Probabilistic and Topological Semantics for Timed Automata

Christel Baier[1], Nathalie Bertrand[2], Patricia Bouyer[3,4],
Thomas Brihaye[5], Marcus Größer[1]

[1]TU Dresden, Germany

[2]IRISA, INRIA Rennes, France

[3]LSV, CNRS/ENS Cachan, France

[4]Oxford University, UK
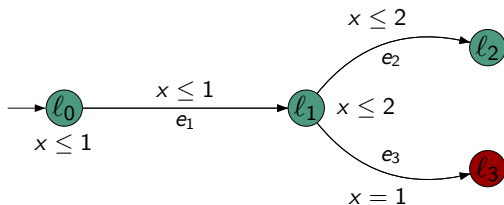
[5]Université de Mons-Hainaut, Belgium

Séminaire 68NQRT – 31/01/08

Motivation

- ▶ Timed automata: idealized mathematical model
  - ▶ infinite precision
  - ▶ instantaneous events
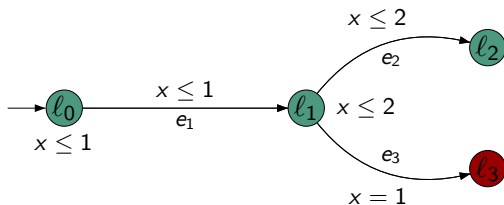
Motivation

- ▶ Timed automata: idealized mathematical model
  - ▶ infinite precision
  - ▶ instantaneous events

- ▶ Few traces may violate the property

$$\mathcal{A} \not\models \mathbf{G} \bullet \quad \text{but} \quad \mathcal{A} \approx\!\!\!| \mathbf{G} \bullet$$

Motivation

▶ Timed automata: idealized mathematical model
  ▶ infinite precision
  ▶ instantaneous events

▶ Few traces may violate the property

$$\mathcal{A} \not\models \mathbf{G} \bullet \quad \text{but} \quad \mathcal{A} \models_{\approx} \mathbf{G} \bullet$$

Aim: Relax the semantics of timed automata.

Big and small sets

Given $\mathcal{A}$ and φ, we want to define $\mathcal{A} \approx \varphi$ s.t.

$$\{\rho \mid \rho \not\models \varphi\} \quad \lll \quad \{\rho \mid \rho \models \varphi\}$$

Big and small sets

Given $\mathcal{A}$ and φ, we want to define $\mathcal{A} \approx \varphi$ s.t.

$$\{\rho \mid \rho \not\models \varphi\} \quad \lll \quad \{\rho \mid \rho \models \varphi\}$$

Probability	$\mathbb{P}(\{\rho \mid \rho \not\models \varphi\}) = 0$	$\mathbb{P}(\{\rho \mid \rho \models \varphi\}) = 1$
Topology	$\{\rho \mid \rho \not\models \varphi\}$ is meager	$\{\rho \mid \rho \models \varphi\}$ is large

Big and small sets

Given $\mathcal{A}$ and φ, we want to define $\mathcal{A} \approx\!\!\!\mid \varphi$ s.t.

$$\{\rho \mid \rho \not\models \varphi\} \quad \lll \quad \{\rho \mid \rho \models \varphi\}$$

Probability	$\mathbb{P}(\{\rho \mid \rho \not\models \varphi\}) = 0$	$\mathbb{P}(\{\rho \mid \rho \models \varphi\}) = 1$
Topology	$\{\rho \mid \rho \not\models \varphi\}$ is meager	$\{\rho \mid \rho \models \varphi\}$ is large

Banach-Mazur games relate the two notions in the framework of finite systems [VV06]
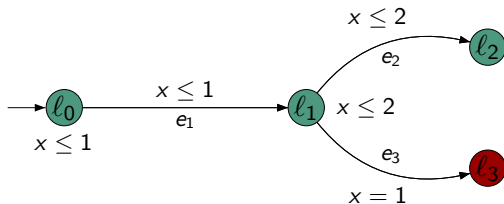
Outline

