

Learning One-Clock Timed Automata

Jie An¹, Mingshuai Chen², Bohua Zhan³, Naijun Zhan³, and Miaomiao Zhang¹

¹ School of Software Engineering, Tongji University, Shanghai, China
 {1510796, miaomiao}@tongji.edu.cn

² Lehrstuhl für Informatik 2, RWTH Aachen University, Aachen, Germany
 chenms@cs.rwth-aachen.de

³ State Key Lab. of Computer Science, Institute of Software, CAS, Beijing, China &
 University of Chinese Academy of Sciences, Beijing, China
 {bzhan, znj}@ios.ac.cn

Abstract. We present an algorithm for active learning of deterministic timed automata with a single clock. The algorithm is within the framework of Angluin’s L^* algorithm and inspired by existing work on the active learning of symbolic automata. Due to the need of guessing for each transition whether it resets the clock, the algorithm is of exponential complexity in the size of the learned automata. Before presenting this algorithm, we propose a simpler version where the teacher is assumed to be *smart* in the sense of being able to provide the reset information. We show that this simpler setting yields a polynomial complexity of the learning process. Both of the algorithms are implemented and evaluated on a collection of randomly generated examples. We furthermore demonstrate the simpler algorithm on the functional specification of the TCP protocol.

Keywords: Automaton learning · Active learning · One-clock timed automata · Timed language · Reset-logical-timed language

1 Introduction

In her seminal work [7], Angluin introduced the L^* algorithm for learning a regular language from queries and counterexamples within a query-answering framework. The Angluin-style learning therefore is also termed *active learning* or *query learning*, which is distinguished from *passive learning*, i.e., generating a model from a given data set. Following this line of research, an increasing number of efficient active learning methods (cf. [35]) have been proposed to learn, e.g., Mealy machines [31,27], I/O automata [2], register automata [22,1,12], nondeterministic finite automata [9], Büchi automata [16,25], symbolic automata [26,15,8] and Markov decision processes [33], to name just a few. Full-fledged libraries, tools and applications are also available for automata-learning tasks [10,24,17,18].

For real-time systems where timing constraints play a key role, however, learning a formal model is much more complicated. As a classical model for real-time systems, timed automata [4] have an infinite set of timed actions. This yields a fundamental difference to finite automata featuring finite alphabets. Moreover, it is difficult to detect resets of clock variables from observable behaviors of the system. This makes learning formal models of timed systems a challenging yet interesting problem.

Related work. Various attempts have been carried out in the literature on learning timed models, which can be classified into two tracks. The first track pursues active learning methods, e.g. [19] for learning event-recording automata [5], which are time automata that, for every untimed action a , a clock is used to record the time of the last occurrence of a . The underlying learning algorithm, however, is prohibitively complex due to too many degrees of freedom and multiple clocks for recording events. The other track pursues passive learning. In [39,38], an algorithm was proposed to learn deterministic real-time automata (i.e., loosely, timed automata with one single clock that resets at every transition [14]) from labelled time-stamped event sequences. The basic idea is that the learner organizes a tree sketching traces of the data set while merging nodes of the tree following a certain heuristic function. A passive learning algorithm for timed automata with one clock was further proposed in [36,37]. A common weakness of passive learning methods is that the generated model merely accepts all positive traces while rejects all negative ones for the given set of traces, without guaranteeing that it is a correct model of the target system. A theoretical result was established in [37] showing it is possible to obtain the target system by continuously enriching the data set, however the number of iterations is unknown. In addition, the passive learning methods cited above concern only discrete-time semantics of the underlying timed models, i.e., the clock takes values from non-negative integers. We furthermore refer the readers to [11,29] for learning specialized forms of practical timed systems in a passive manner, [34] for passively learning timed automata using genetic programming which scales to automata of the large size, [30] for learning probabilistic real-time automata incorporating clustering techniques in machine learning, and [33] for L^* -based learning of Markov decision processes with testing and sampling.

In this paper, we present the first active learning method for deterministic one-clock timed automata (DOTAs) under continuous-time semantics¹. Such timed automata provide simple models while preserving adequate expressiveness, and therefore have been widely used in practical real-time systems [32,3,13]. We present our approach in two steps. First, we describe a simpler algorithm, under the assumption that the teacher is *smart* in the sense of being able to provide information about clock resets in membership and equivalence queries. The basic idea is as follows. We define the *reset-logical-timed language* of a DOTA and show that the timed languages of two DOTAs are equivalent if their reset-logical-timed languages are equivalent, which reduces the learning problem to that of learning a reset-logical-timed language. Then we show how to learn the reset-logical-timed language following Maler and D’Antoni’s learning algorithms for symbolic automata [26,15]. We claim the correctness, termination and polynomial complexity of this learning algorithm. Next, we extend this algorithm to the case of a normal teacher. The main difference is that the learner now needs to *guess* the reset information on transitions discovered in the observation table. Due to these guesses, the latter algorithm features exponential complexity in the size of the learned automata. The proposed learning methods are implemented and evaluated on randomly generated examples. We also demonstrate the simpler, polynomial algorithm on a practical case study concerning the functional specification of the TCP protocol. Detailed proofs for theorems and lemmas in this paper can be found in Appendix A.

¹ The proposed learning method applies trivially to discrete-time semantics too.

Structure. Section 2 provides preliminary definitions on one-clock timed automata. The learning algorithm with a smart teacher is presented and analyzed in Section 3. We then present the situation with a normal teacher in Section 4. The experimental results are reported in Section 5. Finally, Section 6 concludes this paper.

2 Preliminaries

Let $\mathbb{R}_{\geq 0}$ and \mathbb{N} be the set of non-negative reals and natural numbers, respectively, and \mathbb{B} the Boolean set. We use \top to stand for true and \perp for false. The projection of an n -tuple \mathbf{x} onto its first two components is denoted by $\Pi_{\{1,2\}}\mathbf{x}$, which extends to a sequence of tuples as $\Pi_{\{1,2\}}(\mathbf{x}_1, \dots, \mathbf{x}_k) = (\Pi_{\{1,2\}}\mathbf{x}_1, \dots, \Pi_{\{1,2\}}\mathbf{x}_k)$.

Timed automata [4], a kind of finite automata extended with a finite set of real-valued clocks, are widely used to model real-time systems. In this paper, we consider a subclass of timed automata with a single clock, termed *one-clock timed automata* (OTAs). Let c be the clock variable, denote by Φ_c the set of clock constraints of the form $\phi ::= \top \mid c \bowtie m \mid \phi \wedge \phi$, where $m \in \mathbb{N}$ and $\bowtie \in \{=, <, >, \leq, \geq\}$.

Definition 1 (One-clock timed automata). A *one-clock timed automaton* (OTA) \mathcal{A} is a 6-tuple $(\Sigma, Q, q_0, F, c, \Delta)$, where Σ is a finite set of actions, called the alphabet; Q is a finite set of locations; $q_0 \in Q$ is the initial location; $F \subseteq Q$ is a set of accepting locations; c is the unique clock; and $\Delta \subseteq Q \times \Sigma \times \Phi_c \times \mathbb{B} \times Q$ is a finite set of transitions.

A transition $\delta = (q, \sigma, \phi, b, q')$ allows a jump from the *source location* q to the *target location* q' by performing the action $\sigma \in \Sigma$ if the constraint $\phi \in \Phi_c$ is satisfied. Meanwhile, clock c is reset to zero if $b = \top$, and remains unchanged otherwise.

A *clock valuation* is a function $\nu: c \mapsto \mathbb{R}_{\geq 0}$ that assigns a non-negative real number to the clock. For $t \in \mathbb{R}_{\geq 0}$, let $\nu + t$ be the clock valuation with $(\nu + t)(c) = \nu(c) + t$. According to the definitions of clock valuation and clock constraint, a transition *guard* can be represented as an interval whose endpoints are in $\mathbb{N} \cup \{\infty\}$. For example, $\phi_1: c < 5 \wedge c \geq 3$ is represented as $[3, 5)$, $\phi_2: c = 6$ as $[6, 6]$, and $\phi_3: \top$ as $[0, \infty)$. We will use the inequality- and interval-representation interchangeably in this paper.

A *state* s of \mathcal{A} is a pair (q, ν) , where $q \in Q$ and ν is a clock valuation. A *run* ρ of \mathcal{A} is a finite sequence $\rho = (q_0, \nu_0) \xrightarrow{t_1, \sigma_1} (q_1, \nu_1) \xrightarrow{t_2, \sigma_2} \dots \xrightarrow{t_n, \sigma_n} (q_n, \nu_n)$, where $\nu_0(c) = 0$, $t_i \in \mathbb{R}_{\geq 0}$ stands for the time delay spending on q_{i-1} before $\delta_i = (q_{i-1}, \sigma_i, \phi_i, b_i, q_i) \in \Delta$ is taken, only if (1) $\nu_{i-1} + t_i$ satisfies ϕ_i , (2) $\nu_i(c) = \nu_{i-1}(c) + t_i$ if $b_i = \perp$, otherwise $\nu_i(c) = 0$, for all $1 \leq i \leq n$. A run ρ is *accepting* if $q_n \in F$.

The *trace* of a run ρ is a timed word, denoted by $\text{trace}(\rho)$. $\text{trace}(\rho) = \epsilon$ if $\rho = (q_0, \nu_0)$, and $\text{trace}(\rho) = (\sigma_1, t_1)(\sigma_2, t_2) \dots (\sigma_n, t_n)$ if $\rho = (q_0, \nu_0) \xrightarrow{t_1, \sigma_1} (q_1, \nu_1) \xrightarrow{t_2, \sigma_2} \dots \xrightarrow{t_n, \sigma_n} (q_n, \nu_n)$. Since t_i is the time delay on q_{i-1} , for $1 \leq i \leq n$, such a timed word is also called *delay-timed word*. The corresponding *reset-delay-timed word* can be defined as $\text{trace}_r(\rho) = (\sigma_1, t_1, b_1)(\sigma_2, t_2, b_2) \dots (\sigma_n, t_n, b_n)$, where b_i is the reset indicator for δ_i , for $1 \leq i \leq n$. If ρ is an accepting run of \mathcal{A} , $\text{trace}(\rho)$ is called an *accepting timed word*. The *recognized timed language* of \mathcal{A} is the set of accepting delay-timed words, i.e., $\mathcal{L}(\mathcal{A}) = \{\text{trace}(\rho) \mid \rho \text{ is an accepting run of } \mathcal{A}\}$. The *recognized reset-timed language* $\mathcal{L}_r(\mathcal{A})$ is defined as $\{\text{trace}_r(\rho) \mid \rho \text{ is an accepting run of } \mathcal{A}\}$.

The delay-timed word $\omega = (\sigma_1, t_1)(\sigma_2, t_2) \cdots (\sigma_n, t_n)$ is observed outside, from the view of the global clock. On the other hand, the behavior can also be observed inside, from the view of the local clock. This results in a *logical-timed word* of the form $\gamma = (\sigma_1, \mu_1)(\sigma_2, \mu_2) \cdots (\sigma_n, \mu_n)$ with

$$\mu_i = \begin{cases} t_i, & \text{if } i = 1 \text{ or } b_{i-1} = \top \\ \mu_{i-1} + t_i, & \text{otherwise.} \end{cases}$$

We will denote the mapping from delay-timed words to logical-timed words above by Γ . Similarly, we introduce *reset-logical-timed word* $\gamma_r = (\sigma_1, \mu_1, b_1)(\sigma_2, \mu_2, b_2) \cdots (\sigma_n, \mu_n, b_n)$ as the counterpart of $\omega_r = (\sigma_1, t_1, b_1)(\sigma_2, t_2, b_2) \cdots (\sigma_n, t_n, b_n)$ in terms of the local clock. Without any substantial change, we can extend the mapping Γ to map reset-delay-timed words to reset-logical-timed words. The *recognized logical-timed language* of \mathcal{A} is given as $L(\mathcal{A}) = \{\Gamma(\text{trace}(\rho)) \mid \rho \text{ is an accepting run of } \mathcal{A}\}$, and the *recognized reset-logical-timed language* of \mathcal{A} as $L_r(\mathcal{A}) = \{\Gamma(\text{trace}_r(\rho)) \mid \rho \text{ is an accepting run of } \mathcal{A}\}$.

