Topics in Timed Automata

B. Srivathsan

RWTH-Aachen
Software modeling and Verification group
Correctness: Safety + Liveness + Fairness

\[ \neg \text{open}, \ x := 0 \]

\[ (x < 5), \ close \]

"Infinitely often, the gate is open for at least 5 s."

Realistic counter-examples: infinite non-Zeno runs
Lecture 8: Non-Zenoness
**Timed Büchi automata**

![Automaton Diagram]

- **Run:** infinite sequence of transitions

<table>
<thead>
<tr>
<th></th>
<th>$q_0$</th>
<th>$q_1$</th>
<th>$q_3$</th>
<th>$q_3$</th>
<th>$q_3$</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>0</td>
<td>0.4</td>
<td>0.9</td>
<td>1.2</td>
<td>2.0</td>
<td>...</td>
</tr>
<tr>
<td>$y$</td>
<td>0</td>
<td>0.4</td>
<td>0.5</td>
<td>0.8</td>
<td>1.6</td>
<td></td>
</tr>
</tbody>
</table>

- **accepting** if infinitely often green state
- **non-Zeno** if time diverges ($\sum_{i \geq 0} \delta_i \rightarrow \infty$)
Büchi non-emptiness problem

Given a TBA, does it have a non-Zeno accepting run

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

Theorem [AD94]

This problem is PSPACE-complete
No infinite run

No non-Zeno run
No infinite run

No non-Zeno run
\[ x \geq 4 \]

No infinite run

\[ x \leq 2 \]

No non-Zeno run

\[ x \leq 1 \]

Non-Zeno run \( \checkmark \)
How do we detect infinite non-Zeno runs given an automaton?
Abstract zone graphs again

\[ \text{ZG}^a(A) : (q_0, Z_0) \rightarrow (q_1, Z_1) \rightarrow (q_2, Z_2) \rightarrow \cdots \]

\[ A : (q_0, v_0) \rightarrow (q_1, v_1) \rightarrow (q_2, v_2) \rightarrow \cdots \]

Sound and complete [Tri09, Li09]

All the above abstractions preserve repeated state reachability
Abstract zone graphs again

\[
\begin{align*}
ZG^a(A) : &\quad (q_0, Z_0) \rightarrow (q_1, Z_1) \rightarrow (q_2, Z_2) \rightarrow \cdots \\
&\quad \psi \quad \psi \quad \psi \\
A : &\quad (q_0, v_0) \rightarrow (q_1, v_1) \rightarrow (q_2, v_2) \rightarrow \cdots
\end{align*}
\]

Sound and complete [Tri09, Li09]
All the above abstractions preserve **repeated state reachability**

What about **non-Zenoness**?
Time progress criterion [AD94]
\[ \wedge_{x \in X} \text{unbounded}(x) \lor \text{fluctuating}(x) \]

Region graph:

\[ (s_1, 0 = x < y) \rightarrow (s_0, 0 = x = y) \rightarrow (s_0, 0 = x = y) \rightarrow (s_2, 0 = y = x) - \rightarrow \]
Time progress criterion [AD94]

\( \forall x \in X \ \text{unbounded}(x) \lor \text{fluctuating}(x) \)

Region graph:

\[ (s_1, 0 = x < y) \rightarrow (s_0, 0 = x = y) \rightarrow (s_1, 0 = x = y) \rightarrow (s_2, 0 = y < x) \rightarrow \]

Zone graph with Extra\( ^+_M \):

\[ (s_0, 0 \leq x = y) \rightarrow (s_1, 0 \leq x \leq y) \rightarrow (s_0, 0 \leq x = y) \rightarrow (s_2, 0 \leq y \leq x) \rightarrow \]
The time progress criterion is not sound on zones.

**Region graph:**

\[
\begin{align*}
(s_0, 0 = x = y) &\rightarrow (s_1, 0 = x < y) \\
(s_1, 0 = x < y) &\rightarrow (s_0, 0 = x = y) \\
(s_0, 0 = x = y) &\rightarrow (s_2, 0 = y < x) \\
(s_2, 0 = y < x) &\rightarrow \end{align*}
\]

**Zone graph with Extra\(_M^+\):**

\[
\begin{align*}
(s_0, 0 \leq x = y) &\rightarrow (s_1, 0 \leq x \leq y) \\
(s_1, 0 \leq x \leq y) &\rightarrow (s_0, 0 \leq x = y) \\
(s_0, 0 \leq x = y) &\rightarrow (s_2, 0 \leq y \leq x) \\
(s_2, 0 \leq y \leq x) &\rightarrow \end{align*}
\]

