

Verifying Probabilistic Timed Automata Against Deterministic-Timed-Automata Specifications

Anonymous Author(s)

ABSTRACT

Probabilistic timed automata (PTAs) are timed automata extended with discrete probability distributions. They serve as a mathematical model for a wide range of applications that involve both stochastic and timed behaviours. In this paper, we study model checking of linear-time temporal properties over PTAs. In particular, we consider linear-time properties that can be encoded through deterministic timed automata (DTAs) with finite acceptance criterion. DTAs are a deterministic subclass of timed automata that can recognize a wide range of timed formal languages, thus can be effectively used to specify timed behaviours of systems. We show that through a product construction, model checking of PTAs against DTA-specifications can be reduced to solving reachability probabilities over PTAs, thus can be effectively solved by known algorithms on PTA-reachability. Our experimental results demonstrate the efficiency of our approach. As far as we know, we are the first to consider linear-time model checking of PTAs.

ACM Reference Format:

Anonymous Author(s). 1997. Verifying Probabilistic Timed Automata Against Deterministic-Timed-Automata Specifications. In *Proceedings of 21st ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2018)*. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.475/123.4>

1 INTRODUCTION

Stochastic timed systems are systems that exhibit both timed and stochastic behaviours. Such systems play a dominant role in many real-world applications (cf. [?]), hence addressing fundamental issues such as safety and performance over these systems are important. *Probabilistic timed automata* (PTAs) [? ? ?] serve as a good mathematical model for these systems. They extend the well-known model of timed automata [?] (for nonprobabilistic timed systems) with discrete probability distributions, and Markov Decision Processes (MDPs) [?] (for untimed probabilistic systems) with timing constraints.

Formal verification of PTAs has received much attention in recent years [?]. For branching-time model checking of PTAs, the problem is reduced to computation of reachability probabilities over MDPs through well-known finite abstraction for timed automata (namely *regions* and *zones*) [? ? ?]. Advanced techniques for branching-time model checking of PTAs such as inverse method and symbolic method have been explored in [? ? ? ?]. Extension with *cost* or *reward*, resulting in *priced* PTAs, has also been investigated. On

one hand, Berendsen *et al.* [?] proved that cost-bounded reachability probability is undecidable over priced PTAs. On the other hand, Jurdzinski *et al.* [?] and Kwiatkowska *et al.* [?] proved that several notions of accumulated (discounted) cost are computable over priced PTAs. Most verification algorithms for PTAs have been implemented in the model checker PRISM [?]. Computational complexity of several verification problems for PTAs is studied in [? ? ?].

A shortcoming of existing verification approaches for PTAs is that they all considered branching-time properties. As far as we know, no results have ever considered linear-time model checking for PTAs. Linear-time temporal properties are however important as they can specify complex timed behaviours induced by e.g. finite sequences of timed events. In particular, we focus on linear-time temporal properties that can be encoded by deterministic timed automata (DTAs). DTA is the deterministic version of timed automata. Although DTA is weaker than general timed automata, it can recognize a wide class of formal timed languages, and express interesting properties which cannot be expressed in branching-time logics [?]. The problem to verify DTA-specifications over stochastic timed models has only been investigated for continuous-time Markov processes (cf. [? ? ? ? ?]), a completely different formalism for stochastic timed systems which assigns probability distributions to time elapses. In this paper, we study verification of DTA-specifications over PTAs. As far as we know, we are the first to conduct this line of research.

Our Contributions. We show that through a product construction, the optimal probability of PTA-paths accepted by a DTA w.r.t the finite acceptance criterion can be computed exactly by known algorithms for reachability probabilities over PTAs. The novelty of our product construction is that to enable the DTA to keep track of the next location after a probabilistic jump in the PTA, one needs to integrate either the set of regions of the DTA or a local conjunction over the rules of the DTA. We demonstrate experimental results on several case studies and show that our approach is effective to analyse linear-time properties over PTAs.

2 PRELIMINARIES

In the whole paper, we denote by \mathbb{N} , \mathbb{N}_0 , \mathbb{Z} , and \mathbb{R} the sets of all positive integers, non-negative integers, integers, and real numbers, respectively.

For an infinite word w , $\text{inf}(w)$ is the set of symbols that occur infinitely many times in w . For a finite word w the last symbol is denoted by $\text{last}(w)$

2.1 Clock Valuations, Clock Constraints and Clock Equivalences

In this part, we fix a finite set \mathcal{X} of *clocks*.

Clock Valuations. Let \mathcal{X} be a finite set of *clocks*. A *clock valuation* is a function $\nu : \mathcal{X} \rightarrow [0, \infty)$. The set of clock valuations is denoted by $\text{Val}(\mathcal{X})$. Given a clock valuation ν , a subset $X \subseteq \mathcal{X}$ of clocks and a non-negative real number t , we let (i) $\nu[X := 0]$ be the clock valuation such that $\nu[X := 0](x) = 0$ for $x \in X$ and $\nu[X := 0](x) = \nu(x)$ otherwise, and (ii) $\nu + t$ be the clock valuation such that $(\nu + t)(x) = \nu(x) + t$ for all $x \in \mathcal{X}$. Moreover, we denote by $\mathbf{0}$ the clock valuation such that $\mathbf{0}(x) = 0$ for all $x \in \mathcal{X}$. *Clock Constraints.* The set of *clock constraints* $CC(\mathcal{X})$ over \mathcal{X} is generated by the following grammar:

$$\phi := \text{true} \mid x \leq d \mid c \leq x \mid x + c \leq y + d \mid \neg\phi \mid \phi \wedge \phi$$

where $x, y \in \mathcal{X}$ and $c, d \in \mathbb{N}_0$. We write **false** for a short hand of $\neg\text{true}$. The satisfaction relation \models between valuations ν and clock constraints ϕ is defined through substituting every $x \in \mathcal{X}$ appearing in ϕ by $\nu(x)$ and standard semantics for logical connectives. For a given clock constraint ϕ , we denote by $\llbracket \phi \rrbracket$ the set of all clock valuations that satisfy ϕ .

Clock Equivalence. Consider a nonnegative integer N which acts a threshold for relevant clock values: values held by clocks are treated the same if they exceed N . With such a fixed N , the standard notion of clock equivalence (see [?]) is an equivalence relation \sim_N over $\text{Val}(\mathcal{X})$ as follows: for any two clock valuations ν, ν' , $\nu \sim_N \nu'$ iff the following conditions hold:

- for all $x \in \mathcal{X}$, $\nu(x) > N$ iff $\nu'(x) > N$;
- for all $x \in \mathcal{X}$, if $\nu(x) \leq N$ then (i) $\lfloor \nu(x) \rfloor = \lfloor \nu'(x) \rfloor$ and (ii) $\text{frac}(\nu(x)) > 0$ iff $\text{frac}(\nu'(x)) > 0$;
- for all $x, y \in \mathcal{X}$, if $\nu(x), \nu(y) \leq N$ then $\text{frac}(\nu(x)) \bowtie \text{frac}(\nu(y))$ iff $\text{frac}(\nu'(x)) \bowtie \text{frac}(\nu'(y))$ for all $\bowtie \in \{<, =, >\}$.

Equivalence classes of \sim_N are conventionally called *regions*. The equivalence class that contains a given clock valuation ν is conventionally denoted by $[\nu]_{\sim}$.

2.2 Probabilistic Timed Automata

To introduce the notion of probabilistic timed automata (PTAs), we first define the notion of discrete probability distributions.

Discrete Probability Distributions. A *discrete probability distribution* over a countable non-empty set U is a function $q : U \rightarrow [0, 1]$ such that $\sum_{z \in U} q(z) = 1$. The *support* of q is defined as $\text{supp}(q) := \{z \in U \mid q(z) > 0\}$. The set of discrete probability distributions over U is denoted by $\mathcal{D}(U)$. For $u \in U$, let μ_u be the *point distribution at u* which assigns probability 1 to u .

Definition 2.1 (Probabilistic Timed Automata (PTAs) [?]). A *probabilistic timed automaton* (PTA) \mathcal{C} is a tuple

$$\mathcal{C} = (L, \ell^*, \mathcal{X}, \text{Act}, \text{inv}, \text{enab}, \text{prob}, \mathcal{L}) \quad (1)$$

where

- L is a finite set of *locations* and $\ell^* \in L$ is the *initial location*;
- \mathcal{X} is a finite set of *clocks*;
- Act is a finite set of *actions*;

- $\text{inv} : L \rightarrow CC(\mathcal{X})$ is an *invariant condition*;
- $\text{enab} : L \times \text{Act} \rightarrow CC(\mathcal{X})$ is an *enabling condition*;
- $\text{prob} : L \times \text{Act} \rightarrow \mathcal{D}(2^{\mathcal{X}} \times L)$ is a *probabilistic transition function*;
- AP is a finite set of *atomic propositions* and $\mathcal{L} : L \rightarrow 2^{AP}$ is a *labelling function*.