An OTA is a *deterministic one-clock timed automaton* (DOTA) if there is at most one run for a given delay-timed word. In other words, for any location $q \in Q$ and action $\sigma \in \Sigma$, the guards of transitions outgoing from q labelled with σ are disjoint subsets of $\mathbb{R}_{\geq 0}$. We say a DOTA is *complete* if for any of its location $q \in Q$ and action $\sigma \in \Sigma$, the corresponding guards form a partition of $\mathbb{R}_{\geq 0}$. This means any given delay-timed word has exactly one run. Any DOTA \mathcal{A} can be transformed into a complete DOTA (referred to as COTA) \mathbb{A} accepting the same timed language as follows:

1. Augment Q with a “sink” location q_s which is not an accepting location.
2. For every $q \in Q$ and $\sigma \in \Sigma$, if there is no outgoing transition from q labelled with σ , introduce a (resetting) transition from q to q_s with label σ and guard $[0, \infty)$.
3. Otherwise, let S be the subset of $\mathbb{R}_{\geq 0}$ not covered by the guards of transitions from q with label σ . Write S as a union of intervals I_1, \dots, I_k in a minimal way, then introduce a (resetting) transition from q to q_s with label σ and guard I_j for each $1 \leq j \leq k$.

Example 1. Fig. 1 depicts the transformation of a DOTA \mathcal{A} (left part) into a COTA \mathbb{A} (right part). First, a non-accepting “sink” location $q_s = q_2$ is introduced. Second, we introduce three fresh transitions (marked in blue) from q_1 to q_2 as well as transitions from q_2 to itself. At last, for location q_0 and label a , the existing guards cover $(1, 3)$, with complement $[0, 1] \cup [3, \infty)$. Hence, we introduce transitions $(q_0, a, [0, 1], \top, q_2)$ and $(q_0, a, [3, \infty), \top, q_2)$. Two fresh transitions from q_1 to q_2 are introduced similarly.

From now on, we assume that we are working with complete DOTAs.

3 Learning from a Smart Teacher

In this section, we consider the case of learning a COTA \mathbb{A} with a smart teacher. Our learning algorithm relies on the following reduction of the equivalence over timed languages to that of reset-logical timed languages.

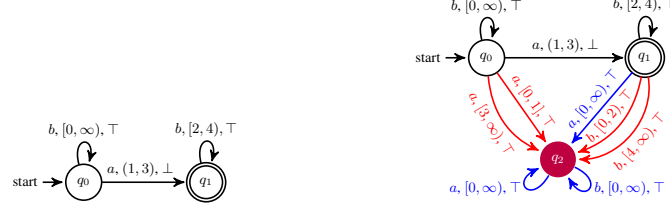


Fig. 1: A DOTA \mathcal{A} on the left and the corresponding COTA \mathbb{A} on the right. The initial location is indicated by ‘start’ and an accepting location is doubly circled.

Theorem 1. *Given two DOTAs \mathcal{A} and \mathcal{B} , if $L_r(\mathcal{A}) = L_r(\mathcal{B})$, then $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$.*

Theorem 1 assures that $L_r(\mathcal{H}) = L_r(\mathbb{A})$ implies $\mathcal{L}(\mathcal{H}) = \mathcal{L}(\mathbb{A})$, that is, to construct a COTA \mathbb{A} that recognizes a target timed language $\mathcal{L} = \mathcal{L}(\mathbb{A})$, it suffices to learn a COTA \mathcal{H} which recognizes the same reset-logical timed language. For equivalence queries, instead of checking directly whether $L_r(\mathcal{H}) = L_r(\mathbb{A})$, the contraposition of Theorem 1 guarantees that we can perform equivalence queries over their timed counterparts: if $\mathcal{L}(\mathcal{H}) = \mathcal{L}(\mathbb{A})$, then \mathcal{H} recognizes the target language already; otherwise, a counterexample making $\mathcal{L}(\mathcal{H}) \neq \mathcal{L}(\mathbb{A})$ yields an evidence also for $L_r(\mathcal{H}) \neq L_r(\mathbb{A})$.

We now describe the behavior of the teacher who keeps an automaton \mathbb{A} to be learnt, while providing knowledge about the automaton by answering membership and equivalence queries through an oracle she maintains. For the membership query, the teacher receives a logical-timed word γ and returns whether γ is in $L(\mathbb{A})$. In addition, she is smart enough to return the reset-logical-timed word γ_r that corresponds to γ (the exact correspondence is described in Sect. 3.1). For the equivalence query, the teacher is given a hypothesis \mathcal{H} and decides whether $\mathcal{L}(\mathcal{H}) = \mathcal{L}(\mathbb{A})$. If not, she is smart enough to return a reset-delayed-timed word ω_r as a counterexample. The usual case where a teacher can deal with only standard delay-timed words will be discussed in Sect. 4.

Remark 1. The assumption that the teacher can respond with timed words coupled with reset information is reasonable, in the sense that the learner can always infer and detect the resets of the logical clock by referring to a global clock on the wall, as long as he can observe running states of \mathbb{A} , i.e., observing the clock valuation of the system whenever an event happens therein. This conforms with the idea of combining automata learning with white-box techniques, as exploited in [21], providing that in many application scenarios source code is available for the analysis.

In what follows, we elaborate the learning procedure including membership queries, hypotheses construction, equivalence queries and counterexample processing.

3.1 Membership query

In our setting, the oracle maintained by the smart teacher can be regarded as a COTA \mathbb{A} that recognizes the target timed language \mathcal{L} , and thereby its logical-timed language $L(\mathbb{A})$ and reset-logical-timed counterpart $L_r(\mathbb{A})$. In order to collect enough information for constructing a hypothesis, the learner makes membership queries as “Is the logical-timed word γ in $L(\mathbb{A})$?”. If there does not exist a run ρ such that $\Gamma(\text{trace}(\rho)) = \gamma$,

meaning that there is some k such that the run is blocked after the k 'th action (i.e. γ is *invalid*) and hence the teacher gives a negative answer, associated with a reset-logical-timed word γ_r where all b_i 's with $i > k$ are set to \top ; If there exists a run ρ (which is unique due to the determinacy of \mathbb{A}) that admits γ (i.e., γ is *valid*), the teacher answers “Yes”, if ρ is accepting, or “No” otherwise, while in both cases providing the corresponding reset-logical-timed word γ_r , with $\Pi_{\{1,2\}}\gamma_r = \gamma$.

For the sake of simplicity, we define a function π that maps a logical-timed word to its unique reset-logical-timed counterpart in membership queries. Information gathered from the membership queries is stored in a timed observation table defined as follows.

Definition 2 (Timed observation table). A timed observation table for a COTA \mathbb{A} is a 7-tuple $\mathbf{T} = (\Sigma, \Sigma, \Sigma_r, S, R, E, f)$ where Σ is the finite alphabet; $\Sigma = \Sigma \times \mathbb{R}_{\geq 0}$ is the infinite set of logical-timed actions; $\Sigma_r = \Sigma \times \mathbb{R}_{\geq 0} \times \mathbb{B}$ is the infinite set of reset-logical-timed actions; $S, R \subset \Sigma_r^*$ and $E \subset \Sigma^*$ are finite sets of words, where S is called the set of prefixes, R the boundary, and E the set of suffixes. Specifically,

- S and R are disjoint, i.e., $S \cup R = S \uplus R$;
- The empty word is by default both a prefix and a suffix, i.e., $\epsilon \in E$ and $\epsilon \in S$;
- $f: (S \cup R) \cdot E \mapsto \{-, +\}$ is a classification function such that for a reset-logical-timed word γ_r , $\gamma_r \cdot e \in (S \cup R) \cdot E$, $f(\gamma_r \cdot e) = -$ if $\Pi_{\{1,2\}}\gamma_r \cdot e$ is invalid, otherwise if $\Pi_{\{1,2\}}\gamma_r \cdot e \notin L(\mathbb{A})$, $f(\gamma_r \cdot e) = -$, and $f(\gamma_r \cdot e) = +$ if $\Pi_{\{1,2\}}\gamma_r \cdot e \in L(\mathbb{A})$;

Given a table \mathbf{T} , we define $row: S \cup R \mapsto (E \mapsto \{+, -\})$ as a function mapping each $\gamma_r \in S \cup R$ to a vector indexed by $e \in E$, each of whose components is defined as $f(\gamma_r \cdot e)$, denoting a potential location.

Before constructing a hypothesis \mathcal{H} based on the timed observation table \mathbf{T} , the learner has to ensure that \mathbf{T} satisfies the following conditions:

- *Reduced*: $\forall s, s' \in S: s \neq s' \text{ implies } row(s) \neq row(s')$;
- *Closed*: $\forall r \in R, \exists s \in S: row(s) = row(r)$;
- *Consistent*: $\forall \gamma_r, \gamma_r' \in S \cup R, row(\gamma_r) = row(\gamma_r') \text{ implies } row(\gamma_r \cdot \sigma_r) = row(\gamma_r' \cdot \sigma_r')$, for all $\sigma_r, \sigma_r' \in \Sigma_r$ satisfying $\gamma_r \cdot \sigma_r, \gamma_r' \cdot \sigma_r' \in S \cup R$ and $\Pi_{\{1,2\}}\sigma_r = \Pi_{\{1,2\}}\sigma_r'$;
- *Evidence-closed*: $\forall s \in S$ and $\forall e \in E$, the reset-logical-timed word $\pi(\Pi_{\{1,2\}}s \cdot e)$ belongs to $S \cup R$;
- *Prefix-closed*: $S \cup R$ is prefix-closed.

A timed observation table \mathbf{T} is *prepared* if it satisfies the above five conditions. To get the table prepared, the learner can perform the following operations:

Making \mathbf{T} closed. If \mathbf{T} is not closed, there exists $r \in R$ such that for all $s \in S$ $row(r) \neq row(s)$. The learner thus can move such r from R to S . Moreover, each reset-logical-timed word $\pi(\Pi_{\{1,2\}}r \cdot \sigma)$ needs to be added to R , where $\sigma = (\sigma, 0)$ for all $\sigma \in \Sigma$. Such an operation is important since it guarantees that at every location all actions in Σ are enabled, while specifying a clock valuation of these actions, despite that some invalid logical-timed words might be involved. Particularly, giving a bottom value 0 as the clock valuation satisfies the precondition of the partition functions that will be described in Sect. 3.2.

Making \mathbf{T} consistent. If \mathbf{T} is not consistent, one inconsistency is resolved by adding $\sigma \cdot e$ to \mathbf{E} , where σ and e can be determined as follows. \mathbf{T} being inconsistent implies that there exist two reset-logical-timed words $\gamma_r, \gamma_r' \in \mathbf{S} \cup \mathbf{R}$ at least, such that $\gamma_r \cdot \sigma_r, \gamma_r' \cdot \sigma_r' \in \mathbf{S} \cup \mathbf{R}$ and $\Pi_{\{1,2\}}\sigma_r = \Pi_{\{1,2\}}\sigma_r'$ for some $\sigma_r, \sigma_r' \in \Sigma_r$, with $\text{row}(\gamma_r) = \text{row}(\gamma_r')$ but $\text{row}(\gamma_r \cdot \sigma_r) \neq \text{row}(\gamma_r' \cdot \sigma_r')$. So, let $\sigma = \Pi_{\{1,2\}}\sigma_r = \Pi_{\{1,2\}}\sigma_r'$ and $e \in \mathbf{E}$ such that $f(\gamma_r \sigma_r \cdot e) \neq f(\gamma_r' \sigma_r' \cdot e)$. Thereafter, the learner fills the table by making membership queries. Note that this operation keeps the set \mathbf{E} of suffixes being a set of logical-timed words.

