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

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.

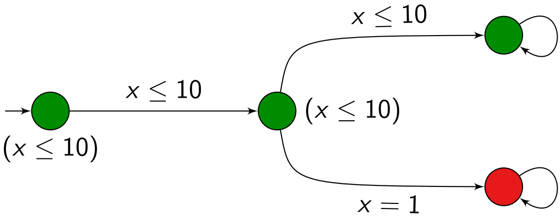
➜ Relax the idealized semantics of timed automata

- 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.

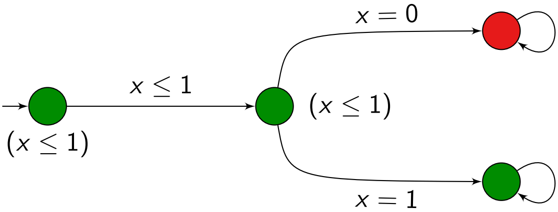
Initial example



Intuition: from the initial state,

this automaton *almost-surely* satisfies "$\mathbf{G}$ green"

A maybe less intuitive example



Does it *almost-surely* satisfy "$\mathbf{G}$ 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

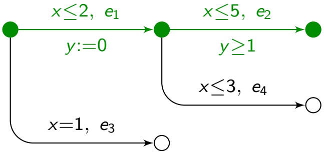
5. Conclusion

Our proposition

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

Our proposition

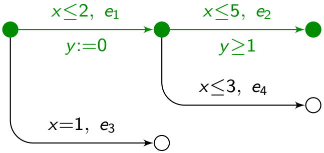
- $\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})$: symbolic path from s firing edges $e_1, \dots, e_n$
- Example:



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

Our proposition

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



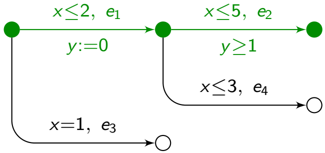
$$\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2}) = \{s_0 \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} s_2 \mid \tau_1 \leq 2,\ \tau_1 + \tau_2 \leq 5,\ \tau_2 \geq 1\}$$

Idea:

From state s_0:

Our proposition

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



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

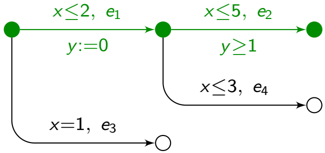
Idea:

From state s_0:

- randomly choose a delay

Our proposition

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



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

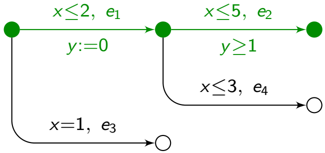
Idea:

From state s_0:

- randomly choose a delay
- then randomly select an edge

Our proposition

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



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

Idea:

From state s_0:

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

Our proposition

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

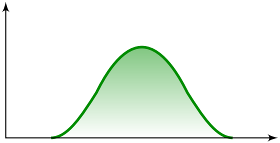
$$\mathbb{P}\Big(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\Big) = \int_{t \in I(s,e_1)} p_{s+t}(e_1)\, \mathbb{P}\Big(\pi(s_t^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n})\Big)\, \mathrm{d}\mu_s(t)$$

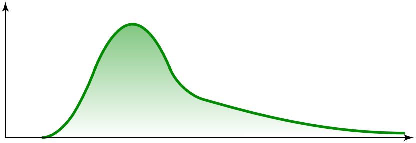
Our proposition

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

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

- $I(s, e_1) = \{\tau \mid s \xrightarrow{\tau, e_1}\}$ and μ_s distribution over $I(s) = \bigcup_e I(s, e)$





Our proposition

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

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

- $I(s,e_1) = \{\tau \mid s \xrightarrow{\tau, e_1}\}$ and μ_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: $\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n\}$

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

- $I(s, e_1) = \{\tau \mid s \xrightarrow{\tau, e_1}\}$ and μ_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

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 μ_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

$$\mathbb{P}\Big(\pi\big(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}\big)\Big) = \int_{t \in I(s,e_1)} p_{s+t}(e_1)\, \mathbb{P}\Big(\pi\big(s_t^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n}\big)\Big)\, \mathrm{d}\mu_s(t)$$

Our proposition

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

- Can be viewed as an n-dimensional integral

Our proposition

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

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

$$\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models \mathcal{C}\}$$

Our proposition

$$\mathbb{P}\Big(\pi\big(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}\big)\Big) = \int_{t \in I(s,e_1)} p_{s+t}(e_1)\, \mathbb{P}\Big(\pi\big(s_t^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n}\big)\Big)\, \mathrm{d}\mu_s(t)$$

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

$$\pi_{\mathcal{C}}\big(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}\big) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models \mathcal{C}\}$$

- Definition over sets of infinite runs:

Our proposition

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

- Can be viewed as an *n*-dimensional integral
- Easy extension to constrained symbolic paths

$$\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models \mathcal{C}\}$$

- Definition over sets of infinite runs:
  - $\mathsf{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \{\varrho \cdot \varrho' \mid \varrho \in \pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\}$

Our proposition

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

- Can be viewed as an n-dimensional integral

- Easy extension to constrained symbolic paths

$$\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models \mathcal{C}\}$$

- Definition over sets of infinite runs:
  - $\mathrm{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \{\varrho \cdot \varrho' \mid \varrho \in \pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\}$
  - $\mathbb{P}\Big(\mathrm{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))\Big) = \mathbb{P}\Big(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\Big)$

Our proposition

$$\mathbb{P}\Big(\pi\big(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}\big)\Big) = \int_{t \in I(s,e_1)} p_{s+t}(e_1)\,\mathbb{P}\Big(\pi\big(s_t^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n}\big)\Big)\,\mathrm{d}\mu_s(t)$$

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

$$\pi_{\mathcal{C}}\big(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}\big) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models \mathcal{C}\}$$

- Definition over sets of infinite runs:
  - $\mathsf{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \{\varrho \cdot \varrho' \mid \varrho \in \pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\}$
  - $\mathbb{P}\Big(\mathsf{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))\Big) = \mathbb{P}\Big(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\Big)$
  - unique extension of $\mathbb{P}$ to the generated σ-algebra

Our proposition

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

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

$$\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models \mathcal{C}\}$$

- Definition over sets of infinite runs:
  - $\mathrm{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \{\varrho \cdot \varrho' \mid \varrho \in \pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\}$
  - $\mathbb{P}\big(\mathrm{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))\big) = \mathbb{P}\big(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\big)$
  - unique extension of $\mathbb{P}$ to the generated σ-algebra
- Property: $\mathbb{P}$ is a probability measure over sets of infinite runs

Our proposition

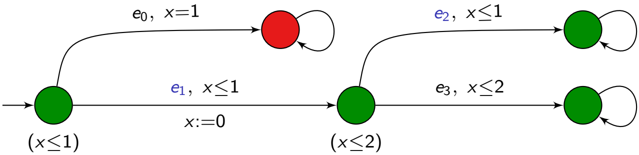
$$\mathbb{P}\Big(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\Big) = \int_{t \in I(s,e_1)} p_{s+t}(e_1)\, \mathbb{P}\Big(\pi(s_t^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n})\Big)\, \mathrm{d}\mu_s(t)$$

- Can be viewed as an *n*-dimensional integral
- Easy extension to constrained symbolic paths

  $$\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{s \xrightarrow{\tau_1, e_1} s_1 \cdots \xrightarrow{\tau_n, e_n} s_n \mid (\tau_1, \cdots, \tau_n) \models \mathcal{C}\}$$

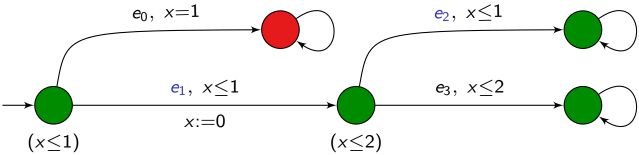
- Definition over sets of infinite runs:
  - $\mathsf{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \{\varrho \cdot \varrho' \mid \varrho \in \pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\}$
  - $\mathbb{P}\Big(\mathsf{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))\Big) = \mathbb{P}\Big(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\Big)$
  - unique extension of $\mathbb{P}$ to the generated σ-algebra
- Property: $\mathbb{P}$ is a probability measure over sets of infinite runs
- Example:
  - $\mathsf{Zeno}(s) \;=\; \bigcup_{M \in \mathbb{N}} \bigcap_{n \in \mathbb{N}} \bigcup_{(e_1, \cdots, e_n) \in E^n} \mathsf{Cyl}(\pi_{\Sigma_i \tau_i \leq M}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))$

An example of computation (with uniform distributions)



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

An example of computation (with uniform distributions)



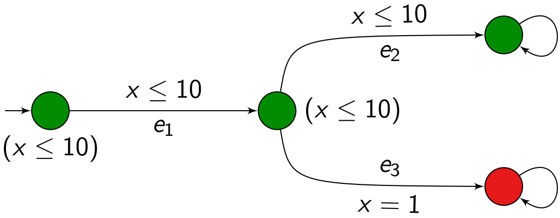
The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})$ is $\frac{1}{4}$.

