arXiv:1504.07838v1 [cs.FL] 29 Apr 2015

Language Emptiness of Continuous-Time Parametric Timed Automata

Nikola Beneš[1⋆], Peter Bezděk[1⋆⋆], Kim G. Larsen[2], and Jiří Srba[2]

[1] Faculty of Informatics, Masaryk University Brno, Czech Republic
[2] Department of Computer Science, Aalborg University, Denmark

Abstract. Parametric timed automata extend the standard timed automata with the possibility to use parameters in the clock guards. In general, if the parameters are real-valued, the problem of language emptiness of such automata is undecidable even for various restricted subclasses. We thus focus on the case where parameters are assumed to be integer-valued, while the time still remains continuous. On the one hand, we show that the problem remains undecidable for parametric timed automata with three clocks and one parameter. On the other hand, for the case with arbitrary many clocks where only one of these clocks is compared with (an arbitrary number of) parameters, we show that the parametric language emptiness is decidable. The undecidability result tightens the bounds of a previous result which assumed six parameters, while the decidability result extends the existing approaches that deal with discrete-time semantics only. To the best of our knowledge, this is the first positive result in the case of continuous-time and unbounded integer parameters, except for the rather simple case of single-clock automata.

1 Introduction

Timed automata [2] are a popular formalism used for modelling of real-time systems. In the classical definition, the clocks in guards are compared to fixed constants and one of the key problems, decidable in PSPACE [1], is the question of language emptiness. More than 20 years ago, Alur, Henzinger and Vardi [3] introduced a parametric variant of the language emptiness problem where clocks in timed automata can be additionally compared to a number of parameters. A clock is *nonparametric* if it is never compared with any of the parameters, otherwise the clock is *parametric*. The parametric language emptiness problem asks whether the parameters in the system can be replaced by constants so that the language of the resulting timed automaton becomes nonempty.

Unfortunately, the parametric language emptiness problem is undecidable for timed automata with three parametric clocks [3]. Yet Alur, Henzinger and Vardi

⋆ Nikola Beneš has been supported by the Czech Science Foundation grant project no. GA15-11089S.

⋆⋆ Peter Bezděk has been supported by the Czech Science Foundation grant project no. GA15-08772S.

Table 1: Decidability of the language (non)emptiness problems

	discrete time integer parameters	continuous time integer parameters	continuous time real parameters
n clocks, m parameters 1 parametric clock only	decidable [3]	**decidable**	undecidable [15]
3 clocks, 1 parameter	**undecidable**	**undecidable**	undecidable [15]
3 clocks, 6 parameters	undecidable [3]	undecidable [3]	undecidable [3]

established a positive decidability result in the case of a single parametric clock. This decidability result was recently extended by Bundala and Ouaknine [9] to the case with two parametric clocks and an arbitrary number of nonparametric clocks. Both positive results are restricted to the discrete-time semantics with only integer delays. The problem of decidability of integer parametric language emptiness in the continuous-time semantics has been open for over 20 years. The parametric language emptiness problem has two variants, which we call *reachability* (existence of a parameter valuation s.t. the language is nonempty) and *safety* (existence of a parameter valuation s.t. the language is empty).

Our main contributions, summarised in Table 1, are: (i) undecidability of the reachability and safety problems (in discrete and continuous-time semantics) for three parametric clocks, no additional nonparametric clocks and one integer parameter and (ii) decidability of the reachability and safety problems in the continuous-time semantics for one parametric clock with an arbitrary number of integer parameters and an unlimited number of additional nonparametric clocks. For reachability the problem is further decidable in NEXPTIME.

Related work. Our undecidability result holds both for discrete and continuous time semantics and it uses only a single parameter with three parametric clocks, hence strengthening the result from [3] where six parameters were necessary for the reduction. In [9] the authors established NEXPTIME-completeness of the parametric reachability problem for the case of a single parametric clock but only for the discrete-time semantics. Parametric TCTL model checking of timed automata, in the discrete-time setting, was also studied in [8,18]. Our decision procedure for one parametric clock is, to the best of our knowledge, the first one that deals with continuous-time semantics without any restriction on the usage of parameters and without bounding the range of the parameters.

Reachability for parametric timed automata was shown decidable for certain (strict) subclasses of parametric timed automata, either by bounding the range of parameters [13] or by imposing syntactic restrictions on the use of parameters as in L/U automata [6,12]. The study of parametric timed automata in continuous time with parameters ranging over the rational or real numbers showed undecidability already for one parametric clock [15], or for two parametric clocks with exclusively strict guards [10]. We thus focus solely on integer-valued parameters in this paper.

Parametric reachability problems for interrupt timed automata were investigated by Bérard, Haddad, Jovanović and Lime [7] with a number of positive decidability results although their model is incomparable with the formalism of timed automata studied in this paper. Other approaches include the inverse method of [17] where the authors describe a procedure for deriving constrains on parameters in order to satisfy that timed automata remain time-abstract equivalent, however, the termination of the procedure is in general not guaranteed.

2 Definitions

We shall now introduce parametric timed automata, the studied problems and give an example of a parametric system for alarm sensor coordination.

Let $\mathbb{N}_0$ denote the set of nonnegative integers and $\mathbb{R}_{\geq 0}$ the set of nonnegative real numbers. Let $\mathcal{C}$ be a finite set of *clocks* and let $\mathcal{P}$ be a finite set of *parameters*. A *simple clock constraint* is an expression of the form $x \bowtie c$ where $x \in \mathcal{C}$, $c \in \mathbb{N}_0 \cup \mathcal{P}$ and $\bowtie \in \{<, \leq, =, \geq, >\}$. A *guard* is a conjunction of simple clock constraints, we denote the set of all guards by $\mathcal{G}$. A conjunction of simple clock constraints that contain only upper bounds on clocks, i.e. $\bowtie \in \{<, \leq\}$, is called an *invariant* and the set of all invariants is denoted by $\mathcal{I}$.

A *clock valuation* is a function $\nu : \mathcal{C} \to \mathbb{R}_{\geq 0}$ that assigns to each clock its nonnegative real-time age and *parameter valuation* is a function $\gamma : \mathcal{P} \to \mathbb{N}_0$ that assigns to each parameter its nonnegative integer value. Given a clock valuation ν, a parameter valuation γ and a guard (or invariant) $g \in \mathcal{G}$, we write $\nu, \gamma \models g$ if the guard expression g, after the substitution of all clocks $x \in \mathcal{C}$ with $\nu(x)$ and all parameters $p \in \mathcal{P}$ with $\gamma(p)$, is true. By ν_0 we denote the initial clock valuation where $\nu_0(x) = 0$ for all $x \in \mathcal{C}$. For a clock valuation ν and a delay $d \in \mathbb{R}_{\geq 0}$, we define the clock valuation $\nu + d$ by $(\nu + d)(x) = \nu(x) + d$ for all $x \in \mathcal{C}$.

Definition 1 (Parametric Timed Automaton). *A* parametric timed automaton (PTA) *over the set of clocks $\mathcal{C}$ and parameters $\mathcal{P}$ is a tuple $A = (\Sigma, L, \ell_0, F, I, \to)$ where Σ is a finite* input alphabet*, L is a finite set of* locations*, $\ell_0 \in L$ is the* initial location*, $F \subseteq L$ is the set of* final (accepting) locations*, $I : L \to \mathcal{I}$ is an* invariant function *assigning invariants to locations, and $\to \subseteq L \times \mathcal{G} \times \Sigma \times 2^{\mathcal{C}} \times L$ is the set of transitions, written as $\ell \xrightarrow{g,a,R} \ell'$ whenever $(\ell, g, a, R, \ell') \in \to$.*

For the rest of this section, let $A = (\Sigma, L, \ell_0, F, I, \to)$ be a fixed PTA. We say that a clock $x \in \mathcal{C}$ is a *parametric clock* in A if there is a simple clock constraint of the form $x \bowtie p$ with $p \in \mathcal{P}$ that appears in a guard or an invariant of A. Otherwise, if the clock x is never compared to any parameter, we call it a *nonparametric clock*.

