S}_i)_{0 \leq i \leq p}$ as follows: $\mathcal{S}_i = (V_i, \mathcal{J}_i)$ is a system over $\{x_j \mid j \in I_i\}$ and

$$\begin{cases} \begin{cases} V_i(x_j) = V^{\mathsf{b}}(x_j) & \text{if } (i = p \text{ and } j \in I_i) \text{ or if } j \in I_i \smallsetminus \{n_i\} \\ V_i(x_{n_i}) = V^{\mathsf{b}}(x_{n_i}) \wedge \mathbf{F}_{>M}\, \Psi(\mathcal{S}_{i+1}) & \text{if } i \neq p \end{cases} \\ \mathcal{J}_i = \mathcal{J}^{\mathsf{b}}_{|I_i} \text{ is the restriction of } \mathcal{J}^{\mathsf{b}} \text{ to variables } \{x_j \mid j \in I_i\} \end{cases}$$

From Lemma 19, formula ψ^{b} is equivalent to formula $\Psi(\mathcal{S}_0)$ defined above. That way, we have reduced our initial problem to that of finding $\mathsf{MTL}_{\mathbf{F}}$ formulae equivalent to systems $\mathcal{S} = (V, \mathcal{J})$ where constraints in $\mathcal{J}$ imply that all variables are bounded.

Decomposition of bounded systems of difference inequations. We fix $\mathcal{S} = (V, \mathcal{J})$. We assume that the variables involved in $\mathcal{J}$ are $\{x_i \mid 0 \le i \le n\}$, and that they are bounded by M. Following region decompositions of timed automata [AD94], we split $\mathcal{J}$ in systems where constraints are regions. Roughly, a region specifies in which elementary intervals (interval of the form $(c; c+1)$ or singleton $\{c\}$ for $c \le M$) lie the differences $x_i - x_j$. It is then sufficient to find $\mathsf{MTL}_{\mathbf{F}}$ formulae for systems $\mathcal{S} = (V, \mathcal{J})$ where $\mathcal{J}$ represents a bounded region.

A region R can be equivalently characterized by sets of variables $(X_i)_{0 \le i \le p}$ (that form a partition of $\{x_i \mid 0 \le i \le n\}$) such that[2]

- $x \in X_0$ iff $\langle x \rangle = 0$,
- $x, y \in X_i$ iff $\langle x \rangle = \langle y \rangle$,
- $x \in X_i$ and $y \in X_j$ with $i < j$ implies $\langle x \rangle < \langle y \rangle$.

Let $\mathcal{S}' = (V', \mathcal{J}')$ be the system over $\{X_i \mid 1 \le i \le p\}$ (X_i are viewed as variables here) such that for every $1 \le i \le p$, $V'(X_i) = \bigwedge_{x \in X_i} \mathbf{F}_{=\lfloor x \rfloor} V(x)$, and $\mathcal{J}'$ is the system $0 < X_1 < \ldots < X_p < 1$.

If we can find an $\mathsf{MTL}_{\mathbf{F}}$ formula ψ' equivalent to $\mathcal{S}'$, then formula[3]

$$\left(\bigwedge_{x \in X_0} \mathbf{F}_{=\lfloor x \rfloor} V(x) \right) \wedge \psi'$$

will be equivalent to $\mathcal{S}$.

$\mathsf{MTL}_{\mathbf{F}}$ *formulae for simple systems.* It remains to find $\mathsf{MTL}_{\mathbf{F}}$ formulae $\Psi_{[1\ldots p],r}$ equivalent to systems $\mathcal{S}_{p,r} = (V, \mathcal{J}_{p,r})$ over $\{X_i \mid 1 \le i \le p\}$, where r is any rational and $\mathcal{J}_{p,r}$ is the set of constraints $0 < X_1 < \cdots < X_p < r$. Note that we assume we have a unique function V which is used for all systems $\mathcal{S}_{p,r}$ even if it is a notation abuse. We do the construction by induction on p: $\Psi_{[1],r} = \mathbf{F}_{<r} V(X_1)$, and $\Psi_{[1\ldots p],r}$ is the conjunction of the following four formulae Φ_1 to Φ_4, distinguishing between the possible positions of the variables:

- if there is no variable in the interval $\left(0, \frac{r}{p}\right]$ and all p variables are in the interval $\left(\frac{r}{p}, r\right)$:
$$\Phi_1 = \Psi_1 \vee \mathbf{F}_{<\frac{r}{p}} (\Psi_1) .$$
where
$$\Psi_1 = \bigvee_{i=1}^{p-1} \left(\left(\mathbf{F}_{=r-\frac{i.r}{p}} V(X_p) \right) \wedge \Psi_{[1\ldots p-1],r-\frac{i.r}{p}} \right)$$
The formula Φ_1 distinguishes between the possible positions for the last variable X_p: it is in one of the intervals $\left[r - \frac{i.r}{p}\right]$ or $\left(r - \frac{i.r}{p}, r - \frac{(i-1).r}{p}\right)$ with $1 \le i \le p-1$.

[2] $\langle \alpha \rangle$ represents the fractional part of α.

[3] $\lfloor x \rfloor$ represents the lower bound of the interval in which variable x lies in R (if interval for x is $\{c\}$ or $(c; c+1)$, then $\lfloor x \rfloor$ is c).