**Zone graph with Extra\(_{LU}^+\):**

\[
\begin{align*}
(s_0, \top) &\rightarrow (s_1, \top) \\
(s_1, \top) &\rightarrow (s_0, \top) \\
(s_0, \top) &\rightarrow (s_2, \top) \\
(s_2, \top) &\rightarrow \end{align*}
\]
The time progress criterion is not sound on zones
From TBA to Strongly non-Zeno TBA

Key Idea: reduce non-Zenoness to Büchi acceptation
From TBA to Strongly non-Zeno TBA

Key Idea: reduce non-Zenoness to Büchi acceptation
From TBA to Strongly non-Zeno TBA

Key Idea: reduce non-Zenoness to Büchi acceptation
Adding a clock for non-Zenoness [TYB05]

\[ A' : \text{strongly non-Zeno TBA} \]
\[ |X| + 1 \text{ clocks and at most } 2 \cdot |Q| \text{ states} \]

**Theorem [TYB05]**

A has a non-Zeno accepting run iff \( ZG^a(A') \) has an **accepting** run.
Adding a clock for non-Zenoness [TYB05]

A' : strongly non-Zeno TBA

$|X| + 1$ clocks and at most $2 \cdot |Q|$ states

Theorem [TYB05]

A has a non-Zeno accepting run iff $ZG^a(A')$ has an accepting run

**Question**: Is this good enough?
Adding one clock leads to an exponential blowup in the zone graph! [HSW12]
Guard $t \geq 1$ Allows to Count...

Run of $V$: 2 different zones in $s_0$

$$\cdots (s_0, y \leq x_1 \leq x_2) \xrightarrow{y \leq d} (s_1, y \leq x_1 \leq x_2 \& y \leq d) \xrightarrow{\{x_1\}}$$

$$\cdots (s_0, 0 = x_1 \leq y \leq x_2) \xrightarrow{y \leq d} (s_1, x_1 \leq y \leq x_2 \& y \leq d) \xrightarrow{\{x_1\}}$$

$$\cdots (s_0, 0 = x_1 \leq y \leq x_2) \cdots$$
Guard $t \geq 1$ Allows to Count...

Run of $V'$: $d + 2$ different zones in $s_0$

\[
\cdots (s_0, y \leq x_1 \leq x_2 \leq t) \xrightarrow{(y \leq d) \& (t \geq 1), t := 0} \{x_1\} \\
(s_0, 0 = x_1 \leq t \leq y \leq x_2 \& y - t \geq 0) \xrightarrow{(y \leq d) \& (t \geq 1), t := 0} \{x_1\} \\
(s_0, 0 = x_1 \leq t \leq y \leq x_2 \& y - t \geq 1) \xrightarrow{(y \leq d) \& (t \geq 1), t := 0} \{x_1\} \\
(s_0, 0 = x_1 \leq t \leq y \leq x_2 \& y - t \geq 2) \xrightarrow{(y \leq d) \& (t \geq 1), t := 0} \{x_1\} \\
\cdots \\
(s_0, 0 = x_1 \leq t \leq y \leq x_2 \& y - t \geq d) \\
\]

Remark: $y - t \geq c$ implies $x_2 - x_1 \geq c$
...and Leads to a Combinatorial Explosion

\[
\begin{array}{c}
(y \leq d) \\
\downarrow \quad \quad \quad \downarrow \\
\{x_1\} \\
\vdots \\
\{x_{k-1}\}
\end{array}
\]

\[
\begin{array}{c}
V_k \\
\rightarrow \\
R_k \\
\rightarrow \\
A_n
\end{array}
\]

Lemma

\[ZG^a(A_n)\] has linear size in \(n\)

Key Idea: at \(V_k\) only two possible zones that collapse to the same zone after \(R_{k-1}\).
...and Leads to a Combinatorial Explosion

\[(y \leq d) \land (t \geq 1)\]

\[
\begin{align*}
&\{t\} \\
\Rightarrow & V'_k \\
\Rightarrow & R_k \\
\Rightarrow & V'_n \\
\Rightarrow & R_n \\
\Rightarrow & A'_n
\end{align*}
\]

Lemma

\[ZG^a(A'_n) \text{ has size exponential in } n\]

Key Idea: at \( V'_k \), \( \bigwedge_{i \in [k;n]} x_i - x_{i-1} \geq c_i \) with \( c_i \in [0;d] \) chosen non-deterministically
What we have:

- $\mathit{ZG}^a(A_n)$ has size $O(n)$
- $\mathit{ZG}^a(A'_n)$ has size $O(2^n)$

Coming next:

$A \mid \mathit{ZG}^a(A_n)\mid .O(|X|^2)$ algorithm [HSW12]
When does a path in \( ZG(A) \) yield only Zeno runs?

