2024 IEEE 63rd Conference on Decision and Control (CDC)
December 16-19, 2024. MiCo, Milan, Italy

# Verification of strong detectability of labeled real-time automata — A concurrent-composition method

Kuize Zhang and Alessandro Giua

*Abstract*— **Real-time automata are a widely-used class of real-time systems. In this paper, two versions of strong detectability are formulated for a labeled real-time automaton (LRTA) which means after some delay (the number of observed labels or real-time delay), along every generated infinite run, one can determine the current and subsequent states by observing the generated timed label sequence. By using the concurrent composition defined and computed in one of the authors' previous papers, necessary and sufficient conditions for the negations of the two strong versions of detectability are given. It is also proven that the verification problems for the two definitions of strong detectability are both coNP-complete.**

## I. Introduction

### A. Background

The *concurrent-composition* method in *labeled finite-state automata* (LFSAs) proposed in [1] by characterizing the *negation* of strong detectability has provided a unified method to verify almost all inference-based properties [2] such as strong versions of detectability, diagnosability, and predictability. Compared with the classical widely-used methods — the detector method [3] used for verifying strong versions of detectability, the twin-plant method [4] and the verifier method [5], [6] used for verifying diagnosability and predictability, the advantage of the concurrent-composition method lies in that it does not depend on any assumption, but the detector method, the twin-plant method, the verifier method, all depend on two fundamental assumptions of deadlock-freeness (an automaton will always run) and divergence-freeness (the running of an automaton will always be eventually observed), resulting in that these three methods (and their variants) only apply to a very restrictive subclass of LFSAs. In addition, the four methods have almost the same complexity. Hence whenever encountering a problem related to an inference-based property, the concurrent composition is the tool of the first choice.

In [7], [8], the definition of concurrent composition was *nontrivially* extended to *labeled weighted automata over monoids*, and necessary and sufficient conditions for strong versions of detectability were given based on the concurrent composition; particularly, for such automata over the monoid $(\mathbb{Q}^k, +)$, the concurrent-composition computation problem was proven to be NP-complete, and the strong detectability verification problem was proven to be coNP-complete. Later, in [9], the concurrent composition was used to verify two strong versions of detectability of labeled unambiguous weighted automata over rational semirings in exponential time (but the authors wrongly claimed that their algorithms ran in polynomial time). In [10], the concurrent composition was extended to *labeled real-time automata* (LRTAs) which are a widely-used class of real-time systems and a notion of diagnosability using infinite runs was formulated and verified based on the concurrent composition, the concurrent-composition computation problem was proven to be NP-complete and the diagnosability verification problem was proven to be coNP-complete.

The strong detectability verification problem in general labeled timed automata is PSPACE-complete [7], [11]. In these two papers, the negations of two strong versions of detectability were verified by using the combination of the classical parallel composition of two labeled timed automata and the region automaton [12] of a timed automaton. The combination was used earlier in [13] to verify the negation of diagnosability of labeled time automata.

### B. Contribution

In this paper, for LRTAs, we define two versions of strong detectability, which means there is a delay such that along every generated infinite run, after the delay one can determine the current and subsequent states by observing the generated timed label sequence, where a label represents an output. In the first version, the delay $k$ is the number of generated labels, that is, one observes a generated timed label sequence with at least a number $k$ of labels; in the second version, the delay $t$ is the real-time delay. Based on the concurrent composition formulated in [10], necessary and sufficient conditions for the negations of the two strong versions of detectability are given. The characterization of the first version is simpler but the characterization of the second version is much more involved. Moreover, we prove that both the necessary and sufficient conditions for the negations of the two versions can be verified in NP by using the technique of computing concurrent composition proposed in [10].

### C. Structure of the paper

In Section II, we present the background of our work, including notation, complexity results on state estimates in LRTAs proven in [14], and the concurrent composition formulated and computed in [10]. In Section III, we show the main results, including two strong versions of detectability,

This work was supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

Kuize Zhang and Alessandro Giua are with Department of Electrical and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy (kuize.zhang@unica.it and giua@unica.it).

their necessary and sufficient conditions based on the concurrent composition, and the complexity results on verifying these two versions of detectability. Section IV ends up the paper with a short conclusion.

## II. Preliminaries

### A. Notation

For an alphabet $\Sigma$, $\Sigma^*$ and $\Sigma^\omega$ denote the set of finite strings (including the empty string $\epsilon$) and the set of infinite strings over $\Sigma$. Elements of an alphabet are called *letters*. We also denote $\Sigma^+ := \Sigma^* \setminus \{\epsilon\}$. For a string $w \in \Sigma^*$, $|w|$ denotes its length, that is, the number of elements of $\Sigma$, counting repetitions, occurring in $w$; $w^\omega$ denotes the concatenation of infinitely many copies of $w$. For a string $s_1 \dots s_n$, where $s_1, \dots, s_n$ are letters, $s_1 =: \mathrm{init}(s_1 \dots s_n)$, $s_n =: \mathrm{last}(s_1 \dots s_n)$. For a string $(a_1, b_1) \dots (a_n, b_n) =: s$, $a_1 \dots a_n =: s(L)$, $b_1 \dots b_n =: s(R)$. As usual, $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ denote the sets of real numbers, rational numbers, integers, respectively. $\mathbb{R}_{\geq 0}$ and $\mathbb{R}_+$ denote the sets of nonnegative real numbers and positive real numbers, respectively. $\mathbb{Q}_{\geq 0}, \mathbb{Q}_+, \mathbb{Z}_{\geq 0}, \mathbb{Z}_+$ have analogous meanings. $[\![m, n]\!]$ denotes the set of integers no less than $m$ and no greater than $n$. $\subset$ denotes set inclusion and $\subsetneq$ denotes strict set inclusion.

### B. Labeled real-time automata

LRTAs are a special type of labeled timed automata. In an LRTA, there is only one clock and the clock will be reset upon each transition's execution.