W.l.o.g, we assume that both Act and AP is disjoint from $[0, \infty)$. Below we fix a PTA \mathcal{C} in the form (1). The semantics of PTAs is as follows.

States and Transition Relation. A *state* of \mathcal{C} is a pair (ℓ, ν) in $L \times \text{Val}(\mathcal{X})$ such that $\nu \models \text{inv}(\ell)$. The set of all states is denoted by $S_{\mathcal{C}}$. The *transition relation* \rightarrow consists of all triples $((\ell, \nu), a, (\ell', \nu'))$ satisfying that

- $(\ell, \nu), (\ell', \nu')$ are states and $a \in \text{Act} \cup [0, \infty)$;
- if $a \in [0, \infty)$ then $\nu + \tau \models \text{inv}(\ell)$ for all $\tau \in [0, a]$ and $(\ell', \nu') = (\ell, \nu + a)$;
- if $a \in \text{Act}$ then $\nu \models \text{enab}(\ell, a)$ and there exists a pair $(X, \ell'') \in \text{supp}(\text{prob}(\ell, a))$ such that $(\ell', \nu') = (\ell'', \nu[X := 0])$.

By convention, we write $s \xrightarrow{a} s'$ instead of $(s, a, s') \in \rightarrow$. We omit the subscript ' \mathcal{C} ' in ' $S_{\mathcal{C}}$ ' if the underlying context is clear. The *probability transition kernel* \mathbf{P} is the function $\mathbf{P} : S \times \text{Act} \times S \rightarrow [0, 1]$ such that

$$\mathbf{P}((\ell, \nu), a, (\ell', \nu')) = \begin{cases} 1 & \text{if } (\ell, \nu) \xrightarrow{a} (\ell', \nu') \text{ and } a \in [0, \infty) \\ \sum_{Y \in B} \text{prob}(\ell, a)(Y, \ell') & \text{if } (\ell, \nu) \xrightarrow{a} (\ell', \nu') \text{ and } a \in \text{Act} \\ 0 & \text{otherwise} \end{cases}$$

where $B := \{X \subseteq \mathcal{X} \mid \nu' = \nu[X := 0]\}$.

Well-formedness. We say that \mathcal{C} is *well-formed* if for every state (ℓ, ν) and action $a \in \text{Act}$ such that $\nu \models \text{enab}(\ell, a)$ and for every $(X, \ell') \in \text{supp}(\text{prob}(\ell, a))$, one has that $\nu[X := 0] \models \text{inv}(\ell')$. The well-formedness is to ensure that when an action is enabled, the next state after taking this action will always be legal. In the rest of the paper, we always assume that the underlying PTA is well-formed. PTAs that are not well-formed can be repaired to satisfy the well-formedness condition [?].

Paths. A *finite path* ρ (under \mathcal{C}) is a finite sequence

$$\langle s_0, a_0, s_1, \dots, a_{n-1}, s_n \rangle \quad (n \geq 0)$$

in $S \times ((\text{Act} \cup [0, \infty)) \times S)^*$ such that (i) $s_0 = (\ell^*, \mathbf{0})$, (ii) $a_{2k} \in [0, \infty)$ for all integers $0 \leq k \leq \frac{n}{2}$, (iii) $a_{2k+1} \in \text{Act}$ for all integers $0 \leq k \leq \frac{n-1}{2}$ and (iv) for all $0 \leq k \leq n-1$, $s_k \xrightarrow{a_k} s_{k+1}$. The length of ρ is n , denoted by $|\rho|$.

An *infinite path* (under \mathcal{C}) is an infinite sequence

$$\langle s_0, a_0, s_1, a_1, \dots \rangle$$

in $(S \times (\text{Act} \cup [0, \infty)))^\omega$ such that for all $n \in \mathbb{N}_0$, $\langle s_0, a_0, \dots, a_{n-1}, s_n \rangle$ is a finite path. The set of finite (resp. infinite) paths under \mathcal{C} is denoted by $\text{Paths}_{\mathcal{C}}^*$ (resp. $\text{Paths}_{\mathcal{C}}^\omega$).

Schedulers. A *scheduler* (or *adversary*) is a function σ from the set of finite paths into $\text{Act} \cup [0, \infty)$ such that for all finite paths $\rho = s_0 a_0 \dots s_n$, (i) $\sigma(\rho) \in \text{Act}$ if n is odd, (ii) $\sigma(\rho) \in [0, \infty)$ if n is even, and (iii) there exists a state s' such

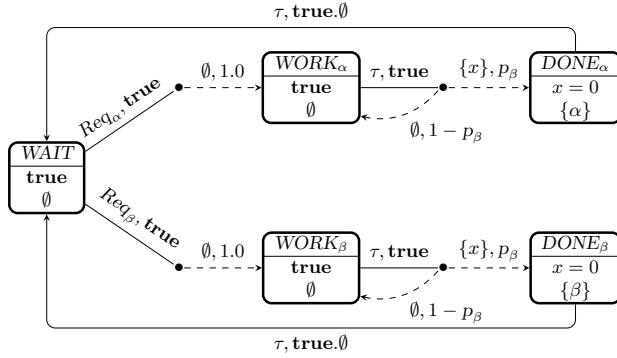


Figure 1: A Task Complete Example

that $s_n \xrightarrow{\sigma(\rho)} s'$. A finite path $\rho = s_0 a_0 \dots s_n$ is said to *follow* a scheduler σ if for all $0 \leq m \leq n$, $a_m = \sigma(s_0 a_0 \dots s_m)$. Likewise, an infinite path $s_0 a_0 s_1 a_1 \dots$ *follows* a scheduler σ if for all $n \in \mathbb{N}_0$, $a_n = \sigma(s_0 a_0 \dots s_n)$. The set of finite (resp. infinite) paths following a scheduler σ is denoted by $\text{Paths}_{\mathcal{C}, \sigma}^*$ (resp. $\text{Paths}_{\mathcal{C}, \sigma}^\omega$). We note that the set $\text{Paths}_{\mathcal{C}, \sigma}^*$ is countably-infinite from definition.

Probability Spaces under Schedulers. Let σ be any scheduler for \mathcal{C} . The probability space for \mathcal{C} w.r.t σ is defined as $(\Omega^{\mathcal{C}, \sigma}, \mathcal{F}^{\mathcal{C}, \sigma}, \mathbb{P}^{\mathcal{C}, \sigma})$ where $\Omega^{\mathcal{C}, \sigma} := \text{Paths}_{\mathcal{C}, \sigma}^*$, $\mathcal{F}^{\mathcal{C}, \sigma}$ is the smallest σ -algebra generated by all cylinder sets induced by finite paths (a finite path ρ induces the cylinder set $\text{Cyl}(\rho)$ of all infinite paths in $\text{Paths}_{\mathcal{C}, \sigma}^\omega$ with ρ being their (common) prefix) and $\mathbb{P}^{\mathcal{C}, \sigma}$ is the unique probability measure such that for all finite paths $\rho = s_0 a_0 \dots a_{n-1} s_n$ in $\text{Paths}_{\mathcal{C}, \sigma}^*$, $\mathbb{P}^{\mathcal{C}, \sigma}(\text{Cyl}(\rho)) = \prod_{k=0}^{n-1} \mathbf{P}(s_k, \sigma(s_0 a_0 \dots a_{k-1} s_k), s_{k+1})$. Intuitively, the probability space under σ is induced by a Markov chain where the state space is $\text{Paths}_{\mathcal{C}, \sigma}^*$ and the one-step probability transition matrix is determined by \mathbf{P} and σ .

Zenoness and Time-Divergent Schedulers. An infinite path $\pi = s_0 a_0 s_1 a_1 \dots$ is *zeno* if $\sum_{n=0}^\infty d_n = \infty$, where $d_n := a_n$ if $a_n \in [0, \infty)$ and $d_n := 0$ otherwise. Then a scheduler σ is *time divergent* if $\mathbb{P}^{\mathcal{C}, \sigma}(\{\pi \mid \pi \text{ is zeno}\}) = 0$. In the rest of the paper, we only consider time-divergent schedulers. The purpose to restrict to time-divergent schedulers is to eliminate non-realistic zeno behaviours such as performing infinitely many actions within a bounded amount of time.