A configuration of A is a pair (ℓ, ν) where $\ell \in L$ is the current location and ν is the current clock valuation. For every parameter valuation γ we define the corresponding timed transition system $T_\gamma(A)$ where states are all configurations

(ℓ, ν) of A that satisfy the location invariants, i.e. $\nu, \gamma \models I(\ell)$, and the transition relation is defined as follows:

- $(\ell, \nu) \xrightarrow{d} (\ell, \nu + d)$ where $d \in \mathbb{R}_{\geq 0}$ if $\nu + d, \gamma \models I(\ell)$;
- $(\ell, \nu) \xrightarrow{a} (\ell', \nu')$ where $a \in \Sigma$ if there is a transition $\ell \xrightarrow{g,a,R} \ell'$ in A such that $\nu, \gamma \models g$ and $\nu', \gamma \models I(\ell')$ where for all $x \in \mathcal{C}$ we define $\nu'(x) = 0$ if $x \in R$ and $\nu'(x) = \nu(x)$ otherwise.

A *timed language* of A under a parameter valuation γ, denoted by $L_\gamma(A)$, is the collection of all accepted *timed words* of the form $(a_0, d_0)(a_1, d_1) \ldots (a_n, d_n) \in (\Sigma \times \mathbb{R}_{\geq 0})^*$ such that in the transition system $T_\gamma(A)$ there is a computation $(\ell_0, \nu_0) \xrightarrow{d_0} (\ell'_0, \nu'_0) \xrightarrow{a_0} (\ell_1, \nu_1) \xrightarrow{d_1} \cdots \xrightarrow{a_{n-1}} (\ell_n, \nu_n) \xrightarrow{d_n} (\ell'_n, \nu'_n) \xrightarrow{a_n} (\ell_{n+1}, \nu_{n+1})$ where $\ell_{n+1} \in F$.

We can now define two problems for parametric timed automata, namely the reachability problem (reaching desirable locations) and safety problem (avoiding undesirable locations). Note that the problems are not completely dual, as the safety problem contains a hidden alternation of quantifiers.

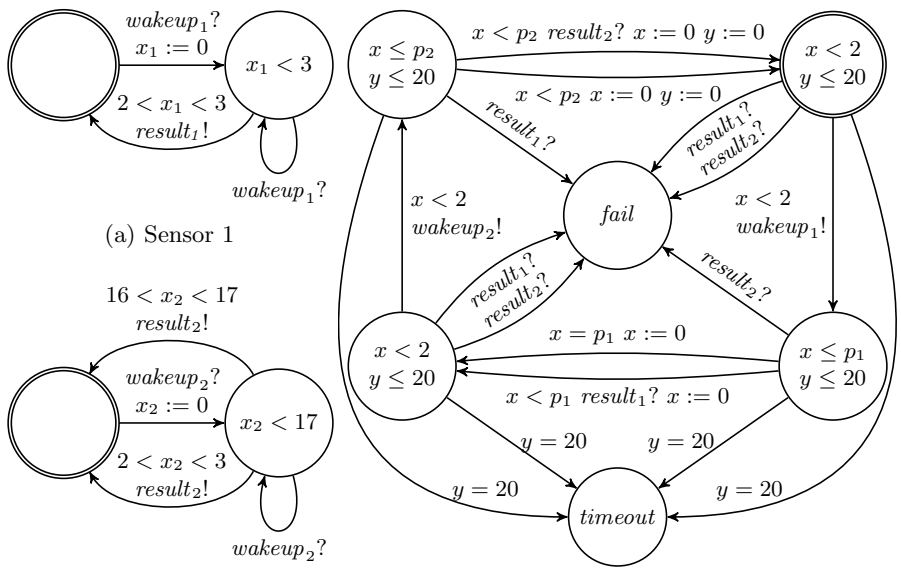
Problem 1 (Reachability Problem for PTA). Given a PTA A, is there a parameter valuation γ such that $L_\gamma(A) \neq \emptyset$?

Problem 2 (Safety Problem for PTA). Given a PTA A, is there a parameter valuation γ such that $L_\gamma(A) = \emptyset$?

We shall now present a small case study of a wireless fire alarm system [11] modelled as a parametric timed automaton. In the alarm setup, a number of wireless sensors communicate with the alarm controller over a limited number of communication channels (in our simplified example we assume just a single channel). The wireless alarm system uses a variant of Time Division Multiple Access (TDMA) protocol in order to guarantee a safe communication of multiple sensors over a shared communication channel. In TDMA the data stream is divided into frames and each frame consists of a number of time slots allocated for exclusive use by the present wireless sensors. Each sensor is assigned a single slot in each frame where it can transmit on the shared channel.

We model each sensor as a timed automaton with two locations as shown in Figure 1a and 1b. The sensor in Figure 1a waits in its initial location until it receives a $wakeup_1$ message from the controller. After this, it takes strictly between 2 to 3 seconds to gather the current status of the sensor and transmit it as $result_1$ message back to the controller. Any subsequent wakeup signals during the transmission phase are ignored and after the transmission phase is finished, the sensor is ready to receive another wakeup signal. The sensor in Figure 1b has a more complex behaviour as transmitting the answer $result_2$ can take either strictly between 2 to 3 seconds, or 16 to 17 seconds.

The controller presented in Figure 1c is responsible for synchronising the two sensors and for assigning them their time slots so that no transmissions interfere. The parametric clock x of the controller determines the size of the time slots. First, it takes at most 2 seconds for the controller to wake up the first sensor



(a) Sensor 1

(b) Sensor 2

(c) Controller with parameters p_1 and p_2

Fig. 1: Wireless Fire Alarm System

after which it waits until the elapsed time reaches the value of the parameter p_1. If it receives the result of the reading of the first sensor in this time slot, it moves immediately into the next location where it performs the wakeup of the second sensor. If the first sensor does not deliver any result and the clock x reaches the value p_1, it also moves to the next location. Now a symmetric control is performed for the second sensor. If any of the two sensors transmit during the time the controller transmits the wakeup signals, we enter the location *fail*. The fail location is also reached if $result_2$ is received in the time slot of the first sensor and vice versa. The second clock y is used to simply measure the duration of the whole frame; whenever the duration of the frame reaches 20 seconds, the controller enters the *timeout* location.

We assume a standard handshake synchronisation of the controller and the two sensors running in parallel that results in a flat product timed automaton with two parameters p_1 and p_2. Note that x is the only parametric clock in our example. Now, our task is to find suitable values of the parameters that guide the duration of the time slots for the two sensors so that there is no behaviour of the protocol where it fails or timeouts. This question is equivalent to the safety problem on the constructed PTA where we mark *fail* and *timeout* as the accepting (undesirable) locations.

The obvious parameter valuation where $\gamma(p_1) = 5$ and $\gamma(p_2) = 19$ guarantees that the location *fail* is unreachable but it is not an acceptable solution as the duration of the frame becomes 24 and we reach *timeout*. However, there is another parameter valuation where $\gamma(p_1) = 5$ and $\gamma(p_2) = 9$ that guarantees

that there is no possibility to fail or timeout. This is due to the fact that if the response time of the second sensor is too long, it skips one slot and the answer fits into an appropriate slot in the next frame.

In Section 4 we provide an algorithmic solution for finding such a parameter valuation that guarantees a given safety/reachability criterion. Note that as we are concerned with language (non)emptiness only, we employ two simplifications in the rest of the paper: First, we assume that the considered PTA have no invariants, as moving all invariants to guards preserves the language. Second, we assume that the alphabet is a singleton set as renaming all actions into a single action preserves language (non)emptiness.