1. **Introduction**

2. **Probabilistic semantics and almost-sure model-checking**
   - Probabilistic semantics
   - Almost-sure model-checking

3. **Topological semantics and fair model-checking**
   - Topology
   - Meager sets and Banach-Mazur games

4. **Results on the two semantics**
   - Finite paths
   - Infinite paths

5. **Related work**

6. **Conclusion**

Symbolic paths

Symbolic path

$\mathcal{A}$ timed-automaton, s state and $e_1 \cdots e_n$ edges

$$\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n}) = \{\rho = s \xrightarrow{\tau_1, e_1} \cdots \xrightarrow{\tau_n, e_n} s_n \mid \rho \text{ run of } \mathcal{A}\}$$

$$\pi((\ell_0, 0), e_1 e_2) = \{(\ell_0, 0) \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} s_2 \mid 0 \leq \tau_1 \leq 1; 0 \leq \tau_1 + \tau_2 \leq 2\}$$

Probabilistic semantics

Intuitively: From state s, 1. randomly choose a delay
2. randomly select an edge

Probabilistic semantics

Intuitively: From state s,   1. randomly choose a delay
                                         2. randomly select an edge

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

Probabilistic semantics

Intuitively: From state s,   1. randomly choose a delay

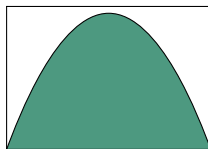   2. randomly select an edge

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

- $I(s, e_1) = \{\tau \mid s \xrightarrow{\tau, e_1} \}$
- μ_s "fair" distrib. over $I(s) = \bigcup_e I(s, e)$

Probabilistic semantics

Intuitively: From state s, 1. randomly choose a delay
2. randomly select an edge

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

▶ $I(s, e_1) = \{\tau \mid s \xrightarrow{\tau, e_1}\}$
▶ μ_s "fair" distrib. over $I(s) = \bigcup_e I(s, e)$

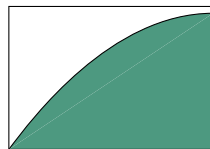Examples of μ_s when $I(s)$ is a bounded interval

$I(s)$ $I(s)$ $I(s)$
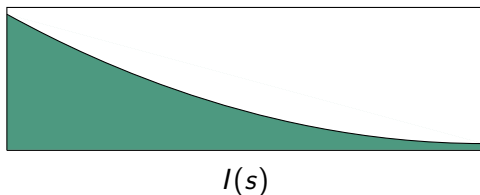
Probabilistic semantics

Intuitively: From state s,   1. randomly choose a delay

                                              2. randomly select an edge

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

▶ $I(s, e_1) = \{\tau \mid s \xrightarrow{\tau, e_1}\}$

▶ μ_s "fair" distrib. over $I(s) = \bigcup_e I(s, e)$

Example of μ_s when $I(s)$ is unbounded

$I(s)$

Probabilistic semantics

Intuitively: From state s,   1. randomly choose a delay

                                  2. randomly select an edge

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

- $I(s, e_1) = \{\tau \mid s \xrightarrow{\tau, e_1}\}$
- μ_s "fair" distrib. over $I(s) = \bigcup_e I(s, e)$
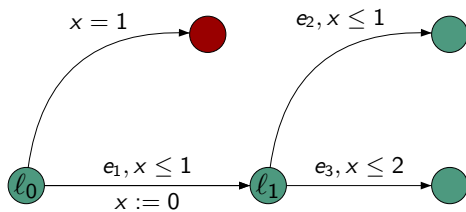- p_{s+t} distrib. over transitions enabled in $s + t$

