A Determinizable Class of Timed Automata

Rajeev Alur[1] Limor Fix[2*] Thomas A. Henzinger[2**]

[1] AT&T Bell Laboratories, Murray Hill, NJ
[2] Department of Computer Science, Cornell University, Ithaca, NY

Abstract. We introduce the class of *event-recording timed automata* (ERA). An event-recording automaton contains, for every event a, a clock that records the time of the last occurrence of a. The class ERA is, on one hand, expressive enough to model (finite) timed transition systems and, on the other hand, determinizable and closed under all boolean operations. As a result, the language inclusion problem is decidable for event-recording automata. We present a translation from timed transition systems to event-recording automata, which leads to an algorithm for checking if two timed transition systems have the same set of timed behaviors.

We also consider *event-predicting timed automata* (EPA), which contain clocks that predict the time of the next occurrence of an event. The class of *event-clock automata* (ECA), which contain both event-recording and event-predicting clocks, is a suitable specification language for real-time properties. We provide an algorithm for checking if a timed automaton meets a specification that is given as an event-clock automaton.

1 Introduction

Finite automata are instrumental for the modeling and analysis of many phenomena within computer science. In particular, automata theory plays an important role in the verification of concurrent finite-state systems [10, 16]. In the trace model for concurrent computation, a system is identified with its behaviors. Assuming that a behavior is represented as a sequence of states or events, the possible behaviors of a system can be viewed as a formal language, and the system can be modeled as an automaton that generates the language (a complex system is modeled as the product of automata that represent the component systems). Since the admissible behaviors of the system also constitute a formal language, the requirements specification can be given by another automaton (the adequacy of automata as a specification formalism is justified by the fact that competing formalisms such as linear temporal logic are no more expressive). The verification problem of checking that a system meets its specification,

* Supported in part by the Office of Naval Research under contract N00014-91-J-1219, the National Science Foundation under grant CCR-8701103, and by DARPA/NSF under grant CCR-9014363.

** Supported in part by the National Science Foundation under grant CCR-9200794 and by the United States Air Force Office of Scientific Research under contract F49620-93-1-0056.

then, reduces to testing language inclusion between two automata. The decision procedure for language inclusion typically involves the complementation of the specification automaton, which in turn relies upon determinization [9, 15].

To capture the behavior of a real-time system, the model of computation needs to be augmented with a notion of time. For this purpose, *timed automata* [3] provide a simple, and yet powerful, way of annotating state-transition graphs with timing constraints, using finitely many real-valued variables called *clocks*. A timed automaton, then, accepts *timed words*—strings in which each symbol is paired with a real-valued time-stamp. While the theory of timed automata allows the automatic verification of certain real-time requirements of finite-state systems [1, 3, 4, 8], and the solution of certain delay problems [2, 6], the general verification problem (i.e., language inclusion) is undecidable for timed automata [3]. This is because, unlike in the untimed case, the nondeterministic variety of timed automata is strictly more expressive than the deterministic variety. The notion of nondeterminism allowed by timed automata, therefore, seems too permissive, and we hesitate to accept timed automata as the canonical model for finite-state real-time computation [5].

In this paper, we obtain a determinizable class of timed automata by restricting the use of clocks. The clocks of an *event-clock automaton* have a fixed, predefined association with the symbols of the input alphabet (the alphabet symbols typically represent events). The *event-recording clock* of the input symbol a is a history variable whose value always equals the time of the last occurrence of a relative to the current time; the *event-predicting clock* of a is a prophecy variable whose value always equals the time of the next occurrence of a relative to the current time (if no such occurrence exists, then the clock value is undefined). Thus, unlike a timed automaton, an event-clock automaton does not control the reassignments of its clocks and, at each input symbol, all clock values of the automaton are determined solely by the input word. This property allows the determinization of event-clock automata, which, in turn, leads to a complementation procedure. Indeed, the class ECA of event-clock automata is closed under all boolean operations (timed automata are not closed under complement), and the language inclusion problem is decidable for event-clock automata.

While event-predicting clocks are useful for the specification of timing requirements, automata that contain only event-recording clocks (*event-recording automata*) are a suitable abstract model for real-time systems. We confirm this claim by proving that event-recording automata are as powerful as another popular model for real-time computation, *timed transition systems* [7]. A timed transition system associates with each transition a lower bound and an upper bound on the time that the transition may be enabled without being taken (many related real-time formalisms also use lower and upper time bounds to express timing constraints [13, 14]). A run of a timed transition system, then, is again a timed word—a sequence of time-stamped state changes. We construct, for a given timed transition system T with a finite set of states, an event-recording automaton that accepts precisely the runs of T. This result leads to an algorithm for checking the equivalence of two finite timed transition systems.

