On Characteristic Formulae for Event-Recording Automata

Omer Landry Nguena Timo
LaBRI, Université Bordeaux I & CNRS
351 cours de la Libération,
F-33405 Talence Cedex, France
omer-landry.nguena-timo@labri.fr

Pierre-Alain Reynier
LIF, Université de Provence & CNRS
39 rue Joliot-Curie,
F-13453 Marseille Cedex 13, France
pierre-alain.reynier@lif.univ-mrs.fr

Abstract

A standard bridge between automata theory and logic is provided by the notion of characteristic formula. This paper investigates this problem for the class of event-recording automata. An attempt to express in Event-recording logic (ERL) characteristic formula for timed simulation and bisimulation can be found in Sorea's thesis, but appears to be erroneous. We introduce an extension of the logic ERL, called WT_μ. We prove it is strictly more expressive than ERL, and that its model-checking problem against event-recording automata is EXPTIME-complete. We provide constructions for characterizing event-recording automata up to timed bisimilarity, and timed similarity. Finally, combining these two results we obtain decision procedures for checking timed similarity and timed bisimilarity for event-recording automata and we study the complexity issues.

1 Introduction

In the untimed setting, automata and logics are central tools for the formal verification of reactive systems. While the system is usually modelled as an automaton, the specification may be described both as a formula of a logic or as an automaton. In the first case the correctness of the system reduces to a model checking problem, whereas in the second case it requires to compare the two automata, and different relations can be envisaged, such as bisimulation or language inclusion. A standard bridge between automata theory and logic is provided by the notion of *characteristic formula* [7, 14]. A characteristic formula is a formula in a temporal logic that completely characterizes the behaviour of an automaton modulo some chosen relation. For the class of timed automata [3], a solution has first been proposed in [8], providing formulae in greatest only fixpoint logic L_ν. Then, these results have been improved in [1], yielding linear constructions.

Event-recording automata (ERA) [4] and timed automata [3] are timed extension of finite automata through addition of a finite set of real-valued *clocks*. They have been put forward to model continuous-time real-time systems. Event-recording Automata is a restricted class of timed automata. Whereas transitions in (untimed) finite automata are labelled with actions, every transition in ERA and timed automata is labelled with a triplet made of a constraint on clocks, an action and a set of clocks to be reset when the transition is taken. In both timed models the time elapses continuously in states and the values of clocks do change accordingly. A transition is firable when the *clock constraint* in it is satisfied by the current values of clocks. Timed automata neither restrict clocks and actions in models, nor the set of clocks to be reset when transitions are taken. ERA considers a bijective mapping between the set of clocks and the set of actions; and when a transition is taken, only the unique clock associated to the action of the transition is reset. In the opposite of timed automata, ERA are closed under boolean operations [3]. It has thus attracted attention to characterize its expressive power in terms of some timed logic [11, 6], using linear-time logics. This paper investigates the problem of identifying a branching-time logic devoted to event-based specifications that allows to construct characteristic formulae for ERA. Sorea introduced such a logic, named Event-Recording Logic (ERL), which extends the fixpoint mu-calculus by allowing the use of event-clocks. However, the construction proposed in her PhD thesis [13] for bisimulation is erroneous, and we will see that ERL cannot express timed bisimilarity for ERA.

After recalling standard definitions in Section 2, we consider in Section 3 the fixpoint timed logic WT_μ [10], to express the characteristic formulae. The definition of this logic is closer from the definition of L_ν as it separates quantification over discrete successors and time successors. We prove that it is strictly more expressive than ERL, and that its model-checking problem over ERA is EXPTIME-complete. Finally, we provide formulae constructions in WT_μ for timed (bi)similarity together with complexity issues in Section 4. Then we present a bug in the ERL-based construction proposed in [13]. Due to lack of space, omitted proofs can be found in [9].

2 Preliminaries

Let Σ be a finite alphabet, Σ^* is the set of finite words over Σ. The sets $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{Q}_{\geq 0}$, $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ are respectively the sets of natural, rational, non-negative rational, real and non-negative real numbers. 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 $\mathscr{X}$ of variables, called *clocks*. A *clock valuation* over $\mathscr{X}$ is a mapping $v : \mathscr{X} \to \mathbb{T}$ that assigns to each clock a time value. The set of all clock valuations over X is denoted $\mathbb{T}^{\mathscr{X}}$. Let $t \in \mathbb{T}$, the valuation $v+t$ is defined by $(v+t)(x) = v(x)+t$, $\forall x \in \mathscr{X}$. For a subset r of $\mathscr{X}$, we denote by $v[r \leftarrow 0]$ the valuation such that for each $x \in r$, $(v[r \leftarrow 0])(x) = 0$ and for each $x \in \mathscr{X} \setminus r$, $(v[r \leftarrow 0])(x) = v(x)$. Finally, $\mathbf{0}$ denotes the valuation mapping every clock on 0.

