# State-based opacity of real-time automata

Kuize Zhang

Control Systems Group
Technical University of Berlin
10587 Berlin, Germany

13 July 2021

AUTOMATA 2021, Marseille, France

kuize.zhang@campus.tu-berlin.de

# Content

# Background

- Opacity is a confidentiality property (firstly proposed by (Mazaré, 2004)) used to characterize information flow security, and has been widely used to describe all kinds of scenarios in security/privacy problems.

# Background

- Opacity is a confidentiality property (firstly proposed by (Mazaré, 2004)) used to characterize information flow security, and has been widely used to describe all kinds of scenarios in security/privacy problems.
- It describes whether a labeled (aka partially-observed) system can forbid an external intruder from making sure whether some secrets have been visited,

# Background

- Opacity is a confidentiality property (firstly proposed by (Mazaré, 2004)) used to characterize information flow security, and has been widely used to describe all kinds of scenarios in security/privacy problems.
- It describes whether a labeled (aka partially-observed) system can forbid an external intruder from making sure whether some secrets have been visited, given that the intruder knows complete knowledge of the system's structure but can only see outputs generated by the system.

# A general framework for opacity

Run-based opacity (Bryans et al., 2008)

$$q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} q_n \qquad (\forall \text{ secret run})$$

$$q'_0 \xrightarrow{e'_1} q'_1 \xrightarrow{e'_2} \cdots \xrightarrow{e'_m} q'_m \qquad (\exists \text{ non-secret run})$$

$$\text{s.t. } \ell(e_1 \dots e_n) = \ell(e'_1 \dots e'_m) \qquad (\text{the same label seq.})$$

# Two special classes of opacity: I

## Language-based (aka trace-based) opacity

| | |
|---|---|
| $e_1 \dots e_n$ | (∀ secret trace) |
| $e'_1 \dots e'_m$ | (∃ non-secret trace) |
| s.t. $\ell(e_1 \dots e_n) = \ell(e'_1 \dots e'_m)$ | (the same label seq.) |

# Two special classes of opacity: I

## Language-based (aka trace-based) opacity

$e_1 \ldots e_n$ (∀ secret trace)

$e'_1 \ldots e'_m$ (∃ non-secret trace)

s.t. $\ell(e_1 \ldots e_n) = \ell(e'_1 \ldots e'_m)$ (the same label seq.)

## Verification results in untimed automata

# Two special classes of opacity: I

## Language-based (aka trace-based) opacity

$e_1 \dots e_n$ (∀ secret trace)

$e'_1 \dots e'_m$ (∃ non-secret trace)

s.t. $\ell(e_1 \dots e_n) = \ell(e'_1 \dots e'_m)$ (the same label seq.)

## Verification results in untimed automata

- undecidable in labeled finite automata (LFAs) with $\epsilon$-labeling functions (Bryans et al., 2008)

# Two special classes of opacity: I

## Language-based (aka trace-based) opacity

$e_1 \dots e_n$ (∀ secret trace)

$e'_1 \dots e'_m$ (∃ non-secret trace)

s.t. $\ell(e_1 \dots e_n) = \ell(e'_1 \dots e'_m)$ (the same label seq.)

## Verification results in untimed automata

- undecidable in labeled finite automata (LFAs) with $\epsilon$-labeling functions (Bryans et al., 2008)
- EXPTIME in LFAs when secret languages and non-secrete languages are regular (Lin, 2011)

# Two special classes of opacity: II

**State-based opacity (specified according to the time when secrets visited)**

$$q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_i} q_i \xrightarrow{e_{i+1}} \cdots \xrightarrow{e_n} q_n \qquad (\forall \text{ secret state})$$

$$q'_0 \xrightarrow{e'_1} q'_1 \xrightarrow{e'_2} \cdots \xrightarrow{e'_j} q'_j \xrightarrow{e'_{j+1}} \cdots \xrightarrow{e'_m} q'_m \qquad (\exists \text{ non-secret state})$$

$$\text{s.t. } \ell(e_1 \dots e_i) = \ell(e'_1 \dots e'_j) =: \gamma_1$$

$$\ell(e_{i+1} \dots e_n) = \ell(e'_{j+1} \dots e'_m) =: \gamma_2 \qquad \text{(the same label seq.)}$$

# Two special classes of opacity: II

## State-based opacity (specified according to the time when secrets visited)

$$q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_i} q_i \xrightarrow{e_{i+1}} \cdots \xrightarrow{e_n} q_n \qquad (\forall \text{ secret state})$$

$$q'_0 \xrightarrow{e'_1} q'_1 \xrightarrow{e'_2} \cdots \xrightarrow{e'_j} q'_j \xrightarrow{e'_{j+1}} \cdots \xrightarrow{e'_m} q'_m \qquad (\exists \text{ non-secret state})$$

$$\text{s.t. } \ell(e_1 \dots e_i) = \ell(e'_1 \dots e'_j) =: \gamma_1$$

$$\ell(e_{i+1} \dots e_n) = \ell(e'_{j+1} \dots e'_m) =: \gamma_2 \qquad (\text{the same label seq.})$$

## Verification results in untimed automata (plenty of)

Initial-state opacity (ISO) ($i = j = 0$), current-state opacity (CSO, $i = n, j = m$), infinite-step opacity (InfSO), and $K$-step opacity (KSO, $|\gamma_2| \leq K$) are PSPACE-complete in LFAs, and equivalent (Saboori and Hadjicostis, 2013) (Cassez, Dubreil, and Marchand, 2009) (Wu and Lafortune, 2013).

# Results in timed automata (rare)

## Language-based opacity

# Results in timed automata (rare)

## Language-based opacity

- decidable in (labeled) real-time automata when secret languages and non-secrete languages are those recognized by real-time automata (Wang, Zhan, and An, 2018)

# Results in timed automata (rare)

## Language-based opacity

- decidable in (labeled) real-time automata when secret languages and non-secrete languages are those recognized by real-time automata (Wang, Zhan, and An, 2018)

## State-based opacity

# Results in timed automata (rare)

## Language-based opacity

- decidable in (labeled) real-time automata when secret languages and non-secrete languages are those recognized by real-time automata (Wang, Zhan, and An, 2018)

## State-based opacity

- CSO is undecidable in time-deterministic event recording automata (Cassez, Dubreil, and Marchand, 2009).

# Results in timed automata (rare)

## Language-based opacity

- decidable in (labeled) real-time automata when secret languages and non-secrete languages are those recognized by real-time automata (Wang, Zhan, and An, 2018)

## State-based opacity

- CSO is undecidable in time-deterministic event recording automata (Cassez, Dubreil, and Marchand, 2009).
- ISO is decidable in real-time automata (Wang, Zhan, and An, 2018).

# Results in timed automata (rare)

## Language-based opacity

- decidable in (labeled) real-time automata when secret languages and non-secrete languages are those recognized by real-time automata (Wang, Zhan, and An, 2018)

## State-based opacity

- CSO is undecidable in time-deterministic event recording automata (Cassez, Dubreil, and Marchand, 2009).
- ISO is decidable in real-time automata (Wang, Zhan, and An, 2018).
- ISO, CSO, KSO, InfSO in real-time automata with complexity upper bounds on verification (Zhang, 2021)

# Content

A (labeled) real-time automaton (RTA) is a tuple

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

where

A (labeled) real-time automaton (RTA) is a tuple

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

where

- $Q$ is a finite set of states,

A (labeled) real-time automaton (RTA) is a tuple

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

where

- $Q$ is a finite set of states,
- $E$ is a finite set of events,

A (labeled) real-time automaton (RTA) is a tuple

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

where

- $Q$ is a finite set of states,
- $E$ is a finite set of events,
- $Q_0 \subset Q$ is a set of initial states,

A (labeled) real-time automaton (RTA) is a tuple

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

where

- $Q$ is a finite set of states,
- $E$ is a finite set of events,
- $Q_0 \subset Q$ is a set of initial states,
- $\Delta \subset Q \times E \times Q$ is the transition relation (elements of $\Delta$ are transitions),

A (labeled) real-time automaton (RTA) is a tuple

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

where

- $Q$ is a finite set of states,
- $E$ is a finite set of events,
- $Q_0 \subset Q$ is a set of initial states,
- $\Delta \subset Q \times E \times Q$ is the transition relation (elements of $\Delta$ are 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 $a \in \mathbb{Q}_{\geq 0}$ and $b \in \mathbb{Q}_{\geq 0} \cup \{+\infty\}$, respectively,

A (labeled) real-time automaton (RTA) is a tuple

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

where

- $Q$ is a finite set of states,
- $E$ is a finite set of events,
- $Q_0 \subset Q$ is a set of initial states,
- $\Delta \subset Q \times E \times Q$ is the transition relation (elements of $\Delta$ are 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 $a \in \mathbb{Q}_{\geq 0}$ and $b \in \mathbb{Q}_{\geq 0} \cup \{+\infty\}$, respectively,
- $\Sigma$ is a finite set of labels/outputs,

A (labeled) real-time automaton (RTA) is a tuple

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

where

- $Q$ is a finite set of states,
- $E$ is a finite set of events,
- $Q_0 \subset Q$ is a set of initial states,
- $\Delta \subset Q \times E \times Q$ is the transition relation (elements of $\Delta$ are 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 $a \in \mathbb{Q}_{\geq 0}$ and $b \in \mathbb{Q}_{\geq 0} \cup \{+\infty\}$, respectively,
- $\Sigma$ is a finite set of labels/outputs,
- $\ell : E \to \Sigma \cup \{\epsilon\}$ is the labeling function.