3 Undecidability for Three Parametric Clocks

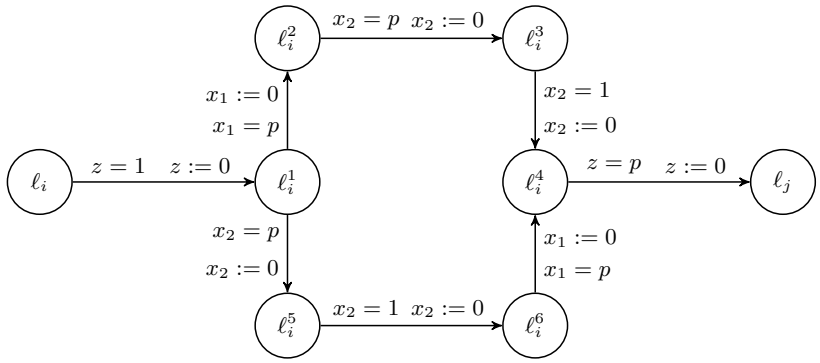
We shall now provide a reduction from the halting/boundedness problems of two counter Minsky machine to the reachability/safety problems on PTA. A *Minsky machine* with two nonnegative counters c_1 and c_2 is a sequence of labelled instructions $1 : inst_1;\ 2 : inst_2;\ \ldots, n : inst_n$ where $inst_n = HALT$ and each $inst_i$, $1 \leq i < n$, is of one of the following forms (for $r \in \{1, 2\}$ and $1 \leq j, k \leq n$):

- (Increment) i: c_r`++; goto` j
- (Test and Decrement) i: `if` c_r`=0 then goto` k `else (`c_r`--; goto` j`)`

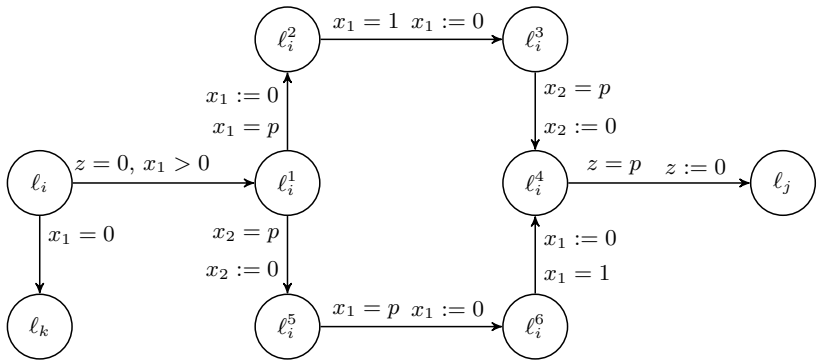
A configuration is a triple (i, v_1, v_2) where i is the current instruction and $v_1, v_2 \in \mathbb{N}_0$ are the values of the counters c_1 and c_2, respectively. A computation step between configurations is defined in the natural way. If starting from the initial configuration $(1, 0, 0)$ the machine reaches the instruction $HALT$ (note that the computation is deterministic) then we say it *halts*, otherwise it *loops*. The problem whether a given Minsky machine halts is undecidable [16]. The boundedness problem, i.e. the question whether there is a constant K such that $v_1 + v_2 \leq K$ for any configuration (i, v_1, v_2) reachable from $(1, 0, 0)$, is also undecidable [14].

The reduction from a two counter Minsky machine to PTA with a single parameter p and three parametric clocks x_1, x_2 and z is depicted in Figure 2. The reduction rules are shown only for the instructions handling the first counter. The rules for the second counter are symmetric. We also omit the transition labels as they are not relevant for the emptiness problem. The reduction preserves the property that whenever we are in a configuration (ℓ_i, ν) where $\nu(z) = 0$ then $\nu(x_1)$ and $\nu(x_2)$ represent the exact values of the counters c_1 resp. c_2, and the next instruction to be executed is the one with label i. Note also that there are no invariants used in the constructed automaton.

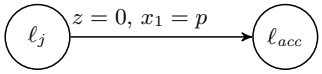
Lemma 1. *Let M be a Minsky machine. Let A be the PTA built according to the rules in Figures 2a and 2b (without the transitions for safety) and where ℓ_1 is the initial location and ℓ_n is the only accepting location. The Minsky machine M halts iff there is a parameter valuation γ such that $L_\gamma(A) \neq \emptyset$.*



(a) Increment i: c_1++; goto j



(b) Test and decrement i: if c_1=0 then goto k else (c_1--; goto j)



(c) For safety, add this for every instruction i: c_1++; goto j

Fig. 2: Encoding of Minsky Machine as PTA with a single parameter p

Proof (Sketch). We only sketch a part of the proof to show the basic idea. We argue that from the configuration (ℓ_i, ν) where $\nu(z) = 0$ and where $\nu(x_1)$ and $\nu(x_2)$ represent the counter values, there is a unique way to move from ℓ_i to ℓ_j (or possibly also to ℓ_k in the case of the test and decrement instruction) where again $\nu(z) = 0$ and the counter values are updated accordingly. As there are no invariants in the automaton, we can always delay long enough so that we get stuck in a given location, but this behaviour will not influence the language emptiness problem we are interested in.

Consider the automaton for the increment instruction from Figure 2a and assume we are in a configuration (ℓ_i, ν) where $\nu(z) = 0$, $\nu(x_1) = v_1$ and $\nu(x_2) = v_2$. First note that if $v_1 \geq p$ then there is no execution ending in ℓ_k due to the forced delay of one time unit on the transition from ℓ_i to ℓ_i^1 and the guard $x_1 = p$

tested in both the upper and lower branch in the automaton. Assume thus that $v_1 < p$. If $v_1 \geq v_2$ then we can perform the following execution with uniquely determined time delays: $(\ell_i, [x_1 \mapsto v_1, x_2 \mapsto v_2, z \mapsto 0]) \xrightarrow{1} (\ell_i^1, [x_1 \mapsto v_1+1, x_2 \mapsto v_2+1, z \mapsto 0]) \xrightarrow{p-v_1-1} (\ell_i^2, [x_1 \mapsto 0, x_2 \mapsto p-v_1+v_2, z \mapsto p-v_1-1]) \xrightarrow{v_1-v_2} (\ell_i^3, [x_1 \mapsto v_1-v_2, x_2 \mapsto 0, z \mapsto p-v_2-1]) \xrightarrow{1} (\ell_i^4, [x_1 \mapsto v_1-v_2+1, x_2 \mapsto 0, z \mapsto p-v_2]) \xrightarrow{v_2} (\ell_j, [x_1 \mapsto v_1+1, x_2 \mapsto v_2, z \mapsto 0])$. In this case where $v_1 \geq v_2$, executing the lower branch of the automaton will result in getting stuck in the location ℓ_i^6 as here necessarily $\nu(x_1) > p$. Clearly, there is a unique way of getting to ℓ_j in which the clock valuation of x_1 was incremented by one, hence faithfully simulating the increment instruction of the Minsky machine. The other cases and instructions are dealt with similarly, see Appendix A. □

Lemma 2. *Let M be a Minsky machine. Let A be the PTA built according to the rules in Figures 2a, 2b and 2c (including the transitions for safety) and where ℓ_1 is the initial location and ℓ_{acc} is the only accepting location. The Minsky machine M is bounded iff there is a parameter valuation γ such that $L_\gamma(A) = \emptyset$.*

Proof. If the computation of the Minsky machine is unbounded then clearly, for any parameter value of p, the Minsky machine will eventually try to make one of the counters larger or equal than p (using the increment instruction). Necessarily, we will then have $\nu(x_1) = p$ or $\nu(x_2) = p$ in the location ℓ_j where we end after performing the increment instruction i, implying that we can reach the accepting location ℓ_{acc} due to the transition added in Figure 2c and hence the language is nonempty. On the other hand, if the parameter p is large enough and the computation bounded (note that the boundedness condition $\exists K.\ v_1 + v_2 \leq K$ is equivalent to $\exists K.\ \max\{v_1, v_2\} \leq K$), we will not be able to enter the accepting location ℓ_{acc} and the language is empty. □

We now conclude with the main theorem of this section, tightening the previously known undecidability result that used six parameters and three parametric clocks [3]. The theorem is valid for both the continuous-time and the discrete-time semantics due to the exact guards in all transitions of the constructed PTA that allow to take transitions only after integer delays.