2 Event-clock Automata

Timed words and timed languages

We study formal languages of timed words.[3] A *timed word* $\bar{w}$ over an alphabet Σ is a finite sequence $(a_0, t_0)(a_1, t_1)\ldots(a_n, t_n)$ of symbols $a_i \in \Sigma$ that are paired with nonnegative real numbers $t_i \in \mathrm{R}^+$ such that the sequence $\bar{t} = t_1 t_2 \ldots t_n$ of time-stamps is nondecreasing (i.e., $t_i \leq t_{i+1}$ for all $0 \leq i < n$). Sometimes we denote the timed word $\bar{w}$ by the pair $(\bar{a}, \bar{t})$. A *timed language* over the alphabet Σ is a set of timed words over Σ. The boolean operations of union, intersection, and complement of timed languages are defined as usual. Given a timed language $\mathcal{L}$ over the alphabet Σ, the projection $\mathit{Untime}(\mathcal{L})$ is obtained by discarding the time-stamps: $\mathit{Untime}(\mathcal{L}) \subseteq \Sigma^*$ consists of all strings $\bar{a}$ for which there exists a sequence $\bar{t}$ of time-stamps such that $(\bar{a}, \bar{t}) \in \mathcal{L}$.

Automata with clocks

Timed automata are finite-state machines that are constrained with timing requirements so that they accept (or generate) timed words (and thus define timed languages); they were proposed in [3] as an abstract model for finite-state real-time systems. A timed automaton operates with finite control—a finite set of locations and a finite set of real-valued variables called *clocks*. Each edge between locations specifies a set of clocks to be reset (i.e., restarted). The value of a clock always records the amount of time that has elapsed since the last time the clock was reset: if the clock z is reset while reading the i-th symbol of a timed input word $(\bar{a}, \bar{t})$, then the value of z while reading the j-th symbol, for $j > i$, is $t_j - t_i$ (assuming that the clock z is not reset at any position between i and j). The edges of the automaton put certain arithmetic constraints on the clock values; that is, the automaton control may proceed along an edge only when the values of the clocks satisfy the corresponding constraints.

Each clock of a timed automaton, therefore, is a real-valued variable that records the time difference between the current input symbol and another input symbol, namely, the input symbol on which the clock was last reset. This association between clocks and input symbols is determined dynamically by the behavior of the automaton. An event-clock automaton, by contrast, employs clocks that have a tight, predefined, association with certain symbols of the input word. Suppose that we model a real-time system so that the alphabet symbols represent events of the system. In most cases, it will suffice to know, for each event, the time that has elapsed since the last occurrence of the event. For example, to model a delay of 1 to 2 seconds between the input and output events of a device, it suffices to use a clock z that records the time that has elapsed since the last input event, and require the constraint $1 < z < 2$ when the output event occurs. This observation leads us to the definition of clocks that have a fixed association with input symbols and cannot be reset arbitrarily.

[3] For the clarity of exposition, we limit ourselves to finite words. Our results can be extended to the framework of ω-languages.

Event-recording and event-predicting clocks

Let Σ be a finite alphabet. For every symbol $a \in \Sigma$, we write x_a to denote the *event-recording clock* of a. Given a timed word $\bar{w} = (a_0, t_0)(a_1, t_1) \dots (a_n, t_n)$, the value of the clock x_a at the j-th position of $\bar{w}$ is $t_j - t_i$, where i is the largest position preceding j such that a_i equals a. If no occurrence of a precedes the j-th position of $\bar{w}$, then the value of the clock x_a is "undefined," denoted by $\perp$. We write $\mathrm{R}_{\perp}^{+} = \mathrm{R}^{+} \cup \{\perp\}$ for the set of nonnegative real numbers together with the special value $\perp$. Formally, we define for all $0 \le j \le n$,

$$val(\bar{w}, j)(x_a) = \begin{cases} t_j - t_i & \text{if there exists } i \text{ such that } 0 \le i < j \text{ and } a_i = a \\ & \quad \text{and for all } k \text{ with } i < k < j,\ a_k \ne a, \\ \perp & \text{if } a_k \ne a \text{ for all } k \text{ with } 0 \le k < j. \end{cases}$$

That is, the event-recording clock x_a behaves exactly like an automaton clock that is reset every time the automaton encounters the input symbol a. The value of x_a, therefore, is determined by the input word, not by the automaton. Auxiliary variables that record the times of last occurrences of events have been used extensively in real-time reasoning, for example, in the context of model-checking for timed Petri nets [17], and in assertional proof methods [11, 14].

Event-recording clocks provide timing information about events in the past. The dual notion of event-predicting clocks provides timing information about future events. For every symbol $a \in \Sigma$, we write y_a to denote the *event-predicting clock* of a. At each position of the timed word $\bar{w}$, the value of the clock y_a indicates the time of the next occurrence of a relative to the time of the current input symbol; the special value $\perp$ indicates the absence of a future occurrence of a. Formally, we define for all $0 \le j \le n$,

$$val(\bar{w}, j)(y_a) = \begin{cases} t_i - t_j & \text{if there exists } i \text{ such that } j < i \le n \text{ and } a_i = a \\ & \quad \text{and for all } k \text{ with } j < k < i,\ a_k \ne a, \\ \perp & \text{if } a_k \ne a \text{ for all } k \text{ with } j < k \le n. \end{cases}$$

The event-predicting clock y_a can be viewed as an automaton clock that is reset, every time the automaton encounters the input symbol a, to a nondeterministic negative starting value, and checked for 0 at the subsequent occurrence of a.