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$
- observable transition $(q, e, q') \in \Delta$ with $e \in E_o$

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$
- observable transition $(q, e, q') \in \Delta$ with $e \in E_o$
- unobservable transition $(q, e, q') \in \Delta$ with $e \in E_{uo}$

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$
- observable transition $(q, e, q') \in \Delta$ with $e \in E_o$
- unobservable transition $(q, e, q') \in \Delta$ with $e \in E_{uo}$
- $\ell$ extended to $E \times \mathbb{R}_{\geq 0}$: $\ell((e,t)) = \begin{cases} (\ell(e), t) & \text{if } e \in E_o, \\ \epsilon & \text{if } e \in E_{uo}. \end{cases}$

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$
- observable transition $(q, e, q') \in \Delta$ with $e \in E_o$
- unobservable transition $(q, e, q') \in \Delta$ with $e \in E_{uo}$
- $\ell$ extended to $E \times \mathbb{R}_{\geq 0}$: $\ell((e, t)) = \begin{cases} (\ell(e), t) & \text{if } e \in E_o, \\ \epsilon & \text{if } e \in E_{uo}. \end{cases}$
- $\ell$ recursively extended to $E^*$ and also to $(E \times \mathbb{R}_{\geq 0})^*$ analogously.

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$
- observable transition $(q, e, q') \in \Delta$ with $e \in E_o$
- unobservable transition $(q, e, q') \in \Delta$ with $e \in E_{uo}$
- $\ell$ extended to $E \times \mathbb{R}_{\geq 0}$: $\ell((e,t)) = \begin{cases} (\ell(e), t) & \text{if } e \in E_o, \\ \epsilon & \text{if } e \in E_{uo}. \end{cases}$
- $\ell$ recursively extended to $E^*$ and also to $(E \times \mathbb{R}_{\geq 0})^*$ analogously.
- A path is either $\epsilon$ or a sequence $q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} q_n$, where $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$ for all $i \in [\![1, n]\!]$.

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$
- observable transition $(q, e, q') \in \Delta$ with $e \in E_o$
- unobservable transition $(q, e, q') \in \Delta$ with $e \in E_{uo}$
- $\ell$ extended to $E \times \mathbb{R}_{\geq 0}$: $\ell((e,t)) = \begin{cases} (\ell(e), t) & \text{if } e \in E_o, \\ \epsilon & \text{if } e \in E_{uo}. \end{cases}$
- $\ell$ recursively extended to $E^*$ and also to $(E \times \mathbb{R}_{\geq 0})^*$ analogously.
- A path is either $\epsilon$ or a sequence $q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} q_n$, where $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$ for all $i \in [\![1, n]\!]$.
- A run is either $\epsilon$ or 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 $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$, $t_i \in \mu(e_i)_{q_{i-1}q_i}$ for all $i \in [\![1, n]\!]$.

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$
- observable transition $(q, e, q') \in \Delta$ with $e \in E_o$
- unobservable transition $(q, e, q') \in \Delta$ with $e \in E_{uo}$
- $\ell$ extended to $E \times \mathbb{R}_{\geq 0}$: $\ell((e,t)) = \begin{cases} (\ell(e), t) & \text{if } e \in E_o, \\ \epsilon & \text{if } e \in E_{uo}. \end{cases}$
- $\ell$ recursively extended to $E^*$ and also to $(E \times \mathbb{R}_{\geq 0})^*$ analogously.
- A path is either $\epsilon$ or a sequence $q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} q_n$, where $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$ for all $i \in [\![1, n]\!]$.
- A run is either $\epsilon$ or 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 $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$, $t_i \in \mu(e_i)_{q_{i-1}q_i}$ for all $i \in [\![1, n]\!]$.
- The timed word of $\pi$ 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 $i \in [\![1, n]\!]$.

- observable event set $E_o = \{e \in E | \ell(e) \in \Sigma\}$
- unobservable event set $E_{uo} = \{e \in E | \ell(e) = \epsilon\}$
- observable transition $(q, e, q') \in \Delta$ with $e \in E_o$
- unobservable transition $(q, e, q') \in \Delta$ with $e \in E_{uo}$
- $\ell$ extended to $E \times \mathbb{R}_{\geq 0}$: $\ell((e,t)) = \begin{cases} (\ell(e), t) & \text{if } e \in E_o, \\ \epsilon & \text{if } e \in E_{uo}. \end{cases}$
- $\ell$ recursively extended to $E^*$ and also to $(E \times \mathbb{R}_{\geq 0})^*$ analogously.
- A path is either $\epsilon$ or a sequence $q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} q_n$, where $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$ for all $i \in [\![1, n]\!]$.
- A run is either $\epsilon$ or 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 $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$, $t_i \in \mu(e_i)_{q_{i-1}q_i}$ for all $i \in [\![1, n]\!]$.
- The timed word of $\pi$ 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 weight $\mathrm{WT}_\pi$ of $\pi$ is defined by $t'_n$.

## Example 1

Consider the RTA $\mathcal{A}_1$:

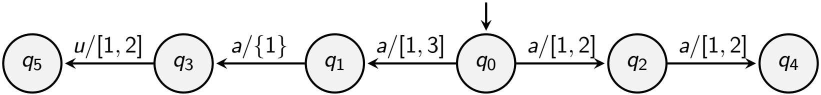



Figure 1: An RTA $\mathcal{A}_1$, $q_0$ is the initial state, $a$ is an observable event, $\ell(a) = a$, $u$ is unobservable, $\ell(u) = \epsilon$.

## Example 1

Consider the RTA $\mathcal{A}_1$:

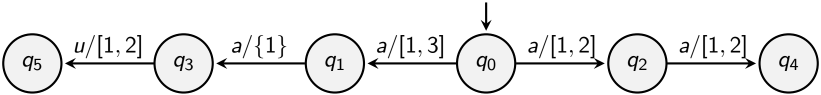



Figure 1: An RTA $\mathcal{A}_1$, $q_0$ is the initial state, $a$ is an observable event, $\ell(a) = a$, $u$ is unobservable, $\ell(u) = \epsilon$.

$$q_0 \xrightarrow{a} q_1 \xrightarrow{a} q_3 \xrightarrow{u} q_5, \qquad \text{(path)}$$

## Example 1

Consider the RTA $\mathcal{A}_1$:

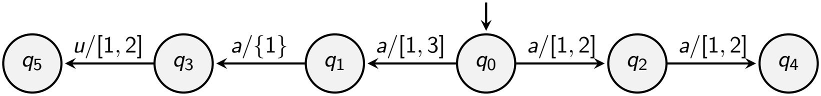



Figure 1: An RTA $\mathcal{A}_1$, $q_0$ is the initial state, $a$ is an observable event, $\ell(a) = a$, $u$ is unobservable, $\ell(u) = \epsilon$.

$$q_0 \xrightarrow{a} q_1 \xrightarrow{a} q_3 \xrightarrow{u} q_5, \qquad \text{(path)}$$

$$\pi = q_0 \xrightarrow{a/2} q_1 \xrightarrow{a/1} q_3 \xrightarrow{u/1} q_5, \qquad \text{(run)}$$

## Example 1

Consider the RTA $\mathcal{A}_1$:

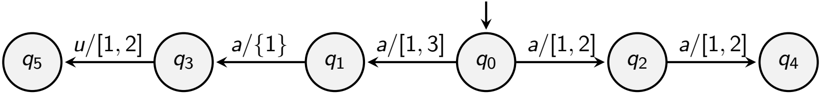



Figure 1: An RTA $\mathcal{A}_1$, $q_0$ is the initial state, $a$ is an observable event, $\ell(a) = a$, $u$ is unobservable, $\ell(u) = \epsilon$.

