Topics in Timed Automata

B. Srivathsan

RWTH-Aachen
Software modeling and Verification group
Reachability for timed automata

Key idea: Compute the zone graph, use abstraction for termination

\[ q_3 = q_1 \land Z_3 \subseteq a(Z_1)? \]
Reachability for timed automata

Key idea: Compute the zone graph, use abstraction for termination

Coarser the abstraction, smaller the zone graph
**Condition 1:** \( a \) should have **finite range**

**Condition 2:** \( a \) should be sound \( \Rightarrow a(W) \) can contain only valuations **simulated** by \( W \)
Theorem [LS00]

Coarsest simulation relation is EXPTIME-hard
Bounds and abstractions

Theorem [LS00]

Coarsest simulation relation is EXPTIME-hard

\[
\begin{align*}
(y &\leq 3) & & (x < 4) \\
(x &< 1) & & (x > 6) \\
(y &< 1)
\end{align*}
\]
Bounds and abstractions

Theorem [LS00]

Coarsest simulation relation is EXPTIME-hard

\( (y \leq 3) \quad (x < 4) \quad (x < 1) \quad (x > 6) \quad (y < 1) \)

\textbf{M-bounds} [AD94]

\[ M(x) = 6, \quad M(y) = 3 \]

\[ \nu \preceq_M \nu' \]

\textbf{LU-bounds} [BBLP04]

\[ L(x) = 6, \quad L(y) = -\infty \]

\[ U(x) = 4, \quad U(y) = 3 \]

\[ \nu \preceq_{LU} \nu' \]
Abstractions in literature [BBLP04, Bou04]

Last lecture: **Efficiently** using the $M$-bounds based $\text{Closure}_M$ abstraction
Lecture 7:

Lower-upper bounds for abstraction
**LU-guards:** guards consistent with given $L$ and $U$

LU-guards for $L(x) = 3$, $U(x) = 5$, $L(y) = 8$, $U(y) = -\infty$

$$x \geq 0, x \geq 1, x \geq 2, x \geq 3$$

$$x \leq 0, x \leq 1, \ldots, x \leq 5$$

$$y \geq 0, y \geq 1, \ldots, y \geq 8$$

(same with $<$ and $>$)
**LU-automata:** automata with only LU-guards

$L(x) = 3, U(x) = 5, L(y) = 8, U(y) = -\infty$

\[ q_0 \xrightarrow{x \geq 2, \{x\}} q_1 \]

\[ y \geq 7 \]

\[ q_1 \xrightarrow{y \leq 7, \{x\}} \]

\[ 8/35 \]
LU-automata: automata with only LU-guards

\[ L(x) = 3, \ U(x) = 5, \ L(y) = 8, \ U(y) = -\infty \]
What do we need?

1. An abstraction $\text{abs}_{LU}$ that is sound and complete for all LU-automata

2. Efficient inclusion testing $Z \subseteq \text{abs}_{LU}(Z')$
Step 1:

LU-regions
Classic regions [AD94]: $v'$ belongs to $[v]^M$ if:

- **Invariance by guards:** $v'$ satisfies the same guards as $v$,
- **Invariance by time-ellipse:** for every time elapse $\delta \in \mathbb{R}_{\geq 0}$, there is a $\delta' \in \mathbb{R}_{\geq 0}$ such that $v' + \delta' \in [v + \delta]^M$. 

![Diagram showing region $[v]^M$ and $[v + \delta]^M$]
Classic regions [AD94]: \( \nu' \) belongs to \([\nu]^M\) if:

- **Invariance by guards:** \( \nu' \) satisfies the same guards as \( \nu \), \( \checkmark \)
- **Invariance by time-elapse:** for every time elapse \( \delta \in \mathbb{R}_{\geq 0} \), there is a \( \delta' \in \mathbb{R}_{\geq 0} \) such that \( \nu' + \delta' \in [\nu + \delta]^M \).
Classic regions [AD94]: $v'$ belongs to $[v]^M$ if:

- **Invariance by guards:** $v'$ satisfies the same guards as $v$, $\checkmark$

- **Invariance by time-ellipse:** for every time elapse $\delta \in \mathbb{R}_{\geq 0}$, there is a $\delta' \in \mathbb{R}_{\geq 0}$ such that $v' + \delta' \in [v + \delta]^M$. 