**Blocking clocks**

\( x \) never reset but checked for upper bound

**Zero-checks**

\( x \) and \( y \) should be 0 all along the path
Theorem

Blocking clocks can be detected in $|ZG_a(A)| \cdot (|X| + 1)$ time.
Blocking clocks

\[ x \leq 5 \]

\[ y \leq 2 \]

\[ z \leq 1 \]

Theorem: Blocking clocks can be detected in \( |ZG_a(A)| \cdot (|X| + 1) \) time.
Theorem

Blocking clocks can be detected in $|ZG_a(A)| \cdot (|X| + 1)$ time.
Blocking clocks can be detected in $|ZG_A| \cdot (|X| + 1)$ time.
Theorem

Blocking clocks can be detected in $|ZG_a(A)| \cdot (|X| + 1)$ time.
Theorem
Blocking clocks can be detected in $|ZG^a(A)| \cdot (|X| + 1)$ time
The case of zero checks

All states are in the scope of a zero check!

State $s_2$ is clear: all zero-checks are preceded by resets!
Zero-checks

\[ (x = 0) \]

Can time elapse here?
Zero-checks

Time can elapse at a node if every zero-check is preceded by a reset.
Zero-checks

Time can elapse at a node if every zero-check is \textbf{preceded} by a reset

Guessing Zone Graph ($GZG^a(A)$):

\[
(q, Z, Y) \xrightarrow{\{x\}} (q', Z', Y \cup \{x\})
\]

\[
(q, Z, Y) \xrightarrow{(x=0)} \text{enabled only if } x \in Y
\]

\[
(q, Z, Y) \xrightarrow{\tau} (q, Z, \emptyset)
\]
Zero checks (1st example)

\[ \{x\} \quad (y = 0) \]

\[ \{y\} \quad (x = 0) \]

\[ z_1 : (s_1, 0 = x \leq y) \]

\[ z_0 : (s_0, 0 = x = y) \]

\[ z_2 : (s_2, 0 = y \leq x) \]
Zero checks (1st example)

\[ z_1 : (s_1, 0 = x \leq y), \emptyset \]
\[ z_0 : (s_0, 0 = x = y), \emptyset \]
\[ z_2 : (s_2, 0 = y \leq x), \emptyset \]
Zero checks (1st example)

\[
\begin{align*}
  z_1 : (s_1, 0 = x \leq y), \emptyset \\
  z_0 : (s_0, 0 = x = y), \emptyset \\
  z_2 : (s_2, 0 = y \leq x), \emptyset \\
\end{align*}
\]
Zero checks (2nd example)

\[ z_2 : (s_2, 0 = x = y), \emptyset \]

\[ z_3 : (s_0, 0 = y \leq x), \emptyset \]

\[ z_4 : (s_1, 0 = x \leq y), \emptyset \]

\[ z_1 : (s_0, 0 = x = y), \emptyset \]
Theorem [HSW12]

A has a non-Zeno run iff there is an SCC in $GZG^a(A)$ that contains:

- an accepting node
- no blocking clocks
- a clear node $(q, Z, \emptyset)$

Complexity: $|GZG^a(A)| \cdot (|X| + 1)$
$2^{|X|}$ more nodes in $GZG^a(A)$ than in $ZG^a(A)$ due to $Y$ sets?
2^{|X|} more nodes in GZG^a(A) than in ZG^a(A) due to Y sets?

**Theorem**

- For each reachable node \((q, Z)\), \(Z\) entails a total order on \(X\).
- \(\text{Extra}_M, \text{Extra}^+_M\) preserve the order.
- \(Y\) respects this order; only \(|X| + 1\) sets needed.
2\(|X|\) more nodes in \(GZG^a(A)\) than in \(ZG^a(A)\) due to \(Y\) sets?

**Theorem**

- For each reachable node \((q, Z)\), \(Z\) entails a **total order** on \(X\).
- \(\text{Extra}_M, \text{Extra}_M^+\) preserve the order.
- \(Y\) respects this order; only \(|X| + 1\) sets needed.