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

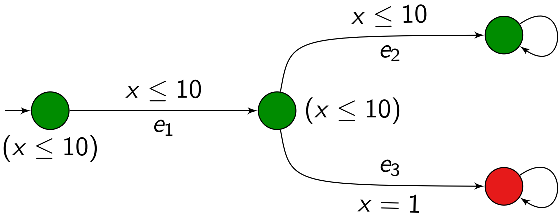
$$= \int_0^1 \int_0^1 \left(\frac{\mathbb{P}\big(\pi(s_2)\big)}{2}\mathrm{d}\mu_{s_1}(u)\right) \mathrm{d}\mu_{s_0}(t)$$

$$= \int_0^1 \int_0^1 \left(\frac{1}{2}\frac{\mathrm{d}u}{2}\right)\mathrm{d}t \quad = \frac{1}{4}$$

Back to the first example

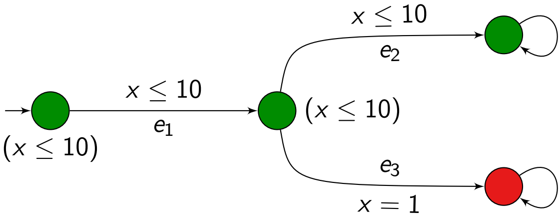


Back to the first example



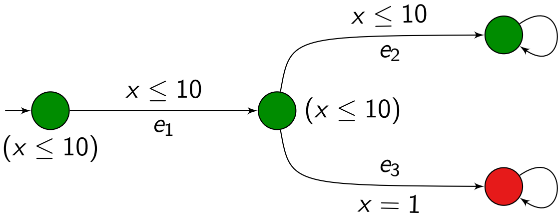
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 1$

Back to the first example



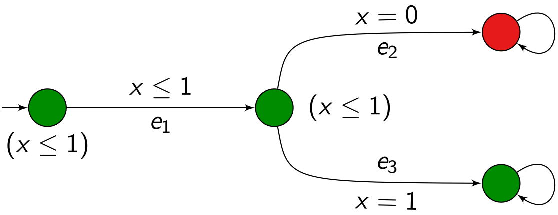
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 1$
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_3}\big)\Big) = 0$

Back to the first example

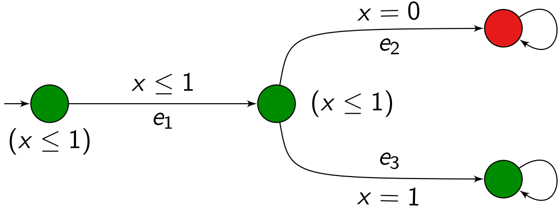


- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 1$
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_3}\big)\Big) = 0$
- $\mathbb{P}\Big(\mathbf{G}\ \text{green}\Big) = 1$

Back to the second example

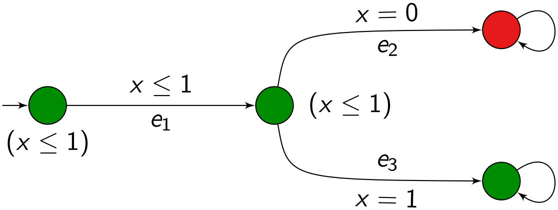


Back to the second example



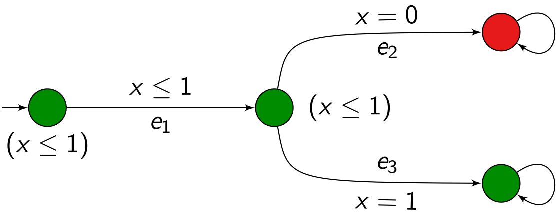
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 0$

Back to the second example



- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 0$
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_3}\big)\Big) = 1$

Back to the second example



- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 0$
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_3}\big)\Big) = 1$
- $\mathbb{P}\Big(\mathbf{G}\ \text{green}\Big) = 1$

Almost-sure satisfaction

If φ is an LTL (or ω-regular) property,

$$s \mathrel{|\!\!\approx} \varphi \quad \overset{\text{def}}{\Leftrightarrow} \quad \underbrace{\mathbb{P}\Big(\{\varrho \in \mathsf{Runs}(s) \mid \varrho \models \varphi\}\Big)}_{\overset{\text{def}}{=}\ \mathbb{P}\left(s \models \varphi\right)} = 1$$

Almost-sure satisfaction

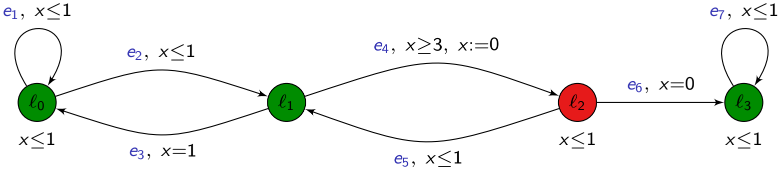
If φ is an LTL (or ω-regular) property,

$$s \mathrel{|\!\!\approx} \varphi \quad \overset{\text{def}}{\Leftrightarrow} \quad \underbrace{\mathbb{P}\Big(\{\varrho \in \mathsf{Runs}(s) \mid \varrho \models \varphi\}\Big)}_{\overset{\text{def}}{=} \mathbb{P}(s \models \varphi)} = 1$$

