# On Characteristic Formulae for Event-Recording Automata

Omer Landry Nguena Timo, Pierre-Alain Reynier

# On Characteristic Formulae for Event-Recording Automata

Omer-Landry Nguena-Timo[1] and Pierre-Alain Reynier[2]

[1] LaBRI, Université Bordeaux I & CNRS, France
nguena@labri.fr
[2] LIF, Université Aix-Marseille & CNRS, France
pierre-alain.reynier@lif.univ-mrs.fr

**Abstract.** A standard bridge between automata theory and logic is provided by the notion of characteristic formula. This paper investigates this problem for the class of event-recording automata (ERA), a subclass of timed automata in which clocks are associated with actions and that enjoys very good closure properties (complementation, determinization...). We first study the problem of expressing characteristic formulae for ERA in Event-Recording Logic (ERL), a logic introduced by Sorea to express event-based timed specifications. We prove that the construction proposed by Sorea for ERA without invariants is false. More generally, we prove that bisimulation can not be expressed in ERL for the class of ERA, even without invariants.
Then, we introduce the logic $\mathrm{WT}_\mu$, a new logic for event-based timed specifications, closer to the timed logic $\mathcal{L}_\nu$. We prove that it is strictly more expressive than ERL, and that its model-checking problem against ERA is EXPTIME-complete. Finally, we provide constructions for characterizing ERA up to timed (bi)similarity and study the complexity issues.

## 1 Introduction

In the untimed setting, automata and logics are central tools for the formal verification of reactive systems. While the system is usually modelled as an automaton, the specification may be described both as a formula of a logic or as an automaton. In the first case the correctness of the system reduces to a model checking problem, whereas in the second case it requires to compare the two automata, and different relations can be envisaged, such as bisimulation [14] or language inclusion. A standard bridge between automata theory and logic is provided by the notion of *characteristic formula*. A characteristic formula is a formula in a temporal logic that completely characterizes the behaviour of an automaton modulo some choosen relation. For the class of timed automata [3], a solution has first been proposed in [11], providing formulae in the logic $\mathcal{L}_\nu$. Then, these results have been improved in [1], yielding linear constructions.

The subclass of Event-Recording Automata [4] (ERA) is obtained by restricting clocks to be associated with events. This class enjoys good closure properties such as determinization and complementation. It has thus attracted attention to

characterize its expressive power in terms of some timed logic [13, 8], but logics considered there are linear-time. This paper investigates the problem of constructing characteristic formulae for the class of event-recording automata, up to timed similarity and timed bisimilarity, using a branching-time logic devoted to event-based timed specifications. Such a logic, called Event-Recording Logic (ERL) and introduced by Sorea in [15], extends the mu-calculus by allowing the use of event-clocks.

After recalling standard definitions in Section 2, we first study in Section 3 the problem of expressing characteristic formula for timed bisimulation for ERA in the logic ERL. We prove that an existing attempt, which can be found in [16], is not correct. We also show that this logic can not characterize ERA up to timed bisimilarity, even when we only consider the subclass of ERA without invariants. Then, we consider in Section 4 a new timed logic, called $\mathrm{WT}_\mu$ [12], to express the characteristic formulae. The definition of this logic is closer from the definition of $\mathcal{L}_\nu$ as it separates quantifications over discrete successors and time successors. We prove that it is indeed strictly more expressive than ERL, and that its model-checking problem over ERA is EXPTIME-complete. Finally, we provide formulae constructions in $\mathrm{WT}_\mu$ for timed (bi)similarity together with complexity issues in Section 5.

## 2 Preliminaries

Let $\Sigma$ be a finite alphabet, $\Sigma^*$ is the set of finite words over $\Sigma$. The sets $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{Q}_{\geq 0}$, $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ are respectively the sets of natural, rational, non-negative rational, real and non-negative real numbers. Given a real number $x$, $\lfloor x \rfloor$ (resp. $\langle x \rangle$) denotes its integral part (resp. its fractionnal part). We consider as time domain $\mathbb{T}$ the set $\mathbb{Q}_{\geq 0}$ or the set $\mathbb{R}_{\geq 0}$. We consider a finite set $\mathcal{X}$ of variables, called *clocks*. A *clock valuation* over $\mathcal{X}$ is a mapping $v : \mathcal{X} \to \mathbb{T}$ that assigns to each clock a time value. The set of all clock valuations over $\mathcal{X}$ is denoted $\mathbb{T}^{\mathcal{X}}$. Let $t \in \mathbb{T}$, the valuation $v + t$ is defined by $(v + t)(x) = v(x) + t$, $\forall x \in \mathcal{X}$. For a clock $y \in \mathcal{X}$, we denote by $v[y := 0]$ the valuation such that for each clock $x \in \mathcal{X}$, $(v[y := 0])(x) = 0$ if $x = y$, and $(v[y := 0])(x) = v(x)$ otherwise. Finally, $\mathbf{0}$ denotes the valuation mapping every clock on 0.

In the context of event-recording automata, each clock refers to a specific action. Then, we associate clocks with letters of an alphabet. Given an alphabet $\Sigma$, we then denote by $\mathcal{X}_\Sigma$ the set of clocks $\{x_a \mid a \in \Sigma\}$. We may also write $\mathbb{T}^\Sigma$ to represent the set of clock valuations $\mathbb{T}^{\mathcal{X}_\Sigma}$.

Given a set of clocks $\mathcal{X}_\Sigma$, we introduce two sets of clock constraints over $\mathcal{X}_\Sigma$. The most general one, denoted by $\mathcal{C}(\Sigma)$, is defined by the grammar "$g ::= x \sim c \mid x - y \sim c \mid g \wedge g \mid \mathtt{tt}$" where $x, y \in \mathcal{X}_\Sigma$, $c \in \mathbb{Q}_{\geq 0}$, $\sim \in \{<, \leq, =, \geq, >\}$ and $\mathtt{tt}$ stands for true. We also use the proper subset $\mathcal{C}_{up}(\Sigma)$ of *upper bounds* constraints consisting only of conjunctions of constraints of the form $x \prec c$ with $\prec \in \{<, \leq\}$. We write $v \models g$ when the clock valuation $v$ satisfies the clock constraint $g$ and denote by $[\![g]\!]$ the set of clock valuations $v$ such that $v \models g$ holds.

### 2.1 Timed Transition Systems

Timed transition systems describe systems which combine discrete and continuous evolutions. They are used to define the behavior of timed systems such as Timed Automata [3], or Event-Clock Automata [4] (see below).

**Definition 1 (Timed Transition System (TTS)).** *A* timed transition system *over the alphabet $\Sigma$ is a transition system $\mathcal{S} = \langle Q, q_0, \Sigma, \rightarrow \rangle$, where $Q$ is the set of states, $q_0 \in Q$ is the initial state, and the transition relation $\rightarrow \subseteq Q \times (\Sigma \cup \mathbb{T}) \times Q$ consists of continuous transitions $q \xrightarrow{d} q'$ ($d \in \mathbb{T}$), and discrete transitions $q \xrightarrow{a} q'$ ($a \in \Sigma$).*

Moreover, we require the following standard properties for TTS :

- Time-Determinism : if $q \xrightarrow{d} q'$ and $q \xrightarrow{d} q''$ with $d \in \mathbb{T}$, then $q' = q''$,
- 0-Delay : $q \xrightarrow{0} q$,
- Additivity : if $q \xrightarrow{d} q'$ and $q' \xrightarrow{d'} q''$ with $d,\ d' \in \mathbb{T}$, then $q \xrightarrow{d+d'} q''$,
- Continuity : if $q \xrightarrow{d} q'$, then for every $d'$ and $d''$ in $\mathbb{T}$ such that $d = d' + d''$, there exists $q''$ such that $q \xrightarrow{d'} q'' \xrightarrow{d''} q'$.

With these properties, a *run* of $\mathcal{S}$ can be defined as a finite sequence of moves $\rho = q_0 \xrightarrow{d_0} q'_0 \xrightarrow{a_0} q_1 \xrightarrow{d_1} q'_1 \xrightarrow{a_1} q_2 \ldots \xrightarrow{a_n} q_{n+1}$ where discrete and continuous transitions alternate. To such a run corresponds the timed word $w = (a_i, \tau_i)_{0 \leq i \leq n}$ over $\Sigma$ where $\tau_i = \sum_{j=0}^{i} d_j$ is the time at which $a_i$ happens, and we say that the timed word $w$ is accepted by $\mathcal{S}$. The language of $\mathcal{S}$, denoted $\mathcal{L}(\mathcal{S})$, is defined as the set of timed words that are accepted by $\mathcal{S}$.

### 2.2 Event-Recording Automata

We consider the restriction of Event-Clock Automata to Event-Recording Automata.

**Definition 2 (Event-Recording Automata (ERA) [4]).** *An* event-recording automaton *over the alphabet $\Sigma$ is a tuple $\mathcal{A} = \langle L, \ell_0, \Sigma, T, I \rangle$ where:*

- *$L$ is a finite set of locations,*
- *$\ell_0 \in L$ is the initial location,*
- *$T \subseteq L \times \mathcal{C}(\Sigma) \times \Sigma \times L$ is a finite set of transitions,*
- *$I : L \rightarrow \mathcal{C}_{up}(\Sigma)$ associates an upper bound constraint with each location.*

*We say that an* ERA *is without invariants if the mapping $I$ associates $\mathtt{tt}$ to each location. In this case we may remove component $I$ of the definition of $\mathcal{A}$.*

Without loss of generality, we assume that the clock constraints of transitions are consistent with invariants. More formally, we have, for any $v \in \mathbb{T}^{\Sigma}$:

$$\forall (\ell, g, a, \ell') \in T, v \models g \Rightarrow (v \models I(\ell)) \wedge (v[x_a := 0] \models I(\ell'))$$

The semantics of an event-recording automaton $\mathcal{A}$ is defined in the terms of a timed transition system. Intuitively, it manipulates exactly one clock per action, which allows to measure time elapsed since the last occurrence of this action. The formal definition is given by:

**Definition 3 (Semantics of an ERA).** *Given an* ERA $\mathcal{A} = \langle L, \ell_0, \Sigma, T, I\rangle$, *its semantics is given by the* TTS $\mathcal{S}_\mathcal{A}$ *defined by* $\mathcal{S}_\mathcal{A} = \langle Q, q_0, \Sigma, \to\rangle$ *where* $Q = \{(\ell, v) \in L \times \mathbb{T}^\Sigma \mid v \models I(\ell)\}$, $q_0 = (\ell_0, \mathbf{0})$, *and* $\to$ *consists of continous and discrete transitions:* $\forall (\ell, v) \in Q$,

**Time-elapsing steps:** $\forall d \in \mathbb{T}$, *we have* $(\ell, v) \xrightarrow{d} (\ell, v + d)$ *iff* $v + d \models I(\ell)$,
**Discrete steps:** $\forall a \in \Sigma$, *we have* $(\ell, v) \xrightarrow{a} (\ell', v')$ *iff there exists a transition* $t = (\ell, g, a, \ell') \in T$ *such that* $v \models g$ *and* $v' = v[x_a := 0]$.

