Almost-Sure Model Checking of Infinite Paths in One-Clock Timed Automata

Christel Baier[1] Nathalie Bertrand[2] Patricia Bouyer[3]
Thomas Brihaye[4] Marcus Größer[1]

[1]Technische Universität Dresden, Germany
[2]IRISA, INRIA, Rennes, France
[3]LSV, CNRS, ENS Cachan, France
[4]Université de Mons-Hainaut, Belgium

Outline

1. Introduction

2. A probabilistic semantics

3. Solving the qualitative model-checking problem

4. Conclusion

Motivations

- Timed automata, an idealized mathematical model for real-time systems

Motivations

- Timed automata, an idealized mathematical model for real-time systems
  - assumes infinite precision of clocks
  - assumes instantaneous actions
  - *etc...*

Motivations

- Timed automata, an idealized mathematical model for real-time systems
  - assumes infinite precision of clocks
  - assumes instantaneous actions
  - *etc...*

➜ notion of strong robustness defined in [DDR04]

Motivations

- Timed automata, an idealized mathematical model for real-time systems
  - assumes infinite precision of clocks
  - assumes instantaneous actions
  - *etc...*

➜ notion of strong robustness defined in [DDR04]

- In a model, only few traces may violate the correctness property: they may hence not be relevant...

Motivations

- Timed automata, an idealized mathematical model for real-time systems
  - assumes infinite precision of clocks
  - assumes instantaneous actions
  - *etc...*

➜ notion of strong robustness defined in [DDR04]

- In a model, only few traces may violate the correctness property: they may hence not be relevant...

➜ topological notion of tube acceptance in [GHJ97]

Motivations

- Timed automata, an idealized mathematical model for real-time systems
  - assumes infinite precision of clocks
  - assumes instantaneous actions
  - *etc...*

➜ notion of strong robustness defined in [DDR04]

- In a model, only few traces may violate the correctness property: they may hence not be relevant...

➜ topological notion of tube acceptance in [GHJ97]

➜ notion of fair correctness in [VV06] based on probabilities
(for untimed systems) + topological characterization

Motivations

- Timed automata, an idealized mathematical model for real-time systems
  - assumes infinite precision of clocks
  - assumes instantaneous actions
  - *etc...*

➜ notion of strong robustness defined in [DDR04]

- In a model, only few traces may violate the correctness property: they may hence not be relevant...

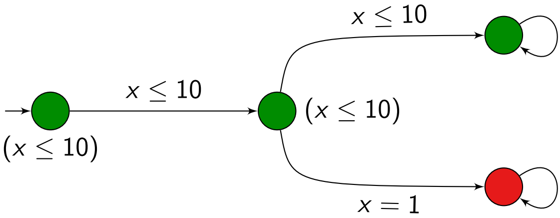
➜ topological notion of tube acceptance in [GHJ97]

➜ notion of fair correctness in [VV06] based on probabilities (for untimed systems) + topological characterization

Our aim:

Use probabilities to "relax" the semantics of timed automata

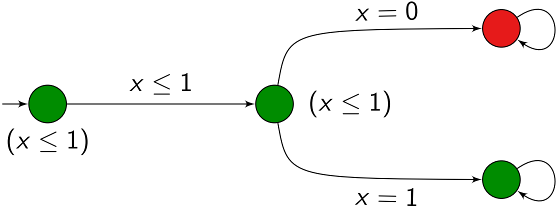
Initial example



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

3. Solving the qualitative model-checking problem

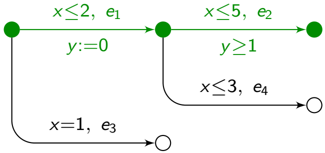
4. Conclusion

Our proposition

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

Our proposition

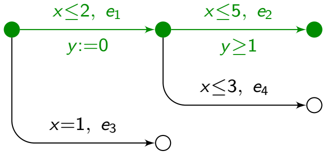
- $\pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n})$: symbolic path from s firing edges $e_1, \ldots, e_n$
- Example:



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

Our proposition

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



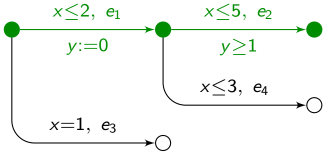
$$\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2}) = \{s_0 \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} s_2 \mid \tau_1 \leq 2,\ \tau_1 + \tau_2 \leq 5,\ \tau_2 \geq 1\}$$