Note that Φ_1 does not exactly express the above property: it may contain some more cases, but still expresses that $0 < X_1 < \cdots < X_p < r$. The same remark also applies for the other three formulae.

– if there is $0 < h < p$ variables in the interval $\left(0, \frac{r}{p}\right)$ and $p - h$ variables in the interval $\left(\frac{r}{p}, r\right)$:

$$\Phi_2 = \Psi_{[1\ldots h],\frac{r}{p}} \wedge \mathbf{F}_{=\frac{r}{p}} \left(\Psi_{[h+1\ldots p],r-\frac{r}{p}}\right).$$

– if there is $0 < h < p$ variables in the interval $\left(0, \frac{r}{p}\right)$, one variable at date $\frac{r}{p}$, and $p - h - 1$ variables in the interval $\left(\frac{r}{p}, r\right[$:

$$\Phi_3 = \Psi_{[1\ldots h],\frac{r}{p}} \wedge \mathbf{F}_{=\frac{r}{p}} \left(V(X_{h+1}) \wedge \Psi_{[h+2\ldots p],r-\frac{r}{p}}\right).$$

– last case, if all variables are in the interval $\left(0, \frac{r}{p}\right)$:

$$\Phi_4 = \mathbf{F}_{<\frac{r}{p}} \left(V(X_1) \wedge \mathbf{F}_{<\frac{r}{p}} \left(V(X_2) \wedge (\cdots)\right)\right)$$

It can easily be proved, by induction, that the resulting formula is equivalent to $\mathcal{S}_{p,r}$. □

Our construction from $\mathsf{TPTL}_\mathbf{F}$ to $\mathsf{MTL}_\mathbf{F}$ is exponential. We first compute the normal form of the $\mathsf{TPTL}_\mathbf{F}$ formula φ by choosing for every disjunction one of the disjuncts: the normal form is then the disjunction of all the formulae obtained by such choices. This gives an exponential number of formulae whose disjunction corresponds to φ, the size of each formula being linear in the size of φ. The reduction to bounded systems produces for each formula an exponential number of systems (whose size is polynomial in the size of φ). Then for each system we compute the corresponding MTL formula which has an exponential size in the size of the system. The MTL formula for φ is finally a combination of this exponential number of exponential formulae, its size is thus simply exponential.

It is known [AFH96] that the satisfiability problem for TPTL and MTL is undecidable for the interval-based semantics, whereas it has been proved recently that the satisfiability problem for MTL is decidable but non primitive recursive for the pointwise semantics [OW05]. As a corollary of the previous proof (in particular of the construction of the system), we get:

Corollary 20. *The satisfiability problem for* $\mathsf{TPTL}_\mathbf{F}$ *(and thus* $\mathsf{MTL}_\mathbf{F}$*) is NP-complete for the interval-based semantics.*

First guess for each disjunction of the formula one of the disjuncts, and build the system $\mathcal{S} = (V, \mathcal{J})$ for the new formula which is directly in normal form, then guess an order on the variables which is consistent with the constraints in $\mathcal{J}$, finally solve a simple linear programming problem. For each guess, the problem can be solved in polynomial time and all guesses are independent, we thus get that the problem is in NP. As SAT is a subproblem of the satisfiability of $\mathsf{TPTL}_\mathbf{F}$, we conclude that the latter is NP-complete.

5 Conclusion

In this paper we have proved the conjecture (first proposed in [AH90]) that the logic TPTL is strictly more expressive than MTL. However we have also proved that the TPTL formula $\mathbf{G}\,(a \rightarrow x.\mathbf{F}\,(b \wedge \mathbf{F}\,(c \wedge x \leq 1)))$, which had been proposed as an example of formula which could not be expressed in MTL, has indeed an equivalent formula in MTL for the interval-based semantics. We have thus proposed another formula of TPTL which can not be expressed in MTL.

As side results, we have obtained that MTL+Past is strictly more expressive than MTL, which is a main difference with the untimed framework where past modalities do not add any expressive power to LTL [Kam68,GPSS80]. In the timed framework, no such result was known, it was only known that past modalities add expressive power to MITL (a strict subset of MTL) under the pointwise semantics [AH92b].

Linear models we have used for proving above expressiveness results can be viewed as special cases of branching-time models. Our results thus apply to the branching-time logic TCTL (by replacing the modality $\mathbf{U}$ with the modality $\mathbf{AU}$), and translate as: TCTL with explicit clocks [HNSY94] is strictly more expressive than TCTL with subscripts [ACD93], as conjectured in [Alu91,Yov93].

Finally, we have proved that the fragment of TPTL which only uses the $\mathbf{F}$ modality can be translated in MTL. However the construction we provide suffers from an exponential blowup. An interesting problem would then be to study the conciseness of the fragment of TPTL compared with MTL.

As further developments, we would like to study automata formalisms equivalent to both logics TPTL and MTL. Three existing works may appear as interesting starting points, namely [AH92b,LW05,OW05].

References

[ACD90] Rajeev Alur, Costas Courcoubetis, and David Dill. Model-checking for real-time systems. In *Proc. 5th Annual Symposium on Logic in Computer Science (LICS'90)*, pages 414–425. IEEE Computer Society Press, 1990.

[ACD93] Rajeev Alur, Costas Courcoubetis, and David Dill. Model-checking in dense real-time. *Information and Computation*, 104(1):2–34, 1993.