*Finally, we simply denote by* $\mathcal{L}(\mathcal{A})$ *the language of timed words* $\mathcal{L}(\mathcal{S}_\mathcal{A})$.

We say that an ERA is *determinisitic* whenever, for every location $\ell \in L$, letter $a \in \Sigma$ and valuation $v \in \mathbb{T}^\Sigma$, there exists *at most one* transition $(\ell, g, a, \ell') \in T$ such that $v \models g$ holds.

As it has been introduced for timed automata in [3], a time-abstract bisimulation based on the construction of regions can also be defined for ERA. We briefly recall here this construction, and refer the reader to [4] for more details.

**Definition 4 (Clock Region).** *We consider a constant* $K \in \mathbb{N}$. *A* clock region *is an equivalence class of the relation* $\simeq_K$ *over clock valuations. For two valuations* $v, v' \in \mathbb{T}^\Sigma$, *we have* $v \simeq_K v'$ *iff the following conditions hold:*

1. $\forall x \in \mathcal{X}_\Sigma$, *if* $v(x) \leq K$ *or* $v'(x) \leq K$, *then* $\lfloor v(x)\rfloor = \lfloor v'(x)\rfloor$,
2. $\forall x \in \mathcal{X}_\Sigma$ *s.t.* $v(x) \leq K$, *then* $\langle v(x)\rangle = 0 \iff \langle v'(x)\rangle = 0$,
3. $\forall x, y \in \mathcal{X}_\Sigma$ *s.t.* $|v(x) - v(y)| \leq K$, *then* $\langle v(x)\rangle \leq \langle v(y)\rangle \iff \langle v'(x)\rangle \leq \langle v'(y)\rangle$.

We let $R_K(\Sigma)$ be the set of clock regions for constant $K$. We recall that the size of $R_K(\Sigma)$ is in $2^{O(m.\log Km)}$ where $m = |\Sigma|$ (see [4]). When the constant $K$ is clear from the context, we denote by $[v]$ the clock region that contains $v$, and by $[\![r]\!]$ the set of clock valuations whose clock region is equal to $r$. To define the region automaton of an ERA $\mathcal{A}$, we can assume that all the constants occuring in its clock constaints are natural numbers (otherwise, all constants need to be multiplied by the least common multiple of the denominators of all rational numbers appearing in clock constraints).

**Definition 5 (Region Automaton).** *Given an* ERA $\mathcal{A} = \langle L, \ell_0, \Sigma, T, I\rangle$ *with integral constants. Let* $K$ *be some positive integer. We define the region automaton of* $\mathcal{A}$ *for constant* $K$, *denoted by* $\mathcal{R}_K(\mathcal{A}) = \langle R_K(\mathcal{A}), \Sigma \cup \{\tau\}, \to\rangle$, *as follows* [3]*:*

- $R_K(\mathcal{A}) = \{(\ell, r) \in L \times R_K(\Sigma) \mid \exists v \in [\![r]\!]$ *s.t.* $v \models I(\ell)\}$

[3] $\tau$ is an action not in $\Sigma$ intended to represent time elapsing.

– $(\ell, r) \xrightarrow{\tau} (\ell, r') \iff \exists \delta \in \mathbb{T}$ *s.t.* $(\ell, v) \xrightarrow{\delta} (\ell, v')$ *in* $\mathcal{S}_{\mathcal{A}}, r = [v]$ *and* $r' = [v']$
– $\forall a \in \Sigma, (\ell, r) \xrightarrow{a} (\ell, r') \iff \exists (\ell, v) \xrightarrow{a} (\ell, v')$ *in* $\mathcal{S}_{\mathcal{A}}$ *s.t.* $r = [v]$ *and* $r' = [v']$

It is well known that if $K$ is larger than the largest integer constant that appears in the clock constraints of $\mathcal{A}$, then $\mathcal{R}_K(\mathcal{A})$ is a time-abstract bisimulation of $\mathcal{S}_{\mathcal{A}}$.

### 2.3 Event-Recording Logic

**Definition 6 (Event-Recording Logic (ERL) [15]).** *Let $\Sigma$ be a finite alphabet,* Var *be a finite set of variables, the formulae of the Event-Recording Logic over $\Sigma$ and* Var *are defined by the grammar:*

$$\varphi ::= \mathtt{tt} \mid \mathtt{ff} \mid X \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid [g, a]\varphi \mid \langle g, a \rangle \varphi \mid \mu X.\varphi \mid \nu X.\varphi$$

*where $g \in \mathcal{C}(\Sigma)$, $a \in \Sigma$ and $X \in$* Var*.*

In the timed logic $\mathcal{L}_\nu$ [11], the formulae have their own clocks and the semantics is then defined using a valuation for the clocks of the formula. When defining the semantics of ERL formulae over some alphabet $\Sigma$, the clock constraints range over event clocks associated with $\Sigma$. Then, the semantics is defined for TTS corresponding to ERA over the same alphabet $\Sigma$, and the clock constraints are evaluated over the valuation of the ERA. Moreover, variables of ERL formulae are dealt with using assignment functions. Formally, an assignment function of variables Var over the set $Q$ is a function $\mathcal{V} : \mathsf{Var} \to \mathcal{P}(Q)$. The updating notation $\mathcal{V}[X := Q']$ denotes the assignment $\mathcal{V}'$ that agrees with $\mathcal{V}$ on all variables except $X$, where $\mathcal{V}'(X) = Q' \subseteq Q$.

**Definition 7 (Semantics of ERL).** *Let $\Sigma$ be a finite alphabet,* Var *be a finite set of variables, $\mathcal{A} = \langle L, \ell_0, \Sigma, T, I \rangle$ be an* ERA [4] *over $\Sigma$ and $\mathcal{S}_{\mathcal{A}} = \langle Q, q_0, \Sigma, \to \rangle$ be its associated* TTS*. Consider a formula $\varphi \in$ ERL over $\Sigma$ and* Var *and an assignment function $\mathcal{V}$ of* Var *over $Q$. The semantics of $\varphi$ for $\mathcal{A}$ under $\mathcal{V}$, denoted $[\![\varphi]\!]^{\mathcal{A}}_{\mathcal{V}}$, is given by the set of states $(\ell, v) \in Q$ for which the formula holds, and is defined inductively as follows:*

$$\begin{aligned}
[\![\mathtt{tt}]\!]^{\mathcal{A}}_{\mathcal{V}} &:= Q \\
[\![\mathtt{ff}]\!]^{\mathcal{A}}_{\mathcal{V}} &:= \emptyset \\
[\![X]\!]^{\mathcal{A}}_{\mathcal{V}} &:= \mathcal{V}(X) \\
[\![\varphi_1 \wedge \varphi_2]\!]^{\mathcal{A}}_{\mathcal{V}} &:= [\![\varphi_1]\!]^{\mathcal{A}}_{\mathcal{V}} \cap [\![\varphi_2]\!]^{\mathcal{A}}_{\mathcal{V}} \\
[\![\varphi_1 \vee \varphi_2]\!]^{\mathcal{A}}_{\mathcal{V}} &:= [\![\varphi_1]\!]^{\mathcal{A}}_{\mathcal{V}} \cup [\![\varphi_2]\!]^{\mathcal{A}}_{\mathcal{V}} \\
[\![[g, a]\varphi]\!]^{\mathcal{A}}_{\mathcal{V}} &:= \{(\ell, v) \in Q \mid \forall \delta \in \mathbb{T}, \forall (\ell, g', a, \ell') \in T, v + \delta \models g \wedge g' \Rightarrow \\
&\qquad (\ell', v') \in [\![\varphi]\!]^{\mathcal{A}}_{\mathcal{V}}, \text{ where } v' = (v + \delta)[x_a := 0]\} \\
[\![\langle g, a\rangle\varphi]\!]^{\mathcal{A}}_{\mathcal{V}} &:= \{(\ell, v) \in Q \mid \exists \delta \in \mathbb{T}, \exists (\ell, g', a, \ell') \in T \text{ s.t. } v + \delta \models g \wedge g' \text{ and} \\
&\qquad (\ell', v') \in [\![\varphi]\!]^{\mathcal{A}}_{\mathcal{V}}, \text{ where } v' = (v + \delta)[x_a := 0]\} \\
[\![\mu X.\varphi]\!]^{\mathcal{A}}_{\mathcal{V}} &:= \cap \{Q' \subseteq Q \mid [\![\varphi]\!]^{\mathcal{A}}_{\mathcal{V}[X:=Q']} \subseteq Q'\} \\
[\![\nu X.\varphi]\!]^{\mathcal{A}}_{\mathcal{V}} &:= \cup \{Q' \subseteq Q \mid Q' \subseteq [\![\varphi]\!]^{\mathcal{A}}_{\mathcal{V}[X:=Q']}\}
\end{aligned}$$

[4] Note that we extend the definition of [15] to ERA with invariants.

Using standard definitions, we say that a variable $X$ is *bounded* (resp. *free*) in a formula $\varphi$ whenever it is (resp. it is not) under the scope of a fix-point operator $\mu$ or $\nu$. It is easy to verify that if all variables are bounded in a formula $\varphi$ (we say that $\varphi$ is a *sentence*), then the semantics of $\varphi$ does not depend on the assignment function. In this case, we omit the subscript $\mathcal{V}$, and given an ERA $\mathcal{A}$, and a configuration $q$ of $\mathcal{A}$, for a sentence $\varphi$, we write $\mathcal{A}, q \models \varphi$ whenever we have $q \in [\![\varphi]\!]^{\mathcal{A}}$. We also use the shortcut $\mathcal{A} \models \varphi$ whenever $\mathcal{A}, q_0^{\mathcal{A}} \models \varphi$. Moreover, we say that a bounded variable $X$ is *guarded* if it is in the scope of an operator $\langle\cdot\rangle$ or $[\cdot]$. According to [15], one can assume that every bounded variable is guarded.

*Remark 1 (On greatest fixpoints).* To express characteristic formulae, we shall see later that we need greatest fixpoints on systems of inequations. In this case, we will use a slightly different presentation. Given a finit set $\mathsf{Var}$ of variables, we will associate to each variable $X$ a formula $\mathcal{D}(X)$ over the variables $\mathsf{Var}$. $\mathcal{D}$ is then called a declaration, and the semantics associated with this definition is the largest solution of the system of inequations $X \subseteq \mathcal{D}(X)$ for any $X \in \mathsf{Var}$. It can be proven (see [5] or [7]) that this presentation is equivalent. To specify the declaration used, we will add it as subscript of the satisfaction relation $\models$, writing $\mathcal{A}, q \models_{\mathcal{D}} X$.

### 2.4 Timed Behavioral Relations

We now recall the standard definitions of timed simulation and timed bisimulation. These definitions are given for TTS and can thus be used for ERA.

**Definition 8 (Timed simulation and timed bisimulation).** *Consider two* TTS $\mathcal{S}_1 = \langle Q_1, q_0^1, \Sigma, \rightarrow_1 \rangle$ *and* $\mathcal{S}_2 = \langle Q_2, q_0^2, \Sigma, \rightarrow_2 \rangle$. *A* timed simulation between $\mathcal{S}_1$ and $\mathcal{S}_2$ *is a relation* $\mathcal{R} \subseteq Q_1 \times Q_2$ *such that whenever* $q_1 \mathcal{R} q_2$ *and* $\alpha \in \Sigma \cup \mathbb{T}$*, then:*

- *If* $q_1 \xrightarrow{\alpha} q_1'$ *then there exists* $q_2' \in Q_2$ *such that* $q_2 \xrightarrow{\alpha} q_2'$ *and* $q_1' \mathcal{R} q_2'$.