Making \mathbf{T} evidence-closed. If \mathbf{T} is not evidence-closed, then the learner needs to add all prefixes of $\pi(\Pi_{\{1,2\}}s \cdot e)$ to \mathbf{R} for every $s \in \mathbf{S}$ and $e \in \mathbf{E}$, except those already in $\mathbf{S} \cup \mathbf{R}$. Similarly, the learner needs to fill the table through membership queries.

The condition that a timed observation table \mathbf{T} is reduced and prefix-closed is inherently preserved by the aforementioned operations, together with the counterexample processing described later in Sect. 3.3. Furthermore, a table may need several rounds of these operations before being prepared (cf. Algorithm 1), since certain conditions may be violated by different, interleaved operations.

3.2 Hypothesis construction

As soon as the timed observation table \mathbf{T} is prepared, a hypothesis can be constructed in two steps, i.e., the learner first builds a DFA \mathbf{M} based on the information in \mathbf{T} , and then transforms \mathbf{M} to a hypothesis \mathcal{H} , which will later be shown as a COTA.

Given a prepared timed observation table $\mathbf{T} = (\Sigma, \Sigma, \Sigma_r, \mathbf{S}, \mathbf{R}, \mathbf{E}, f)$, a DFA $\mathbf{M} = (Q_M, \Sigma_M, \Delta_M, q_M^0, F_M)$ can be built as follows:

- the finite set of locations $Q_M = \{q_{\text{row}(s)} \mid s \in \mathbf{S}\}$;
- the initial location $q_M^0 = q_{\text{row}(e)}$ for $e \in \mathbf{S}$;
- the set of accepting locations $F_M = \{q_{\text{row}(s)} \mid f(s \cdot e) = + \text{ for } s \in \mathbf{S} \text{ and } e \in \mathbf{E}\}$;
- the finite alphabet $\Sigma_M = \{\sigma_r \in \Sigma_r \mid \gamma_r \cdot \sigma_r \in \mathbf{S} \cup \mathbf{R} \text{ for } \gamma_r \in \Sigma_r^*\}$;
- the finite set of transitions $\Delta_M = \{(q_{\text{row}(\gamma_r)}, \sigma_r, q_{\text{row}(\gamma_r \cdot \sigma_r)}) \mid \gamma_r \cdot \sigma_r \in \mathbf{S} \cup \mathbf{R} \text{ for } \gamma_r \in \Sigma_r^* \text{ and } \sigma_r \in \Sigma_r\}$.

The constructed DFA \mathbf{M} is compatible with the timed observation table \mathbf{T} in the sense captured by the following lemma.

Lemma 1. *For a prepared timed observation table $\mathbf{T} = (\Sigma, \Sigma, \Sigma_r, \mathbf{S}, \mathbf{R}, \mathbf{E}, f)$, for every $\gamma_r \cdot e \in (\mathbf{S} \cup \mathbf{R}) \cdot \mathbf{E}$, the constructed DFA $\mathbf{M} = (Q_M, \Sigma_M, \Delta_M, q_M^0, F_M)$ accepts $\pi(\Pi_{\{1,2\}}\gamma_r \cdot e)$ if and only if $f(\gamma_r \cdot e) = +$.*

The learner then transforms the DFA \mathbf{M} to a hypothesis $\mathcal{H} = (\Sigma, Q, q_0, F, c, \Delta)$, with $Q = Q_M$, $q_0 = q_M^0$, $F = F_M$, c being the clock and Σ the given alphabet as in \mathbf{T} . The set of transitions Δ in \mathcal{H} can be constructed as follows: For any $q \in Q_M$ and $\sigma \in \Sigma$, let $\Psi_{q,\sigma} = \{\mu \mid (q, (\sigma, \mu, b), q') \in \Delta_M\}$, then the partition function $P^c(\cdot)$ (defined below) applying to $\Psi_{q,\sigma}$ returns k intervals, written as I_1, \dots, I_k , satisfying $\mu_i \in I_i$ for any $1 \leq i \leq k$, where $k = |\Psi_{q,\sigma}|$; consequently, for every $(q, (\sigma, \mu_i, b_i), q') \in \Delta_M$, a fresh transition $\delta_i = (q, \sigma, I_i, b_i, q')$ is added to Δ .

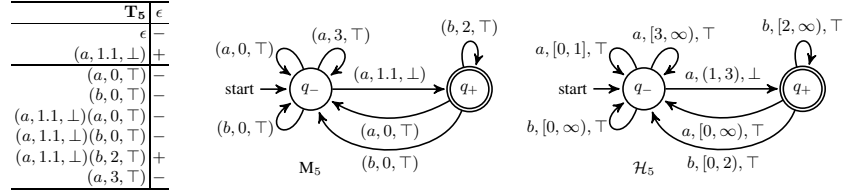


Fig. 2: The prepared timed observation table \mathbf{T}_5 , the corresponding DFA M_5 and hypothesis \mathcal{H}_5 .

Definition 3 (Partition function). Given a list of clock valuations $\ell = \mu_0, \mu_1, \dots, \mu_n$ with $0 = \mu_0 < \mu_1 < \dots < \mu_n$, and $\lfloor \mu_i \rfloor \neq \lfloor \mu_j \rfloor$ if $\mu_i, \mu_j \in \mathbb{R}_{\geq 0} \setminus \mathbb{N}$ and $i \neq j$ for all $1 \leq i, j \leq n$, let $\mu_{n+1} = \infty$, then a partition function $P^c(\cdot)$ mapping ℓ to a set of intervals $\{I_0, I_1, \dots, I_n\}$, which is a partition of $\mathbb{R}_{\geq 0}$, is defined as

$$I_i = \begin{cases} [\mu_i, \mu_{i+1}), & \text{if } \mu_i \in \mathbb{N} \wedge \mu_{i+1} \in \mathbb{N}; \\ (\lfloor \mu_i \rfloor, \mu_{i+1}), & \text{if } \mu_i \in \mathbb{R}_{\geq 0} \setminus \mathbb{N} \wedge \mu_{i+1} \in \mathbb{N}; \\ [\mu_i, \lfloor \mu_{i+1} \rfloor], & \text{if } \mu_i \in \mathbb{N} \wedge \mu_{i+1} \in \mathbb{R}_{\geq 0} \setminus \mathbb{N}; \\ (\lfloor \mu_i \rfloor, \lfloor \mu_{i+1} \rfloor], & \text{if } \mu_i \in \mathbb{R}_{\geq 0} \setminus \mathbb{N} \wedge \mu_{i+1} \in \mathbb{R}_{\geq 0} \setminus \mathbb{N}. \end{cases}$$

Remark 2. Definition 3 is adapted from that in [15] by imposing additional assumptions of the list of clock valuations in order to guarantee $\mu_i \in I_i$, for any $0 \leq i \leq n$, due to the underlying continuous-time semantics. Whereas, by \mathbf{T} being prepared and the normalization function described in Sect. 3.3, the set of clock valuations $\Psi_{q,\sigma}$ can be arranged into a list $\ell_{q,\sigma} = \mu_0, \mu_1, \dots, \mu_n$ satisfying such assumptions given in Definition 3 for any $q \in Q_M$ and $\sigma \in \Sigma$.

Example 2. Suppose \mathbb{A} in Fig. 1 recognizes the target timed language. Then the prepared table \mathbf{T}_5 , the corresponding DFA M_5 and hypothesis \mathcal{H}_5 are depicted in Fig. 2. Here, the subscript 5 indicates the fifth iteration of \mathbf{T} (Details concerning the constructions and the entire learning process are enclosed in Appendix B.).

Lemma 2. Given a DFA $M = (Q_M, \Sigma_M, \delta_M, q_M^0, F_M)$, which is generated from a prepared timed observation table \mathbf{T} , the hypothesis $\mathcal{H} = (\Sigma, Q, q_0, F, c, \Delta)$ is transformed from M . For all $\gamma_r \cdot e \in (S \cup R) \cdot E$, \mathcal{H} accepts the reset-logical-timed word $\pi(\Pi_{\{1,2\}} \gamma_r \cdot e)$ iff $f(\gamma_r \cdot e) = +$.

Theorem 2. The hypothesis \mathcal{H} is a COTA.

Given a clock valuation μ , we denote the region containing μ as $\llbracket \mu \rrbracket$, defined as $\llbracket \mu \rrbracket = [\mu, \mu]$ if $\mu \in \mathbb{N}$, and $\llbracket \mu \rrbracket = (\lfloor \mu \rfloor, \lfloor \mu \rfloor + 1)$ otherwise. The following theorem establishes the compatibility of the constructed hypothesis \mathcal{H} with the timed observation table \mathbf{T} .

Theorem 3. For $\gamma_r \cdot e \in (S \cup R) \cdot E$, let $\pi(\Pi_{\{1,2\}} \gamma_r \cdot e) = (\sigma_1, \mu_1, b_1) \cdots (\sigma_n, \mu_n, b_n)$. Then for every $\mu'_i \in \llbracket \mu_i \rrbracket$, the hypothesis \mathcal{H} accepts the reset-logical-timed word $\gamma'_r = (\sigma_1, \mu'_1, b_1) \cdots (\sigma_n, \mu'_n, b_n)$ if $f(\gamma_r \cdot e) = +$, and cannot accept it if $f(\gamma_r \cdot e) = -$.

3.3 Equivalence query and counterexample processing

Suppose that the teacher knows a COTA \mathbb{A} which recognizes the target timed language \mathcal{L} . Then to answer an equivalence query is to determine whether $\mathcal{L}(\mathcal{H}) = \mathcal{L}(\mathbb{A})$, which can be divided into two timed language inclusion problems, i.e., whether $\mathcal{L}(\mathcal{H}) \subseteq \mathcal{L}(\mathbb{A})$ and $\mathcal{L}(\mathbb{A}) \subseteq \mathcal{L}(\mathcal{H})$. Most decision procedures for language inclusion proceed by complementation and emptiness checking of the intersection [20]: $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ iff $\mathcal{L}(A) \cap \overline{\mathcal{L}(B)} = \emptyset$. The fact that deterministic timed automata can be complemented [6] enables solving the inclusion problem by checking the emptiness of the resultant product automata $\mathcal{H} \times \overline{\mathbb{A}}$ and $\overline{\mathcal{H}} \times \mathbb{A}$. The complementation technique, however, does not apply to nondeterministic timed automata even if with only one single clock [4], which we plan to incorporate in our learning framework in future work. We therefore opt for² the alternative method presented by Ouaknine and Worrell in [28] showing that the language inclusion problem of timed automata with one clock (regardless of their determinacy) is decidable by reduction to a reachability problem on an infinite graph. That is, there exists a delay-timed word ω that leads to a *bad configuration* if $\mathcal{L}(\mathcal{H}) \not\subseteq \mathcal{L}(\mathbb{A})$. In detail, the corresponding run ρ of ω ends in an accepting location in \mathcal{H} but the counterpart ρ' of ω in \mathbb{A} is not accepting. Consequently, the teacher can provide the reset-delay-timed word ω_r resulting from ω by running \mathbb{A} as a negative counterexample ctx_- . Similarly, a positive counterexample $ctx_+ = (\omega_r, +)$ can be generated if $\mathcal{L}(\mathbb{A}) \not\subseteq \mathcal{L}(\mathcal{H})$. An algorithm elaborating the equivalence query is provided in Appendix C.