Probabilistic semantics

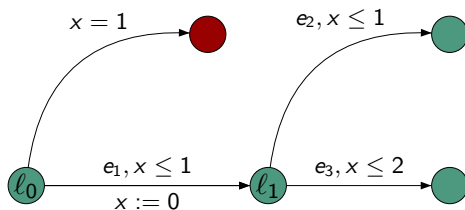Intuitively: From state s, 1. randomly choose a delay
2. randomly select an edge

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

- $I(s, e_1) = \{\tau \mid s \xrightarrow{\tau, e_1}\}$
- μ_s "fair" distrib. over $I(s) = \bigcup_e I(s, e)$
- p_{s+t} distrib. over transitions enabled in $s + t$
- $s \xrightarrow{t, e_1} s_t$

Example of probability computation

Example of probability computation

$$\mathbb{P}(\pi((\ell_0, 0), e_1 e_2)) = \frac{1}{4}$$

$$\mathbb{P}(\pi((\ell_0, 0), e_1 e_2)) = \int_{t=0}^{1} \mathbb{P}(\pi((\ell_1, 0), e_2)) d\mu_{(\ell_0, 0)}(t)$$

$$= \int_{t=0}^{1} \int_{u=0}^{1} \frac{1}{2} d\mu_{(\ell_1, 0)}(u) dt$$

$$= \int_{t=0}^{1} \int_{u=0}^{1} \frac{1}{2} \frac{du}{2} dt = \frac{1}{4}$$

Probabilistic semantics (infinite runs)

Cylinder generated by π: $\mathsf{Cyl}(\pi) = \{\rho_1 \cdot \rho_2 \mid \rho_1 \in \pi\}$

- $\mathbb{P}(\mathsf{Cyl}(\pi)) = \mathbb{P}(\pi)$
- extension of $\mathbb{P}$ to the σ-algebra generated by all $\mathsf{Cyl}(\pi)$

Probabilistic semantics (infinite runs)

Cylinder generated by π: $\mathsf{Cyl}(\pi) = \{\rho_1 \cdot \rho_2 \mid \rho_1 \in \pi\}$

► $\mathbb{P}(\mathsf{Cyl}(\pi)) = \mathbb{P}(\pi)$

► extension of $\mathbb{P}$ to the σ-algebra generated by all $\mathsf{Cyl}(\pi)$

Almost-sure model-checking of LTL

Let φ be an LTL formula.

$$\mathcal{A} \models_{\mathbb{P}} \varphi \quad \overset{\text{def}}{\Leftrightarrow} \quad \mathbb{P}(\{\rho \mid \rho \models \varphi\}) = 1$$

Outline

1. Introduction

2. Probabilistic semantics and almost-sure model-checking
   - Probabilistic semantics
   - Almost-sure model-checking

3. Topological semantics and fair model-checking
   - Topology
   - Meager sets and Banach-Mazur games

4. Results on the two semantics
   - Finite paths
   - Infinite paths

5. Related work

6. Conclusion

A notion of dimension

Polyedron associated with a symbolic path $\pi = \pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})$

$$\mathrm{Pol}(\pi) = \{(\tau_1, \cdots, \tau_n) \in (\mathbb{R}^+)^n \mid s \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} \cdots \xrightarrow{\tau_n, e_n} s_n\}$$
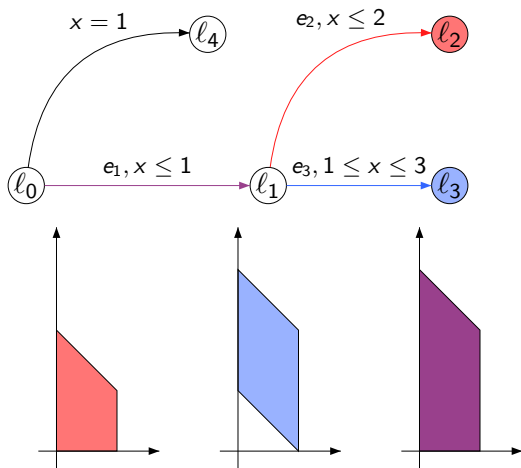
A notion of dimension