$$q_0 \xrightarrow{a} q_1 \xrightarrow{a} q_3 \xrightarrow{u} q_5, \qquad \text{(path)}$$

$$\pi = q_0 \xrightarrow{a/2} q_1 \xrightarrow{a/1} q_3 \xrightarrow{u/1} q_5, \qquad \text{(run)}$$

$$\tau(\pi) = (a,2)(a,3)(u,4), \qquad \text{(timed word)}$$

## Example 1

Consider the RTA $\mathcal{A}_1$:

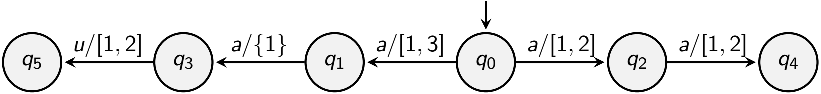



Figure 1: An RTA $\mathcal{A}_1$, $q_0$ is the initial state, $a$ is an observable event, $\ell(a) = a$, $u$ is unobservable, $\ell(u) = \epsilon$.

$$q_0 \xrightarrow{a} q_1 \xrightarrow{a} q_3 \xrightarrow{u} q_5, \qquad \text{(path)}$$

$$\pi = q_0 \xrightarrow{a/2} q_1 \xrightarrow{a/1} q_3 \xrightarrow{u/1} q_5, \qquad \text{(run)}$$

$$\tau(\pi) = (a,2)(a,3)(u,4), \qquad \text{(timed word)}$$

$$\mathrm{WT}_\pi = 4, \qquad \text{(weight)}$$

## Example 1

Consider the RTA $\mathcal{A}_1$:

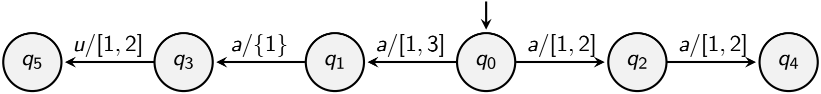


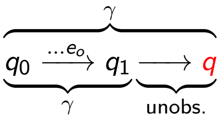

Figure 1: An RTA $\mathcal{A}_1$, $q_0$ is the initial state, $a$ is an observable event, $\ell(a) = a$, $u$ is unobservable, $\ell(u) = \epsilon$.

$$
\begin{aligned}
q_0 \xrightarrow{a} q_1 \xrightarrow{a} q_3 \xrightarrow{u} q_5, &\qquad \text{(path)}\\
\pi = q_0 \xrightarrow{a/2} q_1 \xrightarrow{a/1} q_3 \xrightarrow{u/1} q_5, &\qquad \text{(run)}\\
\tau(\pi) = (a,2)(a,3)(u,4), &\qquad \text{(timed word)}\\
\mathrm{WT}_\pi = 4, &\qquad \text{(weight)}\\
\ell(\tau(\pi)) = (a,2)(a,3). &\qquad \text{(timed label seq.)}
\end{aligned}
$$

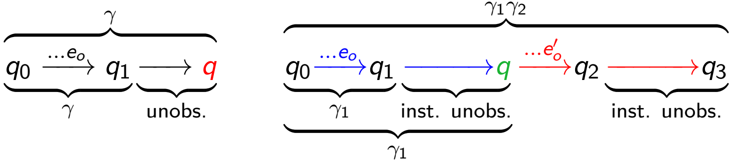
- A run $\pi$ is called instantaneous if $\mathrm{WT}_\pi = 0$, called noninstantaneous if $\mathrm{WT}_\pi > 0$.

- A run $\pi$ is called instantaneous if $\mathsf{WT}_\pi = 0$, called noninstantaneous if $\mathsf{WT}_\pi > 0$.
- A run $\pi$ is called unobservable if $\ell(e_1 \dots e_n) = \epsilon$, called observable if $\ell(e_1 \dots e_n) \in \Sigma^+$.

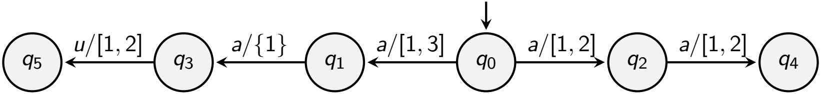
- A run $\pi$ is called instantaneous if $\mathrm{WT}_\pi = 0$, called noninstantaneous if $\mathrm{WT}_\pi > 0$.
- A run $\pi$ is called unobservable if $\ell(e_1 \dots e_n) = \epsilon$, called observable if $\ell(e_1 \dots e_n) \in \Sigma^+$.
- Given $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^*$, $[\gamma]$ denotes the set of runs $\pi$ of $\mathcal{A}$ starting from initial states such that $\ell(\tau(\pi)) = \gamma$. last($[\gamma]$)



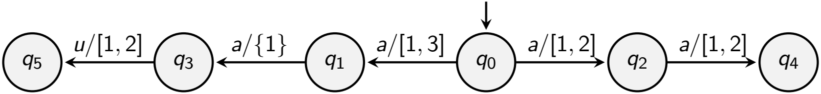
- A run $\pi$ is called instantaneous if $\mathrm{WT}_\pi = 0$, called noninstantaneous if $\mathrm{WT}_\pi > 0$.
- A run $\pi$ is called unobservable if $\ell(e_1 \dots e_n) = \epsilon$, called observable if $\ell(e_1 \dots e_n) \in \Sigma^+$.
- Given $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^*$, $[\gamma]$ denotes the set of runs $\pi$ of $\mathcal{A}$ starting from initial states such that $\ell(\tau(\pi)) = \gamma$. $\mathrm{last}([\gamma])$
- $\mathrm{interm}(\gamma_1, \gamma_2) = \{q \in Q | (\exists \text{ runs } \pi_1, \pi_2)[(\mathrm{init}(\pi_1) \in Q_0) \wedge (\mathrm{last}(\pi_1) = \mathrm{init}(\pi_2) = q) \wedge (\ell(\tau(\pi_1)) = \gamma_1) \wedge (\ell(\tau(\pi_1\pi_2)) = \gamma_1\gamma_2) \wedge (\mathrm{WT}_{\pi_1} = \mathrm{last}_R(\gamma_1)) \wedge (\mathrm{WT}_{\pi_2} = \mathrm{last}_R(\gamma_2) - \mathrm{last}_R(\gamma_1))]\}$: the set of states $\mathcal{A}$ can be in when $\mathcal{A}$ has just generated timed label seq. $\gamma_1$, given that the current timed label seq. is $\gamma_1\gamma_2 \in (\Sigma \times \mathbb{R}_{\geq 0})^*$.



## Example 2 (cont. $\mathcal{A}_1$)

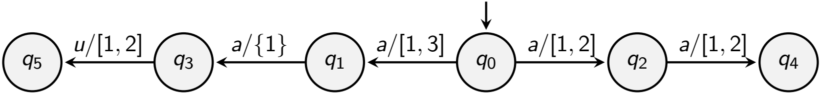


## Example 2 (cont. $\mathcal{A}_1$)



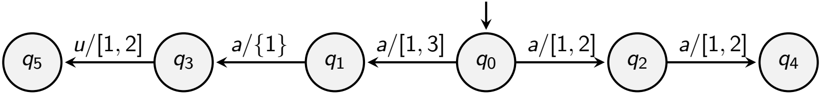

$$\text{last}([(a,2)]) = \{q_1, q_2\},$$

## Example 2 (cont. $\mathcal{A}_1$)




$$\text{last}([(a,2)]) = \{q_1, q_2\},$$
$$\text{last}([(a,2)(a,3)]) = \{q_3, q_4, q_5\},$$

### Example 2 (cont. $\mathcal{A}_1$)




$$\text{last}([(a,2)]) = \{q_1, q_2\},$$
$$\text{last}([(a,2)(a,3)]) = \{q_3, q_4, q_5\},$$
$$\text{interm}(\mathcal{A}_1, (a,2), (a,3)) = \{q_1, q_2\}.$$

# Current-state estimate

For $\mathcal{A}$, $x \subset Q$, and $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^*$, the current-state estimate is

$$\mathcal{M}(\mathcal{A}, \gamma|x) := \{q \in Q | (\exists q_0 \in x)(\exists n \in \mathbb{N})(\exists m \in \mathbb{N}) \left(\exists \text{ a run } \pi = q_0 \xrightarrow{e_1/t_1} \cdots \xrightarrow{e_n/t_n} q_n \xrightarrow{e_{n+1}/0} \cdots \xrightarrow{e_{n+m}/0} q\right) [(e_n \in E_o) \wedge (e_{n+1} \ldots e_{n+m} \in (E_{uo})^*) \wedge \ell(\tau(\pi)) = \gamma]\}.$$

# Current-state estimate

For $\mathcal{A}$, $x \subset Q$, and $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^*$, the current-state estimate is

$$\mathcal{M}(\mathcal{A}, \gamma | x) := \{q \in Q | (\exists q_0 \in x)(\exists n \in \mathbb{N})(\exists m \in \mathbb{N}) \left(\exists \text{ a run } \pi = q_0 \xrightarrow{e_1/t_1} \cdots \xrightarrow{e_n/t_n} q_n \xrightarrow{e_{n+1}/0} \cdots \xrightarrow{e_{n+m}/0} q\right) [(e_n \in E_o) \wedge (e_{n+1} \dots e_{n+m} \in (E_{uo})^*) \wedge \ell(\tau(\pi)) = \gamma]\}.$$

$\mathcal{M}(\mathcal{A}, \gamma)$ denotes the set of states $\mathcal{A}$ can be in when $\gamma$ has been generated.