![Diagram showing invariance by guards and time-ellipse](image)
Classic regions [AD94]: \( \nu' \) belongs to \([\nu]^M\) if:

- **Invariance by guards:** \( \nu' \) satisfies the same guards as \( \nu \), \( \checkmark \)
- **Invariance by time-ellipse:** for every time elapse \( \delta \in \mathbb{R}_{\geq 0} \), there is a \( \delta' \in \mathbb{R}_{\geq 0} \) such that \( \nu' + \delta' \in [\nu + \delta]^M \).
Classic regions [AD94]: \( \nu' \) belongs to \([\nu]^M\) if:

- **Invariance by guards**: \( \nu' \) satisfies the same guards as \( \nu \), √

- **Invariance by time-elapse**: for every time elapse \( \delta \in \mathbb{R}_{\geq 0} \), there is a \( \delta' \in \mathbb{R}_{\geq 0} \) such that \( \nu' + \delta' \in [\nu + \delta]^M \). ×
Classic regions [AD94]: $v'$ belongs to $[v]^M$ if:

- **Invariance by guards:** $v'$ satisfies the same guards as $v$, \(\checkmark\)

- **Invariance by time-ela$pse:** for every time elapse $\delta \in \mathbb{R}_{\geq 0}$, there is a $\delta' \in \mathbb{R}_{\geq 0}$ such that $v' + \delta' \in [v + \delta]^M$. \(\checkmark\)
Classic regions [AD94]: \( \nu' \) belongs to \( [\nu]^M \) if:

- **Invariance by guards:** \( \nu' \) satisfies the same guards as \( \nu \), √
- **Invariance by time-elapse:** for every time elapse \( \delta \in \mathbb{R}_{\geq 0} \), there is a \( \delta' \in \mathbb{R}_{\geq 0} \) such that \( \nu' + \delta' \in [\nu + \delta]^M \). √
Classic regions [AD94]: $v'$ belongs to $[v]^M$ if:

- **Invariance by guards:** $v'$ satisfies the same guards as $v$, ✓
- **Invariance by time-elapse:** for every time elapse $\delta \in \mathbb{R}_{\geq 0}$, there is a $\delta' \in \mathbb{R}_{\geq 0}$ such that $v' + \delta' \in [v + \delta]^M$. ✓
Classic regions [AD94]: Given $M$, $\nu'$ belongs to $[\nu]^M$ if:

- **Invariance by guards:** $\nu'$ satisfies the same guards as $\nu$,
- **Invariance by time-elapsed:** for every pair of clocks $x, y$ with:

  \[
  \nu(x) \leq M_x, \quad \nu(y) \leq M_y
  \]

  \[
  \lfloor \nu(x) \rfloor = \lfloor \nu'(x) \rfloor \quad \text{and} \quad \lfloor \nu(y) \rfloor = \lfloor \nu'(y) \rfloor
  \]

  we have:

  - if $0 < \{\nu(x)\} < \{\nu(y)\}$, then $0 < \{\nu'(x)\} < \{\nu'(y)\}$
  - if $0 < \{\nu(x)\} = \{\nu(y)\}$, then $0 < \{\nu'(x)\} = \{\nu'(y)\}$

  $\lfloor \nu(x) \rfloor$: integer part of $\nu(x)$

  $\{\nu(x)\}$: fractional part of $\nu(x)$
Invariance by (LU-) guards: $\nu(x)$ is less than both $L_x$, $U_x$
Invariance by (LU-) guards: \( \nu(x) > L_x \)
Invariance by (LU-) guards: $\nu(x) > U_x$
Invariance by time-elapse: $v(x) \leq U_x, \quad v(y) \leq L_y$
Invariance by time-elapse: $v(x) > U_x$, $v(y) \leq L_y$
Invariance by time-elapse: \( v(x) \leq U_x, \quad v(y) > L_y \)
LU-regions

