Timed-automata-based verification of MITL over signals

Thomas Brihaye¹, Gilles Geeraerts², Hsi-Ming Ho¹, and Benjamin Monmege³

1 Université de Mons, Belgium, {thomas.brihaye,hsi-ming.ho}@umons.ac.be
2 Université libre de Bruxelles, Belgium, gigeerae@ulb.ac.be
3 Aix Marseille Univ, CNRS, LIF, France, benjamin.monmege@univ-amu.fr

Abstract

It has been argued that the most suitable semantic model for real-time formalisms is the non-negative real line (signals), i.e. the continuous semantics, which naturally captures the continuous evolution of system states. Existing tools like Uppaal are, however, based on ω-sequences with timestamps (timed words), i.e. the pointwise semantics. Furthermore, the support for logic formalisms is very limited in these tools. In this article, we amend these issues by a compositional translation from Metric Temporal Interval Logic (MITL) to signal automata. Combined with an emptiness-preserving encoding of signal automata into timed automata, we obtain a practical automata-based approach to MITL model-checking over signals. We implement the translation in our tool MIGHTYL and report on case studies using LTSmin as the back-end.

1998 ACM Subject Classification F.4.1 Mathematical Logic, F.1.1 Models of Computation

Keywords and phrases real-time temporal logic, timed automata, real-time systems

Digital Object Identifier 10.4230/LIPIcs.TIME.2017.?

1 Introduction

Many computer programs nowadays control critical applications, and need to enforce complex requirements in order to guarantee safe, dependable and efficient operation of the whole system. Among these requirements, real-time specifications (such as ‘every request is eventually followed by an acknowledgement within 3 time units’) are common. In this framework, computer interact with an environment that is intrinsically continuous, and ensuring thin real-time constraints is known to be a very difficult task.

Different kinds of formalisms have been proposed over the past 30 years to specify those real-time models (often by means of automata) and requirements (usually by means of some logic language). On the automata side, the model of timed automata [2] is arguably widely accepted today, a success which is due in part to the tool support provided by UPPAAL [35] and other verification tools such as KRONOS [12], TiAMO [11], ... As far as logics are concerned, several proposals have been made in the literature during the past 30 years (such as MTL [33], TPTL [7], TCTL [1], ...) but the recent research seems to focus mainly on MTL, for theoretical reasons (we think here of the works of Ouaknine and Worrell on the decidability of MTL [38]); and on MITL [4] for more practical motivations [10,13,14,16,31,36].

Indeed, since its introduction in 1996, MITL has been advocated as a good ‘trade-off between realistic modelling of time and feasible verification of timing properties’ [4]. MITL is at the same time a real-time extension of LTL, the most widely accepted logic in the non-real-time case; and a restriction of MTL, whose expressive power makes it undecidable in most practical cases [6,38]. Unfortunately, tool support for MITL is still lacking today,
Timed-automata-based verification of MITL over signals

albeit MITL’s clear practical interest (and indeed, the need for such tool support is repeatedly emphasised in several papers [4, 10, 36]). UPPAAL, the most prominent real-time model checker, supports only a restricted subset of TCTL; and the alternatives are either not publicly available, or too restricted, or too experimental (see the related work hereinafter for a more comprehensive picture). We believe this is due to the relative lack of maturity of automata-based support for MITL, at least when compared with LTL.

Another point of debate in the community is the choice of the semantics for real-time models. The two different options are known as the pointwise and continuous semantics. In the pointwise semantics, executions of the system are timed words, i.e. sequences of pairs (timestamp, system state). That is, the system’s states can only be observed at selected timestamps (which are non-negative real values). In the continuous semantics, executions are signals, i.e. sequences of contiguous intervals during which the states of the system does not change and can be continuously observed. While the pointwise semantics is the most common today (probably due to the success of timed automata which have initially been defined in this framework), it has been argued [8, 29] that the continuous semantics models time more faithfully, and it is indeed adopted in many works about control of hybrid systems [41], synthetic biology [9], etc. Apart from these practical considerations, the difference between these two semantics matters as it changes the expressive power of the logic1. For example, the following formula (asking that \(p\) holds exactly in an interval of the form \([0, a]\) for some \(a \geq 0\)) is satisfiable in the continuous semantics only:

\[ p \land F(\neg p) \land G(\neg p \Rightarrow G(\neg p)) \land \neg(p U (\neg p)). \]

**Contribution.** In order to remedy the lack of comprehensive tool support for MITL in the pointwise semantics, we have recently introduced MightyL [15], an efficient tool that turns MITL formulae into a network of timed automata (expressed in the UPPAAL language) accepting the same language. These timed automata can then be used to perform satisfiability or model-checking, using off-the-shelf model checkers such as UPPAAL or LTSMin. The central point of the efficiency of our construction is its compositional feature: we output a network of timed automata (one per subformula) instead of a single, monolithic, one. In the present work, we extend this line of research to the realm of continuous semantics by revisiting the compositional translation of MITL into signal automata (i.e. automata akin to timed automata, but that accept signals instead of timed words).

More precisely, we introduce, in Section 3, a compositional translation that turns an MITL formula \(\varphi\) into a network of signal automata \(C_{init} \times \prod \chi C_{\chi}\), one for each subformula \(\chi\) in \(\varphi\), plus an extra signal automaton \(C_{init}\) (extending the ideas of our previous work [15] to the continuous setting). However, as is, this translation would not allow us to rely on the currently available tools for timed systems since most of them (and in particular, UPPAAL) rely on the pointwise semantics. So, in Section 4, we present an emptiness-preserving and compositional transformation from signal automata to timed automata (see Theorem 11). Concretely, given a signal automaton \(\mathcal{A}\) modelling a system, and a property \(\varphi\) to be checked on \(\mathcal{A}\), we can perform model-checking by: (i) building the network of signal automata \(C_{init} \times \prod \chi C_{\chi}\) from \(\neg \varphi\) using the procedure of Section 3; (ii) translating, using the techniques of Section 4, \(\mathcal{A}\), \(C_{init}\) and all \(C_{\chi}\) into corresponding timed automata \(B^{A}, B_{init}^{A}\) and \(B_{\chi}\) (for all subformulae \(\chi\)) respectively; and (iii) checking (using a model-checker for timed automata) whether the language \(B^{A} \times B_{init}^{A} \times \prod \chi B_{\chi}\) is empty. If this is the case, then the properties of our translation ensure that this emptiness holds if and only if the language of \(\mathcal{A} \times C_{init} \times \prod \chi C_{\chi}\) is empty, which holds if and only if \(\mathcal{A} \models \varphi\), by construction. We have implemented this approach as

---

1 As for MTL, for instance, which becomes decidable on finite words in the pointwise semantics [38].
an extension of MIGHTYL and report on experiments in Section 5. The preliminary results are very encouraging, as our approach compares well or outperforms previous approaches from the literature.

**Related work.** The most similar work to ours is [32] where the authors propose a compositional translation from MITL with past operators [5] to signal automata. The translation works by rewriting the input formula into one with only past operators using projections [22]. Each past subformula can then be handled by a simple component, and the resulting automaton is obtained by synchronising the components via newly introduced propositions. An advantage of this approach is that it directly supports past operators. Unfortunately, the rewriting step does not work for unbounded future operators; this severely limits the applicability of the translation (for example, the liveness property $\text{GF}p$ cannot be expressed in the bounded-future fragment). Also, as far as we know, it has never been implemented. By contrast, while our translation deals only with future MITL, one may use projections to remove past operators from the input formula.