An LRTA is a septuple

$$\mathcal{A} = (Q, E, Q_0, \Delta, \mu, \Sigma, \ell), \tag{1}$$

where $Q$ is a nonempty finite set of *states*, $E$ is an (finite) *alphabet* of *events*, $Q_0 \subset Q$ is a nonempty set of *initial states*, $\Delta \subset Q \times E \times Q$ is the *transition relation* and elements of $\Delta$ are called *transitions*, $\mu$ assigns to each transition $(q, e, q') \in \Delta$ (also written as $q \xrightarrow{e} q'$) a nonempty interval $\mu(e)_{qq'}$ of $\mathbb{R}_{\geq 0}$ with left endpoint and right endpoint being $a$ and $b$, where $a \in \mathbb{Q}_{\geq 0}$, $b \in \mathbb{Q}_{\geq 0} \cup \{+\infty\}$, $a \leq b$, $\Sigma$ is an alphabet of *labels*, and $\ell : E \to \Sigma \cup \{\epsilon\}$ is the *labeling function*. Removing $\mu$, $\mathcal{A}$ degenerates to an LFSA.

When $\mathcal{A}$ enters state $q$, the next event to occur is some $e$ such that $(q, e, q') \in \Delta$ and it will occur with a delay $t \in \mu(e)_{qq'}$; if no such event exists, $q$ is a *dead* state from which no further evolution is possible. When event $e \in E$ occurs, the *label* $\ell(e)$ of $e$ will be observed if $\ell(e) \neq \epsilon$, in this case $e$ is called *observable*; while nothing will be observed if $\ell(e) = \epsilon$, in this case $e$ is called *unobservable*. A transition $(q, e, q')$ is called *observable* (resp., *unobservable*) if $e$ is observable (resp., unobservable). We denote by $E_o$ and $E_{uo}$ the sets of observable events and unobservable events, respectively. Labeling function $\ell$ is extended to $E \times \mathbb{R}_{\geq 0}$ as follows: $\ell((e, t)) = (\ell(e), t)$ if $e \in E_o$, $\ell((e, t)) = \epsilon$ otherwise. Then $\ell$ is recursively extended to $E^* \cup E^\omega$ as $\ell(e_1 \dots e_n) = \ell(e_1) \dots \ell(e_n)$ and $\ell(e_1 \dots e_n \dots) = \ell(e_1) \dots \ell(e_n) \dots$ and also to $(E \times \mathbb{R}_{\geq 0})^* \cup (E \times \mathbb{R}_{\geq 0})^\omega$ analogously.

A *path* of $\mathcal{A}$ is defined by a sequence $q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} q_n$, where $n \in \mathbb{Z}_{\geq 0}$, $(q_{i-1}, e_i, q_i) \in \Delta$ for all $i \in [\![1, n]\!]$. When $n = 0$, the path degenerates to a single state $q_0$. A path is called a *cycle* if its start state and terminal state coincide. For two states $q$ and $q'$, $q'$ is called *reachable from* $q$ if there is a path from $q$ to $q'$. A state $q$ is called *reachable* if either $q \in Q_0$ or $q$ is reachable from some initial state. A *run* of $\mathcal{A}$ is a sequence $q_0 \xrightarrow{e_1/t_1} q_1 \xrightarrow{e_2/t_2} \cdots \xrightarrow{e_n/t_n} q_n =: \pi$, where $n \in \mathbb{Z}_{\geq 0}$, $(q_{i-1}, e_i, q_i) \in \Delta$, $t_i \in \mu(e_i)_{q_{i-1}q_i}$ for all $i \in [\![1, n]\!]$. We say the run $\pi$ is over path $q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} q_n$. Sometimes, we write a run or a path as $q_0 \to q_n$ for short if the intermediate states, events, and times are not needed to be written explicitly. Denote $q_0 =: \mathrm{init}(q_0 \to q)$ and $q =: \mathrm{last}(q_0 \to q)$. The *timed word* of run $\pi$ is defined by $\tau(\pi) = (e_1, t'_1)(e_2, t'_2) \dots (e_n, t'_n)$, where $t'_i = \sum_{k=1}^{i} t_k$ for all $i \in [\![1, n]\!]$. The *length* of a path/run/timed word is the length of its event sequence. The *weight/duration* $\mathrm{WT}_\pi$ of run $\pi$ and the *weight/duration* $\mathrm{WT}_{\tau(\pi)}$ of timed word $\tau(\pi)$ are both defined by $t'_n$. A path or run is called *unobservable* if $\ell(e_1 \dots e_n) = \epsilon$, and called *observable* otherwise. A run is called *instantaneous* if its weight is equal to 0. For a *dead* state $q \in Q$, add an unobservable transition $(q, u, q)$ with $\mu(u)_{qq} = [0, +\infty)$. This modification is reasonable because whenever $\mathcal{A}$ transitions to such a state $q$, it will always stay there and no label will be generated, but time will still elapse.

For a run $\pi$ starting from some initial state, $\ell(\tau(\pi)) \in (\Sigma \times \mathbb{R}_{\geq 0})^*$ is called a *timed label sequence generated by* $\mathcal{A}$. In this case, we observe $\ell(e_i)$ at time $t'_i$ if $e_i \in E_o$, observe nothing at time $t'_i$ if $e_i \in E_{uo}$, $i \in [\![1, n]\!]$. More generally, a sequence $(\sigma_1, t_1) \dots (\sigma_n, t_n) =: \gamma$ in $(\Sigma \times \mathbb{R}_{\geq 0})^*$ is called a *timed label sequence* if $t_1 \leq \cdots \leq t_n$. The *weight* $\mathrm{WT}_\gamma$ of timed label sequence $\gamma$ is defined as $t_n$. Particularly, $\mathrm{WT}_\epsilon := 0$. The *length* of a timed label sequence is the length of its label sequence. The *timed language* $L(\mathcal{A})$ generated by $\mathcal{A}$ is defined by the set of timed words of all runs of $\mathcal{A}$ starting from initial states; $\mathcal{L}(\mathcal{A})$ is the set of timed label sequences generated by $\mathcal{A}$.