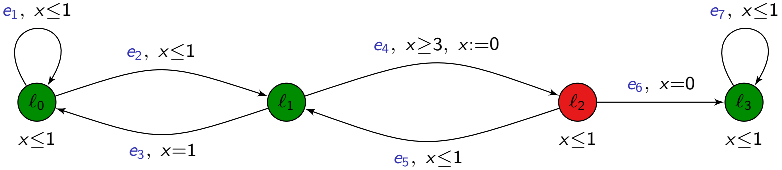
Qualitative model-checking question: $s \mathrel{|\!\!\approx} \varphi$?

Outline

An example

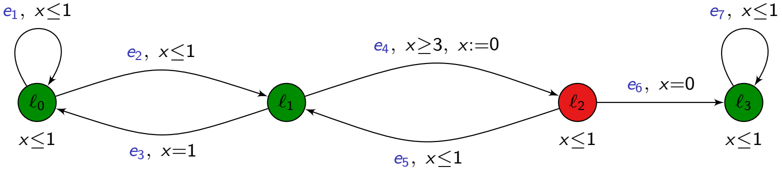

e_1, $x\leq 1$
e_2, $x\leq 1$
e_4, $x\geq 3$, $x:=0$
e_7, $x\leq 1$
e_6, $x=0$
ℓ_0
ℓ_1
ℓ_2
ℓ_3
$x\leq 1$
e_3, $x=1$
e_5, $x\leq 1$
$x\leq 1$
$x\leq 1$

An example



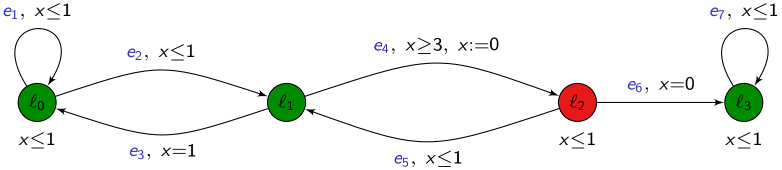
$\mathcal{A} \not\models \mathbf{G}(\text{green} \Rightarrow \mathbf{F}\ \text{red})$

An example



$\mathcal{A} \not\models \mathbf{G}(\text{green} \Rightarrow \mathbf{F}\ \text{red})$ but $\mathcal{A} \mathrel{|\!\!\approx} \mathbf{G}(\text{green} \Rightarrow \mathbf{F}\ \text{red})$

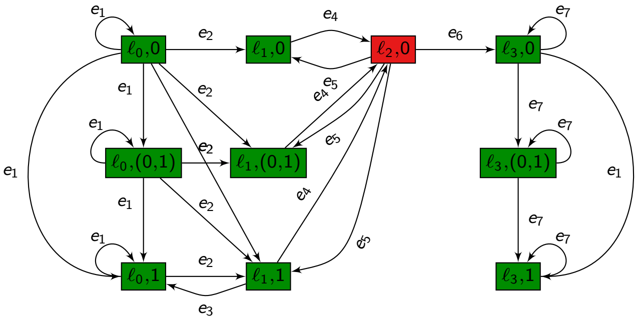
An example



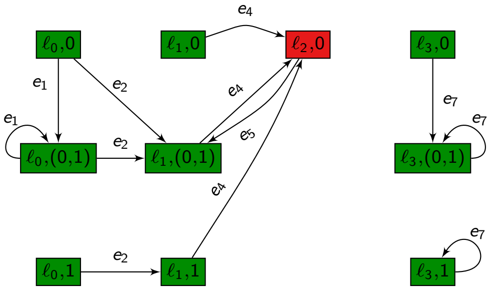
$\mathcal{A} \not\models \mathbf{G}(\text{green} \Rightarrow \mathbf{F}\ \text{red})$ but $\mathcal{A} \mathrel{|\!\!\approx} \mathbf{G}(\text{green} \Rightarrow \mathbf{F}\ \text{red})$

