Topics in Timed Automata

B. Srivathsan

RWTH-Aachen
Software modeling and Verification group
$\mathcal{L}(A) \subseteq \mathcal{L}(B)$

Is $\mathcal{L}(A) \cap \overline{\mathcal{L}(B)}$ empty?
System

\[ \mathcal{L}(A) \subseteq \mathcal{L}(B) \]

Specification

Is \[ \mathcal{L}(A) \cap \overline{\mathcal{L}(B)} \] empty?

first determinize \( B \)
Lecture 2:
Determinizing timed automata
$g_1$ and $g_2$ should be mutually exclusive. For every $(q, v)$ there is only one choice.
For every \((q, v)\) there is only one choice.

\(g_1\) and \(g_2\) should be mutually exclusive.
For every \((q, v)\) there is only one choice.
For every \((q, v)\) there is only one choice

g_1 and g_2 should be mutually exclusive
Deterministic Timed Automata

\[ g_i \land g_j \text{ is unsatisfiable} \]

complete if

\[ g_1 \lor g_2 \lor \ldots \lor g_k = \top \]

A theory of timed automata

R. Alur and D. Dill, TCS'90
Deterministic Timed Automata

A theory of timed automata
R. Alur and D. Dill, TCS'90
Deterministic Timed Automata

A DTA has a unique run on every timed word

A theory of timed automata

R. Alur and D. Dill, TCS'90
\[ q_0 \xrightarrow{x = 1, a, \{x\}} q_1 \xrightarrow{x = 1, a, \{x\}} \] a DTA

\[ q_0 \xrightarrow{a, \{x\}} q_1 \xrightarrow{a} q_2 \xrightarrow{x = 1, a} \] not a DTA
Accepting states:  \((q_F, \star)\) and \((\star, q'_F)\) for union

\((q_F, q'_F)\) for intersection
Accepting states: \((q_F, \star)\) and \((\star, q'_F)\) for union
\((q_F, q'_F)\) for intersection
Theorem

DTA are **closed** under **union** and **intersection**
Complementation

Unique run

A DTA has a unique run on every timed word

⇒ DTA are closed under complement
   (interchange accepting and non-accepting states)
Every DTA is a TA: \( \mathcal{L}(DTA) \subseteq \mathcal{L}(TA) \)

But there is a TA that cannot be complemented (Lecture 1)

\[ \therefore \quad \mathcal{L}(DTA) \subset \mathcal{L}(TA) \]
DTA
Unique run
Closed under $\cup$, $\cap$, comp.
$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$
Given a TA, **when** do we know if we **can** determinize it?
Given a TA, **when** do we know if we **can** determinize it?

**Theorem [Finkel’06]**  
Given a TA, checking **if** it can be determinized is **undecidable**
Given a TA, when do we know if we can determinize it?

**Theorem [Finkel’06]**
Given a TA, checking if it can be determinized is undecidable

Following next: some sufficient conditions for determinizing
To reset or not to reset?

First solution: Whenever $a$, reset $x$.  

$$\begin{align*}
\{s, t\} & \quad \text{if } a \cdot q \cdot a \\
\{s, t\} & \quad \text{if } a \cdot q \cdot a
\end{align*}$$
To reset or not to reset?

First solution:
Whenever \( a \), reset \( x \).
To reset or not to reset?

First solution:
Whenever $a$, reset $x$.
To reset or not to reset?