We write C_{Σ} for the set $\{x_a, y_a \mid a \in \Sigma\}$ of event-recording and event-predicting clocks. For each position j of a timed word $\bar{w}$, the *clock-valuation function* $val(\bar{w}, j)$, then, is a mapping from C_{Σ} to $\mathrm{R}_{\perp}^{+}$. The clock constraints compare clock values to rational constants or to the special value $\perp$. Let $\mathrm{Q}_{\perp}$ denote the set of nonnegative rational numbers together with $\perp$. Formally, a *clock constraint* over the set C of clocks is a boolean combination of atomic formulas of the form $z \le c$ and $z \ge c$, where $z \in C$ and $c \in \mathrm{Q}_{\perp}$. The clock constraints over C are interpreted with respect to clock-valuation functions from C to $\mathrm{R}_{\perp}^{+}$: the atom $\perp = \perp$ evaluates to true, and all other comparisons that involve $\perp$ (e.g., $\perp \ge 3$) evaluate to false. For a clock-valuation function γ and a clock constraint ϕ, we write $\gamma \models \phi$ to denote that according to γ the constraint ϕ evaluates to true.

Syntax and semantics of event-clock automata

An event-clock automaton is a (nondeterministic) finite-state machine whose edges are annotated both with input symbols and with clock constraints over event-recording and event-predicting clocks. Formally, a *event-clock automaton* A consists of a finite input alphabet Σ, a finite set L of locations, a set $L_0 \subseteq L$ of start locations, a set $L_f \subseteq L$ of accepting locations, and a finite set E of edges. Each edge is a quadruple (ℓ, ℓ', a, ϕ) with a source location $\ell \in L$, a target location $\ell' \in L$, an input symbol $a \in \Sigma$, and a clock constraint ϕ over the clocks C_Σ.

Now let us consider the behavior of an event-clock automaton over the timed input word $\bar{w} = (a_0, t_0)(a_1, t_1)\ldots(a_n, t_n)$. Starting in one of the start locations and scanning the first input pair (a_0, t_0), the automaton scans the input word from left to right, consuming, at each step, an input symbol together with its time-stamp. In location ℓ scanning the i-th input pair (a_i, t_i), the automaton may proceed to location ℓ' and the $i+1$-st input pair iff there is an edge (ℓ, ℓ', a, ϕ) such that a equals the current input symbol a_i and $val(\bar{w}, i)$ satisfies the clock constraint ϕ. Formally, a *computation* of the event-clock automaton A over the timed input word $\bar{w}$ is a finite sequence

$$\ell_0 \xrightarrow{e_0} \ell_1 \xrightarrow{e_1} \ell_2 \xrightarrow{e_2} \cdots \xrightarrow{e_{n-1}} \ell_n \xrightarrow{e_n} \ell_{n+1}$$

of locations $\ell_i \in L$ and edges $e_i = (\ell_i, \ell_{i+1}, a_i, \phi_i) \in E$ such that $\ell_0 \in L_0$ and for all $0 \leq i \leq n$, $val(\bar{w}, i) \models \phi_i$; the computation is *accepting* if $\ell_{n+1} \in L_f$. The timed language $\mathcal{L}(A)$ defined by the event-clock automaton A, then, consists of all timed words $\bar{w}$ such that A has an accepting computation over $\bar{w}$. We write ECA for the class of timed languages that are definable by event-clock automata.

The event-clock automaton A is an *event-recording automaton* if all clock constraints of A contain only event-recording clocks; A is an *event-predicting automaton* if the clock constraints of A contain only event-predicting clocks. The class of timed languages that can be defined by these two restricted types of event-clock automata are denoted ERA and EPA, respectively.

Examples of event-clock automata

The event-clock automaton A_1 of Figure 2 uses two event-recording clocks, x_a and x_b. The location ℓ_0 is the start location of A_1, and also the sole accepting location. The clock constraint $x_a < 1$ that is associated with the edge from ℓ_2 to ℓ_3 ensures that c occurs within 1 time unit of the preceding a. A similar mechanism of checking the value of x_b while reading d ensures that the time difference between b and the subsequent d is always greater than 2. Thus, the timed language $\mathcal{L}(A_1)$ defined by A_1 consists of all timed words of the form $((abcd)^m, \bar{t})$ such that $m \geq 0$ and for all $0 \leq j < m$, $t_{4j+2} < t_{4j} + 1$ and $t_{4j+3} > t_{4j+1} + 2$. Note that the timed language $\mathcal{L}(A_1)$ can also be defined using event-predicting clocks: require $y_c < 1$ while reading a, and $y_d > 2$ while reading b.