[AD94] Rajeev Alur and David Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.

[AFH96] Rajeev Alur, Tomás Feder, and Thomas A. Henzinger. The benefits of relaxing punctuality. *Journal of the ACM*, 43(1):116–146, 1996.

[AH90] Rajeev Alur and Thomas A. Henzinger. Real-time logics: Complexity and expressiveness. In *Proc. 5th Annual Symposium on Logic in Computer Science (LICS'90)*, pages 390–401. IEEE Computer Society Press, 1990. Preliminary version of [AH93].

[AH92a] Rajeev Alur and Thomas A. Henzinger. Back to the future: towards a theory of timed regular languages. In *Proc. 33rd Annual Symposium on Foundations of Computer Science (FOCS'92)*, pages 177–186. IEEE Computer Society Press, 1992.

[AH92b] Rajeev Alur and Thomas A. Henzinger. Logics and models of real-time: a survey. In *Real-Time: Theory in Practice, Proc. REX Workshop 1991*, volume 600 of *Lecture Notes in Computer Science*, pages 74–106. Springer, 1992.

[AH93] Rajeev Alur and Thomas A. Henzinger. Real-time logics: Complexity and expressiveness. *Information and Computation*, 104(1):35–77, 1993.

[AH94] Rajeev Alur and Thomas A. Henzinger. A really temporal logic. *Journal of the ACM*, 41(1):181–204, 1994.

[Alu91] Rajeev Alur. *Techniques for Automatic Verification of Real-Time Systems.* PhD thesis, Stanford University, Stanford, CA, USA, 1991.

[BCL05] Patricia Bouyer, Franck Cassez, and François Laroussinie. Modal logics for timed control. Research Report LSV-05-04, Laboratoire Spécification & Vérification, ENS de Cachan, France, 2005.

[Bou04] Patricia Bouyer. Forward analysis of updatable timed automata. *Formal Methods in System Design*, 24(3):281–320, 2004.

[EH86] E. Allen Emerson and Joseph Y. Halpern. "Sometimes" and "not never" revisited: On branching versus linear time temporal logic. *Journal of the ACM*, 33(1):151–178, 1986.

[Eme91] E. Allen Emerson. *Temporal and Modal Logic*, volume B (Formal Models and Semantics) of *Handbook of Theoretical Computer Science*, pages 995–1072. MIT Press Cambridge, 1991.

[GPSS80] Dov M. Gabbay, Amir Pnueli, Saharon Shelah, and Jonathan Stavi. On the temporal analysis of fairness. In *Conference Record 7th ACM Symposium on Principles of Programming Languages (POPL'80)*, pages 163–173. ACM Press, 1980.

[Hen98] Thomas A. Henzinger. It's about time: Real-time logics reviewed. In *Proc. 9th International Conference on Concurrency Theory (CONCUR'98)*, volume 1466 of *Lecture Notes in Computer Science*, pages 439–454. Springer, 1998.

[HNSY94] Thomas A. Henzinger, Xavier Nicollin, Joseph Sifakis, and Sergio Yovine. Symbolic model-checking for real-time systems. *Information and Computation*, 111(2):193–244, 1994.

[Kam68] Johan A.W. Kamp. *Tense Logic and the Theory of Linear Order.* PhD thesis, UCLA, Los Angeles, CA, USA, 1968.

[Koy90] Ron Koymans. Specifying real-time properties with metric temporal logic. *Real-Time Systems*, 2(4):255–299, 1990.

[Lar95] François Laroussinie. About the expressive power of CTL combinators. *Information Processing Letters*, 54(6):343–345, 1995.

[LMS02] François Laroussinie, Nicolas Markey, and Philippe Schnoebelen. Temporal logic with forgettable past. In *Proc. 17th Annual Symposium on Logic in Computer Science (LICS'02)*, pages 383–392. IEEE Computer Society Press, 2002.

[LPZ85] Orna Lichtenstein, Amir Pnueli, and Lenore D. Zuck. The glory of the past. In *Proc. Conference on Logics of Programs*, volume 193 of *Lecture Notes in Computer Science*, pages 413–424. Springer-Verlag, 1985.

[LW05] Slawomir Lasota and Igor Walukiewicz. Alternating timed automata. In *Proc. 8th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'05)*, volume 3441 of *Lecture Notes in Computer Science*, pages 250–265. Springer, 2005.

[MR05] Nicolas Markey and Jean-François Raskin. Model checking restricted sets of timed paths. *Theoretical Computer Science*, 2005. To appear.

[Ost92] Jonathan S. Ostroff. Formal methods for the specification and design of real-time safety critical systems. *Journal of Systems and Software*, 18(1):33–60, 1992.

[OW05] Joël Ouaknine and James B. Worrell. On the decidability of metric temporal logic. In *Proc. 19th Annual Symposium on Logic in Computer Science (LICS'05)*. IEEE Computer Society Press, 2005. To appear.

[Pnu77] Amir Pnueli. The temporal logic of programs. In *Proc. 18th Annual Symposium on Foundations of Computer Science (FOCS'77)*, pages 46–57. IEEE Computer Society Press, 1977.

[Ras99] Jean-François Raskin. *Logics, Automata and Classical Theories for Deciding Real-Time*. PhD thesis, University of Namur, Namur, Belgium, 1999.