First solution:
Whenever $a$, reset $x$.
To reset or not to reset?
First solution:
Whenever $a$, reset $x_a$
Event-recording clocks: time since last occurrence of event

\[ a \rightarrow x_a \]

Event-clock automata: a determinizable subclass of timed automata

Alur, Henzinger, Fix. *TCS’99*
Event-recording automata

\{ ( (abcd)^k, \tau ) \mid a - c \text{ distance is} < 1 \text{ and } b - d \text{ distance is} > 2 \}

\{ (ab^*b, \tau ) \mid \text{distance between first and last letters is} 1 \}

\begin{align*}
q_0 & \xrightarrow{a} q_1 \\
q_2 & \xrightarrow{b} q_3 \\
q_3 & \xrightarrow{c} q_2 \\
q_0 & \xrightarrow{d} q_2
\end{align*}

\begin{align*}
x_a & < 1 \\
x_b & > 2
\end{align*}
Event-recording automata

\( \{ ( (ab\!cd)^k, \tau ) \mid a - c \text{ distance is } < 1 \text{ and } b - d \text{ distance is } > 2 \} \)

\( \{ (ab^*b, \tau) \mid \text{distance between first and last letters is } 1 \} \)

non-deterministic
Determinizing ERA: modified subset construction

exponential in the number of states
DTA

Unique run

Closed under $\cup$, $\cap$, comp.

$L(DTA) \subset L(TA)$

Determinizable subclasses

ERA
To reset or not to reset?
To \textit{reset} or not to \textit{reset}?

\textbf{Coming next:} slightly modified version of BBBB-09

When are timed automata determinizable?

Baier, Bertrand, Bouyer, Brihaye. \textit{ICALP'09}
\[ q \]

\[
\begin{align*}
\{x\} \\
(\text{a, } g_1) \\
(\text{a, } g_2)
\end{align*}
\]

\[
\begin{align*}
\{ (s, \quad ), (t, \quad ) \} \\
\{ (s, \quad ) \} \\
\{ (t, \quad ) \} \\
\{ \quad \}
\end{align*}
\]
\[ q \]

\[ a, g_1 \]

\[ \{x\} \]

\[ s \]

\[ a, g_2 \]

\[ t \]
\[ a, g_1 \quad a, g_2 \quad a, x \leq 5 \quad a, x > 2 \]
\[ a, g_1, g_2 \]

\[ \{x\} \]

\[ a, x \leq 5 \]

\[ a, x > 2 \]
Reset a new clock $z_i$ at level $i$
\{(q_1, \sigma_1), (q_2, \sigma_2), \ldots, (q_k, \sigma_k)\}

\[\sigma_j : X \mapsto \{z_0, \ldots, z_i\}\]

Reset a **new** clock \(z_i\) at level \(i\)
\{(q_1, \sigma_1), (q_2, \sigma_2), \ldots, (q_k, \sigma_k)\}

\sigma_j : X \mapsto \{z_0, \ldots, z_i\}

When do finitely many clocks suffice?

Reset a \textbf{new} clock \(z_i\) at level \(i\)
Conditions:
- $g$ has integer constants
- $R$ is non-empty iff $g$ has some constraint $x = c$

Implication:
- Along a timed word, a reset of an IRTA happens only at integer timestamps
\[ x = 1, a \]
\[ \{x\} \]

**an IRTA**

\[ a \]
\[ \{x\} \]

\[ a \]
\[ x = 1, a \]
\[ \{x\} \]

**not an IRTA**
\[ q_0 \xrightarrow{x = 1, a} q_1 \; \{x\} \]

an IRTA

\[ q_0 \xrightarrow{a} q_0 \; \{x\} \]

\[ q_0 \xrightarrow{a} q_1 \xrightarrow{x = 1, a} q_2 \]

not an IRTA

Next: **determinizing** IRTA using the **subset construction**
\( M: \) max constant from among guards

\[ Z_{i_1} \]
\[ \vdots \]
\[ Z_{i_2} \]
\[ \vdots \]
\[ Z_{i_k} \]

\[ z_{i_1} z_{i_2} \ldots z_{i_k} \] active clocks

Assume the semantics of timed word \((\mathcal{w}, \tau)\) such that \(\tau_1 < \tau_2 < \cdots < \tau_k\)

- If \( k \geq M + 1 \), then \( z_{i_1} > M \) (as reset is only in integers)
- Replace \( z_{i_1} \) with \( \perp \) and reuse \( z_{i_1} \) further
**DTA**

- Unique run
- Closed under $\cup$, $\cap$, comp.