The duality of the two types of clocks is further illustrated by the automata of Figure 2. The event-recording automaton A_2 accepts all timed words of the

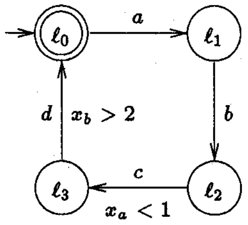
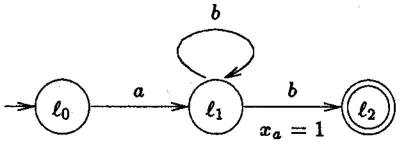


Fig. 1. Event-recording automaton A_1



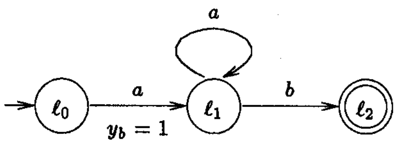


Fig. 2. Event-recording automaton A_2 and event-predicting automaton A_3

form $(ab^*b, \bar{t})$ such that the time difference between the two extreme symbols is 1, which is enforced by the event-recording clock x_a. It is easy to check that there is no event-predicting automaton that defines the timed language $\mathcal{L}(A_2)$. The event-predicting automaton A_3, on the other hand, accepts all timed words of the form $(aa^*b, \bar{t})$ such that the time difference between the two extreme symbols is 1; for this purpose, the event-predicting clock y_b is used to predict the time of the first b. There is no event-recording automaton that defines $\mathcal{L}(A_3)$.

3 Deterministic Event-clock Automata

A finite-state machine (with a single start location) is deterministic iff all input symbols that label edges with the same source location are pairwise distinct. We consider for event-clock automata the notion of determinism that was proposed for timed automata in [3]. The event-clock automaton $A = (\Sigma, L, L_0, L_f, E)$ is *deterministic* if A has a single start location (i.e., $|L_0| = 1$) and any two edges with the same source location and the same input symbol have mutually exclusive clock constraints; that is, if $(\ell, \ell', a, \phi_1) \in E$ and $(\ell, \ell'', a, \phi_2) \in E$ then for all clock-valuation functions γ, if $\gamma \models \phi_1$ then $\gamma \not\models \phi_2$. The determinism condition ensures that at each step during a computation, the choice of the next edge is uniquely determined by the current location of the automaton, the input word, and the current position of the automaton along the input word. It is easy to check that every deterministic event-clock automaton has at most one computation over any given timed input word.

Of our examples from the previous section, the event-clock automata A_1 and A_3 are deterministic. While the automaton A_2 is nondeterministic, it can be determinized without changing its language, by adding the clock constraint $x_a < 1$ to the self-loop at location ℓ_1.

In the theory of finite-state machines, it is well-known that every nondeterministic automaton can be determinized; that is, the deterministic and nondeterminstic varieties of finite-state machines define the same class of languages (the regular languages). In the case of timed automata, however, the nondeterministic variety is strictly more expressive than its deterministic counterpart [3]. We now show that the event-clock automata form a determinizable subclass of the timed automata.

Theorem 1 (Determinization). *For every event-clock (event-recording; event-predicting) automaton A, there is a deterministic event-clock (event-recording; event-predicting) automaton that defines $\mathcal{L}(A)$.*

Proof. Let A be the given event-clock automaton with the location set L. The locations of the determinized automaton $Det(A)$ are the nonempty subsets of L. Consider a location $L' \subseteq L$ of $Det(A)$, and an input symbol $a \in \Sigma$. Let $E' \subseteq E$ be the set of all a-labeled edges of A whose source locations are in L'. Then, for every nonempty subset $E'' \subseteq E'$, there is an edge from L' to L'' labeled with the input symbol a and the clock constraint ϕ iff L'' contains precisely the target locations of the edges in E'', and ϕ is the conjunction of all clock constraints of E''-edges and all negated clock constraints of $(E' - E'')$-edges. It is easy to check that the clock constraints on different a-labeled edges starting from L' are mutually exclusive. ■

Notice that the determinization of an event-clock automaton causes an exponential blow-up in the number of locations, but changes neither the number of clocks nor the constants that occur in clock constraints.

The key for the determinization of event-clock automata is the property that at each step during a computation, all clock values are determined solely by the input word. We therefore obtain derminizable superclasses of event-clock automata if we add more clocks that do not violate this property. For example, for each input symbol a and each natural number i, we could employ a clock z_a^i that records the time since the i-th occurrence of a, and a clock x_a^i that records the time since the i-th-to-last occurrence of a (i.e., $x_a = x_a^1$). Or, more ambitiously, we may want to use for each linear temporal formula φ a *formula-recording clock* x_φ that measures the time since the last position of the input word at which φ was true, and a *formula-predicting clock* y_φ that measures the time until the next position at which φ will be true.

4 Properties of Event-Clock Automata

Event-clock automata as labeled transition systems

We now consider an alternative semantics for event-clock automata, using labeled transition systems. Let $A = (\Sigma, L, L_0, L_f, E)$ be an event-clock automaton. A *state* of A is a pair (ℓ, γ) that consists of a location $\ell \in L$ and a clock-valuation function γ from C_Σ to $\mathrm{R}_\perp^+$, which determines the values of all clocks. The state (ℓ, γ) is *initial* if $\ell \in L_0$ and $\gamma(x_a) = \perp$ for all input symbols $a \in \Sigma$; (ℓ, γ) is *final* if $\ell \in L_f$ and $\gamma(y_a) = \perp$ for all $a \in \Sigma$. We write S_A for the (infinite) set of states of the event-clock automaton A and define a labeled transition relation over S_A to capture the behavior of A over timed words.

