Probabilities in Timed Automata

Patricia Bouyer

LSV, CNRS, ENS Cachan, France

Based on joint works with Christel Baier (Dresden, Germany), Nathalie Bertrand (Rennes, France), Thomas Brihaye (Mons, Belgium), Marcus Größer (Dresden, Germany) and Nicolas Markey (Cachan, France)
Outline

1. Introduction

2. A probabilistic semantics for timed automata

3. Solving the qualitative model-checking problem

4. Towards solutions to the quantitative model-checking problem

5. Conclusion
Motivations

Our aim
Propose an alternative semantics to timed automata that measures how likely properties are satisfied.
Motivations

Our aim

Propose an alternative semantics to timed automata that measures how likely properties are satisfied.

→ Relax the idealized semantics of timed automata
Motivations

Our aim
Propose an alternative semantics to timed automata that measures how likely properties are satisfied.

→ Relax the idealized semantics of timed automata
  • Only few traces may violate/validate the correctness property, and they may moreover be due to assumptions made in timed automata, like infinite precision, instantaneous events, etc
Motivations

Our aim
Propose an alternative semantics to timed automata that measures how likely properties are satisfied.

→ Relax the idealized semantics of timed automata
  - Only few traces may violate/validate the correctness property, and they may moreover be due to assumptions made in timed automata, like infinite precision, instantaneous events, etc
  - Related works include robust semantics, implementability issues, etc
Motivations

Our aim
Propose an alternative semantics to timed automata that measures how likely properties are satisfied.

⇒ Relax the idealized semantics of timed automata
  ● Only few traces may violate/validate the correctness property, and they may moreover be due to assumptions made in timed automata, like infinite precision, instantaneous events, etc
  ● Related works include robust semantics, implementability issues, etc

⇒ Propose a new timed and probabilistic model
Motivations

Our aim
Propose an alternative semantics to timed automata that measures how likely properties are satisfied.

⇒ Relax the idealized semantics of timed automata
  - Only few traces may violate/validate the correctness property, and they may moreover be due to assumptions made in timed automata, like infinite precision, instantaneous events, etc
  - Related works include robust semantics, implementability issues, etc

⇒ Propose a new timed and probabilistic model
  - Related models include continuous-time Markov chains, but also probabilistic timed automata.
Initial example

**Intuition:** from the initial state,
this automaton *almost-surely* satisfies “\( G \text{ green} \)”
A maybe less intuitive example

\[
\begin{align*}
(x \leq 1) & \quad x \leq 1 \\
(x \leq 1) & \quad (x \leq 1) \\
x = 0 & \quad x = 1
\end{align*}
\]

Does it \textit{almost-surely} satisfy “G green”?
Outline

1. Introduction

2. A probabilistic semantics for timed automata

3. Solving the qualitative model-checking problem

4. Towards solutions to the quantitative model-checking problem

5. Conclusion
Our proposition

\[ \pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n}) : \text{symbolic path from } s \text{ firing edges } e_1, \ldots, e_n \]
Our proposition

- $\pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n})$: symbolic path from $s$ firing edges $e_1, \ldots, e_n$
- **Example:**

$$
\pi(s_0 \xrightarrow{e_1, e_2}) = \{ s_0 \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} s_2 \mid \tau_1 \leq 2, \tau_1 + \tau_2 \leq 5, \tau_2 \geq 1 \}
$$
Our proposition

- $\pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n})$: symbolic path from $s$ firing edges $e_1, \ldots, e_n$
- Example:

\[ \pi(s_0 \xrightarrow{e_1} e_2) = \{ s_0 \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} s_2 \mid \tau_1 \leq 2, \tau_1 + \tau_2 \leq 5, \tau_2 \geq 1 \} \]

Idea:

From state $s_0$: 

- randomly choose a delay
- then randomly select an edge
- then continue
Our proposition

- \( \pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n}) \): symbolic path from \( s \) firing edges \( e_1, \ldots, e_n \)
- Example:

\[
\pi(s_0 \xrightarrow{e_1} e_2) = \{ s_0 \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} s_2 | \tau_1 \leq 2, \tau_1 + \tau_2 \leq 5, \tau_2 \geq 1 \}
\]

Idea:

From state \( s_0 \):

- randomly choose a delay
Our proposition

- $\pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n})$: symbolic path from $s$ firing edges $e_1, \ldots, e_n$

Example:

$\pi(s_0 \xrightarrow{e_1} e_2) = \{s_0 \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} s_2 \mid \tau_1 \leq 2, \tau_1 + \tau_2 \leq 5, \tau_2 \geq 1\}$

Idea:

From state $s_0$:

- randomly choose a delay
- then randomly select an edge
Our proposition

\[ \pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n}) \text{: symbolic path from } s \text{ firing edges } e_1, \ldots, e_n \]

**Example:**

\[ \pi(s_0 \xrightarrow{e_1, e_2}) = \{ s_0 \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} s_2 \mid \tau_1 \leq 2, \tau_1 + \tau_2 \leq 5, \tau_2 \geq 1 \} \]

**Idea:**

From state \( s_0 \):

- randomly choose a delay
- then randomly select an edge
- then continue
Our proposition

Symbolic path: \( \pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{ s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \} \)

\[
\mathbb{P}\left( \pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) \right) = \int_{t \in I(s, e_1)} p_{s+t}(e_1) \mathbb{P}\left( \pi(s_{t}^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n}) \right) d\mu_s(t)
\]
Our proposition

Symbolic path: \( \pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n\} \)

\[ P(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \int_{t \in I(s, e_1)} p_{s+t}(e_1) P(\pi(s_t \xrightarrow{e_2} \cdots \xrightarrow{e_n})) \, d\mu_s(t) \]

- \( l(s, e_1) = \{\tau \mid s \xrightarrow{\tau, e_1}\} \) and \( \mu_s \) distribution over \( l(s) = \bigcup_e l(s, e) \)
Our proposition