When receiving a counterexample $ctx = (\omega_r, +/ -)$, the learner first converts it to a reset-logical-timed word $\gamma_r = I(\omega_r) = (\sigma_1, \mu_1, b_1)(\sigma_2, \mu_2, b_2) \cdots (\sigma_n, \mu_n, b_n)$. By definition, γ_r and ω_r share the same sequence of transitions in \mathbb{A} . Furthermore, by the contraposition of Theorem 1, γ_r is an evidence for $L_r(\mathcal{H}) \neq L_r(\mathbb{A})$ if ω_r is an evidence for $\mathcal{L}(\mathcal{H}) \neq \mathcal{L}(\mathbb{A})$.

Additionally, by the definition of clock constraints Φ_c , at any location, if an action σ is enabled, i.e., its guard is satisfied, w.r.t. the clock value $\mu \in \mathbb{R}_{\geq 0} \setminus \mathbb{N}$, then σ should be enabled w.r.t. any clock value $\lfloor \mu \rfloor + \theta$ at the location, where $\theta \in (0, 1)$. Specifically, only one transition is available for σ at the location on the interval $\llbracket \mu \rrbracket$, because the target automaton is deterministic. Therefore, in order to avoid unnecessarily distinguishing timed words and violating the assumptions of the list ℓ for the partition function, the learner needs to apply a *normalization function* g to normalize reset-logical-timed words.

Definition 4 (Normalization). A normalization function g maps a reset-logical-timed word $\gamma_r = (\sigma_1, \mu_1, b_1)(\sigma_2, \mu_2, b_2) \cdots (\sigma_n, \mu_n, b_n)$ to another reset-logical-timed word by resetting any logical clock to its integer part plus a constant fractional part, i.e., $g(\gamma_r) = (\sigma_1, \mu'_1, b_1)(\sigma_2, \mu'_2, b_2) \cdots (\sigma_n, \mu'_n, b_n)$, where $\mu'_i = \mu_i$ if $\mu_i \in \mathbb{N}$, $\mu'_i = \lfloor \mu_i \rfloor + \theta$ for some fixed constant $\theta \in (0, 1)$ otherwise.

² Remark that the learning complexity (Sect. 3.5) is measured in terms of the number of queries rather than the time complexity of the specific method for checking the equivalence (nor membership). The latter hence brings no significant impacts over the learning performance. Additionally, the specific method of equivalence checking is not the main concern.

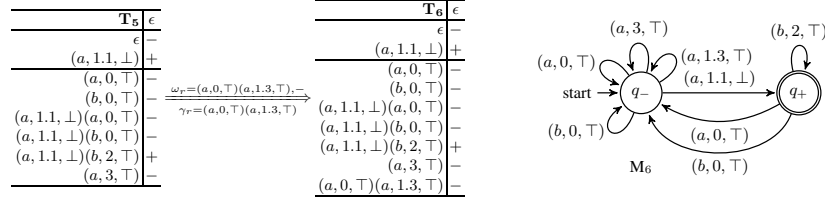


Fig. 3: An illustration of the necessity of normalization by the normalization function.

We will instantiate $\theta = 0.1$ in what follows. Clearly our approach works for any other θ valued in $(0, 1)$. This *normalization* process guarantees the assumptions needed for Definition 3.

Example 3. Consider the prepared table T_5 in Fig. 3 (as in Fig. 2). When the learner asks an equivalence query with hypothesis \mathcal{H}_5 , the teacher answers that $\mathcal{L}(\mathcal{H}_5) \neq \mathcal{L}(\mathbb{A})$, where \mathbb{A} in Fig. 1 is the target automaton, and provides a counterexample $(\omega_r, -)$ with $\omega_r = (a, 0, \top)(a, 1.3, \top)$, which can be transformed to a reset-logical-timed word $\gamma_r = (a, 0, \top)(a, 1.3, \top)$. If he adds prefixes of γ_r to the table directly, the learner will get a prepared table T_6 and thus construct a DFA M_6 . Unfortunately, the partition function defined in Definition 3 is not applicable to $(a, 1.3, \top)$ and $(a, 1.1, \perp)$ any more. On the other hand, if he adds the prefixes of the normalized reset-logical-timed word, i.e., $\gamma'_r = (a, 0, \top)(a, 1.1, \top)$, to T_5 , the learner will then get an inconsistent table whose consistency can be retrieved by the operation of “making T consistent” as expected.

The following theorem guarantees that the normalized reset-logical-timed word γ'_r is also an evidence for $L_r(\mathcal{H}) \neq L_r(\mathbb{A})$. Therefore, the learner can use it as a counterexample and thus adds all the prefixes of γ'_r to \mathbf{R} except those already in $\mathbf{S} \cup \mathbf{R}$.

Theorem 4. *Given a valid reset-logical-timed word γ_r of \mathbb{A} , its normalization $\gamma'_r = g(\gamma_r)$ shares the same sequence of transitions in \mathbb{A} .*

3.4 Learning algorithm

We present in Algorithm 1 the learning procedure integrating all the previously stated ingredients, including preparing the table, membership and equivalence queries, hypothesis construction and counterexample processing. The learner first initializes the timed observation table $\mathbf{T} = (\Sigma, \Sigma, \Sigma_r, \mathbf{S}, \mathbf{R}, \mathbf{E}, f)$, where $\mathbf{S} = \{\epsilon\}$, $\mathbf{E} = \{\epsilon\}$, while for every $\sigma \in \Sigma$, he builds a logical-timed word $\gamma = (\sigma, 0)$ and then obtains its reset counterpart $\pi(\gamma) = (\sigma, 0, b)$ by triggering a membership query to the teacher, which is then added to \mathbf{R} . Thereafter, the learner can fill the table by additional membership queries. Before constructing a hypothesis, the learner performs several rounds of operations described in Sect. 3.1 until \mathbf{T} is prepared. Then, a hypothesis \mathcal{H} is constructed leveraging an intermediate DFA M and submitted to the teacher for an equivalence query. If the answer is positive, \mathcal{H} recognizes the target language. Otherwise, the learner receives a counterexample ctx and then conducts the counterexample processing to update \mathbf{T} as described in Sect. 3.3. The whole procedure repeats until the teacher gives a positive answer to an equivalence query.

Algorithm 1: Learning one-clock timed automaton with a smart teacher

```

input : the timed observation table  $\mathbf{T} = (\Sigma, \Sigma_r, S, R, E, f)$ .
output: the hypothesis  $\mathcal{H}$  recognizing the target language  $\mathcal{L}$ .
1  $S \leftarrow \{\epsilon\}; R \leftarrow \{\pi(\gamma) \mid \gamma = (\sigma, 0), \forall \sigma \in \Sigma\}; E \leftarrow \{\epsilon\};$  // initialization
2 fill  $\mathbf{T}$  by membership queries;
3  $equivalent \leftarrow \perp$ ;
4 while  $equivalent = \perp$  do
5    $prepared \leftarrow is\_prepared(\mathbf{T});$  // whether the table is prepared
6   while  $prepared = \perp$  do
7     if  $\mathbf{T}$  is not closed then  $make\_closed(\mathbf{T});$ 
8     if  $\mathbf{T}$  is not consistent then  $make\_consistent(\mathbf{T});$ 
9     if  $\mathbf{T}$  is not evidence-closed then  $make\_evidence\_closed(\mathbf{T});$ 
10     $prepared \leftarrow is\_prepared(\mathbf{T});$ 
11   $M \leftarrow build\_DFA(\mathbf{T});$  // transforming  $\mathbf{T}$  to a DFA  $M$ 
12   $\mathcal{H} \leftarrow build\_hypothesis(M);$  // constructing a hypothesis  $\mathcal{H}$  from  $M$ 
13   $equivalent, ctx \leftarrow equivalence\_query(\mathcal{H});$ 
14  if  $equivalent = \perp$  then
15     $ctx\_processing(\mathbf{T}, ctx);$  // counterexample processing
16 return  $\mathcal{H};$ 

```

To facilitate the analysis of correctness, termination and complexity of Algorithm 1, we introduce the notion of *symbolic state* that combines each location with its clock regions: a symbolic state of a COTA $\mathbb{A} = (\Sigma, Q, q_0, F, c, \Delta)$ is a pair $(q, \llbracket \mu \rrbracket)$, where $q \in Q$ and $\llbracket \mu \rrbracket$ is a region containing μ . If κ is the maximal constant appearing in the clock constraints of \mathbb{A} , then there exist $2\kappa + 2$ such regions, including $[n, n]$ with $0 \leq n \leq \kappa$, $(n, n + 1)$ with $0 \leq n < \kappa$, and (κ, ∞) for each location, so there are a total of $|Q| \times (2\kappa + 2)$ symbolic states. Then the correctness and termination of Algorithm 1 is stated in the following theorem, based on the fact that there is an injection from S (or equivalently, the locations of \mathcal{H}) to symbolic states of \mathbb{A} .

Theorem 5. *Algorithm 1 terminates and returns a COTA \mathcal{H} which recognizes the target timed language \mathcal{L} .*

3.5 Complexity

Given a target timed language \mathcal{L} which is recognized by a COTA \mathbb{A} , let $n = |Q|$ be the number of locations of \mathbb{A} , $m = |\Sigma|$ the size of the alphabet, and κ the maximal constant appearing in the clock constraints of \mathbb{A} . In what follows, we derive the complexity of Algorithm 1 in terms of the number of queries.

By the proof of Theorem 5, \mathcal{H} has at most $n(2\kappa + 2)$ locations (the size of S) distinguished by E . Thus, $|E|$ is at most $n(2\kappa + 2)$ in order to distinguish these locations. Therefore, the number of transitions of \mathcal{H} is bounded by $mn^2(2\kappa + 2)^3$. Furthermore, as every counterexample adds at least one fresh transition to the hypothesis \mathcal{H} , where we consider each interval of the partition corresponds to a transition, this means that the number of counterexamples and equivalence queries is at most $mn^2(2\kappa + 2)^3$.

Now, we consider the number of membership queries, that is, to compute $(|S| + |R|) \times |E|$. Let h be the maximal length of counterexamples returned by the teacher, which is polynomial in the size of \mathbb{A} according to Theorem 5 in [37], bounded by n^2 . There are three cases of extending R by adding fresh rows, namely during the processing of counterexamples, making \mathbf{T} closed, and making \mathbf{T} evidence-closed. The

first case adds at most $hmn^2(2\kappa + 2)^3$ rows to \mathbf{R} , while the latter two add at most $n(2\kappa + 2) \times m$ and $n^2(2\kappa + 2)^2$, respectively, yielding that the size of \mathbf{R} is bounded by $\mathcal{O}(hmn^2\kappa^3)$, where $\mathcal{O}(\cdot)$ is the big Omicron notation. As a consequence, the number of membership queries is bounded by $\mathcal{O}(mn^5\kappa^4)$. So, the total complexity is $\mathcal{O}(mn^5\kappa^4)$.

It is worth noting the above analysis is given in the worst case, where all partitions need to be fully refined. But, in practice we can learn the automaton without refining most partitions, and therefore the number of equivalence and membership queries, as well as the number of locations in the learned automaton are much fewer than the corresponding worst-case bounds. This will be demonstrated by examples in Sect. 5.

3.6 Accelerating Trick

In the timed observation table, the function f maps invalid reset-logical-timed words as well as certain valid ones to “—” when the teacher maintains a COTA \mathbb{A} as the oracle. The learner thus needs multiple rounds of queries to distinguish the “sink” location from other unaccepting locations. If the function f is extended to map invalid reset-logical-timed words to a distinct symbol, say “ \times ”, when we let a DOTA \mathcal{A} be the oracle, then the learner will take much fewer queries. We will later show in the experiments that such a trick significantly accelerates the learning process.

4 Learning from a Normal Teacher

In this section, we consider the problem of learning timed automata with a normal teacher. As before, we assume the timed language to be learned comes from a complete DOTA. For the normal teacher, inputs to membership queries are delay-timed words, and the teacher returns whether the word is in the language (without giving any additional information). Inputs to equivalence queries are candidate DOTAs, and the teacher either answers they are equivalent or provides a delay-timed word as a counterexample.