Reachability. An infinite path $\pi = (\ell_0, \nu_0) a_0 (\ell_1, \nu_1) a_1 \dots$ is said to *visit* a subset $U \subseteq L$ of locations *eventually* if there exists $n \in \mathbb{N}_0$ such that $\ell_n \in U$. The set of infinite paths in $\text{Paths}_{\mathcal{C}, \sigma}^\omega$ that visit U eventually is denoted by $\text{Reach}_{\mathcal{C}, \sigma}^U$. From the fact that the set $\text{Paths}_{\mathcal{C}, \sigma}^*$ is countably-infinite, $\text{Reach}_{\mathcal{C}, \sigma}^U$ is measurable since it is a countable union of cylinder sets.

Example 2.2. In the figure, WAIT, WORK_s and DONE_s ($s \in \{\alpha, \beta\}$) are locations and x is the only clock. Below each location first comes (vertically) its invariant condition and then the set of labels assigned to the location. For example, $\text{inv}(\text{DONE}_\alpha) = (x = 2)$ and $\mathcal{L}(\text{DONE}_\alpha) = \{\alpha\}$. The four dot points together with corresponding arrows refer to four

actions and their enabling conditions and probability transition functions. For example, the upper dot at the right of WORK_α refers to an action whose name is τ , the enabling condition for τ (from WORK_α) is **true** (cf. the solid line emitting from WORK_α), and the probability distribution for this action is to reset x and go to DONE_α with probability p_α and to reset x and go back to DONE_α with probability $1 - p_\alpha$. The PTA models a machine which deals with two different kinds of jobs.

2.3 Deterministic Timed Automata

Definition 2.3 (Nondeterministic Timed Automata (NTAs) [??]). A nondeterministic timed automaton (NTA) \mathcal{A} is a tuple

$$\mathcal{A} = (Q, \Sigma, \mathcal{X}, \Delta) \quad (2)$$

where

- Q is a finite set of *modes*;
- Σ is a finite *alphabet* of *symbols* disjoint from $[0, \infty)$;
- \mathcal{X} is a finite set of *clocks*;
- $\Delta \subseteq Q \times \Sigma \times \text{CC}(\mathcal{X}) \times 2^{\mathcal{X}} \times Q$ is a finite set of *rules*.

And \mathcal{A} is called *deterministic* iff

- (1) (*determinism*): whenever $(q_1, b_1, \phi_1, X_1, q'_1), (q_2, b_2, \phi_2, X_2, q'_2) \in \Delta$, if $(q_1, b_1) = (q_2, b_2)$ and $\llbracket \phi_1 \rrbracket \cap \llbracket \phi_2 \rrbracket \neq \emptyset$ then $(\phi_1, X_1, q'_1) = (\phi_2, X_2, q'_2)$;
- (2) (*totality*): for all $(q, b) \in Q \times \Sigma$ and $\nu \in \text{Val}(\mathcal{X})$, there exists $(q, b, \phi, X, q') \in \Delta$ such that $\nu \models \phi$.

Below we fix a DTA \mathcal{A} in the form (??). Given $q \in Q$, $\nu \in \text{Val}(\mathcal{X})$ and $b \in \Sigma$, the triple $(\Phi_{q,b}^\nu, \mathbf{X}_{q,b}^\nu, \mathbf{q}_{q,b}^\nu) \in \text{CC}(\mathcal{X}) \times 2^{\mathcal{X}} \times Q$ are determined such that $(q, b, \Phi_{q,b}^\nu, \mathbf{X}_{q,b}^\nu, \mathbf{q}_{q,b}^\nu) \in \Delta$ is the unique rule satisfying $\nu \models \Phi_{q,b}^\nu$. We illustrate the semantics of DTAs as follows.

Configurations and One-Step Transition Function. A *configuration* of \mathcal{A} is a pair (q, ν) , where $q \in Q$ and $\nu \in \text{Val}(\mathcal{X})$. The *one-step transition function*

$$\kappa : (Q \times \text{Val}(\mathcal{X})) \times (\Sigma \cup [0, \infty)) \rightarrow Q \times \text{Val}(\mathcal{X})$$

is defined by: $\kappa((q, \nu), a) := (\mathbf{q}_{q,a}^\nu, \nu[\mathbf{X}_{q,a}^\nu := 0])$ for $a \in \Sigma$; $\kappa((q, \nu), a) := (q, \nu + a)$ for $a \in [0, \infty)$. For the sake of convenience, we write $(q, \nu) \xrightarrow{a} (q', \nu')$ instead of $\kappa((q, \nu), a) = (q', \nu')$.

Infinite Time Words and Runs. An *infinite time word* is an infinite sequence $\{a_n\}_{n \in \mathbb{N}_0}$ such that $a_{2n} \in [0, \infty)$ and $a_{2n+1} \in \Sigma$ for all n . The *run* of \mathcal{A} on an infinite word $w = \{a_n\}_{n \in \mathbb{N}_0}$ with *initial configuration* (q, ν) , denoted by $\mathcal{A}_{q, \nu}(w)$, is the unique infinite sequence $\{(q_n, \nu_n, a_n)\}_{n \in \mathbb{N}_0}$ which satisfies that $(q_0, \nu_0) = (q, \nu)$ and $(q_n, \nu_n) \xrightarrow{a_n} (q_{n+1}, \nu_{n+1})$ for all $n \in \mathbb{N}_0$. The trajectory of $\mathcal{A}_{q, \nu}(w)$, an infinite string over Q , is defined as follow $\text{traj}(\mathcal{A}_{q, \nu}(w)) := q_0 q_1 \dots$.

Now we illustrate the acceptance condition for DTAs. In this paper, we focus on infinite acceptance condition.

Definition 2.4 (Timed Rabin Automata (TRAs)). A *timed Rabin Automata* (TRA) is a tuple

$$\mathcal{A} = (Q, \Sigma, \mathcal{X}, \Delta, \mathcal{F}) \quad (3)$$

where $(Q, \Sigma, \mathcal{X}, \Delta)$ is a timed automaton, and \mathcal{F} is a finite set of pairs $\mathcal{F} = \{(H_1, K_1), \dots, (H_n, K_n)\}$, where H_i and

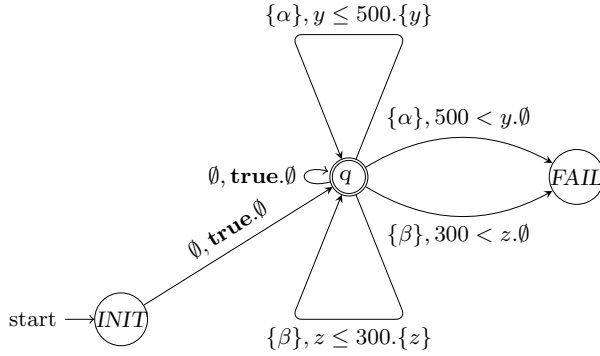


Figure 2: A DTA Specification

K_i are subset of Q for all $i < n$. A set $Q' \subseteq Q$ is called Rabin accepting by \mathcal{F} , denoted by $\mathbf{ACC}(Q', \mathcal{F})$, if there exists $1 \leq i \leq n$ such that $Q' \cap H_i = \emptyset$ and $Q' \cap K_i \neq \emptyset$. An infinite word w is accepted \mathcal{A} with initial configuration (q, ν) iff $\text{inf}(\text{traj}(\mathcal{A}_{(q, \nu)}(w)))$ is Rabin accepting by \mathcal{F} .

Example 2.5. Consider the DTA depicted in Figure 2 which works as a specification for the PTA in Example 2.2. INIT , q and FAIL are modes with $\mathcal{F} = \{\{\text{FAIL}\}, \{q\}\}$, y, z are clocks and arrows between modes are rules. For example, there are five rules emitting from q , one is $(q, \{\beta\}, 300 < z, \emptyset, \text{FAIL})$ and another is $(q, \emptyset, \text{true}, \emptyset, q)$. INIT is the initial mode to read the label of the initial location of a PTA in the product construction, and FAIL is a trap mode. Note that this DTA does not satisfy the totality condition. However, this can be remedied by adding rules leading to a deadlock mode without changing the acceptance behaviour of the DTA. This DTA specified the property that every α job should be done within 500 units of time after last α job done and every β job should be done within 300 units of time after last β job done.

3 THE PTA-TRA PROBLEM

In this section, we define the problem of model-checking PTAs against TRA-specifications. The problem takes a PTA and a TRA as input, and computes the probability that infinite paths under the PTA are accepted by the TRA. Informally, the TRA encodes the linear-time property by judging whether an infinite path is accepted or not through the external behaviour of the path, thus the problem is to compute the probability that the external behaviour of PTA meets the criterion specified by the TRA. In practice, the TRA is often used to capture all good (or bad) behaviours, so the problem can be treated as a task to evaluated to what extent the PTA behaves in a good (or bad) way.