Symbolic path: \( \pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{ s \xrightarrow{\tau_1,e_1} s_1 \cdots \xrightarrow{\tau_n,e_n} s_n \} \)

\[
P(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \int_{t \in I(s,e_1)} p_{s+t}(e_1) P(\pi(s_t \xrightarrow{e_2} \cdots \xrightarrow{e_n})) \, d\mu_s(t)
\]

- \( I(s, e_1) = \{ \tau \mid s \xrightarrow{\tau,e_1} \} \) and \( \mu_s \) distribution over \( I(s) = \bigcup_e I(s, e) \)
- \( p_{s+t} \) distribution over transitions enabled in \( s + t \)
  (given by weights on transitions)
Our proposition

Symbolic path: \( \pi(s^{e_1} \rightarrow \cdots \rightarrow e_n) = \{s^{\tau_1,e_1} \rightarrow s_1 \cdots \rightarrow s_n\} \)

\[
P(\pi(s^{e_1} \rightarrow \cdots \rightarrow e_n)) = \int_{t \in l(s,e_1)} p_{s+t}(e_1) P(\pi(s_t^{e_1} \rightarrow \cdots \rightarrow e_n)) \, d\mu_s(t)
\]

- \( l(s, e_1) = \{\tau \mid s^{\tau,e_1}\} \) and \( \mu_s \) distribution over \( l(s) = \bigcup_e l(s, e) \)
- \( p_{s+t} \) distribution over transitions enabled in \( s + t \)
  (given by weights on transitions)
- \( s^t \rightarrow s + t^{e_1} \rightarrow s_t^{e_1} \)
Our proposition

Symbolic path: $\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1,e_1} s_1 \cdots \xrightarrow{\tau_n,e_n} s_n\}$

- $I(s, e_1) = \{\tau \mid s \xrightarrow{\tau,e_1}\}$ and $\mu_s$ distribution over $I(s) = \bigcup_e I(s, e)$
- $p_{s+t}$ distribution over transitions enabled in $s + t$
  (given by weights on transitions)
- $s \xrightarrow{t} s + t \xrightarrow{e_1} s_t^{e_1}$
Our proposition

\[ \mathbb{P}(\pi_1 s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) = \int_{t \in I(s,e_1)} p_{s+t}(e_1) \mathbb{P}(\pi(s_t^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n} )) \, d\mu_s(t) \]
Our proposition

\[ \mathbb{P}\left(\pi(s^{e_1} \rightarrow \cdots \rightarrow e_n)\right) = \int_{t \in I(s, e_1)} p_{s+t}(e_1) \mathbb{P}\left(\pi(s_t^{e_1} \rightarrow \cdots \rightarrow e_n)\right) \, d\mu_s(t) \]

- Can be viewed as an \( n \)-dimensional integral
Our proposition

\[
P(\pi(s^{e_1} \cdots e_n)) = \int_{t \in I(s,e_1)} p_{s+t}(e_1) P(\pi(s_{t}^{e_1} e_2 \cdots e_n)) \, d\mu_s(t)
\]

- Can be viewed as an \(n\)-dimensional integral
- Easy extension to constrained symbolic paths

\[
\pi_C(s^{e_1} \cdots e_n) = \{s^{\tau_1, e_1} \cdots \tau_n, e_n} s_n | (\tau_1, \cdots, \tau_n) \models C\}
\]
Our proposition

\[
\mathbb{P}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) = \int_{t \in I(s,e_1)} p_{s+t}(e_1) \mathbb{P}(\pi(s_t \xrightarrow{e_2} \cdots \xrightarrow{e_n} )) \, d\mu_s(t)
\]

- Can be viewed as an \( n \)-dimensional integral

- Easy extension to constrained symbolic paths

\[
\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ) = \{ s \xrightarrow{\tau_1,e_1} s_1 \cdots \xrightarrow{\tau_n,e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models C\}
\]

- Definition over sets of infinite runs:
Our proposition

\[ \mathbb{P}(\pi(s \overset{e_1}{\rightarrow} \cdots \overset{e_n}{\rightarrow})) = \int_{t \in I(s, e_1)} p_{s+t}(e_1) \mathbb{P}(\pi(s_t \overset{e_2}{\rightarrow} \cdots \overset{e_n}{\rightarrow})) \, d\mu_s(t) \]

- Can be viewed as an \( n \)-dimensional integral
- Easy extension to constrained symbolic paths
  \[ \pi_C(s \overset{e_1}{\rightarrow} \cdots \overset{e_n}{\rightarrow}) = \{ s \overset{\tau_1, e_1}{\rightarrow} s_1 \cdots \overset{\tau_n, e_n}{\rightarrow} s_n \mid (\tau_1, \cdots, \tau_n) \models C \} \]
- Definition over sets of infinite runs:
  - \( \text{Cyl}(\pi_C(s \overset{e_1}{\rightarrow} \cdots \overset{e_n}{\rightarrow})) = \{ \varrho \cdot \varrho' \mid \varrho \in \pi_C(s \overset{e_1}{\rightarrow} \cdots \overset{e_n}{\rightarrow}) \} \)
Our proposition

\[
P(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) = \int_{t \in l(s,e_1)} p_{s+t}(e_1) P(\pi(s_t \xrightarrow{e_2} \cdots \xrightarrow{e_n} )) \, d\mu_s(t)
\]

- Can be viewed as an \(n\)-dimensional integral
- Easy extension to constrained symbolic paths

\[
\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ) = \{s \xrightarrow{\tau_1,e_1} s_1 \cdots \xrightarrow{\tau_n,e_n} s_n \mid (\tau_1,\cdots,\tau_n) \models C\}
\]