The algorithm here is based on the procedure in the previous section. We still maintain observation tables where the elements in $\mathbf{S} \cup \mathbf{R}$ are reset-logical-timed words and the elements in \mathbf{E} are logical-timed words. In order to obtain delay-timed words for the membership queries, we need to *guess* clock reset information for transitions in the table. More precisely, in order to convert a logical-timed word to a delay-timed word, it is necessary to know clock reset information for all but the last transition. Hence, it is necessary to guess reset information for each word in $\mathbf{S} \cup \mathbf{R}$ (since $\mathbf{S} \cup \mathbf{R}$ is prefix-closed, this is equivalent to guessing reset information for the last transition of each word). Also, for each entry in $(\mathbf{S} \cup \mathbf{R}) \times \mathbf{E}$, it is necessary to guess all but the last transition in \mathbf{E} . The algorithm can be thought of as exploring a search tree, where branching is caused by guesses, and successor nodes are constructed by the usual operations of preparing a table and dealing with a counterexample.

The detailed process is given in Algorithm 2. The learner maintains a set of table instances, named *ToExplore*, which contains all table instances that still need to be explored.

The initial tables in *ToExplore* are as follows. Each table has $\mathbf{S} = \mathbf{E} = \{\epsilon\}$. For each $\sigma \in \Sigma$, there is one row in \mathbf{R} corresponding to the logical-timed word $\omega = (\sigma, 0)$.

Algorithm 2: Learning one-clock timed automaton with a normal teacher

input : the timed observation table $\mathbf{T} = (\Sigma, \Sigma, \Sigma_r, S, R, E, f)$.
output: the hypothesis \mathcal{H} recognizing the target language \mathcal{L} .

```

1  $ToExplore \leftarrow \emptyset; S \leftarrow \{\epsilon\}; R \leftarrow \{\pi(\gamma) \mid \gamma = (\sigma, 0), \forall \sigma \in \Sigma\}; E \leftarrow \{\epsilon\};$  // initialization
2  $currentTable \leftarrow (\Sigma, \Sigma, \Sigma_r, S, R, E, f);$ 
3  $tables \leftarrow guess\_and\_fill(currentTable);$  // guess resets and fill all table instances
4  $ToExplore.insert(tables);$  // insert table instances  $tables$  into  $ToExplore$ 
5  $currentTable \leftarrow ToExplore.pop();$  // pop out head instance as the current table
6  $equivalent \leftarrow \perp;$ 
7 while  $equivalent = \perp$  do
8    $prepared \leftarrow is\_prepared(currentTable);$  // whether the current table is prepared
9   while  $prepared = \perp$  do
10     if  $currentTable$  is not closed then
11        $tables \leftarrow guess\_and\_make\_closed(currentTable); ToExplore.insert(tables);$ 
12        $currentTable \leftarrow ToExplore.pop();$ 
13     if  $currentTable$  is not consistent then
14        $tables \leftarrow guess\_and\_make\_consistent(currentTable); ToExplore.insert(tables);$ 
15        $currentTable \leftarrow ToExplore.pop();$ 
16     if  $currentTable$  is not evidence-closed then
17        $tables \leftarrow guess\_and\_make\_evidence\_closed(currentTable); ToExplore.insert(tables);$ 
18        $currentTable \leftarrow ToExplore.pop();$ 
19      $prepared \leftarrow is\_prepared(currentTable);$ 
20    $M \leftarrow build\_DFA(currentTable);$  // transforming  $currentTable$  to a DFA  $M$ 
21    $\mathcal{H} \leftarrow build\_hypothesis(M);$  // constructing a hypothesis  $\mathcal{H}$  from  $M$ 
22    $equivalent, ctx \leftarrow equivalence\_query(\mathcal{H});$  //  $ctx$  is a delay-timed word
23   if  $equivalent = \perp$  then
24      $tables \leftarrow guess\_and\_ctx\_processing(currentTable, ctx);$  // counterexample processing
25      $ToExplore.insert(tables);$ 
26      $currentTable \leftarrow ToExplore.pop();$ 
27 return  $\mathcal{H};$ 

```

It is necessary to guess a reset b for each ω thereby transforming it to a reset-logical-timed word $\omega_r = (\sigma, 0, b)$. There are $2^{|\Sigma|}$ possible combinations of guesses. These tables are filled by making membership queries (in this case, the membership queries for each table are the same). The resulting $2^{|\Sigma|}$ tables form the initial tables in $ToExplore$.

In each iteration of the algorithm, one table instance is taken out of $ToExplore$. The learner checks whether the table is closed, consistent, and evidence closed. If the table is not closed, i.e. there exists $r \in R$ such that $row(r) \neq row(s)$ for all $s \in S$, the learner moves r from R to S . Then for each $\sigma \in \Sigma$, the element $r \cdot (\sigma, 0)$ is added to R , and a guess has to be made for its reset information. Hence, $2^{|\Sigma|}$ unfilled table instances will be generated. Next, for each entry in the $|\Sigma|$ new rows of R , it is necessary to guess reset information for all but the last transition in $e \in E$. After this guess, it is now possible to fill the table instances by making membership queries with transformed delay-timed words. Hence, there are at most $2^{(\sum_{e_i \in E \setminus \{\epsilon\}} (|e_i| - 1)) \times |\Sigma|}$ filled table instances for one unfilled table instance. All filled table instances are inserted into $ToExplore$.

If the table is not consistent, i.e. there exist some $\gamma_r, \gamma'_r \in S \cup R$ and $\sigma_r \in \Sigma_r$ such that $\gamma_r \cdot \sigma_r, \gamma'_r \cdot \sigma_r \in S \cup R$ and $row(\gamma_r) = row(\gamma'_r)$, but $row(\gamma_r \cdot \sigma_r) \neq row(\gamma'_r \cdot \sigma_r)$. Let $e \in E$ be one place where they are different. Then $\sigma_r \cdot e$ needs to be added to E . For each entry in $S \cup R$, all but the last transition in $\sigma_r \cdot e$ need to be guessed, then the table can be filled. $2^{(|\sigma_r \cdot e| - 1) \times (|S| + |R|)}$ filled table instances will be generated and inserted into $ToExplore$. The operation for making tables evidence-closed is analogous.

Once the current table is prepared, the learner builds a hypothesis \mathcal{H} and makes an equivalence query to the teacher. If the answer is positive, then \mathcal{H} is a COTA which recognizes the target timed language \mathcal{L} ; otherwise, the teacher gives a delay-timed word ω as a counterexample. The learner first finds the longest reset-logical-timed word in \mathbf{R} which, when converted to a delay-timed word, agrees with a prefix of ω . The remainder of ω , however, needs to be converted to a reset-logical-timed word by guessing reset information. The corresponding prefixes are then added to \mathbf{R} . Hence, at most $2^{|\omega|}$ unfilled table instances are generated. For each unfilled table instance, at most $2^{(\sum_{e_i \in E \setminus \{\epsilon\}} (|e_i| - 1)) \times |\omega|}$ filled tables are produced and inserted into *ToExplore*.

Throughout the learning process, the learner adds a finite number of table instances to *ToExplore* at every iteration. Hence, the search tree is finite-branching. Moreover, if all guesses are correct, the resulting table instance will be identical to the observation table in the learning process with a smart teacher (apart from the guessing processes, the basic table operations are the same as those in Section 3.1). This means, with an appropriate search order, for example, taking the table instance that requires the least number of guesses in *ToExplore* at every iteration, the algorithm terminates and returns the same table as in the learning process with a smart teacher, which is a COTA that recognizes the target language \mathcal{L} . In conformity to Theorem 1, the algorithm may terminate even if the corresponding reset-logical-timed languages are not equivalent, while yielding correct COTAs recognizing the same delay-timed language.

Theorem 6. *Algorithm 2 terminates and returns a COTA \mathcal{H} which recognizes the target timed language \mathcal{L} .*

Complexity analysis. If $\mathbf{T} = (\Sigma, \Sigma, \Sigma_r, S, \mathbf{R}, E, f)$ is the final observation table for the correct candidate COTA, the number of guessed resets in $S \cup \mathbf{R}$ is $|S| + |\mathbf{R}|$, and the number of guessed resets for entries in each row of the table is $\sum_{e_i \in E \setminus \{\epsilon\}} (|e_i| - 1)$. Hence, the total number of guessed resets is $(|S| + |\mathbf{R}|) \times (1 + \sum_{e_i \in E \setminus \{\epsilon\}} (|e_i| - 1))$. Assuming an appropriate search order (for example according to the number of guesses in each table), this yields the number of table instances considered before termination as $\mathcal{O}(2^{(|S| + |\mathbf{R}|) \times (1 + \sum_{e_i \in E \setminus \{\epsilon\}} (|e_i| - 1))})$.

5 Implementation and Experimental Results

To investigate the efficiency and scalability of the proposed methods, we implemented a prototype³ in PYTHON for learning deterministic one-clock timed automata. The examples include a practical case concerning the functional specification of the TCP protocol [23] and a set of randomly generated DOTAs to be learnt. All of the evaluations have been carried out on a 3.6GHz Intel Core-i7 processor with 8GB RAM running 64-bit Ubuntu 16.04.

Functional specification of the TCP protocol. In [23], a state diagram on page 23 specifies state changes during a TCP connection triggered by causing events while leading to resulting actions. As observed by Ouaknine and Worrell in [28], such a functional specification of the protocol can be represented as a one-clock timed automaton. In our

³ Available at <https://github.com/Leslieaj/OTALearning>.

Table 1: Experimental results on random examples for the smart teacher situation.

| Case ID | $ \Delta _{\text{mean}}$ | #Membership | | | #Equivalence | | | n_{mean} | t_{mean} |
|---------|--------------------------|-------------|-------------------|------------|--------------|-------------------|------------|-------------------|-------------------|
| | | N_{\min} | N_{mean} | N_{\max} | N_{\min} | N_{mean} | N_{\max} | | |
| 4_4_20 | 16.3 | 118 | 245.0 | 650 | 20 | 30.1 | 42 | 4.5 | 24.7 |
| 7_2_10 | 16.9 | 568 | 920.8 | 1393 | 23 | 31.3 | 37 | 9.1 | 14.6 |
| 7_4_10 | 25.7 | 348 | 921.7 | 1296 | 34 | 50.9 | 64 | 9.3 | 38.0 |
| 7_6_10 | 26.0 | 351 | 634.5 | 1050 | 35 | 44.7 | 70 | 7.8 | 49.6 |
| 7_4_20 | 34.3 | 411 | 1183.4 | 1890 | 52 | 70.5 | 93 | 9.5 | 101.7 |
| 10_4_20 | 39.1 | 920 | 1580.9 | 2160 | 61 | 73.1 | 88 | 11.7 | 186.7 |
| 12_4_20 | 47.6 | 1090 | 2731.6 | 5733 | 66 | 97.4 | 125 | 16.0 | 521.8 |
| 14_4_20 | 58.4 | 1390 | 2238.6 | 4430 | 79 | 107.7 | 135 | 16.0 | 515.5 |

Case ID: $n_m\kappa$, consisting of the number of locations, the size of the alphabet and the maximum constant appearing in the clock constraints, respectively, of the corresponding group of \mathcal{A} 's.

$|\Delta|_{\text{mean}}$: the average number of transitions in the corresponding group.

#Membership & #Equivalence: the number of conducted membership and equivalence queries, respectively. N_{\min} : the minimal, N_{mean} : the mean, N_{\max} : the maximum.

n_{mean} : the average number of locations of the learned automata in the corresponding group.

t_{mean} : the average wall-clock time in seconds, including that taken by the learner and by the teacher.

setting, the corresponding DOTA \mathcal{A} to be learnt is configured to have $|Q| = 11$ states with the two CLOSED states collapsed, $|\Sigma| = 10$ after abstracting the causing events and the resulting actions, $|F| = 2$, and $|\Delta| = 19$ with appropriately specified timing constraints including guards and resets. Using the algorithm with the smart teacher, a correct DOTA \mathcal{H} is learned in 155 seconds after 2600 membership queries and 28 equivalence queries. Specifically, \mathcal{H} has 15 locations excluding a sink location connected by 28 transitions. The introduction of 4 new locations comes from splitting of guards along transitions, which however can be trivially merged back with other locations. The figures depicting \mathcal{A} and \mathcal{H} can be found in Appendix D.

