Topics in Timed Automata

B. Srivathsan

RWTH-Aachen
Software modeling and Verification group
Reachability: Does something **bad** happen?

“The gate is still open when the train is 2 minutes away from the crossing”

This problem is PSPACE-complete

A theory of timed automata

R. Alur and D.L. Dill, TCS’94
Tools

- **UPPAAL:**
  Uppsala university (*Sweden*), Aalborg university (*Denmark*)

- **KRONOS:**
  Verimag (*France*)

- **RED**
  National Taiwan University (*Taiwan*)

- **Rabbit**
  Brandenburg TU Cottbus (*Germany*)
Tools

- **UPPAAL:**
  Uppsala university (*Sweden*), Aalborg university (*Denmark*)

- **KRONOS:**
  Verimag (*France*)

- **RED**
  National Taiwan University (*Taiwan*)

- **Rabbit**
  Brandenburg TU Cottbus (*Germany*)

and still research on for efficient algorithms . . .
Lecture 6: Reachability
Timed Automata

Run: finite sequence of transitions

- accepting if ends in green state
Reachability problem

Given a TA, does it have an accepting run

Theorem [AD94]
This problem is PSPACE-complete

first solution based on Regions
Key idea: Maintain sets of valuations reachable along a path.

\[ (x \leq 5) \quad (y \geq 7) \quad \{x\} \]
Key idea: Maintain sets of valuations reachable along a path

\( x = y \geq 0 \)  \( x = y \geq 0 \)  \( y - x \geq 7 \)  \( y - x \geq 7 \)

Easy to describe convex sets
Zones and zone graph

- **Zone**: set of valuations defined by conjunctions of constraints:

  \[
  x \sim c \quad x - y \sim c
  \]

  e.g. \((x - y \geq 1) \land (y < 2)\)

- **Representation**: by DBM [Dil89]

Sound and complete [DT98]

Zone graph preserves state reachability
Problem of non-termination

\[ (y = 1) \]

\[ \{x, y\} \rightarrow q_1 \]

\[ q_0 \rightarrow \{y\} \]
Abstractions

potentially infinite...

Zone graph
Abstractions

Zone graph

potentially infinite...
Abstractions

Zone graph

potentially infinite...

\( q_0, \quad Z_0 \)

\( q_1, \quad Z_1 \)

\( q_2, \quad Z_2 \)

\( \vdots \)

\( q_3, \quad Z_3 \)

\( \vdots \)

\( \alpha(Z_0) \)

\( q_0, \quad Z_0 \)
Abstractions

potentially infinite...

Zone graph

$\alpha(Z_0)$

$q_0$, $Z_0$

$q_1$, $Z_1$

$q_2$, $Z_2$

$q_3$, $Z_3$

$: \quad : \quad :$
Abstractions

potentially infinite...

Zone graph

\[ q_0, Z_0 \]
\[ q_1, Z_1 \]
\[ q_2, Z_2 \]
\[ q_3, Z_3 \]

\[ \ldots, \ldots \]

\[ a(Z_0) \]
\[ q_0, Z_0 \]
\[ q_1, Z_1 \]
\[ \ldots, W_1 \]
Abstractions

Zone graph

potentially infinite...
Abstractions

potentially infinite...
Abstractions

Zone graph

potentially infinite...

\[ q_0, \quad Z_0 \]

\[ q_1, \quad Z_1 \]

\[ q_2, \quad Z_2 \]

\[ q_3, \quad Z_3 \]

\[ \ldots \]

\[ \ldots \]

\[ \alpha(Z_0) \]

\[ q_0, \quad Z_0 \]

\[ q_1, \quad Z_1 \]

\[ q_2, \quad Z_2 \]

\[ q_3, \quad Z_3 \]

\[ \ldots \]

\[ \ldots \]

\[ \alpha(W_1) \]

\[ q_1, \quad Z_1 \]

\[ q_2, \quad Z_2 \]

\[ q_3, \quad Z_3 \]

\[ \ldots \]

\[ \ldots \]

\[ \alpha(W_2) \]

\[ q_2, \quad W_2 \]

\[ \alpha(W_3) \]

\[ q_3, \quad W_3 \]
Abstractions

Find $\alpha$ such that number of \textit{abstracted} sets is \textit{finite}
Abstractions

Coarser the abstraction, smaller the abstracted graph
**Condition 1:** Abstractions should have **finite range**

**Condition 2:** Abstractions should be sound $\Rightarrow a(W)$ can contain only valuations **simulated** by $W$
**Condition 1:** Abstractions should have **finite range**