Given a set of clocks $\mathscr{X}$, we introduce the sets of clock constraints over $\mathscr{X}$ denoted by $\mathscr{C}(\mathscr{X})$, and defined by the grammar "$g ::= x \sim c \mid g \wedge g$" where $x \in \mathscr{X}$, $c \in \mathbb{Q}_{\geq 0}$, $\sim \in \{<, \leq, =, \geq, >\}$ and we define the always true constraint $\mathfrak{tt} := \bigwedge_{x \in X} x \geq 0$. The set of *guards* over $\mathscr{X}$ is defined by the grammar " $\xi ::= g \mid \xi \vee \xi \mid \neg\xi$ " where g is a clock constraint over X. We write $v \models \xi$ (or $v \in [\![\xi]\!]$) when the clock valuation v satisfies ξ. The guard $\neg\xi$ stands for the negation of ξ: $v \in [\![\neg\xi]\!]$ iff $v \notin [\![\xi]\!]$.

2.1 Timed Transition Systems and Timed Behavioral Relations

Timed transition systems describe systems which combine discrete and continuous evolutions. They are used to define the behavior of timed systems [3, 4]. A *timed transition system (*TTS*)* over the alphabet Σ is a transition system $\mathscr{S} = \langle Q, q_0, \Sigma, \to \rangle$, where Q is the set of states, $q_0 \in Q$ is the initial state, and the transition relation $\to \subseteq Q \times (\Sigma \cup \mathbb{T}) \times Q$ consists of continuous transitions $q \xrightarrow{d} q'$ (with $d \in \mathbb{T}$), and discrete transitions $q \xrightarrow{a} q'$ (with $a \in \Sigma$). Moreover, we require the following standard properties for TTS: TIME-DETERMINISM (if $q \xrightarrow{d} q'$ and $q \xrightarrow{d} q''$ with $d \in \mathbb{R}_{\geq 0}$, then $q' = q''$), 0-DELAY ($q \xrightarrow{0} q$), ADDITIVITY (if $q \xrightarrow{d} q'$ and $q' \xrightarrow{d'} q''$ with $d,\ d' \in \mathbb{R}_{\geq 0}$, then $q \xrightarrow{d+d'} q''$), and CONTINUITY (if $q \xrightarrow{d} q'$, then for every d' and d'' in $\mathbb{R}_{\geq 0}$ such that $d = d' + d''$, there exists q'' such that $q \xrightarrow{d'} q'' \xrightarrow{d''} q'$). With these properties, a *run* of S is defined as a finite sequence of moves $\rho = q_0 \xrightarrow{d_0} q'_0 \xrightarrow{a_0} q_1 \xrightarrow{d_1} q'_1 \xrightarrow{a_1} q_2 \ldots \xrightarrow{a_n} q_{n+1}$ where discrete and continuous transitions alternate. To such a run corresponds the timed word $w = (a_i, \tau_i)_{0 \leq i \leq n}$ over Σ, where a_i occurs at time $\tau_i = \sum_{j=0}^{i} d_j$; and we say that w belong to the language of $\mathscr{S}$ denoted by $\mathscr{L}(\mathscr{S})$.

Definitions of timed simulation and timed bisimulation are given for TTS and they will be used for ERA. Consider two TTS $\mathscr{S}_1 = \langle Q_1, q_0^1, \Sigma, \to_1 \rangle$ and $\mathscr{S}_2 = \langle Q_2, q_0^2, \Sigma, \to_2 \rangle$. A *timed simulation between $\mathscr{S}_1$ and $\mathscr{S}_2$* is a relation $\mathscr{R} \subseteq Q_1 \times Q_2$ such that whenever $q_1 \mathscr{R} q_2$ and $\alpha \in \Sigma \cup \mathbb{T}$, then:

- If $q_1 \xrightarrow{\alpha} q'_1$ then there exists $q'_2 \in Q_2$ such that $q_2 \xrightarrow{\alpha} q'_2$ and $q'_1 \mathscr{R} q'_2$.

A *timed bisimulation between $\mathscr{S}_1$ and $\mathscr{S}_2$* is a relation $\mathscr{R} \subseteq Q_1 \times Q_2$ such that whenever $q_1 \mathscr{R} q_2$ and $\alpha \in \Sigma \cup \mathbb{T}$, then:

- If $q_1 \xrightarrow{\alpha} q'_1$ then there exists $q'_2 \in Q_2$ such that $q_2 \xrightarrow{\alpha} q'_2$ and $q'_1 \mathscr{R} q'_2$.

- If $q_2 \xrightarrow{\alpha} q_2'$ then there exists $q_1' \in Q_1$ such that $q_1 \xrightarrow{\alpha} q_1'$ and $q_1' \mathscr{R} q_2'$.

We write $q_1 \prec q_2$ (resp. $q_1 \sim q_2$) iff there exists a timed simulation (resp. a timed bisimulation) $\mathscr{R}$ with $q_1 \mathscr{R} q_2$. Finally, we say that *a* TTS $\mathscr{S}_2$ *simulates a* TTS $\mathscr{S}_1$ (resp. $\mathscr{S}_1$ *and* $\mathscr{S}_2$ *are bisimilar*) whenever there exists a timed simulation (resp. a timed bisimulation) between $\mathscr{S}_1$ and $\mathscr{S}_2$ such that the pair (q_0^1, q_0^2) of their initial states belongs to the relation $\mathscr{R}$, and then we write $\mathscr{S}_1 \prec \mathscr{S}_2$ (resp. $\mathscr{S}_1 \sim \mathscr{S}_2$).