[RSH98] Jean-François Raskin, Pierre-Yves Schobbens, and Thomas A. Henzinger. Axioms for real-time logics. In *Proc. 9th International Conference on Concurrency Theory (CONCUR'98)*, volume 1466 of *Lecture Notes in Computer Science*, pages 219–236. Springer, 1998.

[SC85] A. Prasad Sistla and Edmund M. Clarke. The complexity of propositional linear temporal logics. *Journal of the ACM*, 32(3):733–749, 1985.

[TR04] Prasanna Thati and Grigore Rosu. Monitoring algorithms for metric temporal logic specifications. In *Proc. 4th International Workshop on Runtime Verification (RV'04)*, Electronic Notes in Computer Science. Elsevier, 2004. To appear.

[TW96] Denis Thérien and Thomas Wilke. Temporal logic and semidirect products: an effective characterization of the until hierarchy. In *Proc. 37th Annual Symposium on Foundations of Computer Science (FOCS'96)*, pages 256–263. IEEE Computer Society Press, 1996.

[Var96] Moshe Y. Vardi. An automata-theoretic approach to linear temporal logic. In *Proc. Logics for Concurrency: Structure versus Automata*, volume 1043 of *Lecture Notes in Computer Science*, pages 238–266. Springer, 1996.

[VW86] Moshe Y. Vardi and Pierre Wolper. An automata-theoretic approach to automatic program verification. In *Proc. 1st Annual Symposium on Logic in Computer Science (LICS'86)*, pages 322–344. IEEE Computer Society Press, 1986.

[Yov93] Sergio Yovine. *Méthodes et outils pour la vérification symbolique de systèmes temporisés*. PhD thesis, Institut National Polytechnique de Grenoble, Grenoble, France, 1993.

A Proofs of Section 3

Lemma 3. *For all $\varphi \in \mathsf{MTL}_{p,k}$ with $0 \leq k \leq N$, for all $x \in \left[2-p, 2-\frac{(k+2)p}{N+3}\right)$,*

$$\mathcal{A}_{p,N+3}, x \models_i \varphi \iff \mathcal{B}_{p,N+3}, x \models_i \varphi$$

Proof. We can assume that φ is of the form $\varphi_1 \,\mathbf{U}_{=kp}\, \varphi_2$ or $\varphi_1 \,\mathbf{U}_{(kp,(k+1)p)}\, \varphi_2$ with $k \in \mathbb{N}$ as every formula is a boolean combination of atomic propositions and such formulae.

The proof will be done by induction on k and then on φ.

Case $k = 0$**.** In both models, interval $\left[2-p, 2-\frac{2p}{N+3}\right)$ are similar, atomic propositions (and boolean combinations) have the same truth values on both models.

Induction step. We take $1 \leq k \leq N$, and we assume that the lemma has been proved for $k-1$. We take some formula $\varphi \in \mathsf{MTL}_{p,k}$. φ is either of the form $\varphi_1 \mathbf{U}_{=lp} \varphi_2$ with $l \geq 1$ or $\varphi_1 \mathbf{U}_{(lp,(l+1)p)} \varphi_2$ with $l \in \mathbb{N}$. Both formulae φ_1 and φ_2 are in $\mathsf{MTL}_{p,k-1}$. We now take $x \in \left[2-p, 2-\frac{(k+2)p}{N+3}\right)$.

- We assume that $\varphi = \varphi_1 \mathbf{U}_{=lp} \varphi_2$ with $l \geq 1$.
  - We assume that $\mathcal{A}_{p,N+3}, x \models_i \varphi_1 \mathbf{U}_{=lp} \varphi_2$. It means that $\mathcal{A}_{p,N+3}, x + lp \models_i \varphi_2$ and $\forall 0 < t < lp$, $\mathcal{A}_{p,N+3}, x+t \models_i \varphi_1$.
    Obviously, as $x + lp \geq 2$, $\mathcal{B}_{p,N+3}, x + lp \models_i \varphi_2$ (Lemma 2, first point). Take some $0 < t < lp$.
    * if $x + t < 2 - \frac{((k-1)+2)p}{N+3} = 2 - \frac{(k+1)p}{N+3}$, by induction hypothesis (φ_1 has depth $k-1$), $\mathcal{B}_{p,N+3}, x+t \models_i \varphi_1$.
    * if $2 - \frac{(k+1)p}{N+3} \leq x + t < x + lp$ (in which case $x < x + t - \frac{p}{N+3}$ and thus $\mathcal{A}_{p,N+3}, x+t-\frac{p}{N+3} \models_i \varphi_1$), using Lemma 2 (second point), we get that $\mathcal{B}_{p,N+3}, x+t \models_i \varphi_1$.

    Thus $\mathcal{B}_{p,N+3}, x \models_i \varphi_1 \mathbf{U}_{=lp} \varphi_2$.
  - We assume that $\mathcal{B}_{p,N+3}, x \models_i \varphi_1 \mathbf{U}_{=lp} \varphi_2$. It means that $\mathcal{B}_{p,N+3}, x+lp \models_i \varphi_2$ and $\forall 0 < t < lp$, $\mathcal{B}_{p,N+3}, x+t \models_i \varphi_1$.
    Obviously, as $x + lp \geq 2$, $\mathcal{A}_{p,N+3}, x + lp \models_i \varphi_2$ (Lemma 2, first point). Take some $0 < t < lp$.
    * if $x + t < x + lp - \frac{p}{N+3}$, $\mathcal{B}_{p,N+3}, x+t+\frac{p}{N+3} \models_i \varphi_1$, and thus, using Lemma 2 second point, $\mathcal{A}_{p,N+3}, x+t \models_i \varphi_1$.
    * if $x+lp-\frac{p}{N+3} \leq x+t < x+lp$, in particular we have $x+t \geq 2-\frac{p}{N+3} > 2 - \frac{5p}{4(N+3)}$. From Lemma 2 first point, $\mathcal{A}_{p,N+3}, x+t \models_i \varphi_1$.