# Current-state estimate

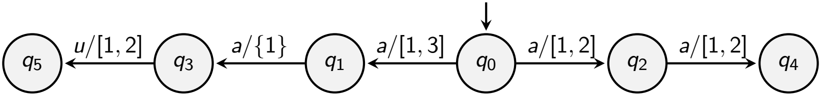
For $\mathcal{A}$, $x \subset Q$, and $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^*$, the current-state estimate is

$$\mathcal{M}(\mathcal{A}, \gamma | x) := \{q \in Q | (\exists q_0 \in x)(\exists n \in \mathbb{N})(\exists m \in \mathbb{N}) \left(\exists \text{ a run } \pi = q_0 \xrightarrow{e_1/t_1} \cdots \xrightarrow{e_n/t_n} q_n \xrightarrow{e_{n+1}/0} \cdots \xrightarrow{e_{n+m}/0} q\right) [(e_n \in E_o) \wedge (e_{n+1} \dots e_{n+m} \in (E_{uo})^*) \wedge \ell(\tau(\pi)) = \gamma]\}.$$

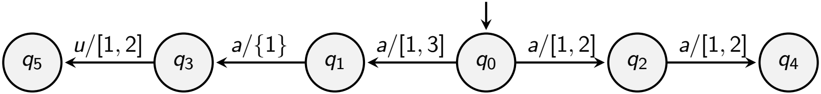
$\mathcal{M}(\mathcal{A}, \gamma)$ denotes the set of states $\mathcal{A}$ can be in when $\gamma$ has been generated.

$\mathcal{M}(\mathcal{A}, \gamma | Q_0) =: \mathcal{M}(\mathcal{A}, \gamma) \subset \text{last}([\gamma])$ for $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^*$.

## Example 3 (cont. $\mathcal{A}_1$)

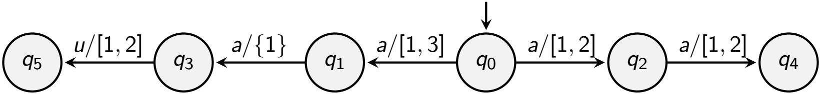


## Example 3 (cont. $\mathcal{A}_1$)



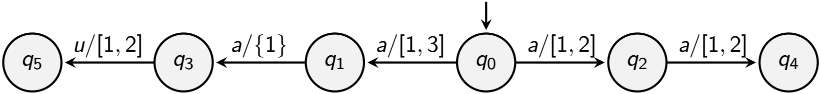

$$\text{last}([(a,2)]) = \{q_1, q_2\},$$

## Example 3 (cont. $\mathcal{A}_1$)



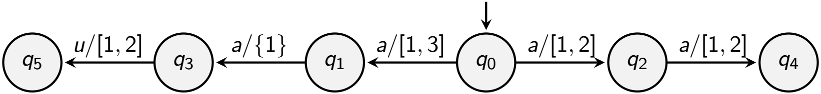

$$\text{last}([(a,2)]) = \{q_1, q_2\},$$
$$\mathcal{M}(\mathcal{A}_1, (a,2)) = \{q_1, q_2\},$$

## Example 3 (cont. $\mathcal{A}_1$)



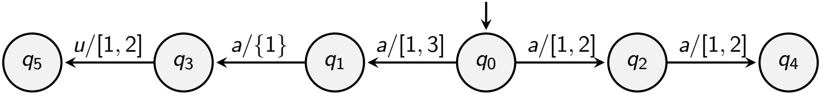

$$\mathrm{last}([(a,2)]) = \{q_1, q_2\},$$
$$\mathcal{M}(\mathcal{A}_1, (a,2)) = \{q_1, q_2\},$$
$$\mathrm{last}([(a,2)(a,3)]) = \{q_3, q_4, q_5\},$$

## Example 3 (cont. $\mathcal{A}_1$)




$$\begin{aligned} \mathrm{last}([(a,2)]) &= \{q_1, q_2\}, \\ \mathcal{M}(\mathcal{A}_1, (a,2)) &= \{q_1, q_2\}, \\ \mathrm{last}([(a,2)(a,3)]) &= \{q_3, q_4, q_5\}, \\ \mathcal{M}(\mathcal{A}_1, (a,2)(a,3)) &= \{q_3, q_4\}, \end{aligned}$$

## Example 3 (cont. $\mathcal{A}_1$)




$$\begin{aligned}
\text{last}([(a,2)]) &= \{q_1, q_2\},\\
\mathcal{M}(\mathcal{A}_1, (a,2)) &= \{q_1, q_2\},\\
\text{last}([(a,2)(a,3)]) &= \{q_3, q_4, q_5\},\\
\mathcal{M}(\mathcal{A}_1, (a,2)(a,3)) &= \{q_3, q_4\},\\
\mathcal{M}(\mathcal{A}_1, (a,2)(a,3)) &\subsetneq \text{last}([(a,2)(a,3)]).
\end{aligned}$$

# Content

Language generated by RTA $\mathcal{A}$: $\mathcal{L}(\mathcal{A}) = \{\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^* | \mathcal{M}(\mathcal{A}, \gamma) \neq \emptyset\}$

Language generated by RTA $\mathcal{A}$: $\mathcal{L}(\mathcal{A}) = \{\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^* | \mathcal{M}(\mathcal{A}, \gamma) \neq \emptyset\}$

Specify a subset $Q_S \subset Q$ of secret states.

Language generated by RTA $\mathcal{A}$: $\mathcal{L}(\mathcal{A}) = \{\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^* | \mathcal{M}(\mathcal{A}, \gamma) \neq \emptyset\}$

Specify a subset $Q_S \subset Q$ of secret states.

**Definition 4 (ISO)**

An RTA $\mathcal{A}$ is called initial-state opaque (ISO) w.r.t. $Q_S$ if for every $\gamma \in \mathcal{L}(\mathcal{A})$, $\text{init}([\gamma]) \not\subset Q_S$.

Language generated by RTA $\mathcal{A}$: $\mathcal{L}(\mathcal{A}) = \{\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^* | \mathcal{M}(\mathcal{A}, \gamma) \neq \emptyset\}$

Specify a subset $Q_S \subset Q$ of secret states.

**Definition 4 (ISO)**

An RTA $\mathcal{A}$ is called initial-state opaque (ISO) w.r.t. $Q_S$ if for every $\gamma \in \mathcal{L}(\mathcal{A})$, $\text{init}([\gamma]) \not\subset Q_S$.

ISO means that when observing a timed label sequence $\gamma \in \mathcal{L}(\mathcal{A})$, not all possible initial states are secret, so that one cannot make sure whether the initial state is secret.

Language generated by RTA $\mathcal{A}$: $\mathcal{L}(\mathcal{A}) = \{\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^* | \mathcal{M}(\mathcal{A}, \gamma) \neq \emptyset\}$

Specify a subset $Q_S \subset Q$ of secret states.

**Definition 4 (ISO)**

An RTA $\mathcal{A}$ is called initial-state opaque (ISO) w.r.t. $Q_S$ if for every $\gamma \in \mathcal{L}(\mathcal{A})$, $\text{init}([\gamma]) \not\subset Q_S$.

ISO means that when observing a timed label sequence $\gamma \in \mathcal{L}(\mathcal{A})$, not all possible initial states are secret, so that one cannot make sure whether the initial state is secret.

**Definition 5 (CSO)**

An RTA $\mathcal{A}$ is called current-state opaque (CSO) w.r.t. $Q_S$ if for every $\gamma \in \mathcal{L}(\mathcal{A})$, in $\mathcal{M}(\mathcal{A}, \gamma)$ there exists at least one non-eventually-secret state.

### Definition 6

A state $q$ of an RTA $\mathcal{A}$ is called eventually secret if either (1) $q$ is secret or (2) there is an unobservable path starting from $q$ and along each of such paths at least one secret state will be visited.