For two states $s, s' \in S_A$, an input symbol $a \in \Sigma$, and a real-valued time delay $\delta \in \mathrm{R}^+$, let $s \xrightarrow{a} s'$ if the automaton A may proceed from the state s to the state s' by reading the input symbol a, and let $s \xrightarrow{\delta} s'$ if A may proceed from s to s' by letting time δ pass. Formally, $(\ell, \gamma) \xrightarrow{a} (\ell', \gamma')$ if there is a clock-valuation function γ'' and an edge $(\ell, \ell', a, \phi) \in E$ such that $\gamma = \gamma''[y_a := 0]$ (i.e., γ agrees with γ'' on all clocks except y_a, which in γ evaluates to 0), $\gamma' = \gamma''[x_a := 0]$, and $\gamma \models \phi$; and $(\ell, \gamma) \xrightarrow{\delta} (\ell', \gamma')$ if $\ell = \ell'$ and for all input symbols $b \in \Sigma$,

1. if $\gamma(x_b) = \perp$ then $\gamma'(x_b) = \perp$, else $\gamma'(x_b) = \gamma(x_b) + \delta$;
2. if $\gamma'(y_b) = \perp$ then $\gamma(y_b) = \perp$, else $\gamma(y_b) = \gamma'(y_b) + \delta$.

We inductively extend the labeled transition relation to timed words: $s \xrightarrow{(a_0, t_0)} s'$ if there is a state $s'' \in S_A$ such that $s \xrightarrow{t_0} s''$ and $s'' \xrightarrow{a_0} s'$; if $\bar{w} = (a_0, t_0) \ldots (a_n, t_n)$ and $\bar{w}' = \bar{w}(a_{n+1}, t_{n+1})$, then $s \xrightarrow{\bar{w}'} s'$ if there is a state s'' such that $s \xrightarrow{\bar{w}} s''$ and $s'' \xrightarrow{(a_{n+1}, t_{n+1} - t_n)} s'$. The following lemma shows the correctness of the labeled-transition-system semantics for event-clock automata.

Lemma 2. *The event-clock automaton A accepts the timed word $\bar{w}$ iff $s \xrightarrow{\bar{w}} s'$ for some initial state s and some final state s' of A.*

The region construction

The analysis of timed automata builds on the so-called region construction, which transforms a timed automaton into an untimed finite-state machine [1, 3]. Here we apply the region construction to event-clock automata. We consider again the given event-clock automaton A and begin with defining the region-equivalence relation $\cong_A$ as a finite partition of the infinite state space S_A.

We assume that all clock constraints of A contain only integer constants (otherwise, all constants need to be multiplied by the least common multiple of the denominators of all rational numbers that appear in the clock constraints of A). Let c be the largest integer constant that appears in a clock constraint of A. Informally, two clock-valuation functions γ and γ' from C_Σ to $\mathrm{R}_\perp^+$ are *region-equivalent*, written $\gamma \cong_A \gamma'$, if γ and γ' agree on which clocks have the undefined value $\perp$, agree on the integral parts of all defined clock values that are at most c, and agree on the ordering of the fractional parts of all defined clock values (the fractional part of the event-recording clock x_a according to γ is $\gamma(x_a) - \lfloor \gamma(x_a) \rfloor$; the fractional part of the event-predicting clock y_a is $\lceil \gamma(y_a) \rceil - \gamma(y_a)$). Two states $(\ell, \gamma), (\ell', \gamma') \in S_A$ are *region-equivalent* if $\ell = \ell'$ and $\gamma \cong_A \gamma'$. A formal definition of the region-equivalence relation $\cong_A$ is given in [3].

A *region* of the event-clock automaton A is an $\cong_A$-equivalence class of states in S_A. The number of A-regions is finite—linear in the number of locations, exponential in the number of clocks (that is, exponential in the size of the input alphabet), and exponential in the size of the clock constraints of A. The region equivalence is instrumental for analyzing event-clock automata, because $\cong_A$ is a bisimulation.

Lemma 3. *For all states $s_1, s_1', s_2 \in S_A$ of an event-clock automaton A, all input symbols a of A, and all real-valued time delays $\delta \in \mathrm{R}^+$, if $s_1 \cong_A s_1'$ and $s_1 \xrightarrow{(a,\delta)} s_2$, then there is a state $s_2' \in S_A$ and a time delay $\delta' \in \mathrm{R}^+$ such that $s_2 \cong_A s_2'$ and $s_1' \xrightarrow{(a,\delta')} s_2'$.*

Now we are ready to define the *region automaton* $Reg(A)$ of A, an untimed finite-state machine over the input alphabet Σ. The locations of $Reg(A)$ are the regions of A. A region is starting if it contains an initial state of A, and accepting if it contains a final state of A. There is an edge from the region ρ to the region ρ' labeled with the input symbol a if there are two states $s \in \rho$ and $s' \in \rho'$, and a time delay $\delta \in \mathrm{R}^+$, such that $s \xrightarrow{(a,\delta)} s'$. From Lemmas 2 and 3 it follows that the region automaton $Reg(A)$ defines the untimed language $Untime(\mathcal{L}(A))$.