Below we fix a well-formed PTA \mathcal{C} taking the form (1) and a TRA \mathcal{A} taking the form (3) with the difference that the set of clocks for \mathcal{C} (resp. for \mathcal{A}) is denoted by \mathcal{X}_1 (resp. \mathcal{X}_2). W.l.o.g., we assume that $\mathcal{X}_1 \cap \mathcal{X}_2 = \emptyset$ and $\Sigma = 2^{AP}$. We first show how an infinite path in $\text{Paths}_{\mathcal{C}}^\omega$ can be interpreted as an infinite word.

Definition 3.1 (Infinite Paths as Infinite Words). Given an infinite path

$$\pi = (\ell_0, \nu_0) a_0 (\ell_1, \nu_1) a_1 (\ell_2, \nu_2) a_2 \dots a_{2n} (\ell_{2n+1}, \nu_{2n+1}) a_{2n+1} (\ell_{2n+2}, \nu_{2n+2}) \dots$$

under \mathcal{C} (note that $\nu_0 = \mathbf{0}$), the infinite word $\mathcal{L}(\pi)$ over $2^{AP} \cup [0, \infty)$ is defined as

$$\mathcal{L}(\pi) := a_0 \mathcal{L}(\ell_2) a_2 \mathcal{L}(\ell_4) \dots a_{2n} \mathcal{L}(\ell_{2n+2}) \dots$$

Recall that $a_{2n} \in [0, \infty)$ and $a_{2n+1} \in \text{Act}$.

REMARK 1. Informally, the interpretation in Definition 3.1 works by (i) dropping (a) the initial location ℓ_0 , (b) all clock valuations ν_n 's, (c) all locations ℓ_{2n+1} 's following a time-elapse, (d) all internal actions a_{2n+1} 's of \mathcal{C} and (ii) replacing every ℓ_{2n} ($n \geq 1$) by $\mathcal{L}(\ell_{2n})$. The interpretation captures only external behaviours including time-elapses and labels of locations upon state-change, and discards internal behaviours such as the concrete locations, clock valuations and actions. Although the interpretation ignores the initial location, we deal with it in our acceptance condition where the initial location is preprocessed by the TRA.

REMARK 2. Our interpretation is different from $[\text{? ? ?}]$. In the style from $[\text{? ? ?}]$, an infinite path $(\ell_0, \nu_0) a_0 (\ell_1, \nu_1) a_1 \dots$ is interpreted as $a_0 \mathcal{L}(\ell_0) a_2 \mathcal{L}(\ell_2) \dots$, reversing the locations and actions/time-elapses. In contrast, our interpretation follows a natural way that preserves the order of external events in an infinite path. This advantage allows one to specify DTAs (for linear-time properties) in a straightforward way.

Based on Definition 3.1, we define the finite acceptance condition as follows. For an infinite path $\pi = (\ell_0, \nu_0) a_0 (\ell_1, \nu_1) a_1 \dots$ under \mathcal{C} , we denote by $\text{init}(\pi)$ the initial location ℓ_0 .

Definition 3.2 (Path Acceptance). An infinite path π under \mathcal{C} is *infinitely accepted* by \mathcal{A} w.r.t initial configuration (q, ν) , abbreviated as $\mathbf{ACC}(\mathcal{A}, (q, \nu), \pi)$, if the infinite word $\mathcal{L}(\pi)$ is accepted by \mathcal{A} w.r.t $(\kappa((q, \nu), \mathcal{L}(\text{init}(\pi))), \mathbf{0})$. Notice that \mathbf{ACC} is already used but it is easy to distinguish the two different usage from the context.

In the definitions above, the initial location omitted in Definition 3.1 is preprocessed by specifying explicitly that the initial configuration is $(\kappa((q, \nu), \mathcal{L}(\text{init}(\pi))), \mathbf{0})$.

Now we define the notion of acceptance probabilities over infinite paths under \mathcal{C} .

Definition 3.3 (Acceptance Probabilities). The probability that \mathcal{C} observes \mathcal{A} under scheduler σ , initial mode $q \in Q$ and F , denoted by $\mathbf{p}_{q,F}^\sigma$, is defined by:

$$\mathbf{p}_q^\sigma := \mathbb{P}^{\mathcal{C}, \sigma} \left(\text{AccPaths}_{\mathcal{C}, \sigma}^{\mathcal{A}, q} \right)$$

where $\text{AccPaths}_{\mathcal{C}, \sigma}^{\mathcal{A}, q}$ is the set of paths in \mathcal{C} that falls into the Rabin-accepted language of \mathcal{A}

$$\text{AccPaths}_{\mathcal{C}, \sigma}^{\mathcal{A}, q} = \{ \pi \in \text{Paths}_{\mathcal{C}, \sigma}^\omega \mid \mathbf{ACC}(\mathcal{A}, (q, \mathbf{0}), \pi) \}$$

Again, from the fact that the set $Paths_{\mathcal{C},\sigma}^*$ is countably-infinite, $AccPaths_{\mathcal{C},\sigma}^{A,q}$ is measurable since it can be represented in the form of a countable intersect and countable union of some cylinder sets.

Now the PTA-TRA problem is as follows.

- **Input:** a well-formed PTA \mathcal{C} , a TRA \mathcal{A} , an initial mode q ;
- **Output:** $\inf_{\sigma} p_q^{\sigma}$ and $\sup_{\sigma} p_q^{\sigma}$, where σ ranges over all time-divergent schedulers.

We refer to the problem as PTA-DTA if \mathcal{A} is deterministic.

4 THE PRODUCT CONSTRUCTION

In this section, we introduce the core part of our algorithms to solve the PTA-DTA problem and **deterministic TRA is referred as DTA**. The core part is a product construction which given a PTA \mathcal{C} and a DTA \mathcal{A} , output a PTA which preserves the probability of the set of infinite paths of \mathcal{C} accepted by \mathcal{A} . Below we fix a well-formed PTA \mathcal{C} in the form (1) and a DTA \mathcal{A} in the form (??) with the difference that the set of clocks for \mathcal{C} (resp. for \mathcal{A}) is denoted by \mathcal{X}_1 (resp. \mathcal{X}_2). W.l.o.g., we assume that $\mathcal{X}_1 \cap \mathcal{X}_2 = \emptyset$ and $\Sigma = 2^{AP}$. We let \mathcal{G} be the set of regions w.r.t \sim_N , where N is the maximal integer appearing in the clock constraints of \mathcal{A} .

The Main Idea. The intuition of the product construction is to let \mathcal{A} reads external actions of \mathcal{C} while \mathcal{C} evolves along the time axis. The major difficulty is that when \mathcal{C} performs actions in Act , there is a probabilistic choice between the target locations. Then \mathcal{A} needs to know the labelling of the target location and the rule (in Δ) used for the transition. A naive solution is to integrate each single rule Δ into the enabling condition $enab$ in \mathcal{C} . However, this simple solution does not work since a single rule in Δ fixes the labelling of a location in \mathcal{C} , while the probabilistic distribution given by $prob$ can jump to locations with different labels. We solve this difficulty by integrating into the enabling condition $enab$ enough information on clock valuations under \mathcal{A} so that the rule used for the transition (in \mathcal{A}) is clear. In detail, we introduce two versions of the product construction, each having a computational advantage against the other.

Product Construction (First Version). The *product PTA* $\mathcal{C} \otimes \mathcal{A}_q$ between \mathcal{C} and \mathcal{A} with initial mode q is defined as the PTA

$(L_{\otimes}, \ell_{\otimes}^*, \mathcal{X}_{\otimes}, Act_{\otimes}, inv_{\otimes}, enab_{\otimes}, prob_{\otimes}, \mathcal{L}_{\otimes})$, where:

- $L_{\otimes} := L \times Q$;
- $\ell_{\otimes}^* := (\ell^*, q^*)$ where q^* is the unique mode such that $\kappa((q, \mathbf{0}), \mathcal{L}(\ell^*)) = (q^*, \mathbf{0})$;
- $\mathcal{X}_{\otimes} := \mathcal{X}_1 \cup \mathcal{X}_2$;
- $Act_{\otimes} := Act \times \mathcal{G}$;
- $inv_{\otimes}(\ell, q) := inv(\ell)$ for all $(\ell, q) \in L_{\otimes}$;
- $enab_{\otimes}((\ell, q), (a, R)) := enab(\ell, a) \wedge \phi_R$ for all $(\ell, q) \in L_{\otimes}$, where ϕ_R is any clock constraint such that $\llbracket \phi_R \rrbracket = R$;
- $\mathcal{L}_{\otimes}(\ell, q) := \{q\}$ for all $(\ell, q) \in L_{\otimes}$

- $prob_{\otimes}$ is given by

$$prob_{\otimes}((\ell, q), (a, R))(Y, (\ell', q')) :=$$

$$\begin{cases} prob(\ell, a)(Y \cap \mathcal{X}_1, \ell') & \text{if } (q, \mathcal{L}(\ell'), \phi_R^{q, \mathcal{L}(\ell')}, Y \cap \mathcal{X}_2, q') \in \Delta \\ 0 & \text{otherwise} \end{cases}$$

where $(q, \mathcal{L}(\ell'), \phi_R^{q, \mathcal{L}(\ell')}, Y \cap \mathcal{X}_2, q')$ is the unique rule such that for all $\nu \in R$, $\nu \in \llbracket \phi_R^{q, \mathcal{L}(\ell')} \rrbracket$. The uniqueness follows from determinism and totality of DTAs.