Compositional translations that support unbounded future operators also exist in the literature [21,36,37]. One difference of these with our translation is that they are formulated in terms of non-standard models such as timed signal transducers or hierarchical timed automata. This deviation from the more common models, we believe, has contributed to the lack of implementation of these translations. Another difference is that the components constructed by these approaches are testers whereas those constructed by ours are positive testers [17,40]; that is, suppose we introduce a new proposition $p_\chi$ for the subformula $\chi = \varphi_1 \mathcal{U} \varphi_2$, a tester enforces $p_\chi \Leftrightarrow \varphi_1 \mathcal{U} \varphi_2$ to hold at all times while a positive tester only enforces the weaker formula $p_\chi \Rightarrow \varphi_1 \mathcal{U} \varphi_2$ to hold at all times. This may affect the performance of verification algorithms [43]. Moreover, the weaker condition allows us to impose some minimality criteria on transitions for further performance gains (see Section 5).

The original translation from MITL to signal automata in [4] is a monolithic tableau-based procedure which follows roughly the same lines as the tableau-based translation from LTL to Büchi automata [27]: the locations of the resulting automaton are labelled by sets of subformulae, and the transitions between them are obtained by ‘expanding’ the labels. Like our translation, it also enforces minimality when generating transitions. However, the procedure is much more involved than the LTL counterpart and seems difficult to realise in practice. A simplified tableau-based translation is given in [25,26] where an implementation—the only implementation of an MITL to signal automata translation we are aware of—is also reported. Nevertheless, the translation only works for the upper-bound fragment of MITL, and the tool is not publicly available.

Besides automata-based approaches, there are also proposals to apply SMT (Satisfiability Modulo Theories) solvers [19] to satisfiability/model-checking for MITL over signals [10,31]. The SMT approach is straightforward to implement and there are publicly available tools. However, it is essentially a ‘bounded model-checking’ approach and therefore is inherently incomplete, unless very large (impractical) bounds are used.

## 2 Model-checking signal automata against MITL

This section introduces the main objects we study—the logic MITL over signals and signal automata—as well as the model-checking problem we tackle.

---

2 These models are, however, not more expressive than signal automata.
Timed-automata-based verification of MITL over signals

Signals. An interval $I$ is a non-empty convex subset of $\mathbb{R}_{\geq 0}$. If $I$ is bounded (sup($I$) exists), we write $|I|$ for sup($I$) − inf($I$). Let AP be a finite set of atomic propositions. A state $\sigma$ over AP is a subset of AP, i.e. $\sigma \in 2^{AP}$. A signal $\gamma$ over $2^{AP}$ is a function that maps each $t \in \mathbb{R}_{\geq 0}$ to a state over AP. Throughout this work, we restrict ourselves to signals that are finitely variable, i.e. the number of discontinuities is finite in each bounded interval. We rely on timed state sequences to represent signals. Intuitively, a timed state sequence partitions the reals into a sequence of contiguous time intervals during which the state remains constant. A state sequence $I = I_0I_1I_2\cdots$ is an infinite sequence of states $\sigma_i \in 2^{AP}$. An interval sequence $\bar{I} = I_0I_1I_2\cdots$ is an infinite sequence of intervals such that: 1. for all $i \geq 0$, $I_i$ and $I_{i+1}$ are adjacent, i.e. sup($I_i$) = inf($I_{i+1}$) and $I_i \cap I_{i+1} = \emptyset$; 2. for each $t \in \mathbb{R}_{\geq 0}$, we have $t \in I_i$ for some $i \geq 0$. An interval sequence is said bipartite if it alternates between singular and open intervals, i.e. $I_i$ is singular for all even $i \geq 0$. Then, a timed state sequence over $2^{AP}$ is a pair $\kappa = (\bar{\sigma}, \bar{I})$ where $\bar{\sigma}$ is a state sequence over $2^{AP}$ and $\bar{I}$ is an interval sequence. We let $\kappa(t) = \sigma_i$ if $t \in I_i$ for some $i \geq 0$. We write $[\gamma]$ (respectively, $[\gamma]^b$) for the set of all timed state sequences (respectively, timed state sequences with bipartite interval sequences) $\kappa$ such that $\kappa(t) = \gamma(t)$ for all $t \in \mathbb{R}_{\geq 0}$.

Metric Interval Temporal Logic (MITL). We consider the satisfiability and model-checking problems for Metric Interval Temporal Logic (MITL), a real-time extension of Linear Temporal Logic (LTL), allowing temporal operators to be labelled with non-singular intervals. Formally, MITL formulae over AP are generated by the grammar:

$$\varphi ::= T \mid p \mid \varphi \land \varphi \mid \neg \varphi \mid \varphi U t \varphi,$$

where $p \in AP$ and $I$ is a non-singular interval with endpoints in $\mathbb{N}_{\geq 0} \cup \{\infty\}$ ($I$ is assumed to be $(0, \infty)$ when omitted).

In this work, we focus on the continuous semantics for MITL, in which formulae are interpreted over signals. Given a signal $\gamma$ over $2^{AP}$, $t \in \mathbb{R}_{\geq 0}$, and an MITL formula $\varphi$, the satisfaction relation $\gamma, t \models \varphi$ is defined as follows (following [4], we adopt the strict-future semantics for the temporal operators):

$$= \gamma, t \models T;$$

$$= \gamma, t \models p \text{ if } p \in \gamma(t);$$

$$= \gamma, t \models \varphi_1 \land \varphi_2 \text{ if } \gamma, t \models \varphi_1 \text{ and } \gamma, t \models \varphi_2;$$

$$= \gamma, t \models \neg \varphi \text{ if } \gamma, t \not\models \varphi;$$

$$= \gamma, t \models \varphi_1 U t \varphi_2 \text{ if there exists } t' > t \text{ such that } t' - t \in I, \gamma, t' \models \varphi_2 \text{ and } \gamma, t'' \models \varphi_1 \text{ for all } t'' \in (t, t').$$

We write $S(\varphi)$ for the set of all signals $\gamma$ such that $\gamma \models \varphi$.

We will use standard syntactic sugar, e.g. $\varphi_1 \lor \varphi_2 \equiv \neg(\neg \varphi_1 \land \neg \varphi_2)$, $\perp \equiv \neg T$, $\varphi_1 \Rightarrow \varphi_2 \equiv \neg \varphi_1 \lor \varphi_2$, the ‘eventually’ operator $F \varphi \equiv T U t \varphi$, the ‘globally’ operator $G \varphi \equiv \neg F \neg \varphi$, and the ‘release’ operator $\varphi_1 R t \varphi_2 \equiv \neg(\neg \varphi_1 U t (\neg \varphi_2))$. Hence, the semantics of the release operator can be defined as follows:

$$= \gamma, t \models \varphi_1 R t \varphi_2 \text{ if for all } t' > t \text{ such that } t' - t \in I, \gamma, t' \models \varphi_2 \text{ or there exists } t'' \in (t, t') \text{ such that } \gamma, t'' \models \varphi_1.$$
Signal automata. Our tool support for MITL will be based on automata. We first give a formal definition of signal automata, and we will also present the classical timed automata afterwards. Like [4], we equip these automata with generalised Büchi acceptance conditions.

From now on, a propositional constraint $\phi$ over $AP$ is a set of states over $AP$; that we denote by means of a Boolean formula over $AP$. For example, assuming $AP = \{p, q, r\}$, the propositional constraint $p \land \neg q$ denotes $\{\{p, r\}, \{p\}\}$. Let $X$ be a finite set of clocks. The set $\mathcal{G}(X)$ of clock constraints $g$ over $X$ is generated by the grammar $g ::= \top \mid \bot \mid g \land g \mid x \leq c$ where $\infty \in \{\leq, <, \geq, >\}$, $x \in X$ and $c \in \mathbb{N}$. A valuation $v$ of $X$ is a mapping $v : X \rightarrow \mathbb{R}_{\geq 0}$.

We denote by $0$ the valuation that maps every clock to $0$. The satisfaction of a constraint $g$ by a valuation $v$ is defined in the usual way and noted $v \models g$. For $t \in \mathbb{R}_{\geq 0}$, let $v + t$ be the valuation defined by $(v + t)(x) = v(x) + t$ for all $x \in X$. For $\lambda \subseteq X$, let $v[\lambda \leftarrow 0]$ be the valuation defined by $(v[\lambda \leftarrow 0])(x) = 0$ if $x \in \lambda$, and $(v[\lambda \leftarrow 0])(x) = v(x)$ otherwise.