- Definition over sets of infinite runs:
  - \(\text{Cyl}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) = \{\varrho \cdot \varrho' \mid \varrho \in \pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )\}\)
  - \(P(\text{Cyl}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ))) = P(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ))\)
Our proposition

\[ P(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) = \int_{t \in I(s, e_1)} p_{s+t}(e_1) P(\pi(s_{t}^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n} )) \, d\mu_s(t) \]

- Can be viewed as an \( n \)-dimensional integral

- Easy extension to constrained symbolic paths

\[ \pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ) = \{ s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models C \} \]

- Definition over sets of infinite runs:
  - \( \text{Cyl}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) = \{ \varrho \cdot \varrho' \mid \varrho \in \pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ) \} \)
  - \( P(\text{Cyl}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ))) = P(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) \)
  - unique extension of \( P \) to the generated \( \sigma \)-algebra
Our proposition

\[ \mathbb{P}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) = \int_{t \in I(s,e_1)} p_{s+t}(e_1) \mathbb{P}(\pi(s_1^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n} )) \, d\mu_s(t) \]

- Can be viewed as an \(n\)-dimensional integral

- Easy extension to constrained symbolic paths

\[ \pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models C \}\]

- Definition over sets of infinite runs:
  - \( \text{Cyl}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) = \{\varrho \cdot \varrho' \mid \varrho \in \pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )\} \)
  - \( \mathbb{P}(\text{Cyl}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ))) = \mathbb{P}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) \)
  - unique extension of \( \mathbb{P} \) to the generated \(\sigma\)-algebra

- Property: \( \mathbb{P} \) is a probability measure over sets of infinite runs
A probabilistic semantics for timed automata

Our proposition

\[ \mathbb{P}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \int_{t \in I(s,e_1)} p_{s+t}(e_1) \mathbb{P}(\pi(s_t \xrightarrow{e_2} \cdots \xrightarrow{e_n})) \, d\mu_s(t) \]

- Can be viewed as an \textit{n}-dimensional integral

- Easy extension to constrained symbolic paths

\[ \pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1,e_1} s_1 \cdots \xrightarrow{\tau_n,e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models C\} \]

- Definition over sets of infinite runs:
  - \( \text{Cyl}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \{\rho \cdot \rho' \mid \rho \in \pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\} \)
  - \( \mathbb{P}(\text{Cyl}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))) = \mathbb{P}(\pi_C(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) \)
  - unique extension of \( \mathbb{P} \) to the generated \( \sigma \)-algebra

- Property: \( \mathbb{P} \) is a probability measure over sets of infinite runs

- Example:

\[ \text{Zeno}(s) = \bigcup_{M \in \mathbb{N}} \bigcap_{n \in \mathbb{N}} \bigcup_{(e_1, \cdots, e_n) \in E^n} \text{Cyl}(\pi_{\Sigma_i \tau_i \leq M}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) \]
An example of computation (with uniform distributions)

The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1} e_2)$ is $\frac{1}{4}$. 
An example of computation (with uniform distributions)

The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1} e_2)$ is $\frac{1}{4}$.

$$
\mathbb{P}(\pi(s_0 \xrightarrow{e_1} e_2)) = \int_0^1 \mathbb{P}(\pi(s_1 \xrightarrow{e_2})) d\mu_{s_0}(t) + \int_1^1 \frac{\mathbb{P}(\pi(s_1 \xrightarrow{e_2}))}{2} d\mu_{s_0}(t)
$$

$$
= \int_0^1 \int_0^1 \left( \frac{\mathbb{P}(\pi(s_2))}{2} d\mu_{s_1}(u) \right) d\mu_{s_0}(t)
$$

$$
= \int_0^1 \int_0^1 \left( \frac{1}{2} \frac{du}{2} \right) dt = \frac{1}{4}
$$
Back to the first example

\[
\begin{align*}
&x \leq 10 \\
&x = 1
\end{align*}
\]
Back to the first example

\[
P(\pi(s_0 \xrightarrow{e_1} e_2)) = 1
\]
Back to the first example

\[ \Pr(\pi(s_0 \xrightarrow{e_1} e_2)) = 1 \]

\[ \Pr(\pi(s_0 \xrightarrow{e_1} e_3)) = 0 \]
Back to the first example

\[
\begin{align*}
P(\pi(s_0 \xrightarrow{e_1} e_2) & = 1 \\
P(\pi(s_0 \xrightarrow{e_1} e_3) & = 0 \\
P(G \text{ green}) & = 1
\end{align*}
\]
Back to the second example

\[ (x \leq 1) \]

\[ (x \leq 1) \]

\[ x = 0 \quad e_2 \]

\[ x = 1 \quad e_3 \]

\[ x = 0 \quad e_2 \]

\[ x = 1 \quad e_3 \]

\[ (x \leq 1) \]

\[ P \in \pi (s_0 e_1 \rightarrow e_2 \rightarrow) \]

\[ P \in \pi (s_0 e_1 \rightarrow e_3 \rightarrow) \]

\[ \pi = 0 \]

\[ \pi = 1 \]
Back to the second example

\[\mathbb{P}(\pi(s_0 \xrightarrow{e_1} e_2)) = 0\]
Back to the second example

\[ (x \leq 1) \]

\[ (x \leq 1) \]

\[ e_1 \]

\[ e_2 \]

\[ x = 0 \]

\[ e_3 \]

\[ x = 1 \]

\[ P(\pi(s_0 \xrightarrow{e_1} s_0 \xrightarrow{e_2} )) = 0 \]

\[ P(\pi(s_0 \xrightarrow{e_1} s_0 \xrightarrow{e_3} )) = 1 \]
Back to the second example

\[ x \leq 1 \]

\[ P(\pi(s_0 \xrightarrow{e_1} e_2)) = 0 \]

\[ P(\pi(s_0 \xrightarrow{e_1} e_3)) = 1 \]

\[ P(\text{G green}) = 1 \]
Almost-sure satisfaction

If \( \varphi \) is an LTL (or \( \omega \)-regular) property,

\[
\begin{align*}
\models s \varphi \quad & \overset{\text{def}}{\iff} \quad P\left(\{ \varrho \in \text{Runs}(s) \mid \varrho \models \varphi \}\right) = 1 \\
& \overset{\text{def}}{=} P(s \models \varphi)
\end{align*}
\]
Almost-sure satisfaction