2.2 Event-Recording Automata

We consider the class of Event-Recording Automata (ERA), introduced in [4]. In this context, each clock refers to a specific action. Then, we associate clocks with letters of an alphabet. Given an alphabet Σ, we then denote by $\mathscr{X}_\Sigma$ the set of clocks $\{x_a \mid a \in \Sigma\}$. Intuitively, in any configuration, the value of the clock x_a represents the delay elapsed since the last occurrence of the action a (or since the beginning of the run if no action a occurred yet).

An *event-recording automaton(*ERA*) [4]* over the alphabet Σ is a tuple $\mathscr{A} = \langle L, \ell_0, \Sigma, T \rangle$ where, L is a finite set of locations, $\ell_0 \in L$ is the initial location, and $T \subseteq L \times \mathscr{C}(\mathscr{X}_\Sigma) \times \Sigma \times L$ is a finite set of transitions. An ERA is deterministic if $[\![g' \wedge g'']\!] = \emptyset$ whenever (ℓ, g', a, ℓ') and (ℓ, g'', a, ℓ'').

The semantics of an event-recording automaton $\mathscr{A}$, is defined in the terms of a timed transition system. Intuitively, it manipulates exactly one clock per action, which allows to measure time elapsed since the last occurrence of this action. The formal definition is given by: given an ERA $\mathscr{A} = \langle L, \ell_0, \Sigma, T \rangle$, its semantics is given by the TTS $\mathscr{S}_\mathscr{A}$ defined by $\mathscr{S}_\mathscr{A} = \langle Q, q_0, \Sigma, \rightarrow \rangle$ where $Q = L \times \mathbb{T}^{\mathscr{X}_\Sigma}$, $q_0 = (\ell_0, \mathbf{0})$, and $\rightarrow$ consists of continuous and discrete moves:

Delay steps: $\forall d \in \mathbb{T}$, we have $(\ell, \nu) \xrightarrow{d} (\ell, \nu + d)$,

Discrete steps: $\forall a \in \Sigma$, we have $(\ell, \nu) \xrightarrow{a} (\ell', \nu')$ iff there exists a transition $t = (\ell, g, a, \ell') \in T$ such that $\nu \models g$ and $\nu' = \nu[x_a := 0]$.

The language of an ERA $\mathscr{A}$, denoted $\mathscr{L}(\mathscr{A})$, is the language $\mathscr{L}(\mathscr{S}_\mathscr{A})$ of its TTS $\mathscr{S}_\mathscr{A}$. A basic problem on ERA consists in testing the emptiness of its language. As $\mathscr{S}_\mathscr{A}$ is infinite, a standard solution is based on a finite time abstract bisimulation called the region construction [4]. We assume the reader is familiar with the *region construction* of [3] for timed automata. Given an integer K, we denote by $\mathscr{R}_K(\mathscr{A})$ the region automaton w.r.t. constant K. Recall that the number of clock regions for ERA on alphabet Σ and maximal constant K is in $2^{O(|\Sigma| \log K |\Sigma|)}$ (see [4]). A standard solution to the emptiness testing considers region automata w.r.t maximal constant that occurs in ERAs.

Let $\mathscr{A}$ and $\mathscr{B}$ be two ERA. We say that $\mathscr{A}$ *simulates* $\mathscr{B}$ and we write $\mathscr{A} \prec \mathscr{B}$, (resp. $\mathscr{A}$ *and* $\mathscr{B}$ *are bisimilar* and we write $\mathscr{A} \sim \mathscr{B}$) whenever there exists a timed simulation (resp. a timed bisimulation) between $\mathscr{S}_\mathscr{A}$ and $\mathscr{S}_\mathscr{B}$. It is standard that: if $\mathscr{A} \prec \mathscr{B}$, then $\mathscr{L}(\mathscr{A}) \subseteq \mathscr{L}(\mathscr{B})$; and, if $\mathscr{B}$ is deterministic and $\mathscr{L}(\mathscr{A}) \subseteq \mathscr{L}(\mathscr{B})$, then $\mathscr{A} \prec \mathscr{B}$.

Let $\mathscr{A}$ be an ERA. We say that a sentence φ is a characteristic formula for $\mathscr{A}$ if and only if, according to the behavioural relation considered, the following equivalence holds:

[Simulation:] $\forall \mathscr{B} \in \text{ERA}, \mathscr{A} \prec \mathscr{B} \iff \mathscr{B} \models \varphi$

[Bisimulation:] $\forall \mathscr{B} \in \text{ERA}, \mathscr{A} \sim \mathscr{B} \iff \mathscr{B} \models \varphi$.

Let us introduce some notations. Given an ERA $\mathscr{A} = \langle L, \ell_0, \Sigma, T \rangle$, a location $\ell \in L$ and a letter $a \in \Sigma$, we denote by $Out(\ell, a) = \{t = (\ell, g, a, \ell') \in T\}$, the set of a-labelled transitions leaving ℓ and we denote by $F(\ell, a) = \{\ell' \mid \exists (\ell, g, a, \ell') \in Out(\ell, a)\}$, the set of locations reached by an a from location ℓ. We also define the guard $En(\ell, a) = \bigvee \{g \mid \exists (\ell, g, a, \ell') \in Out(\ell, a)\}$, the disjunction of clock constraints of a-labelled transitions leaving ℓ.