Analogously, an *infinite path*, an *infinite run*, the *timed word*, *weight*, and the *timed label sequence* of an infinite run can be defined, where such timed words are called *timed $\omega$-words*, and such timed label sequences are called *timed $\omega$-label sequences*. The weight of an infinite run can be either a nonnegative real number or $+\infty$. The *timed $\omega$-language* $L^\omega(\mathcal{A})$ generated by $\mathcal{A}$ is defined by the set of timed $\omega$-words of all infinite runs of $\mathcal{A}$ starting from initial states; $\mathcal{L}^\omega(\mathcal{A})$ is the set of timed $\omega$-label sequences generated by $\mathcal{A}$.

Consider an LRTA $\mathcal{A}$. Given a subset $Q' \subset Q$ of states and a timed label sequence $\gamma = (\sigma_1, t_1) \dots (\sigma_n, t_n) \in (\Sigma \times \mathbb{R}_{\geq 0})^*$, the *current-state estimate* of $\mathcal{A}$ with respect to $Q'$ and $\gamma$ is defined by

$$\begin{aligned}\mathcal{M}(\mathcal{A}, \gamma | Q') = \{q \in Q | (\exists \text{ run } \pi)[(\mathrm{init}(\pi) \in Q') \wedge \\ (\mathrm{last}(\pi) = q) \wedge (\ell(\tau(\pi)) = \gamma) \wedge \\ (\mathrm{WT}_\pi = \mathrm{WT}_\gamma)]\}.\end{aligned} \tag{2}$$

Particularly, denote

$$\mathcal{M}(\mathcal{A}, \gamma | Q_0) =: \mathcal{M}(\mathcal{A}, \gamma).$$

$\mathcal{M}(\mathcal{A},\gamma|Q')$ exactly contains the set of states that can be reached from a state in $Q'$ by a run $\pi$ which produces timed label sequence $\gamma$ and has weight $\mathrm{WT}_\pi$ equal to $\mathrm{WT}_\gamma$.

$\mathcal{M}(\mathcal{A},\epsilon|Q')$ can be computed in P, while $\mathcal{M}(\mathcal{A},\gamma|Q')$ can be computed in NP if all $t_1,\dots,t_n$ belong to $\mathbb{Q}$ [14, Theorem 3.1].

Consider a timed label sequence $\gamma = (\sigma_1,t_1)\dots(\sigma_n,t_n) \in (\Sigma\times\mathbb{R}_{\geq 0})^*$ and $t\in\mathbb{R}_+$ with $t > \mathrm{WT}_\gamma$. Define the *current-state estimate* of $\mathcal{A}$ with respect to $\gamma$ and $Q'\subset Q$ at instant $t$ as

$$\begin{aligned}
\mathcal{M}(\mathcal{A},\gamma,t|Q') = \{q\in Q|(\exists \text{ unobservable run } \pi)[ && \text{(3a)}\\
(\mathrm{init}(\pi)\in\mathcal{M}(\mathcal{A},\gamma|Q'))\wedge && \text{(3b)}\\
(\mathrm{last}(\pi)=q)\wedge && \text{(3c)}\\
(\mathrm{WT}_\pi = t-\mathrm{WT}_\gamma)]\}\cup && \text{(3d)}\\
\{q\in Q|(\exists \text{ unobservable run} && \text{(3e)}\\
\pi \xrightarrow{e'/t'} q')[ && \text{(3f)}\\
(\mathrm{init}(\pi)\in\mathcal{M}(\mathcal{A},\gamma|Q'))\wedge && \text{(3g)}\\
(\mathrm{last}(\pi)=q)\wedge && \text{(3h)}\\
(\mathrm{WT}_\pi < t-\mathrm{WT}_\gamma < && \text{(3i)}\\
\mathrm{WT}_\pi + t')]\}. && \text{(3j)}
\end{aligned}$$

Similarly, denote

$$\mathcal{M}(\mathcal{A},\gamma,t|Q_0) =: \mathcal{M}(\mathcal{A},\gamma,t). \tag{4}$$

$\mathcal{M}(\mathcal{A},\gamma,t|Q')$ exactly contains the set of states that can be reached from a state in $Q'$ after exactly time interval $t$ by a run which produces timed label sequence $\gamma$ and has weight greater than or equal to $t$.

Also by [14, Theorem 3.1], $\mathcal{M}(\mathcal{A},\gamma,t|Q')$ can be computed in NP if all $t_1,\dots,t_n,t$ belong to $\mathbb{Q}$.

We summarize these complexity results on state estimates as follows.

*Proposition 2.1:* Consider an LRTA $\mathcal{A}$, a subset $Q'\subset Q$ of states, a time label sequence $\gamma=(\sigma_1,t_1)\dots(\sigma_n,t_n)\in(\Sigma\times\mathbb{Q}_{\geq 0})^+$ and $t,t'\in\mathbb{Q}_+$ with $t>t_n$. $\mathcal{M}(\mathcal{A},\epsilon|Q')$ can be computed in P, while $\mathcal{M}(\mathcal{A},\gamma|Q')$, $\mathcal{M}(\mathcal{A},\gamma,t|Q')$, and $\mathcal{M}(\mathcal{A},\epsilon,t'|Q')$ can be computed in NP.

*Remark 1:* The method proposed in [15], [14] to compute an observer of an LRTA can be slightly modified to verify the two definitions of opacity in constant-time labeled automata (CTLAs) studied in [16], where the CTLAs are actually special LRTAs whose time intervals are singletons. In addition, the main results obtained in [17] (that is, Alg. 2 and Alg. 3 therein) are special cases of Proposition 2.1.

Based on similar argument, by [14, Lemma 2.2], we have the following result.

*Proposition 2.2:* Consider an LRTA $\mathcal{A}$ and two subsets $Q_1',Q_2'\subset Q$ of states. Whether there is $t\in\mathbb{Q}_+$ such that $Q_2'\subset\mathcal{M}(\mathcal{A},\epsilon,t|Q_1')$ can be checked in NP.