## Definition 6

A state $q$ of an RTA $\mathcal{A}$ is called eventually secret if either (1) $q$ is secret or (2) there is an unobservable path starting from $q$ and along each of such paths at least one secret state will be visited.

## Proposition 1

*A state $q$ is not eventually secret iff (1) $q \notin Q_S$ and (2) either there is no unobservable path from $q$ or there is an unobservable path from $q$ without any secret state that either ends at a dead state or contains a cycle.*

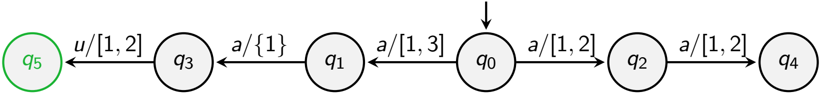
## Definition 6

A state $q$ of an RTA $\mathcal{A}$ is called eventually secret if either (1) $q$ is secret or (2) there is an unobservable path starting from $q$ and along each of such paths at least one secret state will be visited.

## Proposition 1

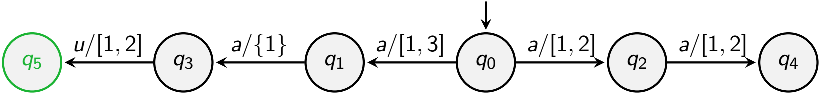
*A state $q$ is not eventually secret iff (1) $q \notin Q_S$ and (2) either there is no unobservable path from $q$ or there is an unobservable path from $q$ without any secret state that either ends at a dead state or contains a cycle.*

## Example 7 (cont. $\mathcal{A}_1$)



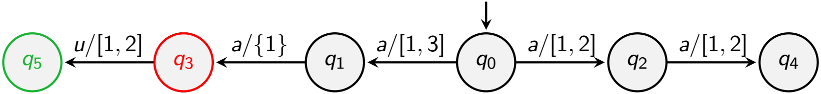

Let $Q_S = \{q_5\}$. Then $q_3$ is eventually secret because of the unique unobservable path $q_3 \xrightarrow{u} q_5$ (with $q_5$ dead, i.e., no transition starts at $q_5$).

Example 8 (cont. $\mathcal{A}_1$)



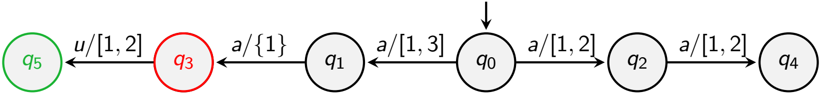

Let $Q_S = \{q_5\}$.

Example 8 (cont. $\mathcal{A}_1$)



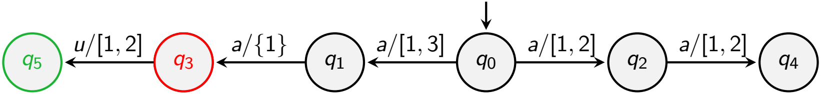

Let $Q_S = \{q_5\}$. In Example 7, we have shown $q_3$ is eventually secret.

Example 8 (cont. $\mathcal{A}_1$)




Let $Q_S = \{q_5\}$. In Example 7, we have shown $q_3$ is eventually secret. In addition, none of $q_1, q_0, q_2, q_4$ is eventually secret.

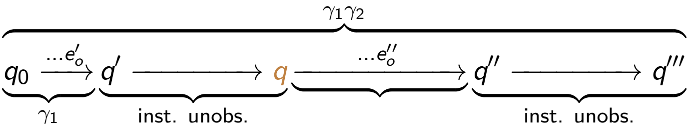
Example 8 (cont. $\mathcal{A}_1$)




Let $Q_S = \{q_5\}$. In Example 7, we have shown $q_3$ is eventually secret. In addition, none of $q_1, q_0, q_2, q_4$ is eventually secret. Hence $\mathcal{A}_1$ is not CSO w.r.t. $\{q_5\}$.

## Definition 9 (InfSO and KSO)

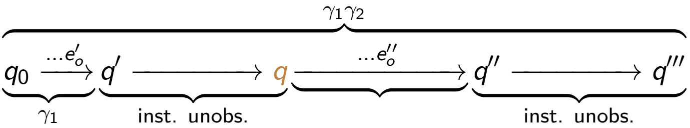
An RTA $\mathcal{A}$ is called infinite-step opaque (InfSO) w.r.t. $Q_S$ if for all $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{A})$ such that $1 \leq |\gamma_2|$, interm$(\gamma_1, \gamma_2)$ contains at least one non-secret state $q$.




(*)

## Definition 9 (InfSO and KSO)

An RTA $\mathcal{A}$ is called infinite-step opaque (InfSO) w.r.t. $Q_S$ if for all $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{A})$ such that $1 \le |\gamma_2|$, interm$(\gamma_1, \gamma_2)$ contains at least one non-secret state $q$.




(*)

When observing $\gamma_1\gamma_2$ with $1 \le |\gamma_2|$, one cannot make sure whether the state when $\gamma_1$ has just been generated is secret.

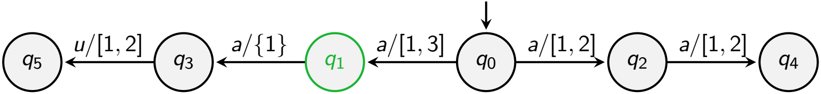
## Definition 9 (InfSO and KSO)

An RTA $\mathcal{A}$ is called infinite-step opaque (InfSO) ($K$-step opaque (KSO)) w.r.t. $Q_S$ if for all $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{A})$ such that $1 \le |\gamma_2| (\le K)$, $\mathrm{interm}(\gamma_1, \gamma_2)$ contains at least one non-secret state $q$.

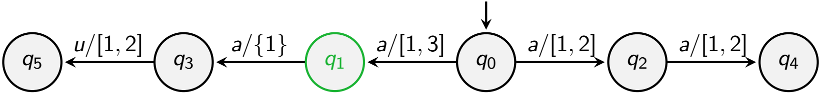
$$\overbrace{\underbrace{q_0 \xrightarrow{\dots e_o'}}_{\gamma_1} \underbrace{q' \longrightarrow q}_{\text{inst. unobs.}} \underbrace{\xrightarrow{\dots e_o''}}_{(\le K \text{ obs. events})} \underbrace{q'' \longrightarrow q'''}_{\text{inst. unobs.}}}^{\gamma_1\gamma_2} \qquad (*)$$

When observing $\gamma_1\gamma_2$ with $1 \le |\gamma_2| (\le K)$, one cannot make sure whether the state when $\gamma_1$ has just been generated is secret.

## Example 10 (cont. $\mathcal{A}_1$)



## Example 10 (cont. $\mathcal{A}_1$)




For $(a,3)(a,4)$, we only have

$$\overbrace{\underbrace{q_0 \xrightarrow{a/3}}_{\gamma_1=(a,3)} \underbrace{q_1 \xrightarrow{\quad\epsilon\quad} q_1}_{\text{unobs. secret}}}^{\gamma_1\gamma_2=(a,3)(a,4)} \xrightarrow{a/1} q_3 \implies \text{interm}(\mathcal{A}_1,(a,3),(a,4)) = \{q_1\}$$

which violates InfSO, i.e., $\mathcal{A}_1$ is not InfSO w.r.t. $\{q_1\}$.

## Definition 11

For an RTA $\mathcal{A}$, we define its pre-observer as a deterministic automaton

$$\mathcal{A}_{\text{obs}}^{\text{pre}} = (X, \Sigma \times \mathbb{R}_{\geq 0}, x_0, \delta_{\text{obs}}^{\text{pre}}), \tag{1}$$

where $X \subset 2^Q \setminus \{\emptyset\}$ is the state set, $\Sigma \times \mathbb{R}_{\geq 0}$ the (infinite) alphabet, $x_0 = \mathcal{M}(\mathcal{A}, \epsilon) \in X$ the unique initial state, $\delta_{\text{obs}}^{\text{pre}} \subset X \times (\Sigma \times \mathbb{R}_{\geq 0}) \times X$ the transition relation: for all $x, x' \in X$ and $(\sigma, t) \in \Sigma \times \mathbb{R}_{\geq 0}$, $(x, (\sigma, t), x') \in \delta_{\text{obs}}^{\text{pre}}$ iff $x' = \mathcal{M}(\mathcal{A}, (\sigma, t)|x)$. For all $x \subset Q$ different from $x_0$, $x \in X$ iff there is $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^+$ such that $x = \mathcal{M}(\mathcal{A}, \gamma)$.