*A relation* $\mathcal{R}$ *is a* timed bisimulation between $\mathcal{S}_1$ and $\mathcal{S}_2$ *iff the relations* $\mathcal{R}$ *and* $\mathcal{R}^{-1}$ *are timed simulations.*

For states $q_1, q_2$, we write $q_1 \prec q_2$ (resp. $q_1 \sim q_2$) if and only if there exists a timed simulation (resp. a timed bisimulation) $\mathcal{R}$ with $q_1 \mathcal{R} q_2$.

Finally, we say that *a* TTS $\mathcal{S}_2$ *simulates a* TTS $\mathcal{S}_1$ (resp. $\mathcal{S}_1$ *and* $\mathcal{S}_2$ *are bisimilar*) whenever there exists a timed simulation (resp. a timed bisimulation) between $\mathcal{S}_1$ and $\mathcal{S}_2$ such that the pair $(q_0^1, q_0^2)$ of their initial states belongs to the relation $\mathcal{R}$, and then we write $\mathcal{S}_1 \prec \mathcal{S}_2$ (resp. $\mathcal{S}_1 \sim \mathcal{S}_2$). We naturally extend these notations to ERA.

**Definition 9 (Characteristic formulae).** *Let* $\mathcal{A}$ *be an* ERA. *We say that a sentence* $\varphi \in$ ERL *is a characteristic formula for* $\mathcal{A}$ *if and only if, according to the behavioural relation considered, the following equivalence holds:*

**Simulation:** $\quad \forall \mathcal{B} \in \text{ERA}, \mathcal{A} \prec \mathcal{B} \iff \mathcal{B} \models \varphi$

**Bisimulation:** $\forall \mathcal{B} \in \mathrm{ERA}, \mathcal{A} \sim \mathcal{B} \iff \mathcal{B} \models \varphi$

The following standard result relates simulation with language inclusion.

**Proposition 1.** *Let $\mathcal{A}_1$ and $\mathcal{B}_2$ be two* ERA*, we have the following implications:*

*(i) if $\mathcal{A}_1 \prec \mathcal{A}_2$, then $\mathcal{L}(\mathcal{A}_1) \subseteq \mathcal{L}(\mathcal{A}_2)$,*
*(ii) if $\mathcal{A}_2$ is deterministic and $\mathcal{L}(\mathcal{A}_1) \subseteq \mathcal{L}(\mathcal{A}_2)$, then $\mathcal{A}_1 \prec \mathcal{A}_2$.*

## 3 On the use of ERL for characterizing bisimulation

As the logic ERL has been introduced to describe behaviours related to events, it is natural to try to write in this logic characteristic formulae for timed bisimulation for ERA. An attempt can be found in Sorea's thesis [16] for the class of ERA without invariants. We will first show in this section that this attempt is erroneous, by providing two counter-examples to illustrate how the construction fails. Then, we will prove that it is in fact not possible to express timed bisimilarity for ERA (even without invariants) in the logic ERL.

### 3.1 On the construction proposed in [16]

In [16], the author addresses the problem of constructing characteristic bisimulation formulae for ERA without invariants using ERL formulae with greatest fixpoints. We recall here the proposed construction and explain why it fails.

Before presenting the construction, we introduce some additional notations. Given an ERA without invariants $\mathcal{A} = \langle L, \ell_0, \Sigma, T \rangle$, a location $\ell \in L$ and a letter $a \in \Sigma$, we define:

- the set of $a$-labelled transitions leaving $\ell$:
  $\mathsf{Out}(\ell, a) = \{t = (\ell, g, a, \ell') \in T\}$
- the union of clock constraints of $a$-labelled transitions leaving $\ell$:
  $\mathsf{En}(\ell, a) = \bigvee \{g \mid \exists (\ell, g, a, \ell') \in \mathsf{Out}(\ell, a)\}$
- the set of locations reached by an $a$ from location $\ell$:
  $\mathsf{F}(\ell, a) = \{\ell' \mid \exists (\ell, g, a, \ell') \in \mathsf{Out}(\ell, a)\}$

The formulae defined in [16] are constructed as follows. One considers a variable $\Phi^{\mathcal{A}}(\ell)$ for each location $\ell \in L$, and then the greatest solution of the system associated with the declaration $\mathcal{D}$ defined by:

$$\Phi^{\mathcal{A}}(\ell) \stackrel{\mathcal{D}}{=} \bigwedge_{a \in \Sigma} \begin{pmatrix} \bigwedge_{(\ell,g,a,\ell') \in \mathsf{Out}(\ell,a)} \langle g, a \rangle \Phi^{\mathcal{A}}(\ell') \\ \wedge [\mathsf{En}(\ell, a), a] \left( \bigvee_{\ell' \in \mathsf{F}(\ell,a)} \Phi^{\mathcal{A}}(\ell') \right) \\ \wedge [\neg \mathsf{En}(\ell, a), a] \mathtt{ff} \end{pmatrix} \tag{1}$$

These definitions should verify the following correctness property: for any ERA $\mathcal{B}$, one has $\mathcal{B} \models_{\mathcal{D}} \Phi^{\mathcal{A}}(\ell_0)$ if and only if $\mathcal{A} \sim \mathcal{B}$.

Note that the construction introduces as clock constraints formulae obtained by disjunctions and negations. They can be rewritten in the syntax of ERL using the property $[g_1 \vee g_2, a]\varphi \equiv [g_1, a]\varphi \wedge [g_2, a]\varphi$.

Before proving that the construction is not correct, we give some intuition on how it fails. To express bisimulation for a finite state automaton $\mathcal{A}$, the standard approach consists in building a formula $\Phi^{\mathcal{A}}(q)$ for each state $q$ of $\mathcal{A}$, and considering the greatest solution of this system. Roughly, this formula verifies that any behaviour of $\mathcal{A}$ can be performed, and conversely that any possible behaviour corresponds to some of $\mathcal{A}$. More formally, the standard formula for state $q$ looks like:

$$\Phi^{\mathcal{A}}(q) = \bigwedge_{a\in\Sigma}\left(\left(\bigwedge_{q\xrightarrow{a}q'\in\mathcal{A}}\langle a\rangle\Phi^{\mathcal{A}}(q')\right)\wedge\left([a]\bigvee_{q\xrightarrow{a}q'\in\mathcal{A}}\Phi^{\mathcal{A}}(q')\right)\right) \tag{2}$$

This is the way characteristic formulae for bisimulation are defined for instance in [11, 1]. In the construction of [16], the first conjunct corresponds to the first part of (2) while the two other conjuncts correspond to the second part of (2). But we can see that both parts are not well encoded. In the first one, notice that the constraint $\langle g, a\rangle\Phi^{\mathcal{A}}(\ell')$ implies the existence of *at least one time successor in g* that corresponds to the edge while *all time successors in g* should be able to fire this edge. In the second part, it is required that all $a$-successors occuring in $\mathsf{En}(\ell, a)$ correspond to some $a$-successor of $\ell$. But the $a$-successors of $\ell$ may have different clock constraints, and thus should not all be allowed in the whole set $\mathsf{En}(\ell, a)$. We will see in Section 5 that the first point can be solved using the richer logic $\mathrm{WT}_\mu$, and that the second point can be solved using the region construction.

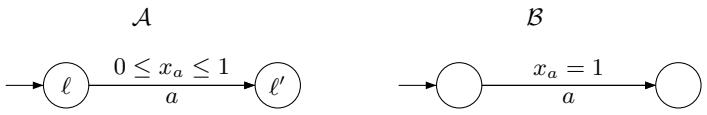


**Fig. 1.** A counter-example to [16].

We provide a counter-example exhibiting the first aspect. Consider the two ERA depicted on Figure 1. It is easy to see that $\mathcal{A}$ and $\mathcal{B}$ are not timed bisimilar. Let us write the formulae for $\mathcal{A}$ ($\Sigma = \{a\}$) according to (1):

$$\Phi^{\mathcal{A}}(\ell) = \langle 0 \le x_a \le 1, a\rangle[\mathtt{tt}, a]\mathtt{ff} \wedge [0 \le x_a \le 1, a][\mathtt{tt}, a]\mathtt{ff} \wedge [x_a > 1, a]\mathtt{ff}$$

We have $\mathcal{B} \models_{\mathcal{D}} \Phi^{\mathcal{A}}(\ell)$, what shows that the construction is not correct. More precisely, this is due to the uncompleteness of the first part of the formula of (1).

Consider the two ERA depicted on Figure 2. It is easy to verify that $\mathcal{A}$ and $\mathcal{B}$ are not timed bisimilar. However, the formulae for the ERA $\mathcal{A}$ according to (1) (with $\Sigma = \{a\}$) are:

$$\begin{aligned}
\Phi^{\mathcal{A}}(\ell_0) &= \langle 0 \le x_a \le 1, a\rangle\Phi^{\mathcal{A}}(\ell_1) \wedge \langle 1 \le x_a \le 2, a\rangle\Phi^{\mathcal{A}}(\ell_2)\\
&\quad \wedge[0 \le x_a \le 2](\Phi^{\mathcal{A}}(\ell_1) \vee \Phi^{\mathcal{A}}(\ell_2)) \wedge [x_a > 2, a]\mathtt{ff}\\
\Phi^{\mathcal{A}}(\ell_1) &= \langle x_a = 0, a\rangle\Phi^{\mathcal{A}}(\ell_3) \wedge [x_a = 0, a]\Phi^{\mathcal{A}}(\ell_3) \wedge [x_a > 0, a]\mathtt{ff}\\
\Phi^{\mathcal{A}}(\ell_2) &= [\mathtt{tt}, a]\mathtt{ff}\\
\Phi^{\mathcal{A}}(\ell_3) &= [\mathtt{tt}, a]\mathtt{ff}
\end{aligned}$$

One can verify that $\mathcal{B}, q_0^{\mathcal{B}} \models_{\mathcal{D}} \Phi^{\mathcal{A}}(\ell_0)$ and thus the construction fails. It is worth noticing here that this is due the constraint $[0 \leq x_a \leq 2](\Phi^{\mathcal{A}}(\ell_1) \vee \Phi^{\mathcal{A}}(\ell_2))$ which is not enough restrictive.