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

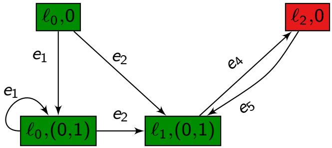
The classical region automaton



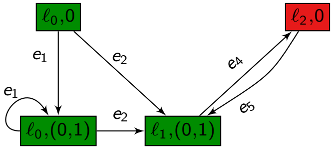
The pruned region automaton



The pruned region automaton

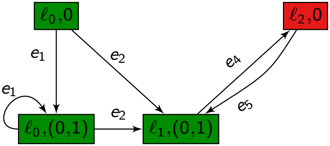


The pruned region automaton



... viewed as a finite Markov chain $MC(\mathcal{A})$

The pruned region automaton



... viewed as a finite Markov chain $MC(\mathcal{A})$

Theorem

For single-clock timed automata,

$$\mathcal{A} \mathrel{|\!\!\approx} \varphi \quad \text{iff} \quad \mathbb{P}(MC(\mathcal{A}) \models \varphi) = 1$$

Result

Theorem

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

- of LTL is PSPACE-Complete
- of ω-regular properties is NLOGSPACE-Complete

Result

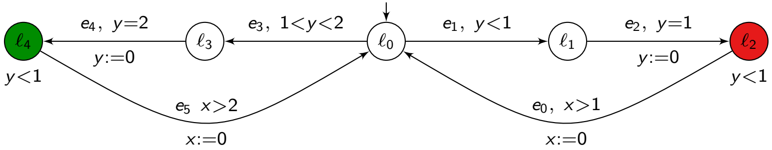
Theorem

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

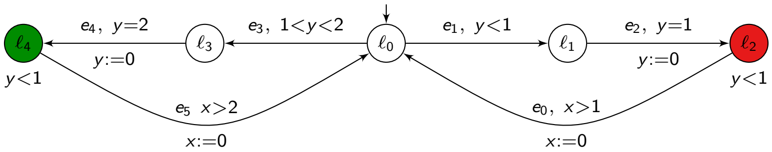
- of LTL is PSPACE-Complete
- of ω-regular properties is NLOGSPACE-Complete

- 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

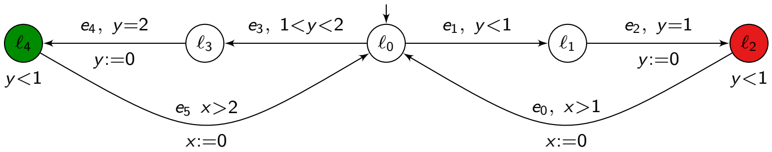


An example with two clocks



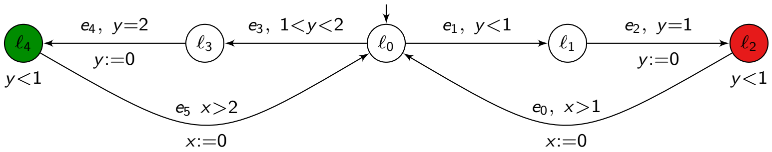
- If the previous algorithm was correct, $\mathcal{A} \mathrel{|\!\!\approx} \mathbf{G}\,\mathbf{F}$ red $\wedge$ $\mathbf{G}\,\mathbf{F}$ green

An example with two clocks



- If the previous algorithm was correct, $\mathcal{A} \mathrel{|\!\!\approx} \mathbf{G}\,\mathbf{F}\ \text{red} \wedge \mathbf{G}\,\mathbf{F}\ \text{green}$
- However, we can prove that $\mathbb{P}\Big(\mathbf{G}\,\neg\text{red}\Big) > 0$

An example with two clocks



- If the previous algorithm was correct, $\mathcal{A} \models_{\approx} \mathbf{G}\,\mathbf{F}$ red $\wedge$ $\mathbf{G}\,\mathbf{F}$ green
- However, we can prove that $\mathbb{P}\Big(\mathbf{G}\,\neg\text{red}\Big) > 0$
- There is a *strange* convergence phenomenon: along an execution, if $\delta_i > 0$ is the delay in location ℓ_4, then we have that $\sum_i \delta_i \leq 1$

A note on Zeno behaviours

- The set of Zeno behaviours is measurable:

$$\mathsf{Zeno}(s) \;=\; \bigcup_{M \in \mathbb{N}} \bigcap_{n \in \mathbb{N}} \bigcup_{(e_1,\cdots,e_n) \in E^n} \mathsf{Cyl}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))$$

A note on Zeno behaviours

- The set of Zeno behaviours is measurable:

$$\mathsf{Zeno}(s) \;=\; \bigcup_{M\in\mathbb{N}} \bigcap_{n\in\mathbb{N}} \bigcup_{(e_1,\cdots,e_n)\in E^n} \mathsf{Cyl}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))$$

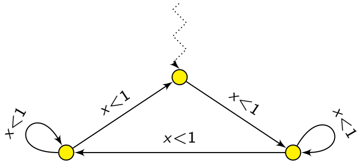
- In single-clock timed automata, we can decide in NLOGSPACE whether $\mathbb{P}\Big(\mathsf{Zeno}(s)\Big) = 0$:

A note on Zeno behaviours

- The set of Zeno behaviours is measurable:

$$\mathsf{Zeno}(s) \;=\; \bigcup_{M\in\mathbb{N}} \bigcap_{n\in\mathbb{N}} \bigcup_{(e_1,\cdots,e_n)\in E^n} \mathsf{Cyl}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))$$

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

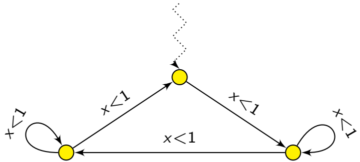


A note on Zeno behaviours

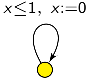
- The set of Zeno behaviours is measurable:

$$\mathrm{Zeno}(s) = \bigcup_{M\in\mathbb{N}} \bigcap_{n\in\mathbb{N}} \bigcup_{(e_1,\cdots,e_n)\in E^n} \mathrm{Cyl}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}))$$

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



  - an interesting notion of non-Zeno timed automata



Outline

Quantitative model-checking

How likely an automaton will satisfy a property?
I.e., what is the value $\mathbb{P}\big(s \models \varphi\big)$?

Towards quantitative analysis

- The abstraction $MC(\mathcal{A})$ 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 $MC(\mathcal{A})$ 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 $MC(\mathcal{A})$ 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.
  ☞ 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.
  ☞ 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 $MC(\mathcal{A})$ 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:
  - 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_ε^- and p_ε^+ such that:

$$\begin{cases} p_\varepsilon^- \leq \mathbb{P}\big(s_0 \models \varphi\big) \leq p_\varepsilon^- + \varepsilon \\ p_\varepsilon^+ - \varepsilon \leq \mathbb{P}\big(s_0 \models \varphi\big) \leq p_\varepsilon^+ \end{cases}$$

Towards quantitative analysis

- The abstraction $MC(\mathcal{A})$ is no more correct.
- Can be reduced to solving a system of differential equations.
  ☞ 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_ε^- and p_ε^+ such that:

$$\begin{cases} p_\varepsilon^- \leq \mathbb{P}\big(s_0 \models \varphi\big) \leq p_\varepsilon^- + \varepsilon \\ p_\varepsilon^+ - \varepsilon \leq \mathbb{P}\big(s_0 \models \varphi\big) \leq p_\varepsilon^+ \end{cases}$$

  - we will be able to decide the threshold problem

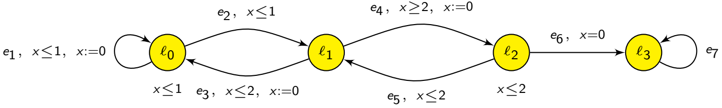
Towards quantitative analysis

- The abstraction $MC(\mathcal{A})$ is no more correct.
- Can be reduced to solving a system of differential equations.
  ☞ 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_ε^- and p_ε^+ such that:

$$\begin{cases} p_\varepsilon^- \leq \mathbb{P}\big(s_0 \models \varphi\big) \leq p_\varepsilon^- + \varepsilon \\ p_\varepsilon^+ - \varepsilon \leq \mathbb{P}\big(s_0 \models \varphi\big) \leq p_\varepsilon^+ \end{cases}$$

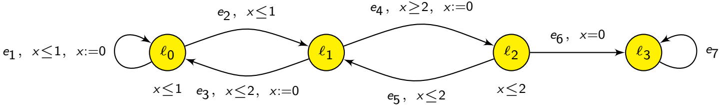
  - we will be able to decide the threshold problem:
    "Given $\mathcal{A}$, φ, $c \in \mathbb{Q}$, and $\sim \in \{<, \leq, =, \geq, >\}$, does $\mathbb{P}\big(s_0 \models \varphi\big) \sim c$ in $\mathcal{A}$?"

An example



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

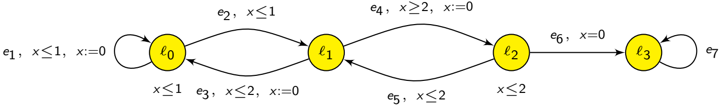
An example



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

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

An example



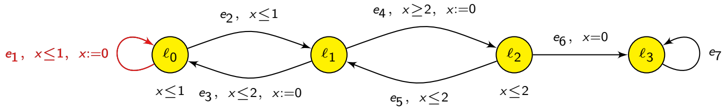
$+$ distributions $\quad \mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$

μ_s uniform distribution when $I(s)$ is bounded

$+$ uniform weights on transitions

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

An example



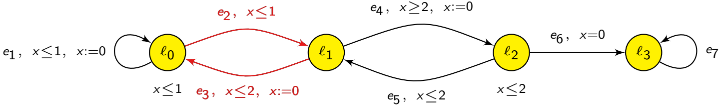
+ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$