If $\varphi$ is an LTL (or $\omega$-regular) property,

$$s \models \varphi \iff \mathbb{P}(\{q \in \text{Runs}(s) \mid q \models \varphi\}) = 1$$

Qualitative model-checking question: $s \models \varphi$?
Outline

1. Introduction

2. A probabilistic semantics for timed automata

3. Solving the qualitative model-checking problem

4. Towards solutions to the quantitative model-checking problem

5. Conclusion
An example

\[ \ell_0, x \leq 1 \]
\[ e_1, x \leq 1 \]
\[ e_2, x \leq 1 \]
\[ x \leq 1 \]
\[ e_3, x = 1 \]

\[ \ell_1 \]
\[ e_4, x \geq 3, x := 0 \]
\[ e_5, x \leq 1 \]

\[ \ell_2 \]
\[ e_6, x = 0 \]
\[ e_7, x \leq 1 \]
\[ \ell_3 \]

\[ x \leq 1 \]

Indeed, almost surely, paths are of the form \( e^*_1 e_2 e_4 e_5 e_6 e_7 \).
An example

\[ e_1, x \leq 1 \]
\[ e_2, x \leq 1 \]
\[ e_3, x = 1 \]
\[ e_4, x \geq 3, x := 0 \]
\[ e_5, x \leq 1 \]
\[ e_6, x = 0 \]
\[ e_7, x \leq 1 \]

\[ \mathcal{A} \not\models G(\text{green} \Rightarrow F \text{ red}) \]
An example

\[ e_1, \ x \leq 1 \]
\[ e_2, \ x \leq 1 \]
\[ e_3, \ x = 1 \]
\[ e_4, \ x \geq 3, \ x := 0 \]
\[ e_5, \ x \leq 1 \]
\[ e_6, \ x = 0 \]
\[ e_7, \ x \leq 1 \]

\[ A \not\models G(\text{green} \Rightarrow F \text{ red}) \quad \text{but} \quad A \models G(\text{green} \Rightarrow F \text{ red}) \]
An example

Indeed, almost surely, paths are of the form $e_1^* e_2 (e_4 e_5)^\omega$
The classical region automaton

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,1 \xrightarrow{e_1, e_2} \ell_1,0 \xrightarrow{e_2} \ell_1,1 \xrightarrow{e_3} \ell_0,1 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2, e_4} \ell_1,1 \xrightarrow{e_3} \ell_0,1 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2, e_5} \ell_2,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_2,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]

\[ \ell_0,0 \xrightarrow{e_1} \ell_0,(0,1) \xrightarrow{e_1, e_2} \ell_1,(0,1) \xrightarrow{e_2} \ell_3,0 \]
The pruned region automaton

\[ \ell_0,0, \ell_0,0, (0,1), \ell_0,0, 1, \ell_3,0, \ell_3,0, (0,1), \ell_3,0, 1 \]

... viewed as a finite Markov chain $MC(A)$

**Theorem**

For single-clock timed automata, $A \approx \varphi$ iff $P(MC(A) | = \varphi) = 1$.
The pruned region automaton
The pruned region automaton

... viewed as a finite Markov chain $MC(A)$
The pruned region automaton

\[ \ell_0, 0 \leftarrow e_1 \rightarrow \ell_0, (0, 1) \leftarrow e_2 \rightarrow \ell_1, (0, 1) \leftarrow e_5 \rightarrow \ell_2, 0 \]

... viewed as a finite Markov chain \( MC(A) \)

**Theorem**

For single-clock timed automata,

\[ A \models \varphi \text{ iff } P(MC(A) \models \varphi) = 1 \]
Result

Theorem
For single-clock timed automata, the almost-sure model-checking
- of LTL is PSPACE-Complete
- of $\omega$-regular properties is NLOGSPACE-Complete
Result

Theorem

For single-clock timed automata, the almost-sure model-checking

- of LTL is PSPACE-Complete
- of \( \omega \)-regular properties is NLOGSPACE-Complete

Complexity:

- size of single-clock region automata = polynomial \([LMS04]\)
- apply result of \([CSS03]\) to the finite Markov chain

Correctness: the proof is rather involved

- requires the definition of a topology over the set of paths
- notions of largeness (for proba 1) and meagerness (for proba 0)
- link between probabilities and topology thanks to the topological games called Banach-Mazur games
An example with two clocks

If the previous algorithm was correct,

However, we can prove that

There is a strange convergence phenomenon: along an execution, if $\delta_i > 0$ is the delay in location $\ell_4$, then we have that $P_i \delta_i \leq 18/29$
An example with two clocks

If the previous algorithm was correct, $\mathcal{A} \models GF \text{ red} \land GF \text{ green}$
An example with two clocks

- If the previous algorithm was correct, $\mathcal{A} \models GF \text{ red} \land GF \text{ green}$
- However, we can prove that $P(G \neg \text{red}) > 0$
An example with two clocks

- If the previous algorithm was correct, $\mathcal{A} \models \mathbf{G} \mathbf{F} \text{ red} \land \mathbf{G} \mathbf{F} \text{ green}$

- However, we can prove that $\mathbb{P}(\mathbf{G} \neg\text{red}) > 0$

- There is a strange convergence phenomenon: along an execution, if $\delta_i > 0$ is the delay in location $\ell_4$, then we have that $\sum_i \delta_i \leq 1$
A note on Zeno behaviours

- The set of Zeno behaviours is measurable:

\[
\text{Zeno}(s) = \bigcup_{M \in \mathbb{N}} \bigcap_{n \in \mathbb{N}} \bigcup_{(e_1, \ldots, e_n) \in E^n} \text{Cyl}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} ))
\]
A note on Zeno behaviours