3 A μ-calculus for Event-Recording Automata

We present here a weak timed μ-calculus for ERA that has been introduced in [10]. Its definition distinguishes between delay successors and discrete successors, as it is done in the logic L_ν for instance. We show that it is strictly more expressive than the logic ERL. We will show in the next section that it allows to express timed (bi)similarity for ERA while ERL does not.

3.1 The Logic WT_μ

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 $g \in \mathscr{C}(\mathscr{X}_\Sigma)$, $a \in \Sigma$ and $X \in Var$.

As for the logic ERL, the semantics is defined for TTS associated with ERA. We use auxiliary assignment functions, and the notions of free (bound) variable, sentence...

For a given ERA $\mathscr{A} = \langle L, \ell_0, \Sigma, T \rangle$ with associated TTS $\mathscr{S}_\mathscr{A} = \langle Q, q_0, \Sigma, \to \rangle$, a given formula $\varphi \in \mathrm{WT}_\mu$, and an assignment function $\mathscr{V} : Var \to \mathscr{P}(Q)$, we define the set of states satisfying the formula, denoted $[\![\varphi]\!]^\mathscr{A}_\mathscr{V}$, inductively as follows:

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

An ERA $\mathscr{A} = \langle L_\mathscr{A}, \ell_0^\mathscr{A}, \Sigma, T_\mathscr{A} \rangle$ is a model of a sentence φ, and we write $\mathscr{A} \models \varphi$ if $(\ell_0, \mathbf{0}) \in [\![\varphi]\!]^\mathscr{A}$. Note that the valuation in the subscript of $[\![]\!]$ is removed for sentences.

Let ξ, g_1, g_2 be three constraints such that $[\![\xi]\!] = [\![g_1]\!] \cup [\![g_2]\!]$. One [10] can show that $\langle \xi \rangle \varphi$ is equivalent to $\langle g_1 \rangle \varphi \vee \langle g_2 \rangle \varphi$ and $[\xi]\varphi$ is equivalent to $[g_1]\varphi \wedge [g_2]\varphi$. In consequence we can extend the syntax of WT_μ by allowing guards to occurs in the modalities $\langle\rangle$ and $[]$.

Remark ***(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 $\mathscr{D}(X)$ over the variables Var. $\mathscr{D}$ is then called a declaration, and the semantics associated with this definition is the largest solution of the system of inequations $X \subseteq \mathscr{D}(X)$ for any $X \in Var$. It can be proved (see [5]) that this presentation is equivalent. To specify the declaration used, we will add it as subscript of the satisfaction relation $\models$, writing $\mathscr{A}, q \models_\mathscr{D} X$.

3.2 Expressiveness and Model-Checking results

Relation with L_ν The logic L_ν over the finite set of clocks $\mathscr{X}$, the set of identifiers *Var*, and the set of events Σ is defined as the set of formulas generated by the following grammar[1]:
"$\varphi ::= \mathtt{tt} \mid \mathtt{ff} \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid x \underline{in} \varphi \mid x \bowtie c \mid \langle a \rangle \varphi \mid [a]\varphi \mid \langle \delta \rangle \varphi \mid [\delta]\varphi \mid X \mid \nu X.\varphi(X)$", where $a \in \Sigma$, $x \in \mathscr{X}$ is a clock variable, $c \in \mathbb{Q}_{\geq 0}$, X is a variable, and $\bowtie \in \{\leq, \geq, <, >\}$.

The logic L_ν allows for the recursive definition of formulas by including a set *Var* of variables. L_ν allows only the greatest fixpoint operator. A formula is interpreted over timed automata. Here, we adapt the interpretation on an ERA $\mathscr{A}$ with associated TTS $\mathscr{S}_\mathscr{A} = \langle Q, q_0, \Sigma, \rightarrow \rangle$. Formulas are interpreted over *states* of the form $(\ell, v) \in Q$ where ℓ is a location of $\mathscr{A}$, v is a valuation of clocks in $\mathscr{X}_\Sigma$. We only present the semantics for the non standard operators $x \bowtie c$, $\langle \delta \rangle$, $[\delta]$, and $x \underline{in} \varphi$:

- $[\![x_a \bowtie c]\!]^\mathscr{A}_\mathscr{V} := \{(\ell, v) \in Q \mid v(x_a) \bowtie c\}$
- $[\![[\delta]\varphi]\!]^\mathscr{A}_\mathscr{V} := \{(\ell, v) \in Q \mid \forall d \in \mathbb{T}, (\ell, v+d) \in [\![\varphi]\!]^\mathscr{A}_\mathscr{V}\}$
- $[\![\langle \delta \rangle \varphi]\!]^\mathscr{A}_\mathscr{V} := \{(\ell, v) \in Q \mid \exists d \in \mathbb{T} \text{ s.t. } (\ell, v+d) \in [\![\varphi]\!]^\mathscr{A}_\mathscr{V}\}$
- $[\![x_a \underline{in} \varphi]\!]^\mathscr{A}_\mathscr{V} := \{(\ell, v) \in Q \mid (\ell, v[x_a := 0]) \in [\![\varphi]\!]^\mathscr{A}_\mathscr{V}\}$