    Thus $\mathcal{A}_{p,N+3}, x \models_i \varphi_1 \mathbf{U}_{=lp} \varphi_2$.
- We assume that $\varphi = \varphi_1 \mathbf{U}_{(lp,(l+1)p)} \varphi_2$ with $l \geq 1$.
  We can do the same proof as for the case $= lp$ (we keep the same distance before φ_2 holds).
- We assume We assume that $\varphi = \varphi_1 \mathbf{U}_{<p} \varphi_2$.
  - We assume that $\mathcal{A}_{p,N+3}, x \models_i \varphi_1 \mathbf{U}_{<p} \varphi_2$. It means that $\mathcal{A}_{p,N+3}, x+t \models_i \varphi_2$ for some $0 < t < p$ and $\forall 0 < t' < t$, $\mathcal{A}_{p,N+3}, x+t' \models_i \varphi_1$.
    * $0 < t \leq \frac{p}{N+3}$, then we simply take $d = t$, and by induction hypothesis (all $x+d' < 2-\frac{(k+1)p}{N+3}$ whenever $d' \leq d$), we get that $\mathcal{B}_{p,N+3}, x+d \models_i \varphi_1$ and for all $0 < d' < d$, $\mathcal{B}_{p,N+3}, x+d' \models_i \varphi_1$.
    * if $\frac{p}{N+3} < t < p - \frac{p}{N+3}$, then we simply take $d = t + \frac{p}{N+3}$, and we get that $\mathcal{B}_{p,N+3}, x+d \models_i \varphi_2$ (Lemma 2), and for all $\frac{p}{N+3} < d' < d$, $\mathcal{B}_{p,N+3}, x+d' \models_i \varphi_1 \iff \mathcal{A}_{p,N+3}, x+d'-\frac{p}{N+3} \models_i \varphi_1$. We deduce that $\mathcal{B}_{p,N+3}, x+d' \models_i \varphi_1$. Assume that $0 < d' \leq \frac{p}{N+3}$, we have that $x + \frac{p}{N+3} \in \left[2-p, 2-\frac{(k+1)p}{N+3}\right)$. By induction hypothesis, $\mathcal{A}_{p,N+3}, x+d' \models_i \varphi_1 \iff \mathcal{B}_{p,N+3}, x+d' \models_i \varphi_1$. We thus get that $\mathcal{B}_{p,N+3}, x+d' \models_i \varphi_1$.

- $*$ if $p - \frac{p}{N+3} \leq t < p$, we take $d = t$. In that case $x + d > 2 - \frac{5p}{4(N+3)}$, thus using Lemma 2, we get that $\mathcal{B}_{p,N+3}, x + d \models_i \varphi_2$. We take now $\frac{p}{N+3} < d' < d$. We have that $\mathcal{A}_{p,N+3}, x + d' - \frac{p}{N+3} \models_i \varphi_1 \iff \mathcal{B}_{p,N+3}, x + d' \models_i \varphi_1$ (Lemma 2). As $0 < x + d' - \frac{p}{N+3} < t$, we get that $\mathcal{B}_{p,N+3}, x + d' \models_i \varphi_1$. We take $0 < d' \leq \frac{p}{N+3}$, in this case, $x+d' < 2 - \frac{(k+1)p}{N+3}$, by induction hypothesis, we get that $\mathcal{A}_{p,N+3}, x + d' \models_i \varphi_1 \iff \mathcal{B}_{p,N+3}, x + d' \models_i \varphi_1$, thus $\mathcal{B}_{p,N+3}, x + d' \models_i \varphi_1$ (as $0 < d' < t$).

  We get that $\mathcal{B}_{p,N+3}, x \models_i \varphi_1 \mathbf{U}_{<p} \varphi_2$.
- We assume that $\mathcal{B}_{p,N+3}, x \models_i \varphi_1 \mathbf{U}_{<p} \varphi_2$. It means that $\mathcal{B}_{p,N+3}, x+t \models_i \varphi_2$ for some $0 < t < p$ and $\forall 0 < t' < t$, $\mathcal{B}_{p,N+3}, x + t' \models_i \varphi_1$.
  - $*$ if $t > \frac{p}{N+3}$, we take $d = t - \frac{p}{N+3}$. Using Lemma 2 (second point), we get that $\mathcal{A}_{p,N+3} x + d \models_i \varphi_2 \iff \mathcal{B}_{p,N+3}, x + t \models_i \varphi_2$, thus $\mathcal{A}_{p,N+3} x + d \models_i \varphi_2$. Similarly, for all $0 < d' < d$, $\mathcal{A}_{p,N+3}, x + d' \models_i \varphi_1 \iff \mathcal{B}_{p,N+3}, x + d' + \frac{p}{N+3} \models_i \varphi_1$. As $d' + \frac{p}{N+3} < t$, we get that $\mathcal{A}_{p,N+3}, x + d' \models_i \varphi_1$.
  - $*$ if $t \leq \frac{p}{N+3}$, we take $d = t$. By induction hypothesis (as $x + d' < 2 - \frac{(k+1)p}{N+3}$ for all $0 < d' < d$), we get that $\mathcal{A}_{p,N+3}, x + d \models_i \varphi_2$ and for all $0 < d' < d$, $\mathcal{A}_{p,N+3}, x + d' \models_i \varphi_1$.