$L(DTA) \subset L(TA)$

**Determinizable subclasses**

- ERA
- IRTA
\begin{align*}
\{(q_1, \sigma_1), (q_2, \sigma_2), \ldots, (q_k, \sigma_k)\} \\
\sigma_j : X \mapsto \{z_0, \ldots, z_i\}
\end{align*}

When do finitely many clocks suffice?

Reset a new clock $z_i$ at level $i$
Strongly non-Zeno automata

A TA is strongly non-Zeno if there is $K \in \mathbb{N}$:

**every** sequence of greater than $K$ transitions **elapses** at least 1 time unit

![Diagram](https://via.placeholder.com/150)

$x < 1, a$

$q_0 \rightarrow q_1$

not SNZ

$x = 1, a$

$q_0 \rightarrow q_1$

SNZ
Finitely many clocks suffice in the subset construction for strongly non-Zeno automata

(The number of clocks depends on size of region automaton...)

When are timed automata determinizable?

Baier, Bertrand, Bouyer, Brihaye. ICALP’09
Complexity of subset construction

\[ \{(q_1, \sigma_1), (q_2, \sigma_2) \ldots (q_k, \sigma_k)\} \]

\[ \sigma_j : X \mapsto \{z_0, \ldots, z_{p-1}\} \]
Complexity of subset construction

\[ \{(q_1, \sigma_1), (q_2, \sigma_2) \ldots (q_k, \sigma_k)\} \]

\[ \sigma_j : X \mapsto \{z_0, \ldots, z_{p-1}\} \]

\[ \sigma_j : \quad \_ \quad \_ \quad \_ \quad \_ \quad \ldots \quad \_ \quad |X| \text{ places} \]

\[ p \text{ choices} \]
Complexity of subset construction

\( \{(q_1, \sigma_1), (q_2, \sigma_2) \ldots (q_k, \sigma_k)\} \)

\( \sigma_j : X \mapsto \{z_0, \ldots, z_{p-1}\} \)

\( \sigma_j : \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad |X| \text{ places} \)

\( p \text{ choices} \)

\( \text{no. of } \sigma_j : \quad p^{|X|} \)

\( \text{no. of } (q_j, \sigma_j) : \quad |Q| \cdot p^{|X|} \)
Complexity of subset construction

\[ \{(q_1, \sigma_1), (q_2, \sigma_2) \ldots (q_k, \sigma_k)\} \]

\[ 2^{|Q|} \cdot p^{|X|} \]

\[ \sigma_j : X \mapsto \{z_0, \ldots, z_{p-1}\} \]

\[ \sigma_j : \begin{array}{ccccccccc} \quad & \quad & \quad & \quad & \ldots & \quad & \quad & \quad & \quad \\ \uparrow & & & & & & & & \\ p \text{ choices} \end{array} \]

no. of \( \sigma_j \): \( p^{|X|} \)

no. of \( (q_j, \sigma_j) \): \( |Q| \cdot p^{|X|} \)

\[ \rightarrow \text{doubly exponential} \text{ in the size of initial automaton} \]
DTA
Unique run
Closed under $\cup$, $\cap$, comp.
$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$

Determinizable subclasses
ERA
IRTA
SNZ
Closure properties of ERA, IRTA, SNZ

- **Union:** disjoint union ✓
- **Intersection:** product construction ✓
- **Complement:** determinize & interchange acc. states ✓
DTA
Unique run
Closed under $\cup$, $\cap$, comp.

$\mathcal{L}(DTA) \subseteq \mathcal{L}(TA)$

Determinizable subclasses
ERA
IRTA
SNZ

ERA, IRTA, SNZ
Incomparable
Closed under $\cup$, $\cap$, comp.
Perspectives

Other related work:

- Event-predicting clocks (Alur, Henzinger, Fix’99)
- Bounded two-way timed automata (Alur, Henzinger’92)

For the future:

- Infinite timed words: Safra?
- Efficient algorithms