Definition 1. A signal automaton (SA) over $2^{AP}$ is a tuple $A = (L, L_0, \alpha, X, \beta, \Delta, F)$ where

- $L$ is a finite set of locations;
- $L_0 \subseteq L$ is the set of initial locations;
- $\alpha$ is the location labelling function that assigns to each location $\ell \in L$ a propositional constraint $\alpha(\ell) \subseteq 2^{AP}$;
- $X$ is a finite set of clocks;
- $\beta$ is the location labelling function that assigns to each location $\ell \in L$ a clock constraint $\beta(\ell) \in \mathcal{G}(X)$;
- $\Delta \subseteq L \times 2^X \times L$ is the set of transitions where each transition consists of the source location, the clocks to be reset with this transition, and the target location;
- $F \subseteq 2^L$ is the family of sets of accepting locations.

A run $\pi$ of $A$ on a signal $\gamma$ over $2^{AP}$ is an infinite sequence of the following form:

$$\rightarrow (\ell_0, I_0) \xrightarrow{v_1} (\ell_1, I_1) \xrightarrow{v_2} (\ell_2, I_2) \xrightarrow{v_3} \ldots$$

where: 1. for all $i \geq 0$, $\ell_i$ is a locations of $A$; 2. the sequence $I_0 I_1 I_2 \cdots$ is an interval sequence; 3. for all $i \geq 0$: $\lambda_i \subseteq X$; 4. for all $i \geq 0$: $v_i$ is a valuation of $X$; and that satisfies the following:

- [Initiality] $\ell_0 \in L_0$ and $v_0 = 0$; and
- [Consequence] For all $i \geq 0$: $(\ell_i, \lambda_{i+1}, \ell_{i+1}) \in \Delta$ and $v_{i+1} = (v_i + |I_i|)[\lambda_{i+1} \leftarrow 0]$; and
- [Timing] $v_\pi(t) = \beta(\ell_\pi(t))$ for all $t \geq 0$, assuming $v_\pi(t) = v_i + (t - \sup(I_i))$ and $\ell_\pi(t) = \ell_i$ if $t \in I_i$ for some $i \geq 0$; and
- [ Adequation] $\gamma(t) \in \alpha(\ell_\pi(t))$ for all $t \geq 0$.

We say that $\pi$ is bipartite if $I_0 I_1 I_2 \cdots$ is bipartite. We say that $\pi$ is accepting if for all $F \in \mathcal{F}$: $\{i \mid \ell_i \in F\}$ is infinite. A signal $\gamma$ is accepted by $A$ if there is an accepting run of $A$ on $\gamma$.

We write $\mathcal{S}(A)$ for the set of signals accepted by $A$. For two SAs $A_1$ and $A_2$, we denote by $A_1 \times A_2$ their (asynchronous) product, defined in a manner similar to [4]: intuitively, in each location of this product, we can either fire only a transition of $A_1$ (provided that that the guard in the current location of $A_2$ is consistent with the one in destination of the transition), or only a transition of $A_2$, or fire a transition in both signal automata in case their guards need to evolve synchronously. In particular, we have $\mathcal{S}(A_1 \times A_2) = \mathcal{S}(A_1) \cap \mathcal{S}(A_2)$.

We focus on the class of bipartite SA whose runs are bipartite by construction. An SA $A = (L, L_0, \alpha, X, \beta, \Delta, F)$ is bipartite if there exists a partition of $L$ into $L^{sing}$, $L^{open}$ respecting the conditions given hereinafter. Intuitively, when reading a bipartite signal, $A$ is in a location of $L^{sing}$ ($L^{open}$) when it traverses a singular (respectively open) interval of $\gamma$:
Timed-automata-based verification of MITL over signals

We introduce hereinafter. Concretely, the outcome of our construction for an $\exists$-formula $\phi$ is a network of SA that accepts an AP-decoration of $S(\phi)$. In other words, the signals accepted by our construction are over $AP \cup AP_\phi$ and their projections on AP yields $S(\phi)$, as stated in Theorem 8 at the end of the section.

3 Note that a product of bipartite SAs is a bipartite SA.
For each (not necessarily temporal) subformula $\psi$ of $\phi$, we denote by $P_\psi$ the set of atomic propositions $p_\chi \in AP_\psi$ such that $\chi$ is a top-level temporal subformula of $\psi$, i.e. the outermost operator of $\chi$ is $U_1$ or $R_1$, yet $\chi$ does not occur under the scope of another $U_1$ or $R_1$ in $\psi$. For instance, $P_{\psi_1 \psi_2 \psi_3 (\psi_4 U \psi_5)} = \{p_{\psi_1}, p_{\psi_2}, p_{U_1 (\psi_4 U \psi_5)}\}$. For a signal $\gamma'$ over $2^P$ (where $P'$ is a set of atomic propositions) and $P \subseteq P'$, we denote by $\text{proj}_P (\gamma')$ the projection of $\gamma'$ onto $P$, i.e. the signal obtained from $\gamma'$ by hiding all the atomic propositions $p \notin P$. For a set of signals $S$ over $2^P$ and $P \subseteq P'$, we write $\text{proj}_P (S) = \{\text{proj}_P (\gamma') \mid \gamma' \in S\}$. Conversely, we say a signal $\gamma'$ over $2^P$ extends a signal $\gamma$ over $2^P$ ($P \subseteq P'$) if $\text{proj}_P (\gamma') = \gamma$.

**Formulae over $AP \cup AP_\psi$.** We define some syntactic operations on Boolean combinations over $AP \cup AP_\psi$ that will be used in the components that we describe later. Specifically, for a subformula $\varphi$ of $\psi$, we define formulae $\overline{\psi}$ (that introduces the trigger variables in subformulae), $\ast \psi$ (that ensures that we do not pull any trigger of $\psi$), $\sim \psi$ (that checks that $\psi$ does not hold, while none of its triggers are pulled), and $\hat{\psi}$ (that checks $\psi$ while triggering a minimal set of triggers).

The formula $\overline{\psi}$ is obtained from $\psi$ by replacing all top-level temporal subformulae with their corresponding triggers. Formally, $\overline{\psi}$ is defined inductively as follows (where $p \in AP$):

\[
\begin{align*}
\overline{\psi_1 \psi_2} &= \overline{\psi_1} \psi_2 \\
\overline{\psi_1 \psi_2} &= \overline{\psi_1} \psi_2
\end{align*}
\]

The formula $\ast \psi$, read as “do not pull the triggers of $\psi$”, is used to ensure that our components only follow the ‘minimal models’ of $\psi$. It is defined as the conjunction of the negations of all $p_\chi \in P_\psi$. As a concrete example,

\[
\ast((\neg p \lor \psi_4 U \psi_5) \land (q \lor \psi_3 R (\psi_4 U \psi_5))) = \neg p_{\varphi_4} U \psi_5_2 \land \neg p_{\varphi_3} R (\psi_4 U \psi_5).
\]

The formula $\sim \psi$ asserts that $\overline{\psi}$ is false and none of its triggers are pulled: $\sim \psi = \overline{\overline{\psi}} \ast \psi$.