For ERA, the fragment of WT_μ without the least fixpoint operator is a fragment of L_ν [8]. This inclusion follows from the fact that the modal operators $[g]\varphi$, $\langle g \rangle \varphi$, $[a]\varphi$ and $\langle a \rangle \varphi$ of WT_μ are respectively equivalent to $[\delta](\neg g \vee \varphi)$[2], $\langle \delta \rangle (g \wedge \varphi)$, $[a](x_a \underline{in} \varphi)$ and $\langle a \rangle (x_a \underline{in} \varphi)$ of L_ν. As L_ν is a fragment of T_μ without the least fixpoint operator, we get that WT_μ is a fragment of T_μ, what justifies its name.

Relation with ERL We compare WT_μ with ERL. The syntax of ERL [12] is similar to the syntax of WT_μ, except that the modal operators for ERL are only of the form $\langle g, a \rangle$ or $[g, a]$. Their semantics is as follows:

- $[\![\langle g, a \rangle \varphi]\!]^\mathscr{A}_\mathscr{V} := \{(\ell, v) \in Q \mid \exists\, d \in \mathbb{T},\ \exists (\ell, g, a, \ell') \in T \text{ s.t. } v+d \models g \text{ and } (\ell', v+d[x_a := 0]) \in [\![\varphi]\!]^\mathscr{A}_\mathscr{V}\}$
- $[\![[g, a] \varphi]\!]^\mathscr{A}_\mathscr{V} := \{(\ell, v) \in Q \mid \forall\, d \in \mathbb{T}, \forall (\ell, g, a, \ell') \in T, v+d \models g \Rightarrow (\ell', v+d[x_a := 0]) \in [\![\varphi]\!]^\mathscr{A}_\mathscr{V}\}$

Theorem 1. WT_μ *is strictly more expressive than* ERL.

The inclusion of ERL in WT_μ is trivial (replace any operator $[g, a]$, resp. $\langle g, a \rangle$, by the two operators $[g][a]$, resp. $\langle g \rangle \langle a \rangle$). To show that WT_μ is strictly more expressive than the logic ERL, one may consider the formula $[0 \leq x_a \leq 1]\langle a \rangle$; this formula requires the existence of *some* discrete move with the event a in *all* the time instants at which the value of x_a is between 0 and 1; such an alternation of quantification cannot be expressed in ERL. An alternative proof can be found in [9].

Model-Checking Given an ERA $\mathscr{A}$ and a WT_μ sentence φ, the model-checking problem of $\mathscr{A}$ against φ consists in determining whether the relation $\mathscr{A} \models \varphi$ holds or not.

Theorem 2. *The model-checking problem for* ERA *against* WT_μ *sentences is EXPTIME-complete.*

EXPTIME membership can be deduced from the EXPTIME membership of the same problem for timed automata against L_ν [2]. More precisely, for an ERA $\mathscr{A}$ and a WT_μ formula φ, one can solve the problem in time $O((|\mathscr{R}_K(\mathscr{A})| \times |\varphi|)^{n+1})$, where K is the maximal constant in $\mathscr{A}$ and φ, and n is the number of alternations of greatest and least fixpoints quantifiers in φ. EXPTIME hardness follows from the EXPTIME hardness of the model-checking of ERA against ERL [13], as WT_μ extends ERL.

[1] This grammar is different, but equivalent to the one in [8]

[2] Note that the negation of a clock constraint is a disjunction of clock constraints, *i.e.* a guard.

4 Characteristic Formulae Constructions

In the sequel, we consider an ERA $\mathscr{A} = \langle L_{\mathscr{A}}, \ell_0^{\mathscr{A}}, \Sigma, T_{\mathscr{A}} \rangle$ over the alphabet Σ. Let $\ell \in L_{\mathscr{A}}$ and $a \in \Sigma$, we first introduce an operation, denoted $Split(\ell, a)$, related to the determinization of ERA. $Split(\ell, a)$ is a finite set of constraints $\{g_1, \ldots, g_n\} \subseteq \mathscr{C}(\mathscr{X}_\Sigma)$ such that: it partitions $En(\ell, a)$ meaning that $[\![\bigvee_i g_i]\!] = [\![En(\ell, a)]\!]$ and $\forall i \neq j, [\![g_i]\!] \cap [\![g_j]\!] = \emptyset$; and secondly, its elements "match" the clock constraints of a-labelled transitions leaving ℓ manning that $\forall i \in \{1, \ldots, n\}, \forall (\ell, g, a, \ell') \in T_{\mathscr{A}}, [\![g_i]\!] \subseteq [\![g]\!]$ 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 [3], and then be optimized using some merging operations on zones. It is worth noticing that in the worst case, the size of $Split(\ell, a)$ may be $|Out(\ell, a)| \times 2^{O(|\Sigma| \log K |\Sigma|)}$, with K the largest integer constant of $\mathscr{A}$ (due to the region construction). However, if the ERA $\mathscr{A}$ is deterministic, then its size is linear in the size of $Out(\ell, a)$. Indeed, the determinism implies that the clock constraints of a-labelled transitions leaving ℓ are disjoint.