### Definition 11

For an RTA $\mathcal{A}$, we define its pre-observer as a deterministic automaton

$$\mathcal{A}_{\text{obs}}^{\text{pre}} = (X, \Sigma \times \mathbb{R}_{\geq 0}, x_0, \delta_{\text{obs}}^{\text{pre}}), \tag{1}$$

where $X \subset 2^Q \setminus \{\emptyset\}$ is the state set, $\Sigma \times \mathbb{R}_{\geq 0}$ the (infinite) alphabet, $x_0 = \mathcal{M}(\mathcal{A}, \epsilon) \in X$ the unique initial state, $\delta_{\text{obs}}^{\text{pre}} \subset X \times (\Sigma \times \mathbb{R}_{\geq 0}) \times X$ the transition relation: for all $x, x' \in X$ and $(\sigma, t) \in \Sigma \times \mathbb{R}_{\geq 0}$, $(x, (\sigma, t), x') \in \delta_{\text{obs}}^{\text{pre}}$ iff $x' = \mathcal{M}(\mathcal{A}, (\sigma, t)|x)$. For all $x \subset Q$ different from $x_0$, $x \in X$ iff there is $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^+$ such that $x = \mathcal{M}(\mathcal{A}, \gamma)$.

## Definition 11

For an RTA $\mathcal{A}$, we define its pre-observer as a deterministic automaton

$$\mathcal{A}_{\text{obs}}^{\text{pre}} = (X, \Sigma \times \mathbb{R}_{\geq 0}, x_0, \delta_{\text{obs}}^{\text{pre}}), \tag{1}$$

where $X \subset 2^Q \setminus \{\emptyset\}$ is the state set, $\Sigma \times \mathbb{R}_{\geq 0}$ the (infinite) alphabet, $x_0 = \mathcal{M}(\mathcal{A}, \epsilon) \in X$ the unique initial state, $\delta_{\text{obs}}^{\text{pre}} \subset X \times (\Sigma \times \mathbb{R}_{\geq 0}) \times X$ the transition relation: for all $x, x' \in X$ and $(\sigma, t) \in \Sigma \times \mathbb{R}_{\geq 0}$, $(x, (\sigma, t), x') \in \delta_{\text{obs}}^{\text{pre}}$ iff $x' = \mathcal{M}(\mathcal{A}, (\sigma, t)|x)$. For all $x \subset Q$ different from $x_0$, $x \in X$ iff there is $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^+$ such that $x = \mathcal{M}(\mathcal{A}, \gamma)$.

- After $\delta_{\text{obs}}^{\text{pre}}$ is recursively extended to $\delta_{\text{obs}}^{\text{pre}} \subset X \times (\Sigma \times \mathbb{R}_{\geq 0})^* \times X$, one has for all $x \in X$ and $(\sigma_1, t_1) \ldots (\sigma_n, t_n) =: \gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^+$, $(x_0, \gamma, x) \in \delta_{\text{obs}}^{\text{pre}}$ iff $\mathcal{M}(\mathcal{A}, \tau(\gamma)) = x$, where $\tau(\gamma) = (\sigma_1, t_1)(\sigma_1, t_1 + t_2) \ldots (\sigma_n, t_1 + \cdots + t_n)$.

## Definition 11

For an RTA $\mathcal{A}$, we define its pre-observer as a deterministic automaton

$$\mathcal{A}_{\text{obs}}^{\text{pre}} = (X, \Sigma \times \mathbb{R}_{\geq 0}, x_0, \delta_{\text{obs}}^{\text{pre}}), \tag{1}$$

where $X \subset 2^Q \setminus \{\emptyset\}$ is the state set, $\Sigma \times \mathbb{R}_{\geq 0}$ the (infinite) alphabet, $x_0 = \mathcal{M}(\mathcal{A}, \epsilon) \in X$ the unique initial state, $\delta_{\text{obs}}^{\text{pre}} \subset X \times (\Sigma \times \mathbb{R}_{\geq 0}) \times X$ the transition relation: for all $x, x' \in X$ and $(\sigma, t) \in \Sigma \times \mathbb{R}_{\geq 0}$, $(x, (\sigma, t), x') \in \delta_{\text{obs}}^{\text{pre}}$ iff $x' = \mathcal{M}(\mathcal{A}, (\sigma, t)|x)$. For all $x \subset Q$ different from $x_0$, $x \in X$ iff there is $\gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^+$ such that $x = \mathcal{M}(\mathcal{A}, \gamma)$.

- After $\delta_{\text{obs}}^{\text{pre}}$ is recursively extended to $\delta_{\text{obs}}^{\text{pre}} \subset X \times (\Sigma \times \mathbb{R}_{\geq 0})^* \times X$, one has for all $x \in X$ and $(\sigma_1, t_1) \dots (\sigma_n, t_n) =: \gamma \in (\Sigma \times \mathbb{R}_{\geq 0})^+$, $(x_0, \gamma, x) \in \delta_{\text{obs}}^{\text{pre}}$ iff $\mathcal{M}(\mathcal{A}, \tau(\gamma)) = x$, where $\tau(\gamma) = (\sigma_1, t_1)(\sigma_1, t_1 + t_2) \dots (\sigma_n, t_1 + \dots + t_n)$.
- Alphabet $\Sigma \times \mathbb{R}_{\geq 0}$ is not finite, one cannot compute the whole $\mathcal{A}_{\text{obs}}^{\text{pre}}$. Next, we define observer $\mathcal{A}_{\text{obs}}$ as a finite sub-automaton of $\mathcal{A}_{\text{obs}}^{\text{pre}}$.

## Definition 12

For an RTA $\mathcal{A}$, consider its pre-observer $\mathcal{A}_{\text{obs}}^{\text{pre}} = (X, \Sigma \times \mathbb{R}_{\geq 0}, x_0, \delta_{\text{obs}}^{\text{pre}})$, we define its observer as a finite automaton

$$\mathcal{A}_{\text{obs}} = (X, \Sigma_{\text{obs}}, x_0, \delta_{\text{obs}}), \tag{2}$$

where $\Sigma_{\text{obs}}$ (resp., $\delta_{\text{obs}}$) is a finite subset of $\Sigma \times \mathbb{Q}_{\geq 0}$ (resp., $\delta_{\text{obs}}^{\text{pre}}$), such that if there exists a transition from $x \in X$ to $x' \in X$ in $\delta_{\text{obs}}^{\text{pre}}$ then at least one such transition belongs to $\delta_{\text{obs}}$.

## Definition 12

For an RTA $\mathcal{A}$, consider its pre-observer $\mathcal{A}_{\text{obs}}^{\text{pre}} = (X, \Sigma \times \mathbb{R}_{\geq 0}, x_0, \delta_{\text{obs}}^{\text{pre}})$, we define its observer as a finite automaton

$$\mathcal{A}_{\text{obs}} = (X, \Sigma_{\text{obs}}, x_0, \delta_{\text{obs}}), \quad (2)$$

where $\Sigma_{\text{obs}}$ (resp., $\delta_{\text{obs}}$) is a finite subset of $\Sigma \times \mathbb{Q}_{\geq 0}$ (resp., $\delta_{\text{obs}}^{\text{pre}}$), such that if there exists a transition from $x \in X$ to $x' \in X$ in $\delta_{\text{obs}}^{\text{pre}}$ then at least one such transition belongs to $\delta_{\text{obs}}$.

## Remark 1

## Definition 12

For an RTA $\mathcal{A}$, consider its pre-observer $\mathcal{A}_{\text{obs}}^{\text{pre}} = (X, \Sigma \times \mathbb{R}_{\geq 0}, x_0, \delta_{\text{obs}}^{\text{pre}})$, we define its observer as a finite automaton

$$\mathcal{A}_{\text{obs}} = (X, \Sigma_{\text{obs}}, x_0, \delta_{\text{obs}}), \tag{2}$$

where $\Sigma_{\text{obs}}$ (resp., $\delta_{\text{obs}}$) is a finite subset of $\Sigma \times \mathbb{Q}_{\geq 0}$ (resp., $\delta_{\text{obs}}^{\text{pre}}$), such that if there exists a transition from $x \in X$ to $x' \in X$ in $\delta_{\text{obs}}^{\text{pre}}$ then at least one such transition belongs to $\delta_{\text{obs}}$.