Polyedron associated with a symbolic path $\pi = \pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_n})$

$$\mathsf{Pol}(\pi) = \{(\tau_1, \cdots, \tau_n) \in (\mathbb{R}^+)^n \mid s \xrightarrow{\tau_1, e_1} s_1 \xrightarrow{\tau_2, e_2} \cdots \xrightarrow{\tau_n, e_n} s_n\}$$

Dimension of a symbolic path

$$\dim(\pi) = \top \quad \overset{\mathrm{def}}{\Leftrightarrow}$$

- $\dim(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_{n-1}})) = \top$, and
- $\mathsf{Pol}(\pi)$ is of maximal dimension in $\bigcup_e \mathsf{Pol}(\pi(s \xrightarrow{e_1} \cdots \xrightarrow{e_{n-1}} \xrightarrow{e}))$

Dimension on an example
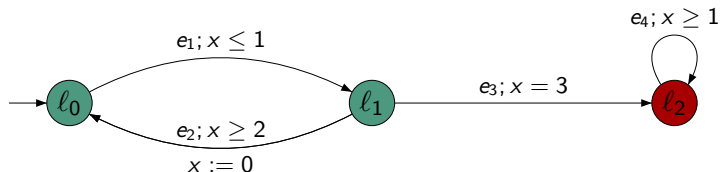

$Pol(e_1 e_2)$

$Pol(e_1 e_3)$

$Pol(e_1 \cdot)$

$Pol(\pi((\ell_0, 0), e_1 e_2))$ is of max. dim. in $Pol(\pi((\ell_0, 0), e_1 \cdot))$
$\dim(\pi((\ell_0, 0), e_1 e_2)) = \top$ $\dim(\pi((\ell_0, 0), e_1 e_3)) = \top$

Topology on runs

Topology T_A on $\text{Runs}(\mathcal{A}, s)$

Basic open sets of T_A are $\text{Cyl}(\pi)$ of defined dimension

From $s_0 = (\ell_0, 0)$, basic open sets are

$$\text{Cyl}(\pi(s, (e_1 e_2)^*)) \qquad \text{Cyl}(\pi(s, e_1(e_2 e_1)^*))$$

Meager and large sets

A set of runs X is nowhere dense if $\mathring{\bar{X}} = \emptyset$.

X is meager if it is a countable union of nowhere dense sets

X is large if its complement is meager

Meager and large sets

A set of runs X is nowhere dense if $\overset{\circ}{\bar{X}} = \emptyset$.

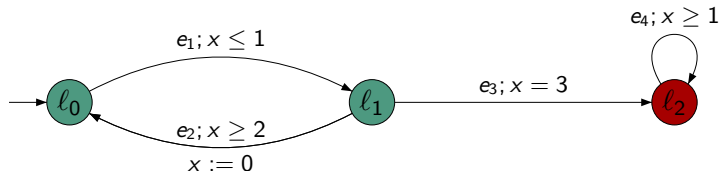X is meager if it is a countable union of nowhere dense sets

X is large if its complement is meager

- $\pi(s_0, e_1 e_3 e_4)$ is nowhere dense
- $\{\pi(s_0, (e_1 e_2)^* e_1 e_3 e_4^*)\}$ is meager
- $\{\pi(s_0, (e_1 e_2)^*)\} \cup \{\pi(s_0, e_1 (e_2 e_1)^*)\}$ is large

Large model-checking
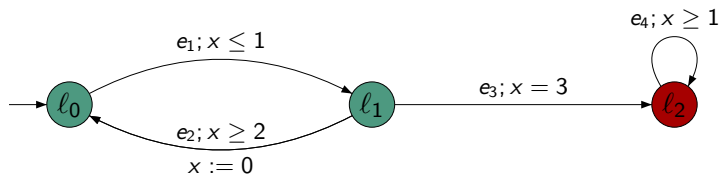
Large model-checking