**Definition:** \( v' \) belongs to \( \langle v \rangle^{LU} \) if:

- **Invariance by guards:** \( v' \) satisfies the same guards as \( v \),
- **Invariance by time-ellipse:** for every pair of clocks \( x, y \) with:

\[
\begin{align*}
  v(x) &\leq U_x, \quad v(y) \leq L_y \\
  \lfloor v(x) \rfloor &= \lfloor v'(x) \rfloor \quad \text{and} \quad \lfloor v(y) \rfloor = \lfloor v'(y) \rfloor,
\end{align*}
\]

we have:

- if \( 0 < \{v(x)\} < \{v(y)\} \), then \( 0 < \{v'(x)\} < \{v'(y)\} \)
- if \( 0 < \{v(x)\} = \{v(y)\} \), then \( 0 < \{v'(x)\} = \{v'(y)\} \)
Step 2:

An abstraction $\text{abs}_{LU}$
\[ v \sqsubseteq_{LU} v' \]

if

\[ \exists \delta' \in \mathbb{R}_{\geq 0} \text{ s.t. } v' + \delta' \in \langle v \rangle^{LU} \]
\[ \nu \sqsubseteq_{LU} \nu' \]

if

\[ \exists \delta' \in \mathbb{R}_{\geq 0} \text{ s.t. } \nu' + \delta' \in \langle \nu \rangle_{LU} \]

**Definition**

\[ \text{abs}_{LU}(W) = \{ \nu \mid \exists \nu' \in W \text{ s.t. } \nu \sqsubseteq_{LU} \nu' \} \]
\[ \nu \sqsubseteq_{LU} \nu' \]

if

\[ \exists \delta' \in \mathbb{R}_{\geq 0} \text{ s.t. } \nu' + \delta' \in \langle \nu \rangle_{LU} \]

**Definition**

\[
\text{abs}_{LU}(W) = \{ \nu | \exists \nu' \in W \text{ s.t. } \nu \sqsubseteq_{LU} \nu' \}
\]

**abs}_{LU} is sound and complete**
Example

The diagram illustrates a two-dimensional space with axes labeled $x$ and $y$. The region of interest is shaded and labeled with $U_y$ and $L_y$ for the vertical boundaries and $U_x$ and $L_x$ for the horizontal boundaries. The coordinates are given as $0$, $U_x$, and $L_x$ along the $x$-axis, and $U_y$ and $L_y$ along the $y$-axis.
Example
Example

\[ |LU(Z)| = \frac{23}{35} \]
Example
Example
Example

\[ \text{abs} \left( Z \right) \]
Example

\[ \text{abs}_{LU}(Z) \]
The diagram illustrates the relationship between various sets and their closures. Here are the key components:

- **Non-convex** set $\nu_{\leq LU}$
- **Convex** set $\nu_{\geq LU}$
- **Closure** $\text{Closure}_M$
- **Extra** $\text{Extra}_M$
- **Extra** $\text{Extra}_M^+$
- **Extra** $\text{Extra}_L^U$

The arrows indicate the direction of inclusion or containment between these sets. The diagram shows how these sets interrelate through various inclusion properties.
Time-elapsed zone $Z$: if $\nu \in Z$, then $\nu + \delta \in Z$ for all $\delta \in \mathbb{R}_{\geq 0}$

\[
\alpha_{\preceq_{LU}} \text{ coincides with } \text{abs}_{LU}
\]

If $Z$ is time-elapsed, then $\alpha_{\preceq_{LU}}(Z) = \text{abs}_{LU}(Z)$

Better abstractions for timed automata

F. Herbreteau, B. Srivathsan, I. Walukiewicz. LICS’12
Time-elapsed zone $Z$: if $\nu \in Z$, then $\nu + \delta \in Z$ for all $\delta \in \mathbb{R}_{\geq 0}$

\[ a_{\preceq LU} \text{ coincides with } \text{abs}_{LU} \]

If $Z$ is time-elapsed, then $a_{\preceq LU}(Z) = \text{abs}_{LU}(Z)$

**Optimality**

$a_{\preceq LU}(Z)$ is the **coarsest** abstraction that is **sound** and **complete** for all LU-automata