Theorem 1. *The reachability and safety problems are undecidable for PTA with one integer parameter, three parametric clocks and no further nonparametric clocks in the continuous-time as well as the discrete-time semantics.*

4 Decidability for One Parametric Clock

In this section, we show that both the reachability and safety problems for PTA with a single parametric clock are decidable. Our general strategy is similar to that of [3], i.e. reducing the original PTA (which has continuous-time semantics in our case) into a so-called *parametric 0/1-timed automaton* with just a single clock. It is shown in [3] that the set of parameter valuations that ensure language nonemptiness of a given parametric 0/1-timed automaton with single clock is

effectively computable. Moreover, in [9] the authors show that the reachability problem for parametric 0/1-timed automata is polynomial-time reducible to the halting problem of parametric bounded one-counter machines, which is in NP. As the parametric 0/1-timed automaton is going to be exponential in the size of the original PTA, this makes the reachability problem for PTA with a single parametric clock belong to the NEXPTIME complexity class.

A 0/1-timed automaton is a timed automaton with discrete time, in which all the delays are explicitly encoded via two kinds of delay transitions: 0-transitions and 1-transitions. Formally, we enrich the syntax of a timed automaton with two transition relations $\xrightarrow{0}, \xrightarrow{1} \subseteq L \times L$ and modify the semantics so that $(\ell, \nu) \xrightarrow{0} (\ell', \nu)$ iff $\ell \xrightarrow{0} \ell'$ and $(\ell, \nu) \xrightarrow{1} (\ell', \nu + 1)$ iff $\ell \xrightarrow{1} \ell'$; other delays in the timed transition system are no longer possible.

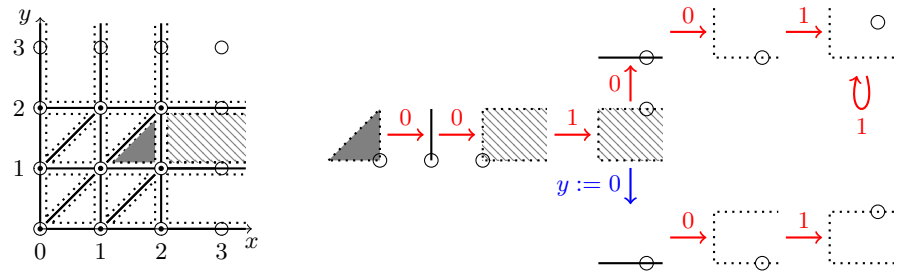
Note that this treatment of $\xrightarrow{0}$ and $\xrightarrow{1}$ as special transitions differs slightly from the original definition of [3], in which a 0/1 label is given to every transition of the 0/1-timed automaton. This change is only cosmetic; the ability to distinguish between 0/1-transitions and action transitions will be useful in later proofs.

Corner-Point Abstraction. As we are concerned with continuous time, our reduction to 0/1-timed automata is more convoluted than that of [3], in which the nonparametric clocks were eliminated by moving their integer values into locations. In our setting, using region abstraction to eliminate nonparametric clocks will not allow us to correctly identify the 0/1 delays. We thus choose to use *corner-point abstraction* [4] that is finer than the region-based one. In this abstraction, each region is associated with a set of its corner points. Note that the original definition only deals with timed automata that are bounded, while we want to be more general here. For this reason, we extend the original definition with extra corner points for unbounded regions.

We first define the region equivalence [2]. Let $M \in \mathbb{N}_0$ be the largest constant appearing in the constraints of a given timed automaton. Note that in the original definition the largest constant is considered for each clock independently. For the sake of readability, we consider M to be a common upper bound for each clock. Let ν, ν' be clock valuations. Let further $fr(t)$ be the fractional part of t and $\lfloor t \rfloor$ be the integral part of t. We define an equivalence relation $\equiv$ on clock valuations by $\nu \equiv \nu'$ if and only if the following three conditions are satisfied:

- for all $x \in \mathcal{C}$ either $\nu(x) \geq M$ and $\nu'(x) \geq M$ or $\lfloor \nu(x) \rfloor = \lfloor \nu'(x) \rfloor$;
- for all $x, y \in \mathcal{C}$ such that $\nu(x) \leq M$ and $\nu(y) \leq M$, $fr(\nu(x)) \leq fr(\nu(y))$ if and only if $fr(\nu'(x)) \leq fr(\nu'(y))$;
- for all $x \in \mathcal{C}$ such that $\nu(x) \leq M$, $fr(\nu(x)) = 0$ if and only if $fr(\nu'(x)) = 0$.

We define a *region* as an equivalence class of clock valuations induced by $\equiv$. A region r' is a time successor of a region r if for all $\nu \in r$ there exists $d \in \mathbb{R}_{>0}$ such that $\nu + d \in r'$ and for all d', $0 \leq d' \leq d$, we have $\nu + d' \in r \cup r'$. As the time successor is unique if it exists, we use $succ(r)$ to denote the time successor of r. Moreover, if no time successor of r exists, we let $succ(r) = r$.



(a) Corner points where $M = 2$ and $\mathcal{C} = \{x, y\}$

(b) Fragment of an evolution of a region with a corner point (locations are omitted for simplicity)

Fig. 3: Corner point abstraction

An (M^{+1})-*corner point* $\alpha : \mathcal{C} \to \mathbb{N}_0 \cap [0, M+1]$ is a function which assigns an integer value from the interval $[0, M+1]$ to each clock. We define the successor of the M^{+1}-corner point α, denoted by $succ(\alpha)$, as follows:

$$\text{for each } x \in \mathcal{C}, \quad succ(\alpha)(x) = \begin{cases} \alpha(x) + 1 & \alpha(x) \leq M \\ M + 1 & \text{otherwise} \ . \end{cases}$$

For $R \subseteq \mathcal{C}$, we define the reset of the corner point α, denoted by $\alpha[R]$, as follows:

$$\text{for each } x \in \mathcal{C}, \quad \alpha[R](x) = \begin{cases} \alpha(x) & x \notin R \\ 0 & x \in R \ . \end{cases}$$

We say α is a corner point of a region r whenever α is in the topological closure of r. The construction of the corner-point abstraction is illustrated in Figure 3. Notice the corner points in unbounded regions.

Construction of the Parametric 0/1-Timed Automaton. Now we show how to construct for a given PTA with one parametric clock an equivalent 0/1-PTA with just one clock. Let $A = (\Sigma, L, \ell_0, F, I, \to)$ be the original PTA over the set of clocks $\mathcal{C}$ and parameters $\mathcal{P}$. Let x_{p} denote the only parametric clock.

We first modify the automaton by adding a fresh clock z as follows: every transition $\ell \xrightarrow{g,a,R} \ell'$ is changed into $\ell \xrightarrow{g \wedge z<1,a,R'} \ell'$ where $R' = R$ if $x_{\mathrm{p}} \notin R$, and $R' = R \cup \{z\}$ otherwise. To every location ℓ we then add a new self-loop transition $\ell \xrightarrow{z=1,a,\{z\}} \ell$. Intuitively, the new clock z will always contain the fractional part of x_{p}. We call this new automaton A'. Clearly, this modification preserves the language (non)emptiness of the original automaton A.

In the second step, we use the corner-point abstraction of A' with respect to all clocks except for x_{p} to create the 0/1-timed automaton with a single clock. Let $\hat{\mathcal{C}} = (\mathcal{C} \cup \{z\}) \setminus \{x_{\mathrm{p}}\}$ and let M be the largest constant appearing in the guards concerning the clocks in $\hat{\mathcal{C}}$. In the following, we consider regions and

corner-points with respect to clocks in $\hat{\mathcal{C}}$ and the bound M. Let *Reg* denote the set of all such regions and let *Cp* denote the set of all corresponding corner-points, i.e. $Cp = (\mathbb{N}_0 \cap [0, M+1])^{\hat{\mathcal{C}}}$.