Random examples for a smart teacher. We randomly generated 80 DOTAs in eight groups, with each group having different numbers of locations, size of alphabet, and maximum constant appearing in clock constraints. As shown in Table 1, the proposed learning method succeeds in all cases in identifying a DOTA that recognizes the same timed language. In particular, the number of membership queries and that of equivalence queries appear to grow polynomially with the size of the problem⁴, and are much smaller than the worst-case bounds estimated in Sect. 3.5. Moreover, the learned DOTAs do not have prominent increases in the number of locations (by comparing n_{mean} with the first component of Case IDs). The average wall-clock time including both time taken by the learner and by the teacher is recorded in the last column t_{mean} , of which, however, often over 90% is spent by the teacher for checking equivalences w.r.t. small \mathbf{T} 's while around 50% by the learner for checking the preparedness condition w.r.t. large \mathbf{T} 's.

Without the accelerating trick. It is worth noting that all of the results reported above are carried out on an implementation equipped with the accelerating trick discussed in

⁴ An exception w.r.t. the group 7_6_10 is due to relatively simple DOTAs generated occasionally.

Table 2: Experimental results on random examples for the normal teacher situation.

| Case ID | $ \Delta _{\text{mean}}$ | #Membership | | | #Equivalence | | | n_{mean} | t_{mean} | # $\mathbf{T}_{\text{explored}}$ | #Learnt |
|---------|--------------------------|-------------|-------------------|------------|--------------|-------------------|------------|-------------------|-------------------|----------------------------------|---------|
| | | N_{\min} | N_{mean} | N_{\max} | N_{\min} | N_{mean} | N_{\max} | | | | |
| 3_2_10 | 4.8 | 43 | 83.7 | 167 | 5 | 8.8 | 14 | 3.0 | 0.9 | 149.1 | 10/10 |
| 4_2_10 | 6.8 | 67 | 134.0 | 345 | 6 | 13.3 | 24 | 4.0 | 7.4 | 563.0 | 10/10 |
| 5_2_10 | 8.8 | 75 | 223.9 | 375 | 9 | 15.2 | 24 | 5.0 | 35.5 | 2811.6 | 10/10 |
| 6_2_10 | 11.9 | 73 | 348.3 | 708 | 10 | 16.7 | 30 | 5.6 | 59.8 | 5077.6 | 7/10 |
| 4_4_20 | 16.3 | 231 | 371.0 | 564 | 27 | 30.9 | 40 | 4.0 | 137.5 | 8590.0 | 6/10 |

#Membership & #Equivalence: the number of conducted membership and equivalence queries with the cached methods, respectively. N_{\min} : the minimal, N_{mean} : the mean, N_{\max} : the maximum.

$\mathbf{T}_{\text{explored}}$: the average number of the explored table instances.

#Learnt: the number of the learnt DOTAs in the case (learnt/total).

Sect. 3.6. We remark that when dropping this trick, the average number of membership queries blow up with a factor of 2.16 in average for all the 8 groups, and 1.04 for the average number of equivalence queries, leading to dramatic increases also in the computation time (including that in operating tables). The alternative implementation and experimental results without the accelerating trick can also be found in the tool page (under the `dev` branch).

Random examples for a normal teacher. Due to its prohibitively high, exponential complexity, the algorithm with a normal teacher failed (memory out) in identifying DOTAs for almost all the above examples, except 6 cases out of the 10 in group 4_4_20. We therefore randomly generated 40 extra DOTAs classified into 4 groups. With the accelerating trick, the learner need not guess the resets in elements of \mathbf{E} for an entry in $\mathbf{S} \cup \mathbf{R}$ if the querying result of the entry is the sink location. We also omitted the checking of the evidence-closed condition, since it may add redundant rows in \mathbf{R} , leading to more guesses and thereby a larger search space. This omission does not affect the correctness of the algorithm. Moreover, as different table instances may generate repeated queries, we cached the results of membership queries and counterexamples, such that the numbers of membership and equivalence queries to the teacher can be significantly reduced. Table 2 shows the performance of the algorithm in this setting with a normal teacher. Results without caching are available in the tool page (under the `normal` branch).

6 Conclusion

We have presented a polynomial active learning method for deterministic one-clock timed automata from a smart teacher who can tell information about clock resets in membership and equivalence queries. Our technique is based on converting the problem to that of learning reset-logical-timed languages. We then extend the method to learning DOTAs from a normal teacher who receives delay-timed words for membership queries, by guessing reset information in the observation table. We evaluate both methods on randomly generated examples and (for the case with smart teacher) the functional specification of the TCP protocol.

Moving forward, an extension of our active learning method to nondeterministic OTAs and timed automata involving multiple clocks is of particular interest.

References

1. F. Aarts, P. Fiterau-Brostean, H. Kuppens, and F. W. Vaandrager. Learning register automata with fresh value generation. In *ICTAC'15*, pages 165–183, 2015.
2. F. Aarts and F. W. Vaandrager. Learning I/O automata. In *CONCUR'10*, pages 71–85, 2010.
3. J. Abdullah, G. Dai, M. Mohaqeqi, and W. Yi. Schedulability analysis and software synthesis for graph-based task models with resource sharing. In *RTAS'18*, pages 261–270, 2018.
4. R. Alur and D. L. Dill. A theory of timed automata. *Theor. Comput. Sci.*, 126(2):183–235, 1994.
5. R. Alur, L. Fix, and T. A. Henzinger. Event-clock automata: A determinizable class of timed automata. *Theor. Comput. Sci.*, 211(1-2):253–273, 1999.
6. R. Alur and P. Madhusudan. Decision problems for timed automata: A survey. In *SFM-RT'04*, pages 1–24, 2004.
7. D. Angluin. Learning regular sets from queries and counterexamples. *Inf. Comput.*, 75(2):87–106, 1987.
8. G. Argyros and L. D’Antoni. The learnability of symbolic automata. In *CAV'18*, pages 427–445, 2018.
9. B. Bollig, P. Habermehl, C. Kern, and M. Leucker. Angluin-style learning of NFA. In *IJCAI'09*, pages 1004–1009, 2009.
10. B. Bollig, J.-P. Katoen, C. Kern, M. Leucker, D. Neider, and D. R. Piegdon. libalf: The automata learning framework. In *CAV'10*, pages 360–364, 2010.
11. B. Caldwell, R. Cardell-Oliver, and T. French. Learning time delay Mealy machines from programmable logic controllers. *IEEE Trans. Automation Science and Engineering*, 13(2):1155–1164, 2016.
12. S. Cassel, F. Howar, B. Jonsson, and B. Steffen. Active learning for extended finite state machines. *Formal Asp. Comput.*, 28(2):233–263, 2016.
13. D. E. Denning and G. M. Sacco. Timestamps in key distribution protocols. *Commun. ACM*, 24(8):533–536, 1981.
14. C. Dima. Real-time automata. *Journal of Automata, Languages and Combinatorics*, 6(1):3–23, 2001.
15. S. Drews and L. D’Antoni. Learning symbolic automata. In *TACAS'17*, pages 173–189, 2017.
16. A. Farzan, Y. Chen, E. M. Clarke, Y. Tsay, and B. Wang. Extending automated compositional verification to the full class of omega-regular languages. In *TACAS'08*, pages 2–17, 2008.
17. P. Fiterau-Brostean, R. Janssen, and F. W. Vaandrager. Combining model learning and model checking to analyze TCP implementations. In *CAV'16*, pages 454–471, 2016.
18. P. Fiterau-Brostean, T. Lenaerts, E. Poll, J. de Ruiter, F. W. Vaandrager, and P. Verleg. Model learning and model checking of SSH implementations. In *SPIN'17*, pages 142–151, 2017.
19. O. Grinchtein, B. Jonsson, and M. Leucker. Learning of event-recording automata. *Theor. Comput. Sci.*, 411(47):4029–4054, 2010.
20. J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley Publishing Company, 1979.
21. F. Howar, B. Jonsson, and F. W. Vaandrager. Combining black-box and white-box techniques for learning register automata. In *Computing and Software Science - State of the Art and Perspectives*, pages 563–588. Springer International Publishing, 2019.
22. F. Howar, B. Steffen, B. Jonsson, and S. Cassel. Inferring canonical register automata. In *VMCAI'12*, pages 251–266, 2012.
23. Information Science Institute, University of Southern California. Transmission control protocol (DARPA internet program protocol specification). <https://www.rfc-editor.org/rfc/rfc793.txt>, 1981.

24. M. Isberner, F. Howar, and B. Steffen. The open-source learnlib - A framework for active automata learning. In *CAV'15*, pages 487–495, 2015.
25. Y. Li, Y. Chen, L. Zhang, and D. Liu. A novel learning algorithm for büchi automata based on family of dfas and classification trees. In *TACAS'17*, pages 208–226, 2017.
26. O. Maler and I. Mens. Learning regular languages over large alphabets. In *TACAS'14*, pages 485–499, 2014.
27. T. Margaria, O. Niese, H. Raffelt, and B. Steffen. Efficient test-based model generation for legacy reactive systems. In *HLDVT'04*, pages 95–100, 2004.
28. J. Ouaknine and J. Worrell. On the language inclusion problem for timed automata: Closing a decidability gap. In *LICS'04*, pages 54–63, 2004.
29. F. Pastore, D. Micucci, and L. Mariani. Timed k-tail: Automatic inference of timed automata. In *ICST'17*, pages 401–411, 2017.
30. J. Schmidt, A. Ghorbani, A. Hapfelmeier, and S. Kramer. Learning probabilistic real-time automata from multi-attribute event logs. *Intell. Data Anal.*, 17(1):93–123, 2013.
31. M. Shahbaz and R. Groz. Inferring mealy machines. In *FM'09*, pages 207–222, 2009.
32. M. Stigge, P. Ekberg, N. Guan, and W. Yi. The digraph real-time task model. In *RTAS'11*, pages 71–80, 2011.
33. M. Tappler, B. K. Aichernig, G. Bacci, M. Eichlseder, and K. G. Larsen. L^* -based learning of Markov decision processes. In *FM'19*, pages 651–669, 2019.
34. M. Tappler, B. K. Aichernig, K. G. Larsen, and F. Lorber. Time to learn - learning timed automata from tests. In *FORMATS'19*, pages 216–235, 2019.
35. F. W. Vaandrager. Model learning. *Commun. ACM*, 60(2):86–95, 2017.
36. S. Verwer, M. de Weerd, and C. Witteveen. One-clock deterministic timed automata are efficiently identifiable in the limit. In *LATA'09*, pages 740–751, 2009.
37. S. Verwer, M. de Weerd, and C. Witteveen. The efficiency of identifying timed automata and the power of clocks. *Inf. Comput.*, 209(3):606–625, 2011.
38. S. Verwer, M. de Weerd, and C. Witteveen. Efficiently identifying deterministic real-time automata from labeled data. *Machine Learning*, 86(3):295–333, 2012.
39. S. Verwer, M. D. Weerd, and C. Witteveen. An algorithm for learning real-time automata. *Electrical Engineering Mathematics & Computer Science*, 2007.