  We get that $\mathcal{A}_{p,N+3}, x \models_i \varphi_1 \mathbf{U}_{<p} \varphi_2$. □

Lemma 5. *For every $\varphi \in \mathsf{MTL}_{p,N}$,*

$$(\mathcal{A}_{p,N+3}, 0) \models_p \varphi \iff (\mathcal{B}_{p,N+3}, 0) \models_p \varphi$$

Proof. We can suppose that φ is of the form $\varphi_1 \mathbf{U}_{=kp} \varphi_2$ or $\varphi_1 \mathbf{U}_{(kp,(k+1)p)} \varphi_2$ with $k \in \mathbb{N}$ as every formula can be rewritten as a boolean combination of atomic propositions and such formulae.

We first give some notations: if i is a position in $\mathcal{A}_{p,N+3}$, we note $\check{\imath}$ the position in $\mathcal{B}_{p,N+3}$ which corresponds to the same date (as there is one b more in $\mathcal{A}_{p,N+3}$, i and $\check{\imath}$ may differ by 1), and similarly, if j is a position in $\mathcal{B}_{p,N+3}$, we note $\hat{\jmath}$ the position in $\mathcal{A}_{p,N+3}$ which corresponds to the same date. Note that $\hat{\jmath}$ is always correctly defined, whereas $\check{\imath}$ is not defined at date $2 - \frac{5p}{4(N+3)}$ because there is no action at this date in $\mathcal{B}_{p,N+3}$. If i (resp. j) is a position in $\mathcal{A}_{p,N+3}$ (resp. $\mathcal{B}_{p,N+3}$), we note $\tau_i^{\mathcal{A}_{p,N+3}}$ (resp. $\tau_j^{\mathcal{B}_{p,N+3}}$) the date corresponding to this position.

It is easy to treat formulae of the type $\varphi_1 \mathbf{U}_{=kp} \varphi_2$, as no action occurs both in $\mathcal{A}_{p,N+3}$ and $\mathcal{B}_{p,N+3}$ at time kp. Thus, for every $k \in \mathbb{N}$, $\mathcal{A}_{p,N+3}, 0 \not\models_p \varphi$ and $\mathcal{B}_{p,N+3}, 0 \not\models_p \varphi$.

We now focus on formulae of the form $\varphi = \varphi_1 \mathbf{U}_{(kp,(k+1)p)} \varphi_2$, and we distinguishing three cases:

– **Case** $(k+1)p \leq 2-p$. As no action occurs neither in $\mathcal{A}_{p,N+3}$, nor in $\mathcal{B}_{p,N+3}$, we get that $\mathcal{A}_{p,N+3}, 0 \not\models_p \varphi$ and $\mathcal{B}_{p,N+3}, 0 \not\models_p \varphi$; this implies that $\mathcal{A}_{p,N+3}, 0 \models_p \varphi \iff \mathcal{B}_{p,N+3}, 0 \models_p \varphi$.

– **Case** $kp \geq 2$. We assume that $(\mathcal{A}_{p,N+3}, 0) \models_p \varphi$. There exists a position i in $\mathcal{A}_{p,N+3}$ such that $\tau_i^{\mathcal{A}_{p,N+3}} \in (kp, (k+1)p)$, $(\mathcal{A}_{p,N+3}, i) \models_p \varphi_2$ and $\forall\ 0 < i' < i$, $(\mathcal{A}_{p,N+3}, i') \models_p \varphi_1$. We take $j = \check{\imath}$, and applying the first point of Lemma 2, we get that $(\mathcal{B}_{p,N+3}, j) \models_p \varphi_2$. We now show that $\forall 0 < j' < j$, $(\mathcal{B}_{p,N+3}, j') \models_p \varphi_1$. Take such a j'. If $j' = 1$, by hypothesis we have $(\mathcal{A}_{p,N+3}, 1) \models \varphi_1$ and as $\tau_1^{\mathcal{A}_{p,N+3}} = 2 - p + \frac{p}{2(N+3)}$, Lemma 3 gives us that $(\mathcal{B}_{p,N+3}, 1) \models_p \varphi_1$. Let $2 \leq j' < j$, then $2 \leq \hat{\jmath}' < i$ so $(\mathcal{A}_{p,N+3}, \hat{\jmath}' - 1) \models_p \varphi_1$ which, using the second point of Lemma 2, implies that $(\mathcal{B}_{p,N+3}, j') \models_p \varphi_1$. Thus we get that $(\mathcal{B}_{p,N+3}, 0) \models_p \varphi$.

