Theoretical Informatics and Applications Will be set by the publisher
Informatique Théorique et Applications

ON CHARACTERISTIC FORMULAE FOR EVENT-RECORDING AUTOMATA *

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

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. 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 incorrect. More generally, we prove that timed bisimilarity cannot in general be expressed in ERL for the class of ERA, and study under which conditions on ERA it can be. Then, we introduce the logic WT_μ, a new logic for event-based timed specifications closer to the timed logic $\mathcal{L}_\nu$ that was introduced by Laroussinie, Larsen and Weise. We prove that it is strictly more expressive than ERL, and that its model-checking problem against ERA is EXPTIME-complete. Finally, we provide characteristic formulae constructions in WT_μ for characterizing the general class of ERA up to timed (bi)similarity and study the complexity issues.

1991 Mathematics Subject Classification. 03B44,68Q60.

1. Introduction

In the untimed setting, automata and logics are central tools for the formal verification of reactive systems. While a system is usually modelled as an automaton, the specification may be described either as a formula of a logic or as an automaton.

Keywords and phrases: Timed logic, bisimulation, event-clock automata.

* *The second author is partly supported by the ANR project ECSPER (ANR JC09 472677).*

[1] LaBRI, Université Bordeaux I & CNRS, France.

[2] LIF, Université Aix-Marseille & CNRS, France.

In the first case the correctness of the system reduces to a model checking problem, whereas in the second case it requires a comparison of the behaviour of the two automata, and different relations can be envisaged, such as bisimilarity [16] 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 chosen relation. Timed automata [3] is a well known formalism for modelling real-time systems. They are obtained by adding real-valued variables called clocks to finite-state automata, and contain two kind of transitions, discrete transitions and time-elapsing transitions. For this class, a solution has first been proposed in [12], providing characteristic formulae in the logic $\mathcal{L}_\nu$. Then, these results have been improved in [1], yielding characteristic formulae whose size is linear in that of the automaton.

The class of Event-Recording Automata [4] (ERA), which forms a subclass of timed automata, 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 [9, 15], 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.

As ERA can be linearly translated into timed automata, results of [1] can be used to build characteristic formulae in the logic $\mathcal{L}_\nu$ whose size is linear in that of the ERA. However, as ERA are strictly less expressive than timed automata, our motivation is to find a weaker logic, with a decidable satisfiability problem (the status of the satisfiability problem for $\mathcal{L}_\nu$ is still an open problem [12]). There exists a logic which is a natural candidate, the so-called Event-Recording Logic (ERL), introduced by Sorea in [17]. This logic extends the mu-calculus by allowing the use of event-clocks and has a decidable satisfiability problem. In this paper, we prove that it is in general impossible to express timed bisimilarity for ERA in ERL. More precisely, we identify two large subclasses of ERA which cannot be characterized by ERL, and provide restrictions on the constants used in ERA which yield subclasses that can be characterized by ERL.

To overcome these limitations, we consider a new timed logic for event-clocks, called WT_μ [13], and provide characteristic formulae constructions for timed similarity and timed bisimilarity. In addition, the satisfiability problem for the fragment of WT_μ we use here is proved to be decidable in [13].

After recalling standard definitions in Section 2, we study in Section 3 the problem of expressing characteristic formulae for timed bisimilarity for ERA in the logic ERL. We prove that it is in general impossible, and detail how restrictions on the nature of constants used in ERA impact this negative result. In addition, we explain why an existing attempt, which can be found in [18], is not correct. Then, we consider in Section 4 our new timed logic WT_μ to express the characteristic formulae. The definition of this logic is closer to 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 characteristic formulae constructions in WT_μ for timed (bi)similarity together with complexity issues in Section 5. We end with a positive result for ERL: for ERA with a fixed granularity and without invariants, it is possible to build characteristic formulae in ERL.

Part of the results presented here appeared in [14].

2. Preliminaries

Let Σ be a finite alphabet and let Σ^* be the set of finite words over Σ. The sets $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{Q}_{\geq 0}$ and $\mathbb{R}_{\geq 0}$ are the sets of natural, rational, non-negative rational and non-negative real numbers respectively. Given a real number x, $\lfloor x \rfloor$ (resp. $\langle x \rangle$) denotes its integral part (resp. its fractional 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 to 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 Σ, 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 [1] "$g ::= x \sim c \mid x - y \sim c \mid g \wedge g \mid \mathtt{tt}$" 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 allow empty conjunctions which, as usual, stand for $\mathtt{tt}$. We write $v \models g$ when the clock valuation v satisfies the clock constraint g, using the standard semantics. We also denote by $[\![g]\!]$ the set of clock valuations v such that $v \models g$ holds.

The *granularity* of a set of clock constraints $\mathcal{C}_0 \subseteq \mathcal{C}(\Sigma)$ is defined as the pair $(d, M) \in \mathbb{N} \times \mathbb{N}$ where d (resp. M) is the least common multiple of denominators (resp. the maximal value) of constants appearing in clock constraints of $\mathcal{C}_0$. Conversely, we say that $r \in \mathbb{Q}_{\geq 0}$ can be produced by granularity (d, M) iff $r \leq M$ and there exist $p, q \in \mathbb{N}$ such that $r = \frac{p}{q}$ and q divides d.

In addition, we also consider as granularities the pairs (∞, M) and (d, ∞) which respectively denote constants that belong to $\mathbb{Q}_{\geq 0} \cap [0, M]$ and to $\{\frac{p}{d} \mid p \in \mathbb{N}\}$.

[1] Constraints of the form $x - y \sim c$ are called *diagonal constraints*.

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].

Definition 2.1 (Timed Transition System (TTS))**.** A *timed transition system* over the alphabet Σ 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 (or delay) 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 transitions $\rho = q_0 \xrightarrow{d_0} q'_0 \xrightarrow{a_0} q_1 \xrightarrow{d_1} q'_1 \xrightarrow{a_1} q_2 \dots \xrightarrow{a_n} q_{n+1}$ 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 Σ where $\tau_i = \sum_{j=0}^{i} d_j$ is the absolute 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. In this context, for each action $a \in \Sigma$, the system owns a distinguished clock denoted by x_a. This clock records the amount of time that elapsed since the last occurence of the event a. Therefore, clock x_a is reset precisely when event a occurs (we also assume that all clocks are initially equal to 0).

Definition 2.2 (Event-Recording Automata (ERA) [4])**.** An *event-recording automaton* over the alphabet Σ is a tuple $\mathcal{A} = \langle L, \ell_0, \Sigma, E, I \rangle$ where:

- L is a finite set of locations,
- $\ell_0 \in L$ is the initial location,
- $E \subseteq L \times \mathcal{C}(\Sigma) \times \Sigma \times L$ is a finite set of edges,
- $I : L \to \mathcal{C}_{up}(\Sigma)$ 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 from the definition of $\mathcal{A}$. The class of ERA without invariants is denoted by $\mathrm{ERA}^{\mathrm{lazy}}$.

The granularity of an ERA $\mathcal{A}$ is defined as the granularity of all clock constraints of $\mathcal{A}$. Given a granularity (d, M), the class of ERA defined using only constants that can be produced by (d, M) is denoted by $\mathrm{ERA}_{(d,M)}$.

We may also combine these subscripts with the exponent lazy.