### C. The notion of concurrent composition

Next we introduce the main tool — concurrent composition. For two LFSAs, in their concurrent composition, observable transitions are synchronized and unobservable transitions interleave [1]. The concurrent composition of two LRTAs [10] is a natural generalization of the concurrent composition of two LFSAs, and fundamentally more complex. The concurrent composition of two LFSAs can be computed in time polynomial in the sizes of the two LFSAs [1], but the concurrent-composition computation problem of two LRTAs is NP-complete [10]. We will use a variant of the concurrent composition proposed and computed in [10].

*Definition 1:* For an LRTA $\mathcal{A}$, the concurrent composition of an LRTA $\mathcal{A}$ and itself, called the *self-composition* of $\mathcal{A}$, denoted as $\mathrm{CC}(\mathcal{A})$, is defined by

$$(Q',E_o',Q_0',\Delta',\mu',\Sigma,\ell'), \tag{5}$$

where

- $Q'=Q\times Q$;
- $E_o'=\{(e_1,e_2)\in E_o\times E_o|\ell(e_1)=\ell(e_2)\}$;
- $Q_0'=Q_0\times Q_0$ is the set of initial states;
- $\Delta'\subset Q'\times E'\times Q'$ is the transition relation;
- $\ell'(e_1,e_2)=\ell(e_1)=\ell(e_2)$ for all $(e_1,e_2)\in E_o'$.

For all states $(q_1,q_2),(q_3,q_4)\in Q'$ and events $(e_1,e_2)\in E_o'$, $((q_1,q_2),(e_1,e_2),(q_3,q_4))\in\Delta'$ if and only if there are two runs:

$$\pi_1 := q_1 \xrightarrow{\bar{e}_u^1/\bar{t}_u^1\dots\bar{e}_u^n/\bar{t}_u^n} q_5 \xrightarrow{e_1/t_1} q_7 \xrightarrow{\tilde{e}_u^1/0\dots\tilde{e}_u^m/0} q_3, \tag{6a}$$
$$\pi_2 := q_2 \xrightarrow{\hat{e}_u^1/\hat{t}_u^1\dots\hat{e}_u^r/\hat{t}_u^r} q_6 \xrightarrow{e_2/t_2} q_8 \xrightarrow{\breve{e}_u^1/0\dots\breve{e}_u^s/0} q_4, \tag{6b}$$

where states $q_5,q_6,q_7,q_8\in Q$, $\bar{e}_u^1\dots\bar{e}_u^n\in(E_{uo})^*$, $\tilde{e}_u^1\dots\tilde{e}_u^m\in(E_{uo})^*$, $\hat{e}_u^1\dots\hat{e}_u^r\in(E_{uo})^*$, $\breve{e}_u^1,\dots,\breve{e}_u^s\in(E_{uo})^*$, $\bar{t}_u^1,\dots,\bar{t}_u^n,t_1,\hat{t}_u^1,\dots,\hat{t}_u^r,t_2\in\mathbb{R}_{\geq 0}$, $\sum_{i=1}^n\bar{t}_u^i+t_1=\sum_{i=1}^r\hat{t}_u^i+t_2$. The two runs' weights are equal. Such $\pi_1$ and $\pi_2$ are called left and right *admissible runs* of transition $((q_1,q_2),(e_1,e_2),(q_3,q_4))$. Define the weight of the transition as $\mu'(((q_1,q_2),(e_1,e_2),(q_3,q_4)))=+$ if the transition has an admissible run with positive weight; define its weight as $\mu'(((q_1,q_2),(e_1,e_2),(q_3,q_4)))=0$ if the transition only has weight-0 admissible runs.

An observable transition $(q_1,q_2)\xrightarrow{(e_1,e_2)}(q_3,q_4)$ in $\mathrm{CC}(\mathcal{A})$ is interpreted as follows: at the beginning $\mathcal{A}$ is in state $q_1$ or $q_2$ and transition to state $q_3$ or $q_4$ after some common time delay when event $e_1$ or $e_2$ occurs. That is, in the two cases, the two observable events $e_1$ and $e_2$ occur simultaneously. Therefore, after $e_1$ and $e_2$, we only consider instantaneous transitions. Positive weight for the observable transition means the transition from $q_1$ to $q_3$ may cost positive time. Zero weight for the observable transition means that the transition from $q_1$ to $q_3$ never costs time. A complete procedure for computing $\mathrm{CC}(\mathcal{A})$ is referred to Section III.B of [10].

*Example 1:* An LRTA $\mathcal{A}_1$ is depicted in Fig. 1. The reachable part of self-composition $\mathrm{CC}(\mathcal{A}_1)$ is illustrated in Fig. 2. $((q_0,q_0),(e_1,e_2),(q_3,q_4))$ is an observable transition, $q_0\xrightarrow{u/1}q_1\xrightarrow{e_1/2}q_3$ and $q_0\xrightarrow{u/0.9}q_2\xrightarrow{e_2/2.1}q_4$ are two of its admissible runs, where both of them produce the timed label sequence $(\sigma,3)$.

*Theorem 2.3 ([10]):* Consider an LRTA $\mathcal{A}$, its self-composition $\mathrm{CC}(\mathcal{A})$ computation problem is NP-complete.

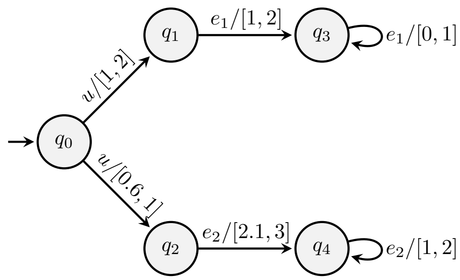


Fig. 1. LRTA $\mathcal{A}_1$, where $q_0$ is the initial state (having an input arrow from nowhere), $u$ is unobservable, $e_1$ and $e_2$ are observable and $\ell(e_1) = \ell(e_2) = \sigma$.

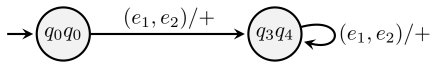


Fig. 2. Reachable part of self-composition $\mathrm{CC}(\mathcal{A}_1)$, where LRTA $\mathcal{A}_1$ is shown in Fig. 1.