Assume that $(\mathcal{B}_{p,N+3}, 0) \models_p \varphi$. There exists a position j such that $\tau_j^{\mathcal{B}_{p,N+3}} \in (kp, (k+1)p)$, $(\mathcal{B}_{p,N+3}, j) \models_p \varphi_2$ and $\forall\ 0 < j' < j$, $(\mathcal{B}_{p,N+3}, j') \models_p \varphi_1$. We take $i = \hat{\jmath}$. By Lemma 2 first point, $(\mathcal{A}_{p,N+3}, i) \models_p \varphi_2$. We now show that $\forall 0 < i' < i$, $(\mathcal{A}_{p,N+3}, i') \models_p \varphi_1$. Take such a i'. Let $1 \leq i' < i$, if $\tau_{i'}^{\mathcal{A}_{p,N+3}} \geq 2 - \frac{p}{N+3}$, we have that $(\mathcal{B}_{p,N+3}, \check{\imath}') \models_p \varphi_1$ and by Lemma 2 first point, this implies that $(\mathcal{A}_{p,N+3}, i') \models_p \varphi_1$. If $\tau_{i'}^{\mathcal{A}_{p,N+3}} < 2 - \frac{p}{N+3}$, let j' be such that $\tau_{j'}^{\mathcal{B}_{p,N+3}} = \tau_{i'}^{\mathcal{A}_{p,N+3}} + \frac{p}{N+3}$, we have that $j' < j$ so $(\mathcal{B}_{p,N+3}, j') \models_p \varphi_1$, which, by Lemma 2 second point, implies $(\mathcal{A}_{p,N+3}, i') \models_p \varphi_1$. We thus get that $(\mathcal{A}_{p,N+3}, 0) \models_p \varphi$.

– **Case** $kp = 2-p$ **(*i.e.* $\varphi = \varphi_1 \mathbf{U}_{(2-p,2)} \varphi_2$).** We assume that $(\mathcal{A}_{p,N+3}, 0) \models_p \varphi$. There exists a position i in $\mathcal{A}_{p,N+3}$ such that $\tau_i^{\mathcal{A}_{p,N+3}} \in (2-p, 2)$, $(\mathcal{A}_{p,N+3}, i) \models_p \varphi_2$ and $\forall 0 < i' < i$, $(\mathcal{A}_{p,N+3}, i') \models_p \varphi_1$. Either $\tau_i^{\mathcal{A}_{p,N+3}} < 2 - \frac{p}{N+3}$, in which case we take j such that $\tau_j^{\mathcal{B}_{p,N+3}} = \tau_i^{\mathcal{A}_{p,N+3}} + \frac{p}{N+3}$. Lemma 2 second point implies that $(\mathcal{B}_{p,N+3}, j) \models_p \varphi_2$. By Lemma 2 second point, we get $\forall 0 < i' < i$, $(\mathcal{A}_{p,N+3}, i') \models_p \varphi_1$ implies that $\forall 2 \leq j' < j$, $(\mathcal{B}_{p,N+3}, j') \models_p \varphi_1$. The case $j' = 1$ is obtained from $(\mathcal{A}_{p,N+3}, 1) \models_p \varphi_1$ *via* Lemma 3. On the other hand, if $\tau_i^{\mathcal{A}_{p,N+3}} \geq 2 - \frac{p}{N+3}$, we take $j = \check{\imath}$. We have $(\mathcal{A}_{p,N+3}, i) \models_p \varphi_2$, and by Lemma 2 first point, this raises that $(\mathcal{B}_{p,N+3}, j) \models_p \varphi_2$. The rest of the proof for $\tau_i^{\mathcal{A}_{p,N+3}} \geq 2 - \frac{p}{N+3}$ is identical to the case $\tau_i^{\mathcal{A}_{p,N+3}} < 2 - \frac{p}{N+3}$.

Suppose that $(\mathcal{B}_{p,N+3}, 0) \models_p \varphi$. There exists a position j of $\mathcal{B}_{p,N+3}$ such that $\tau_j^{\mathcal{B}_{p,N+3}} \in (2-p, 2)$, $(\mathcal{B}_{p,N+3}, j) \models_p \varphi_2$ and $\forall 0 < j' < j$, $(\mathcal{B}_{p,N+3}, j') \models_p \varphi_1$. If $j = 1$, we take $i = 1$, Lemma 3 implies that $(\mathcal{A}_{p,N+3}, 1) \models_p \varphi_2$. If $j > 1$, $\tau_j^{\mathcal{B}_{p,N+3}} > 2 - p + \frac{p}{N+3}$ and we take i such that $\tau_i^{\mathcal{A}_{p,N+3}} = \tau_j^{\mathcal{B}_{p,N+3}} - \frac{p}{N+3}$. Lemma 2 second point raises $(\mathcal{A}_{p,N+3}, i) \models_p \varphi_2$, and this same lemma gives that $\forall 1 \leq j' < j$, $(\mathcal{A}_{p,N+3}, j') \models_p \varphi_1$. Thus $(\mathcal{A}_{p,N+3}, 0) \models_p \varphi$. $\square$

B Proofs of Section 4

We show that the solutions of the system $\mathcal{S}_\varphi$ are exactly the models satisfying φ, *i.e.* that $\kappa, t, \alpha[x \mapsto t] \models \varphi \Leftrightarrow \kappa, t, \alpha[x \mapsto t] \vdash \mathcal{S}_\varphi$.