- The set of Zeno behaviours is measurable:
  \[ \text{Zeno}(s) = \bigcup_{M \in \mathbb{N}} \bigcap_{n \in \mathbb{N}} \bigcup_{(e_1, \ldots, e_n) \in E^n} \text{Cyl}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n} )) \]

- In single-clock timed automata, we can decide in NLOGSPACE whether \( P(\text{Zeno}(s)) = 0 \):
A note on Zeno behaviours

- The set of Zeno behaviours is measurable:
  \[ \text{Zeno}(s) = \bigcup_{M \in \mathbb{N}} \bigcap_{n \in \mathbb{N}} \bigcup_{(e_1, \ldots, e_n) \in E^n} \text{Cyl}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) \]

- In single-clock timed automata, we can decide in NLOGSPACE whether \( P(\text{Zeno}(s)) = 0 \):
  - check whether there is a purely Zeno BSCC in \( MC(A) \)
A note on Zeno behaviours

- The set of Zeno behaviours is measurable:
  \[ \text{Zeno}(s) = \bigcup_{M \in \mathbb{N}} \bigcap_{n \in \mathbb{N}} \bigcup_{(e_1, \ldots, e_n) \in E^n} \text{Cyl}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) \]

- In single-clock timed automata, we can decide in NLOGSPACE whether \( P(\text{Zeno}(s)) = 0 \):
  - check whether there is a purely Zeno BSCC in \( MC(A) \)

- an interesting notion of non-Zeno timed automata

\[ x \leq 1, \ x := 0 \]
Outline

1. Introduction

2. A probabilistic semantics for timed automata

3. Solving the qualitative model-checking problem

4. Towards solutions to the quantitative model-checking problem

5. Conclusion
Quantitative model-checking

How likely an automaton will satisfy a property?
I.e., what is the value $P(s \models \varphi)$?
Towards quantitative analysis

- The abstraction $MC(A)$ is no more correct.
Towards quantitative analysis

- The abstraction $MC(\mathcal{A})$ is no more correct.
- Can be reduced to solving a system of differential equations.
Towards quantitative analysis

- The abstraction $MC(A)$ is no more correct.
- Can be reduced to solving a system of differential equations.
  - hard to solve in general, even for simple distributions.
Towards quantitative analysis

- The abstraction $MC(A)$ is no more correct.
- Can be reduced to solving a system of differential equations. ⚠️ hard to solve in general, even for simple distributions
- We will describe a restricted framework in which:
Towards quantitative analysis

- The abstraction \( MC(\mathcal{A}) \) is no more correct.

- Can be reduced to solving a system of differential equations. 
  It is hard to solve in general, even for simple distributions.

- We will describe a restricted framework in which:
  - we will compute a closed-form expression for the probability.
Towards quantitative analysis

- The abstraction $MC(\mathcal{A})$ is no more correct.
- Can be reduced to solving a system of differential equations. It is hard to solve in general, even for simple distributions.
- We will describe a restricted framework in which:
  - we will compute a closed-form expression for the probability
  - we will be able to approximate the probability
Towards quantitative analysis

- The abstraction $MC(A)$ is no more correct.

- Can be reduced to solving a system of differential equations. It is hard to solve in general, even for simple distributions.

- We will describe a restricted framework in which:
  - we will compute a closed-form expression for the probability
  - we will be able to approximate the probability, i.e., for every $\varepsilon > 0$, we will compute two rationals $p^-\varepsilon$ and $p^+\varepsilon$ such that:

\[
\begin{cases}
  p^-\varepsilon \leq P(s_0 \models \varphi) \leq p^-\varepsilon + \varepsilon \\
  p^+\varepsilon - \varepsilon \leq P(s_0 \models \varphi) \leq p^+\varepsilon
\end{cases}
\]
Towards quantitative analysis

- The abstraction \( MC(\mathcal{A}) \) is no more correct.

- Can be reduced to solving a system of differential equations. It is hard to solve in general, even for simple distributions.

- We will describe a restricted framework in which:
  - we will compute a closed-form expression for the probability
  - we will be able to approximate the probability, i.e., for every \( \varepsilon > 0 \), we will compute two rationals \( p^-_\varepsilon \) and \( p^+_\varepsilon \) such that:
    \[
    \begin{align*}
    p^-_\varepsilon & \leq P(s_0 \models \phi) \leq p^-_\varepsilon + \varepsilon \\
    p^+_\varepsilon - \varepsilon & \leq P(s_0 \models \phi) \leq p^+_\varepsilon
    \end{align*}
    \]
  - we will be able to decide the threshold problem
Towards quantitative analysis

- The abstraction $MC(\mathcal{A})$ is no more correct.
- Can be reduced to solving a system of differential equations. It is hard to solve in general, even for simple distributions.
- We will describe a restricted framework in which:
  - we will compute a closed-form expression for the probability
  - we will be able to approximate the probability, i.e., for every $\varepsilon > 0$, we will compute two rationals $p_\varepsilon^-$ and $p_\varepsilon^+$ such that:
    \[
    \begin{cases}
    p_\varepsilon^- \leq \mathbb{P}(s_0 \models \varphi) \leq p_\varepsilon^- + \varepsilon \\
    p_\varepsilon^+ - \varepsilon \leq \mathbb{P}(s_0 \models \varphi) \leq p_\varepsilon^+
    \end{cases}
    \]
  - we will be able to decide the threshold problem:
    “Given $\mathcal{A}$, $\varphi$, $c \in \mathbb{Q}$, and $\sim \in \{<, \leq, =, \geq, >\}$, does $\mathbb{P}(s_0 \models \varphi) \sim c$ in $\mathcal{A}$?”
An example

\[\ell_0 \xrightarrow{x \leq 1} \ell_1 \xrightarrow{x \leq 1} \ell_0 \]
\[\ell_1 \xrightarrow{x \leq 1} \ell_2 \xrightarrow{x \leq 1} \ell_1 \]
\[\ell_2 \xrightarrow{x \leq 1} \ell_3 \xrightarrow{x \leq 1} \ell_2 \]
\[\ell_3 \xrightarrow{x \leq 1} \ell_0 \xrightarrow{x \leq 1} \ell_3 \]

\[e_1, x \leq 1, x := 0 \]
\[e_2, x \leq 1 \]
\[e_3, x \leq 2, x := 0 \]
\[e_4, x \geq 2, x := 0 \]
\[e_5, x \leq 2 \]
\[e_6, x = 0 \]
\[e_7 \]