## III. Main Results

### A. Definitions of strong label-detectability and strong time-detectability for LRTAs

In this subsection, we define two versions of strong detectability.

*Definition 2 (SLD):* An LRTA $\mathcal{A}$ is called *strongly label-detectable* if there is $k \in \mathbb{Z}_+$ such that for every timed $\omega$-word $w \in L^\omega(\mathcal{A})$, for each prefix $\gamma$ of $\ell(w)$, if $|\gamma| \ge k$, then $|\mathcal{M}(\mathcal{A}, \gamma)| = 1$.

By Definition 2, if an LRTA $\mathcal{A}$ is strongly label-detectable, then there is a delay $k$ such that after observing at least $k$ generated labels, one can determine the current and subsequent states.

When the delay $k$ in Definition 2 is changed to real-time delay rather than the number of observed labels as in Definition 2, the definition of strong detectability can be reformulated as follows.

*Definition 3 (STD):* An LRTA $\mathcal{A}$ is called *strongly time-detectable* if there is time delay $t \in \mathbb{R}_{\ge 0}$ such that for every timed $\omega$-word $w \in L^\omega(\mathcal{A})$ satisfying $\mathrm{WT}_w = +\infty$, for each prefix $w'$ of $w$, if $\mathrm{WT}_{w'} > t$, then $|\mathcal{M}(\mathcal{A}, \ell(w'))| = 1$ when $\mathrm{WT}_{w'} = \mathrm{WT}_{\ell(w')}$, and $|\mathcal{M}(\mathcal{A}, \ell(w'), \mathrm{WT}_{w'})| = 1$ when $\mathrm{WT}_{w'} > \mathrm{WT}_{\ell(w')}$.

By Definition 3, if an LRTA $\mathcal{A}$ is strongly time-detectable, then there is a real-time delay $t$ such that along every generated infinite run with weight $+\infty$, after time $t$, one can determine the current and subsequent states.

### B. Necessary and sufficient conditions for strong versions of detectability based on concurrent composition

*1) A necessary and sufficient condition for strong label-detectability (with respect to Definition 2):*

*Theorem 3.1:* An LRTA $\mathcal{A}$ is not strongly label-detectable if and only if in its self-composition $\mathrm{CC}(\mathcal{A})$,

(i) there exists a path

$$q'_0 \xrightarrow{s'_1} q'_1 \xrightarrow{s'_2} q'_1 \xrightarrow{s'_3} q'_2 \tag{7}$$

such that

$$q'_0 \in Q'_0; q'_1, q'_2 \in Q'; s'_1, s'_3 \in (E'_o)^*; \tag{8a}$$
$$s'_2 \in (E'_o)^+; q'_2(L) \ne q'_2(R); \tag{8b}$$

(ii) in $\mathcal{A}$, there exists a cycle reachable from $q'_2(L)$.

**Proof** By Definition 2, $\mathcal{A}$ is not strongly label-detectable if and only if for all $k \in \mathbb{Z}_+$, there exists $w_k \in L^\omega(\mathcal{A})$ and $\gamma \sqsubset \ell(w_k)$, such that $|\gamma| \ge k$ and $|\mathcal{M}(\mathcal{A}, \gamma)| > 1$.

"if": Arbitrarily given $k \in \mathbb{Z}_+$, consider path $q'_0 \xrightarrow{s'_1} q'_1 \xrightarrow{(s'_2)^k} q'_1 \xrightarrow{s'_3} q'_2 =: \pi'$, we choose an admissible run of the path as $q'_0(L) \xrightarrow{\bar{s}_1} q'_1(L) \xrightarrow{\bar{s}_2} q'_1(L) \xrightarrow{\bar{s}_3} q'_2(L) =: \pi_L$ (in which the weights are omitted, the same below), then $\ell(\bar{s}_1) = \ell'(s'_1)$, $\ell(\bar{s}_2) = \ell'((s'_2)^k)$, $\ell(\bar{s}_3) = \ell'(s'_3)$, and $\mathcal{M}(\mathcal{A}, \gamma) \supset \{q'_2(L), q'_2(R)\}$, where $\gamma = \ell(\tau(\pi_L))$; by condition (ii) there also exists a run $q'_2(L) \xrightarrow{\bar{s}_4} q_3 \xrightarrow{\bar{s}_5} q_3$, where $\bar{s}_5 \in E^+$. Note that $q_3 \xrightarrow{\bar{s}_5} q_3$ can be repeated for infinitely many times. Choose

$$w_k = \tau(\pi),$$

where $\pi = q'_0(L) \xrightarrow{\bar{s}_1} q'_1(L) \xrightarrow{\bar{s}_2} q'_1(L) \xrightarrow{\bar{s}_3} q'_2(L) \xrightarrow{\bar{s}_4} q_3 \left(\xrightarrow{\bar{s}_5} q_3\right)^\omega$, one has $w_k \in L^\omega(\mathcal{A})$, $\gamma \sqsubset \ell(w_k)$, $|\gamma| \ge k+2$, and $|\mathcal{M}(\mathcal{A}, \gamma)| > 1$. That is, $\mathcal{A}$ is not strongly label-detectable.