Finally, the formula $\hat{\psi}$ is defined as $\text{mm}(\overline{\psi})$ where $\text{mm}(\phi)$ is defined inductively as follows:

\[
\begin{align*}
\text{mm}(\top) &= \top & \text{mm}(\bot) &= \bot & \text{mm}(p) &= p & \text{mm}(\neg p) &= \neg p \\
\text{mm}(\phi_1 \lor \phi_2) &= \text{mm}(\phi_1) \lor \text{mm}(\phi_2) & \text{mm}(\phi_1 \land \phi_2) &= \text{mm}(\phi_1) \land \text{mm}(\phi_2)
\end{align*}
\]

First of all, we notice that formulae $\overline{\psi}$ and $\hat{\psi}$ are equivalent, once we have projected away the propositions that are not in $AP$, in the following sense:

**Proposition 3.** For a subformula $\psi$ of $\varphi$, if $\sigma \models \overline{\psi}$ for some state $\sigma$ over $AP \cup P_\psi$, there is a state $\sigma'$ over $AP \cup P_\psi$ such that $\sigma' \models \hat{\psi}$ and $\text{proj}_{AP} (\sigma) = \text{proj}_{AP} (\sigma')$ (and vice versa).

**Proof.** By induction on the structure of $\overline{\psi}$. For the direct implication, if $\overline{\psi} = \overline{\psi_1} \lor \overline{\psi_2}$ then one of the following must hold:

- $\sigma \models \overline{\psi_1}$ and $\sigma \not\models \overline{\psi_2}$: apply the induction hypothesis on $\sigma \setminus P_{\psi_2}$ and $\overline{\psi_1}$ (note that $P_{\psi_1} \cap P_{\psi_2} = \emptyset$, and $\overline{\psi_1}$ is in negative normal form).
- $\sigma \not\models \overline{\psi_1}$ and $\sigma \models \overline{\psi_2}$: apply the induction hypothesis on $\sigma \setminus P_{\psi_2}$ and $\overline{\psi_2}$.
- $\sigma \models \overline{\psi_1}$ and $\sigma \models \overline{\psi_2}$: If $\sigma \setminus P_{\psi_2} \models \overline{\psi_2}$, apply the induction hypothesis on $\sigma \setminus P_{\psi_2}$ and $\overline{\psi_1}$. Otherwise let $\sigma' = \sigma \setminus (P_{\psi_1} \cup P_{\psi_2})$. The other cases of $\overline{\psi}$ are immediate. The other implication of the proof is simpler. 

\[\blacksquare\]
Minimality of triggers. The real impact of \( \hat{\psi} \) with respect to \( \psi \) is to ensure the minimality of triggers pulled during an execution. Indeed, we now show that if \( \varphi \) is satisfied by a signal \( \gamma \) (over \( 2^\mathcal{AP} \)), then there must be a way to extend \( \gamma \) into a signal \( \gamma' \) over \( 2^\mathcal{AP}U\mathcal{AP}_\varphi \) such that the triggers \( \mathcal{AP}_\varphi \) are only pulled when necessary in \( \gamma' \), and vice versa. This will be crucial to make our approach efficient in practice, as it reduces the behaviours of the product SA that accepts the whole formula \( \varphi \). This observation is formalised in the following two propositions.

\begin{itemize}
  \item \bf Proposition 4. \item For a signal \( \gamma \) over \( 2^\mathcal{AP} \), we have \( \gamma, 0 \models \varphi \) if and only if there exists a signal \( \gamma' \) over \( 2^\mathcal{AP}U\mathcal{AP}_\varphi \) extending \( \gamma \) such that \( \gamma', 0 \models \hat{\varphi} \), and for all \( \chi \in \mathcal{P}_\varphi \) and \( t \in \mathbb{R}_{\geq 0} \), \( \text{proj}_{\mathcal{AP}_\varphi}(\gamma') \models (\gamma') \models (p_\chi \Rightarrow \chi) \).
  \end{itemize}

\textbf{Proof.} For the direct implication, let \( \chi \) be a signal over \( 2^\mathcal{AP} \) extending \( \gamma \) such that \( p_\chi \in \zeta(t) \) if and only if \( \gamma', t \models \chi \) for each \( \chi \in \mathcal{P}_\varphi \) and \( t \in \mathbb{R}_{\geq 0} \) (note that \( \zeta \) is necessarily finitely-variable as \( \gamma \) is finitely-variable [4]). If \( \zeta, 0 \models \hat{\varphi} \), simply let \( \gamma' = \gamma \) and we are done.

If \( \zeta, 0 \not\models \hat{\varphi} \), apply Proposition 3 to \( \zeta(0) \) and \( \varphi \) to obtain a state \( \sigma \) such that \( \sigma \models \hat{\varphi} \). Finally, let \( \gamma'(0) = \sigma \) and \( \gamma'(t) = \zeta(t) \setminus \mathcal{P}_\varphi \) for all \( t \in \mathbb{R}_{\geq 0} \). The other implication is immediate. \footnote{Note that inf(\( t \)) = 0.}

\begin{itemize}
  \item \bf Proposition 5. \item For a signal \( \gamma \) over \( 2^\mathcal{AP}U\mathcal{P}_\varphi \), where either \( \chi = \psi_1 \mathcal{R}_1 \psi_2 \) or \( \chi = \psi_1 \mathcal{R}_2 \psi_2 \), we have \( \gamma, t \models (p_\chi \Rightarrow \chi) \) for all \( t \in \mathbb{R}_{\geq 0} \) if and only if there exists a signal \( \gamma' \) over \( 2^\mathcal{AP}U\mathcal{P}_\varphi \) extending \( \gamma \) such that
  \end{itemize}

By expanding \( \hat{\psi} \) and \( \hat{\varphi} \) with respect to Proposition 3, we have \( \text{proj}_{\mathcal{AP}U\mathcal{P}_\varphi}(\gamma') \models (\gamma') \models (p_\chi \Rightarrow \chi) \) for all \( t \in \mathbb{R}_{\geq 0} \).

\textbf{Proof.} Assume that \( \chi = \psi_1 \mathcal{U}_1 \psi_2 \) and let \( \zeta \) be a signal over \( 2^\mathcal{AP}U\mathcal{P}_\varphi \) extending \( \gamma \) such that \( p_\chi \in \zeta(t) \) if and only if \( \gamma, t \models \theta \) for each \( p_\chi \in \mathcal{P}_\psi_1 \cup \mathcal{P}_\psi_2 \) and \( t \in \mathbb{R}_{\geq 0} \). For each \( t \in \mathbb{R}_{\geq 0} \) such that \( \gamma, t \models p_\chi \), since \( \gamma, t \models \chi \) also holds, exactly one of the following must be true (note that inf(\( t \)) = 0):

1. there is \( t' > t \), \( t' - t \in I \) such that \( \gamma, t' \models \psi_2 \) and \( \gamma, t'' \models \psi_1 \land \neg \psi_2 \) for all \( t'' \in (t, t') \);
2. there is \( t' > t \) such that \( \gamma, t'' \models \psi_1 \land \psi_2 \) for all \( t'' \in (t, t') \);
3. there are \( t' > t \) and \( t'' > t' \) such that in \( \gamma, \psi_1 \land \neg \psi_2 \) always holds in \( (0, t'] \) and \( \psi_1 \land \psi_2 \) always holds in \( (t', t'') \).

It follows that we can obtain a ‘minimal labelling’ from \( \zeta \) via Proposition 3. More precisely, we apply Proposition 3 to constant segments of \( \zeta \) and \( \psi_1 \land \psi_2 \) or both \( \psi_1 \land \neg \psi_2 \), as required by the interpretation of \( p_\chi \) in \( \gamma \). For example, in the first case above, \( \gamma'(t') \) for each \( t'' \in (t, t') \) is obtained by applying Proposition 3 to \( \zeta(t'') \setminus \mathcal{P}_{\psi_1} \) and \( \psi_1 \); \( \gamma'(t') \) is obtained by applying Proposition 3 to \( \zeta(t') \setminus \mathcal{P}_{\psi_1} \) and \( \psi_2 \). Similar arguments can be made for \( \chi = \psi_1 \mathcal{R}_2 \psi_2 \). The other implication is simpler. \footnote{Note that inf(\( t \)) = 0.}

\textbf{Corollary 6.} For a signal \( \gamma \) over \( 2^\mathcal{AP} \), we have \( \gamma, 0 \models \varphi \) if and only if there exists a signal \( \gamma' \) over \( 2^\mathcal{AP}U\mathcal{P}_\varphi \) extending \( \gamma \) such that \( \gamma', 0 \models \hat{\varphi} \), and for all \( \chi \in \Phi \) and \( t \in \mathbb{R}_{\geq 0} \), \( \gamma', t \models p_\chi \Rightarrow \text{Expand}_\chi \) (where \text{Expand}_\chi \) is one of the formulae in Proposition 5).
The components. We are now ready to present the components $C_\chi$ for $\chi \in \Phi$.