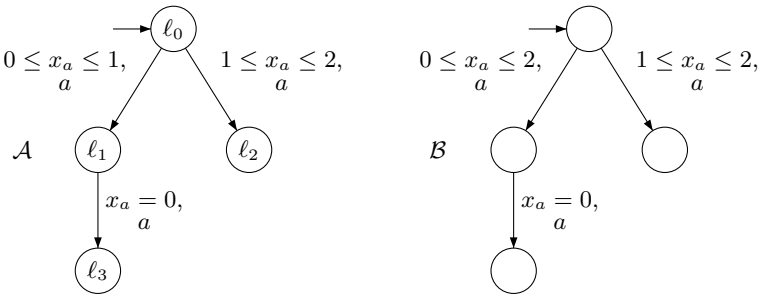


**Fig. 2.** A second counter-example to [16].

### 3.2 Impossibility Result for ERL

The construction of [16] was proposed for the class of ERA without invariants. It would be rather easy to prove that the logic ERL cannot express timed bisimilarity for ERA with invariants as this logic can not quantify over time elapsing independantly of the firing of a discrete transition. We prove here a stronger result by showing that the logic ERL can not express timed bisimulation for the restricted class of ERA without invariants. Following previous discussion, the logic ERL lacks a way to require the existence of a discrete transition for *all* the time successors satisfying some clock constraint. We will use this remark to prove the following main result:

**Theorem 1.** *The logic* ERL *can not express timed bisimilarity for* ERA*, even* without invariants*.*

*Proof.* We consider the ERA $\mathcal{A}$ depicted on Figure 1 and proceed by contradiction. We thus assume that there exists a ERL formula $\varphi$ characterizing $\mathcal{A}$ up to timed bisimilarity. To simplify the presentation, we assume that $\mathcal{A}$ is defined over the alphabet restricted to letter $a$, but the result would hold for any alphabet.

We denote by $d \in \mathbb{N}_{>0}$ the greatest denominator of constants appearing in clock constraints of $\varphi$. In the sequel, we call *granularity of* $\varphi$ the value $\frac{1}{d}$.

In a first step, we *simplify the formula* $\varphi$. By Knaster-Tarski theorem, we have the following equalities: (for any ERL formula $\Phi$, any ERA $\mathcal{B}$ and any $\mathcal{V}$)

$$[\![\mu X.\Phi(X)]\!]^{\mathcal{B}}_{\mathcal{V}} = [\![\bigvee_{i\geq 0} \Phi^i(\mathtt{ff})]\!]^{\mathcal{B}}_{\mathcal{V}}; \qquad [\![\nu X.\Phi(X)]\!]^{\mathcal{B}}_{\mathcal{V}} = [\![\bigwedge_{i\geq 0} \Phi^i(\mathtt{tt})]\!]^{\mathcal{B}}_{\mathcal{V}}$$

As mentionned before, we can assume that all variables of sentences of ERL are guarded, *i.e.* are under the scope of the operator $\langle\cdot\rangle$ or $[\cdot]$. A consequence is that

when interpreting fixpoints over structures without loops, one can limit above infinite disjunctions and conjunctions up to the maximal length of executions of the structure. For an ERA whose maximal depth [5] is 1 (such as $\mathcal{A}$ for instance), we can replace in $\varphi$ the fixpoints operators by the above equations with index $i$ ranging over the set $\{0,1,2\}$. We denote by $\mathit{Unfold}_1$ this operation, and by $\mathrm{ERA}_{d\leq 1}$ the set of ERA whose maximal depth is smaller or equal to 1. Then, we have:

$$\forall \mathcal{B} \in \mathrm{ERA}_{d\leq 1},\ \mathcal{B} \models \varphi \iff \mathcal{B} \models \mathit{Unfold}_1(\varphi) \tag{3}$$

Thus, the outermost operators of the formula $\mathit{Unfold}_1(\varphi)$ belong to the set $\{\vee, \wedge, \langle\cdot\rangle, [\cdot]\}$. We can then transform the formula $\mathit{Unfold}_1(\varphi)$ in a standard conjunctive normal form and write $\mathit{Unfold}_1(\varphi) = \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m_i} \Phi_{i,j}$ where every formula $\Phi_{i,j}$ has as outermost operator either $\langle\cdot\rangle$ or $[\cdot]$. Now, as the ERA $\mathcal{A}$ is of maximal depth 1 and is naturally timed bisimilar to itself, it satisfies this formula in its initial configuration $q_0^{\mathcal{A}}$, and thus there exists $i \in \{1,\ldots,k\}$ such that $\mathcal{A}, q_0^{\mathcal{A}} \models \Phi_{i,j}$ for any $j \in \{1,\ldots,m_i\}$. To ease the reading, we omit in the sequel the index $i$. Up to a reordering of the formulae $\Phi_j$, we can suppose that there exists an index $p$ such that a formula $\Phi_j$ has as outermost operator the operator $\langle\cdot\rangle$ if and only if $j \leq p$.

In this second part, we *define an* ERA $\mathcal{B}$ which is not not bisimilar to $\mathcal{A}$. This ERA $\mathcal{B}$ is defined over $\Sigma = \{a\}$ and contains exactly two locations, denoted respectively $\ell_1$ and $\ell_1'$, such that the first one is initial. We denote by $q_0^{\mathcal{B}} = (\ell_1, 0)$ the initial configuration of $\mathcal{B}$. In the sequel, we will define a finite set of rational numbers $\mathcal{F}$. We exactly add one edge $(\ell_1, g_f, a, \ell_1')$ for each $f \in \mathcal{F}$, with the constraint $g_f$ defined as $x_a = f$. It is easy to verify that $\mathcal{A}$ and $\mathcal{B}$ are not timed bisimilar as there necessary exists some point in the interval $[0,1]$ that does no belong to $\mathcal{F}$. We now detail how we build the set $\mathcal{F}$ to ensure that $\mathcal{B}, q_0^{\mathcal{B}} \models \varphi$. For each $j \in \{1,\ldots,p\}$, we can write $\Phi_j = \langle g_j, a\rangle \xi_j$ for some constraint $g_j$ and formula $\xi_j$. By construction, we have $\mathcal{A}, q_0^{\mathcal{A}} \models \Phi_j$, and thus there exists a delay $\delta \in \mathbb{T}$ such that the steps $q_0^{\mathcal{A}} \xrightarrow{\delta} (\ell, \delta) \xrightarrow{a} (\ell', 0)$ exist in $\mathcal{A}$ with $\mathcal{A}, (\ell', 0) \models \xi_j$. Note that independantly of the delay after which the $a$-labelled transition is fired, the configuration reached is the same. As the constraint $g_j$ is defined with granularity $\frac{1}{d} \in \mathbb{Q}_{>0}$, we can choose $\delta_j \in \mathbb{Q}_{\geq 0} \cap [0,1]$ such that $q_0^{\mathcal{A}} \xrightarrow{\delta_j} (\ell, \delta_j) \xrightarrow{a} (\ell', 0)$ with $\mathcal{A}, (\ell', 0) \models \xi_j$. Finally, the finite set of rational values $\mathcal{F}$ is defined as $\mathcal{F} = \{\delta_j \mid 1 \leq j \leq p\}$.

It remains to prove that the ERA $\mathcal{B}$ *satisfies the formula* $\varphi$. As the maximal depth of $\mathcal{B}$ is 1, and using property (3), it is sufficient to prove that for any $j$, we have $\mathcal{B}, q_0^{\mathcal{B}} \models \Phi_j$. First consider formulae $\Phi_j$ for $j > p$. In this case the formula is of the form $[g_j, a]\xi_j$. Then the property holds because any $a$-labelled transition firable from $q_0^{\mathcal{B}}$ in $\mathcal{B}$ also exists in $\mathcal{A}$, leading to identical configurations $(\ell', 0)$ and $(\ell_1', 0)$, with no actions available in $\ell'$ and $\ell_1'$. Second, we consider a formula $\Phi_j$ with $j \leq p$. In this case, the choice of the delay $\delta_j \in \mathcal{F}$ ensures that the transitions $q_0^{\mathcal{B}} \xrightarrow{\delta_j} (\ell_1, \delta_j) \xrightarrow{a} (\ell_1', 0)$ exist in $\mathcal{B}$ and as $\mathcal{A}, (\ell', 0) \models \xi_j$, we also have $\mathcal{B}, (\ell_1', 0) \models \xi_j$.

[5] The maximal depth of an ERA denotes the length of a longest untimed path.

Finally, we have proven that $\mathcal{B} \models \varphi$ holds while $\mathcal{A}$ and $\mathcal{B}$ are not timed bisimilar, thus yielding a contradiction. □

## 4 A $\mu$-calculus for Event-Recording Automata

We introduce here a new $\mu$-calculus for ERA, called $\mathrm{WT}_\mu$ [12]. This stands for *Weak Timed $\mu$-calculus*, as it can be seen as a timed $\mu$-calculus (as $\mathrm{T}_\mu$ [9] or $\mathcal{L}_\nu$ [11]) devoted to the weak class of timed systems represented by ERA. Its definition differs from ERL in that it separates delay successors and discrete successors, as it is done for instance in the logic $\mathcal{L}_\nu$. We prove in this section that it is strictly more expressive than the logic ERL and that it preserves the good model-checking properties of ERL. We will show in the next section that it allows to express timed (bi)similarity for ERA.

### 4.1 The Logic $\mathrm{WT}_\mu$

**Definition 10 (Syntax).** *Let $\Sigma$ be a finite alphabet and $\mathsf{Var}$ be a finite set of variables. A formula $\varphi$ of $\mathrm{WT}_\mu$ is generated using the following grammar:*

$$\varphi ::= \mathtt{tt} \mid \mathtt{ff} \mid X \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \langle a \rangle \varphi \mid \langle g \rangle \varphi \mid [a]\varphi \mid [g]\varphi \mid \mu X.\varphi \mid \nu X.\varphi$$

*where $g \in \mathcal{C}(\Sigma)$, $a \in \Sigma$ and $X \in \mathsf{Var}$.*

As for the logic ERL, we use auxiliary assignment functions, and the notions of free variable, bounded variable, and sentence.

**Definition 11 (Semantics).** *For a given* ERA $\mathcal{A} = \langle L, \ell_0, \Sigma, T, I \rangle$ *with associated* TTS $\mathcal{S}_\mathcal{A} = \langle Q, q_0, \Sigma, \to \rangle$*, a given formula $\varphi \in \mathrm{WT}_\mu$, and an assignment function $\mathcal{V} : \mathsf{Var} \to \mathcal{P}(Q)$, the set of states satisfying the fomula, denoted $[\![\varphi]\!]^\mathcal{A}_\mathcal{V}$, is inductively defined as follows:*

$$\begin{array}{rcl}
[\![\langle a \rangle \varphi]\!]^\mathcal{A}_\mathcal{V} & := & \{(\ell, v) \in Q \mid \exists (\ell, g, a, \ell') \in T \text{ s.t. } v \models g \text{ and} \\
 & & (\ell', v') \in [\![\varphi]\!]^\mathcal{A}_\mathcal{V}, \text{ where } v' = v[x_a := 0]\} \\
[\![\langle g \rangle \varphi]\!]^\mathcal{A}_\mathcal{V} & := & \{(\ell, v) \in Q \mid \exists \delta \in \mathbb{T} \text{ s.t. } v + \delta \models g \text{ and } (\ell, v + \delta) \in [\![\varphi]\!]^\mathcal{A}_\mathcal{V}\} \\
[\![[a] \varphi]\!]^\mathcal{A}_\mathcal{V} & := & \{(\ell, v) \in Q \mid \forall (\ell, g, a, \ell') \in T, v \models g \Rightarrow \\
 & & (\ell', v') \in [\![\varphi]\!]^\mathcal{A}_\mathcal{V}, \text{ where } v' = v[x_a := 0]\} \\
[\![[g] \varphi]\!]^\mathcal{A}_\mathcal{V} & := & \{(\ell, v) \in Q \mid \forall \delta \in \mathbb{T}, v + \delta \models g \Rightarrow (\ell, v + \delta) \in [\![\varphi]\!]^\mathcal{A}_\mathcal{V}\} \\
[\![\mu X.\varphi]\!]^\mathcal{A}_\mathcal{V} & := & \cap \{Q' \subseteq Q \mid [\![\varphi]\!]^\mathcal{A}_{\mathcal{V}[X:=Q']} \subseteq Q'\} \\
[\![\nu X.\varphi]\!]^\mathcal{A}_\mathcal{V} & := & \cup \{Q' \subseteq Q \mid Q' \subseteq [\![\varphi]\!]^\mathcal{A}_{\mathcal{V}[X:=Q']}\}
\end{array}$$

*The cases of atomic and boolean formulae are standard.*

### 4.2 Expressivity

As expected, the logic $\mathrm{WT}_\mu$ increases the expressive power of ERL. Before proving this main result, we introduce some definitions.