"only if": Assume that $\mathcal{A}$ is not strongly label-detectable. Choose $k > |Q|^2$, $w_k \in L^\omega(\mathcal{A})$, and $\gamma \sqsubset \ell(w_k)$ such that $|\gamma| \ge k$ and $|\mathcal{M}(\mathcal{A}, \gamma)| > 1$. Then there exist two different runs $\pi_1$ and $\pi_2$ starting at initial states and ending at different states such that $\tau(\pi_1) = \tau(\pi_2) \sqsubset w_k$, and after the last observable events of $\pi_1$ and $\pi_2$, the runs are unobservable and instantaneous, and starting at the last state of $\pi_1$ there is an infinite run. By definition of $\mathrm{CC}(\mathcal{A})$, from $\pi_1$ and $\pi_2$ one can construct a path of $\mathrm{CC}(\mathcal{A})$ as in (7) by the Pigeonhole Principle, because $\mathrm{CC}(\mathcal{A})$ has at most $|Q|^2$ states. On the other hand, because $\mathcal{A}$ has finitely many states, and based on the infinite run starting at the last state of $\pi_1$, condition (ii) holds. □

*Example 2:* Reconsider the LRTA $\mathcal{A}_1$ in Fig. 1 and its self-composition $\mathrm{CC}(\mathcal{A}_1)$ in Fig. 2. One sees a path $(q_0, q_0) \xrightarrow{(e_1,e_2)} (q_3, q_4) \xrightarrow{(e_1,e_2)} (q_3, q_4)$ as in (7) in $\mathrm{CC}(\mathcal{A}_1)$ and a cycle on $q_3$ in $\mathcal{A}_1$, then by Theorem 3.1, $\mathcal{A}_1$ is not strongly label-detectable. Directly by Definition 2, choose run $q_0 \xrightarrow{u/1} q_1 \xrightarrow{e_1/2} q_3 \left(\xrightarrow{e_1/1} q_3\right)^\omega =: \pi$ and timed $\omega$-word $w = \tau(\pi) = (u, 1)(e_1, 3)(e_1, 4) \ldots \in L^\omega(\mathcal{A}_1)$, $\ell(w) = (\sigma, 3)(\sigma, 4) \ldots$. For all $k \in \mathbb{Z}_+$, $\mathcal{M}(\mathcal{A}_1, (\sigma, 3)(\sigma, 4) \ldots (\sigma, k+2)) = \{q_3, q_4\}$ which is not a singleton, also by the cycle on $q_3$, we conclude that $\mathcal{A}_1$ is not strongly label-detectable.

*2) A necessary and sufficient condition for strong time-detectability (with respect to Definition 3):* The procedure for deriving a necessary and sufficient condition for strong time-detectability is much more complicated. To this end, we need to define a special class of transitions for $\mathrm{CC}(\mathcal{A})$. A transition $(q_1, q_2) \xrightarrow{(e_1,e_2)} (q_3, q_4)$ is called *time-unbounded* if it has two admissible runs each of which contains a transition of $\mathcal{A}$ whose time interval is unbounded before the terminating state of the observable transition (e.g., $q_7$ and $q_8$ in (6)). By definition, for a time-unbounded transition, the weight of each of its two admissible runs as in (6) can be arbitrarily large. The two transitions with unbounded time intervals can be two unobservable transitions in the two paths as in (6a) and (6b) before $e_1$ and $e_2$, respectively, can be the two observable transitions as in (6a) and (6b) with events $e_1$ and $e_2$, respectively, can also be the observable transition in (6a) and an unobservable transition in (6b) before $e_2$, or vice versa. A slight change of the proof of [10, Theorem 3.1] implies the following result.

*Proposition 3.2:* Whether a transition $(q_1, q_2) \xrightarrow{(e_1,e_2)} (q_3, q_4)$ is time-unbounded can be checked in NP.

In addition, we also need the following results.

*Proposition 3.3:* Consider an LRTA $\mathcal{A}$ and a reachable state $q \in Q$. Starting from $q$ there is an infinite run with weight $+\infty$ if and only if some cycle is reachable from $q$ and in the cycle there is a transition whose interval contains a positive number.

*Proposition 3.4:* An LRTA $\mathcal{A}$ is not strongly time-detectable if and only if for all $t \in \mathbb{R}_{\geq 0}$, there exists $w_t \in L^\omega(\mathcal{A})$ satisfying $\mathrm{WT}_{w_t} = +\infty$ and $w' \sqsubset w_t$ such that $\mathrm{WT}_{w'} > t$, $|\mathcal{M}(\mathcal{A}, \ell(w'))| > 1$ when $\mathrm{WT}_{w'} = \mathrm{WT}_{\ell(w')}$, and $|\mathcal{M}(\mathcal{A}, \ell(w'), \mathrm{WT}_{w'})| > 1$ when $\mathrm{WT}_{w'} > \mathrm{WT}_{\ell(w')}$.

*Theorem 3.5:* An LRTA $\mathcal{A}$ is not strongly time-detectable if and only if at least one of the following six conditions holds.

(A) In the self-composition $\mathrm{CC}(\mathcal{A})$, there exists a path

$$q_0' \xrightarrow{s_1'} q_1', \tag{9}$$

where $q_0' \in Q_0'$, $s_1' \in (E_o')^+$, $q_1'(L) \neq q_1'(R)$, $q_0' \xrightarrow{s_1'} q_1'$ contains at least one time-unbounded transition, and in $\mathcal{A}$ starting from $q_1'(L)$ there is an infinite run with weight $+\infty$.

(B) In $\mathrm{CC}(\mathcal{A})$, there exists a path

$$q_0' \xrightarrow{s_1'} q_1' \xrightarrow{s_2'} q_1' \xrightarrow{s_3'} q_2', \tag{10}$$

where $q_0' \in Q_0'$, $s_1', s_3' \in (E_o')^*$, $s_2' \in (E_o')^+$, $q_2'(L) \neq q_2'(R)$, $q_1' \xrightarrow{s_2'} q_1'$ contains at least one transition with weight $+$, and in $\mathcal{A}$ starting from $q_2'(L)$ there is an infinite run with weight $+\infty$.