Examples of ERA are depicted in Figures 1 and 2, pages 9 and 14 respectively. Note that all these ERA are without invariants.

Without loss of generality, we assume that the clock constraints of edges are consistent with invariants. This technical assumption ensures that the configuration reached after a discrete transition is a correct configuration. More formally, we have, for any $v \in \mathbb{T}^\Sigma$:

$$\forall (\ell, g, a, \ell') \in E, v \models g \Rightarrow (v \models I(\ell)) \wedge (v[x_a := 0] \models I(\ell'))$$

This property can easily be ensured by a syntactic transformation of the model. More precisely, each edge $e = (\ell, g, a, \ell')$ is replaced by the edge $\overline{e} = (\ell, \overline{g}, a, \ell')$ where $\overline{g}$ is obtained from g as follows. Consider the constraint g_1 obtained by projecting the constraint $I(\ell')$ on clocks different from x_a (this means that if $I(\ell')$ constrains the clock x_a, then this constraint is relaxed). Then we let $\overline{g}$ be the conjunction $g \wedge I(\ell) \wedge g_1$.

The semantics of an event-recording automaton $\mathcal{A}$ is defined in terms of a timed transition system. Intuitively, it manipulates exactly one clock per action, which allows to measure the time elapsed since the last occurrence of this action. The formal definition is given by [2]:

Definition 2.3 (Semantics of an ERA)**.** Given an ERA $\mathcal{A} = \langle L, \ell_0, \Sigma, E, I \rangle$, 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 time-elapsing 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 an edge $e = (\ell, g, a, \ell') \in E$ 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 $\mathcal{L}(\mathcal{S}_\mathcal{A})$.

In the previous definition, the set of states of the TTS $\mathcal{S}_\mathcal{A}$ is restricted to valuations compatible with the invariant of the current location. In particular, this provides continuity of invariant-staisfaction during the course of a transition. In addition, as invariants are defined by upper bound contraints, when firing a time-elapsing transition $(\ell, v) \xrightarrow{d} (\ell, v + d)$, all intermediate valuations $v + d'$, with $d \leq d'$, do satisfy $v + d' \models I(\ell)$.

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

We assume the reader is familiar with the *region construction* of [3] for timed automata. For the sake of completeness, we recall here the main definitions and properties we will use in what follows.

[2]The definition slightly differs from the original definition of [4] as it assigns 0 as the initial value of clocks. This modification allows us to simplify our constructions, but the original framework could also be handled.

Definition 2.4 (Clock Region)**.** We consider a constant $K \in \mathbb{N}$. We define 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 $\langle v(x) \rangle \leq \langle v(y) \rangle \iff \langle v'(x) \rangle \leq \langle v'(y) \rangle$.

A *clock region* is an equivalence class of the relation $\simeq_K$.

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. To define the region automaton of an ERA $\mathcal{A}$, we can assume that all the constants occurring in its clock constraints 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 2.5 (Region Automaton)**.** Let $\mathcal{A} = \langle L, \ell_0, \Sigma, E, I \rangle$ be an ERA with integral constants. Let K be some positive integer. We define the region automaton of $\mathcal{A}$ for constant K, denoted by $\mathcal{R}_K(\mathcal{A}) = \langle R_K(\mathcal{A}), \Sigma \cup \{\tau\}, \rightarrow \rangle$, as follows [3]:

- $R_K(\mathcal{A}) = \{(\ell, r) \in L \times R_K(\Sigma) \mid \exists v \in r \text{ s.t. } v \models I(\ell)\}$
- $(\ell, r) \xrightarrow{\tau} (\ell, r') \iff \exists \delta \in \mathbb{T}$ 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 time abstract bisimilar [3] to $\mathcal{S}_\mathcal{A}$.

2.3. Event-Recording Logic

Definition 2.6 (Event-Recording Logic (ERL) [17])**.** Let Σ be a finite alphabet, Var be a finite set of variables, the formulae of the Event-Recording Logic over Σ 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 $X \in \mathsf{Var}$.

In the timed logic $\mathcal{L}_\nu$ [12], 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 Σ, the clock constraints range over event clocks associated with Σ. Then, the semantics is defined for TTS corresponding to ERA over the same alphabet Σ, and the clock constraints are evaluated over the valuations 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 $\mathcal{V}'(X) = Q' \subseteq Q$.

[3] τ is an action not in Σ intended to represent time-elapsing.

Definition 2.7 (Semantics of ERL)**.** Let Σ be a finite alphabet, Var be a finite set of variables, $\mathcal{A} = \langle L, \ell_0, \Sigma, E, I\rangle$ be an ERA [4] over Σ and $\mathcal{S}_\mathcal{A} = \langle Q, q_0, \Sigma, \to\rangle$ be its associated TTS. Consider a formula $\varphi \in$ ERL over Σ and Var and an assignment function $\mathcal{V}$ of Var over Q. The semantics of φ 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:

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

Using standard definitions, we say that an occurence of a variable X is *bound* (resp. *free*) in a formula φ whenever it is (resp. it is not) under the scope of a fixpoint operator μ or ν. It is easy to verify that if all variables are bound in a formula φ (we say that φ is a *sentence*), then the semantics of φ 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 φ, 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 $\mathcal{A}, q^\mathcal{A}_0 \models \varphi$, where $q^\mathcal{A}_0$ denotes the initial configuration of $\mathcal{A}$. Moreover, we say that a bound variable X is *guarded* if it is in the scope of an operator $\langle\cdot\rangle$ or $[\cdot]$. According to [17], one can assume that every bound variable is guarded.

Remark 2.8 (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 finite set Var of variables, we will associate to each variable X a formula $\mathcal{D}(X)$ over the variables 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 proved (see [5] or [8]) that this presentation can be translated into an equivalent formula with greatest fixpoints. For each variable $X \in \mathsf{Var}$, there exists a formula $\varphi^\mathcal{D}_X$, with only greatest fixpoints, which has an equivalent satisfiability set. In this setting, we will add the declaration $\mathcal{D}$ as subscript to the satisfaction relation $\models$, and write $\mathcal{A}, q \models_\mathcal{D} X$ to denote $\mathcal{A}, q \models \varphi^\mathcal{D}_X$.

[4] Note that we extend the definition of [17] to ERA with invariants.

2.4. Timed Behavioral Relations and Characteristic Formulae

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 2.9 (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 $q_1 \xrightarrow{\alpha}_1 q_1'$ then there exists $q_2' \in Q_2$ such that $q_2 \xrightarrow{\alpha}_2 q_2'$ 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 timed 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 2.10. Let $\mathcal{A}$ and $\mathcal{B}$ be two ERA. $\mathcal{A}$ *simulates* $\mathcal{B}$ ($\mathcal{A} \prec \mathcal{B}$) iff $\mathcal{S}_\mathcal{A} \prec \mathcal{S}_\mathcal{B}$. $\mathcal{A}$ *and* $\mathcal{B}$ *are timed bisimilar* ($\mathcal{A} \sim \mathcal{B}$) iff $\mathcal{S}_\mathcal{A} \sim \mathcal{S}_\mathcal{B}$.

Note that in an ERA, invariants reduce the possible delay transitions. In a location without invariant, any delay transition is possible, even if it leads to a deadlock configuration. Thus, if two configurations (ℓ, v) and (ℓ', v') are bisimilar, this implies that ℓ owns a non-trivial invariant iff ℓ' does.