4.1 Characteristic Formulae for Timed Bisimulation

A characteristic formula characterising a location of an ERA up to timed bisimilarity should offer a description of: all the actions from the alphabet that are enabled in the location; which node is entered by taking a given transition, together with the reset associated with it; and the fact that arbitrary delays are allowed in the location.

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

$$\Phi^{\sim\mathscr{A}}(\ell) \overset{\mathscr{D}_{\sim\mathscr{A}}}{=} \begin{cases} \bigwedge_{a\in\Sigma} \bigwedge_{(\ell,g,a,\ell')\in T_{\mathscr{A}}} [g]\langle a\rangle\, \Phi^{\sim\mathscr{A}}(\ell') \quad \wedge \quad [\mathtt{tt}]\Phi^{\sim\mathscr{A}}(\ell) & (\mathscr{C}_1) \\ \wedge & \\ \bigwedge_{a\in\Sigma} \bigwedge_{g\in Split(\ell,a)} [g][a] \bigvee_{(\ell,g',a,\ell')\in T_{\mathscr{A}} \mid [\![g]\!]\subseteq[\![g']\!]} \Phi^{\sim\mathscr{A}}(\ell') \quad \wedge \quad \bigwedge_{a\in\Sigma} [\neg En(\ell,a)][a]\mathtt{ff} & (\mathscr{C}_2) \end{cases}$$

We give some intuition on its definition. Let $\mathscr{B}$ be an ERA and analyze how the definition of $\Phi^{\sim\mathscr{A}}(\ell)$ constrains a location m of $\mathscr{B}$ that satisfies $\Phi^{\sim\mathscr{A}}(\ell)$. Assume that the current state in $\mathscr{S}_{\mathscr{A}}$ is (ℓ, v) and the current state in $\mathscr{S}_{\mathscr{B}}$ is (m, v).
The part $\mathscr{C}_1$ expresses the simulation constraints ($\mathscr{A} \prec \mathscr{B}$). The left-hand side of $\mathscr{C}_1$ is the sub-formula $\bigwedge_{a\in\Sigma}\bigwedge_{(\ell,g,a,\ell')\in T_{\mathscr{A}}}[g]\langle a\rangle\, \Phi^{\sim\mathscr{A}}(\ell')$ which requires that any discrete transition from (ℓ, v) also exists from (m, v); or more precisely, for any transition in $\mathscr{A}$ from (ℓ, v) and *for all delays* after which it is firable, *there exists* a corresponding transition from (m, v) leading to a related (bisimilar) state. The right hand-side of $\mathscr{C}_1$, $[\mathtt{tt}]\Phi^{\sim\mathscr{A}}(\ell)$, handles the case of delay transitions. Note that it would be easy to handle invariants in ERA. The part $\mathscr{C}_2$ requires any discrete transition from (m, v) to be related to some discrete transition from (ℓ, v); it also requires the target state of any discrete transition from (m, v) to be related to the target state of some discrete transition from (ℓ, v). The right-hand side of $\mathscr{C}_2$, $\bigwedge_{a\in\Sigma}[\neg En(\ell, a)][a]\mathtt{ff}$ states that a-transitions can happen from (m, v) only in the time instants at which a-transitions can happen from (ℓ, v). The left-hand side of $\mathscr{C}_2$,$\bigwedge_{a\in\Sigma}\bigwedge_{g\in Split(\ell,a)}[g][a]\bigvee_{(\ell,g',a,\ell')\in T_{\mathscr{A}} \mid [\![g]\!]\subseteq[\![g']\!]}\Phi^{\sim\mathscr{A}}(\ell')$ uses the decomposition $Split(\ell, a)$ of the guard $En(\ell, a)$ to express that any a-transition firable from (m, v) corresponds to some firable a-transition of (ℓ, v). In case of non determinism, the target state of an a-transition from (m, v) is non deterministically related to the target state of some a-transition from (ℓ, v); this choice is done according to the constraint satisfied by the valuation v. Note that the second property of the operator *Split* ensures the completeness of this construction.

Let us comment the size of the formulas. Due to the use of the operator *Split*, these formulae are in the worst case of size $|\mathscr{A}| \times 2^{O(|\Sigma| \log K |\Sigma|)}$, with K the largest integer constant of $\mathscr{A}$, whereas if $\mathscr{A}$

is deterministic, then their size is linear in the size of $\mathscr{A}$. We believe that this exponential blow-up is not avoidable, and detail why formulae of [1], which have a linear size, cannot be used directly in our context. In the second part of the formulae ($\mathscr{C}_2$), they indeed compare, after the discrete firing, the clock valuation with the guards of $\mathscr{A}$. As for ERA, when a discrete transition labelled by a is fired the clock x_a is reset, one can not recover the value of this clock x_a before the firing. We solve this problem by splitting the set $En(\ell,a)$ to determine which transitions of $\mathscr{A}$ were firable. Moreover, note that this exponential blow-up has no consequences on the theoretical time complexity of timed bisimilarity checking, as linear formulae would lead to the same complexity.

The following result states the correctness of the previous construction.