μ_s uniform distribution when $I(s)$ is bounded

+ uniform weights on transitions

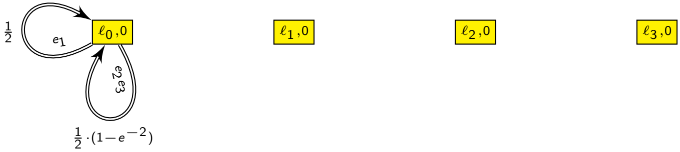
We construct a finite Markov chain $MC'(\mathcal{A})$ with macro-edges:

An example

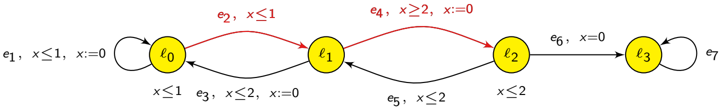


+ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
μ_s uniform distribution when $I(s)$ is bounded
+ uniform weights on transitions

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

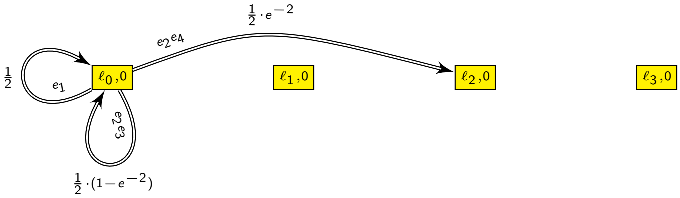


An example

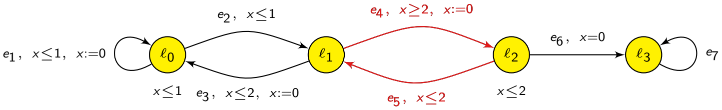


+ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
μ_s uniform distribution when $I(s)$ is bounded
+ uniform weights on transitions

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

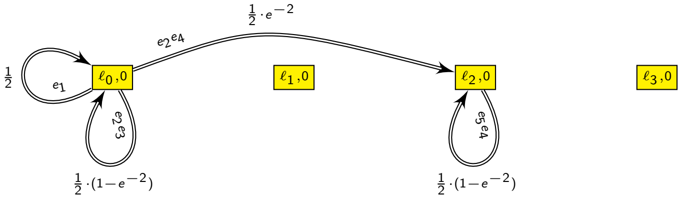


An example

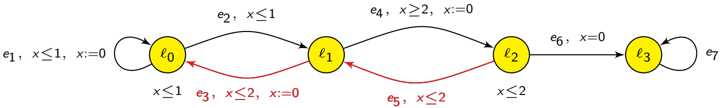


+ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
μ_s uniform distribution when $I(s)$ is bounded
+ uniform weights on transitions

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

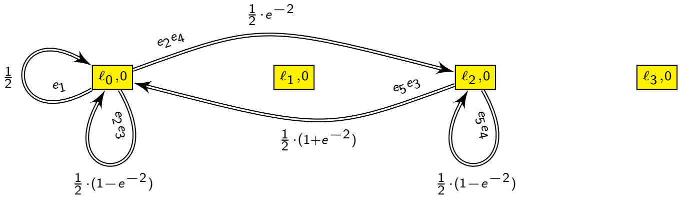


An example

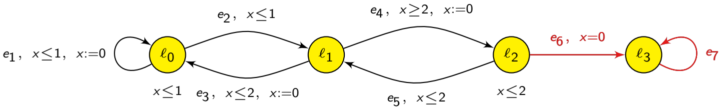


+ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
μ_s uniform distribution when $I(s)$ is bounded
+ uniform weights on transitions

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



An example

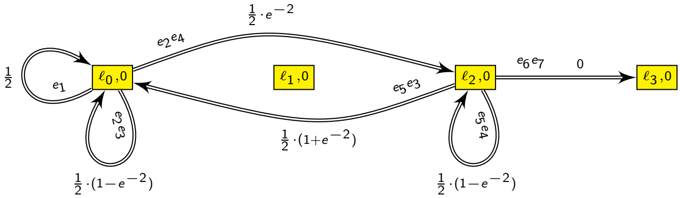


+ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$

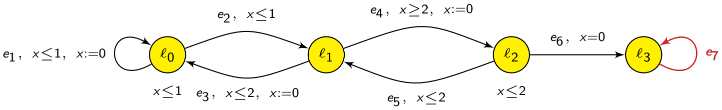
μ_s uniform distribution when $I(s)$ is bounded