Theorem 4 (Untiming). *For every event-clock automaton A, the untimed language $Untime(\mathcal{L}(A))$ is regular.*

Closure properties and decision problems

While the class of timed automata is not closed under complement, and the language inclusion (verification) problem for timed automata is undecidable, the subclass of event-clock automata is well-behaved.

Theorem 5 (Closure properties). *Each of the classes* ECA, ERA, *and* EPA *of timed languages are closed under union, intersection, and complement.*

Proof. Closure under union is trivial, because event-clock automata admit multiple start locations. Closure under intersection is also straightforward, because the standard automata-theoretic product construction $A_1 \times A_2$ for two given event-clock (event-recording; event-predicting) automata A_1 and A_2 yields an event-clock (event-recording; event-predicting) automaton. Closure under complement relies on the determinization construction: given an event-clock (event-recording; event-predicting) automaton A, the event-clock (event-recording; event-predicting) automaton $\neg Det(A)$ that results from complementing the acceptance condition of $Det(A)$ (interchange the accepting and the nonaccepting states of $Det(A)$) defines the complement of the timed language $\mathcal{L}(A)$. ∎

Unlike (nondeterministic) timed automata, however, event-clock automata are not closed under hiding and renaming of input symbols. This is because the timed language $\mathcal{L}$ that contains all timed words $\bar{w} = (\bar{a}, \bar{t})$ over a unary alphabet in which no two symbols occur with time difference 1 (i.e., $t_j - t_i \neq 1$ for all positions i and j of $\bar{w}$) cannot be defined by a timed automaton [3]. With complementation and renaming (or hiding), on the other hand, $\mathcal{L}$ is easily definable from a language in ERA $\cap$ EPA.

The determinization, closure properties, and region construction can be used to solve decision problems for event-clock automata. To check if the timed language of an event-clock automaton A is empty, we construct the region automaton $Reg(A)$ and check if the untimed language of $Reg(A)$ is empty. To check if the language of the event-clock automaton A_1 is included in the language of the event-clock automaton A_2, we determinize A_2, complement $Det(A_2)$, take the product with A_1, and check if the language of the resulting event-clock automaton $A_1 \times \neg Det(A_2)$ is empty by constructing the corresponding region automaton.

Theorem 6 (Language inclusion). *The problem of checking if $\mathcal{L}(A_1) \subseteq \mathcal{L}(A_2)$ for two event-clock automata A_1 and A_2 is decidable in PSPACE.*

On the other hand, the problem of checking if the language of a given event-recording (or event-predicting) automaton is empty can be shown to be PSPACE-hard (similar to the hardness proof for emptiness of timed automata [3]).

Relationship between classes of timed automata

We briefly review the definition of a timed automaton [3]. A (nondeterministic) *timed automaton* A consists of a finite input alphabet Σ, a finite set L of locations, a set $L_0 \subseteq L$ of start locations, a set $L_f \subseteq L$ of accepting locations, a finite set C of clocks, and a finite set E of edges. Each edge e is labeled with an input symbol, a clock constraint over C, and a *reset condition* $C_e \subseteq C$ that specifies the clocks that are reset to 0 when the edge e is traversed. Every timed automaton A, then, defines a timed language $\mathcal{L}(A)$, and we write NTA for the class of timed languages that are definable by timed automata. The class NTA is closed under union and intersection, but not under complement.

The definition of determinism for timed automata is the same as for event-clock automata. We write DTA for the class of timed languages that are definable by deterministic timed automata. Since DTA is closed under all boolean operations, DTA is strictly contained in NTA.

Theorem 7 (Relationship between classes).

(1) ERA $\not\subseteq$ EPA (2) EPA $\not\subseteq$ ERA (3) ERA $\cup$ EPA $\subset$ ECA
(4) ECA $\subset$ NTA (5) ERA $\subset$ DTA (6) EPA $\not\subseteq$ DTA
(7) DTA $\not\subseteq$ ECA

Proof. For (1), the language of the event-recording automaton A_2 of Figure 2 is not definable by an event-predicting automaton. For (2), the language of the event-predicting automaton A_3 of Figure 2 cannot be defined by an event-recording automaton. Similarly, for (3) it is possible to combine A_2 and A_3 into an event-clock automaton whose language is neither in ERA nor in EPA.

Every event-clock automaton can be tranlated into a timed automaton. While the translation preserves determinism for event-recording automata, event-predicting clocks introduce nondeterminism. The inclusions (4) and (5) follow. Inclusion (4) is strict, because ECA is closed under complement while NTA is not. Inclusion (5) is strict because of (7). For (6), the timed language $\{(a^n b, t_0 \ldots t_n) \mid \exists 0 \leq i < n. t_n - t_i = 1\}$ is in EPA but not in DTA. For (7), the timed language $\{(aaa, t_0 t_1 t_2) \mid t_2 - t_0 = 1\}$ is in DTA but not in ECA. ■

In [5], we defined another subclass of NTA that is closed under all boolean operations, namely, the class 2DTA of timed languages that are definable by deterministic twoway automata that can read the input word a bounded number of times. While ECA is easily seen to be contained in 2DTA, and while there are obvious similarities between event-predicting clocks and the twoway reading of the timed input word, the exact relationship between event-clock automata and deterministic twoway automata remains to be studied. However, because they admit nondeterminism, event-clock automata are perhaps more suited for specification than deterministic twoway automata.