**Extra\(_{LU}\), Extra\(_{LU}^+\) do not preserve order**

**Theorem [HS11]**

Non-Zenoness from LU-abstract zone graphs is **NP-complete**

**Theorem [HS11]**

A slight weakening of \(\text{Extra}_{LU}, \text{Extra}_{LU}^+\) preserves order
<table>
<thead>
<tr>
<th>$A$</th>
<th>$ZG^a(A)$</th>
<th>$ZG^a(A')$</th>
<th>$GZG^a(A)$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>size</td>
<td>size</td>
<td>otf</td>
</tr>
<tr>
<td>Train-Gate2 (mutex)</td>
<td>134</td>
<td>194</td>
<td>194</td>
</tr>
<tr>
<td>Train-Gate2 (bound. resp.)</td>
<td>988</td>
<td>227482</td>
<td>352</td>
</tr>
<tr>
<td>Train-Gate2 (liveness)</td>
<td>100</td>
<td>217</td>
<td>35</td>
</tr>
<tr>
<td>Fischer3 (mutex)</td>
<td>1837</td>
<td>3859</td>
<td>3859</td>
</tr>
<tr>
<td>Fischer4 (mutex)</td>
<td>46129</td>
<td>96913</td>
<td>96913</td>
</tr>
<tr>
<td>Fischer3 (liveness)</td>
<td>1315</td>
<td>4962</td>
<td>52</td>
</tr>
<tr>
<td>Fischer4 (liveness)</td>
<td>33577</td>
<td>147167</td>
<td>223</td>
</tr>
<tr>
<td>FDDI3 (liveness)</td>
<td>508</td>
<td>1305</td>
<td>44</td>
</tr>
<tr>
<td>FDDI5 (liveness)</td>
<td>6006</td>
<td>15030</td>
<td>90</td>
</tr>
<tr>
<td>FDDI3 (bound. resp.)</td>
<td>6252</td>
<td>41746</td>
<td>59</td>
</tr>
<tr>
<td>CSMA/CD4 (collision)</td>
<td>4253</td>
<td>7588</td>
<td>7588</td>
</tr>
<tr>
<td>CSMA/CD5 (collision)</td>
<td>45527</td>
<td>80776</td>
<td>80776</td>
</tr>
<tr>
<td>CSMA/CD4 (liveness)</td>
<td>3038</td>
<td>9576</td>
<td>1480</td>
</tr>
<tr>
<td>CSMA/CD5 (liveness)</td>
<td>32751</td>
<td>120166</td>
<td>8437</td>
</tr>
</tbody>
</table>

- Combinatorial explosion may **occur** in practice
- **Optimized** use of $GZG^a(A)$ gives best results
Conclusion

- Strongly non-Zeno construction can cause exponential blowup

- A guessing zone graph construction for non-Zenoness
Bibliography 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.

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

B. Bérard, B. Bouyer, and A. Petit.
Analysing the pgm protocol with UPPAAL.

Uppaal 4.0.

Kronos: a mode-checking tool for real-time systems.
Bibliography II

P. Bouyer.
Untameable timed automata!

P. Bouyer.
Forward analysis of updatable timed automata.

C. Courcoubetis and M. Yannakakis.
Minimum and maximum delay problems in real-time systems.

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.

Extended version: Using non-convex approximations for efficient analysis of timed automata.

R. Gómez and H. Bowman.
Efficient detection of zeno runs in timed automata.
M. Hendriks, G. Behrmann, K. G. Larsen, P. Niebert, and F. Vaandrager.
Adding symmetry reduction to Uppaal.

F. Herbreteau and B. Srivathsan.
Coarse abstractions make zeno behaviours difficult to detect.

K. Havelund, A. Skou, K. Larsen, and K. Lund.
Formal modeling and analysis of an audio/video protocol: An industrial case study using UPPAAL.

F. Herbreteau, B. Srivathsan, and I. Walukiewicz.
Efficient emptiness check for timed büchi automata.

Guided controller synthesis for climate controller using UPPAAL TiGA.

Guangyuan Li.
Checking timed büchi automata emptiness using lu-abstractions.

François Laroussinie and Ph. Schnoebelen.
The state explosion problem from trace to bisimulation equivalence.
S. Tripakis.
Verifying progress in timed systems.

S. Tripakis.
Checking timed büchi emptiness on simulation graphs.
ACM Transactions on Computational Logic, 10(3):??–??, 2009.

S. Tripakis, S. Yovine, and A. Bouajjani.
Checking timed büchi automata emptiness efficiently.

J. Zhao, X. Li, and G. Zheng.
A quadratic-time dbm-based successor algorithm for checking timed automata.