Let φ be an LTL formula.

$$\mathcal{A} \approx_{\mathcal{T}} \varphi \quad \overset{\text{def}}{\Leftrightarrow} \quad \{\rho \mid \rho \models \varphi\} \text{ is large}$$

Large model-checking

Large model-checking

Let φ be an LTL formula.

$$\mathcal{A} \approx_T \varphi \quad \overset{\text{def}}{\Leftrightarrow} \quad \{\rho \mid \rho \models \varphi\} \text{ is large}$$

$\{\pi(s_0, (e_1 e_2)^*)\} \cup \{\pi(s_0, e_1(e_2 e_1)^*)\}$ is large

$$\mathcal{A} \approx_T \mathbf{G} \bullet$$

Banach-Mazur games

Let (E, T) be a topological space, $\mathcal{B}$ a basis of T and $C \subseteq E$.

- Player 1 picks some $B_1 \in \mathcal{B}$

Banach-Mazur games

Let (E, T) be a topological space, $\mathcal{B}$ a basis of T and $C \subseteq E$.

▶ Player 1 picks some $B_1 \in \mathcal{B}$

▶ Player 2 picks $B_2 \in \mathcal{B}$ such that $B_1 \supseteq B_2$

Banach-Mazur games

Let (E, T) be a topological space, $\mathcal{B}$ a basis of T and $C \subseteq E$.

- ▶ Player 1 picks some $B_1 \in \mathcal{B}$
- ▶ Player 2 picks $B_2 \in \mathcal{B}$ such that $B_1 \supseteq B_2$
- ▶ Player 1 picks $B_3 \in \mathcal{B}$ such that $B_1 \supseteq B_2 \supseteq B_3$

Banach-Mazur games

Let (E, T) be a topological space, $\mathcal{B}$ a basis of T and $C \subseteq E$.

- Player 1 picks some $B_1 \in \mathcal{B}$
- Player 2 picks $B_2 \in \mathcal{B}$ such that $B_1 \supseteq B_2$
- Player 1 picks $B_3 \in \mathcal{B}$ such that $B_1 \supseteq B_2 \supseteq B_3$
- and so on... $B_1 \supseteq B_2 \supseteq B_3 \supseteq B_4 \supseteq B_5 \cdots$

The play is winning for Player 1 whenever $\bigcap_{i=1}^{n} B_i \cap C \neq \emptyset$.
Otherwise Player 2 wins.

Banach-Mazur games

Let (E, T) be a topological space, $\mathcal{B}$ a basis of T and $C \subseteq E$.

- Player 1 picks some $B_1 \in \mathcal{B}$
- Player 2 picks $B_2 \in \mathcal{B}$ such that $B_1 \supseteq B_2$
- Player 1 picks $B_3 \in \mathcal{B}$ such that $B_1 \supseteq B_2 \supseteq B_3$
- and so on... $B_1 \supseteq B_2 \supseteq B_3 \supseteq B_4 \supseteq B_5 \cdots$

The play is winning for Player 1 whenever $\bigcap_{i=1}^{n} B_i \cap C \neq \emptyset$.
Otherwise Player 2 wins.

Theorem [Oxtoby 57]

Player 2 has a winning strategy iff C is meager.

Let's play Banach-Mazur games!

- Classical topology on $\mathbb{R}$,
  $\mathcal{B} = \{(r, r') \mid r \neq r' \in \mathbb{Q}\}$,
  $C = (0, 1)$.
  $\longrightarrow$ Player 1 can always choose B_{2i+1} included in a closed
  sub-interval of B_{2i}

  Player 1 wins the game, hence $(0, 1)$ is not meager.

Let's play Banach-Mazur games!

- Classical topology on $\mathbb{R}$,
  $\mathcal{B} = \{(r, r') \mid r \neq r' \in \mathbb{Q}\}$,
  $C = (0, 1)$.
  $\longrightarrow$ Player 1 can always choose B_{2i+1} included in a closed
  sub-interval of B_{2i}
  Player 1 wins the game, hence $(0, 1)$ is not meager.