+ distributions \( \mu_s : t \mapsto e^{-t} \) when \( I(s) = \mathbb{R}_+ \)
+ \( \mu_s \) uniform distribution when \( I(s) \) is bounded
+ uniform weights on transitions
An example

Towards solutions to the quantitative model-checking problem

$\ell_0, x \leq 1, x := 0$

$e_2, x \leq 1$

$x \leq 1$

$\ell_1, x \leq 2, x := 0$

$\ell_2, x \leq 2$

$\ell_3, x \leq 2$

$e_4, x \geq 2, x := 0$

$e_5, x \leq 2$

$e_6, x = 0$

$e_7$

$+$ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$

$\mu_s$ uniform distribution when $I(s)$ is bounded

$+$ uniform weights on transitions

We construct a finite Markov chain $MC'(A)$ with macro-edges:
An example

$$\begin{align*}
el_0, \ x \leq 1, \ x := 0 \\
e_2, \ x \leq 1 \\
e_4, \ x \geq 2, \ x := 0 \\
e_6, \ x := 0 \\
el_1, \ x \leq 1 \\
e_3, \ x \leq 2, \ x := 0 \\
e_5, \ x \leq 2 \\
el_2, \ x \leq 2 \\
el_3 \\
el_7
\end{align*}$$

+ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$

$\mu_s$ uniform distribution when $I(s)$ is bounded

+ uniform weights on transitions

We construct a finite Markov chain $MC'(A)$ with macro-edges:
An example

\[ \ell_0, x \leq 1, x := 0 \]
\[ \ell_1, \quad e_2, \quad x \leq 1 \]
\[ \ell_2, \quad e_4, \quad x \geq 2, \quad x := 0 \]
\[ \ell_3, \quad e_6, \quad x = 0 \]
\[ e_7 \]

+ distributions \( \mu_s : t \mapsto e^{-t} \) when \( I(s) = \mathbb{R}_+ \)
+ \( \mu_s \) uniform distribution when \( I(s) \) is bounded
+ uniform weights on transitions

We construct a finite Markov chain \( MC'(A) \) with macro-edges:
An example

We construct a finite Markov chain $MC'(A)$ with macro-edges:

$\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$

$\mu_s$ uniform distribution when $I(s)$ is bounded

+ uniform weights on transitions
An example

\[ e_1, \ x \leq 1, \ x := 0 \]
\[ e_2, \ x \leq 1 \]
\[ e_3, \ x \leq 2, \ x := 0 \]
\[ e_4, \ x \geq 2, \ x := 0 \]
\[ e_5, \ x \leq 2 \]
\[ e_6, \ x = 0 \]
\[ e_7 \]

+ distributions \( \mu_s : t \mapsto e^{-t} \) when \( I(s) = \mathbb{R}^+ \)
+ \( \mu_s \) uniform distribution when \( I(s) \) is bounded
+ uniform weights on transitions

We construct a finite Markov chain \( MC'(A) \) with macro-edges:
An example

+ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
+ $\mu_s$ uniform distribution when $I(s)$ is bounded
+ uniform weights on transitions

We construct a finite Markov chain $MC'(A)$ with macro-edges:
Towards solutions to the quantitative model-checking problem

An example

\[ e_1, \ x \leq 1, \ x := 0 \]
\[ e_2, \ x \leq 1 \]
\[ e_3, \ x \leq 2, \ x := 0 \]
\[ e_4, \ x \geq 2, \ x := 0 \]
\[ e_5, \ x \leq 2 \]
\[ e_6, \ x = 0 \]
\[ e_7 \]

+ distributions \( \mu_s : t \mapsto e^{-t} \) when \( I(s) = \mathbb{R}^+ \)
\( \mu_s \) uniform distribution when \( I(s) \) is bounded
+ uniform weights on transitions

We construct a finite Markov chain \( MC'(A) \) with macro-edges:
Towards solutions to the quantitative model-checking problem

An example

\[ \ell_0, x \leq 1, x := 0 \rightarrow \ell_1, x \leq 1, x := 0 \]
\[ \ell_1, x \leq 1, x := 0 \rightarrow \ell_2, x \leq 2, x := 0 \]
\[ \ell_2, x \leq 2, x := 0 \rightarrow \ell_3, x = 0 \]
\[ \ell_0, x \leq 1, x := 0 \rightarrow \ell_1, e_2, x \leq 1 \]
\[ \ell_1, x \leq 1, x := 0 \rightarrow \ell_2, e_4, x \geq 2, x := 0 \]
\[ \ell_2, x \leq 2, x := 0 \rightarrow \ell_3, e_5, x \leq 2 \]
\[ \ell_3, x = 0 \rightarrow \ell_0, e_6, x = 0 \]

+ distributions \( \mu_s : t \mapsto e^{-t} \) when \( I(s) = \mathbb{R}_+ \)
   \( \mu_s \) uniform distribution when \( I(s) \) is bounded
+ uniform weights on transitions