**Definition 12.** *Given two sentences $\varphi$ and $\varphi'$ in* $\mathrm{ERL} \cup \mathrm{WT}_\mu$*, we say that they are* equivalent *if and only if, for any* ERA $\mathcal{A}$*, we have* $[\![\varphi]\!]^{\mathcal{A}} = [\![\varphi']\!]^{\mathcal{A}}$.
*We say that a logic $\mathcal{L}_2$ is* more expressive *than a logic $\mathcal{L}_1$ if for any sentence in $\mathcal{L}_1$, there exists an equivalent sentence in $\mathcal{L}_2$.*

Then we can state the following property:

**Proposition 2.** *Given a sentence $\varphi \in \mathrm{ERL}$, we denote by $\hat{\varphi}$ the sentence of* $\mathrm{WT}_\mu$ *obtained by substituting any operator $[g, a]$ (resp. $\langle g, a\rangle$) by the two operators $[g][a]$ (resp. $\langle g\rangle\langle a\rangle$). Then $\varphi$ and $\hat{\varphi}$ are equivalent.*

*Proof.* Proceeding by induction on the length of the formula $\varphi$, the result directly follows from the definitions. □

In the sequel, we consider the ERA $\mathcal{A}_1$ reduced to a single location $\ell$ with no invariant and no transitions. We denote by $Q$ its set of configurations.

**Proposition 3.** *For any* ERL *sentence $\varphi$, we have $[\![\varphi]\!]^{\mathcal{A}_1} = \emptyset$ or $[\![\varphi]\!]^{\mathcal{A}_1} = Q$.*

*Proof.* According to [15], one can assume that the formulae of ERL are guarded, that is every bounded variable is in the scope of an operator $\langle\cdot\rangle$ or $[\cdot]$. Then, since automaton $\mathcal{A}_1$ contains no transition, we have, for any variable assignment $\mathcal{V}$, that $[\![[g, a]\varphi]\!]^{\mathcal{A}_1}_{\mathcal{V}} = Q = [\![\mathtt{tt}]\!]^{\mathcal{A}_1}_{\mathcal{V}}$ and $[\![\langle g, a\rangle\varphi]\!]^{\mathcal{A}_1}_{\mathcal{V}} = \emptyset = [\![\mathtt{ff}]\!]^{\mathcal{A}_1}_{\mathcal{V}}$. As a consequence, any ERL formula in which every variable is bounded (a sentence) is equivalent to a formula obtained by the following grammar: $\varphi ::= \mathtt{tt} \mid \mathtt{ff} \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \mu X.\varphi \mid \nu X.\varphi$. The result follows by induction on the length of the formula. □

**Theorem 2.** *The logic* $\mathrm{WT}_\mu$ *is strictly more expressive than the logic* ERL *(even for* ERA *without invariants).*

*Proof.* First, Proposition 2 exactly proves that the logic $\mathrm{WT}_\mu$ is more expressive than the logic ERL.

Second, we have to prove that the converse is false. Consider the ERA $\mathcal{A}_1$ introduced above, and note that $\mathcal{A}_1$ has no invariants. We consider the $\mathrm{WT}_\mu$ sentence $\varphi = \langle x_a = 1\rangle\mathtt{tt}$. Then a configuration $(\ell, v)$ of $\mathcal{A}_1$ satisfies sentence $\varphi$ if and only if $v(x_a) \leq 1$. On the other side, Proposition 3 shows that any ERL sentence has a trivial satisfiability set on $\mathcal{A}$. Thus, no ERL sentence is equivalent to $\varphi$, proving the result. □

### 4.3 Model-Checking

We consider the model checking problem of $\mathrm{WT}_\mu$ sentences on ERA models. This problem consists, given a $\mathrm{WT}_\mu$ sentence $\varphi$ and an ERA $\mathcal{A}$, in deciding whether the relation $\mathcal{A} \models \varphi$ holds.

**Theorem 3.** *The Model-Checking problem of* $\mathrm{WT}_\mu$ *on* ERA *is* EXPTIME*-complete, even for the fragment of* $\mathrm{WT}_\mu$ *restricted to greatest fixpoints.*

*Proof.* EXPTIME-*membership:* This easily follows from the EXPTIME-membership of the model-checking of the logic $\mathcal{L}^{+}_{\mu,\nu}$ over timed automata [2]. However, to obtain precise complexity results, we sketch here the reasonning.

We first state the following Lemma:

**Lemma 1.** *Let $\Sigma$ be a finite alphabet. Let $\mathcal{A} \in$ ERA, $\varphi \in \mathrm{WT}_\mu$ be a formula without fixpoint quantifier and $K$ denote the maximal integer constant of $\mathcal{A}$ and $\varphi$. Denote by $X_1, \ldots, X_n$ the free variables $X_1, \ldots, X_n$ of $\varphi$ and let $\mathcal{V}$ be an assignment function over these variables such that for any $i$, $\mathcal{V}(X_i)$ is a union of regions in $R_K(\mathcal{A})$. Then, the semantics $[\![\varphi]\!]^{\mathcal{A}}_{\mathcal{V}}$ is also a union of regions of $R_K(\mathcal{A})$.*

*Proof.* We proceed by induction on the length of $\varphi$ and consider the type of $\varphi$:

- $\varphi = \mathtt{tt}$ or $\varphi = \mathtt{ff}$. The result follows as $Q_{\mathcal{A}}$ and $\emptyset$ are union of regions.
- $\varphi = \varphi_1 \wedge \varphi_2$ or $\varphi = \varphi_1 \vee \varphi_2$. The result follows from the induction property as union of regions are closed under boolean operations.
- $\varphi = X_i$ for some $i \in \{1, \ldots, n\}$. Then $[\![\varphi]\!]^{\mathcal{A}}_{\mathcal{V}} = \mathcal{V}(X_i)$ and the result follows from the hypothesis on $\mathcal{V}$.
- $\varphi = \langle g \rangle \varphi'$ or $\varphi = [g]\varphi'$ with $g \in \mathcal{C}(\Sigma)$. By induction property the semantics $[\![\varphi']\!]^{\mathcal{A}}_{\mathcal{V}}$ is a union of regions. Then, the result follows from the time-abstract bisimulation property of clock regions which implies that the time predecessors of a clock region is a union of clock regions.
- $\varphi = \langle a \rangle \varphi'$ or $\varphi = [a]\varphi'$ with $a \in \Sigma$. By induction property the semantics $[\![\varphi']\!]^{\mathcal{A}}_{\mathcal{V}}$ is a union of regions. Then, the result follows from the time-abstract bisimulation property of regions which implies that the predecessors of a region by a discrete transition is a union of regions.

This concludes the proof. □

As a corollary, we get:

**Lemma 2.** *Let $\Sigma$ be a finite alphabet. Let $\mathcal{A} \in$ ERA, and $\varphi$ be a sentence in $\mathrm{WT}_\mu$. Denote by $K$ the maximal integer constant of $\mathcal{A}$ and $\varphi$. Then the semantics of $\varphi$ over $\mathcal{A}$, $[\![\varphi]\!]^{\mathcal{A}}$, is a union of regions of $R_K(\mathcal{A})$. In other terms, we have:*

$$\forall \ell \in L_{\mathcal{A}}, \forall v, v' \in \mathbb{T}^{\Sigma} \text{ s.t. } v \simeq_K v', \mathcal{A}, (\ell, v) \models \varphi \iff \mathcal{A}, (\ell, v') \models \varphi$$

*Proof.* As the semantics of formulae of $\mathrm{WT}_\mu$ leads to monotone functions, Knaster-Tarski theorem implies that fixpoint formulae can be evaluated using eventually infinite intersections and unions given by:

$$[\![\mu X.\varphi(X)]\!]^{\mathcal{A}}_{\mathcal{V}} = \bigcup_{i \geq 0} [\![\varphi^i(\mathtt{ff})]\!]^{\mathcal{A}}_{\mathcal{V}}, \qquad [\![\nu X.\varphi(X)]\!]^{\mathcal{A}}_{\mathcal{V}} = \bigcap_{i \geq 0} [\![\varphi^i(\mathtt{tt})]\!]^{\mathcal{A}}_{\mathcal{V}}$$

As $\emptyset$ and $Q$ are both union of regions, Lemma 1 entails that the iterative evaluation of fixpoints leads also to union of regions. As the number of regions if finite, these evaluations terminate, returning also a union of regions. □

The proof of Lemma 2 thus yields that the model checking problem is decidable. To obtain results on complexity issues, we reduce the model checking problem to an equivalent model checking problem for standard $\mu$-calculus. Therefore, we define the semantics of $\mathrm{WT}_\mu$ over $\mathcal{R}_K(\mathcal{A})$. The only operators for which the semantics is non standard are the following:

$$\begin{aligned}
[\![\langle g\rangle\varphi]\!]_{\mathcal{V}}^{\mathcal{R}_K(\mathcal{A})} &= \{(\ell,r)\in R_K(\mathcal{A}) \mid \exists r'\in R_K(\Sigma) \text{ s.t. } (\ell,r)\xrightarrow{\tau}(\ell,r'), [\![r']\!]\subseteq[\![g]\!] \\
&\quad \text{and } (\ell,r')\in [\![\varphi]\!]_{\mathcal{V}}^{\mathcal{R}_K(\mathcal{A})}\} \\
[\![[g]\varphi]\!]_{\mathcal{V}}^{\mathcal{R}_K(\mathcal{A})} &= \{(\ell,r)\in R_K(\mathcal{A}) \mid \forall r'\in R_K(\Sigma) \text{ s.t. } (\ell,r)\xrightarrow{\tau}(\ell,r'), \text{ if } [\![r']\!]\subseteq[\![g]\!] \\
&\quad \text{then } (\ell,r')\in [\![\varphi]\!]_{\mathcal{V}}^{\mathcal{R}_K(\mathcal{A})}\}
\end{aligned}$$

Then, we can prove the correction of this semantics as in [9, 11]:

$$\forall v\in\mathbb{T}^\Sigma, \mathcal{A}, (\ell,v)\models\varphi \iff \mathcal{R}_K(\mathcal{A}), (\ell,[v])\models\varphi$$

However, the semantics of $\mathrm{WT}_\mu$ over $\mathcal{R}_K(\mathcal{A})$ does not exactly match this of standard mu-calculus. This is due to inclusion testing between $[\![r']\!]$ and $[\![g]\!]$. To solve this problem, we can for instance introduce atomic propositions corresponding to the clocks constraints $g\in\mathcal{C}(\Sigma)$ of the fomula $\varphi$. A predicate $g$ is satisfied in a region $(\ell,r)$ if and only if the inclusion $[\![r]\!]\subseteq[\![g]\!]$ holds. Then, we can write the following equivalences:

$$\langle g\rangle\varphi\equiv\langle\tau\rangle(g\wedge\varphi); \qquad [g]\varphi\equiv[\tau](g\to\varphi)\equiv[\tau](\neg g\vee\varphi)$$

Note that the number of atomic propositions introduced for a formula $\varphi\in\mathrm{WT}_\mu$ is linear in the size of this formula. Another approach consists in enlarging the alphabet to include the clock constraints. This approach is described in [12].