Definition 2.11 (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:

Timed Similarity: $\forall \mathcal{B} \in \text{ERA}, \mathcal{A} \prec \mathcal{B} \iff \mathcal{B} \models \varphi$
Timed Bisimilarity: $\forall \mathcal{B} \in \text{ERA}, \mathcal{A} \sim \mathcal{B} \iff \mathcal{B} \models \varphi$

The following standard result relates similarity with language inclusion.

Proposition 2.12. *Let* $\mathcal{A}_1$ *and* $\mathcal{A}_2$ *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 timed bisimilarity

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 bisimilarity for ERA. We prove in this section that it is in general not possible to express timed

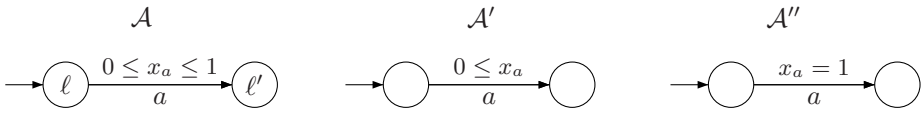

FIGURE 1. Three ERA $\mathcal{A}$, $\mathcal{A}'$ and $\mathcal{A}''$.

bisimilarity for ERA in the logic ERL. We also discuss which syntactic restrictions have to be imposed on ERA to allow ERL to characterize timed bisimilarity. Finally, we recall an attempt of such construction which can be found in Sorea's thesis [18] and detail why it is erroneous.

3.1. Impossibility Result for ERL

It would be rather easy to prove that the logic ERL cannot express timed bisimilarity for ERA with invariants, as this logic cannot quantify over time elapsing transitions independently of the firing of a discrete transition. We prove here a stronger result by showing that the logic ERL cannot express timed bisimilarity for two subclasses of $\mathrm{ERA}^{\mathrm{lazy}}$. As we will see, 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 3.1. *The logic* ERL *cannot express timed bisimilarity for* ERA. *More precisely,* ERL *cannot characterize timed bisimilarity for the classes* $\mathrm{ERA}^{\mathrm{lazy}}_{(d,\infty)}$ *and* $\mathrm{ERA}^{\mathrm{lazy}}_{(\infty,M)}$ *for any* $d, M \geq 1$.

Proof. We consider the ERA without invariants $\mathcal{A}$ and $\mathcal{A}'$ depicted in Figure 1. We will prove that there exists no ERL formula characterizing $\mathcal{A}$ (resp. $\mathcal{A}'$) up to timed bisimilarity among the class $\mathrm{ERA}^{lazy}_{(\infty,1)}$ (resp. $\mathrm{ERA}^{lazy}_{(1,\infty)}$). By contradiction, we assume that there exists a formula $\varphi \in$ ERL characterizing the ERA, and then proceed in the two following steps:

(1) use the underlying untimed structure of the ERA to transform φ into a formula with a simpler structure,
(2) build an ERA which is not timed bisimilar to the original ERA, but still satisfies φ.

To simplify the presentation, we assume that $\mathcal{A}$ and $\mathcal{A}'$ are defined over the alphabet restricted to letter a, but the result would hold for any alphabet.

(1) **Simplification of the formula φ.** Consider a formula Φ such that X is a free variable of Φ. As usual with the Kozen's μ-calculus, the semantics $[\![\Phi]\!]^{\mathcal{B}}_{\mathcal{V}}$ of formula Φ can be viewed as a function $[\![\Phi(X)]\!]^{\mathcal{B}}_{\mathcal{V}} : 2^Q \to 2^Q$ which maps a subset of Q into another subset of Q. According to the definition of the semantics of ERL, it is easy to verify that such a function is monotonic over the complete lattice 2^Q. By Knaster-Tarski theorem,

we have the following equalities:

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

$$\text{where } \begin{cases} [\![\Phi^0(\mathtt{ff})]\!]^{\mathcal{B}}_{\mathcal{V}} = [\![\mathtt{ff}]\!]^{\mathcal{B}}_{\mathcal{V}} = \emptyset \\ [\![\Phi^0(\mathtt{tt})]\!]^{\mathcal{B}}_{\mathcal{V}} = [\![\mathtt{tt}]\!]^{\mathcal{B}}_{\mathcal{V}} = Q \\ [\![\Phi^{i+1}(\lambda)]\!]^{\mathcal{B}}_{\mathcal{V}} = [\![\Phi(X)]\!]^{\mathcal{B}}_{\mathcal{V}[X:=[\![\Phi^i(\lambda)]\!]^{\mathcal{B}}_{\mathcal{V}}]} \end{cases} \quad \text{with } \lambda \in \{\mathtt{ff},\mathtt{tt}\}, \text{ and } i \in \mathbb{N}$$

As mentioned 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 restrict 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 $\mathcal{A}$ and $\mathcal{A}'$), we can replace in φ the fixpoint operators by the above equations with index i ranging over the set $\{0,1,2\}$. We denote by Unfold_1 this operation, and by $\mathrm{ERA}_{\mathrm{depth}\leq 1}$ the set of ERA whose maximal depth is smaller or equal to 1. Then, we have:

$$\forall \mathcal{B} \in \mathrm{ERA}_{\mathrm{depth}\leq 1},\ \mathcal{B} \models \varphi \iff \mathcal{B} \models \mathit{Unfold}_1(\varphi) \tag{3.1}$$

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 disjunctive 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 $[\cdot]$. Consider now the case of the ERA $\mathcal{A}$ (the case of $\mathcal{A}'$ is similar). As $\mathcal{A}$ 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 Φ_j, we can suppose that there exists an index p such that a formula Φ_j has as outermost operator the operator $\langle\cdot\rangle$ if and only if $j \leq p$. These last transformations can be done similarly for $\mathcal{A}'$.

(2) **Construction of an ERA $\mathcal{B}$.** In this second part, we prove the existence of an ERA which is not bisimilar to $\mathcal{A}$ (resp. to $\mathcal{A}'$), but which satisfies the ERL formula. This ERA is defined over $\Sigma = \{a\}$ and contains exactly two locations, denoted respectively ℓ_1 and ℓ_1', such that the first one is initial. We denote by $q_0^{\mathcal{B}} = (\ell_1, 0)$ the initial configuration of $\mathcal{B}$.

- *Case of $\mathcal{A}$.* We detail the construction of an ERA $\mathcal{B} \in \mathrm{ERA}^{\mathrm{lazy}}_{(\infty,1)}$. In the sequel, we will define a finite set of rational numbers $\mathcal{F} \subseteq \mathbb{Q}_{\geq 0} \cap [0,1]$. We add exactly 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 necessarily exists some point in the interval $[0,1]$ that does not belong to $\mathcal{F}$. We now detail how

[5] The maximal depth of an ERA denotes the length of a longest sequence of consecutive edges.

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 ξ_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 independently of the delay after which the a-labelled edge is fired, the configuration reached is the same. As the constraint g_j is defined with rational numbers and as the constraint of the edge between ℓ and ℓ' is $0 \leq x_1 \leq 1$, 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* φ. As the maximal depth of $\mathcal{B}$ is 1, and using property (3.1), it is sufficient to prove that for any j, we have $\mathcal{B}, q_0^{\mathcal{B}} \models \Phi_j$. First consider formulae Φ_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 edge 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 ℓ' and ℓ'_1. Second, we consider a formula Φ_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 $\mathcal{B}, (\ell'_1, 0) \models \xi_j$.