We use the following auxiliary notation. Let $r \in Reg$ and $\alpha \in Cp$.

$$\iota(r,\alpha) = \begin{cases} LESS & \alpha(z) = 1 \text{ and } r \not\models z = 1 \\ MORE & \alpha(z) = 0 \text{ and } r \not\models z = 0 \\ EXACT & \text{otherwise} \end{cases}$$

The 0/1-timed automaton over the singleton set of clocks $\{\hat{x}_\mathrm{p}\}$ is $\hat{A} = (\Sigma, L \times Reg \times Cp, (\ell_0, r_0, \alpha_0), F \times Reg \times Cp, I, \rightarrow)$ where r_0 is the initial region and $\alpha_0(x) = 0$ for all $x \in \hat{\mathcal{C}}$ is the initial corner-point. The transition relation is defined as follows:

- zero delay: $(\ell, r, \alpha) \xrightarrow{0} (\ell, r', \alpha)$ if $r' = succ(r)$ and α is a corner-point of both r and r';
- unit delay: $(\ell, r, \alpha) \xrightarrow{1} (\ell, r, \alpha')$ if $\alpha' = succ(\alpha)$ and both α and α' are corner-points of r;
- action: whenever $\ell \xrightarrow{g,a,R} \ell'$ in A' then let $g_1, \ldots, g_k$ be all the simple clock constraints appearing in g comparing clocks from $\hat{\mathcal{C}}$ and let $h_1, \ldots, h_n$ be the remaining simple clock constraints, i.e. those that consider x_p. For every (ℓ, r, α) that satisfies (1) $r \models g_1 \wedge \cdots \wedge g_k$ and (2) if $\iota(r,\alpha) \neq EXACT$ then no h_i contains equality (=), we set $(\ell, r, \alpha) \xrightarrow{\hat{h}_1 \wedge \cdots \wedge \hat{h}_n, \hat{R}} (\ell', r[R \setminus \{x_\mathrm{p}\}], \alpha[R \setminus \{x_\mathrm{p}\}])$, where $\hat{R} = \{\hat{x}_\mathrm{p}\}$ if $x_\mathrm{p} \in R$ and $\hat{R} = \emptyset$ otherwise. The constraints $\hat{h}_i$ are created as follows: all x_p are changed into $\hat{x}_\mathrm{p}$; if $\iota(r,\alpha) = LESS$, all $<$ are changed into $\leq$ and all $\geq$ are changed into $>$; if $\iota(r,\alpha) = MORE$, all $\leq$ are changed into $<$ and all $>$ are changed into $\geq$.

Theorem 2. *The reachability and safety problems for parametric timed automata over integer parameters with one parametric clock in the continuous-time semantics are decidable. Moreover, the reachability problem is in NEXPTIME.*

Proof (Idea). Due to space constraints, the complete proof can be found in Appendix B. As mentioned above, the modification from A to A' preserves the language (non)emptiness. The idea of the proof is to show that for every given parameter valuation, every run of A' has a corresponding run in $\hat{A}$ and vice versa. This shows that the reachability and safety problems for parametric timed automata with one parametric clock reduce to the reachability and safety problems for parametric 0/1-timed automata. These problems were shown decidable in [3]. The complexity argument is discussed in the beginning of this section. □

5 Conclusion

We have shown that for three parametric clocks with a single integer parameter, both the reachability and safety problems are undecidable in the discrete

as well as the continuous semantics. This improves the previously known undecidability result by Alur, Henzinger and Vardi [3] where six parameters were needed. For the case with a single parametric clock with an unrestricted number of integer parameters and with any number of additional nonparametric clocks, we contributed to the solution of an open problem stated more than 20 years ago by proving a decidability result for reachability and safety problems in the continuous semantics, extending the previously known decidability result for the discrete-time semantics [3]. To achieve this result, we used the corner-point abstraction technique that had to be modified to handle also corner-points in unbounded regions, contrary to the use of the technique in [4]. Not surprisingly, the decidability of the problem in case of two parametric clocks in the continuous-time setting remains open, as it is the case also for a number of other problems over timed automata with two real-time clocks [5]. On the other hand, as demonstrated by our wireless fire alarm case study, the parameter synthesis problem for one parametric clock and an unlimited number of parameters is sufficiently expressive in order to describe nontrivial scheduling problems. As a next step, we will consider moving from corner-point regions into zones and provide an efficient implementation of the presented techniques.

Acknowledgements. We acknowledge a funding from from the EU FP7 grant agreement nr. 318490 (SENSATION) and grant agreement nr. 601148 (CASSTING) and from the Sino-Danish Basic Research Center IDEA4CPS.

References

1. R. Alur, C. Courcoubetis, and D. Dill. Model-checking for real-time systems. In *LICS'90*, pages 414–425. IEEE, 1990.
2. R. Alur and D. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.
3. R. Alur, T.A. Henzinger, and M.Y. Vardi. Parametric real-time reasoning. In *Proceedings of 25th Annual Symposium on Theory of Computing (STOC'93)*, pages 592–601. ACM Press, 1993.
4. Gerd Behrmann, Ansgar Fehnker, Thomas Hune, Kim Guldstrand Larsen, Paul Pettersson, Judi Romijn, and Frits W. Vaandrager. Minimum-cost reachability for priced timed automata. In *HSCC'01*, volume 2034 of *LNCS*, pages 147–161. Springer, 2001.
5. Patricia Bouyer, Thomas Brihaye, and Nicolas Markey. Improved undecidability results on weighted timed automata. *Inform. Proc. Letters*, 98(5):188–194, 2006.
6. Laura Bozzelli and Salvatore La Torre. Decision problems for lower/upper bound parametric timed automata. *Formal Methods in Syst. Design*, 35(2):121–151, 2009.
7. Beatrice Bérard, Serge Haddad, Aleksandra Jovanović, and Didier Lime. Parametric interrupt timed automata. In *RP'13*, volume 8169 of *LNCS*, pages 59–69. Springer, 2013.
8. Véronique Bruyère and Jean-François Raskin. Real-time model-checking: Parameters everywhere. In *FST TCS'03*, volume 2914 of *LNCS*, pages 100–111. Springer, 2003.
9. Daniel Bundala and Joël Ouaknine. Advances in parametric real-time reasoning. In *MFCS'14*, volume 8634 of *LNCS*, pages 123–134. Springer, 2014.

10. Laurent Doyen. Robust parametric reachability for timed automata. *Information Processing Letters*, 102(5):208 – 213, 2007.
11. Sergio Feo-Arenis, Bernd Westphal, Daniel Dietsch, Marco Muñiz, and Siyar Andisha. The wireless fire alarm system: Ensuring conformance to industrial standards through formal verification. In *FM'14*, volume 8442 of *LNCS*, pages 658–672. Springer, 2014.
12. Thomas Hune, Judi Romijn, Mariëelle Stoelinga, and Frits Vaandrager. *Linear parametric model checking of timed automata*. Springer, 2001.
13. A. Jovanović, D. Lime, and O. H. Roux. Integer parameter synthesis for timed automata. In *TACAS 2013*, volume 7795 of *LNCS*, pages 401–415. Springer, 2013.
14. E.V. Kuzmin and D.J. Chalyy. Decidability of boundedness problems for Minsky counter machines. *Automatic Control and Computer Sciences*, 44(7):387–397, 2010.
15. Joseph S Miller. Decidability and complexity results for timed automata and semi-linear hybrid automata. In *Hybrid Systems: Computation and Control*, pages 296–310. Springer, 2000.
16. M.L. Minsky. *Computation: Finite and Infinite Machines*. Prentice, 1967.
17. Étienne André, Thomas Chatain, Laurent Fribourg, and Emmanuelle Encrenaz. An inverse method for parametric timed automata. *ENTCS*, 223(0):29–46, 2008.
18. Farn Wang. Parametric timing analysis for real-time systems. *Information and Computation*, 130(2):131–150, 1996.