We construct a finite Markov chain \( MC'(A) \) with macro-edges:
An example

\[ \ell_0, \ x \leq 1, \ x = 0 \quad e_2, \ x \leq 1 \quad e_4, \ x \geq 2, \ x = 0 \quad e_6, \ x = 0 \]

\[ \ell_1, \ x \leq 2, \ x = 0 \quad e_5, \ x \leq 2 \quad x \leq 2 \]

\[ \ell_2, \ x \leq 2 \quad e_7 \]

\[ e_1, \ x \leq 1, \ x = 0 \]

+ distributions \( \mu_s : t \mapsto e^{-t} \) when \( I(s) = \mathbb{R}_+ \)

\( \mu_s \) uniform distribution when \( I(s) \) is bounded

+ uniform weights on transitions

We construct a finite Markov chain \( MC'(A) \) with macro-edges:

\[ e_1, \frac{1}{2} \cdot (1 - e^{-2}) \]

\[ e_2 e_4, e_2, e_4 \]

\[ e_3, e_3, e_5, e_3 \]

\[ e_5 e_3, e_5 e_4, e_5, e_4 \]

\[ e_6 e_7, e_6 e_7, e_6, e_7 \]

\[ e_7, 1 \]
An example

We construct a finite Markov chain $MC'(A)$ with macro-edges:
Correctness of the abstraction

Theorem
Under some hypotheses, for single-clock automaton $\mathcal{A}$ and property $\varphi$,

$$P_{\mathcal{A}}(s_0 \models \varphi) = P_{MC'(\mathcal{A})}(s_0 \models \Diamond F_{\varphi})$$

for some well-chosen set $F_{\varphi}$. 
Correctness of the abstraction

**Theorem**

Under some hypotheses, for single-clock automaton $\mathcal{A}$ and property $\varphi$,

$$\mathbb{P}_\mathcal{A}(s_0 \models \varphi) = \mathbb{P}_{MC'}(\mathcal{A})(s_0 \models \diamond F \varphi)$$

for some well-chosen set $F \varphi$.

- **Hypotheses:**
  - if $s = (\ell, \alpha)$ and $s' = (\ell, \alpha')$ with $\alpha, \alpha' > M$, $\mu_s = \mu_{s'}$
  - every bounded cycle resets the clock
Correctness of the abstraction

Theorem

Under some hypotheses, for single-clock automaton $\mathcal{A}$ and property $\varphi$,

$$\mathbb{P}_{\mathcal{A}}(s_0 \models \varphi) = \mathbb{P}_{MC'(\mathcal{A})}(s_0 \models \Diamond F_{\varphi})$$

for some well-chosen set $F_{\varphi}$.

- **Hypotheses:**
  - if $s = (\ell, \alpha)$ and $s' = (\ell, \alpha')$ with $\alpha, \alpha' > M$, $\mu_s = \mu_{s'}$
  - every bounded cycle resets the clock

- **Limits of the abstraction:** there may be no closed form for the values labelling the edges of $MC'(\mathcal{A})$. 
We assume furthermore that:

- for every state \( s \), \( I(s) = \mathbb{R}_+ \)
  
  (the timed automaton is ‘reactive’)
Computing the probability

- We assume furthermore that:
  - for every state $s$, $I(s) = \mathbb{R}_+$
    (the timed automaton is ‘reactive’)
  - in every location $\ell$, the distribution over delays has density $t \mapsto \lambda_\ell \cdot e^{-\lambda_\ell \cdot t}$ for some $\lambda_\ell \in \mathbb{Q}_+$
Computing the probability

- We assume furthermore that:
  - for every state \( s \), \( I(s) = \mathbb{R}_+ \)
    (the timed automaton is ‘reactive’)
  - in every location \( \ell \), the distribution over delays has density
    \[ t \mapsto \lambda_\ell \cdot e^{-\lambda_\ell \cdot t} \]
    for some \( \lambda_\ell \in \mathbb{Q}_+ \)

- more general than continuous-time Markov chains [BHHK03]
Towards solutions to the quantitative model-checking problem

Computing the probability

- We assume furthermore that:
  - for every state $s$, $I(s) = \mathbb{R}_+$
    (the timed automaton is ‘reactive’)
  - in every location $\ell$, the distribution over delays has density
    $t \mapsto \lambda_\ell \cdot e^{-\lambda_\ell \cdot t}$ for some $\lambda_\ell \in \mathbb{Q}_+$

  more general than continuous-time Markov chains [BHHK03]

Proposition

Under those hypotheses, $\mathbb{P}(s_0 \models \varphi)$ can be expressed as $f(e^{-r})$ where $r$ is a rational number, and $f \in \mathbb{Q}(X)$ is a rational function.
Towards solutions to the quantitative model-checking problem

Computing the probability

- We assume furthermore that:
  - for every state $s$, $I(s) = \mathbb{R}_+$
    (the timed automaton is ‘reactive’)
  - in every location $\ell$, the distribution over delays has density $t \mapsto \lambda_\ell \cdot e^{-\lambda_\ell \cdot t}$ for some $\lambda_\ell \in \mathbb{Q}_+$
    - more general than continuous-time Markov chains [BHHK03]

Proposition

Under those hypotheses, $\mathbb{P}(s_0 \models \varphi)$ can be expressed as $f \left( e^{-r} \right)$ where $r$ is a rational number, and $f \in \mathbb{Q}(X)$ is a rational function.