- *Case of* $\mathcal{A}'$. We now detail the construction of an ERA $\mathcal{B}' \in \mathrm{ERA}^{\mathrm{lazy}}_{(1,\infty)}$. As above, we can write, for each $1 \leq j \leq p$, $\Phi_j = \langle g_j, a\rangle \xi_j$ for some constraint g_j and formula ξ_j. We denote by M the maximal constant appearing in some constraint g_j. Then, we add to $\mathcal{B}'$ a single edge (ℓ_1, g, a, ℓ'_1) with g defined as $0 \leq x_a \leq \lfloor M \rfloor + 1$. Note that we have in particular $M < \lfloor M \rfloor + 1$.
  It is then easy to verify that all existential formulae Φ_j, with $j \leq p$, are satisfied, due to the choice of M, and that all universal formulae Φ_j, $j > p$, are satisfied because all behaviours of $\mathcal{B}'$ do exist in $\mathcal{A}'$.

Finally, we have proved that there exists $\mathcal{B} \in \mathrm{ERA}^{\mathrm{lazy}}_{(\infty,1)}$ such that $\mathcal{B} \models \varphi$ holds while $\mathcal{A}$ and $\mathcal{B}$ are not timed bisimilar, thus yielding a contradiction (similarly for $\mathcal{B}' \in \mathrm{ERA}^{\mathrm{lazy}}_{(1,\infty)}$ w.r.t. $\mathcal{A}'$). Thus, ERL cannot characterize timed bisimilarity among the subclasses $\mathrm{ERA}^{\mathrm{lazy}}_{(\infty,1)}$ $\mathrm{ERA}^{\mathrm{lazy}}_{(1,\infty)}$. □

3.2. When can ERL characterize timed bisimilarity?

On the granularity of constants. Consider first ERA without invariants as we will discuss this aspect in a second paragraph. We have proved in Theorem 3.1 that ERL cannot in general characterize ERA (without invariants) up to timed bisimilarity. Let us discuss how the nature of constants used in ERA impacts on this result. We consider in this paper a general model of ERA which allows any non-negative rational number (sometimes constants are restricted to natural

numbers). Theorem 3.1 establishes two settings in which ERL fails to characterize timed bisimilarity:

(1) if constants allowed include (bounded) rational numbers with arbitrarily large denominators (class $\mathrm{ERA}^{\mathrm{lazy}}_{(\infty,1)}$),
(2) if constants allowed include unbounded natural numbers (class $\mathrm{ERA}^{\mathrm{lazy}}_{(1,\infty)}$).

In particular, point (2) proves that ERL is not expressive enough for the (standard) setting of ERA involving natural numbers only.

To complete this picture, we will prove a positive result in Subsection 5.3. We establish that for any fixed granularity (d, M), the logic ERL can characterize the class $\mathrm{ERA}^{\mathrm{lazy}}_{(d,M)}$ up to timed bisimilarity. Intuitively, this results follows from the fact that all automata of the class $\mathrm{ERA}^{\mathrm{lazy}}_{(d,M)}$ share a common set of regions. Then the ERL formula expresses timed bisimilarity based on these regions.

On the role of invariants. As ERL quantifies simultaneously on delay transitions and on discrete transitions, it cannot distinguish two ERA which would only differ by the possible delay transitions. To avoid this difficulty, one could introduce a weaker definition of timed bisimilarity, in which any delay transition must be followed by a discrete transition. We believe that such a definition would allow to extend the results presented in the previous paragraph to ERA with invariants.

3.3. On the construction proposed in [18]

In [18], the author addresses the problem of constructing characteristic bisimilarity formulae for ERA with integer constants and 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 $\mathcal{A} = \langle L, \ell_0, \Sigma, E\rangle$, a location $\ell \in L$ and a letter $a \in \Sigma$, we define:

- the set of a-labelled edges leaving ℓ:
  $\mathsf{Out}(\ell, a) = \{(\ell, g, a', \ell') \in E \mid a = a'\}$
- the disjunction of clock constraints of a-labelled edges leaving ℓ:
  $\mathsf{En}(\ell, a) = \bigvee\{g \mid \exists(\ell, g, a, \ell') \in \mathsf{Out}(\ell, a)\}$
- the set of locations reached by an a from location ℓ:
  $\mathsf{F}(\ell, a) = \{\ell' \mid \exists(\ell, g, a, \ell') \in \mathsf{Out}(\ell, a)\}$

The formulae defined in [18] 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:

$$\Phi^{\mathcal{A}}(\ell) \stackrel{\mathcal{D}}{=} \bigwedge_{a\in\Sigma} \left(\begin{array}{c} \bigwedge_{(\ell,g,a,\ell')\in\mathsf{Out}(\ell,a)} \langle g, a\rangle \Phi^{\mathcal{A}}(\ell') \\ \wedge[\mathsf{En}(\ell, a), a] \left(\bigvee_{\ell'\in\mathsf{F}(\ell,a)} \Phi^{\mathcal{A}}(\ell')\right) \\ \wedge[\neg\mathsf{En}(\ell, a), a]\mathtt{ff} \end{array} \right) \tag{3.2}$$

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 bisimilarity 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:

$$\Phi^{\mathcal{A}}(q) = \bigwedge_{a\in\Sigma} \left(\left(\bigwedge_{q \xrightarrow{a} q' \in \mathcal{A}} \langle a \rangle \Phi^{\mathcal{A}}(q') \right) \wedge \left([a] \bigvee_{q \xrightarrow{a} q' \in \mathcal{A}} \Phi^{\mathcal{A}}(q') \right) \right) \tag{3.3}$$

This is the way characteristic formulae for bisimilarity are defined for instance in [1, 12]. In the construction of [18], the first conjunct corresponds to the first part of (3.3) while the two other conjuncts correspond to the second part of (3.3). 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 occurring in $\mathsf{En}(\ell, a)$ correspond to some a-successor of ℓ. But the a-successors of ℓ may have different clock constraints, and thus should not be all 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 WT_μ, and that the second point can be solved using the region construction.

We provide a counter-example exhibiting the first aspect. Consider the two ERA $\mathcal{A}$ and $\mathcal{A}''$ depicted in Figure 1. It is easy to see that $\mathcal{A}$ and $\mathcal{A}''$ are not timed bisimilar. Let us write the characteristic formulae for $\mathcal{A}$ ($\Sigma = \{a\}$) according to (3.2):

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

We have $\mathcal{A}'' \models_{\mathcal{D}} \Phi^{\mathcal{A}}(\ell)$, which shows that the construction is not correct. More precisely, this is due to the incompleteness of the first part of the formula of (3.2).