- Topology on $\mathbb{R}$ induced by $\{(0, a) \mid 0 < a \leq 1\}$,
  $\mathcal{B} = \{(0, a) \mid 0 < a \leq 1\}$,
  $C = (0, 1)$.
  $\longrightarrow$ Player 2 can choose a subsequence of $(0, 1/2^i)$
  Player 2 has a winning strategy, hence $(0, 1)$ is meager.

Outline

Case of finite paths: Perfect match

Theorem

Let $\mathcal{A}$ be a timed automaton and $R(\mathcal{A})$ its region graph.

$$\mathcal{A}, s \models_{\mathbb{P}} \varphi \qquad \Leftrightarrow \qquad \mathcal{A}, s \models_T \varphi$$

Case of finite paths: Perfect match

Theorem

Let $\mathcal{A}$ be a timed automaton and $R(\mathcal{A})$ its region graph.

$$\mathcal{A}, s \models_{\mathbb{P}} \varphi \quad \Leftrightarrow \quad \mathcal{A}, s \models_T \varphi$$
$$\Updownarrow \qquad\qquad \Updownarrow$$
$$R(\mathcal{A}), s \models_{\mathbb{P}} \varphi \quad \Leftrightarrow \quad R(\mathcal{A}), s \models_T \varphi$$

Characterization:

$$\mathcal{A}, s \models \varphi \quad \Leftrightarrow \quad \forall \pi (\pi \not\models \varphi) \Rightarrow \mathsf{dim}(\pi) = \bot.$$

Case of finite paths: Perfect match

Theorem

Let $\mathcal{A}$ be a timed automaton and $R(\mathcal{A})$ its region graph.

$$
\begin{array}{ccc}
\mathcal{A}, s \models_{\mathbb{P}} \varphi & \Leftrightarrow & \mathcal{A}, s \approx_T \varphi \\
\Updownarrow & & \Updownarrow \\
R(\mathcal{A}), s \models_{\mathbb{P}} \varphi & \Leftrightarrow & R(\mathcal{A}), s \approx_T \varphi
\end{array}
$$

Characterization:

$$
\mathcal{A}, s \approx \varphi \quad \Leftrightarrow \quad \forall \pi (\pi \not\models \varphi) \Rightarrow \dim(\pi) = \bot.
$$

Theorem

Over finite timed words, the almost sure and large model-checking problems for LTL are PSPACE-Complete.

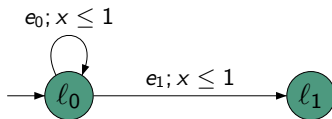# Extension to infinite paths

Naiv extension:

$$\mathbb{P}(s \models \varphi) = 1 \quad \Leftrightarrow \quad \forall \pi (\pi \not\models \varphi) \Rightarrow \dim(\pi) = \bot.$$

Extension to infinite paths

Naiv extension:

$$\mathbb{P}(s \models \varphi) = 1 \quad \Leftrightarrow \quad \forall \pi (\pi \not\models \varphi) \Rightarrow \mathsf{dim}(\pi) = \bot.$$

Hopeless

$\mathbb{P}(s_0 \models \mathbf{F}\, \ell_1) = 1$ but $\pi(s_0, e_0^\omega) \not\models \varphi$ and $\mathsf{dim}(\pi(s_0, e_0^\omega)) = \top$.
$\longrightarrow$ Need for fairness