Theorem 3. *Let $\mathscr{A}$ and $\mathscr{B}$ be two* ERA *over Σ and consider ℓ and m two locations of $\mathscr{A}$ and $\mathscr{B}$ respectively. Then for any valuation $v \in \mathbb{T}^\Sigma$, we have : $(\ell,v) \sim (m,v) \iff \mathscr{B},(m,v) \models_{\mathscr{D}_{\sim\mathscr{A}}} \Phi^{\sim\mathscr{A}}(\ell)$*
In particular, we have: $\mathscr{A} \sim \mathscr{B} \iff \mathscr{B} \models_{\mathscr{D}_{\sim\mathscr{A}}} \Phi^{\sim\mathscr{A}}(\ell_0^{\mathscr{A}})$.

We only present a sketch of proof. It proceeds by double implication. The direct implication is proved by using the co-induction principle.in showing that, considering the assignment function $\mathscr{V}$ over the variables $\Phi^{\sim\mathscr{A}}(\ell)$ defined by $\mathscr{V}(\Phi^{\sim\mathscr{A}}(\ell)) = \{(m,v) \in Q_{\mathscr{B}} \mid (\ell,v) \sim (m,v)\}$ for any $\ell \in L_{\mathscr{A}}$, we have: $\forall \ell \in L_{\mathscr{A}}, [\![\Phi^{\sim\mathscr{A}}(\ell)]\!]^{\mathscr{B}}_{\mathscr{V}} \subseteq [\![\mathscr{D}_{\sim\mathscr{A}}(\Phi^{\sim\mathscr{A}}(\ell))]\!]^{\mathscr{B}}_{\mathscr{V}}$. This follows from an examination of the different conjuncts of $\Phi^{\sim\mathscr{A}}(\ell)$. Conversely, we consider the relation $\mathscr{R} \subseteq Q_{\mathscr{A}} \times Q_{\mathscr{B}}$ defined as $\mathscr{R} = \{((\ell,v),(m,v)) \mid \mathscr{B},(m,v) \models_{\mathscr{D}_{\sim\mathscr{A}}} \Phi^{\sim\mathscr{A}}(\ell)\}$ and show that it is a timed bisimulation. Intuitively conjunct $\mathscr{C}_1$ is used to prove that $\mathscr{R}$ is a timed simulation between $\mathscr{A}$ and $\mathscr{B}$, and $\mathscr{C}_2$ is used to prove that $\mathscr{R}^{-1}$ is a timed simulation between $\mathscr{B}$ and $\mathscr{A}$. □

Using our constructions, one can decide timed bisimilarity of two ERA $\mathscr{A}$ and $\mathscr{B}$ over Σ in time $|\mathscr{A}| \times |\mathscr{B}| \times 2^{O(|\Sigma| \log K|\Sigma|)}$ (K denotes the largest constant of $\mathscr{A}$ and $\mathscr{B}$). Using the previous theorem, this problem reduces to the model checking problem of $\mathscr{B}$ against formula $\Phi^{\sim\mathscr{A}}(\ell_0^{\mathscr{A}})$ under the declaration $\mathscr{D}_{\sim\mathscr{A}}$. Note that $\Phi^{\sim\mathscr{A}}$ contains only greatest fixpoints and thus is alternation-free. From the model-checking results, the time complexity of this problem is in $O(|\mathscr{R}_K(\mathscr{B})| \times |\Phi^{\sim\mathscr{A}}|)$.

The result follows from the size of $\mathscr{R}_K(\mathscr{B})$ and previous remarks on the size of the formulae $\Phi^{\sim\mathscr{A}}$.

4.2 Characteristic Formulae for Timed Simulation

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

$$\Phi^{\succ\mathscr{A}}(\ell) \overset{\mathscr{D}_{\succeq\mathscr{A}}}{=} \bigwedge_{a\in\Sigma} \bigwedge_{(\ell,g,a,\ell')\in T} [g]\langle a\rangle\, \Phi^{\succ\mathscr{A}}(\ell') \quad \wedge \quad [\mathtt{tt}]\, \Phi^{\succ\mathscr{A}}(\ell) \qquad (\mathscr{C}_1')$$

This construction leads to formulae of *size linear* in the size of $\mathscr{A}$. Observe that $\mathscr{C}_1'$ is just $\mathscr{C}_1$ in the formula for timed bisimulation. The following result states the correctness of the previous construction.

Theorem 4. *Let $\mathscr{A}$ and $\mathscr{B}$ be two* ERA *over Σ and consider ℓ and m two locations of $\mathscr{A}$ and $\mathscr{B}$ respectively. Then for any valuation $v \in \mathbb{T}^\Sigma$, we have : $(\ell,v) \prec (m,v) \iff \mathscr{B},(m,v) \models_{\mathscr{D}_{\succ\mathscr{A}}} \Phi^{\succ\mathscr{A}}(\ell)$*
In particular, we have: $\mathscr{A} \prec \mathscr{B} \iff \mathscr{B} \models_{\mathscr{D}_{\succ\mathscr{A}}} \Phi^{\succ\mathscr{A}}(\ell_0^{\mathscr{A}})$

The proof is similar to that of Theorem 3. As for bisimilarity, one can decide timed similarity of two ERA $\mathscr{A}$ and $\mathscr{B}$ over Σ in time $|\mathscr{A}| \times |\mathscr{B}| \times 2^{O(|\Sigma| \log K|\Sigma|)}$ (K denotes the largest constant of $\mathscr{A}$ and $\mathscr{B}$). Moreover, using the determinization procedure for ERA, this procedure can also be used to decide in EXPTIME the language inclusion between two ERA $\mathscr{A}$ and $\mathscr{B}$ (first determinize $\mathscr{B}$, and then check timed simulation). Note that the problem of language inclusion is PSPACE-complete [4], thus this procedure is not optimal. However, the known algorithm 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.