The component $C_\chi$ for $\chi = \psi_1 \mathcal{U} \psi_2$ is given in Figure 1. We now explain how it has been produced. Thanks to Proposition 2, we provide a bipartite $\mathcal{SA}$ (in particular, we will read timed sequences with bipartite interval sequences only), where ‘singular’ locations are on top, and ‘open’ locations at the bottom. First, we focus on locations $\ell_0^s$ and $\ell_0^o$ that are used as long as trigger $p_\chi$ is not pulled: then, there is no need to pull any trigger of $\psi_1$ nor $\psi_2$, which is ensured via the use of formula $\ast \psi_1 \land \ast \psi_2$. Consider then the first time when trigger $p_\chi$ is pulled (by another component automaton): it is either in a singular interval in which case we jump into location $\ell_1^s$ (this creates a pending obligation, since such an ‘until’ with our strict semantics cannot be fulfilled right away in a singular interval: this means, in particular, that we do not need to pull any trigger for $\psi_1$ or $\psi_2$, thus checking $\ast \psi_1 \land \ast \psi_2$), or in an open interval in which case we jump either into location $\ell_1^o$ if $\psi_2$ does not hold (i.e. if $\sim \psi_2$ holds), or into location $\ell_2^o$ if $\psi_2$ holds (i.e. if $\psi_2$ is in the guard) which fulfils right away the new obligation (notice that, in the figure, we did not put $p_\chi$ in the guard of this location, for simplification: we will discuss this point more in detail afterwards).

When $p_\chi$ is first pulled in an open interval (which means we jump into location $\ell_1^o$ or $\ell_2^o$), by the semantics of the ‘until’ operator, $\psi_1$ must also hold in that interval. When in $\ell_1^o$, the successors are the same as in $\ell_0^o$. When in $\ell_1^s$ with a pending obligation, there are two cases for the next jump:

- either $\psi_2$ holds in the next singular interval, and then no trigger of $\psi_1$ needs to be pulled (i.e. guard $\ast \psi_1 \land \sim \psi_2$): if there are no new pulled trigger $p_\chi$, we jump into location $\ell_3^s$; otherwise, we jump into location $\ell_4^s$ where we still have a new pending obligation, but the location is still made accepting to record the fact that the previous obligation has been fulfilled.

- or $\psi_2$ does not hold, in which case $\psi_1$ should hold (i.e. guard $\psi_1 \land \sim \psi_2$): we then jump into location $\ell_2^s$ whether or not a new trigger $p_\chi$ is pulled.

When $p_\chi$ is first pulled in a singular interval (which means we jump into location $\ell_1^s$), there is no need to pull any trigger of $\psi_1$ nor $\psi_2$. Then, while in one of the ‘singular’ locations $\ell_1^s$, $\ell_2^s$ or $\ell_4^s$, with a pending obligation, in the next jump, there are two cases:

- either $\psi_2$ holds in the next open interval, in which case $\psi_1$ should still hold (because of the semantics of the ‘until’ operator): we can jump into the previously introduced location $\ell_3^o$.

- or $\psi_2$ does not hold (then, $\psi_1$ should hold anyway) and we jump either in location $\ell_1^o$ if a new trigger $p_\chi$ is pulled, or in $\ell_2^o$ if no new trigger $p_\chi$ is pulled. Location $\ell_2^o$ has the
Timed-automata-based verification of MITL over signals

Figure 2 The component $\mathcal{C}_x$ for $\psi_1 U_{(0,a)} \psi_2$. We use a Boolean variable $\text{si}$ to signify whether the oldest pending obligation has been pulled in a singular interval or not. The transitions with $\triangleright$ or $\triangleright\triangleright$ reset $x$; the ones with $\triangleright$ (resp. $\triangleright\triangleright$) set $\text{si}$ to true (resp. false). The clock constraint $g$ is defined as $(\text{si} \wedge x < a) \lor (\neg\text{si} \wedge x \leq a)$.

same successors as $\ell_1^0$ but we still need to distinguish them since $\ell_1^1$ must check that a new pending obligation is pulled.

Initially, we do not want to pull any trigger of $\psi_1$ or $\psi_2$, therefore, $\ell_0^0$ and $\ell_1^0$ are the two initial locations, depending on whether trigger $p_\chi$ is initially pulled or not. Accepting locations are the one where either there are no more pending obligations, or a pending obligation has been fulfilled while a new trigger is being pulled (location $\ell_4^1$).

Notice that, thanks to the use of $\ast \psi_1$ and $\hat{\psi}_1$ formulas, only the necessary triggers in $\mathcal{P}_\psi_1 \cup \mathcal{P}_\psi_2$ are pulled during an execution of this component. Indeed, this is not true for location $\ell_3^1$: when going from locations $\ell_0^1$ or $\ell_2^1$, to pull only minimal sets of triggers, we must make sure to go in $\ell_3^1$ only when a new trigger $p_\chi$ is pulled. This requires to split this location into two (one where $p_\chi$ holds, the other where it does not). For simplicity, we did not do it in the figure, but we apply this splitting in the next component we present.

This next component $\mathcal{C}_x$ is the one for $\chi = \psi_1 U_{(0,a)} \psi_2$ (Figure 2), that is obtained by adding a clock $x$ and suitable clock constraints. Intuitively, it suffices to use only one clock because for $I = (0,a)$, all new obligations are implied by the oldest pending obligation. This means that the clock should be reset when entering in a location where a trigger is pulled while all the previous obligations have been fulfilled: this is a priori the case when entering in locations $\ell_1^1$, $\ell_2^1$, and $\ell_3^1$ from locations $\{\ell_0^0, \ell_3^0, \ell_0^1, \ell_3^1\}$. Now, the valuation of $x$ would fix a deadline for the satisfaction of $\psi_2$. Indeed, as long as $\psi_2$ does not hold, we must check that $x < a$. When $\psi_2$ is next fulfilled, we also check that $x < a$. However, this is not correct for two reasons.

First, when checking the requirements $x < a$, this is not correct if the oldest pending obligations appeared in an open interval: indeed, it is still correct to fulfil $\psi_2$ in a singular interval where $x = a$. This requires that we register, when resetting clock $x$, if the trigger is pulled in a singular interval or not. To ease the presentation, we use a Boolean variable $\text{si}$ to record that the trigger has been pulled in a singular interval. Pictorially, we use transitions with $\triangleright$ heads to reset the clock $x$ and setting $\text{si}$ to true, while transitions with $\triangleright\triangleright$ heads reset clock $x$ and set $\text{si}$ to false. Then, the clock constraint that must be checked in singular interval (whether or not $\psi_2$ is currently fulfilled) is not $x < a$ but $g$ defined by $(\text{si} \wedge x < a) \lor (\neg\text{si} \wedge x \leq a)$: in particular, the guard $g$ in location $\ell_2^1$ models the fact...
that if the oldest obligation has been triggered in an open interval ($α_1$ is false), it is not a contradiction to not yet fulfil $ψ_2$ at time $t = a$, but then, the only fireable transitions are the one towards $ℓ_t^2$ and $ℓ_0^3$ where $ψ_2$ then holds. This also explains why guard $g$ does not need to be checked when entering in $ℓ_t^2$ and $ℓ_0^3$.

Second, this cannot be done as such when entering location $ℓ_t^4$ since the guard $g$ must be checked before resetting clock $x$ that records the deadline of the next pending obligation. Indeed, we simply delay the reset and modification of variable $α_1$ to the next transition towards $ℓ_t^2$ or $ℓ_0^3$.