A Appendix: Proof of Lemma 1

Lemma 1. *Let M be a Minsky machine. Let A be the PTA built according to the rules in Figures 2a and 2b (without the transitions for safety) and where ℓ_1 is the initial location and ℓ_n is the only accepting location. The Minsky machine M halts if and only if there is a parameter valuation γ such that $L_\gamma(A) \neq \emptyset$.*

Proof. We shall first argue that from the configuration (ℓ_i, ν) where $\nu(z) = 0$ and where $\nu(x_1)$ and $\nu(x_2)$ represent the counter values, there is a unique way to move from ℓ_i to ℓ_j (or possibly also to ℓ_k in case of test and decrement instruction) where again $\nu(z) = 0$ and the counter values are updated accordingly. As there are no invariants in the automaton, we can always delay long enough so that we get stuck in a given location, but this behaviour will not influence the language emptiness problem we are interested in.

Consider first the automaton for the increment instruction from Figure 2a and assume we are in a configuration (ℓ_i, ν) where $\nu(z) = 0$, $\nu(x_1) = v_1$ and $\nu(x_2) = v_2$. First note that if $v_1 \geq p$ then there is no execution ending in ℓ_k due to the forced delay of one time unit on the transition from ℓ_i to ℓ_i^1 and the guard $x_1 = p$ tested in both the upper and lower branch in the automaton. Assume thus that $v_1 < p$. If $v_1 \geq v_2$ then we can perform the following execution with uniquely determined time delays:

$$\begin{aligned}
(\ell_i, [x_1 \mapsto v_1, x_2 \mapsto v_2, z \mapsto 0]) &\xrightarrow{1} \\
(\ell_i^1, [x_1 \mapsto v_1 + 1, x_2 \mapsto v_2 + 1, z \mapsto 0]) &\xrightarrow{p - v_1 - 1} \\
(\ell_i^2, [x_1 \mapsto 0, x_2 \mapsto p - v_1 + v_2, z \mapsto p - v_1 - 1]) &\xrightarrow{v_1 - v_2} \\
(\ell_i^3, [x_1 \mapsto v_1 - v_2, x_2 \mapsto 0, z \mapsto p - v_2 - 1]) &\xrightarrow{1} \\
(\ell_i^4, [x_1 \mapsto v_1 - v_2 + 1, x_2 \mapsto 0, z \mapsto p - v_2]) &\xrightarrow{v_2} \\
(\ell_j, [x_1 \mapsto v_1 + 1, x_2 \mapsto v_2, z \mapsto 0]).
\end{aligned}$$

In this case where $v_1 \geq v_2$, executing the lower branch of the automaton will result in getting stuck in the location ℓ_i^6 as here necessarily $\nu(x_1) > p$. Assume now that $v_1 < v_2$. If we take upper branch in the automaton now then we get stuck. However, we can execute along the lower branch as follows:

$$\begin{aligned}
(\ell_i, [x_1 \mapsto v_1, x_2 \mapsto v_2, z \mapsto 0]) &\xrightarrow{1} \\
(\ell_i^1, [x_1 \mapsto v_1 + 1, x_2 \mapsto v_2 + 1, z \mapsto 0]) &\xrightarrow{p - v_2 - 1} \\
(\ell_i^5, [x_1 \mapsto p - v_2 + v_1, x_2 \mapsto 0, z \mapsto p - v_2 - 1]) &\xrightarrow{1} \\
(\ell_i^6, [x_1 \mapsto p - v_2 + v_1 + 1, x_2 \mapsto 0, z \mapsto p - v_2]) &\xrightarrow{v_2 - v_1 - 1} \\
(\ell_i^4, [x_1 \mapsto 0, x_2 \mapsto v_2 - v_1 - 1, z \mapsto p - v_1 - 1]) &\xrightarrow{v_1 + 1} \\
(\ell_j, [x_1 \mapsto v_1 + 1, x_2 \mapsto v_2, z \mapsto 0]).
\end{aligned}$$

In both cases, it is clear that the clock valuation of x_1 was incremented by one (due to uniquely given time delays during the computations) and hence they faithfully simulate the behaviour of the Minsky machine.

Regarding the automaton for test and decrement instruction from Figure 2b, assume we are in the configuration (ℓ_i, ν) with $\nu(x_1) = v_1$, $\nu(x_2) = v_2$ and $\nu(z) = 0$. It is clear that if $v_1 = 0$ then we continue from location ℓ_k as expected and if $v_1 > 0$ then we can enter the configuration $(\ell_i^1, x_1 \mapsto v_1, x_2 \mapsto v_2, z \mapsto 0)$—note that the guard $z = 0$ guarantees that no time has elapsed. In the latter case, if $v_1 > v_2$ then we can execute the upper branch as follows:

$$\begin{aligned}
(\ell_i^1, x_1 \mapsto v_1, x_2 \mapsto v_2, z \mapsto 0) &\xrightarrow{p-v_1} \\
(\ell_i^2, x_1 \mapsto 0, x_2 \mapsto p - v_1 + v_2, z \mapsto p - v_1) &\xrightarrow{1} \\
(\ell_i^3, x_1 \mapsto 0, x_2 \mapsto p - v_1 + v_2 + 1, z \mapsto p - v_1 + 1) &\xrightarrow{v_1 - v_2 - 1} \\
(\ell_i^4, x_1 \mapsto v_1 - v_2 - 1, x_2 \mapsto 0, z \mapsto p - v_2) &\xrightarrow{v_2} \\
(\ell_j, x_1 \mapsto v_1 - 1, x_2 \mapsto v_2, z \mapsto 0)&
\end{aligned}$$

and if $v_1 \leq v_2$ we can execute the lower branch as follows:

$$\begin{aligned}
(\ell_i^1, x_1 \mapsto v_1, x_2 \mapsto v_2, z \mapsto 0) &\xrightarrow{p-v_2} \\
(\ell_i^5, x_1 \mapsto p - v_2 + v_1, x_2 \mapsto 0, z \mapsto p - v_2) &\xrightarrow{v_2 - v_1} \\
(\ell_i^6, x_1 \mapsto 0, x_2 \mapsto v_2 - v_1, z \mapsto p - v_1) &\xrightarrow{1} \\
(\ell_i^4, x_1 \mapsto 0, x_2 \mapsto v_2 - v_1 + 1, z \mapsto p - v_1 + 1) &\xrightarrow{v_1 - 1} \\
(\ell_j, x_1 \mapsto v_1 - 1, x_2 \mapsto v_2, z \mapsto 0).&
\end{aligned}$$

Clearly, the clock value in x_1 has been decremented in both cases. Should the lower branch be taken in case $v_1 > v_2$ or the upper branch in case $v_1 \leq v_2$, we get stuck again.

Now if the Minsky machine halts then in the constructed PTA we can reach the accepting location ℓ_n for any parameter valuation $\gamma(p)$ larger than the maximum value of the counters during the computation and the answer to the reachability problem is hence positive. If, on the other hand, the Minsky machine loops then there is no parameter valuation $\gamma(p)$ that will allow us to reach the location ℓ_n. This is due to the fact that either one of the counters exceeds the chosen parameter value and we get stuck or the computation will continue for ever and never reach ℓ_n. □

B Appendix: Proof of Theorem 2

Theorem 2. *The reachability and safety problems for parametric timed automata over integer parameters with one parametric clock in the continuous-time semantics are decidable. Moreover, the reachability problem is in NEXPTIME.*

The semantics of a 0/1-timed automaton is similar to that of a timed automaton except for the fact that the delays are explicitly given by the 0/1-delay transitions and the valuations of clocks are natural numbers. In our case we have only one clock, $\hat{x}_{\mathrm{p}}$, which means that a configuration of $\hat{A}$ is a tuple (ℓ, r, α, t) where (ℓ, r, α) is a location of $\hat{A}$ and $t \in \mathbb{N}_0$ represents the valuation of $\hat{x}_{\mathrm{p}}$.