Apart from standard constructions (e.g., the Cartesian product between L and Q), the product construction also has Cartesian product between Act and \mathcal{G} . Then for each extended action (a, R) , the enabling condition for this action is just the conjunction between $enab(\ell, a)$ and R . This is to ensure that when the action (a, R) is taken, the clock valuation under \mathcal{A} lies in R . Finally in the definition for $prob_{\otimes}$, upon the action (a, R) and the target location ℓ' , the

DTA \mathcal{A} chooses the unique rule $(q, \mathcal{L}(\ell'), \phi_R^{q, \mathcal{L}(\ell')}, Y \cap \mathcal{X}_2, q')$ and then jump to q' with reset set $Y \cap \mathcal{X}_2$. By integrating regions into the enabling condition, the DTA \mathcal{A} can know the status of the clock valuation under \mathcal{A} through its region, hence can decide which rule to use for the transition. This version of product construction works well if the number of regions is not large. We note that the number of regions only depends on N , not on the size of \mathcal{A} . In the following, we introduce another version which depends directly on the size of \mathcal{A} . The second version has an advantage when the number of regions is large.

Product Construction (Second Version). For each $q \in Q$, we let

$$\mathcal{T}_q := \{h : \Sigma \rightarrow CC(\mathcal{X}_2) \mid \forall b \in \Sigma. (q, b, h(b), X, q') \in \Delta \text{ for some } X, q')\}.$$

Intuitively, every element of \mathcal{T}_q is a tuple of clock constraints $\{\phi_b\}_{b \in \Sigma}$, where each clock constraint ϕ_b is chosen from the rules emitting from q and b . The *product PTA* $\mathcal{C} \otimes \mathcal{A}_q$ between \mathcal{C} and \mathcal{A} with initial mode q is defined almost the same as in the first version of the product construction, with the following differences:

- $Act_{\otimes} := Act \times \bigcup_q \mathcal{T}_q$;
- $enab_{\otimes}((\ell, q), (a, h)) := enab(\ell, a) \wedge \bigwedge_{b \in \Sigma} h(b)$ for all $(\ell, q) \in L_{\otimes}$ and $h \in \mathcal{T}_q$, and $enab_{\otimes}((\ell, q), (a, h)) := \text{false}$ otherwise;
- $prob_{\otimes}$ is given by

$$prob_{\otimes}((\ell, q), (a, h))(Y, (\ell', q')) :=$$

$$\begin{cases} prob(\ell, a)(Y \cap \mathcal{X}_1, \ell') & \text{if } (q, \mathcal{L}(\ell'), h(\mathcal{L}(\ell')), Y \cap \mathcal{X}_2, q') \in \Delta \\ 0 & \text{otherwise} \end{cases}$$

The intuition for the second version is that it is also possible to specify the information needed to identify the rule to be chosen by the DTA through a local conjunction of the rules emitting from a mode. For each mode, the local conjunction chooses one clock constraint from rules with the same symbol, and group them together through conjunction. From determinism and totality of DTAs, each conjunction constructed in this way determines which rule to use in the DTA for every

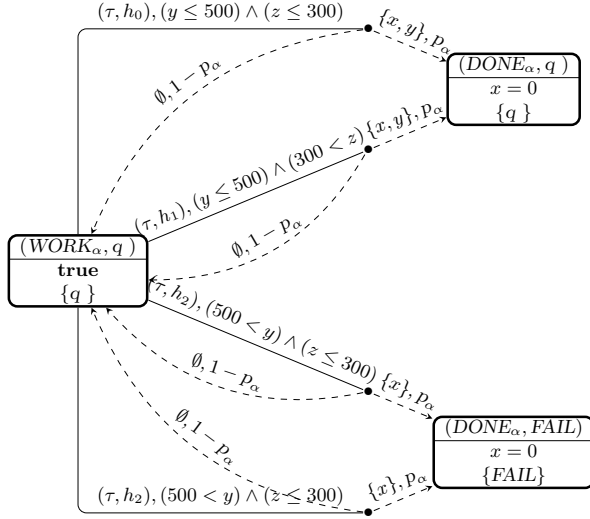


Figure 3: A Part of Product PTA

symbol in a unique way. The advantage of the second version against the first one is that it is more suitable for DTAs with small size and large N (leading to a large number of regions), as the size of the product PTA relies only the size of the DTA.

Example 4.1. Here we represent an running example to show how \mathcal{T}_q works. Here for the accepting mod q in DTA, we have

$\mathcal{T}_q = \{h_0 = \{\emptyset \mapsto \text{true}, \{\alpha\} \mapsto (x \leq 500), \{\beta\} \mapsto (y \leq 300), \{\alpha, \beta\} \mapsto \text{true}\}$
 $h_1 = \{\emptyset \mapsto \text{true}, \{\alpha\} \mapsto (x \leq 500), \{\beta\} \mapsto (300 < y), \{\alpha, \beta\} \mapsto \text{true}\}$
 $h_2 = \{\emptyset \mapsto \text{true}, \{\alpha\} \mapsto (500 < x), \{\beta\} \mapsto (y \leq 300), \{\alpha, \beta\} \mapsto \text{true}\}$
 $h_3 = \{\emptyset \mapsto \text{true}, \{\alpha\} \mapsto (500 < x), \{\beta\} \mapsto (300 < y), \{\alpha, \beta\} \mapsto \text{true}\}$

And a part of the product of Example 2.2 and Example 2.5 is depicted in Figure 2.

REMARK 3. *It is easy to see that the PTA $\mathcal{C} \otimes \mathcal{A}_q$ (in both versions) is well-formed as \mathcal{C} is well-formed and the DTA \mathcal{A} does not introduce extra invariant conditions.*

In the following, we clarify the relationship between \mathcal{C} , \mathcal{A} and $\mathcal{C} \otimes \mathcal{A}_q$. We first show the relationship between paths under \mathcal{C} and paths under $\mathcal{C} \otimes \mathcal{A}_q$. Informally, paths under $\mathcal{C} \otimes \mathcal{A}_q$ are just paths under \mathcal{C} extended with runs of \mathcal{A} .

Transformation \mathcal{T} From Paths under \mathcal{C} into Paths under $\mathcal{C} \otimes \mathcal{A}_q$. Since the two versions of product construction shares similarities, we illustrate the transformation in a unified fashion. The transformation is defined as the function $\mathcal{T} : \text{Paths}_{\mathcal{C}}^* \cup \text{Paths}_{\mathcal{C}}^{\omega} \rightarrow \text{Paths}_{\mathcal{C} \otimes \mathcal{A}_q}^* \cup \text{Paths}_{\mathcal{C} \otimes \mathcal{A}_q}^{\omega}$ which transform a finite or infinite path under \mathcal{C} into one under $\mathcal{C} \otimes \mathcal{A}_q$ as follows. For a finite path

$$\rho = (\ell_0, \nu_0) a_0 \dots a_{n-1} (\ell_n, \nu_n)$$

under \mathcal{C} (note that $(\ell_0, \nu_0) = (\ell^*, \mathbf{0})$ by definition), we define $\mathcal{T}(\rho)$ to be the unique finite path

$$\mathcal{T}(\rho) := ((\ell_0, q_0), \nu_0 \cup \mu_0) a'_0 \dots a'_{n-1} ((\ell_n, q_n), \nu_n \cup \mu_n) \quad (4)$$

under $\mathcal{C} \otimes \mathcal{A}_q$ such that (\dagger)

- $\kappa((q, \mathbf{0}), \mathcal{L}(\ell^*)) = (q_0, \mu_0)$ (note that $\mu_0 = \mathbf{0}$), and
- for all $0 \leq k < n$, if $a_k \in [0, \infty)$ then $a'_k = a_k$ and $(q_k, \mu_k) \xrightarrow{a_k} (q_{k+1}, \mu_{k+1})$, and
- for all $0 \leq k < n$, if $a_k \in \text{Act}$ then $a'_k = (a_k, \xi_k)$ and $(q_k, \mu_k) \xrightarrow{\mathcal{L}(\ell_{k+1})} (q_{k+1}, \mu_{k+1})$, where either (i) the first version of the product construction is taken and ξ_k is the region $[\mu_k]_{\sim}$ or (ii) the second version is taken and ξ_k is the unique function such that for each symbol $b \in \Sigma$, $\xi_k(b)$ is the unique clock constraint appearing in a rule emitting from q_k and with symbol b such that $\mu_k \models \xi_k(b)$.