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:



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

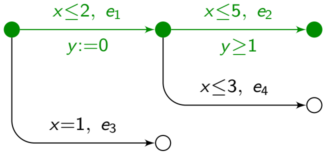
Idea:

From state s_0:

- randomly choose a delay

Our proposition

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



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

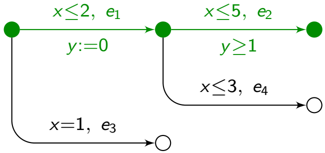
Idea:

From state s_0:

- randomly choose a delay
- then randomly select an edge

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

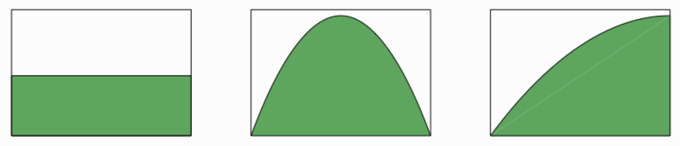
$$\mathbb{P}\left(\pi\left(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}\right)\right) = \int_{t \in I(s, e_1)} p_{s+t}(e_1)\, \mathbb{P}\left(\pi\left(s_t^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n}\right)\right) \mathrm{d}\mu_s(t)$$

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 $I(s) = \bigcup_e I(s, e)$

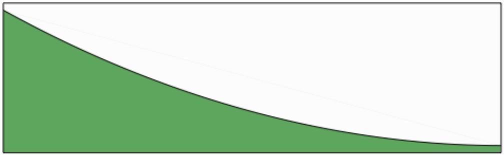


Our proposition

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 $I(s) = \bigcup_e I(s, e)$



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

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

Our proposition

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

- Can be viewed as an n-dimensional integral

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

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

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

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

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

Our proposition

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

- 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

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

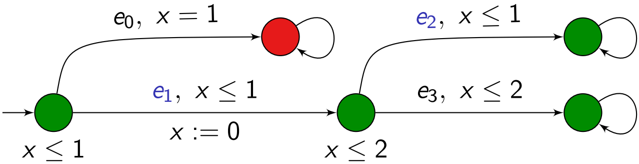
$$\mathbb{P}\Big(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\Big) = \int_{t \in I(s,e_1)} p_{s+t}(e_1)\, \mathbb{P}\Big(\pi(s_t^{e_1} \xrightarrow{e_2} \cdots \xrightarrow{e_n})\Big)\, \mathrm{d}\mu_s(t)$$

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

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

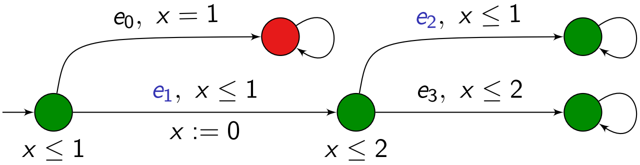
- Definition over sets of infinite runs:
  - $\mathrm{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})) = \{\varrho \cdot \varrho' \mid \varrho \in \pi_{\mathcal{C}}(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})\}$
  - $\mathbb{P}\Big(\mathrm{Cyl}(\pi_{\mathcal{C}}(s \xrightarrow{e_1}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

An example of computation (with uniform distributions)



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

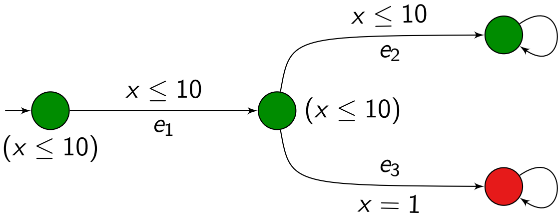
An example of computation (with uniform distributions)



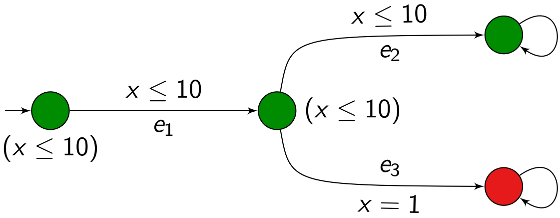
The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})$ is $\frac{1}{4}$.