5 Timed Transition Systems as Event-clock Automata

Timed transition systems

A *transition system* T consists of a set S of states, a set $S_0 \subseteq S$ of initial states, and a finite set $\mathcal{T}$ of transitions. Each transition $\tau \in \mathcal{T}$ is a binary relation over S. For each state $s \in S$, the set $\tau(s)$ gives the possible τ-successors of s; that is, $\tau(s) = \{s' \mid (s, s') \in \tau\}$. The transition system T is *finite* if the set S of states is finite. A *run* $\bar{s}$ of the transition system T is a finite sequence $s_0 \rightarrow s_1 \rightarrow \cdots \rightarrow s_n$ of states such that $s_0 \in S_0$ and for all $0 \leq i < n$, there exists a transition $\tau_i \in \mathcal{T}$ such that $s_{i+1} \in \tau_i(s_i)$. The transition τ is *enabled* at the i-th step of the run $\bar{s}$ if $\tau(s_i)$ is nonempty, and τ is *taken* at the i-th step if $s_i \in \tau(s_{i-1})$ (i.e., multiple transitions may be taken at the same step). A variety of programming systems, such as message-passing systems and shared-memory systems, can be given a transition-system semantics [12].

The model of transition systems is extended to timed transition systems so that it is possible to express real-time constraints on the transitions [7]. A *timed transition system* T consists of a transition system $(S, S_0, \mathcal{T})$ and two functions l and u from $\mathcal{T}$ to R^+ that associate with each transition $\tau \in \mathcal{T}$ a *lower bound* $l(\tau)$ and an upper bound $u(\tau)$. Informally, the transition τ must be enabled continuously for at least $l(\tau)$ time units before it can be taken, and τ must not be enabled continuously for more than $u(\tau)$ time units without being taken. Formally, we associate a real-valued time-stamp with each state change along a run. A *timed run* $\bar{r}$ of the timed transition system T is a finite sequence

$$\xrightarrow{t_0} s_0 \xrightarrow{t_1} s_1 \xrightarrow{t_2} \cdots \xrightarrow{t_n} s_n$$

of states $s_i \in S$ and nondecreasing time-stamps $t_i \in \mathrm{R}^+$ such that $\bar{s}$ is a run of the underlying transition system and

1. *Upper Bound*: if τ is enabled at all steps k for $i \leq k < j$, and not taken at all steps k for $i < k < j$, then $t_j - t_i \leq u(\tau)$;
2. *Lower Bound*: if τ is taken at the j-th step then there is some step $i < j$ such that $t_j - t_i \geq l(\tau)$ and τ is enabled at all steps k for $i \leq k < j$, and not taken at all steps k for $i < k < j$.

In other words, t_0 is the initial time, and the transition system proceeds from the state s_i to the state s_{i+1} at time t_{i+1}. The semantics of the timed transition system T is the set of timed runs of T. Two timed transition systems are *equivalent* if they have the same timed runs.

From timed transition systems to event-recording automata

We now show that the set of timed runs of a finite timed transition system can be defined by an event-recording automaton. For this purpose, we need to switch from the state-based semantics of transition systems to an event-based semantics. With the given timed run $\bar{r}$, we associate the timed word

$$\bar{w}(\bar{r}) \;=\; (\langle \perp, s_0\rangle, t_0)\; (\langle s_0, s_1\rangle, t_1)\; (\langle s_1, s_2\rangle, t_2)\; \ldots\; (\langle s_{n-1}, s_n\rangle, t_n),$$

where $\perp$ is a special symbol not in S (as usual, $S_\perp = S \cup \{\perp\}$). Notice that the timed run $\bar{r}$ and the corresponding timed word $\bar{w}(\bar{r})$ contain the same information: each event (i.e., state change) of $\bar{r}$ is modeled by a pair of states—a source state and a target state. Every finite timed transition system $T = (S, \mathcal{T}, S_0, l, u)$, then, defines a timed language $\mathcal{L}(T)$ over the alphabet $S_\perp \times S$, namely, the set of timed words $\bar{w}(\bar{r})$ that correspond to timed runs $\bar{r}$ of T. It is easy to check that two timed transition systems are equivalent iff they define the same timed language.

Theorem 8 (Timed transition systems). *For every finite timed transition system T, there is an event-recording timed automaton A_T that defines the timed language $\mathcal{L}(T)$.*

Proof. Consider the given finite timed transition system T. Each location of the corresponding event-clock automaton A_T records a state $s \in S$ and, for each transition $\tau \in \mathcal{T}$, a pair of states $\langle \alpha(\tau), \beta(\tau)\rangle \in S_\perp \times S$ such that if τ is enabled in s, then τ has been enabled continuously without being taken since the last state change from $\alpha(\tau)$ to $\beta(\tau)$. In addition, we use a special location ℓ_0 as the sole start location of A_T. Every location is an accepting location.