To illustrate the second aspect, consider the two ERA depicted in Figure 2. It is easy to verify that $\mathcal{B}$ and $\mathcal{B}'$ are not timed bisimilar. However, the formulae for the ERA $\mathcal{B}$ according to (3.2) (with $\Sigma = \{a\}$) are:

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

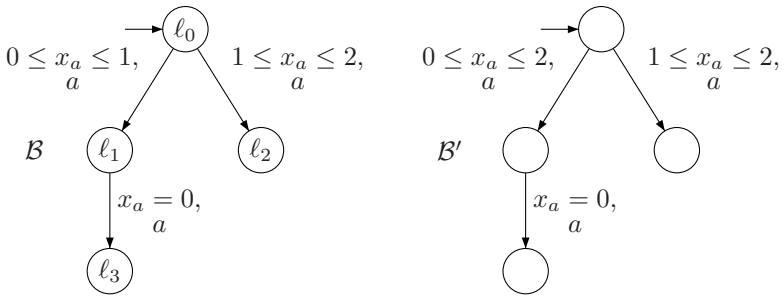

FIGURE 2. Non-bisimilarity because of overlapping edges.

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

4. A μ-calculus for Event-Recording Automata

We present here a weak timed μ-calculus for ERA that has been introduced in [13], and which is called WT_μ. This stands for *Weak Timed μ-calculus*, as it can be seen as a timed μ-calculus (as T_μ [10] or $\mathcal{L}_\nu$ [12]) 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 one to express timed (bi)similarity for ERA.

4.1. The Logic WT_μ

Definition 4.1 (Syntax)**.** Let Σ be a finite alphabet and Var be a finite set of variables. A formula φ of WT_μ 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, bound variable, and sentence.

Definition 4.2 (Semantics)**.** For a given ERA $\mathcal{A} = \langle L, \ell_0, \Sigma, E, I \rangle$ 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 formula, denoted by $[\![\varphi]\!]^{\mathcal{A}}_{\mathcal{V}}$, is

inductively defined as follows:

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

The cases of atomic and Boolean formulae are as in Definition 2.7. We also use shortcuts $[\Sigma]$ and $\langle\Sigma\rangle$ which respectively stand for $\bigwedge_{a\in\Sigma}[a]$ and $\bigvee_{a\in\Sigma}\langle a\rangle$.

Note that formulae of the form $[a]\mathtt{tt}$ or $[g]\mathtt{tt}$ (with g satisfiable) are equivalent to $\mathtt{tt}$, as their semantics are defined by an implication whose right-hand side is $\mathtt{tt}$.

4.2. Expressiveness

We start with the following definition:

Definition 4.3. Given two sentences φ and φ' in $\mathrm{ERL}\cup\mathrm{WT}_\mu$, we say that they are *equivalent* if and only if, for any ERA $\mathcal{A}$, we have $\mathcal{A}\models\varphi \iff \mathcal{A}\models\varphi'$.
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 4.4. *Given a sentence $\varphi\in$ ERL, we denote by $\hat{\varphi}$ the sentence of WT_μ 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 φ and $\hat{\varphi}$ are equivalent.*

Proof. Proceeding by induction on the length of the formula φ, the result directly follows from the definitions. □

We now prove the following theorem which states that, as expected, the logic WT_μ increases the expressive power of ERL:

Theorem 4.5. *The logic WT_μ is strictly more expressive than the logic* ERL *(even for* ERA *without invariants).*

Proof. First, Proposition 4.4 proves that the logic WT_μ is more expressive than the logic ERL.

Second, we have to prove that the converse is false. We will prove (Theorem 5.5) that it is possible to express timed bisimilarity for ERA in the logic WT_μ. Together with Theorem 3.1 which states that it is not possible to express in ERL timed bisimilarity for ERA, this yields the result. □

Note that this result holds for all subclasses of ERA that ERL cannot characterize up to timed bisimilarity. In particular, this entails that WT_μ is strictly

more expressive than ERL on the class of ERA involving only natural numbers, *i.e.* the class $\mathrm{ERA}_{(1,\infty)}$.

4.3. Model-Checking

We consider the model checking problem of WT_μ sentences on ERA models. This problem consists in deciding, given a WT_μ sentence φ and an ERA $\mathcal{A}$, whether the relation $\mathcal{A} \models \varphi$ holds. The rest of this section is devoted to the proof of the following theorem:

Theorem 4.6. *The Model-Checking problem of* WT_μ *on* ERA *is* EXPTIME*-complete, even for the fragment of* WT_μ *restricted to greatest fixpoints.*

EXPTIME*-hardness:* As WT_μ is more expressive than ERL, this result follows from the EXPTIME-hardness of the Model-Checking problem of ERL on ERA (see [18]). For the sake of completeness, and as this result is only sketched in [18], we present here a complete proof.

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 [7]. 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 α' instead, and moves left or right according to δ. 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 τ not in Σ. 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 is $x_{a_i} < x_{b_i} \wedge x_\tau = 1$ if $\alpha = a$, and g_i is $x_{a_i} > x_{b_i} \wedge x_\tau = 1$ 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 τ 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 τ. Finally, we use the following WT_μ formula, with only greatest fixpoints:

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

where 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 φ are polynomial in the sizes of $\mathcal{M}$ and w_0.

Remark 4.7. As in [2], the hardness proof could be done without diagonal constraints.

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

We first state the following Lemma:

Lemma 4.8. *Let Σ be a finite alphabet. Let $\mathcal{A} \in$ ERA, $\varphi \in \mathrm{WT}_\mu$ be a formula without fixpoint quantifier and let K denote the maximal integer constant of $\mathcal{A}$ and φ. Denote by $X_1, \ldots, X_n$ the free variables of φ 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 φ and consider the type of φ:

- $\varphi = \mathtt{tt}$ or $\varphi = \mathtt{ff}$. The result follows as $Q_{\mathcal{A}}$ and $\emptyset$ are both a union of regions.
- $\varphi = \varphi_1 \wedge \varphi_2$ or $\varphi = \varphi_1 \vee \varphi_2$. The result follows from the induction property as the set of union of regions is 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. □

This entails the following lemma:

Lemma 4.9. *Let Σ be a finite alphabet. Let $\mathcal{A} \in$ ERA, and φ be a sentence in WT_μ. Denote by K the maximal integer constant of $\mathcal{A}$ and φ. Then the semantics of φ 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 WT_μ are monotonic functions, Knaster-Tarski theorem implies that fixpoint formulae can be evaluated using formally infinite intersections and unions given by:

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

As $\emptyset$ and Q are both union of regions, Lemma 4.8 entails that the iterative evaluation of fixpoints leads also to union of regions. As the number of regions is finite, these evaluations terminate, returning also a union of regions. □

The proof of Lemma 4.9 thus shows that the model checking problem can be solved symbolically using regions. To obtain results on complexity issues, we reduce the model checking problem to an equivalent model checking problem for standard μ-calculus working on regions. Therefore, we define the semantics of WT_μ over $\mathcal{R}_K(\mathcal{A})$. The only operators for which the semantics is non standard are the following:

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

Then, we can prove the correctness of this semantics as in [10, 12]:

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

However, the semantics of WT_μ 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 formula φ. A predicate g is satisfied in a region (ℓ,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 [13].

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 φ 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 φ [19]. 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 WT_μ over ERA is in EXPTIME, with a precise time complexity.