4.3 Reporting a Bug in [13]

In [13], the author addresses the problem of constructing characteristic bisimulation formulae for ERA using ERL formulae with greatest fixpoints. In Section 3, we established that the formula $[0 \leq x_a \leq 1]\langle a\rangle \mathtt{tt}$ is not equivalent to any ERL formula. In general, WT_μ formulae having a sequence of the form $[g]\langle a\rangle\varphi$ [3][4] are not equivalent to some ERL formula. In the above subsection, characteristic formulae for timed bisimulation and timed simulation involve such kind of sequences. This is intuitively the reason why the construction in [13] is erroneous. More generally, using the same idea, we prove in [9]:

Theorem 5. *The logic* ERL *can not express neither timed bisimilarity nor timed similarity for* ERA.

We only give here a sketch of the proof. We consider an ERA $\mathscr{A}$ composed of two locations and a single edge labelled by a, with the constraint $0 \leq x_a \leq 1$. The proof proceeds by contradiction and assumes the existence of an ERL formula φ characterizing $\mathscr{A}$ up to timed bisimilarity. As we can suppose that φ is guarded (see [12]), it is possible to unfold the fixpoints of φ, and restrict the unfolding to depth 2 (because of the structure of $\mathscr{A}$). Then, the formula contains no more fixpoints, and can be rewritten in conjunctive normal form ($\bigwedge_i \varphi_i$). We finally build an ERA $\mathscr{B}$ with two locations, as $\mathscr{A}$, that has strictly less behaviours than $\mathscr{A}$, thus is not bisimilar to $\mathscr{A}$, but which satisfies φ. Therefore we pick for each φ_i whose outermost modality is of the form $\langle g, a\rangle$ a rational number r in g, and add a transition in $\mathscr{B}$ with constraint $x_a = r$. We can then verify that all formulae φ_i are satisfied by $\mathscr{B}$. □

5 Conclusion

We focused on the construction of characteristic formulae for ERA up to timed (bi)similarity with respect to WT_μ. We also reported a bug in an early construction with the setting of ERL.

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

As future work, we plan to study how the good decidability results of the satisfiability problem for ERL transfer to WT_μ. Such decidability results could be useful for the supervisory control of real-time systems with non controlability assumptions. Ongoing work in that direction are promising.

References

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

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

[3] R. Alur and D. Dill. A theory of timed automata. *Theor. 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.

[3] The action a should be firable in all the timing context at which g is satisfied.

[4] When modelling real-time reactive systems, a could represent an uncontrollable event from the environment.

[5] H. Bekic. Definable operation in general algebras, and the theory of automata and flowcharts. In C. B. Jones, ed., *Programming Languages and Their Definition*, v. 177 of *Lect. Notes in Comput. Sci.*, pp. 30–55. Springer, 1984.

[6] D. D'Souza. A logical characterisation of event clock automata. *Int. J. of Found. of Comput. Sci.*, 14(4):625–640, 2003.

[7] S. Graf and J. Sifakis. A modal characterization of observational congruence on finite terms of CCS. *Inform. and Control*, 68(1-3):125–145, 1986.

[8] F. Laroussinie, K. G. Larsen, and C. Weise. From timed automata to logic—and back. In J. Wiedermann, P. Hájek, eds., *Proc. of 20th Int. Symp. on Math. Found. of Comput. Sci., MFCS '95 (Prague, Aug./Sept. 1995)*, v. 969 of *Lect. Notes in Comput. Sci.*, pp. 529–539. Springer, 1995.

[9] O. Nguena and P.-A. Reynier. On characteristic formulae for event-recording automata. Research report HAL-00383203, HAL, CNRS, 2009.

[10] O. L. Nguena Timo. The logic WTμ. Technical report RR-1460-09, LaBRI, 2009.

[11] J.-F. Raskin and P.-Y. Schobbens. The logic of event clocks—decidability, complexity and expressiveness. *J. of Autom., Lang. and Combinat.*, 4(3):247–286, 1999.

[12] M. Sorea. A decidable fixpoint logic for time-outs. In L. Brim et al., eds., *Proc. of 13th Int. Conf. on Concurrency Theory, CONCUR 2002 (Brno, Aug. 2002)*, v. 2421 of *Lect. Notes in Comput. Sci.*, pp. 255–271. Springer, 2002.

[13] M. Sorea. *Verification of Real-Time Systems through Lazy Approximations*. PhD thesis, Univ. Ulm, 2004.

[14] B. Steffen and A. Ingólfsdóttir. Characteristic formulae for processes with divergence. *Inform. and Comput.*, 110(1):149–163, 1994.