Note that the 0/1-delay transitions in $\hat{A}$ are always deterministic and exclusive: every location (ℓ, r, α) either has an outgoing 0-delay transition or an outgoing 1-delay transition, but not both. Moreover, after a 1-delay transition there always follows a 0-delay transition, except in the case when the 1-delay transition ends in the unbounded region.

Recall the $\iota(r, \alpha)$ notation for $r \in \mathit{Reg}$ and $\alpha \in \mathit{Cp}$:

$$\iota(r, \alpha) = \begin{cases} \mathit{LESS} & \alpha(z) = 1 \text{ and } r \not\models z = 1 \\ \mathit{MORE} & \alpha(z) = 0 \text{ and } r \not\models z = 0 \\ \mathit{EXACT} & \text{otherwise} \end{cases}$$

In order to prove the correctness of our construction, we also define an auxiliary notion of *correspondence*. Let $\nu : (\mathcal{C} \cup \{z\}) \to \mathbb{R}_{\geq 0}$, $r \in \mathit{Reg}$, $\alpha \in \mathit{Cp}$, and $t \in \mathbb{N}_0$. We say that ν corresponds with (r, α, t) if the following holds:

1. $\nu{\restriction}_{\hat{\mathcal{C}}} \in r$;
2. $\lfloor \nu(x_{\mathrm{p}}) \rfloor + f(r, \alpha) = t$, where $f(r, \alpha) = 1$ if $\iota(r, \alpha) = \mathit{LESS}$ and $f(r, \alpha) = 0$ otherwise;
3. $\nu(x_{\mathrm{p}}) \in \mathbb{N}_0 \iff \iota(r, \alpha) = \mathit{EXACT}$.

In the following, let us fix a valuation of all parameters of $\mathcal{P}$. We are going to show that all runs of A' have corresponding runs in $\hat{A}$ and vice versa. Note that due to the construction of A', we shall ignore all runs in which the new clock z becomes larger than 1, as such situations are effectively deadlocks.

Lemma 3. *Let (ℓ, ν) be a configuration of A' with $\nu(z) \leq 1$, let $(\ell, \nu) \xrightarrow{d} (\ell, \nu + d)$ be a delay transition with $d \in [0, 1 - \nu(z)]$, and let $(r, \alpha, t) \in \mathit{Reg} \times \mathit{Cp} \times \mathbb{N}_0$ such that ν corresponds with (r, α, t). Then $(\ell, r, \alpha, t) \to^* (\ell, r', \alpha', t')$ such that $\nu + d$ corresponds with (r', α', t').*

Proof. For simplicity, we assume that d is small enough in the following sense: Either ν and $\nu + d$ (restricted to clocks of $\hat{\mathcal{C}}$) are in the same region, or the region of $\nu + d$ is a successor of the region of ν. This comes without loss of generality, as every delay transition can be split into finitely many such small delay transitions. We also assume that $d > 0$.

If both $\nu{\restriction}_{\hat{\mathcal{C}}}$ and $(\nu + d){\restriction}_{\hat{\mathcal{C}}}$ belong to r then clearly $\lfloor \nu(x_{\mathrm{p}}) + d \rfloor = \lfloor \nu(x_{\mathrm{p}}) \rfloor$ and neither of $\nu(x_{\mathrm{p}})$ and $\nu(x_{\mathrm{p}}) + d$ belong to $\mathbb{N}_0$. This means that $\nu + d$ corresponds with (r, α, t).

Let us now assume that $\nu{\restriction}_{\hat{\mathcal{C}}} \in r$ and $(\nu + d){\restriction}_{\hat{\mathcal{C}}} \in r'$ where r' is the successor of r. There are two possibilities depending on whether (ℓ, r, α) has a 0-delay or a 1-delay transition.

If $(\ell, r, \alpha) \xrightarrow{0} (\ell, r', \alpha)$, this means that also $(\ell, r, \alpha, t) \xrightarrow{0} (\ell, r', \alpha, t)$. We show that $\nu + d$ corresponds with (r', α, t). Condition 1 is clearly satisfied. To show the satisfaction of Conditions 2 and 3, we need to discuss three cases:

- $\nu(z) = 0$: This means that necessarily $r \models z = 0$ and $\alpha(z) = 0$, thus $\iota(r, \alpha) = EXACT$ and $\iota(r', \alpha) = MORE$. Therefore $f(r, \alpha) = f(r', \alpha) = 0$ and the conditions are clearly met as $\lfloor \nu(x_\mathrm{p}) + d \rfloor = \lfloor \nu(x_\mathrm{p}) \rfloor$ and $\nu(x_\mathrm{p}) + d \notin \mathbb{N}_0$.
- $\nu(z) \in (0, 1 - d)$: This means that necessarily neither r nor r' contain a valuation with integer value for z and thus $\iota(r, \alpha) = \iota(r', \alpha) \neq EXACT$. This means that $f(r, \alpha) = f(r', \alpha)$ and the conditions are clearly met as $\lfloor \nu(x_\mathrm{p}) + d \rfloor = \lfloor \nu(x_\mathrm{p}) \rfloor$ and both $\nu(x_\mathrm{p})$, $\nu(x_\mathrm{p}) + d \notin \mathbb{N}_0$.
- $\nu(z) = 1 - d$: This means that necessarily $r' \models z = 1$ and $\alpha(z) = 1$, thus $\iota(r, \alpha) = LESS$ and $\iota(r', \alpha) = EXACT$. This means that $f(r, \alpha) = 1$ while $f(r', \alpha) = 0$. We have $\lfloor \nu(x_\mathrm{p}) + d \rfloor = \lfloor \nu(x_\mathrm{p}) \rfloor + 1$ and $\nu(x_\mathrm{p}) + d \in \mathbb{N}_0$, the conditions are thus met again.

If $(\ell, r, \alpha) \xrightarrow{1} (\ell, r, \alpha')$ then also $(\ell, r, \alpha') \xrightarrow{0} (\ell, r', \alpha')$ as noted above (due to the bound on $\nu(z)$, r is not the unbounded region). This means that $(\ell, r, \alpha, t) \xrightarrow{1}\xrightarrow{0} (\ell, r', \alpha', t+1)$. Here, α' is the successor of α and r' is the successor of r. We show that $\nu + d$ corresponds with $(r', \alpha', t + 1)$. Again, Condition 1 is clearly satisfied. Note that in this case $r \not\models z = 0$ and $\alpha(z) = 0$. This means that $\alpha'(z) = 1$, $\iota(r, \alpha) = MORE$, $\iota(r, \alpha') = LESS$, $f(r, \alpha) = 0$, and $f(r, \alpha') = 1$. This also means that $\nu(z) > 0$ and we only have two cases:

- $\nu(z) \in (0, 1 - d)$: This means that $r' \not\models z = 1$ and thus $\iota(r', \alpha') = LESS$. Condition 3 is clearly satisfied as $\nu(x_\mathrm{p}) + d \notin \mathbb{N}_0$. To show that Condition 2 is satisfied, consider that $f(r', \alpha') = 1$ and $\lfloor \nu(x_\mathrm{p}) + d \rfloor = \lfloor \nu(x_\mathrm{p}) \rfloor$.
- $\nu(z) = 1 - d$: This means that $r' \models z = 1$ and thus $\iota(r', \alpha') = EXACT$. Condition 3 is clearly satisfied as $\nu(x_\mathrm{p}) + d \in \mathbb{N}_0$. To show that Condition 2 is satisfied, consider that $f(r', \alpha') = 0$ and $\lfloor \nu(x_\mathrm{p}) + d \rfloor = \lfloor \nu(x_\mathrm{p}) \rfloor + 1 = t + 1$.