The component for $ψ_1 U_{[0,a]} ψ_2$ is similar and hence omitted. The components for ‘release’ operators follow the same pattern as the ones for ‘until’. Due to lack of place, we present them in Appendix B. Then:

▶ Proposition 7. For each $χ ∈ Φ$, the component $C_χ$ accepts exactly the signals $γ$ over $2^{AP}$ such that $γ,t ⊨ p_χ ⇒ \text{Expand}_χ$ for all $t ∈ \mathbb{R}_{≥0}$ (where $\text{Expand}_χ$ is one of the formulae in Proposition 5).

Finally, we need a simple initial component $C_{init}$ which enforces $ϕ$ at $t = 0$ and $*ϕ$ at all $t > 0$, as suggested by Proposition 5. We can now state the main theorem of this section.

▶ Theorem 8. $\text{proj}_{AP}(S(C_{init} × ∏_{χ ∈ Φ} C_χ)) = S(ϕ)$.

4 From signal automata to timed automata

In this section, we provide a new approach to check the emptiness of signal automata that can be implemented by relying on existing tools for timed automata. To this end, we explain how to encode an SA $A$ into a timed automaton $B^A$ that accepts exactly the ‘time words’ counterparts of the signals accepted by $A$. Moreover, the construction can be used in a compositional manner: if $A$ is the product of a number of component SAs, $B^A$ can be obtained as the product of the TAs that result from applying the construction to the components of $A$. As the construction is emptiness-preserving, it can serve as a bridge between the MITL-to-SA translation in the previous section and existing TA-based tools. We start by recalling formally what are timed automata.

Timed words and timed automata. A time sequence is an infinite sequence $τ = τ_0 τ_1 τ_2 \ldots$ of timestamps such that 1. $τ_0 = 0$; 2. for all $i ≥ 0$, $τ_i ≤ τ_{i+1}$; 3. for all $t ∈ \mathbb{R}_{≥0}$, there is some $i ≥ 0$ such that $τ_i > t$. A timed word $ρ = (σ, τ)$ over $2^{AP}$ is a pair of a state sequence $σ$ over $2^{AP}$ and a time sequence $τ$. Alternatively, we may see $ρ$ as an infinite sequence $(σ_0, τ_0)(σ_1, τ_1)(σ_2, τ_2) \cdots$ of events $(σ_i, τ_i)$. We now define timed automata, with generalised acceptance conditions as before (used by [27] in the untimed setting).

▶ Definition 9. A timed automaton (TA) over $2^{AP}$ is a tuple $A = (L, L_0, X, Δ, F)$ where

- $L$ is a finite set of locations;
- $L_0 ⊆ L$ is the set of initial locations;
- $X$ is a finite set of clocks;
- $Δ ⊆ L × 2^{2^X} × G(X) × 2^X × L$ is the set of transitions;
- $F ⊆ 2^L$ is the family of sets of accepting locations.

A run $π$ of $A$ on a timed word $ρ = (σ_0, τ_0)(σ_1, τ_1)(σ_2, τ_2) \cdots$ over $2^{AP}$ is an infinite sequence

$$(ℓ_0, 0) \xrightarrow{λ_1}{σ_0, 0} (ℓ_1, 1) \xrightarrow{λ_2}{σ_1, 1} (ℓ_2, 2) \xrightarrow{λ_3}{σ_2, 2} \cdots$$
Timed-automata-based verification of MITL over signals

where, for all $i \geq 0$: 1. $\ell_i$ is a locations of $A$; 2. $v_i$ is a valuation of $X$; 3. $d_i = \tau_i - \tau_{i-1}$ (assuming $\tau_{-1} = 0$) 4. $\lambda_i \subseteq X$; and that satisfies the following:

- [Initiality] $\ell_0 \in L_0$; and
- [Consecution] for all $i \geq 0$: $(\ell_i, \phi, g, \lambda_i, \ell_{i+1}) \in \Delta$ with $\sigma_i \in \phi$ and $v_i + d_i \models g$; and
- [Timing] for all $i \geq 0$, $v_{i+1} = (v_i + d_i)\lambda_{i+1} \leftarrow 0$.

We say that $\pi$ is accepting if for all accepting sets $F \subseteq \Delta$, the set $\{i \mid \ell_i \in F\}$ is infinite. A timed word $\rho$ is accepted by $A$ if there is an accepting run of $A$ on $\rho$. We write $\mathcal{L}(A)$ for the set of timed words accepted by $A$. For two TAs $A_1$ and $A_2$, we denote by $A_1 \times A_2$ their (synchronous) product [3]. In particular, we have $\mathcal{L}(A_1 \times A_2) = \mathcal{L}(A_1) \cap \mathcal{L}(A_2)$.

Translation from SA to TA. We first explain how we map signals to timed words. To do so, we select a bipartite state sequence $\kappa$ corresponding to $\gamma$, and we express the state changes along $\kappa$ in a timed word. Formally, for a signal $\gamma$ and a timed state sequence $\kappa = (\sigma_0, I_0)(\sigma_1, I_1) \cdots$ s.t. $\kappa \in [\gamma]^{bp}$ (i.e., $I_1$ is singular for all even $i \geq 0$), we define:

$$[\kappa]_{tw} = (\sigma_0, \text{sup}(I_0))(\sigma_1, \text{inf}(I_1))(\sigma_2, \text{sup}(I_2))(\sigma_3, \text{inf}(I_3)) \cdots$$

Note that we represent a state change at time $t$ by two events with timestamp $t$ (note that $\text{sup}(I_i) = \text{inf}(I_{i+1})$ for each even $i \geq 0$). Abusing notations, we write $[\gamma]_{tw} = \{[\kappa]_{tw} \mid \kappa \in [\gamma]^{bp}\}$ and $\{S\}_{tw} = \bigcup_{\gamma \in S} [\gamma]_{tw}$ for a set $S$ of signals.

**Proposition 10.** Given a (bipartite) SA $A$, we can construct a TA $B^A$ such that $\mathcal{L}(B^A) = [\mathcal{S}(A)]_{tw}$. In particular, if $A = A_1 \times \cdots \times A_n$, then $\mathcal{L}(B^{A_1} \times \cdots \times B^{A_n}) = [\mathcal{S}(A)]_{tw}$.

**Proof (sketch).** For a clock constraint $g \in G(X)$, let $g^{-}$ be the clock constraint obtained from $g$ by replacing all the variables of the form ‘$x < c$’ with ‘$x > c$’ and all ‘$x \leq c$’ with ‘$x \geq c$’. Likewise, let $g^{+}$ be the clock constraint obtained from $g$ by replacing all ‘$x < c$’ with ‘$x \leq c$’ and all ‘$x > c$’ with ‘$x \geq c$’. The following statements hold (for a valuation $v$ of $X$):

- $v \models g^-$ if and only if for some $\delta \in \mathbb{R}_{>0}$, we have $v + t \models g$ for all $t \in (0, \delta]$.
- $v \models g^+$ if and only if for some $\delta \in \mathbb{R}_{>0}$, we have $v' \models g$ for all valuations $v'$ of $X$ such that $v' + t = v$ for some $t \in (0, \delta]$.