Finally, we obtain the reduction desired to a model checking problem of the standard mu-calculus over the region automaton. This problem, for a mu-calculus formula $\varphi$ and a finite structure $\mathcal{S}$, can be solved in time $O((|\mathcal{S}|\times|\varphi|)^{n+1})$, where $n$ is the number of alternations of greatest and least fixpoints quantifiers in $\varphi$ [17]. As the size of $\mathcal{R}_K(\mathcal{A})$ is in $|\mathcal{A}|\times 2^{O(|\Sigma|.\log K|\Sigma|)}$, and $n$ is in $O(|\varphi|)$, we obtain that the model checking problem of $\mathrm{WT}_\mu$ over ERA is in EXPTIME, with a precise time complexity.

EXPTIME-*hardness:* We adapt the proof of [2] to encode the acceptance problem of a word $w_0$ by a Linear Bounded Alternating Turing Machine (LBATM) $\mathcal{M}$ which is EXPTIME-complete [6]. One can assume w.l.o.g that the alphabet of $\mathcal{M}$ is $\{a,b\}$, and let $n=|w_0|$. Configurations of $\mathcal{M}$ are triples $(q,w,i)$ where $i\leq n$ denotes the position of the tape head. A transition $(q,\alpha,\alpha',\delta,q')$ of $\mathcal{M}$ can be fired from $(q,w,i)$ iff $w[i]=\alpha$. Then, it writes $\alpha'$ instead, and moves left or right according to $\delta$. As $\mathcal{M}$ is alternating, $Q$ is partitioned into $Q_{or}$ and $Q_{and}$. A configuration $(q,w,i)$ with $q\in Q_{or}$ (resp. $q\in Q_{and}$) is winning iff $q=q_f$ or there exists an accepting successor configuration (resp. if all its successor configurations are accepting).
As we want to build an ERA $\mathcal{A}$ while the construction of [2] is done for timed automata, we make some modifications to control the resets of clocks. Locations

of $\mathcal{A}$ are pairs $(q, i) \in Q \times \mathbb{N}$, where $i$ denotes the position of the tape head. The value of cell $i$ of the tape is encoded by the relative values of two clocks, say $x_{a_i}$ and $x_{b_i}$. The alphabet of $\mathcal{A}$ thus contains $\Sigma = \{a_i, b_i \mid 1 \leq i \leq n\}$. We add a letter $\tau$ not in $\Sigma$. A transition $(q, \alpha, \alpha', \delta, q')$ is represented in $\mathcal{A}$ by the transitions $(q, i) \xrightarrow{g_i, \sigma_i} (q', i')$, where:

1. $g_i = x_{a_i} < x_{b_i} \wedge x_\tau = 1$ if $\alpha = a$, and $g_i = x_{a_i} > x_{b_i} \wedge x_\tau = 1$ otherwise,
2. $\sigma_i = x_{a_i}$ if $\alpha' = a$, and $\sigma_i = x_{b_i}$ otherwise,
3. $i' = i + 1$ if $\delta = R$ and $i < n$, and $i' = i - 1$ if $\delta = L$ and $i > 1$.

To force time elapsing between two transitions corresponding to moves of $\mathcal{M}$, we use letter $\tau$ and add transitions $(q, i) \xrightarrow{x_\tau = 1, \tau} (q, i)$ for any location $(q, i)$. The initialization of the clocks to represent the word $w_0$ can be done using a sequence of transitions $u_i$ interleaved by transitions labelled by $\tau$. Finally, we use the following $\mathrm{WT}_\mu$ formula, with only greatest fixpoints:

$$\varphi = [\mathtt{tt}][u_1][\tau] \ldots [\mathtt{tt}][u_n][\tau].\nu X.([\mathsf{accept}]\mathtt{ff} \wedge [\mathtt{tt}][\Sigma][\tau]\langle \mathtt{tt} \rangle \langle \Sigma \rangle \langle \tau \rangle X)$$

where $\mathsf{accept}$ denotes a special letter only firable from the final state of $\mathcal{M}$. Then one can prove that $\mathcal{M}$ accepts $w_0$ iff $\mathcal{A} \not\models \varphi$. Note that the size of $\mathcal{A}$ and $\varphi$ are polynomial in the sizes of $\mathcal{M}$ and $w_0$. □

*Remark 2.* As in [2], the hardness proof could be done without diagonal constraints.

## 5 Characteristic Formulae Constructions

We describe in this section formulae constructions in the logic $\mathrm{WT}_\mu$ to express timed similarity and timed bisimilarity for ERA with invariants. In the sequel, we consider an ERA $\mathcal{A} = \langle L_\mathcal{A}, \ell_0^\mathcal{A}, \Sigma, T_\mathcal{A}, I_\mathcal{A} \rangle$ over the alphabet $\Sigma$. Let $\ell \in L_\mathcal{A}$ and $a \in \Sigma$, we first introduce an operation, denoted $\mathsf{Split}(\ell, a)$, related to the determinization of ERA. $\mathsf{Split}(\ell, a)$ is a finite set of constraints $\{g_1, \ldots, g_n\} \subseteq \mathcal{C}(\Sigma)$ such that:

- $(i)$ it partitions the constraint $\mathsf{En}(\ell, a)$: $\bigcup_i [\![g_i]\!] = [\![\mathsf{En}(\ell, a)]\!]$ and $\forall i \neq j, [\![g_i]\!] \cap [\![g_j]\!] = \emptyset$,
- $(ii)$ its elements "match" the clock constraints of $a$-labelled transitions leaving $\ell$: $\forall i \in \{1, \ldots, n\}, \forall (\ell, g, a, \ell') \in T_\mathcal{A}, [\![g_i]\!] \subseteq [\![g]\!]$ or $[\![g_i]\!] \cap [\![g]\!] = \emptyset$.

We do not investigate here how such an operator can be defined as it is not the purpose of this work. It can for instance be defined using the region construction, and then be optimized using some merging operations on zones. It is worth noticing that in the worst case, the size of $\mathsf{Split}(\ell, a)$ may be $|\mathsf{Out}(\ell, a)| \times 2^{O(|\Sigma| \log K |\Sigma|)}$, with $K$ the largest integer constant of $\mathcal{A}$ (due to the region construction). However, if the ERA $\mathcal{A}$ is deterministic, then its size is linear in the size of $\mathsf{Out}(\ell, a)$. Indeed, the determinisim implies that the clock constraints of $a$-labelled transitions leaving $\ell$ are disjoint.

### 5.1 Characteristic Formulae for Timed Bisimilation

**Definition 13.** *We define a declaration $\mathcal{D}_{\sim\mathcal{A}}$ associating a formula to each location $\ell$ of $\mathcal{A}$, and consider the greatest solution of this system of fixpoint equations.*

$$\Phi^{\sim\mathcal{A}}(\ell) \overset{\mathcal{D}_{\sim\mathcal{A}}}{\equiv} \begin{cases} \bigwedge_{a\in\Sigma} \bigwedge_{(\ell,g,a,\ell')\in T_{\mathcal{A}}} [g]\langle a\rangle\ \Phi^{\sim\mathcal{A}}(\ell') & (\mathcal{C}_1) \\ \wedge & \\ [I_{\mathcal{A}}(\ell)]\ \Phi^{\sim\mathcal{A}}(\ell) & (\mathcal{C}_2) \\ \wedge & \\ \bigwedge_{a\in\Sigma} \bigwedge_{g\in\mathsf{Split}(\ell,a)} [g][a] \bigvee_{(\ell,g',a,\ell')\in T_{\mathcal{A}} \mid [\![g]\!]\subseteq[\![g']\!]} \Phi^{\sim\mathcal{A}}(\ell') & (\mathcal{C}_3) \\ \wedge & \\ \bigwedge_{a\in\Sigma} [\neg\mathsf{En}(\ell,a)][a]\mathtt{ff} & (\mathcal{C}_4) \\ \wedge & \\ [\neg I_{\mathcal{A}}(\ell)]\ \mathtt{ff} & (\mathcal{C}_5) \end{cases}$$

Before proving the correctness of this construction, we give some intuition on its definition. Let $\mathcal{B}$ be an ERA and analyze how these formulae constrain $\mathcal{B}$. The parts $\mathcal{C}_1$ and $\mathcal{C}_2$ express the simulation constraints ($\mathcal{A} \prec \mathcal{B}$), while the three other constraints express the converse ($\mathcal{B} \prec \mathcal{A}$). More precisely, note that $\mathcal{C}_1$ requires that any discrete transition of $\mathcal{A}$ also exists in $\mathcal{B}$: for any transition in $\mathcal{A}$ and *for all delays* after which it is firable, *there exists* a corresponding transition in $\mathcal{B}$ leading to a bisimilar configuration. This combination of a universal quantification over delays with an existential quantification over discrete successors was missing in ERL, as shown in Section 3. In the converse direction, discrete transitions are encoded in $\mathcal{C}_3$ and $\mathcal{C}_4$. $\mathcal{C}_4$ states that an $a$ transition can only happen in $\mathcal{B}$ when it is possible in $\mathcal{A}$. $\mathcal{C}_3$ uses the decomposition $\mathsf{Split}(\ell,a)$ of the clock constraint $\mathsf{En}(\ell,a)$ to express that any $a$ transition in $\mathcal{B}$ corresponds to some $a$ transition of $\mathcal{A}$ firable from the same valuation. This corrects the corresponding constraint of the construction of [16] (see Section 3). Finally, $\mathcal{C}_2$ and $\mathcal{C}_5$ handle the case of delay transitions.

*Remark 3 (On the size of formulae $\Phi^{\sim\mathcal{A}}$).* Due to the use of the operator $\mathsf{Split}$, these formulae are in the worst case of size $|\mathcal{A}|\times 2^{O(|\Sigma|\log K|\Sigma|)}$, with $K$ the largest integer constant of $\mathcal{A}$, whereas if $\mathcal{A}$ is deterministic, then their size is linear in the size of $\mathcal{A}$. We believe that this exponential blow-up is not avoidable. Indeed, for ERA, once a discrete transition labelled by $a$ has been fired, one can not recover the value of clock $x_a$ before this firing as it has been reset. Formulae of [1], which have a linear size, compare the clock valuation with the guards after the discrete firing. Moreover, note that this exponential blow-up has no consequences on the theoretical time complexity of timed bisimilarity checking (see Corollary 1), as linear formulae would lead to the same complexity.