+ uniform weights on transitions

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



An example

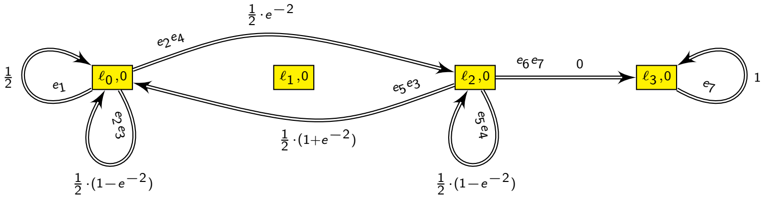


+ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$

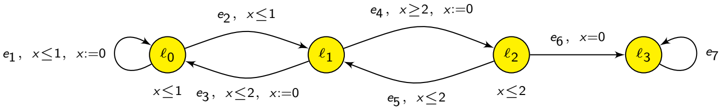
μ_s uniform distribution when $I(s)$ is bounded

+ uniform weights on transitions

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



An example

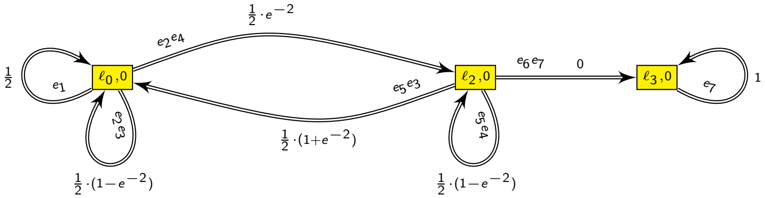


+ distributions $\mu_s : t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$

μ_s uniform distribution when $I(s)$ is bounded

+ uniform weights on transitions

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



Correctness of the abstraction

Theorem

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

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

for some well-chosen set F_φ.

Correctness of the abstraction

Theorem

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

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

for some well-chosen set F_φ.

- **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 φ,

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

for some well-chosen set F_φ.

- **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 $MC'(\mathcal{A})$.

Computing the probability

- 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 ℓ, 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 ℓ, 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]

Computing the probability

- We assume furthermore that:
  - for every state s, $I(s) = \mathbb{R}_+$
    (the timed automaton is 'reactive')
  - in every location ℓ, 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, $\mathbb{P}\Big(s_0 \models \varphi\Big)$ can be expressed as $f\,(e^{-r})$ where r is a rational number, and $f \in \mathbb{Q}(X)$ is a rational function.

Computing the probability

- We assume furthermore that:
  - for every state s, $I(s) = \mathbb{R}_+$
    (the timed automaton is 'reactive')
  - in every location ℓ, 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, $\mathbb{P}\left(s_0 \models \varphi\right)$ 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

$$\mathbb{P}\left(s_0 \models \varphi\right) = f\left(e^{-r}\right)$$

Approximating the probability

$$\mathbb{P}\left(s_0 \models \varphi\right) = f\left(e^{-r}\right)$$

- 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

$$\mathbb{P}\Big(s_0 \models \varphi\Big) = f\left(e^{-r}\right)$$

- 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

$$\mathbb{P}\Big(s_0 \models \varphi\Big) = f\left(e^{-r}\right)$$

- 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

$$\mathbb{P}\Big(s_0 \models \varphi\Big) = f\left(e^{-r}\right)$$

- 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 (α, β) (that we can compute)

Approximating the probability

$$\mathbb{P}\Big(s_0 \models \varphi\Big) = f\left(e^{-r}\right)$$

- 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 (α, β) (that we can compute)

    If the sign of R' is constant over (α', β') (containing e^{-r}), the sign of R will be constant over $(\alpha, \beta) = (a_j, b_j) \subseteq (\alpha', \beta')$ if $R(a_j) \cdot R(b_j) > 0$.

Approximating the probability

$$\mathbb{P}\Big(s_0 \models \varphi\Big) = f\left(e^{-r}\right)$$

- 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 (α, β) (that we can compute)

    If the sign of R' is constant over (α', β') (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 $f\left(e^{-r}\right)$

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 $(\varepsilon_n)_n$ that converges to 0
  - stop when the under- and the over-approximations are on the same side of the threshold c

Outline

Conclusions

- a probabilistic semantics for timed automata which removes "unlikely" (sequences of) events
  $\rightsquigarrow$ extend continuous-time Markov chains
- qualitative model-checking has a topological interpretation
- abstraction and algorithm for qualitative model-checking of ω-regular and LTL properties (one clock)
- quantitative model-checking of ω-regular and LTL properties (restrictive framework)

Conclusions

- a probabilistic semantics for timed automata which removes "unlikely" (sequences of) events
  $\rightsquigarrow$ extend continuous-time Markov chains
- qualitative model-checking has a topological interpretation
- abstraction and algorithm for qualitative model-checking of ω-regular and LTL properties (one clock)
- quantitative model-checking of ω-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
  $\rightsquigarrow$ further interesting (un)decidability results