## Remark 1

- *For an RTA $\mathcal{A}$, it may have more than one observer, because $\Sigma_{\text{obs}}$ may not be unique; but $X$ and $x_0$ must be unique.*

## Definition 12

For an RTA $\mathcal{A}$, consider its pre-observer $\mathcal{A}_{\text{obs}}^{\text{pre}} = (X, \Sigma \times \mathbb{R}_{\geq 0}, x_0, \delta_{\text{obs}}^{\text{pre}})$, we define its observer as a finite automaton

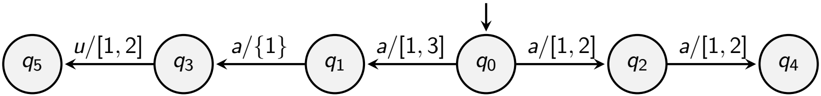
$$\mathcal{A}_{\text{obs}} = (X, \Sigma_{\text{obs}}, x_0, \delta_{\text{obs}}), \tag{2}$$

where $\Sigma_{\text{obs}}$ (resp., $\delta_{\text{obs}}$) is a finite subset of $\Sigma \times \mathbb{Q}_{\geq 0}$ (resp., $\delta_{\text{obs}}^{\text{pre}}$), such that if there exists a transition from $x \in X$ to $x' \in X$ in $\delta_{\text{obs}}^{\text{pre}}$ then at least one such transition belongs to $\delta_{\text{obs}}$.

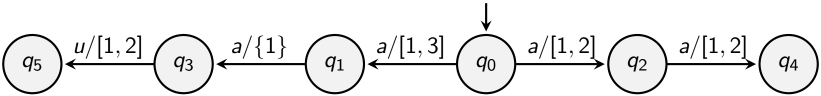
## Remark 1

- *For an RTA $\mathcal{A}$, it may have more than one observer, because $\Sigma_{\text{obs}}$ may not be unique; but $X$ and $x_0$ must be unique.*
- *For a labeled finite automaton, it has a unique observer, which is actually the powerset construction used for determinizing the automaton.*

## Example 13 (cont. $\mathcal{A}_1$)



## Example 13 (cont. $\mathcal{A}_1$)




One of its observers is

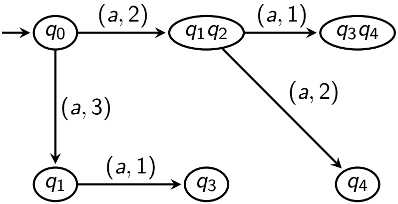



Figure 2: $\mathcal{A}_{1\,\text{obs}}$.

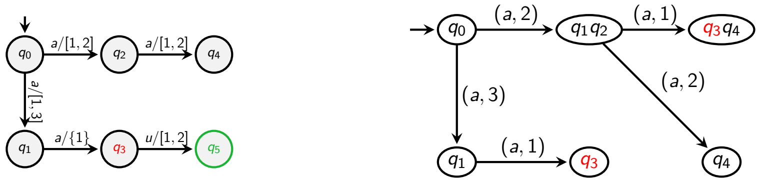
### Theorem 14

*An RTA $\mathcal{A}$ is CSO w.r.t. $Q_S$ iff in observer $\mathcal{A}_{\text{obs}}$, every reachable state $x$ contains at least one non-eventually-secret state of $\mathcal{A}$.*

## Theorem 14

*An RTA $\mathcal{A}$ is CSO w.r.t. $Q_S$ iff in observer $\mathcal{A}_{\text{obs}}$, every reachable state $x$ contains at least one non-eventually-secret state of $\mathcal{A}$.*

## Example 15 (cont. $\mathcal{A}_1$)



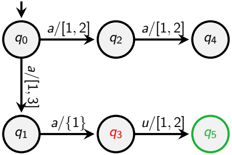

$\mathcal{A}_1$. $\mathcal{A}_{1\,\text{obs}}$.

Let $Q_S = \{q_5\}$, so the eventually secret states are $q_3$ and $q_5$.

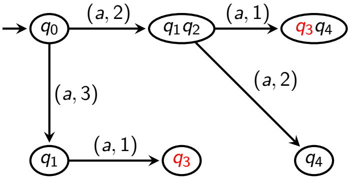
## Theorem 14

*An RTA $\mathcal{A}$ is CSO w.r.t. $Q_S$ iff in observer $\mathcal{A}_{\mathrm{obs}}$, every reachable state $x$ contains at least one non-eventually-secret state of $\mathcal{A}$.*

## Example 15 (cont. $\mathcal{A}_1$)




$\mathcal{A}_1$.




$\mathcal{A}_{1\,\mathrm{obs}}$.

Let $Q_S = \{q_5\}$, so the eventually secret states are $q_3$ and $q_5$. In $\mathcal{A}_{1\,\mathrm{obs}}$, there is a reachable state $\{q_3\}$ which only contains eventually secret states, then $\mathcal{A}_1$ is not CSO w.r.t. $\{q_5\}$.

**Theorem 16**

*For an RTA $\mathcal{A}$, its observer $\mathcal{A}_{\mathrm{obs}}$ can be computed in* 2-EXPTIME *in the size of $\mathcal{A}$.*

### Theorem 16

*For an RTA $\mathcal{A}$, its observer $\mathcal{A}_{\text{obs}}$ can be computed in* 2-EXPTIME *in the size of $\mathcal{A}$.*

### Proof sketch

## Theorem 16

*For an RTA $\mathcal{A}$, its observer $\mathcal{A}_{\text{obs}}$ can be computed in* 2-EXPTIME *in the size of $\mathcal{A}$.*

## Proof sketch

- Compute the initial state $x_0 = \mathcal{M}(\mathcal{A}, \epsilon)$ in polynomial time.

## Theorem 16

*For an RTA $\mathcal{A}$, its observer $\mathcal{A}_{\text{obs}}$ can be computed in 2-EXPTIME in the size of $\mathcal{A}$.*

## Proof sketch

- Compute the initial state $x_0 = \mathcal{M}(\mathcal{A}, \epsilon)$ in polynomial time.
- Starting from $x_0$, find all reachable states step by step together with the corresponding transitions: check for all $x_1, x_2 \subset Q$ and $\sigma \in \Sigma$, whether there is a transition $(x_1, (\sigma, t), x_2)$ for some $t \in \mathbb{Q}_{\geq 0}$ (exponentially many times, each in doubly exponential time).

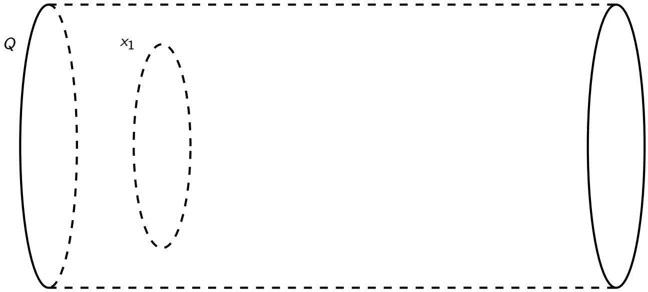
## Theorem 16

*For an RTA $\mathcal{A}$, its observer $\mathcal{A}_{\text{obs}}$ can be computed in 2-EXPTIME in the size of $\mathcal{A}$.*

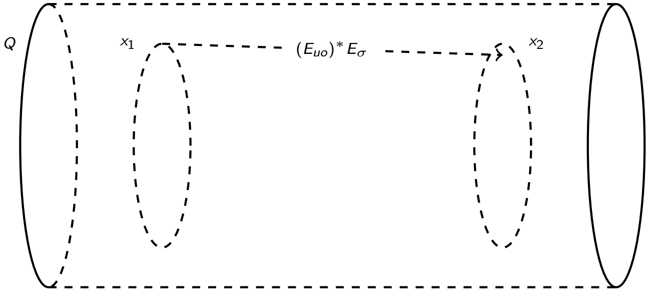
## Proof sketch

- Compute the initial state $x_0 = \mathcal{M}(\mathcal{A}, \epsilon)$ in polynomial time.
- Starting from $x_0$, find all reachable states step by step together with the corresponding transitions: check for all $x_1, x_2 \subset Q$ and $\sigma \in \Sigma$, whether there is a transition $(x_1, (\sigma, t), x_2)$ for some $t \in \mathbb{Q}_{\geq 0}$ (exponentially many times, each in doubly exponential time).
- In addition, for all $x_1, x_2, x_3 \subset Q$, if we find two transitions $(x_1, (\sigma, t), x_2)$ and $(x_1, (\sigma, t'), x_3)$ for some $t, t' \in \mathbb{Q}_{\geq 0}$, then $x_2 \subset x_3$ implies $x_3 \not\subset \mathcal{M}(\mathcal{A}, (\sigma, t)|x_1)$. This guarantees that if there exists a transition from $x_1 \subset Q$ to $x_2 \subset Q$ in $\mathcal{A}_{\text{obs}}^{\text{pre}}$, then there also exists a transition from $x_1 \subset Q$ to $x_2 \subset Q$ in $\mathcal{A}_{\text{obs}}$.