Second attempt

Fair extension:

$$\mathbb{P}(s \models \varphi) = 1 \Leftrightarrow \forall \pi (\pi \text{ is fair} \wedge \pi \not\models \varphi) \Rightarrow \dim(\pi) = \bot.$$
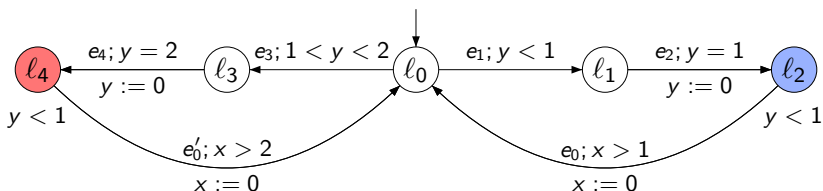
Fair path

$\pi(s, e_1 \cdots e_n)$ is *fair* if any transition with define dimension enabled infinitely often along π is taken infinitely often.

Second attempt

Fair extension:

$$\mathbb{P}(s \models \varphi) = 1 \Leftrightarrow \forall \pi (\pi \text{ is fair} \wedge \pi \not\models \varphi) \Rightarrow \dim(\pi) = \perp.$$

Hopeless $\qquad \varphi = \mathbf{G}\,\mathbf{F}\,\ell_4 \wedge \mathbf{G}\,\mathbf{F}\,\ell_2$

π fair $\Rightarrow \pi \models \varphi$

Hence $\forall \pi (\pi \text{ is fair} \wedge \pi \not\models \varphi) \Rightarrow \dim(\pi) = \perp.$ But $\mathbb{P}(\varphi) < 1.$

$\longrightarrow$ Restriction on the number of clocks

Results

$\mathcal{A}$ single-clock timed automaton

Theorem

Let s be a state of $\mathcal{A}$ and φ and LTL formula.

$$\mathbb{P}(s \models \varphi) = 1 \quad \Leftrightarrow \quad \forall \pi (\pi \text{ is fair} \wedge \pi \not\models \varphi) \Rightarrow \dim(\pi) = \bot$$
$$\Leftrightarrow \quad \{\pi \mid \pi \text{ is fair} \wedge \pi \models \varphi\} \text{ is large}$$

Results

$\mathcal{A}$ single-clock timed automaton

Theorem

Let s be a state of $\mathcal{A}$ and φ and LTL formula.

$$\mathbb{P}(s \models \varphi) = 1 \quad \Leftrightarrow \quad \forall \pi (\pi \text{ is fair} \wedge \pi \not\models \varphi) \Rightarrow \dim(\pi) = \bot$$
$$\Leftrightarrow \quad \{\pi \mid \pi \text{ is fair} \wedge \pi \models \varphi\} \text{ is large}$$

Characterization: BSCC of $R(\mathcal{A})$

Theorem

The almost sure model-checking problem of LTL for single-clock timed automata is PSPACE-Complete.

Outline

Related work

Robustness

- ▶ robust timed automata   [GHJ97,HR00]
- ▶ robust model-checking
               [Puri98,DDR04,DDMR04,ALM05,BMR06,BMR08]

Related work

Robustness

- robust timed automata   [GHJ97,HR00]
- robust model-checking

                    [Puri98,DDR04,DDMR04,ALM05,BMR06,BMR08]

Probabilistic timed models

- probabilistic timed automata *à la* PRISM   [KNSS02]
- real-time probabilistic systems   [ACD91,ACD92]
- continuous-time Markov chains   [BHHK03]

Outline

Conclusion

Summary

▶ probabilistic semantics for timed automata to rule out unlikely events

▶ equivalent topological semantics

▶ decision algorithm for qualitative LTL almost-sure/fair model-checking
  ▶ for finite runs
  ▶ for infinite runs in one-clock timed automata

Conclusion

Summary

- ▶ probabilistic semantics for timed automata to rule out unlikely events
- ▶ equivalent topological semantics
- ▶ decision algorithm for qualitative LTL almost-sure/fair model-checking
  - ▶ for finite runs
  - ▶ for infinite runs in one-clock timed automata

On-going work

- ▶ quantitative model-checking
- ▶ verification of timed logics
- ▶ timed games with a probabilistic semantics