The following result states the correctness of the previous construction.

**Theorem 4.** *Let $\mathcal{A}$ and $\mathcal{B}$ be two* ERA *over $\Sigma$ and consider $\ell$ and $m$ two locations of $\mathcal{A}$ and $\mathcal{B}$ respectively. Then for any valuation $v \in \mathbb{T}^\Sigma$, we have :*

$$(\ell, v) \sim (m, v) \iff \mathcal{B}, (m, v) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)$$

*In particular, we have:* $\mathcal{A} \sim \mathcal{B} \iff \mathcal{B} \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell_0^{\mathcal{A}})$

*Proof.* To prove Theorem 4 we establish successively the two implications:

$\Leftarrow$ If $\mathcal{B}, (m, v) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)$, then we have $(\ell, v) \sim (m, v)$.
$\Rightarrow$ If $(\ell, v) \sim (m, v)$, then $\mathcal{B}, (m, v) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)$ holds.

Let us denote by $Q_{\mathcal{A}}$ and $Q_{\mathcal{B}}$ the set of configurations of $\mathcal{A}$ and $\mathcal{B}$ respectively.
**Proof of $\Leftarrow$.** We consider the relation $\mathcal{R} \subseteq Q_{\mathcal{A}} \times Q_{\mathcal{B}}$ defined as $\mathcal{R} = \{((\ell, v), (m, v)) \mid \mathcal{B}, (m, v) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)\}$ and show that it is a timed bisimulation. In other terms, we must verify the conditions of Definition 8.

($i$) *Step in $\mathcal{A}$.* Consider $\sigma \in \Sigma \cup \mathbb{T}$ such that $(\ell, v) \xrightarrow{\sigma} (\ell', v')$ in $\mathcal{A}$, and show that there exists $m' \in L_{\mathcal{B}}$ such that $(m, v) \xrightarrow{\sigma} (m', v')$ in $\mathcal{B}$ and $(\ell', v')\mathcal{R}(m', v')$. We distinguish two cases according to the nature of $\sigma$.
- If $\sigma = a \in \Sigma$. Then there exists a transition $(\ell, g, a, \ell') \in T_{\mathcal{A}}$ corresponding to this firing. In particular, we have $v \models g$ and $v' = v[x_a := 0]$. By hypothesis, we have $\mathcal{B}, (m, v) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)$. In particular the transition of $\mathcal{A}$ corresponds to a conjunct in part $\mathcal{C}_1$ of $\Phi^{\sim\mathcal{A}}(\ell)$, and we thus have $\mathcal{B}, (m, v) \models_{\mathcal{D}_{\sim\mathcal{A}}} [g]\langle a\rangle\Phi^{\sim\mathcal{A}}(\ell')$. As $v \models g$, this implies the existence of a step $(m, v) \xrightarrow{a} (m', v'')$ in $\mathcal{B}$, with $\mathcal{B}, (m, v'') \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell')$. The semantics of ERA implies that $v'' = v[x_a := 0]$, and then $v'' = v'$, what concludes this case.
- If $\sigma = \delta \in \mathbb{T}$. Then we have $(\ell, v) \xrightarrow{\delta} (\ell, v + \delta)$ in $\mathcal{A}$ what implies that $v + \delta \models I_{\mathcal{A}}(\ell)$. Part $\mathcal{C}_2$ of $\Phi^{\sim\mathcal{A}}(\ell)$ then implies the existence of the transition $(m, v) \xrightarrow{\delta} (m, v + \delta)$ in $\mathcal{B}$, such that $\mathcal{B}, (m, v + \delta) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)$, as desired.

This shows that the relation $\mathcal{R}$ is a timed simulation between $\mathcal{A}$ and $\mathcal{B}$.

($ii$) *Step in $\mathcal{B}$.* Conversely, we show that the relation $\mathcal{R}^{-1}$ is a timed simulation between $\mathcal{B}$ and $\mathcal{A}$. As above, let us consider $\sigma \in \Sigma \cup \mathbb{T}$ such that $(m, v) \xrightarrow{\sigma} (m', v')$ in $\mathcal{B}$, and show that there exists $\ell' \in L_{\mathcal{A}}$ such that $(\ell, v) \xrightarrow{\sigma} (\ell', v')$ in $\mathcal{A}$ and $(\ell', v')\mathcal{R}(m', v')$. Again, we distinguish two cases according to the nature of $\sigma$.
- If $\sigma = a \in \Sigma$. By hypothesis, we have $\mathcal{B}, (m, v) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)$. In particular, part $\mathcal{C}_4$ of this formula is satisfied what implies that $v \models \mathsf{En}(\ell, a)$. Then, as $\mathsf{Split}(\ell, a)$ partitions the constraint $\mathsf{En}(\ell, a)$, there exists a unique clock constraint $g \in \mathsf{Split}(\ell, a)$ such that $v \models g$. The corresponding conjunct of part $\mathcal{C}_3$ implies that $\mathcal{B}, (m', v') \models_{\mathcal{D}_{\sim\mathcal{A}}} \bigvee_{(\ell, g', a, \ell') \in T_{\mathcal{A}} \mid [\![g]\!] \subseteq [\![g']\!]} \Phi^{\sim\mathcal{A}}(\ell')$. The second property of $\mathsf{Split}(\ell, a)$ implies, as $[\![g]\!]$ is not empty, that there exists a transition $(\ell, g', a, \ell') \in T_{\mathcal{A}}$ such that $\mathcal{B}, (m', v') \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell')$ and with $[\![g]\!] \subseteq [\![g']\!]$. As a consequence, we have $v \models g'$ and then $(\ell, v) \xrightarrow{a} (\ell', v'')$ in $\mathcal{A}$, with $v'' = v[x_a := 0] = v'$, what concludes this case.

– If $\sigma = \delta \in \mathbb{T}$. Then we have $(m, v) \xrightarrow{\delta} (m, v+\delta)$ in $\mathcal{B}$. Part $\mathcal{C}_5$ of formula $\Phi^{\sim\mathcal{A}}(\ell)$ implies that $v+\delta \models I_{\mathcal{A}}(\ell)$. Thus, the transition $(\ell, v) \xrightarrow{\delta} (\ell, v+\delta)$ exists in $\mathcal{A}$. Moreover, since $v + \delta \models I_{\mathcal{A}}(\ell)$, part $\mathcal{C}_2$ of the formula $\Phi^{\sim\mathcal{A}}(\ell)$ implies that $(m, v + \delta) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)$, as desired.

This concludes the proof that $\mathcal{R}^{-1}$ is also a timed simulation between $\mathcal{B}$ and $\mathcal{A}$, and thus $\mathcal{R}$ is a timed bisimulation as desired. This concludes the proof of the first implication.

**Proof of $\Rightarrow$.** We assume that the property $\mathcal{B}, (m, v) \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell)$ holds and want to show that the two configurations $(\ell, v)$ and $(m, v)$ are timed bisimilar. Recall that the formulae $\Phi^{\sim\mathcal{A}}(\ell)$ are defined as the greatest solution of a system of inequations. Using the notion of coinduction [14], any solution of these inequations also satisfies these formulae. We consider the assignment function $\mathcal{V}$ over the variabes $\Phi^{\sim\mathcal{A}}(\ell)$ defined by $\mathcal{V}(\Phi^{\sim\mathcal{A}}(\ell)) = \{(m, v) \in Q_{\mathcal{B}} \mid (\ell, v) \sim (m, v)\}$ for any $\ell \in L_{\mathcal{A}}$. It is then sufficient to prove the following inclusions:

$$\forall \ell \in L_{\mathcal{A}}, [\![\Phi^{\sim\mathcal{A}}(\ell)]\!]^{\mathcal{B}}_{\mathcal{V}} \subseteq [\![\mathcal{D}_{\sim\mathcal{A}}(\Phi^{\sim\mathcal{A}}(\ell))]\!]^{\mathcal{B}}_{\mathcal{V}} \tag{4}$$

Let $(m, v) \in [\![\Phi^{\sim\mathcal{A}}(\ell)]\!]^{\mathcal{B}}_{\mathcal{V}}$ (that is such that $(\ell, v) \sim (m, v)$). The proof proceeds by considering each conjunct $\xi$ of $\mathcal{D}_{\sim\mathcal{A}}(\Phi^{\sim\mathcal{A}}(\ell))$.

1. $\xi = [g]\langle a\rangle\Phi^{\sim\mathcal{A}}(\ell')$ for some transition $(\ell, g, a, \ell') \in T_{\mathcal{A}}$. We consider two cases whether this transition can be fired from the configuration $(\ell, v)$ or not. If it is not the case, that is $\forall \delta \in \mathbb{T}, v+\delta \not\models g$, then we trivially have $\mathcal{B}, (m, v) \models \xi$. Otherwise, there exists a delay $\delta \in \mathbb{T}$ such that $v + \delta \models g$. Then, we have $(\ell, v+\delta) \xrightarrow{a} (\ell', v')$ in $\mathcal{A}$, with $v' = (v+\delta)[x_a := 0]$. By bisimulation property and by time determinism, we have that $(\ell, v + \delta) \sim (m, v + \delta)$ and then that there exists a configuration $(m', v'')$ of $\mathcal{B}$ such that $(m, v + \delta) \xrightarrow{a} (m', v'')$ in $\mathcal{B}$ and $(\ell', v') \sim (m', v'')$. Semantics of ERA implies that $v' = v''$ and thus the result follows since, by definition of $\mathcal{V}$, we have $(m', v') \in [\![\Phi^{\sim\mathcal{A}}(\ell')]\!]^{\mathcal{B}}_{\mathcal{V}}$.
2. $\xi = [I_{\mathcal{A}}(\ell)]\Phi^{\sim\mathcal{A}}(\ell)$. For any $\delta \in \mathbb{T}$ such that $v + \delta \models I_{\mathcal{A}}(\ell)$, we have $(\ell, v) \xrightarrow{\delta} (\ell, v+\delta)$ in $\mathcal{A}$. By bisimulation property and time determinism, we then have $(\ell, v + \delta) \sim (m, v + \delta)$. This concludes this case.
3. $\xi = [g][a] \bigvee_{(\ell,g',a,\ell') \in T_{\mathcal{A}} \mid [\![g]\!] \subseteq [\![g']\!]} \Phi^{\sim\mathcal{A}}(\ell')$, for some clock constraint $g \in \mathsf{Split}(\ell, a)$. Consider, if some exists, a delay $\delta \in \mathbb{T}$ such that $v + \delta \models g$ and $(m, v) \xrightarrow{\delta} (m, v + \delta) \xrightarrow{a} (m', v')$ in $\mathcal{B}$. Then, we must show that the following holds: $\mathcal{B}, (m', v') \models_{\mathcal{D}_{\sim\mathcal{A}}} \bigvee_{(\ell,g',a,\ell') \in T_{\mathcal{A}} \mid [\![g]\!] \subseteq [\![g']\!]} \Phi^{\sim\mathcal{A}}(\ell')$. First, we have by bisimulation and time-determi-nism that $(\ell, v) \xrightarrow{\delta} (\ell, v + \delta)$ exists in $\mathcal{A}$ and that $(\ell, v + \delta) \sim (m, v + \delta)$ holds. Bisimulation then imples that there exists a transition $(\ell, v + \delta) \xrightarrow{a} (\ell', v'')$ in $\mathcal{B}$ such that $(\ell', v'') \sim (m', v')$. This implies that there exists a transition $(\ell, g', a, \ell')$ in $T_{\mathcal{A}}$ such that $v + \delta \models g'$. By the second property of $\mathsf{Split}(\ell, a)$, this implies that $[\![g]\!] \subseteq [\![g']\!]$, and thus this transition belongs to the disjunction of $\xi$. In particular, we thus have $\mathcal{B}, (m', v') \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell')$, as required.