□

Lemma 4. *Let (ℓ, ν) be a configuration of A' with $\nu(z) \leq 1$, let $(\ell, \nu) \xrightarrow{a} (\ell', \nu')$ be an action transition, and let $(r, \alpha, t) \in Reg \times Cp \times \mathbb{N}_0$ such that ν corresponds with (r, α, t). Then $(\ell, r, \alpha, t) \xrightarrow{a} (\ell', r', \alpha', t')$ such that ν' corresponds with (r', α', t').*

Proof. The transition $(\ell, \nu) \xrightarrow{a} (\ell', \nu')$ is due to a transition $\ell \xrightarrow{g,a,R} \ell'$ of the timed automaton A' where $\nu \models g$ and $\nu' = \nu[R]$. Let now $g_1, \ldots, g_k$ be all the simple clock constraints of g that consider clocks from $\hat{\mathcal{C}}$ and $h_1, \ldots, h_n$ be the remaining simple clock constraints, as in the construction of the 0/1-timed automaton $\hat{A}$. We know that $r \models g_1 \wedge \cdots g_k$ as $\nu\restriction_{\hat{\mathcal{C}}} \in r$. We thus know that $(\ell, r, \alpha) \xrightarrow{\hat{h}_1 \wedge \cdots \hat{h}_n, a, \hat{R}} (\ell', r[R \setminus \{x_\mathrm{p}\}], \alpha[R \setminus \{x_\mathrm{p}\}]) = (\ell', r', \alpha')$, where $\hat{h}_i$ and $\hat{R}$ are given by the construction. We first need to show that t satisfies all clock constraints $\hat{h}_i$.

- If $h_i = (x_\mathrm{p} < e)$ then $\nu(x_\mathrm{p}) < e$ and thus $\lfloor \nu(x_\mathrm{p}) \rfloor \leq e - 1$. If $\iota(r, \alpha) = \mathit{LESS}$ then $f(r, \alpha) = 1$ and $t \leq (e - 1) + 1 = e$, which satisfies the constraint $\hat{h}_i = (\hat{x}_\mathrm{p} \leq e)$. Otherwise, $f(r, \alpha) = 0$ and $t \leq e - 1$, which satisfies the constraint $\hat{h}_i = (\hat{x}_\mathrm{p} < e)$.
- If $h_i = (x_\mathrm{p} \leq e)$ then $\nu(x_\mathrm{p}) \leq e$. If $\nu(x_\mathrm{p}) = e$ then $\iota(r, \alpha) = \mathit{EXACT}$. Thus $f(r, \alpha) = 0$ and $t = e$, which satisfies $\hat{x}_\mathrm{p} \leq e$. Otherwise, $\nu(x_\mathrm{p}) < e$. Due to the reasoning in the previous item, $t \leq e$ if $\iota(r, \alpha) = \mathit{LESS}$ and $t \leq e - 1$ otherwise. This means that t satisfies $\hat{h}_i$.
- The other two cases ($>$, $\geq$) are dealt with similarly.

We have thus shown that the transition $(\ell, r, \alpha, t) \xrightarrow{a} (\ell', r', \alpha', t')$ exists. Here, $t' = 0$ if $x_\mathrm{p} \in R$ and $t' = t$ otherwise.

We now show that ν' corresponds with (r', α', t'). Condition 1 is clearly satisfied. If $t' = t$ then both $x_\mathrm{p}, z \notin R$, which means that both $\nu(x_\mathrm{p})$ and $\iota(r, \alpha)$ are unchanged. If $t' = 0$ then $x_\mathrm{p}, z \in R$, which means that $\nu(x_\mathrm{p}) = 0$, $\iota(r', \alpha') = \mathit{EXACT}$ and $f(r', \alpha') = 0$. In both cases, ν' corresponds with (r', α', t'). □

Lemma 5. *Let (ℓ, r, α, t) be a configuration of $\hat{A}$, let $(\ell, r, \alpha, t) \xrightarrow{d} (\ell, r', \alpha', t')$ with $d \in \{0, 1\}$ and $r' \models z \leq 1$, and let ν correspond with (r, α, t). Then there exists d' such that $(\ell, \nu) \xrightarrow{d'} (\ell, \nu + d')$ and $\nu + d'$ corresponds with (r', α', t').*

Proof. If $d = 1$, we choose $d' = 0$ and show that $\nu + 0 = \nu$ corresponds with $(r', \alpha', t + 1)$. Clearly, in this case $r' = r$, $\alpha(z) = 0$, and $\alpha'(z) = 1$, which means that $\iota(r, \alpha) = \mathit{MORE}$ while $\iota(r, \alpha') = \mathit{LESS}$. Therefore, $f(r, \alpha) = 0$, $f(r, \alpha') = 1$ and if $\lfloor \nu(x_\mathrm{p}) \rfloor = t$ then $\lfloor \nu(x_\mathrm{p}) \rfloor + 1 = t + 1$.

Let us now assume that $d = 0$. This means that $\alpha' = \alpha$ while r' is the successor region of r. We choose an arbitrary d' such that $(\nu + d')\restriction_{\hat{\mathcal{C}}} \in r'$. To show that $\nu + d'$ corresponds with (r', α, t), we can use the very same reasoning as in the proof of Lemma 3. □

Lemma 6. *Let (ℓ, r, α, t) be a configuration of $\hat{A}$ with $r \models z \leq 1$, let $(\ell, r, \alpha, t) \xrightarrow{a} (\ell', r', \alpha', t')$, and let ν correspond with (r, α, t). Then $(\ell, \nu) \xrightarrow{a} (\ell', \nu')$ and ν' corresponds with (r', α', t').*

Proof. The transition $(\ell, r, \alpha, t) \xrightarrow{a} (\ell', r', \alpha', t')$ in the semantics is due to a transition $(\ell, r, \alpha) \xrightarrow{\hat{h}_1 \wedge \cdots \hat{h}_n, a, \hat{R}} (\ell', r', \alpha')$ of the 0/1-timed automaton $\hat{A}$, which was constructed from a transition $\ell \xrightarrow{g, a, R} \ell'$ of the timed automaton A'.

Clearly, if $r \models g_1 \wedge \cdots g_k$ then so does ν. We also need to show that $\nu \models h_1 \wedge \cdots h_n$. We know that t satisfies $\hat{h}_i$ for all i.

- If $h_i = (x_\mathrm{p} < e)$ then either $\iota(r, \alpha) = \mathit{LESS}$ and $\hat{h}_i = (\hat{x}_\mathrm{p} \leq e)$ or $\hat{h}_i = (\hat{x}_\mathrm{p} < e)$. In the first case, we know that $f(\alpha, r) = 1$, which means that $\lfloor \nu(x_\mathrm{p}) \rfloor + 1 = t$, which implies that $\nu(x_\mathrm{p}) < t \leq e$. In the second case, $f(\alpha, r) = 0$ which means that $\lfloor \nu(x_\mathrm{p}) \rfloor = t$ and thus $\nu(x_\mathrm{p}) < t + 1 \leq e$ as $t \leq e - 1$.

- If $h_i = (x_\mathrm{p} \leq e)$ then either $\iota(r, \alpha) = \mathit{MORE}$ and $\hat{h}_i = (\hat{x}_\mathrm{p} < e)$ or $\hat{h}_i = (\hat{x}_\mathrm{p} \leq e)$. In both cases, if $t < e$ then $t \leq e - 1$ and thus $\lfloor \nu(x_\mathrm{p}) \rfloor + f(r, \alpha) \leq e - 1$. This means that no matter the value of $f(r, \alpha)$, $\nu(x_\mathrm{p}) < e$. If, in the second case, $t = e$ then $\lfloor \nu(x_\mathrm{p}) \rfloor + f(r, \alpha) = e$. If $f(r, \alpha) = 1$ then $\nu(x_\mathrm{p}) < e$. If $f(r, \alpha) = 0$ then this means that $\iota(r, \alpha) = \mathit{EXACT}$ and $\nu(x_\mathrm{p}) = e$ as $\nu(x_\mathrm{p}) \in \mathbb{N}_0$.
- The remaining two cases ($>$, $\geq$) are dealt with similarly.

We now need to show that $\nu' = \nu[R]$ corresponds with (r', α', t'). This is shown exactly as in the proof of Lemma 4. $\square$

The correctness of the construction is now a corollary of the previous four lemmata; this proves the main theorem.