$$\begin{aligned}
\mathbb{P}\Big(\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})\Big) &= \int_0^1 \mathbb{P}\Big(\pi(s_1 \xrightarrow{e_2})\Big)\mathrm{d}\mu_{s_0}(t) + \int_1^1 \frac{\mathbb{P}\Big(\pi(s_1 \xrightarrow{e_2})\Big)}{2}\mathrm{d}\mu_{s_0}(t) \\
&= \int_0^1 \int_0^1 \left(\frac{\mathbb{P}\Big(\pi(s_2)\Big)}{2}\mathrm{d}\mu_{s_1}(u)\right)\mathrm{d}\mu_{s_0}(t) \\
&= \int_0^1 \int_0^1 \left(\frac{1}{2}\frac{\mathrm{d}u}{2}\right)\mathrm{d}t \quad = \frac{1}{4}
\end{aligned}$$

Back to the first example

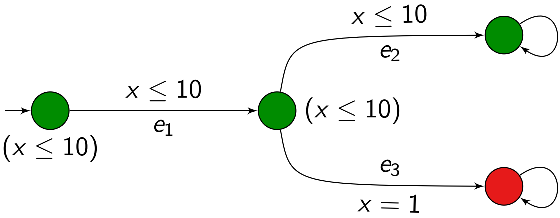


Back to the first example



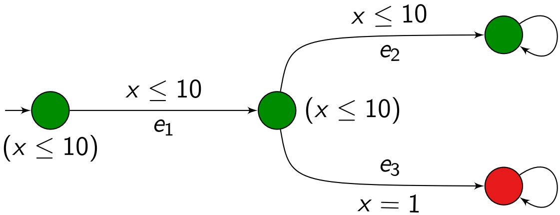
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 1$

Back to the first example



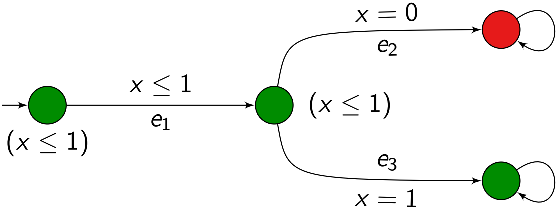
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 1$
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_3}\big)\Big) = 0$

Back to the first example

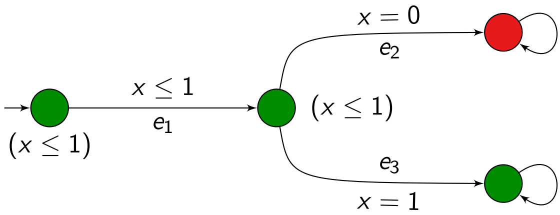


- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 1$
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_3}\big)\Big) = 0$
- $\mathbb{P}\Big(\mathbf{G}\ \text{green}\Big) = 1$

Back to the second example

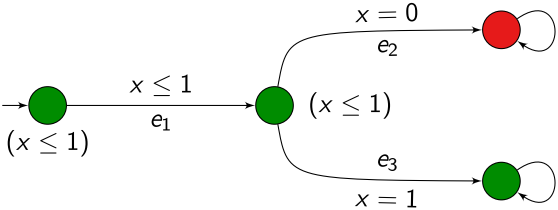


Back to the second example



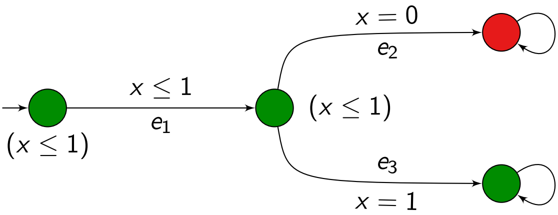
- $\mathbb{P}\Big(\pi\big(s_0 \xrightarrow{e_1}\xrightarrow{e_2}\big)\Big) = 0$

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 model-checking

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

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

Almost-sure model-checking

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

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

We want to decide the almost-sure model-checking...
(This is a qualitative model-checking question)