4. $\xi = [\neg \mathsf{En}(\ell, a)][a]\mathtt{ff}$. By contradiction, assume that the property is not satisfied, that is that there exists a delay $\delta \in \mathbb{T}$ such that $v + \delta \notin \mathsf{En}(\ell, a)$ and $(m, v + \delta) \xrightarrow{a} (m', v')$ in $\mathcal{B}$ for some configuration $(m', v')$. By bisimulation, an $a$-labelled transition is also firable from the configuration $(\ell, v + \delta)$, what contradicts the fact that $v + \delta \notin \mathsf{En}(\ell, a)$.
5. $\xi = [\neg I_{\mathcal{A}}(\ell)]\mathtt{ff}$. By contradiction, assume that the property is not satisfied, that is that there exists a delay $\delta \in \mathbb{T}$ such that $v + \delta \not\models I_{\mathcal{A}}(\ell)$ and $(m, v) \xrightarrow{\delta} (m, v + \delta)$ in $\mathcal{B}$. By bisimulation, we also have $(\ell, v) \xrightarrow{\delta} (\ell, v + \delta)$ in $\mathcal{B}$ what contradicts $v + \delta \not\models I_{\mathcal{A}}(\ell)$.

This concludes the proof of the property (4), and thus the second implication also holds.

This concludes the proof of Theorem 4. □

**Corollary 1.** *One can decide timed bisimilarity of two* ERA $\mathcal{A}$ *and* $\mathcal{B}$ *over* $\Sigma$ *in time* $|\mathcal{A}| \times |\mathcal{B}| \times 2^{O(|\Sigma| \log K|\Sigma|)}$ *(*$K$ *denotes the largest constant of* $\mathcal{A}$ *and* $\mathcal{B}$*).*

*Proof.* Using the previous theorem, this problem reduces to the model checking problem of $\mathcal{B}$ against formula $\Phi^{\sim\mathcal{A}}(\ell_0^{\mathcal{A}})$ under the declaration $\mathcal{D}_{\sim\mathcal{A}}$. Note that $\Phi^{\sim\mathcal{A}}$ contains only greatest fixpoints and thus is alternation-free. As there exists better complexity results for this class (see [7]), the proof of Theorem 3 shows that the time complexity of this problem is in $O(|\mathcal{R}_K(\mathcal{B})| \times |\Phi^{\sim\mathcal{A}}|)$. The result follows from the size of $\mathcal{R}_K(\mathcal{B})$ and previous remarks on the size of the formulae $\Phi^{\sim\mathcal{A}}$. □

### 5.2 Characteristic Formulae for Timed Simulation

**Definition 14.** *We define a declaration* $\mathcal{D}_{\succ\mathcal{A}}$ *associating a formula to each location* $\ell$ *of* $\mathcal{A}$*, and consider the greatest solution of this system of fixpoint equations.*

$$\Phi^{\succ\mathcal{A}}(\ell) \overset{\mathcal{D}_{\succ\mathcal{A}}}{=} \begin{cases} \displaystyle\bigwedge_{a\in\Sigma} \bigwedge_{(\ell,g,a,\ell')\in T} [g]\langle a\rangle\ \Phi^{\succ\mathcal{A}}(\ell') & (\mathcal{C}_1') \\ \wedge & \\ [I_{\mathcal{A}}(\ell)]\ \Phi^{\succ\mathcal{A}}(\ell) & (\mathcal{C}_2') \end{cases}$$

Note that this construction leads to formulae of *size linear* in the size of $\mathcal{A}$. The following result states the correctness of the previous construction.

**Theorem 5.** *Let* $\mathcal{A}$ *and* $\mathcal{B}$ *be two* ERA *over* $\Sigma$ *and consider* $\ell$ *and* $m$ *two locations of* $\mathcal{A}$ *and* $\mathcal{B}$ *respectively. Then for any valuation* $v \in \mathbb{T}^{\Sigma}$*, we have :*

$$(\ell, v) \prec (m, v) \iff \mathcal{B}, (m, v) \models_{\mathcal{D}_{\succ\mathcal{A}}} \Phi^{\succ\mathcal{A}}(\ell)$$

*In particular, we have:* $\mathcal{A} \prec \mathcal{B} \iff \mathcal{B} \models_{\mathcal{D}_{\succ\mathcal{A}}} \Phi^{\succ\mathcal{A}}(\ell_0^{\mathcal{A}})$

We omit the proof as it is similar to that of Theorem 4. As for bisimilarity, we obtain an EXPTIME procedure to decide timed similarity:

**Corollary 2.** *One can decide timed similarity of two* ERA $\mathcal{A}$ *and* $\mathcal{B}$ *over* $\Sigma$ *in time* $|\mathcal{A}| \times |\mathcal{B}| \times 2^{O(|\Sigma| \log K|\Sigma|)}$ *(*$K$ *denotes the largest constant of* $\mathcal{A}$ *and* $\mathcal{B}$*).*

Moreover, this procedure can also be used to decide language inclusion between ERA. More precisely, we have:

**Corollary 3.** *Given two* ERA $\mathcal{A}$ *and* $\mathcal{B}$*, the procedure checking timed simulation leads to an* EXPTIME *procedure to decide whether* $\mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$ *holds or not.*

*Proof.* We first determinize automaton $\mathcal{B}$, resulting in $\mathcal{B}'$. Following [4], the number of locations and transitions of $\mathcal{B}'$ is then exponential in the size of $\mathcal{B}$. Using Proposition 1, language inclusion reduces to $\mathcal{A} \prec \mathcal{B}'$, and then to the model checking problem $\mathcal{B}' \models_{\mathcal{D}_{\succ \mathcal{A}}} \Phi^{\succ \mathcal{A}}(\ell_0^{\mathcal{A}})$. Using previous analysis, this can be checked in time $|\mathcal{R}_K(\mathcal{B}')| \times |\Phi^{\succ \mathcal{A}}|$. Finally, we obtain a procedure to decide this language inclusion in time $|\mathcal{A}| \times 2^{|\mathcal{B}|}$, which belongs thus to EXPTIME. □

Note that the problem of language inclusion is PSPACE-complete [4], thus this procedure is not optimal. However, the known algorithm [4] matching the lower bound consists in guessing a path in the region automaton. A zone-based version of this procedure may thus be an interesting alternative in practice.

## 6 Conclusion

In this paper, we focused on the construction of characteristic formulae for ERA up to timed (bi)similarity. After having shown that the problem could not be solved in the logic ERL, we have introduced the new logic $\mathrm{WT}_\mu$, and have proven that it is strictly more expressive than ERL and that its model checking problem over ERA is EXPTIME-complete. We have finally provided characteristic formulae constructions in $\mathrm{WT}_\mu$ for the whole class of ERA with invariants.

Compared to existing results of [1] for timed automata which can also be applied to ERA using natural translations, we obtain procedures in the same class of complexity (EXPTIME), but our time complexity are more precise. For instance, for a fixed alphabet $\Sigma$ and if constants are encoded in unary, then timed (bi)simulation can be checked in polynomial time! Moreover, our algorithm for model checking $\mathrm{WT}_\mu$ against ERA should also be more efficient than going through $\mathcal{L}_\nu$ and timed automata as it involves only one copy of the event-clocks. Finally, we obtain a non-optimal procedure for inclusion checking between ERA, which we believe could lead to good results in practice.

As future work, we plan to study how the good decidability results of the satisfiability problem for ERL transfer to $\mathrm{WT}_\mu$. We also envisage to adapt the implementation of the procedures of [1] done in the tool CMC [10] to this framework for ERA.

## References

1. L. Aceto, A. Ingólfsdóttir, M. L. Pedersen, and J. Poulsen. Characteristic formulae for timed automata. *Theoretical Informatics and Application*, 34(6):565–584, 2000.

2. L. Aceto and F. Laroussinie. Is your model-checker on time ? *Journal of Logic and Algebraic Programming*, 52–53:7–51, 2002.
3. R. Alur and D. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.
4. R. Alur, L. Fix, and T. A. Henzinger. A determinizable class of timed automata. In *Proc. CAV'94*, volume 818 of *LNCS*, pages 1–13. Springer, 1994.
5. H. Bekic. Definable operation in general algebras, and the theory of automata and flowcharts. In *Programming Languages and Their Definition*, pages 30–55. Springer-Verlag, 1984.
6. A. K. Chandra, D. C. Kozen, and L. J. Stockmeyer. Alternation. *J. ACM*, 28(1):114–133, 1981.
7. R. Cleaveland and B. Steffen. A linear-time model-checking algorithm for the alternation-free modal mu-calculus. *Formal Methods in System Design*, pages 48–58, 1993.
8. D. D'Souza. A logical characterisation of event clock automata. *Int. J. Found. Comput. Sci.*, 14(4):625–640, 2003.
9. T. A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model-checking for real-time systems. *Information and Computation*, 111(2):193–244, 1994.
10. F. Laroussinie and K. G. Larsen. CMC: A tool for compositional model-checking of real-time systems. In *Proc. FORTE-PSTV'98*, pages 439–456. Kluwer Academic, 1998.
11. F. Laroussinie, K. G. Larsen, and C. Weise. From timed automata to logic – and back. In *Proc. MFCS'95*, volume 969 of *LNCS*, pages 529–539. Springer, 1995.
12. O.-L. Nguena-Timo. The logic WT$\mu$. Technical Report RR-1460-09, LaBRI, 2009.
13. J.-F. Raskin and P.-Y. Schobbens. The logic of event clocks - decidability, complexity and expressiveness. *Journal of Automata, Languages and Combinatorics*, 4(3):247–286, 1999.
14. D. Sangiorgi. Bisimulation: From the origins to today. In H. Ganzinger, editor, *Proc. LICS'04*, pages 298–302. IEEE Computer Society Press, July 2004.
15. M. Sorea. A decidable fixpoint logic for time-outs. In *Proc. CONCUR'02*, volume 2421 of *LNCS*, pages 255–271. Springer, 2002.
16. M. Sorea. *Verification of Real-Time Systems through Lazy Approximations*. PhD thesis, University of Ulm, 2004.
17. W. Thomas. Languages, automata, and logic. In *Handbook of formal languages, vol. 3: beyond words*, pages 389–455. Springer-Verlag, 1997.