Likewise, for an infinite path $\pi = (\ell_0, \nu_0) a_0 (\ell_1, \nu_1) a_1 \dots$ under \mathcal{C} , we define $\mathcal{T}(\pi)$ to be the unique infinite path

$$\mathcal{T}(\pi) := ((\ell_0, q_0), \nu_0 \cup \mu_0) a'_0 ((\ell_1, q_1), \nu_1 \cup \mu_1) a'_1 \dots$$

under $\mathcal{C} \otimes \mathcal{A}_q$ such that the three conditions below (\dagger) hold for all $k \in \mathbb{N}_0$ instead of all $0 \leq k < n$. \square

The following lemma shows that \mathcal{T} is a bijection and preserves zenoness.

LEMMA 4.2. *The function \mathcal{T} is a bijection. Moreover, for any infinite path π , π is non-zeno iff $\mathcal{T}(\pi)$ is non-zeno.*

PROOF. The first claim follows straightforwardly from the determinism and totality of DTAs. The second claim follows from the fact that \mathcal{T} preserves time elapses in the transformation. \square

We also show the relationship on schedulers before and after product construction.

Transformation θ From Schedulers under \mathcal{C} into Schedulers under $\mathcal{C} \otimes \mathcal{A}_q$. We define the function θ from the set of schedulers under \mathcal{C} into the set of schedulers under $\mathcal{C} \otimes \mathcal{A}_q$ as follows: for any scheduler σ for \mathcal{C} , $\theta(\sigma)$ (for $\mathcal{C} \otimes \mathcal{A}_q$) is defined such that for any finite path ρ under \mathcal{C} where $\rho = (\ell_0, \nu_0) a_0 \dots a_{n-1} (\ell_n, \nu_n)$ and $\mathcal{T}(\rho)$ is given as in (4),

$$\theta(\sigma)(\mathcal{T}(\rho)) := \begin{cases} \sigma(\rho) & \text{if } n \text{ is even} \\ (\sigma(\rho), \lambda(\rho)) & \text{if } n \text{ is odd} \end{cases}$$

where $\lambda(\rho)$ is either $[\mu_n]_{\sim}$ if the first version of the product construction is taken, or the unique function such that for each symbol $b \in \Sigma$, $\lambda(\rho)(b)$ is the unique clock constraint appearing in a rule emitting from q_k and with symbol b such that $\mu_n \models \lambda(\rho)(b)$. Note that the well-definedness of θ follows from Lemma 4.2. \square

By Lemma 4.2, the product construction and the determinism and totality of DTAs, one can prove straightforwardly the following lemma.

LEMMA 4.3. *The function θ is a bijection.*

Now we show the relationship between infinite paths accepted by a DTA before product construction and infinite paths visiting certain target locations after product construction. Below we lift the function \mathcal{T} to all subsets of paths in the standard fashion: for all subsets $A \subseteq \text{Paths}_{\mathcal{C}}^* \cup \text{Paths}_{\mathcal{C}}^{\omega}$, $\mathcal{T}(A) := \{\mathcal{T}(\omega) \mid \omega \in A\}$.

Definition 4.4 (Traces). Let $\mathcal{T}(\pi) = ((\ell_0, q_0), \nu_0 \cup \mu_0) a'_0((\ell_1, q_1), \nu_1 \cup \mu_1) a'_1 \dots$ the trace of $\mathcal{T}(\pi)$ is defined by $trace(\mathcal{T}(\pi)) := q_0 q_1 \dots$

Verifying Limit Rabin Properties. Paths in $\mathcal{C} \otimes \mathcal{A}_q$ that \mathcal{C} is accepted by \mathcal{A} is

$$RabinPaths_{\mathcal{C} \otimes \mathcal{A}_q, \sigma} = \left\{ \pi \in Paths_{\mathcal{C} \otimes \mathcal{A}_q, \sigma}^\omega \mid \mathbf{ACC}(\inf\{trace(\pi)\}, \mathcal{F}) \right\}$$

and $RabinPaths_{\mathcal{C} \otimes \mathcal{A}_q, \sigma}$ is an limit LT Property [?, Notation10.121].

PROPOSITION 4.5. For any scheduler σ and any initial mode q on DTA \mathcal{A} ,

$$\mathcal{T}\left(AccPaths_{\mathcal{C}, \sigma}^{\mathcal{A}, q}\right) = RabinPaths_{\mathcal{C} \otimes \mathcal{A}_q, \theta(\sigma)}.$$

PROOF. By definition we have

$$AccPaths_{\mathcal{C}, \sigma}^{\mathcal{A}, q} = \left\{ \pi \in Paths_{\mathcal{C}, \sigma}^\omega \mid \mathbf{ACC}(\inf\{traj(\mathcal{A}_{(q^*, 0)}(\mathcal{L}(\pi)))\}, \mathcal{F}) \right\},$$

where $q^* = \kappa((q, 0), \mathcal{L}(\text{init}(\pi)))$. Let $\pi = (\ell_0, \nu_0) a_0(\ell_1, \nu_1) a_1 \dots$ be any infinite path. And by definition of \mathcal{T} we have

$$\mathcal{T}(\pi) = ((\ell_0, q_0), \nu_0 \cup \mu_0) a'_0((\ell_1, q_1), \nu_1 \cup \mu_1) a'_1 \dots$$

$$\mathcal{A}_{(q^*, 0)}(\mathcal{L}(\pi)) = \{(q_n, \mu_n, \mathcal{L}(\pi)_n)\}_{n \in \mathbb{N}_0}.$$

Then it's obvious that

$$trace(\mathcal{T}(\pi)) = q_0 q_1 \dots = traj(\mathcal{A}_{(q^*, 0)}(\mathcal{L}(\pi))).$$

Then we conclude that $\inf\{trace(\mathcal{T}(\pi))\}$ is Rabin accepting by \mathcal{F} iff $\inf\{traj(\mathcal{A}_{(q^*, 0)}(\mathcal{L}(\pi)))\}$ is Rabin accepting by \mathcal{F} . \square

Finally, we demonstrate the relationship between acceptance probabilities before product construction and reachability probabilities after product construction. We also clarify the probability of zenoness before and after the product construction.

THEOREM 4.6. For any scheduler σ and initial mode q ,

$$\mathbf{p}_q^\sigma = \mathbb{P}^{\mathcal{C}, \sigma}\left(AccPaths_{\mathcal{C}, \sigma}^{\mathcal{A}, q}\right) = \mathbb{P}^{\mathcal{C} \otimes \mathcal{A}_q, \theta(\sigma)}\left(RabinPaths_{\mathcal{C} \otimes \mathcal{A}_q, \theta(\sigma)}\right).$$

Moreover, $\mathbb{P}^{\mathcal{C}, \sigma}(\{\pi \mid \pi \text{ is zeno}\}) = \mathbb{P}^{\mathcal{C} \otimes \mathcal{A}_q, \theta(\sigma)}(\{\pi' \mid \pi' \text{ is zeno}\})$.

PROOF. Define the probability measure \mathbb{P}' by: $\mathbb{P}'(A) = \mathbb{P}^{\mathcal{C} \otimes \mathcal{A}_q, \theta(\sigma)}(\mathcal{T}(A))$ for $A \in \mathcal{F}^{\mathcal{C}, \sigma}$. We show that $\mathbb{P}' = \mathbb{P}^{\mathcal{C}, \sigma}$. By [?, Theorem 3.3], it suffices to consider cylinder sets as they form a pi-system (cf. [?, Page 43]). Let $\rho = (\ell_0, \nu_0) a_0 \dots a_{n-1}(\ell_n, \nu_n)$ be any finite path under \mathcal{C} . By definition, we have that

$$\begin{aligned} \mathbb{P}^{\mathcal{C}, \sigma}(Cyl(\rho)) &= \mathbb{P}^{\mathcal{C} \otimes \mathcal{A}_q, \theta(\sigma)}(Cyl(\mathcal{T}(\rho))) \\ &= \mathbb{P}^{\mathcal{C} \otimes \mathcal{A}_q, \theta(\sigma)}(\mathcal{T}(Cyl(\rho))) \\ &= \mathbb{P}'(Cyl(\rho)). \end{aligned}$$

The first equality comes from the fact that both versions of product construction preserves transition probabilities. The second equality is due to $Cyl(\mathcal{T}(\rho)) = \mathcal{T}(Cyl(\rho))$. The final equality follows from the definition. Hence $\mathbb{P}^{\mathcal{C}, \sigma} = \mathbb{P}'$. Then the first claim follows from Proposition 4.5 and the second claim follows from Lemma 4.2. \square

Note that a side result from Theorem 4.6 says that θ preserves time-divergence for schedulers before and after product construction. From Theorem 4.6 and Lemma 4.3, one immediately obtains the following result which transforms the PTA-DTA problem into computing reachability probabilities under the product PTA.