(C) In $\mathrm{CC}(\mathcal{A})$, there exists a path

$$q_0' \xrightarrow{s_1'} q_1', \tag{11}$$

where $q_0' \in Q_0'$, $s_1' \in (E_o')^+$, $q_0' \xrightarrow{s_1'} q_1'$ contains at least one time-unbounded transition, there are two distinct states $\hat{q}, \bar{q}$ of $\mathcal{A}$ such that for some $s \in \mathbb{Q}_+$, $\mathcal{M}(\mathcal{A}, \epsilon, s|\{q_1'(L), q_1'(R)\}) \supset \{\hat{q}, \bar{q}\}$, and either

a) there is an unobservable run $q_1'(L) \to \hat{q}$ with weight $s$ and starting from $\hat{q}$ there is an infinite run with weight $+\infty$, or
b) there is an unobservable run $q_1'(L) \to \hat{q} \to \tilde{q}$ satisfying $\mathrm{WT}_{q_1'(L)\to\hat{q}} < s < \mathrm{WT}_{q_1'(L)\to\hat{q}\to\tilde{q}}$, $\hat{q} \to \tilde{q}$ is of length 1, and starting from $\tilde{q}$ there is an infinite run with weight $+\infty$.

(D) In $\mathrm{CC}(\mathcal{A})$, there exists a path

$$q_0' \xrightarrow{s_1'} q_1' \xrightarrow{s_2'} q_1' \xrightarrow{s_3'} q_2', \tag{12}$$

where $q_0' \in Q_0'$, $s_1', s_3' \in (E_o')^*$, $s_2' \in (E_o')^+$, $q_1' \xrightarrow{s_2'} q_1'$ contains at least one transition with weight $+$, there are two distinct states $\hat{q}, \bar{q}$ of $\mathcal{A}$ such that for some $s \in \mathbb{Q}_+$, $\mathcal{M}(\mathcal{A}, \epsilon, s|\{q_2'(L), q_2'(R)\}) \supset \{\hat{q}, \bar{q}\}$, and either

a) there is an unobservable run $q_2'(L) \to \hat{q}$ with weight $s$ and starting from $\hat{q}$ there is an infinite run with weight $+\infty$, or
b) there is an unobservable run $q_2'(L) \to \hat{q} \to \tilde{q}$ satisfying $\mathrm{WT}_{q_2'(L)\to\hat{q}} < s < \mathrm{WT}_{q_2'(L)\to\hat{q}\to\tilde{q}}$, $\hat{q} \to \tilde{q}$ is of length 1, and starting from $\tilde{q}$ there is an infinite run with weight $+\infty$.

(E) In $\mathrm{CC}(\mathcal{A})$, there exists a path

$$q_0' \xrightarrow{s_1'} q_1', \tag{13}$$

where $q_0' \in Q_0'$, $s_1' \in (E_o')^*$, there are two distinct states $\hat{q}, \bar{q}$ of $\mathcal{A}$ and two unobservable paths

$$q_1'(L) \to \hat{q}, \tag{14a}$$
$$q_1'(R) \to \bar{q}, \tag{14b}$$

such that one of (14a) and (14b) has a transition with unbounded time interval, the other has either a transition with unbounded time interval or a cycle containing a transition whose time interval contains at least one positive number, and starting from $\hat{q}$ there is an infinite run with weight $+\infty$.

(F) In $\mathrm{CC}(\mathcal{A})$, there exists a path

$$q_0' \xrightarrow{s_1'} q_1', \tag{15}$$

where $q_0' \in Q_0'$, $s_1' \in (E_o')^*$, there are two distinct states $\hat{q}, \bar{q}$ of $\mathcal{A}$, either

a) there are two unobservable runs

$$q_1'(L) \to \hat{q}, \tag{16a}$$
$$q_1'(R) \to \bar{q}, \tag{16b}$$

such that $\mathrm{WT}_{q_1'(L)\to\hat{q}} = \mathrm{WT}_{q_1'(R)\to\bar{q}}$, each of $q_1'(L) \to \hat{q}$ and $q_1'(R) \to \bar{q}$ has a cycle with positive weight, and starting from $\hat{q}$ there is an infinite run with weight $+\infty$, or

b) there are two unobservable runs

$$q_1'(L) \to \hat{q}, \tag{17a}$$
$$q_1'(R) \to \bar{q} \to \tilde{q}, \tag{17b}$$

such that $\mathrm{WT}_{q_1'(R)\to\bar{q}} < \mathrm{WT}_{q_1'(L)\to\hat{q}} < \mathrm{WT}_{q_1'(R)\to\bar{q}\to\tilde{q}}$, $\bar{q} \to \tilde{q}$ is of length 1, each of $q_1'(L) \to \hat{q}$ and $q_1'(R) \to \bar{q}$ has a cycle with positive weight, and starting from $\hat{q}$ there is an infinite run with weight $+\infty$, or

c) there are two unobservable runs

$$q_1'(L) \to \hat{q} \to \tilde{q}, \quad (18a)$$
$$q_1'(R) \to \bar{q}, \quad (18b)$$

such that $\mathrm{WT}_{q_1'(L)\to\hat{q}} < \mathrm{WT}_{q_1'(R)\to\bar{q}} < \mathrm{WT}_{q_1'(L)\to\hat{q}\to\tilde{q}}$, $\hat{q} \to \tilde{q}$ is of length 1, each of $q_1'(L) \to \hat{q}$ and $q_1'(R) \to \bar{q}$ has a cycle with positive weight, and starting from $\bar{q}$ there is an infinite run with weight $+\infty$,

*Example 3:* Reconsider the LRTA $\mathcal{A}_1$ in Fig. 1 and its self-composition $\mathrm{CC}(\mathcal{A}_1)$ in Fig. 2. In $\mathrm{CC_A}(\mathcal{A}_1)$, there is no time-unbounded transition, so neither (A) nor (C) in Theorem 3.5 holds. The path $(q_0, q_0) \xrightarrow{(e_1,e_2)/+} (q_3, q_4) \xrightarrow{(e_1,e_2)/+} (q_3, q_4) \xrightarrow{(e_1,e_2)/+} (q_3, q_4)$ is as in (10), so (B) in Theorem 3.5 holds, and we have $\mathcal{A}_1$ is not strongly time-detectable. Directly by Definition 3, for each $t \in \mathbb{R}_{\geq 0}$, we choose infinite run $q_0 \xrightarrow{u_1/1} q_1 \xrightarrow{e_1/2} q_3 \left(\xrightarrow{e_1/1} q_3\right)^{\omega} =: \pi$, and timed $\omega$-word $w_t = \tau(\pi) = (u, 1)(e_1, 3)(e_1, 4) \ldots \in L^{\omega}(\mathcal{A}_1)$ which is actually independent of $t$, $\ell(w_t) = (\sigma, 3)(\sigma, 4) \ldots$. Choose prefix $(u, 1)(e_1, 3)(e_1, 4) \ldots (e_1, n) =: w_t'$ of $\tau(\pi)$ such that $\mathrm{WT}_{w_t'} = n > t$, then $\mathcal{M}(\mathcal{A}_1, \ell((u, 1)(e_1, 3)(e_1, 4) \ldots (e_1, n))) = \mathcal{M}(\mathcal{A}_1, (\sigma, 3)(\sigma, 4) \ldots (\sigma, n)) = \{q_3, q_4\}$ which is not a singleton, we also have $\mathcal{A}_1$ is not strongly time-detectable.