Appendix A Proofs for Lemmas and Theorems

Proof (of Theorem 1). By the definitions of delay-timed word and reset-delay-timed word, it suffices that $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$ if $\mathcal{L}_r(\mathcal{A}) = \mathcal{L}_r(\mathcal{B})$. By the definitions of reset-delay-timed word and reset-logical-timed word with their mutual transforming method, we conclude that $\mathcal{L}_r(\mathcal{A}) = \mathcal{L}_r(\mathcal{B})$ iff $L_r(\mathcal{A}) = L_r(\mathcal{B})$. Hence, if $L_r(\mathcal{A}) = L_r(\mathcal{B})$, then $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$. This completes the proof. \square

Proof (of Lemma 1). A reset-logical-timed word $\gamma_r \in \mathbf{S} \cup \mathbf{R}$ happens in two cases, i.e., $\gamma_r \in \mathbf{S}$ or $\gamma_r \in \mathbf{R}$. For the first case, $\pi(\Pi_{\{1,2\}}\gamma_r \cdot e) \in \mathbf{S} \cup \mathbf{R}$ holds for all $e \in \mathbf{E}$ since \mathbf{T} is evidence-closed. Hence let $\gamma'_r = \pi(\Pi_{\{1,2\}}\gamma_r \cdot e)$, then obviously $\gamma'_r \in \mathbf{S} \cup \mathbf{R}$. Therefore, if $f(\gamma_r \cdot e) = +$, then $f(\gamma'_r \cdot e) = +$, meaning that γ'_r ends in $q_{row(\gamma'_r)} \in F_M$, namely the constructed DFA M accepts $\pi(\Pi_{\{1,2\}}\gamma_r \cdot e)$. Furthermore, if $f(\gamma_r \cdot e) = -$, then $f(\gamma'_r \cdot e) = -$, indicating that γ'_r ends in $q_{row(\gamma'_r)} \notin F_M$. This follows that M does not accept $\pi(\Pi_{\{1,2\}}\gamma_r \cdot e)$.

For the second case, i.e. $\gamma_r \in \mathbf{R}$, then there exists $\gamma'_r \in \mathbf{S}$ such that $row(\gamma'_r) = row(\gamma_r)$ since \mathbf{T} is closed, which further implies that $f(\gamma_r \cdot e) = f(\gamma'_r \cdot e)$ for all $e \in \mathbf{E}$. Thus, it is reduced to the first case. \square

Proof (of Lemma 2). Given a DFA M , by the above construction, for each transition $(q, (\sigma, \mu, b), q') \in \Delta_M$, there is a corresponding transition $\delta = (q, \sigma, I, b, q')$ where $\mu \in I \in P^c(\Psi_{q,\sigma})$ in the hypothesis \mathcal{H} . Hence, given a reset-logical-timed word $\pi(\Pi_{\{1,2\}}\gamma_r \cdot e) = (\sigma_1, \mu_1, b_1) \cdots (\sigma_n, \mu_n, b_n)$, \mathcal{H} accepts this word iff M accepts it. By Lemma 1, \mathcal{H} accepts $\pi(\Pi_{\{1,2\}}\gamma_r \cdot e)$ iff $f(\gamma_r \cdot e) = +$. \square

Proof (of Theorem 2). First, in order to guarantee \mathbf{T} being closed when moving an element $r \in \mathbf{R}$ to \mathbf{S} , the learner adds the reset-logical-timed word $\pi(\Pi_{\{1,2\}}r \cdot (\sigma, 0))$ for every $\sigma \in \Sigma$ to \mathbf{R} , which means that there is always at least a outgoing transition from $q_{row(r)}$ for every action in Σ . Secondly, Definition 3 implies that $P^c(\Psi_{q_{row(r)},\sigma})$ is a partition of $\mathbb{R}_{\geq 0}$ for every $\sigma \in \Sigma$. Hence, \mathcal{H} is a COTA. \square

Proof (of Theorem 3). By Lemma 1, 2 and Theorem 2, for every $\gamma_r \cdot e \in (\mathbf{S} \cup \mathbf{R}) \cdot \mathbf{E}$, there exists a unique accepting run ρ that admits $\pi(\Pi_{\{1,2\}}\gamma_r \cdot e)$ if $f(\gamma_r \cdot e) = +$. Hence, every logical-timed action (σ_i, μ_i, b_i) , with $1 \leq i \leq n$, triggers a transition $\delta_i = (q_i, \sigma_i, \phi_i, b_i, q_{i+1})$ from q_i to q_{i+1} , where $\mu_i \in \phi_i$ by Definition 3. By the above definition, $\llbracket \mu_i \rrbracket \subseteq \phi_i$, therefore (σ_i, μ'_i, b_i) can also trigger the transition δ_i . Hence, there exists a unique accepting run ρ' that admits $\gamma'_r = (\sigma_1, \mu'_1, b_1) \cdots (\sigma_n, \mu'_n, b_n)$, i.e., \mathcal{H} admits γ'_r . Suppose it is not the case when $f(\gamma_r \cdot e) = -$, it is easy to follow $f(\gamma_r \cdot e) = +$ by Lemma 2, which contradicts to $f(\gamma_r \cdot e) = -$. \square

Proof (of Theorem 4). Let $\gamma_r = (\sigma_1, \mu_1, b_1)(\sigma_2, \mu_2, b_2) \cdots (\sigma_n, \mu_n, b_n)$ and its normalization $\gamma'_r = (\sigma_1, \mu'_1, b_1)(\sigma_2, \mu'_2, b_2) \cdots (\sigma_n, \mu'_n, b_n)$. By the definition of g , $\llbracket \mu' \rrbracket = \llbracket \mu \rrbracket$. Therefore, if (σ_i, μ_i, b_i) fires a transition $\delta_i = (q_i, \sigma_i, \phi_i, b_i, q_{i+1})$, then (σ_i, μ'_i, b_i) can also fire the same transition according to the definition of Φ_c . Specifically, by the assumption that \mathbb{A} is deterministic, both the two timed actions can only be taken by the transition. Hence, γ'_r and γ_r share the same sequence of transitions in \mathbb{A} . \square

Proof (of Theorem 5). By Theorem 2, the returned hypothesis \mathcal{H} is a COTA. Then the correctness (i.e. \mathcal{H} recognizes the target timed language) follows directly from the equivalence query. Now we prove the termination. Observe that each reset-logical-timed word $s \in \mathcal{S}$ corresponds to a symbolic state reached after running s on \mathbb{A} . Since \mathbf{T} is reduced, implying that given any two elements $s_1, s_2 \in \mathcal{S}$, there exists $e \in E$ such that running $s_1 \cdot e$ and $s_2 \cdot e$ on \mathbb{A} gives different acceptance results. Further by Theorem 3, s_1 and s_2 must reach different symbolic states of \mathbb{A} . Hence, there is an injection from \mathcal{S} (or equivalently, the locations of \mathcal{H}) to symbolic states of \mathbb{A} . It follows that the size of the set \mathcal{S} is bounded by $|Q| \times (2\kappa + 2)$. Since each iteration of the algorithm either adds at least one element to \mathcal{S} or refines at least one of the partitions along transitions of \mathcal{H} , or both, the algorithm is guaranteed to terminate. \square

Proof (of Theorem 6). The algorithm can be viewed as a breadth-first-search (BFS) on a finite multi-way tree, each of whose nodes is a filled table instance. The depth of a node is the number of guessed resets. In other words, table instances at the same depth have the same number of guesses. The learner takes out a table instance that required the least number of guesses in *ToExplore* at every iteration. If $\mathbf{T} = (\Sigma, \Sigma, \Sigma_r, \mathcal{S}, \mathcal{R}, \mathcal{E}, f)$ is the final table in the learning process with a smart teacher, \mathbf{T} can be found at depth at most $(|\mathcal{S}| + |\mathcal{R}|) \times (1 + \sum_{e_i \in E \setminus \{\epsilon\}} (|e_i| - 1))$ of the tree, since it corresponds to choosing the correct table instance corresponding to the smart teacher situation at every guess. Then the learner can find \mathbf{T} after $2^{(|\mathcal{S}| + |\mathcal{R}|) \times (1 + \sum_{e_i \in E \setminus \{\epsilon\}} (|e_i| - 1))}$ steps in the worst case, since the learner has to check all of the tables at earlier depths before entering depth $(|\mathcal{S}| + |\mathcal{R}|) \times (1 + \sum_{e_i \in E \setminus \{\epsilon\}} (|e_i| - 1))$ and finds \mathbf{T} . Consequently, the algorithm terminates and returns a correct COTA \mathcal{H} which recognizes the target timed language \mathcal{L} . \square

Appendix B Detailed Learning Process for the DOTA \mathcal{A} in Fig. 1

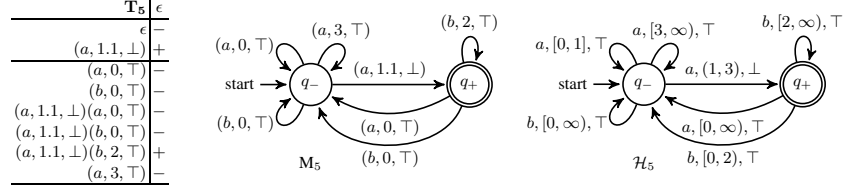
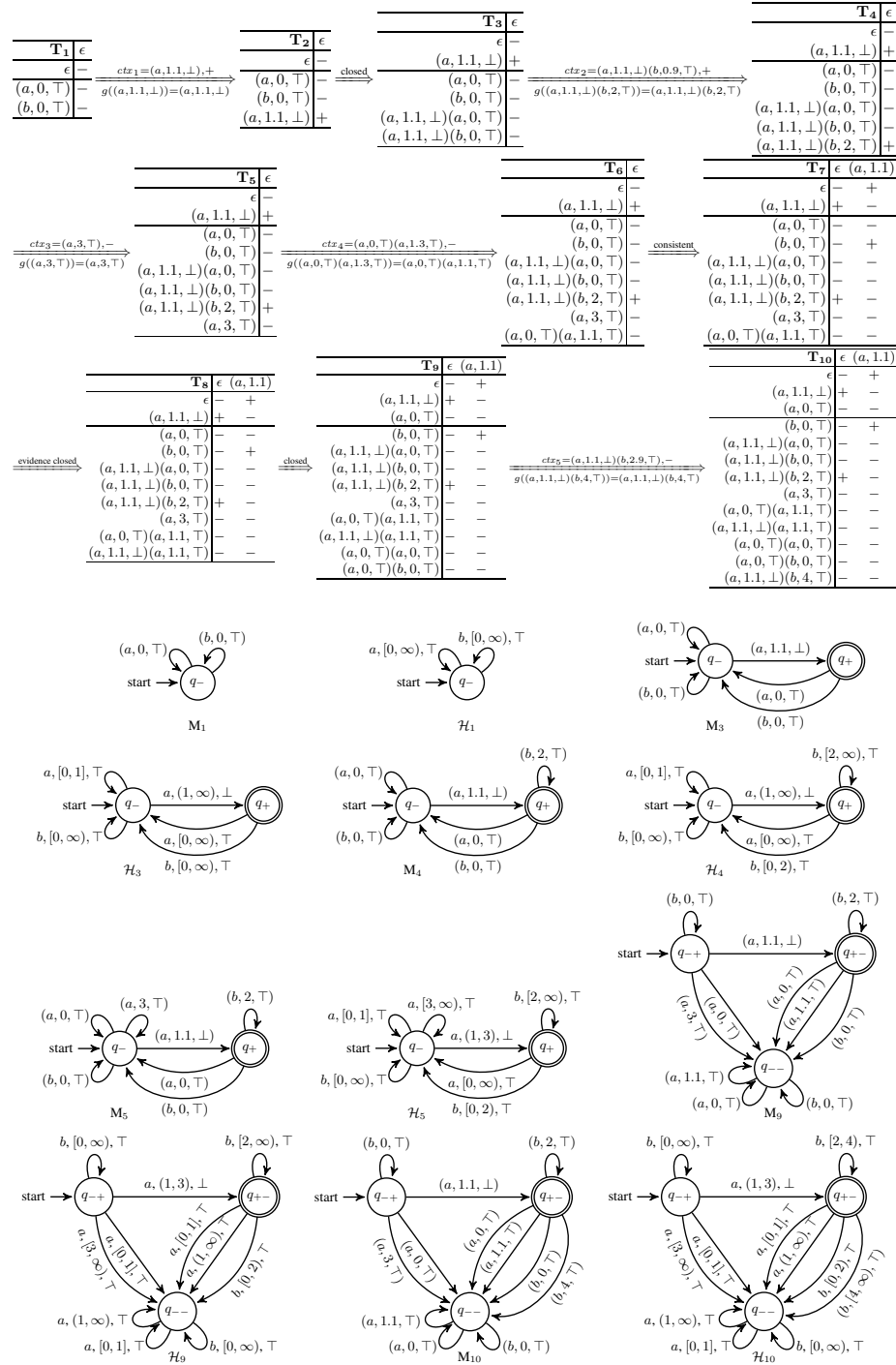


Fig. 4: The prepared timed observation table T_5 , the corresponding DFA M_5 and hypothesis \mathcal{H}_5 . A copy of Fig. 2 for the ease of reading.