**Condition 2:** Abstractions should be sound \( \Rightarrow a(W) \) can contain only valuations **simulated** by \( W \)

**Question:** Why not add all the valuations **simulated** by \( W \)?
Bounds and abstractions

**Theorem [LS00]**

Coarsest simulation relation is EXPTIME-hard

$M(x) = 6$, $M(y) = 3$

$v ≼ M v'$

$(y ≤ 3)$

$(x < 1)$

$(x < 4)$

$(y < 1)$

$(y ≤ 3)$

$(x > 6)$

$(y > 3)$

$(x < 6)$

$(x ≤ 3)$

$(y < 6)$

$(x ≥ 3)$

$(y ≥ 3)$

$(x ≤ 6)$

$(y ≥ 6)$
Bounds and abstractions

**Theorem [LS00]**

The coarest simulation relation is EXPTIME-hard

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

\[ v \preceq_M v' \]

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

Theorem [LS00]

Coarsest simulation relation is EXPTIME-hard

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

\[ \nu \preceq_M \nu' \]

M-bounds [AD94]

\[ (y \leq 3), \ (x < 1), \ (y < 1), \ (x > 6), \ (x < 4) \]
Bounds and abstractions

**Theorem [LS00]**

Coarsest simulation relation is **EXPTIME-hard**

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

**M-bounds [AD94]**

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

\[
\nu \preceq_M \nu'
\]

**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]
Abstractions in literature [BBLP04, Bou04]

\[(\aleph_{LU}) \downarrow \alpha_{LU} \]\n
\[(\aleph_{M}) \downarrow \text{Closure}_M\]

Non-convex

Only convex abstractions used in implementations!
Abstractions in literature [BBLP04, Bou04]

Only convex abstractions used in implementations!
Timed automata

Zone graph

Problem of non-termination

Use finite abstractions

Bounds as parameters

Restriction to convex abstractions

Zones are efficient

Non-convex abstr. are coarser
Timed automata

Zone graph

Problem of non-termination

Use finite abstractions

Bounds as parameters

Restriction to convex abstractions

Zones are efficient

Non-convex abstr. are coarser

Question: Can we benefit from both together?
In this lecture...

**Efficient use of the non-convex Closure approximation**

Using non-convex approximations for efficient analysis of timed automata

F. Herbreteau, D. Kini, B. Srivatsan, I. Walukiewicz. *FSTTCS’11*
Observation 1: We can use abstractions without storing them
Using non-convex abstractions

Standard algorithm: covering tree

$q_3 = q_1 \land a(W_3) \subseteq a(W_1)??$

$q_3, q_1, q_0, q_5, q_4, q_2$

$q_3 = q_1 \land a(W_3) \subseteq a(W_1)$?

Standard algorithm: covering tree
Using non-convex abstractions

Standard algorithm: covering tree

Pick simulation based $a$

Need to store only concrete semantics

$Z \subseteq a(Z')$ for termination

$q_0, q_1, q_2, q_3, q_4, q_5, Z_0, W_1, Z_1, W_2, Z_2, W_3, Z_3, W_4, Z_4, W_5, Z_5, W_6$

$q_3 = q_1 \land a(W_3) \subseteq a(W_1)$?
Using non-convex abstractions

Standard algorithm:

Pick simulation based $\alpha$

$a(\mathcal{W}_3) \subseteq a(\mathcal{W}_1)$?

$q_3 = q_1 \land$

Pick simulation based $\alpha$
Using non-convex abstractions

Standard algorithm:

Pick simulation based $\alpha$

Pick $\alpha(Z_0)$

$q_3 = q_1 \land \alpha(W_3) \subseteq \alpha(W_1)$?
Using non-convex abstractions

Pick simulation based $\alpha$
Using non-convex abstractions

Standard algorithm: covering tree

Pick simulation based \( \alpha \)

Need to store only concrete semantics

Use

\[ Z \subseteq \alpha(Z') \] for termination

\[ q_0, q_1, q_2, q_3 = q_1 \land \alpha(W_3) \subseteq \alpha(W_1)? \]

\[ q_3, q_4, q_5, \] Pick simulation based \( \alpha \)
Using non-convex abstractions

Standard algorithm: covering tree

Pick simulation based $\alpha$

$q_3 = q_1 \land a(Z_3) \subseteq a(Z_1)$?
Using non-convex abstractions

Need to store only concrete semantics

$q_3 = q_1 \land a(Z_3) \subseteq a(Z_1)?$
Using non-convex abstractions

Standard algorithm:

Pick simulation based

Need to store only concrete semantics

Use $Z \subseteq a(Z')$ for termination

$q_3 = q_1 \land Z_3 \subseteq a(Z_1)$?