In what follows, we write $g[\lambda \leftarrow 0]$ for the clock constraint obtained from $g$ by replacing all occurrences of clocks $x \in \lambda$ with 0. For $A = (I, L_0, \alpha, X, \beta, \Delta, F)$ (which by assumption is bipartite and $L = L^{sing} \cup L^{open}$), define $B = (L^A, L^{open}_0, X^A, \Delta^A, F^A)$ where

- $L^A = \{\ell^{sing} \mid \ell \in L^{sing}\} \cup \{\ell^{open}, \ell^{open} \mid \ell \in L^{open}\} \cup \{\ell^{init}\}$;
- $L^{open} = \{\ell^{init}\}$;
- $X^A = X \cup \{y\}$ where $y$ is a fresh clock;
- $\Delta^A = \{\ell^{init}, \beta(\ell) \wedge y = 0, \ell^{sing} \mid \ell \in L_0\}$
  \quad \cup \{\ell^{sing}, \alpha(\ell), \beta(\ell) \wedge y = 0, \ell^{open} \mid (\ell_1, \ell_2) \in \Delta\}$
  \quad \cup \{\ell^{open}, \alpha(\ell), \beta(\ell) \wedge y = 0, \ell^{open}\} \mid (\ell_1, \ell_2) \in \Delta\}$
  \quad \cup \{\ell^{sing}, \alpha(\ell), \beta(\ell) \wedge y = 0, \ell^{open}\} \mid (\ell_1, \ell_2) \in \Delta\}$
  \quad \cup \{\ell^{open}, \alpha(\ell), \beta(\ell) \wedge y = 0, \ell^{open}\} \mid (\ell_1, \ell_2) \in \Delta\}$
  \quad \cup \{\ell^{open}, \alpha(\ell), \beta(\ell) \wedge y = 0, \ell^{open}\} \mid (\ell_1, \ell_2) \in \Delta\}$
- $F^A = \{\ell \in L^{sing} \cap F \cup \{\ell \in L^{open} \cap F \mid F \in F\}$.

Intuitively, the ‘dotted’ locations $\ell^{open}$ are used to allow interleaving and stuttering as $A$ stays in $L^{open}$: this is crucial to make the asynchronous product $A_1 \times \cdots \times A_n$ and the synchronous product $B^{A_1} \times \cdots \times B^{A_n}$ match. Finally, for pragmatic reasons, we make
suitable modifications to $B$ to obtain a strongly non-Zeno $TA B^A$ (i.e. a $TA$ in which time progresses), as in [23].

The proposition above works for any (bipartite) $SA$. For $C_{in}$ or each component $C_\chi$ ($\chi \in \Phi$) in the previous section, however, we can suppress all the ‘dotted’ locations $\hat{\ell}^{sing}, \hat{\ell}^{open}$ and build a much simpler $TA$ (which we denote by $B_{in}$ or $B_\chi$, respectively). Our main result can then be stated as the following theorem, where the projection operator $proj$ is defined in a similar way as in the setting of signals.

\textbf{Theorem 11.} $\text{proj}_{AP} \left( \mathcal{L}(B^A \times B_{in} \times \prod_{\chi \in \Phi} B_\chi) \right) = \text{proj}_{AP} \left( \left[ S(A \times C_{in} \times \prod_{\chi \in \Phi} C_\chi) \right]_{tw} \right)$

for any given $SA A$ over $2^{AP \cup AP^e}$ whose propositional constraints can be written as Boolean combinations over $AP$ (i.e. do not involve atomic propositions in $AP^e$).

As an example, the component $TA B_\chi$ for $\chi = \psi_1 U_{(0,a)} \psi_2$ (in which we use a new atomic proposition $p_{sing}$ that holds on ‘singular’ transitions) is depicted in Figure 3.

5 Implementation and experiments

We have implemented the translation as an extension of our tool MIGHTYL [15]. Given a formula $\varphi$ over $AP$ in MITL, the tool generates the model $TA B^A$ where $A$ is a universal $SA$ over $2^{AP \cup AP^e}$, the initial component $TA B_{in}$, and the corresponding component $TA B_\chi$ for each temporal subformula $\chi$ of $\varphi$ in the UPPAAL XML format. The user can, of course, replace $B^A$ with the model $TA M$ of their choice and perform model-checking with existing $TA$-based tools. Our implementation is publicly available and can be executed directly on the webpage: http://www.uleb.ac.be/di/verif/mightyl. In the following experiments, we use LTSMin [30] (with OPAAL [34], which enables support for UPPAAL XML files) as the back-end model checker and report its execution times (using only a single core) on a Pentium B970 (2.3GHz) machine with 6GB RAM running Ubuntu 17.04. We omit the execution times for MIGHTYL as it is less than 0.1s on all our benchmarks.

\textsuperscript{4} The product of these $TAs$ corresponds to the synchronous product (in which interleaving and stuttering are disallowed [8]) of $C_{in}$ and $C_\chi$ for all $\chi \in \Phi$.

\textsuperscript{5} More precisely, our tool accepts all temporal operators that are labelled with intervals of the form $(0, \infty), [0, \infty), (0, a), [0, a), (0, a] or [0, a]$. If $0$ is included in the interval, the temporal operator is given a weak-future interpretation [99], e.g. $\psi_1 U_{(0,a)} \psi_2 \iff \psi_2 \lor (\psi_1 \land U_{(0,a)} \psi_2)$. Remember that general MITL formulae can be rewriten into formulae of this fragment, e.g., $F_{(0,\infty)} \psi \iff G_{[0,\infty]} F \psi$.

\textsuperscript{6} We require $M$ to be strongly non-Zeno and $\mathcal{L}(M) = [S(A)]_{tw}$ where $A$ is an $SA$ over $2^{AP \cup AP^e}$ that satisfies the conditions in Theorem 11.
Satisfiability of parametric formulae. We consider the satisfiability of a set of parametric MITL formulae modified from [14,24]. The goal of this benchmark set is to give a rough comparison between the performance of our approach in the pointwise semantics (the original aim of MIGHTYL; we refer the reader to [15,39] for more details) with that in the continuous semantics (this article). For $k \geq 2$ and an interval $I$, let:

\[
F(k, I) = \bigwedge_{i=1}^{k} F^I_{p_i}, \quad G(k, I) = \bigwedge_{i=1}^{k} G^I_{p_i},
\]

\[
U(k, I) = (\ldots (p_1 U^I_{p_1} p_2) U^I_{p_2} \ldots) U^I_{p_k},
\]

\[
R(k, I) = (\ldots (p_1 R^I_{p_1} p_2) R^I_{p_2} \ldots) R^I_{p_k},
\]

where $F^I_{p_i}$, $G^I_{p_i}$, etc., are weak-future temporal operators [39]. The formulae in the benchmark set are given in Table 1. For the pointwise case, the actual formulae that we pass to MIGHTYL; for the continuous case, standard rewriting rules are applied to handle the lower-bound temporal operators (e.g. $F_{(5, \infty)} \equiv G_{(0,5)} F_P$). From the execution times in Table 1, it is evident that OPAAL and g++ are not performance bottlenecks. For smaller formulae, the times taken by LTSMIN are very short. For larger formulae, however, as LTSMIN uses depth-first search for OPAAL-generated models, it sometimes goes very deep into the state space and results in out-of-memory.

Validity and redundancy of specifications. We say an MITL formula $\varphi$ is valid if $\neg \varphi$ is not satisfiable. If $\varphi$ is of the form $\bigwedge_{i=1}^{k} \varphi_i$, we say that the conjunct $\varphi_i$ is redundant in $\varphi$ if the formula $(\bigwedge_{i=1}^{k} \varphi_i) \Rightarrow \varphi_i$ is valid. In [20], MITL specifications created by non-expert users are checked for satisfiability, validity, and redundancy. We report the execution times of our approach on some of their checks in Table 2. To see the effect of forcing minimal triggers, we also give the execution times when this is not imposed. We also reproduce the execution times reported in [20] in the table; since we do not impose a priori bounds on state changes (as opposed to [20]) and we use a much less powerful CPU, these numbers are not meant for direct comparison but rather for reference.