For every initial state $s_0 \in S_0$, there is an edge from ℓ_0 to $(s_0, \langle \alpha, \beta\rangle)$ labeled with the input symbol $\langle \perp, s_0\rangle$ and the trivial clock constraint *true*, where $\alpha(\tau) = \perp$ and $\beta(\tau) = s_0$ for all transitions $\tau \in \mathcal{T}$. In addition, there is an edge from $(s, \langle \alpha, \beta\rangle)$ to $(s', \langle \alpha', \beta'\rangle)$ labeled with the input symbol $\langle s, s'\rangle$ and the clock constraint ϕ iff there is a transition $\tau \in \mathcal{T}$ such that $(s, s') \in \tau$, and for all transitions $\tau \in \mathcal{T}$,

1. if τ is enabled in s and $s' \notin \tau(s)$, then $\langle \alpha'(\tau), \beta'(\tau)\rangle = \langle \alpha(\tau), \beta(\tau)\rangle$, else $\langle \alpha'(\tau), \beta'(\tau)\rangle = \langle s, s'\rangle$;
2. if τ is enabled in s, then ϕ contains the conjunct $x_{\langle \alpha(\tau), \beta(\tau)\rangle} \leq u(\tau)$;
3. if $s' \in \tau(s)$, then ϕ contains the conjunct $x_{\langle \alpha(\tau), \beta(\tau)\rangle} \geq l(\tau)$.

Notice that the size of the event-recording automaton A_T is exponential in the size of the timed transition system T. ■

To check if two timed transition systems T_1 and T_2 are equivalent, we construct the corresponding event-recording automata A_{T_1} and A_{T_2} and check if they define the same timed language.

Corollary 9. *The problem of checking if two finite timed transition systems are equivalent is decidable in EXPSPACE.*

References

1. R. Alur, C. Courcoubetis, and D. Dill. Model-checking in dense real-time. *Information and Computation*, 104:2–34, 1993.
2. R. Alur, C. Courcoubetis, and T. Henzinger. Computing accumulated delays in real-time systems. In *Proceedings of the Fifth Conference on Computer-Aided Verification*, Lecture Notes in Computer Science 697, pages 181–193. Springer-Verlag, 1993.
3. R. Alur and D. Dill. Automata for modeling real-time systems. In *Proceedings of the 17th International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science 443, pages 322–335. Springer-Verlag, 1990.
4. R. Alur, T. Feder, and T. Henzinger. The benefits of relaxing punctuality. In *Proceedings of the Tenth ACM Symposium on Principles of Distributed Computing*, pages 139–152, 1991.
5. R. Alur and T. Henzinger. Back to the future: Towards a theory of timed regular languages. In *Proceedings of the 33rd IEEE Symposium on Foundations of Computer Science*, pages 177–186, 1992.
6. C. Courcoubetis and M. Yannakakis. Minimum and maximum delay problems in real-time systems. In *Proceedings of the Third Workshop on Computer-Aided Verification*, Lecture Notes in Computer Science 575, pages 399–409, 1991.
7. T. Henzinger, Z. Manna, and A. Pnueli. Temporal proof methodologies for real-time systems. In *Proceedings of the 18th ACM Symposium on Principles of Programming Languages*, pages 353–366, 1991.
8. T. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model-checking for real-time systems. In *Proceedings of the Seventh IEEE Symposium on Logic in Computer Science*, pages 394–406, 1992.
9. J. Hopcroft and J. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.
10. R. Kurshan. Reducibility in analysis of coordination. In *Lecture Notes in Computer Science*, volume 103, pages 19–39. Springer-Verlag, 1987.
11. N. Lynch and H. Attiya. Using mappings to prove timing properties. *Distributed Computing*, 6:121–139, 1992.
12. Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems.* Springer-Verlag, 1991.
13. M. Merritt, F. Modugno, and M. Tuttle. Time-constrained automata. In *Proceedings of the Workshop on Theories of Concurrency*, Lecture Notes in Computer Science 527, pages 408–423. Springer-Verlag, 1991.
14. F. Schneider, B. Bloom, and K. Marzullo. Putting time into proof outlines. In *Real-Time: Theory in Practice*, Lecture Notes in Computer Science 600, pages 618–639. Springer-Verlag, 1991.
15. A. Sistla, M. Vardi, and P. Wolper. The complementation problem for Büchi automata with applications to temporal logic. *Theoretical Computer Science*, 49:217–237, 1987.
16. P. Wolper, M. Vardi, and A. Sistla. Reasoning about infinite computation paths. In *Proceedings of the 24th IEEE Symposium on Foundations of Computer Science*, pages 185–194, 1983.
17. T. Yoneda, A. Shibayam, B. Schlingloff, and E. Clarke. Efficient verification of parallel real-time systems. In *Proceedings of the Fifth Conference on Computer-Aided Verification*, Lecture Notes in Computer Science 697, pages 321–332. Springer-Verlag, 1993.