Hypothesis construction for T_5 . Suppose \mathbb{A} in Fig. 1 recognizes the target timed language. Then the prepared table T_5 , the corresponding DFA M_5 and hypothesis \mathcal{H}_5 are depicted in Fig. 4 (a copy of Fig. 2 for the ease of reading). The learner first builds the DFA M_5 as follows. For ϵ and $(a, 1.1, \perp)$ in \mathcal{S} , set $Q_{M_5} = \{q_-, q_+\}$ with $row(\epsilon) = -$ and $row((a, 1.1, \perp)) = +$; while $q_{M_5}^0 = q_-$; $F_{M_5} = \{q_+\}$ with $f((a, 1.1, \perp) \cdot \epsilon) = +$; $\Sigma_{M_5} = \{(a, 0, \top), (b, 0, \top), (a, 1.1, \perp), (b, 2, \top), (a, 3, \top)\}$ and in the mean time $\Delta_{M_5} = \{(q_-, (a, 1.1, \perp), q_+), (q_-, (a, 0, \top), q_-), (q_-, (b, 0, \top), q_-), (q_+, (a, 0, \top), q_-), (q_+, (b, 0, \top), q_-), (q_+, (b, 2, \top), q_-), (q_-, (a, 3, \top), q_-)\}$. The DFA M_5 is then transformed to $\mathcal{H}_5 = (\Sigma, Q, q_0, F, c, \Delta)$ with the same set of locations, initial location and set of accepting locations. For location q_- , $\Psi_{q_-, a} = \{0, 3, 1.1\}$. We arrange it to a list $\ell_{q_-, a} = 0, 1.1, 3$ and then $P^c(\ell_{q_-, a}) = \{[0, 1], (1, 3), [3, \infty]\}$. Then for transitions $(q_-, (a, 0, \top), q_-)$, $(q_-, (a, 1.1, \perp), q_+)$ and $(q_-, (a, 3, \top), q_-)$ in Δ_{M_5} , let $\delta_1 = (q_-, a, [0, 1], \top, q_-)$, $\delta_2 = (q_-, a, (1, 3), \perp, q_+)$ and $\delta_3 = (q_-, a, [3, \infty], \top, q_-)$ be fresh transitions. The transformation for other locations and actions is analogous.

The entire learning process. In Fig. 5, a prepared T_1 is the initial instance of the table. The learner builds a DFA M_1 and a hypothesis \mathcal{H}_1 in Fig. 5. After making an equivalence query to the teacher, he receives a counterexample $ctx_1 = ((a, 1.1, \perp), +)$. By transforming the delay-timed-word $(a, 1.1, \perp)$ to a reset-logical-timed word $(a, 1.1, \perp)$, the learner adds the normalized counterpart to the table and thus get the second instance T_2 which is not closed. Hence, he moves $(a, 1.1, \perp)$ from \mathcal{R} to \mathcal{S} , and then adds reset-logical-timed words $(a, 1.1, \perp)(a, 0, \top)$ and $(a, 1.1, \perp)(b, 0, \top)$ to \mathcal{R} after membership queries. The instance T_3 is prepared. After two iterations, he arrives at T_5 . As described in Example 3, the learner normalizes the transformed reset-logical-timed word $(a, 0, \top)(a, 1.3, \top)$ as $(a, 0, \top)(a, 1.1, \top)$. Then he gets T_6 which is not consistent, since $row(\epsilon) = row((a, 0, \top))$ and $\Pi_{\{1, 2\}}((a, 1.1, \perp)) = \Pi_{\{1, 2\}}((a, 1.1, \top))$, but $row((a, 1.1, \perp)) \neq row((a, 0, \top)(a, 1.1, \top))$. Hence, he adds $(a, 1.1) \cdot \epsilon$ to \mathcal{E} for $f((a, 1.1, \perp) \cdot \epsilon) \neq f((a, 0, \top)(a, 1.1, \top) \cdot \epsilon)$ leading to T_7 . The process goes on until the learner finally gets a hypothesis \mathcal{H}_{10} which recognizes the target timed language. Obviously, after combining transitions according to guards in \mathcal{H}_{10} , we get a COTA same to \mathbb{A} as depicted in Fig. 1.

Fig. 5: Iterations of the timed observation table, DFAs and hypotheses w.r.t. \mathcal{A} in Fig. 1.

Appendix C Algorithm for Equivalence Queries

Algorithm 3: equivalence_query(\mathcal{H})

input : a hypothesis \mathcal{H} .
output: *equivalent* : a Boolean value to identify whether $\mathcal{L}(\mathcal{H}) = \mathcal{L}(\mathbb{A})$ where COTA \mathbb{A} recognizes the target language;
ctx : a counterexample.

```

1  equivalent  $\leftarrow \perp$ ; ctx  $\leftarrow \epsilon$ ;
2  flag-, flag+  $\leftarrow \top$ ;
3  if  $\mathcal{L}(\mathcal{H}) \not\subseteq \mathcal{L}(\mathbb{A})$  then
4    flag-  $\leftarrow \perp$ ; // negative counterexample
5    generate a reset-delay-timed word  $\omega_r$  from a bad configuration  $W$ ;
6    ctx-  $\leftarrow (\omega_r, -)$ ;
7  if  $\mathcal{L}(\mathbb{A}) \not\subseteq \mathcal{L}(\mathcal{H})$  then
8    flag+  $\leftarrow \perp$ ; // positive counterexample
9    generate a reset-delay-timed word  $\omega_r'$  from a bad configuration  $W'$ ;
10   ctx+  $\leftarrow (\omega_r', +)$ ;
11  equivalent  $\leftarrow \text{flag}_- \wedge \text{flag}_+$ ;
12  if equivalent =  $\perp$  then
13    ctx  $\leftarrow$  select a counterexample from ctx+ and ctx-;
14  return equivalent, ctx;

```

Appendix D Automata Pertaining to the TCP Protocol

Relabelling actions in [23] results in the automaton to be learned (left of Fig. 6):

$\{a: \text{passive OPEN}, b: \text{rcv SYN}, c: \text{SEND}, d: \text{rcv SYN, ACK}, e: \text{rcv ACK of SYN},$
 $f: \text{CLOSE}, g: \text{rcv FIN}, h: \text{rcv ACK of FIN}, i: \text{Timeout}, j: \text{active OPEN}\}.$

Mapping locations in the learnt automaton (right of Fig. 6) back to that in [23]:

$\{q_1: \text{CLOSED}, q_2: \text{LISTEN}, q_3: \text{SYN SENT}, q_4: \text{SYN RCVD}, q_5: \text{ESTAB},$
 $q_6, q_{15}: \text{FINWAIT} - 1, q_7, q_{14}: \text{CLOSE WAIT}, q_8, q_{13}: \text{CLOSING},$
 $q_9, q_{12}: \text{FINWAIT} - 2, q_{10}: \text{LAST} - \text{ACK}, q_{11}: \text{TIME WAIT}\}.$

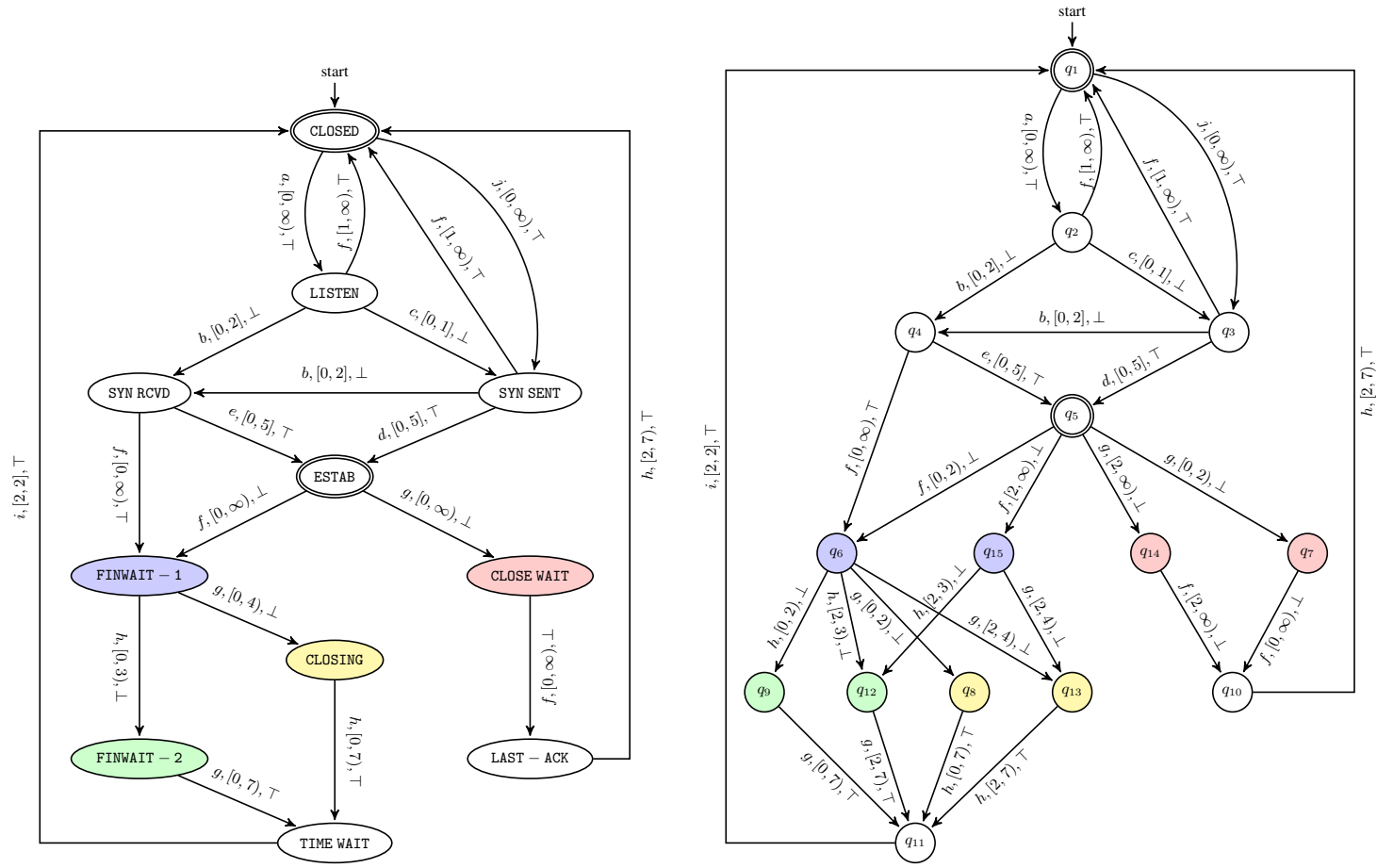


Fig. 6: Left: The functional specification of the TCP protocol with timing constraints. Right: The learnt functional specification of the TCP protocol. Colors indicate the splitting of locations incurred in the learning process.