7 Of course, the resulting formulae are interpreted over signals, in contrast to their pointwise counterparts; but we expect the computational efforts needed to check their satisfiability to be similar.
Our approach

### Table 2 Execution times for the satisfiability, validity and redundancy checks in [20].

<table>
<thead>
<tr>
<th>Formula</th>
<th>Our approach</th>
<th>Our approach w/o minimality</th>
<th>[20]</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \phi_1 = F_{[0,10]}(p_1) \land F_{[0,20]}(p_1) )</td>
<td>5.95s</td>
<td>8.67s</td>
<td>14s</td>
</tr>
<tr>
<td>( \phi_2 = F_{[1,10]}(p_1 \Rightarrow G_{[0,20]}(p_2)) )</td>
<td>3.05s</td>
<td>5.3s</td>
<td>7s</td>
</tr>
<tr>
<td>( \phi_3 = G_{[0,10]}(p_1) \land G_{[0,10]} F_{[0,10]}(p_1) )</td>
<td>7.23s</td>
<td>52.43s</td>
<td>29s</td>
</tr>
<tr>
<td>( \phi_4 = F_{[0,40]}(p_1 \lor p_2) \land F_{[0,40]} F_{[0,30]}(p_1) )</td>
<td>12.12s</td>
<td>( &gt;1200s )</td>
<td>126s</td>
</tr>
</tbody>
</table>

### Table 3 Execution times for the verification tasks in [10].

<table>
<thead>
<tr>
<th>Task</th>
<th>Our approach</th>
<th>Our approach w/o minimality</th>
<th>[10]</th>
</tr>
</thead>
<tbody>
<tr>
<td>( S(A_{lamp}) = \emptyset )</td>
<td>1.15s</td>
<td>-</td>
<td>4.24s</td>
</tr>
<tr>
<td>( S(A_{lamp} \times A_{way}) = \emptyset )</td>
<td>1.79s</td>
<td>1.59s</td>
<td>17.2s</td>
</tr>
<tr>
<td>( S(A_{lamp} \times A_{way}) = \emptyset )</td>
<td>2.53s</td>
<td>196s</td>
<td>257.1s</td>
</tr>
</tbody>
</table>

---

**Model-checking a timed lamp.** We consider a case study of a timed lamp from [10]. The lamp is controlled by two buttons ‘on’ and ‘off’, which can only be pressed instantaneously but not simultaneously. The buttons turn the lamp on and off as expected, and the lamp turns off automatically 5 time units after the last time ‘on’ was pressed. In [10], the system is given as an MITL formula (with past temporal operators) over atomic propositions \( \{ \ell, on, off \} \). While we can make use of projections to remove the past temporal operators [28, 44], it turned out that the resulting formula is too large. For this reason, we model the system directly as an SA \( A_{lamp} \) (Figure 4). Then, via Proposition 10 and Theorem 11, we perform the same verification tasks as [10]: 1. checking the emptiness of \( A_{lamp} \); 2. model-checking \( A_{lamp} \) against \( \varphi_1 = G_{[0,\infty]}(F_{[0,5]}(\neg \ell)) \), i.e. the lamp never stays lit for more than 5 time units; 3. model-checking \( A_{lamp} \) against \( \varphi_2 = F_{[0,\infty]}(G_{[0,5]}(F_{[0,5]} on) \Rightarrow F_{[0,\infty]} (on \land F_{[0,5]} on)) \), i.e. if at some point the light stays on for more than 5 time units, then there is an instant when ‘on’ is pressed, and then it is pressed again before 5 time units. The execution times (with and without minimality criteria) are given in Table 3, where we also reproduce the execution times reported in [10]. Again, these numbers are not meant to be compared directly.

---

**Conclusion and future work**

We proposed a translation from MITL to signal automata based on the same principles as our previous work in the pointwise setting [15]. The main advantages of this translation over the existing ones are that it is compositional and integrates easily with existing tools. To the best of our knowledge, this is the first practical automata-based approach to MITL model-checking over signals. We plan to add to MIGHTYL support for general MITL operators (either via rewriting or directly by components) and other temporal operators (such as those from ECL [28]). On the theoretical side, a possible future direction is to investigate whether the translation can be generalised (possibly with the techniques in [18] or [42]) to deal with signals that are not necessarily finitely-variable.

---

**Figure 4** The SA \( A_{lamp} \). The transitions with solid tips reset clock \( x \).
Timed-automata-based verification of MITL over signals

References


Timed-automata-based verification of MITL over signals


A Making signal automata bipartite

Proof of Proposition 2. For $A = (L, L_0, \alpha, X, \beta, \Delta, \mathcal{F})$, define $A^{bp} = (L^{bp}, L_0^{bp}, \alpha^{bp}, X^{bp}, \beta^{bp}, \Delta^{bp}, \mathcal{F}^{bp})$ where

- $L^{bp} = \{ \ell^s, \ell^e, \ell^o \mid \ell \in L \}$;
- $L_0^{bp} = \{ \ell^s \mid \ell \in L_0 \}$;
- $\alpha^{bp}(\ell^s) = \alpha^{bp}(\ell^e) = \alpha^{bp}(\ell^o) = \alpha(\ell)$ for every $\ell \in L$;
- $X^{bp} = X \cup \{ y \}$ where $y$ is a fresh clock;
- $\beta^{bp}(\ell^s) = \beta^{bp}(\ell^e) = \beta(\ell) \land y = 0$, $\beta^{bp}(\ell^o) = \beta(\ell)$ for every $\ell \in L$;
- $\Delta^{bp} = \{ (\ell_1^s, \lambda, \ell_2^o), (\ell_1^e, \lambda, \ell_2^o), (\ell_1^o, \lambda \cup \{ y \}, \ell_2^o) \mid (\ell_1, \lambda, \ell_2) \in \Delta \}$
  \quad \cup \{ (\ell^o, y), (\ell^e, \emptyset, \ell^o) \mid \ell \in L \};
- $\mathcal{F}^{bp} = \{ \{ \ell^s, \ell^e \mid \ell \in F \} \mid F \in \mathcal{F} \}$. 

Intuitively, we create three copies $\ell^s, \ell^e, \ell^o$ of each location $\ell$ of $A$ and use the clock $y$ to enforce the desired behaviour. In particular, the ‘dotted’ locations $\hat{\ell}$ are used to deal with the situation where the ‘source’ interval is right-closed. One can verify that $A^{bp}$ is bipartite (let $L^x = \{ \ell^x, \hat{\ell}^x \mid \ell \in L \}$) and $S(A) = S(A^{bp})$. \hfill $\blacksquare$

B Signal components for the ‘release’ operators

The component $C_\chi$ for $\chi = \psi_1 \mathcal{R} \psi_2$ (Figure 5) is based on similar ideas as the component for $\psi_1 \mathcal{U} \psi_2$. In this case, an obligation can be satisfied by either $\hat{\psi}_1 \land \hat{\psi}_2$ holding in a singular interval or $\hat{\psi}_1 \land \star \psi_2$ holding in an open interval.

The component $C_\chi$ for $\chi = \psi_1 \mathcal{R}_{\{0,a\}} \psi_2$ is given in Figure 6. In this case, all old obligations are implied by the newest one. We therefore reset the clock $x$ when $p_\chi$ becomes false. The component for $\psi_1 \mathcal{R}_{\{0,a\}} \psi_2$ is similar and hence omitted.
\begin{itemize}
  \item Figure 5 The component $SA C_\chi$ for $\chi = \psi_1 \circ \psi_2$.
\end{itemize}
Timed-automata-based verification of MITL over signals

\[ \neg p \chi \land \ast \psi_1 \land \ast \psi_2 \]

\[ x = a, \neg p \chi \land \ast \psi_1 \land \ast \psi_2 \]

\[ x < a, \neg p \chi \land \ast \psi_1 \land \ast \psi_2 \]

\[ \neg p \chi \land \ast \psi_1 \land \ast \psi_2 \]

\[ x = a, p \chi \land \ast \psi_1 \land \ast \psi_2 \]

\[ x < a, p \chi \land \ast \psi_1 \land \ast \psi_2 \]

Figure 6: The component SAC, for \( \chi = \psi_1 \land R(0, a) \land \psi_2 \). The transitions with ▲ reset \( x \).