COROLLARY 4.7. ([?,]) For any initial mode q ,

$$opt_\sigma \mathbf{p}_q^\sigma = opt_{\sigma'} \mathbb{P}^{\mathcal{C} \otimes \mathcal{A}_q, \sigma'}(RabinPaths_{\mathcal{C} \otimes \mathcal{A}_q, \sigma'})$$

where opt refers to either \inf (infimum) or \sup (supremum), σ (resp. σ') range over all time-divergent schedulers for \mathcal{C} (resp. $\mathcal{C} \otimes \mathcal{A}_q$).

The way [?] discards time-convergent path is making a copy of every location in PTA model and enforcing a transition from the original one to the copy happen when 1 time unit is passed. After transiting to the copy, A transition back to the original one will immediately happend with no delay. And we put a label *tick* in copy. We only deal with paths that satisfy $\Box \Diamond tick$ (i.e. *tick* is satisfied infinitely many times).

Then an MDP $\text{Reg}[\mathcal{C} \otimes \mathcal{A}_q]$ is obtained from the enlarged PTA of $\mathcal{C} \otimes \mathcal{A}_q$ through an region construction. Then we verify the limit rabin property on $\text{Reg}[\mathcal{C} \otimes \mathcal{A}_q]$ by using a standard MEC algorithm. First, We find all MECs satisfy the corresponding property of an Rabin acceptance condition. In order to guarantee time-divergence, we only pick up MECs with at least one location that has an *tick* label and let F_* be the union of those MECs. Then, we turn to resolve the probability reachability to F_* .

LEMMA 4.8. Time Complexity of Verifying Limit Rabin Properties([?, Theorem 10.127]) Let M be a finite MDP and P be a limit LT property specified by a Rabin condition:

$$\bigvee_{1 \leq i \leq n} (\Diamond \Box \neg H_i \wedge \Box \Diamond K_i)$$

Then: the values $opt_\sigma \mathbb{P}^{M, \sigma}(s \models P)$ can be computed in time $\mathcal{O}(\text{poly}(\text{size}(M)) \cdot k)$ where opt refers to either \inf (infimum) or \sup (supremum).

Noting that for $\mathcal{C} \otimes \mathcal{A}_q$, although the upper bound of $|Act_\otimes|$ is $|Act| \cdot |Q| \cdot |\Delta|^{|\Sigma|}$, $|L_\otimes|$ is polynomial to $|L| \cdot |Q|$, and $|\mathcal{X}_\otimes| = |\mathcal{X}_1| + |\mathcal{X}_2|$. The size of $\text{Reg}[\mathcal{C} \otimes \mathcal{A}_q]$ is exponential to $|L| \cdot |Q|$ while the number of transitions is exponential, then $opt_\sigma \mathbf{p}_q^\sigma$ can be calculated in exponential time follows from Lemma 4.8.

In [?], the authors proved that the reachability problem for arbitrary PTAs is *EXPTIME*-complete. Reduction from the PTA reachability problem to the PTA-DTA model-checking problem can be easily constructed as follows.

For an arbitrary PTA $\mathcal{C} = (L, l^*, \mathcal{X}, Act, inv, enab, prob, \mathcal{L})$ and a set of final locations $L_F \subseteq L$. Let $\mathcal{C}' = (L, l^*, \mathcal{X}, Act, inv, enab, prob, \mathcal{L})$ where

$$\mathcal{L}'(l) : L \rightarrow AP \cup \{\text{acc}\} = \begin{cases} \mathcal{L}(l) & \text{if } l \notin L_F \\ \mathcal{L}(l) \cup \{\text{acc}\} & l \in L_F \end{cases}$$

and DTA $\mathcal{A}' = (Q = \{q_0, q_1\}, \Sigma = 2^{AP \cup \{\text{acc}\}}, \mathcal{X} = \emptyset, \Delta, \mathcal{F} = \{(\emptyset, \{q_1\})\})$ where

- $\forall \sigma \in \Sigma, \text{acc} \in \sigma \rightarrow (q_0, \sigma, \text{true}, \emptyset, q_1) \in \text{Delta},$
- $\forall \sigma \in \Sigma, i = 0, 1, (q_i, \sigma, \text{true}, \emptyset, q_i) \in \Delta.$

It's clear that L_F is reachable in \mathcal{C} iff. for \mathcal{C}' and \mathcal{A}' , $\sup_{\sigma} \mathbf{p}_{q_0}^{\sigma} = 1$.

PROPOSITION 4.9. *The PTA-TRA problem is EXPTIME-complete.*

5 UNDECIDABILITY OF PTA-NTA PROBLEM

We show that the qualitative problem for minimum probabilities is already undecidable. We prove this by a reduction from the universality problem of timed automata, which is illustrated as follows.

LEMMA 5.1. *A timed language is accepted by some timed Büchi automaton iff it is accepted by some timed Rabin automaton.*

PROOF. The construction is similar to [?, Theorem 3.20.] \square

LEMMA 5.2. ([?, Theorem 5.2.]) *Given a timed automaton over an alphabet Σ , the problem of deciding whether it accepts all time-divergent timed words over Σ is undecidable.*

The proof of lemma 5.2 is based on a construction of timed Büchi automata and it also holds for timed rabin automata since lemma 5.1.

PROPOSITION 5.3. *Given a non deterministic timed rabin automaton \mathcal{A} over an alphabet Σ , the qualitative problem of the minimal probability that \mathcal{C} observes \mathcal{A} under initial mode $q_{start} \in Q$ is undecidable.*

PROOF. For any non deterministic TRA $\mathcal{A} = (Q, \Sigma, \mathcal{X}, \Delta)$, let $\Sigma = \{b_1, b_2, \dots, b_k\}$.

we construct an $\mathcal{A}' = (Q', \Sigma', \mathcal{X}', \Delta')$ where

$$Q' = Q \cup \{q_{init}\}, \Sigma' = \Sigma \cup \{b_0\}, \Delta' = \Delta \cup \{(q_{init}, b_0, \text{true}, \mathcal{X}, q_{start})\}.$$

We can choose an appropriate AP such that $k+1 \leq |2^{AP}|$ and assign each b_i to a different subset of AP. So we simplify the label of locations in \mathcal{C} by single letters in Σ' .

Let PTA $\mathcal{C} = (L, \ell^*, \mathcal{X}, \text{Act}, \text{inv}, \text{enab}, \text{prob}, \mathcal{L})$ where

- $L := \Sigma'$,
- $\ell^* := b_0$,
- $\mathcal{X} := \emptyset$,
- $\text{Act} := \Sigma$,
- $\text{inv}(b_i) := \text{true}$, for all $b_i \in L$,
- $\text{enab}(b_i, b_j) := \text{true}$, for all $b_i \in L$ and all $b_j \in \text{Act}$,
- $\text{prob}(b_i, b_j) := \mu_{(\emptyset, b_j)}$, for all $b_i \in L$ and all $b_j \in \text{Act}$,
- $\mathcal{L}(b_i) := b_i$, for all $b_i \in L$.

It is natural to see, for any time word $w = \alpha_0 \alpha_1 \alpha_2 \dots$ there is a scheduler $\sigma_w(\rho) := \alpha_{|\rho|}$ such that $\mathbb{P}^{\mathcal{C}, \sigma_w}(\{w\}) = 1$. σ_w is time-divergent since $\text{Paths}_{\mathcal{C}, \sigma}^{\mathcal{C}} = \{w\}$ and w is time-divergent. It's natural that

$$\mathbf{p}_{q_{start}}^{\sigma_w} = \begin{cases} 1 & \text{if } \mathcal{A} \text{ accepts } w \text{ w.r.t. } (q_{start}, \mathbf{0}), \\ 0 & \text{if } \mathcal{A} \text{ rejects } w \text{ w.r.t. } (q_{start}, \mathbf{0}). \end{cases}$$

Then we have $\inf_{\sigma} \mathbb{P}^{\mathcal{C}, \sigma}(\text{AccPaths}_{\mathcal{C}, \sigma}^{\mathcal{A}', q_{init}}) = 1$ iff \mathcal{A} accepts all timewords w.r.t. $(q_{start}, \mathbf{0})$. \square

6 INFINITE-STATE-MDP CONSTRUCTION

Now we present the finite acceptance of nondeterministic timed automata for PTAs.