- Note: the hypothesis “reset all bounded cycles” is necessary to get this form.
Approximating the probability

\[ P(s_0 \models \varphi) = f(e^{-r}) \]
Approximating the probability

\[ \mathbb{P}(s_0 \models \varphi) = f(e^{-r}) \]

- We can compute sequences \((a_i)_i\) and \((b_i)_i\) with
  - \(\lim_i a_i = \lim_i b_i = e^{-r}\)
  - \(a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i\)
Approximating the probability

\[ \mathbb{P}(s_0 \models \varphi) = f(e^{-r}) \]

- We can compute sequences \((a_i)_i\) and \((b_i)_i\) with
  - \(\lim_i a_i = \lim_i b_i = e^{-r}\)
  - \(a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i\)

- As \(e^{-r}\) is transcendental, we can compute an interval \((\alpha, \beta) \ni e^{-r}\) over which \(f\) is monotonic:
Approximating the probability

\[ \mathbb{P}(s_0 \models \varphi) = f(e^{-r}) \]

- We can compute sequences \((a_i)_i\) and \((b_i)_i\) with
  - \(\lim_i a_i = \lim_i b_i = e^{-r}\)
  - \(a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i\)
- As \(e^{-r}\) is transcendental, we can compute an interval \((\alpha, \beta) \ni e^{-r}\) over which \(f\) is monotonic:
  - writing \(f = P/Q\), we have that \(f' = (P'Q - PQ')/Q^2\)
Approximating the probability

\[ P(s_0 \models \varphi) = f(e^{-r}) \]

- We can compute sequences \((a_i)_i\) and \((b_i)_i\) with
  - \(\lim_i a_i = \lim_i b_i = e^{-r}\)
  - \(a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i\)

- As \(e^{-r}\) is transcendental, we can compute an interval \((\alpha, \beta) \ni e^{-r}\) over which \(f\) is monotonic:
  - writing \(f = P/Q\), we have that \(f' = (P'Q - PQ')/Q^2\)
  - by induction on the degree of \(R = P'Q - PQ'\), we prove that the sign of \(R\) is constant over \((\alpha, \beta)\) (that we can compute)
Approximating the probability

$$P(s_0 | \varphi) = f(e^{-r})$$

- We can compute sequences \((a_i)_i\) and \((b_i)_i\) with
  - \(\lim_i a_i = \lim_i b_i = e^{-r}\)
  - \(a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i\)

- As \(e^{-r}\) is transcendental, we can compute an interval \((\alpha, \beta) \ni e^{-r}\) over which \(f\) is monotonic:
  - writing \(f = P/Q\), we have that \(f' = (P'Q - PQ')/Q^2\)
  - by induction on the degree of \(R = P'Q - PQ'\), we prove that the sign of \(R\) is constant over \((\alpha, \beta)\) (that we can compute)

  If the sign of \(R'\) is constant over \((\alpha', \beta')\) (containing \(e^{-r}\)), the sign of \(R\) will be constant over

  \((\alpha, \beta) = (a_j, b_j) \subseteq (\alpha', \beta')\) if \(R(a_j) \cdot R(b_j) > 0\).
Towards solutions to the quantitative model-checking problem

Approximating the probability

\[ P(s_0 \models \varphi) = f(e^{-r}) \]

- We can compute sequences \((a_i)_i\) and \((b_i)_i\) with
  - \(\lim_i a_i = \lim_i b_i = e^{-r}\)
  - \(a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i\)

- As \(e^{-r}\) is transcendental, we can compute an interval \((\alpha, \beta) \ni e^{-r}\) over which \(f\) is monotonic:
  - writing \(f = P/Q\), we have that \(f' = (P'Q - PQ')/Q^2\)
  - by induction on the degree of \(R = P'Q - PQ'\), we prove that the sign of \(R\) is constant over \((\alpha, \beta)\) (that we can compute)
    - If the sign of \(R'\) is constant over \((\alpha', \beta')\) (containing \(e^{-r}\)), the sign of \(R\) will be constant over \((\alpha, \beta) = (a_j, b_j) \subseteq (\alpha', \beta')\) if \(R(a_j) \cdot R(b_j) > 0\).

- When \((a_N, b_N) \subseteq (\alpha, \beta)\), the two sequences \((f(a_i))_{i \geq N}\) and \((f(b_i))_{i \geq N}\) are monotonic and converge to \(f(e^{-r})\)
Deciding the threshold problem

**Theorem**

Under the previous hypotheses, the threshold problem is decidable.
Deciding the threshold problem

Theorem

Under the previous hypotheses, the threshold problem is decidable.

Check whether $c = f(e^{-r})$
Deciding the threshold problem

Theorem

Under the previous hypotheses, the threshold problem is decidable.

- Check whether $c = f(e^{-r})$
- If not:
Deciding the threshold problem

Theorem
Under the previous hypotheses, the threshold problem is decidable.

- Check whether $c = f(e^{-r})$
- If not:
  - use the approximation scheme for a sequence $(\varepsilon_n)_n$ that converges to 0
Deciding the threshold problem

Theorem
Under the previous hypotheses, the threshold problem is decidable.

- Check whether \( c = f(e^{-r}) \)
- If not:
  - use the approximation scheme for a sequence \((e_n)_n\) that converges to 0
  - stop when the under- and the over-approximations are on the same side of the threshold \( c \)
Outline

1. Introduction

2. A probabilistic semantics for timed automata

3. Solving the qualitative model-checking problem

4. Towards solutions to the quantitative model-checking problem

5. Conclusion
Conclusions

- a probabilistic semantics for timed automata which removes “unlikely” (sequences of) events
  \[ \leadsto \text{extend continuous-time Markov chains} \]
- qualitative model-checking has a topological interpretation
- abstraction and algorithm for qualitative model-checking of \( \omega \)-regular and LTL properties (one clock)
- quantitative model-checking of \( \omega \)-regular and LTL properties (restrictive framework)
Conclusions

- a probabilistic semantics for timed automata which removes “unlikely” (sequences of) events
  \[\leadsto\] extend continuous-time Markov chains
- qualitative model-checking has a topological interpretation
- abstraction and algorithm for qualitative model-checking of \(\omega\)-regular and LTL properties (one clock)
- quantitative model-checking of \(\omega\)-regular and LTL properties (restrictive framework)

Ongoing works

- better understand the framework with several clocks
- our semantics can be viewed as a \(\frac{1}{2}\)-player game, hence extend to \(1\frac{1}{2}\)- and \(2\frac{1}{2}\)-player games
  \[\leadsto\] further interesting (un)decidability results