Better abstractions for timed automata

F. Herbreteau, B. Srivathsan, I. Walukiewicz. *LICS’12*
Step 3:
Efficient inclusion
\( \nu \sqsubseteq_{LU} \nu' \)

if

\[ \exists \delta' \in \mathbb{R}_{\geq 0} \text{ s.t. } \nu' + \delta' \in \langle \nu \rangle^{LU} \]

**Definition**

\[
\text{abs}_{LU}(W) = \{ \nu | \exists \nu' \in W \text{ s.t. } \nu \sqsubseteq_{LU} \nu' \}
\]
\[ \nu \sqsubseteq_{LU} \nu' \]

if

\[ \exists \delta' \in \mathbb{R}_{\geq 0} \text{ s.t. } \nu' + \delta' \in \langle \nu \rangle^{LU} \]

**Definition**

\[
\text{abs}_{LU}(W) = \{ \nu | \exists \nu' \in W \text{ s.t. } \nu \sqsubseteq_{LU} \nu' \}
\]

\(Z, Z':\) time-elapsed zones

\[ Z \nsubseteq \text{abs}_{LU}(Z') \text{ iff there exists } \nu \in Z \text{ s.t. } \langle \nu \rangle^{LU} \text{ does not intersect } Z' \]
Efficient inclusion testing

Reduction to two clocks

\[ Z \not\subseteq a_{\leq}^{LU}(Z') \] if and only if there exist 2 clocks \( x, y \) s.t.

\[ \text{Proj}_{xy}(Z) \not\subseteq a_{\leq}^{LU}(\text{Proj}_{xy}(Z')) \]

Complexity: \( O(|X|^2) \), where \( X \) is the set of clocks

Same complexity as \( Z \subseteq Z' \)!

Slightly modified comparison works!

Better abstractions for timed automata

F. Herbreteau, B. Srivathsan, I. Walukiewicz. *LICS’12*
Efficient inclusion testing

Reduction to two clocks

\[ Z \not\subseteq a_{LU}(Z') \text{ if and only if there exist 2 clocks } x, y \text{ s.t.} \]

\[ \text{Proj}_{xy}(Z) \not\subseteq a_{LU}(\text{Proj}_{xy}(Z')) \]

Complexity: \( \mathcal{O}(|X|^2) \), where \( X \) is the set of clocks

Better abstractions for timed automata

F. Herbreteau, B. Srivathsan, I. Walukiewicz. LICS’12
Efficient inclusion testing

Reduction to two clocks

\[ Z \not\subseteq a_{\leq LU}(Z') \text{ if and only if there exist 2 clocks } x, y \text{ s.t.} \]

\[ \text{Proj}_{xy}(Z) \not\subseteq a_{\leq LU}(\text{Proj}_{xy}(Z')) \]

Complexity: \( O(|X|^2) \), where \( X \) is the set of clocks

Same complexity as \( Z \subseteq Z' \)!

Better abstractions for timed automata

F. Herbreteau, B. Srivathsan, I. Walukiewicz. LICS'12
Efficient inclusion testing

Reduction to two clocks

\[ Z \not\subseteq a_{\preceq LU}(Z') \text{ if and only if there exist 2 clocks } x, y \text{ s.t.} \]
\[ \text{Proj}_{xy}(Z) \not\subseteq a_{\preceq LU}(\text{Proj}_{xy}(Z')) \]

Complexity: \(\mathcal{O}(|X|^2)\), where \(X\) is the set of clocks

Same complexity as \(Z \subseteq Z'!\)

Slightly modified comparison works!