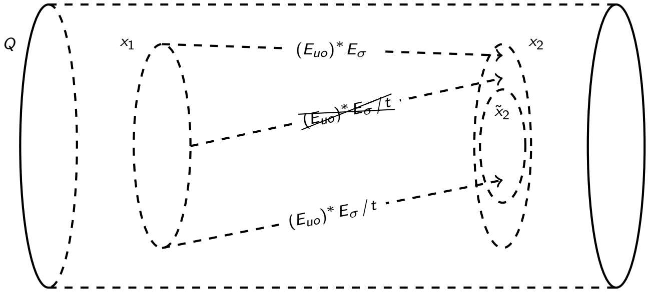

Q


Q
$x_1$

$\sigma \in \Sigma,\ E_\sigma = \{e \in E | \ell(e) = \sigma\}$



$$\sigma \in \Sigma,\ E_\sigma = \{e \in E | \ell(e) = \sigma\}$$

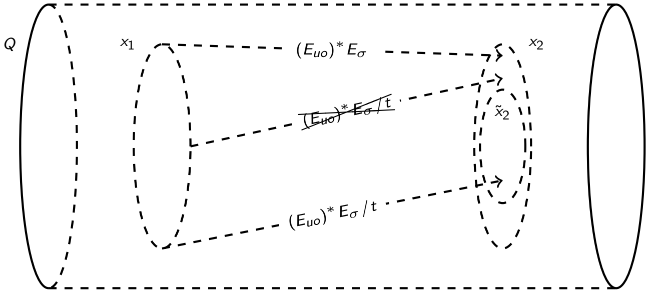



$t$ depends on $x_1, x_2, \tilde{x}_2$

$$x_1 \ni q_1(\exists) \xrightarrow{(E_{uo})^* E_\sigma / t} (\forall) q_2 \in \tilde{x}_2 (\forall\exists)$$

$$x_1 \ni q_1(\forall) \not\xrightarrow{(E_{uo})^* E_\sigma / t} (\forall) q_2 \in x_2 \setminus \tilde{x}_2 (\forall\forall)$$

$\sigma \in \Sigma$, $E_\sigma = \{e \in E | \ell(e) = \sigma\}$




$t$ depends on $x_1, x_2, \tilde{x}_2$

$$x_1 \ni q_1(\exists) \xrightarrow{(E_{uo})^* E_\sigma / t} (\forall) q_2 \in \tilde{x}_2 (\forall\exists)$$

$$x_1 \ni q_1(\forall) \xrightarrow{\not{(E_{uo})^* E_\sigma / t}} (\forall) q_2 \in x_2 \setminus \tilde{x}_2 (\forall\forall)$$

$$\Longrightarrow x_1 \xrightarrow{(\sigma, t)} \mathcal{M}(\mathcal{A}, \epsilon | \tilde{x}_2) \text{ a transition of } \mathcal{A}_{\text{obs}}$$

# Further reading for computing $\mathcal{A}_{\text{obs}}$

- NP-complete exact path length problem in weighted directed graphs $(\mathbb{Q}^k, V, A)$[1]

[1] M. Nykänen and E. Ukkonen (2002). "The exact path length problem". In: *Journal of Algorithms* 42.1, pp. 41–53.

# Further reading for computing $\mathcal{A}_{\text{obs}}$

- NP-complete exact path length problem in weighted directed graphs $(\mathbb{Q}^k, V, A)$[1]
- The exact run length problem in duration directed graphs, the notion of pre-observer, verification of other variants of state-based opacity[2]

[1] M. Nykänen and E. Ukkonen (2002). "The exact path length problem". In: *Journal of Algorithms* 42.1, pp. 41–53.

[2] K. Zhang (2021). "State-Based Opacity of Real-Time Automata". In: *27th IFIP WG 1.5 International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA 2021)*. Ed. by Alonso Castillo-Ramirez, Pierre Guillon, and Kévin Perrot. Vol. 90. Open Access Series in Informatics (OASIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 12:1–12:15.

# Further reading for computing $\mathcal{A}_{\text{obs}}$

- NP-complete exact path length problem in weighted directed graphs $(\mathbb{Q}^k, V, A)$[1]
- The exact run length problem in duration directed graphs, the notion of pre-observer, verification of other variants of state-based opacity[2]
- Presburger arithmetic[3]

[1] M. Nykänen and E. Ukkonen (2002). "The exact path length problem". In: *Journal of Algorithms* 42.1, pp. 41–53.

[2] K. Zhang (2021). "State-Based Opacity of Real-Time Automata". In: *27th IFIP WG 1.5 International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA 2021)*. Ed. by Alonso Castillo-Ramirez, Pierre Guillon, and Kévin Perrot. Vol. 90. Open Access Series in Informatics (OASIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 12:1–12:15.

[3] E. Grädel (1988). "Subclasses of Presburger arithmetic and the polynomial-time hierarchy". In: *Theoretical Computer Science* 56.3, pp. 289–301.

# Further reading for computing $\mathcal{A}_{\text{obs}}$

- NP-complete exact path length problem in weighted directed graphs $(\mathbb{Q}^k, V, A)$[1]
- The exact run length problem in duration directed graphs, the notion of pre-observer, verification of other variants of state-based opacity[2]
- Presburger arithmetic[3]
- Observer of labeled weighted automata over the monoid $(\mathbb{Q}^k, +)$, computable in 2-EXPTIME[4]

[1] M. Nykänen and E. Ukkonen (2002). "The exact path length problem". In: *Journal of Algorithms* 42.1, pp. 41–53.

[2] K. Zhang (2021). "State-Based Opacity of Real-Time Automata". In: *27th IFIP WG 1.5 International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA 2021)*. Ed. by Alonso Castillo-Ramirez, Pierre Guillon, and Kévin Perrot. Vol. 90. Open Access Series in Informatics (OASIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 12:1–12:15.

[3] E. Grädel (1988). "Subclasses of Presburger arithmetic and the polynomial-time hierarchy". In: *Theoretical Computer Science* 56.3, pp. 289–301.

[4] K. Zhang. "Detectability of labeled weighted automata over monoids". https://arxiv.org/abs/2006.14164.

# Content

## Results

## Results

- Notions of state-based opacity in real-time automata (RTAs)

## Results

- Notions of state-based opacity in real-time automata (RTAs)
- Notions of observer and reverse observer of RTAs

## Results

- Notions of state-based opacity in real-time automata (RTAs)
- Notions of observer and reverse observer of RTAs
- Verification of state-based opacity with complexity upper bounds

## Results

- Notions of state-based opacity in real-time automata (RTAs)
- Notions of observer and reverse observer of RTAs
- Verification of state-based opacity with complexity upper bounds

## An open question

Lower bounds on verification of state-based opacity in RTAs (EXPSPACE or 2-EXPTIME?)

Thank you for your attention!

Questions or comments?

# References I


Bryans, J. W., M. Koutny, L. Mazaré, and P. Y. A. Ryan (2008). "Opacity generalised to transition systems". In: *International Journal of Information Security* 7.6, pp. 421–435.

Cassez, F., J. Dubreil, and H. Marchand (2009). "Dynamic Observers for the Synthesis of Opaque Systems". In: *Automated Technology for Verification and Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 352–367.

Grädel, E. (1988). "Subclasses of Presburger arithmetic and the polynomial-time hierarchy". In: *Theoretical Computer Science* 56.3, pp. 289–301.

Lin, F. (2011). "Opacity of Discrete Event Systems and Its Applications". In: *Automatica* 47.3, pp. 496–503.

Mazaré, L. (2004). "Using unification for opacity properties". In: *Verimag Technical Report*.

Nykänen, M. and E. Ukkonen (2002). "The exact path length problem". In: *Journal of Algorithms* 42.1, pp. 41–53.

Saboori, A. and C. N. Hadjicostis (2013). "Verification of initial-state opacity in security applications of discrete event systems". In: *Information Sciences* 246, pp. 115–132.

Wang, L., N. Zhan, and J. An (2018). "The Opacity of Real-Time Automata". In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 37.11, pp. 2845–2856.

# References II

Wu, Y. and S. Lafortune (2013). "Comparative analysis of related notions of opacity in centralized and coordinated architectures". In: *Discrete Event Dynamic Systems* 23.3, pp. 307–339.

Zhang, K. "Detectability of labeled weighted automata over monoids". https://arxiv.org/abs/2006.14164.

— (2021). "State-Based Opacity of Real-Time Automata". In: *27th IFIP WG 1.5 International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA 2021)*. Ed. by Alonso Castillo-Ramirez, Pierre Guillon, and Kévin Perrot. Vol. 90. Open Access Series in Informatics (OASIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 12:1–12:15.