5. Characteristic Formulae Constructions

We describe in this section characteristic formulae constructions in the logic WT_μ to express timed similarity and timed bisimilarity for ERA with invariants. In the sequel, we consider an ERA $\mathcal{A}=\langle L_\mathcal{A},\ell_0^\mathcal{A},\Sigma,E_\mathcal{A},I_\mathcal{A}\rangle$ over the alphabet

Σ. 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. $\mathsf{Split}(\ell, a)$ returns 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 edges leaving ℓ: $\forall i \in \{1, \ldots, n\}, \forall (\ell, g, a, \ell') \in E_{\mathcal{A}}, [\![g_i]\!] \subseteq [\![g]\!]$ 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 $2^{O(|\Sigma| \log K |\Sigma|)}$, 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 determinism implies that the clock constraints of a-labelled edges leaving ℓ are disjoint.

5.1. Characteristic Formulae for Timed Bisimilarity

Definition 5.1. We define a declaration $\mathcal{D}_{\sim\mathcal{A}}$ associating a formula to each location ℓ of $\mathcal{A}$, and consider the greatest solution of this system of fixpoint equations.

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

Note that the construction introduces as clock constraints formulae obtained by disjunctions and negations. They can be rewritten in the syntax of WT_μ using the property that $[g_1 \vee g_2]\varphi$ is equivalent to $[g_1]\varphi \wedge [g_2]\varphi$ (see [13]).

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. Finally, $\mathcal{C}_2$ and $\mathcal{C}_5$ handle the case of delay transitions.

Example 5.2. We illustrate this definition on the ERA $\mathcal{B}$ introduced in Section 3 to show that the construction of [18] is erroneous. This ERA is depicted in Figure 2. Applying the previous definition leads to the following equation for location ℓ_0:

$$\Phi^{\sim\mathcal{B}}(\ell_0) = \left\{ \begin{array}{lllll} & [0 \leq x_a \leq 1]\langle a\rangle\Phi^{\sim\mathcal{B}}(\ell_1) & \wedge & [1 \leq x_a \leq 2]\langle a\rangle\Phi^{\sim\mathcal{B}}(\ell_2) \\ \wedge & [0 \leq x_a < 1][a]\Phi^{\sim\mathcal{B}}(\ell_1) & \wedge & [x_a = 1][a](\Phi^{\sim\mathcal{B}}(\ell_1) \vee \Phi^{\sim\mathcal{B}}(\ell_2)) \\ \wedge & [1 < x_a \leq 2][a]\Phi^{\sim\mathcal{B}}(\ell_2) & \wedge & [2 < x_a][a]\mathtt{ff} \end{array} \right.$$

Observe the splitting of the constraint $0 \leq x_a \leq 2$, obtained by the decomposition Split. This corrects the corresponding constraint of the construction of [18] (see Section 3) which was $[0 \leq x_a \leq 2, a](\Phi^{\sim\mathcal{B}}(\ell_1) \vee \Phi^{\sim\mathcal{B}}(\ell_2))$.

Remark 5.3 (On the satisfiability of WT_μ)**.** In [13], the satisfiability problem is proved to be decidable for a large fragment of WT_μ, which contains restrictions on the nesting of operators. It is easy to verify that the characteristic formulae constructed above for ERA are, if the ERA do not contain invariants, elements of this fragment.

Remark 5.4 (On the size of characteristic formulae $\Phi^{\sim\mathcal{A}}$)**.** Due to the use of the operator Split, these characteristic 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 $\mathcal{A}$. Compared with the construction proposed in [1] which yields formulae whose size is linear in that of the automaton, this complexity may seam to be non-optimal. However, we believe that this exponential blow-up is not avoidable, and detail now why. Characteristic formulae of [1] compare the clock valuation with the guards of edges after the discrete firing, and can then conclude *a posteriori* which edges may have been fired. 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. This observation motivated the introduction of the Split operator, which underlies the worst-case exponential size. Moreover, note that this exponential blow-up has no consequences on the theoretical time complexity of timed bisimilarity checking (see Corollary 5.6), as formulae of linear size would lead to the same complexity.

The following result states the correctness of the previous construction.

Theorem 5.5. *Let $\mathcal{A}$ and $\mathcal{B}$ be two* ERA *over Σ and consider ℓ 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 5.5 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 2.9.

(*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 σ.

- If $\sigma = a \in \Sigma$. Then there exists a transition $(\ell, g, a, \ell') \in E_{\mathcal{A}}$ 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 hence $v'' = v'$, which 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 σ.

- 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 $\mathcal{B}, (m', v') \models_{\mathcal{D}_{\sim\mathcal{A}}} \bigvee_{(\ell, g', a, \ell') \in E_{\mathcal{A}} \mid [\![g]\!] \subseteq [\![g']\!]} \Phi^{\sim\mathcal{A}}(\ell')$. The second property of $\mathsf{Split}(\ell, a)$ implies, as $[\![g]\!]$ is not empty, that there exists a transition $(\ell, g', a, \ell') \in E_{\mathcal{A}}$ 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 $v'' = v[x_a := 0] = v'$, which 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 $\Rightarrow$. Recall that the characteristic formulae $\Phi^{\sim\mathcal{A}}(\ell)$ are defined as the greatest solution of a system of inequalities. Using the notion of coinduction [16], any solution of these inequalities also satisfies these formulae. We consider the assignment function $\mathcal{V}$ over the variables $\Phi^{\sim\mathcal{A}}(\ell)$ 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:

$$\forall \ell \in L_{\mathcal{A}}, [\![\Phi^{\sim\mathcal{A}}(\ell)]\!]^{\mathcal{B}}_{\mathcal{V}} \subseteq [\![\mathcal{D}_{\sim\mathcal{A}}(\Phi^{\sim\mathcal{A}}(\ell))]\!]^{\mathcal{B}}_{\mathcal{V}} \tag{5.1}$$

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 ξ of $\mathcal{D}_{\sim\mathcal{A}}(\Phi^{\sim\mathcal{A}}(\ell))$.

- *(i)* $\xi = [g]\langle a\rangle\Phi^{\sim\mathcal{A}}(\ell')$ for some transition $(\ell,g,a,\ell') \in E_{\mathcal{A}}$. We distinguish between whether this transition can be fired from the configuration (ℓ,v) or not. If it cannot be fired from (ℓ,v), 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 $(m',v') \in [\![\Phi^{\sim\mathcal{A}}(\ell')]\!]^{\mathcal{B}}_{\mathcal{V}}$.
- *(ii)* $\xi = [I_{\mathcal{A}}(\ell)]\Phi^{\sim\mathcal{A}}(\ell)$. 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.
- *(iii)* $\xi = [g][a]\bigvee_{(\ell,g',a,\ell') \in E_{\mathcal{A}} \mid [\![g]\!] \subseteq [\![g']\!]} \Phi^{\sim\mathcal{A}}(\ell')$, 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: $\mathcal{B},(m',v') \models_{\mathcal{D}_{\sim\mathcal{A}}} \bigvee_{(\ell,g',a,\ell') \in E_{\mathcal{A}} \mid [\![g]\!] \subseteq [\![g']\!]} \Phi^{\sim\mathcal{A}}(\ell')$. First, we have by bisimulation and time determinism that $(\ell,v) \xrightarrow{\delta} (\ell,v+\delta)$ exists in $\mathcal{A}$ and that $(\ell,v+\delta) \sim (m,v+\delta)$ holds. Bisimulation then implies 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 (ℓ,g',a,ℓ') in $E_{\mathcal{A}}$ 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 ξ. In particular, we thus have $\mathcal{B},(m',v') \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell')$, as required.
- *(iv)* $\xi = [\neg\mathsf{En}(\ell,a)][a]\mathtt{ff}$. By contradiction, assume that the property is not satisfied, that is, 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 $(\ell,v+\delta)$. This is in contradiction with $v+\delta \notin \mathsf{En}(\ell,a)$.