Definition 6.1 (Finite Acceptance Criterion). Let $F \subseteq Q$ be a set of final modes. An infinite word w is *finitely accepted* by \mathcal{A} w.r.t the initial configuration (q, ν) and F if $\mathcal{A}_{q, \nu}(w) = \{(q_n, \nu_n, a_n)\}_{n \in \mathbb{N}_0}$ satisfies that $q_n \in F$ for some $n \in \mathbb{N}_0$.

Definition 6.2 (Path Acceptance). An infinite path π under \mathcal{C} is *finitely accepted* by \mathcal{A} w.r.t initial configuration (q, ν) , if the infinite word $\mathcal{L}(\pi)$ is finitely accepted by \mathcal{A} w.r.t $(\kappa((q, \nu), \mathcal{L}(\text{init}(\pi))), \mathbf{0})$.

Below we fix a well-formed PTA \mathcal{C} taking the form (1) and a NTA \mathcal{A} taking the form (2) with the difference that the set of clocks for \mathcal{C} (resp. for \mathcal{A}) is denoted by \mathcal{X} (resp. \mathcal{Y}). W.l.o.g., we assume that $\mathcal{X} \cap \mathcal{Y} = \emptyset$ and $\Sigma = 2^{AP}$.

Let PTA be \mathcal{C} with the set \mathcal{X} and the NTA be \mathcal{A} with the set \mathcal{Y} .

The transformation to MDP is as follows.

Let \mathcal{Y} be a fixed finite set of clocks. We use integer Subscript denote a set of new clocks. Formally $\mathcal{Y}_k = \{(t, y) \in \mathbb{N} \times \mathcal{Y} \mid t = k\}$ for $k > 0$. For convenience, we use \mathcal{Y}_0 denote \mathcal{X} .

And $R^{\mathcal{Y}_k}$ is a region for \mathcal{Y}_k .

Definition 6.3 (Product Construction (Infinite-State-MDP)). The product MDP $\mathcal{C} * \mathcal{A}_q$ between \mathcal{C} and \mathcal{A} with initial mode q is defined as the PTA

The transformation to MDP is follows. A state in $\mathcal{C} * \mathcal{A}_q$ is of the form

$$\left(\ell, (q_1, \dots, q_n), \mathcal{X} \cup \left(\bigcup_{k=1}^n \mathcal{Y}_k \right), R \right) \quad (5)$$

where n is an unbounded natural number, ℓ (w.r.t q_i) is a location in \mathcal{C} (w.r.t a mod in \mathcal{A}) and R is a region with clock names being $\mathcal{X} \cup (\bigcup_{k=1}^n \mathcal{Y}_k)$. The intuition is that $(\ell, R \downarrow \mathcal{X})$ reflects the region for \mathcal{C} , $((q_1, R \downarrow \mathcal{Y}_1) \dots, (q_n, R \downarrow \mathcal{Y}_n))$ reflects a power set for \mathcal{A} .

Definition 6.4 (Rename function). Let \mathcal{X} and \mathcal{Y} be two sets of clocks, ν is a clock valuation on \mathcal{X} and $f : \mathcal{X} \leftrightarrow \mathcal{Y}$ is a rename function then $\nu[f] = \nu \circ f^{-1}$.

LEMMA 6.5. Let R is a region with clock names \mathcal{X} and $X \subseteq \mathcal{X}$, $R \downarrow X$ is a region with clock names X .

Definition 6.6 (Time successor). A state

$$s' = \left(\ell, (q_1, \dots, q_n), \mathcal{X} \cup \left(\bigcup_{k=1}^n \mathcal{Y}_k \right), R' \right)$$

is a time successor of s in the form of (5) where either

- $s = s'$ if $\forall \nu \in R, t \in \mathbb{R}_{>0} : \nu + t \in R'$ or

- R' is another unique region if there exist a $\nu \in R$ s.t.

$$\begin{aligned} & \exists t \in \mathbb{R}_{\geq 0} : (\nu + t \in R' \wedge \forall t' \in [0, t] : \\ & ((\nu + t' \in R \cup R') \wedge \nu + t' \models \text{inv}(l))) \end{aligned}$$

Definition 6.7 (Transition relation). The transition relation \rightarrow is the smallest relation such that the following two inference rules are satisfied :

$$\begin{aligned} (\text{Delay}) \quad & \frac{s' \text{ is the time successor of } s}{s \xrightarrow{\tau} \mu_{s'}} \\ (\text{Jump}) \quad & \frac{\nu \in R \quad (\ell, \nu \downarrow \mathcal{X}) \xrightarrow{a} \mu \quad \nu \downarrow \mathcal{X} \models \text{enab}(\ell, a)}{s \xrightarrow{a} \mu^*} \end{aligned}$$

where, let

$$s' = \left(\ell', \left(q_{1_0} \cdots, q_{i_0} \cdots, q_{i_{k_i}} \cdots, q_{n_{k_n}} \right), \mathcal{X} \cup \left(\bigcup_{i=1}^{n'} \bigcup_{j=0}^{k_i} \mathcal{Y}_{i_j} \right), R' \right)$$

$$\mu^*(s') = \begin{cases} \mu(X, \ell') & \dagger \\ 0 & \text{otherwise} \end{cases}$$

The none zero case hold if $(R' \downarrow \mathcal{X}) = [\nu \downarrow \mathcal{X}[X := 0]]_{\sim}$, there exists $(q_i, \mathcal{L}(\ell'), \phi, Y_{i_j}, q_{i_j}) \in \Delta$ such that $R' \downarrow \mathcal{Y}_{i_j} = [(\nu \downarrow \mathcal{Y}_i)[Y_{i_j} := 0][y \mapsto \langle i_j, y \rangle]]_{\sim}$ and $R \downarrow \mathcal{Y}_i \subseteq \llbracket \phi \rrbracket$, k_i is the number of successors of q_i .

7 CONCLUSION AND FUTURE WORK

In this paper, we studied the linear-time model-checking problem PTA-DTA of DTA-specifications over PTAs. To solve the problem, we gave two versions of product construction (between a PTA and a DTA) which both reduce the problem to computing reachability probabilities over PTAs, for which efficient algorithms exist [? ?]. Both the product constructions are nontrivial and are elaborated so that one caters for DTAs with a small number of regions and the other for DTAs with small size. Then we demonstrated two case studies clarifying that the problem PTA-DTA can be applied to real-world applications. Experimental results show that our product construction is efficient to solve the problem. A challenging future work is to study the PTA-DTA problem with general timed-automata specifications. Another future work is to integrate costs or rewards into this problem.

Acknowledgements. We thank Arnd Hartmanns for valuable suggestions on probabilistic timed automata.

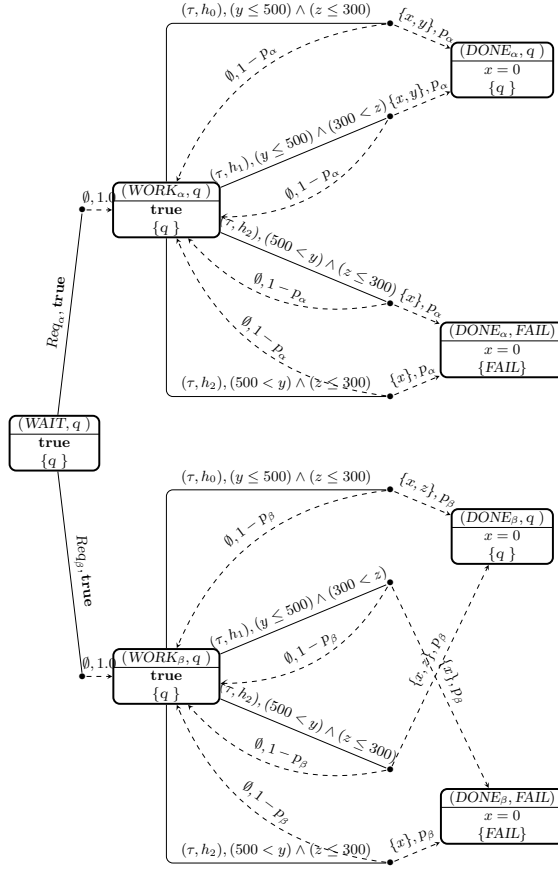


Figure 4: A Big Part of Product PTA

A APPENDIX