Outline

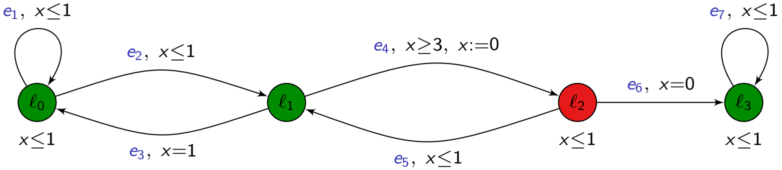
1. Introduction

2. A probabilistic semantics

3. Solving the qualitative model-checking problem

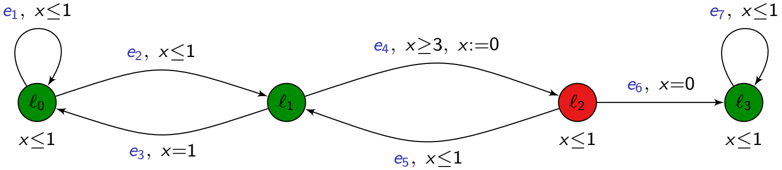
4. Conclusion

An example



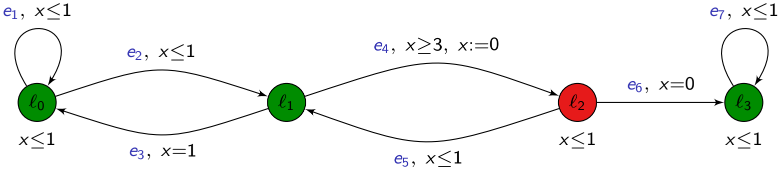
e_1, $x \leq 1$
e_2, $x \leq 1$
e_4, $x \geq 3$, $x := 0$
e_6, $x = 0$
e_7, $x \leq 1$
ℓ_0
ℓ_1
ℓ_2
ℓ_3
$x \leq 1$
e_3, $x = 1$
e_5, $x \leq 1$
$x \leq 1$
$x \leq 1$

An example



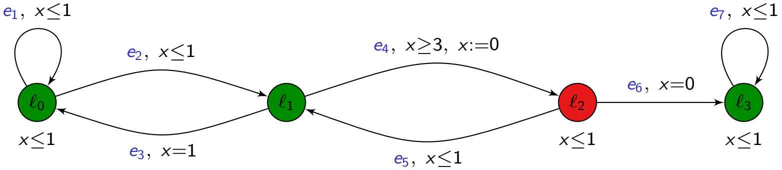
$\mathcal{A} \not\models \mathbf{G}(\text{green} \Rightarrow \mathbf{F}\ \text{red})$

An example



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

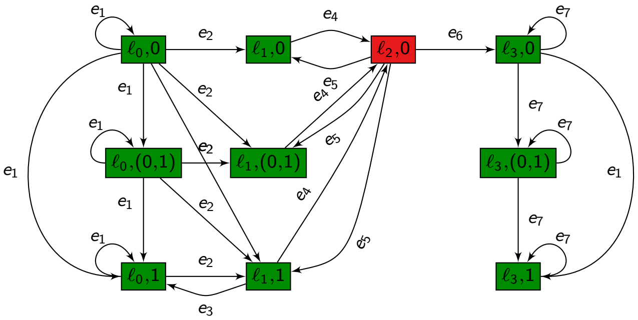
An example



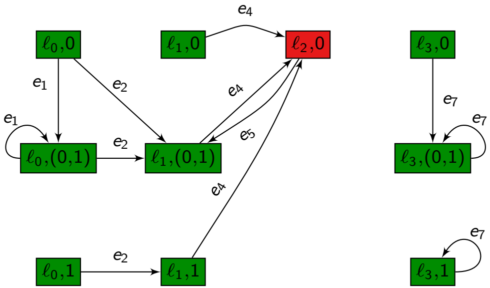
$\mathcal{A} \not\models \mathbf{G}(\text{green} \Rightarrow \mathbf{F}\ \text{red})$ but $\mathcal{A} \mathrel{|\!\!\approx} \mathbf{G}(\text{green} \Rightarrow \mathbf{F}\ \text{red})$