(v) $\xi = [\neg I_{\mathcal{A}}(\ell)]\mathtt{ff}$. By contradiction, assume that the property is not satisfied, that is, 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 $\mathcal{B}$. This is in contradiction with $v+\delta \not\models I_{\mathcal{A}}(\ell)$.

This concludes the proof of the property (5.1), and thus the second implication also holds.

This concludes the proof of Theorem 5.5. □

Corollary 5.6. *One can decide timed bisimilarity of two* ERA $\mathcal{A}$ *and* $\mathcal{B}$ *over* Σ *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 [8]), the proof of Theorem 4.6 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 characteristic formulae $\Phi^{\sim\mathcal{A}}$. □

Note that this complexity result is more precise than the EXPTIME complexity resulting from constructions proposed in [1]. For instance, for a fixed alphabet Σ and if constants are encoded in unary, then timed (bi)similarity of two ERA $\mathcal{A}$ and $\mathcal{B}$ can be checked in polynomial time. In other terms, there is no exponential blow-up in the size of the discrete structures of $\mathcal{A}$ and $\mathcal{B}$.

5.2. Characteristic Formulae for Timed Similarity

Definition 5.7. We define a declaration $\mathcal{D}_{\succ\mathcal{A}}$ associating a formula to each location ℓ of $\mathcal{A}$, and consider the greatest solution of this system of fixpoint equations.

$$\Phi^{\succ\mathcal{A}}(\ell) \overset{\mathcal{D}_{\succ\mathcal{A}}}{=} \left\{ \begin{array}{ll} & \bigwedge_{a\in\Sigma} \bigwedge_{(\ell,g,a,\ell')\in E_{\mathcal{A}}} [g]\langle a\rangle\ \Phi^{\succ\mathcal{A}}(\ell') \qquad (\mathcal{C}_1') \\ \wedge & \\ & [I_{\mathcal{A}}(\ell)]\ \Phi^{\succ\mathcal{A}}(\ell) \qquad (\mathcal{C}_2') \end{array} \right.$$

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

Theorem 5.8. *Let* $\mathcal{A}$ *and* $\mathcal{B}$ *be two* ERA *over* Σ *and consider* ℓ *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 5.5. As for bisimilarity, we obtain an EXPTIME procedure to decide timed similarity:

Corollary 5.9. *One can decide timed similarity of two* ERA $\mathcal{A}$ *and* $\mathcal{B}$ *over* Σ *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 5.10. *Given two* ERA $\mathcal{A}$ *and* $\mathcal{B}$*, the procedure checking timed similarity 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 edges of $\mathcal{B}'$ is then exponential in the size of $\mathcal{B}$. Using Proposition 2.12, 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.

5.3. A positive result for ERL

Following discussion of Subsection 3.2, we consider now the subclass of ERA with a fixed granularity. Let $(d, M) \in \mathbb{N}\times\mathbb{N}$, recall that we denote by $\mathrm{ERA}^{\mathrm{lazy}}_{(d,M)}$ the subclass of ERA composed of models without invariants and such that constants are bounded by M, and use denominators that divide d. We prove the following positive result:

Theorem 5.11. *Let* $(d, M) \in \mathbb{N}\times\mathbb{N}$*. The logic* ERL *can express timed (bi)similarity for the class* $\mathrm{ERA}^{\mathrm{lazy}}_{(d,M)}$.

Proof. Without loss of generality, we can multiply all constants by the same constant and end up with ERA using only integer constants. We thus consider the class $\mathrm{ERA}^{\mathrm{lazy}}_{(1,K)}$. Let $\mathcal{A} \in \mathrm{ERA}^{\mathrm{lazy}}_{(1,K)}$, we detail how we build a formula in ERL which characterizes all elements in $\mathrm{ERA}^{\mathrm{lazy}}_{(1,K)}$ which are timed bisimilar to $\mathcal{A}$. A similar approach can be used for timed similarity. It can first be checked that in our previous construction, WT_μ characteristic formulae used to express timed bisimilarity belong to the following grammar (recall that there are no invariants in $\mathcal{A}$):

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

where $g \in \mathcal{C}(\Sigma)$, $a \in \Sigma$ and $X \in \mathsf{Var}$. More precisely, g are either constraints associated with edges (case of $\mathcal{C}_1$), or constraints resulting from the Split operation (case of $\mathcal{C}_3$). In particular, these constraints only involve integer constants less or equal than K. As a consequence, the constraint g is equivalent to a union of regions, and hence the formula $[g]\varphi$ is equivalent to the formula $\bigwedge_{r|r\subseteq[\![g]\!]}[r]\varphi$,

where the operator $[r]$ is an abuse of notation, as we should use a clock constraint defining r instead.

Note that by Proposition 4.4, we can replace the WT_μ operator $[r][a]$ by the ERL operator $[r, a]$. It remains to handle the combination $[r]\langle a\rangle$, where r denotes a region. As the ERA we consider here have the same granularity, a transition is enabled in a valuation of a region r if and only if it is enabled in all the valuations of r. However, we can not replace formula $[r]\langle a\rangle\varphi$ by formula $\langle r\rangle\langle a\rangle\varphi$ as the first one is equivalent to $\mathtt{tt}$ for all valuations which have no time successors in r. We instead have the following informal equivalence:

$$(\ell, v) \models [r]\langle a\rangle\varphi \iff (\ell, v) \models [r]\mathtt{ff} \vee \langle r\rangle\langle a\rangle\varphi$$

Note that formula $[r]\mathtt{ff}$ requires that v has no time successors in r. But this last formula can not be expressed in ERL, and we can thus not obtain a direct translation. To solve this issue, we use a more complicated construction, by exhibiting one variable for each pair (ℓ, r) composed of a location and of a region, as it is done in [12]. This trick allows us to decide locally whether the valuation has time successors in a region r'. Indeed, this only depends on the current region r. The equation for variable $\Phi^{\sim\mathcal{A}}(\ell, r)$ is then:

$$\Phi^{\sim\mathcal{A}}(\ell, r) \overset{\mathcal{D}_{\sim\mathcal{A}}}{=} \left\{ \begin{array}{ll} & \displaystyle\bigwedge_{(\ell,g,a,\ell')\in E_\mathcal{A}} \ \bigwedge_{r'\in R_K(\Sigma)\mid r'\subseteq[\![g]\!]\wedge r\rightsquigarrow r'} \langle r', a\rangle\ \Phi^{\sim\mathcal{A}}(\ell', r'[x_a := 0]) \\ \wedge & \\ & \displaystyle\bigwedge_{a\in\Sigma}\bigwedge_{r'\in R_K(\Sigma)} [r', a] \bigvee_{(\ell,g',a,\ell')\in E_\mathcal{A}\mid r'\subseteq[\![g']\!]} \Phi^{\sim\mathcal{A}}(\ell', r'[x_a := 0]) \end{array} \right.$$

where the notation $r \rightsquigarrow r'$ means that the region r' is a time successor of the region r, and $r'[x_a := 0]$ denotes the region obtained from r' by resetting x_a. Note that we specify which region is reached when firing a discrete transition. We can then obtain the following equivalence, where $\mathcal{B} \in \mathrm{ERA}^{lazy}_{(1,K)}$ and (m, v) denotes a configuration of $\mathcal{B}$:

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

As a consequence, we obtain $\mathcal{A} \sim \mathcal{B} \iff \mathcal{B} \models_{\mathcal{D}_{\sim\mathcal{A}}} \Phi^{\sim\mathcal{A}}(\ell_0^\mathcal{A}, r_0)$, where r_0 is the unique region containing the initial valuation. We do not detail the proof of the above equivalence as it follows the lines of the proof of Theorem 5.5. □

Example 5.12. We illustrate this last result on the ERA $\mathcal{B}$ depicted in Figure 2. Compared with the WT_μ formula obtained for location ℓ_0 of this ERA in Example 5.2, the ERL formula for this location is obtained using more variables. For location ℓ_0, we distinguish one variable for each region. There are here 6 regions, which we denote by r_0, $r_{0,1}$, r_1, $r_{1,2}$, r_2 and r_∞, according to the associated intervals for clock x_a. We obtain for instance for the variable $\Phi^{\sim\mathcal{B}}(\ell_0, r_1)$ the following

equation:

$$\Phi^{\sim\mathcal{B}}(\ell_0, r_1) = \left\{ \begin{array}{lll} & \langle r_1, a\rangle \Phi^{\sim\mathcal{B}}(\ell_1, r_0) & \wedge \quad \langle r_1, a\rangle \Phi^{\sim\mathcal{B}}(\ell_2, r_0) \\ \wedge & \langle r_{1,2}, a\rangle \Phi^{\sim\mathcal{B}}(\ell_2, r_0) & \wedge \quad \langle r_2, a\rangle \Phi^{\sim\mathcal{B}}(\ell_2, r_0) \\ \wedge & [r_1, a](\Phi^{\sim\mathcal{B}}(\ell_1, r_0) \vee \Phi^{\sim\mathcal{B}}(\ell_2, r_0)) & \wedge \quad [r_{1,2}, a]\Phi^{\sim\mathcal{B}}(\ell_2, r_0) \\ \wedge & [r_2, a]\Phi^{\sim\mathcal{B}}(\ell_2, r_0) & \wedge \quad [r_\infty, a]\mathtt{ff} \end{array} \right.$$

Note that the resulting ERL formula is only correct for ERA without invariants, and with only integral constants bounded by 2, while the WT_μ formula holds for the whole class of ERA.

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 general in the logic ERL, we have introduced the new logic WT_μ, and have proved 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 WT_μ for the whole class of ERA with invariants.

Compared to existing results in [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 we state more precise complexity bounds. For instance, for a fixed alphabet Σ and if constants are encoded in unary, then timed (bi)similarity can be checked in polynomial time. Moreover, our algorithm for model checking WT_μ against ERA can be more efficient than going through $\mathcal{L}_\nu$ and timed automata as it involves only one copy of the event-clocks. Finally, our translation builds formulae in a subclass of WT_μ for which the satisfiability problem is decidable.

As future work, we plan to study how the fragment of WT_μ with a decidable satisfiability problem can be enlarged, for instance to be able to express controllability properties (as in [6]). We also envisage to adapt the implementation of the procedures of [1] done in the tool CMC [11] to this framework for ERA.

References

[1] L. Aceto, A. Ingólfsdóttir, M. L. Pedersen, and J. Poulsen. Characteristic formulae for timed automata. *RAIRO - Theor. Inf. Appl.*, 34(6):565–584, 2000.

[2] L. Aceto and F. Laroussinie. Is your model-checker on time? on the complexity of model checking for timed modal logics. *J. Log. Algebr. Program.*, 52–53:7–51, 2002.

[3] R. Alur and D. Dill. A theory of timed automata. *Theoret. Comput. Sci.*, 126(2):183–235, 1994.

[4] R. Alur, L. Fix, and T. A. Henzinger. Event-clock automata: A determinizable class of timed automata. *Theor. Comput. Sci.*, 211(1-2):253–273, 1999.

[5] H. Bekic. Definable operation in general algebras, and the theory of automata and flowcharts. In C. B. Jones, editor, *Programming Languages and Their Definition*, volume 177 of *LNCS*, pages 30–55. Springer, 1984.

[6] P. Bouyer, F. Cassez, and F. Laroussinie. Timed modal logics for real-time systems: Specification, verification and control. *J. Logic Lang. Inform.*, 20(2):169–203, 2011.
[7] A. K. Chandra, D. Kozen, and L. J. Stockmeyer. Alternation. *J. ACM*, 28(1):114–133, 1981.
[8] R. Cleaveland and B. Steffen. A linear-time model-checking algorithm for the alternation-free modal mu-calculus. *Form. Meth. Syst. Design*, 2(2):121–147, 1993.
[9] D. D'Souza. A logical characterisation of event clock automata. *Int. J. Found. Comput. Sci.*, 14(4):625–640, 2003.
[10] T. A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model-checking for real-time systems. *Inf. Comput.*, 111(2):193–244, 1994.
[11] F. Laroussinie and K. G. Larsen. CMC: A tool for compositional model-checking of real-time systems. In S. Budkowski, A. R. Cavalli, and E. Najm, editors, *Proc. Joint Conf. FORTE-PSTV'98*, volume 135 of *IFIP Conference Proceedings*, pages 439–456. Kluwer Academic, 1998.
[12] F. Laroussinie, K. G. Larsen, and C. Weise. From timed automata to logic – and back. In J. Wiedermann and P. Hájek, editors, *Proc. of 20th Int. Symp. on Mathematical Foundations of Computer Science*, volume 969 of *LNCS*, pages 529–539. Springer, 1995.
[13] O.-L. Nguena-Timo. *Synthèse pour une logique temps-réel faible*. PhD thesis, Université de Bordeaux, 2009.
[14] O.-L. Nguena-Timo and P.-A. Reynier. On characteristic formulae for event-recording automata. In *Proc. 6th Workshop on Fixed Points in Computer Science*, pages 70–78, 2009.
[15] J.-F. Raskin and P.-Y. Schobbens. The logic of event clocks - decidability, complexity and expressiveness. *J. Autom. Lang. Comb.*, 4(3):247–286, 1999.
[16] D. Sangiorgi. Bisimulation: From the origins to today. In H. Ganzinger, editor, *Proc. of 19th IEEE Symposium on Logic in Computer Science*, pages 298–302. IEEE Computer Society Press, 2004.
[17] M. Sorea. A decidable fixpoint logic for time-outs. In L. Brim, P. Jancar, M. Kretínský, and A. Kucera, editors, *Proc. of 13th Int. Conf. on Concurrency Theory*, volume 2421 of *LNCS*, pages 255–271. Springer, 2002.
[18] M. Sorea. *Verification of Real-Time Systems through Lazy Approximations*. PhD thesis, University of Ulm, 2004.
[19] W. Thomas. Languages, automata, and logic. In G. Rozenberg and A. Salomaa, editors, *Handbook of formal languages, vol. 3: beyond words*, pages 389–455. Springer, 1997.

Communicated by (The editor will be set by the publisher).
(The dates will be set by the publisher).