### C. Complexity results on verifying strong label-detectability and strong time-detectability of LRTAs

In this subsection, we give complexity results on verifying the two strong versions of detectability of LRTAs.

*Theorem 3.6:* The verification problems for Definition 2 and Definition 3 both belong to coNP.

**Proof** Consider an LRTA $\mathcal{A}$. By Theorem 2.3, $\mathrm{CC}(\mathcal{A})$ can be computed in NP. After $\mathrm{CC}(\mathcal{A})$ has been computed, both condition (i) and condition (ii) of Theorem 3.1 can be verified in P. Hence the negation of Definition 2 can be verified in NP.

Now we consider Definition 3, we need to prove each of the six conditions in Theorem 3.5 can be verified in NP. By Proposition 3.2, whether (9) contains a time-unbounded transition can be checked in NP. By Proposition 3.3, whether starting from $q_1'(L)$ there is an infinite run with weight $+\infty$ can be checked in P. Hence condition (A) (of Theorem 3.5) can be checked in NP. Similarly, condition (B) can also be checked in NP. Additionally by Theorem 2.3 and the technique proposed in [10] to compute concurrent composition, condition (C), condition (D), and condition (F) can be checked in NP. Condition (E) can be checked in P. □

The reduction (illustrated in [10, Fig. 6]) constructed to prove the coNP-hardness of verifying diagnosability of LRTAs (shown in [10, Thm. 3.5]) implies the following result.

*Theorem 3.7:* The problems of verifying Definition 2 and Definition 3 are both coNP-hard.

## IV. Conclusion

In this paper, we formulated two versions of strong detectability for LRTAs called strong label-detectability and strong time-detectability. Based on the concurrent composition formulated and computed in [10], we gave necessary and sufficient conditions for the two versions and also proved that their verification problems are both coNP-complete. All results obtained in the current paper can be extended to a more general class of automata in which the intervals of transitions are intervals of real numbers whose endpoints are rational numbers, $-\infty$, or $+\infty$ by extending the definition of concurrent composition from LRTAs to this more general class of automata. We believe that the use of the concurrent-composition operator will enable the extension to extent to LRTAs of many other decidable results obtained in the past 3 decades for discrete-event systems modeled by LFSAs.

## References


[1] K. Zhang and A. Giua. On detectability of labeled Petri nets and finite automata. *Discrete Event Dynamic Systems*, 30(3):465–497, 2020.

[2] K. Zhang. A unified concurrent-composition method to state/event inference and concealment in labeled finite-state automata as discrete-event systems. *Annual Reviews in Control*, 56:100902(1–21), 2023.

[3] S. Shu and F. Lin. Generalized detectability for discrete event systems. *Systems & Control Letters*, 60(5):310–317, 2011.

[4] S. Jiang, Z. Huang, V. Chandra, and R. Kumar. A polynomial algorithm for testing diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 46(8):1318–1321, Aug 2001.

[5] T.-S. Yoo and S. Lafortune. Polynomial-time verification of diagnosability of partially observed discrete-event systems. *IEEE Transactions on Automatic Control*, 47(9):1491–1495, Sep. 2002.

[6] S. Genc and S. Lafortune. Predictability of event occurrences in partially-observed discrete-event systems. *Automatica*, 45(2):301–311, 2009.

[7] K. Zhang. Detectability of labeled weighted automata over monoids. *Discrete Event Dynamic Systems*, 32(3):435–494, 2022.

[8] K. Zhang. A new framework for discrete-event systems. *Foundations and Trends® in Systems and Control*, 10(1-2):1–179, 2023.

[9] S. Miao, A. Lai, X. Yu, S. Lahaye, and J. Komenda. Verification of detectability for unambiguous weighted automata using self-composition. In *2023 9th International Conference on Control, Decision and Information Technologies (CoDIT)*, pages 251–256, 2023.

[10] Y. Yan and K. Zhang. Formulation of concurrent composition in labeled real-time automata with an application to fault diagnosis. In *2024 UKACC 14th International Conference on Control (CONTROL)*, pages 281–286, 2024.

[11] W. Dong, X. Yin, K. Zhang, and S. Li. On the verification of detectability for timed systems. In *2022 American Control Conference (ACC)*, pages 3752–3758, 2022.

[12] R. Alur and D. L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.

[13] S. Tripakis. Fault diagnosis for timed automata. In Werner Damm and Ernst Rüdiger Olderog, editors, *Formal Techniques in Real-Time and Fault-Tolerant Systems*, pages 205–221, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[14] K. Zhang. State-based opacity of labeled real-time automata. *Theoretical Computer Science*, 987:114373(1–20), 2024.

[15] K. Zhang. State-based opacity of real-time automata. In *27th International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA 2021)*, volume 90, pages 12:1–12:15, 2021.

[16] J. Li, D. Lefebvre, C.N. Hadjicostis, and Z. Li. Verification of state-based timed opacity for constant-time labeled automata. *IEEE Transactions on Automatic Control*, page online, 2024.

[17] J. Li, D. Lefebvre, C.N. Hadjicostis, and Z. Li. State estimation for constant-time labeled automata under dense time. *Automatica*, 170:111874(1–12), 2024.