$q_0, Z_0$

$q_1, Z_1$

$q_2, Z_2$

$q_3, Z_3$

$q_4, Z_4$

$q_5, Z_5$

Use $Z \subseteq a(Z')$ for termination
Observation 1: We can use abstractions without storing them

Observation 2: We can do the inclusion test efficiently
Coming next...

The inclusion test $Z \subseteq \text{Closure}_M(Z')$
What is $\text{Closure}_M$?

![Graph showing $M(x)$ and $M(y)$]
What is Closure$_M$?
What is $\text{Closure}_M$?

$\text{Closure}_M(Z)$: set of regions that $Z$ intersects
$Z \subseteq \text{Closure}_M(Z')$?
$Z \subseteq \text{Closure}_M(Z')$?
$Z \subseteq \text{Closure}_M(Z')$?

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

\[ x \]

\[ y \]

\[ M(y) \]

\[ M(x) \]

\[ 0 \]

\[ x \]

\[ z \]

\[ z' \]

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

\[ \begin{align*}
Z \not\subseteq \text{Closure}_M(Z') & \iff \exists R. R \text{ intersects } Z, R \text{ does not intersect } Z'
\end{align*} \]
$Z \subseteq \text{Closure}_M(Z')$?

$Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R \text{ intersects } Z, R \text{ does not intersect } Z'$

Coming next: Steps to the efficient algorithm for $Z \not\subseteq \text{Closure}_M(Z')$
Step 1: Representing regions and zones
Step 1: Representing regions and zones

\[ \begin{align*}
  x < 3 & \quad y < \infty \\
  x > 2 & \quad y > 2
\end{align*} \]
Step 1: Representing regions and zones

\[
\begin{align*}
&x < 3 \\
&y < \infty \\
&x > 2 \\
&y > 2
\end{align*}
\]
Step 1: Representing regions and zones

\[ x < 3 \quad y < \infty \]

\[ x > 2 \quad y > 2 \]
Step 1: Representing regions and zones

\[ x - 0 < 3 \quad \text{and} \quad y < \infty \]

\[ x > 2 \quad \text{and} \quad y > 2 \]
Step 1: Representing regions and zones

\[ x - 0 < 3 \quad y < \infty \]
\[ x > 2 \quad y > 2 \]
Step 1: Representing regions and zones

\[ x - 0 < 3 \quad y < \infty \]
\[ 0 - x < -2 \quad y > 2 \]
Step 1: Representing regions and zones

\[ x - 0 < 3 \quad y < \infty \]
\[ 0 - x < -2 \quad y > 2 \]
Step 1: Representing regions and zones

\[ x - 0 < 3 \quad y < \infty \]

\[ 0 - x < -2 \quad y > 2 \]
Step 1: Representing regions and zones

\[ x - 0 < 3 \quad y - 0 < \infty \]
\[ 0 - x < -2 \quad 0 - y < -2 \]
Step 1: Representing regions and zones

\[ x - 0 < 3 \quad y - 0 < \infty \]
\[ 0 - x < -2 \quad 0 - y < -2 \]
Step 1: Representing regions and zones

\[
\begin{align*}
  x - 0 &< 3 \\
  y - 0 &< \infty \\
  0 - x &< -2 \\
  0 - y &< -2
\end{align*}
\]
Step 1: Representing regions and zones

\[
x - 0 < 3 \\
0 - x < -2 \\
y - 0 < \infty \\
0 - y < -2
\]
Step 1: Representing regions and zones

Need a **canonical** representation
Step 1: Representing regions and zones

\[x - 0 < 3 \quad y - 0 < \infty\]

\[0 - x < -2 \quad 0 - y < -2\]

Shortest path should be given by the **direct edge**
Step 1: Representing regions and zones

\[ x - 0 < 3 \quad y - 0 < \infty \]
\[ 0 - x < -2 \quad 0 - y < -2 \]

Shortest path should be given by the direct edge
Step 1: Representing regions and zones

For every zone $Z$, canonical distance graph $G_Z$
Step 2: When is $R \cap Z'$ empty?

Inspired by an observation made in [Bou04]
Step 2: When is \( R \cap Z' \) empty?

Inspired by an observation made in [Bou04]

\[
\min(G_{\mathbb{R}}, G_{\mathbb{Z}'}) = \min(G_{\mathbb{R}(0,x_1,x_2,x_3)}, G_{\mathbb{Z}'(0,x_1,x_2,x_3)})
\]
Step 2: When is $R \cap Z'$ empty?