Better abstractions for timed automata

F. Herbreteau, B. Srivathsan, I. Walukiewicz. LICS'12
If $a \preceq_{LU}$ is best, can we do better?
Question: If $\alpha_{\leq LU}$ is best, can we do better?
Get better LU-bounds!
Global LU-bounds

Naive: $L_x = U_x = 10^6, L_y = U_y = 10^6$

Size of graph $\sim 10^6$
Static analysis: bounds for every $q$

[BBFL03]

$x = 1$
\{x\}

$q_0$ \rightarrow $q_1$

$x = 10^6$
$y = 10^6$

$q_1$ \rightarrow $q_2$

Size of graph $< 10$
Static analysis: bounds for every $q$

[BBFL03]

$x = 1$
\{x\}

$x \geq 2$

$x \leq 1$

$x = 10^6$
\{x, y\}

$y = 10^6$

Size of graph $\sim 10^6$

Need to look at semantics...
LU bounds for every \((q, Z)\) in zone graph
LU bounds for every \((q, Z)\) in zone graph

constants at

depend on subtree
\[ M(x) = -\infty \]

\[ (q, Z, M) \]

All tentative nodes consistent + No more exploration → Terminate!
\[ M(x) = -\infty \]

\[(q, Z, M)\]

\[ x \leq 3 \]
\[ M(x) = 3 \]
\( M(x) = 3 \)

\[(q, Z, M)\]

\[x \leq 3\]
\[ M(x) = 5 \]

\[ (q, Z, M) \]

\[ x \leq 3 \]
\[ M(x) = 5 \]

\[ Z' \subseteq \text{Closure}_M(Z) \]

\[ x \leq 3 \]
$$M(x) = 5$$

$$Z' \subseteq \text{Closure}_M(Z)$$

$$x \leq 3$$

$$x > 6$$
\[ M(x) = 6 \]

\[(q, Z, M)\]

\[ x \leq 3 \]

\[ x > 6 \]

\[ Z' \subseteq \text{Closure}_M(Z) \]
\[ M(x) = 6 \]

\((q, Z, M)\)

\(Z' \subseteq \text{Closure}_M(Z)\)

\((q', Z', M')\)

\[ x \leq 3 \]

\[ x > 6 \]

All tentative nodes consistent → No more exploration → Terminate!
\[ M(x) = 6 \]

\[ (q, Z, M) \]

\[ Z' \subseteq \text{Closure}_M(Z) \]

\[ x \leq 3 \]

\[ x > 6 \]
\[ M(x) = 6 \]

\[(q, Z, M)\]

\[ x \leq 3 \]

\[ x > 6 \]

\[ x \geq 11 \]

\[ Z' \subseteq \text{Closure}_M(Z) \]
\[ M(x) = 11 \]

\[ (q, Z, M) \]

\[ Z' \subseteq \text{Closure}_M(Z) \]

\[ x \leq 3 \]

\[ x > 6 \]

\[ x \geq 11 \]
\[ M(x) = 11 \]

\[ (q, Z, M) \]

\[ Z' \subseteq \text{Closure}_M(Z) \]

\[ x \leq 3 \quad x > 6 \quad x \geq 11 \]

All tentative nodes consistent → No more exploration → Terminate!
\[ M(x) = 11 \]

\[ (q, Z, M) \]

\[ Z' \subseteq \text{Closure}_M(Z) \]

\[ x \leq 3 \]

\[ x > 6 \]

\[ x \geq 11 \]
\[ M(x) = 11 \]

\[(q, Z, M)\]

\[
\begin{align*}
Z' &\subseteq \text{Closure}_M(Z) \\
x &\leq 3 \\
x &> 6 \\
x &\geq 11
\end{align*}
\]

\[
\begin{align*}
x &:= 0 \\
x := 0
\end{align*}
\]
\( M(x) = 11 \)

All tentative nodes consistent
+ No more exploration
→ Terminate!

\( Z' \subseteq \text{Closure}_M(Z) \)
Constant propagation

Theorem (Correctness)
An accepting state is reachable in $A$ iff the constant propagation algorithm reaches a node with accepting state and a non-empty zone.
Key idea: Compute the zone graph, use abstraction for termination

Developments are recent, a lot of (not-so-low) hanging fruit available
References I

R. Alur and D.L. Dill.
A theory of timed automata.

Static guard analysis in timed automata verification.

Lower and upper bounds in zone based abstractions of timed automata.

P. Bouyer.
Forward analysis of updatable timed automata.

François Laroussinie and Ph. Schnoebelen.
The state explosion problem from trace to bisimulation equivalence.