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

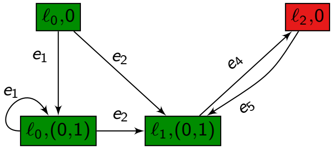
The classical region automaton



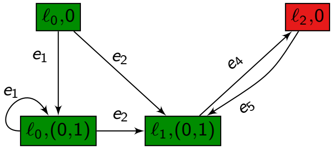
The pruned region automaton



The pruned region automaton

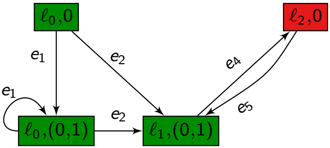


The pruned region automaton



... 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,

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

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

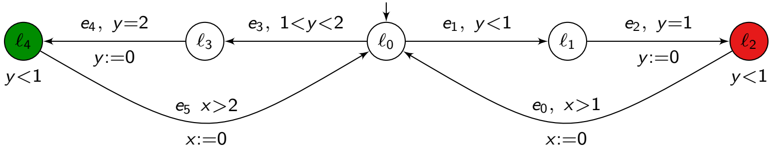
Theorem

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

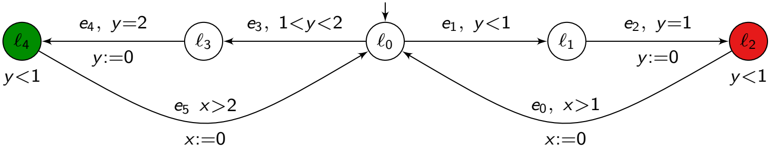
- of LTL is PSPACE-Complete
- of ω-regular properties is NLOGSPACE-Complete

- 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

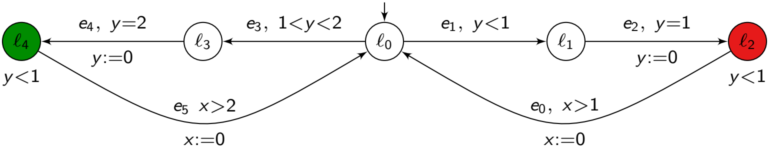


An example with two clocks



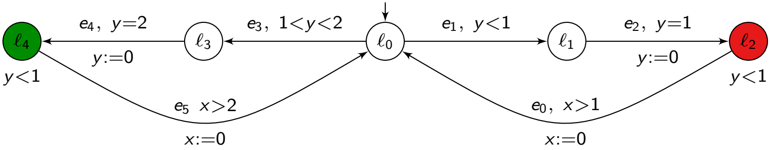
- If the previous algorithm was correct, $\mathcal{A} \models\!\!\!\approx \mathbf{G}\,\mathbf{F}$ red $\wedge$ $\mathbf{G}\,\mathbf{F}$ green

An example with two clocks



- If the previous algorithm was correct, $\mathcal{A} \mid\!\approx \mathbf{G}\,\mathbf{F}\ \text{red} \wedge \mathbf{G}\,\mathbf{F}\ \text{green}$
- 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 $\sum_i \delta_i \le 1$

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:

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

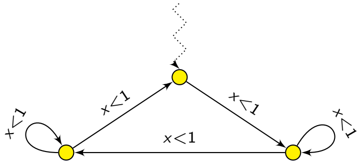
- In single-clock timed automata, we can decide in NLOGSPACE whether $\mathbb{P}\Big(\mathsf{Zeno}(s)\Big) = 0$:

A note on Zeno behaviours

- The set of Zeno behaviours is measurable:

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

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

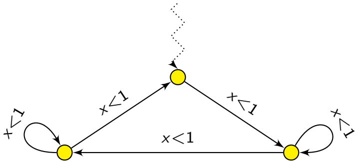


A note on Zeno behaviours

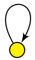
- The set of Zeno behaviours is measurable:

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

- 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 $MC(\mathcal{A})$



  - an interesting notion of non-Zeno timed automata



Outline

1. Introduction

2. A probabilistic semantics

3. Solving the qualitative model-checking problem

4. Conclusion

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
- algorithm for qualitative of LTL (and ω-regular) properties

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
- algorithm for qualitative of LTL (and ω-regular) properties

What else have we done so far?

- (restricted) quantitative model-checking for ω-regular properties
  $\rightsquigarrow$ *to appear at QEST'08*

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
- algorithm for qualitative of LTL (and ω-regular) properties

What else have we done so far?

- (restricted) quantitative model-checking for ω-regular properties

  $\leadsto$ *to appear at QEST'08*

Ongoing work

- our semantics can be viewed as a $\frac{1}{2}$-player game
  $1\frac{1}{2}$- and $2\frac{1}{2}$-player games

  $\leadsto$ further interesting (un)decidability results