$$\begin{aligned}
&\kappa, t, \alpha[x \mapsto t] \models \varphi \\
&\qquad \Leftrightarrow \exists\ v(y) \geq t.\ \kappa, v(y) \models \bigwedge_{k=1}^{l_1} a_k \\
&\qquad\quad \forall\ 1 \leq k \leq l_2.\ v(y) - \alpha[x \mapsto t](x_{i_k}) \sim_k c_k \\
&\qquad\quad \forall\ 1 \leq k \leq l_3.\ \kappa, v(y), \alpha[x \mapsto t] \models x_{j_k}.\mathbf{F}\ \psi_k \\
&\qquad \Leftrightarrow \exists\ v(y) \geq t.\ \kappa, v(y) \models \bigwedge_{k=1}^{l_1} a_k \\
&\qquad\quad \forall\ 1 \leq k \leq l_2.\ v(y) - \alpha[x \mapsto t](x_{i_k}) \sim_k c_k \\
&\qquad\quad \forall\ 1 \leq k \leq l_3.\ \exists\ v_k \colon Y_k \to [v(y), +\infty). \\
&\qquad\qquad\quad \kappa, v_k, \alpha[x \mapsto t, x_{j_k} \mapsto v(y)] \vdash \mathcal{S}_{x_{j_k}.\mathbf{F}\ \psi_{j_k}} \text{ by IH} \\
&\qquad \Leftrightarrow \exists\ v(y) \geq t.\ \kappa, v(y) \models \bigwedge_{k=1}^{l_1} a_k \\
&\qquad\quad \forall\ 1 \leq k \leq l_2.\ v(y) - \alpha[x \mapsto t](x_{i_k}) \sim_k c_k \\
&\qquad\quad \exists \overline{v_k} \colon Y_k \cup \{y\} \to [t, +\infty) \text{ s.t. } \overline{v_k}(y) = v(y) \text{ and} \\
&\qquad\qquad\quad \kappa, \overline{v_k}, \alpha[x \mapsto t, x_{j_k} \mapsto v(y)] \vdash \mathcal{S}_{x_{j_k}.\mathbf{F}\ \psi_{j_k}}[x_{j_k} \leftarrow y] \\
&\qquad\quad \text{because } x_{j_k} \text{ is replaced by } y \text{ and valuation } \overline{v_k} \text{ associates to } y\ v(y) \\
&\qquad\quad \text{which is the value of } x_{j_k} \text{ previously assigned by the context} \\
&\qquad \Leftrightarrow \exists\ v \colon Y \to [t, +\infty) \text{ (extending each } v_k\text{) s.t. } \kappa, v(y) \models \bigwedge_{k=1}^{l_1} a_k \\
&\qquad\quad v(y) - \alpha[x \mapsto t](x) \geq 0 \\
&\qquad\quad \forall\ 1 \leq k \leq l_2.\ v(y) - \alpha[x \mapsto t](x_{i_k}) \sim_k c_k \\
&\qquad\quad \forall\ 1 \leq k \leq l_3.\ \kappa, v, \alpha[x \mapsto t, x_{j_k} \mapsto v(y)] \vdash \mathcal{S}_{x_{j_k}.\mathbf{F}\ \psi_{j_k}}[x_{j_k} \leftarrow y] \\
&\qquad \Leftrightarrow \exists\ v \colon Y \to [t, +\infty).\ \kappa, v(y) \models \bigwedge_{k=1}^{l_1} a_k \\
&\qquad\quad v(y) - \alpha[x \mapsto t](x) \geq 0 \\
&\qquad\quad \forall\ 1 \leq k \leq l_2.\ v(y) - \alpha[x \mapsto t](x_{i_k}) \sim_k c_k \\
&\qquad\quad \forall\ 1 \leq k \leq l_3.\ \kappa, v, \alpha[x \mapsto t] \vdash \mathcal{S}_{x_{j_k}.\mathbf{F}\ \psi_{j_k}}[x_{j_k} \leftarrow y] \\
&\qquad\quad \text{because } x_{j_k} \text{ does not appear anymore in } \mathcal{S}_{x_{j_k}.\mathbf{F}\ \psi_{j_k}}[x_{j_k} \leftarrow y] \\
&\qquad \Leftrightarrow \kappa, t, \alpha[x \mapsto t] \models \mathcal{S}_\varphi
\end{aligned}$$

In fact, in the implications from bottom to top, one is harder to prove, namely $\exists\ \overline{v_k} \colon Y_k \cup \{y\} \to [t, +\infty) \implies \exists\ v_k \colon Y_k \to [v(y), +\infty)$, because, *a priori*, v_k maps Y_k to $[t, +\infty[$. To show that, if $y' \in Y_k$, then $v_k(y') \geq v(y)$, we will use this straightforward lemma:

Lemma 6. *Let $\varphi = x.\mathbf{F}\ (\bigwedge_{k=1}^{l_1} a_k \wedge (\bigwedge_{k=1}^{l_2} x_{i_k} \sim_k c_k) \wedge \bigwedge_{k=1}^{l_3} x_{j_k}.\varphi_{j_k})$. Let $\mathcal{S}_\varphi(Y)$ be the system constructed from φ (and y be the variable associated to x). Let κ, v, α be such that $\kappa, v, \alpha[x \mapsto t] \vdash \mathcal{S}_\varphi$. Then $\forall\ y' \in Y.\ v(y') \geq v(y)$.*