Inspired by an observation made in [Bou04]

$G_R$

$G_{Z'}$

$\min(G_R, G_{Z'})$
Step 2: When is $R \cap Z'$ empty?

Inspired by an observation made in [Bou04]

Lemma

$R \cap Z'$ is empty $\iff$ min($G_R$, $G_{Z'}$) has a negative cycle
Step 2: When is $R \cap Z'$ empty?

Inspired by an observation made in [Bou04]

$G_R$

$G_{Z'}$

$\min(G_R, G_{Z'})$

Lemma

$R \cap Z'$ is empty $\iff$ $\min(G_R, G_{Z'})$ has a negative cycle involving at most 2 clocks!
Step 2: When is $R \cap Z'$ empty?

Inspired by an observation made in [Bou04]

\[ \min(G_R, G_{Z'}) \]

Lemma

$R \cap Z'$ is empty $\iff$ $\min(G_R, G_{Z'})$ has a negative cycle involving at most 2 clocks!
Step 2: When is $R \cap Z'$ empty?

Inspired by an observation made in [Bou04]

$$G_{\text{Proj}_{x_2x_3}}(R)$$

$$G_{\text{Proj}_{x_2x_3}}(Z')$$

Lemma

$R \cap Z'$ is empty $\iff$ $\min(G_R, G_{Z'})$ has a negative cycle involving at most 2 clocks!
Step 2: When is \( R \cap Z' \) empty?

Inspired by an observation made in [Bou04]

\[
\min(G_{Proj_{x_2x_3}}(R), G_{Proj_{x_2x_3}}(Z'))
\]

**Lemma**

\( R \cap Z' \) is empty \( \iff \) \( \min(G_R, G_{Z'}) \) has a **negative cycle** involving at most 2 clocks!
Step 2: When is $R \cap Z'$ empty?

Inspired by an observation made in [Bou04]

\[ G_{\text{Proj}_{x_2x_3}}(R) \]

\[ G_{\text{Proj}_{x_2x_3}}(Z') \]

\[ \min(G_{\text{Proj}_{x_2x_3}}(R), G_{\text{Proj}_{x_2x_3}}(Z')) \]

Lemma

$R \cap Z'$ is empty $\iff \exists x, y. \text{Proj}_{xy}(R) \cap \text{Proj}_{xy}(Z')$ is empty
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R$ intersects $Z$, $R$ does not intersect $Z'$
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R$ intersects $Z$, $R$ does not intersect $Z'$
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R$ intersects $Z$, $R$ does not intersect $Z'$
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R \text{ intersects } Z, R \text{ does not intersect } Z'$
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R$ intersects $Z$, $R$ does not intersect $Z'$
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R \text{ intersects } Z, R \text{ does not intersect } Z'$
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R \text{ intersects } Z, R \text{ does not intersect } Z'$
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R \text{ intersects } Z, R \text{ does not intersect } Z'$
Step 3: Reduction to two clocks

Recall: $Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R$ intersects $Z$, $R$ does not intersect $Z'$
Step 3: Reduction to two clocks

Recall: \( Z \not\subseteq \text{Closure}_M(Z') \iff \exists R. R \text{ intersects } Z, R \text{ does not intersect } Z' \)

Theorem

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

\[ \text{Proj}_{xy}(Z) \not\subseteq \text{Closure}_M(\text{Proj}_{xy}(Z')) \]
Step 3: Reduction to two clocks

Theorem

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

\[ \text{Proj}_{xy}(Z) \not\subseteq \text{Closure}_M(\text{Proj}_{xy}(Z')) \]

Slightly modified edge-edge comparison is enough
Step 3: Reduction to two clocks

Theorem

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

Complexity: \( O(|X|^2) \), where \( X \) is the set of clocks
Step 3: Reduction to two clocks

Theorem

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

\[ \text{Proj}_{xy}(Z) \not\subseteq \text{Closure}_M(\text{Proj}_{xy}(Z')) \]

Same complexity as \( Z \subseteq Z' \)!
So what do we have now...

$q_3 = q_1 \land Z_3 \subseteq \text{Closure}_\alpha(Z_1)$?

Efficient algorithm for $Z \subseteq \text{Closure}_\alpha(Z')$
Overall algorithm

- **Store** concrete semantics: zones
- Compute $ZG(A)$: $Z \subseteq \text{Closure}_{\alpha'}(Z')$ for **termination**
Next lecture: $a_{\leq LU}$, optimality and benchmarks
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.

D. Dill.
Timing assumptions and verification of finite-state concurrent systems.

C. Daws and S. Tripakis.
Model checking of real-time reachability properties using abstractions.

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