A Probabilistic Semantics for Timed Automata

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

[1]Technische Universität Dresden – Germany

[2]Oxford University Computing Laboratory – UK

[3]LSV – CNRS & ENS Cachan – France

Motivation(s)

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

Motivation(s)

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

Motivation(s)

- 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]

Motivation(s)

- 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...

Motivation(s)

- 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]

Motivation(s)

- 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

Motivation(s)

- 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]

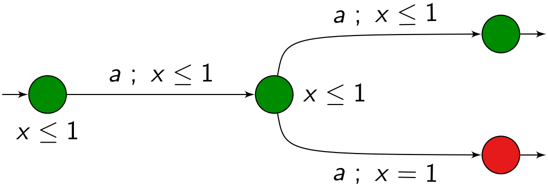
- In a model, only few traces may violate the correctness property: they may hence not be relevant...

➜ topological notion of tube acceptance in [GHJ97]

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

Aim: Use probabilities to “relax” the semantics of timed automata

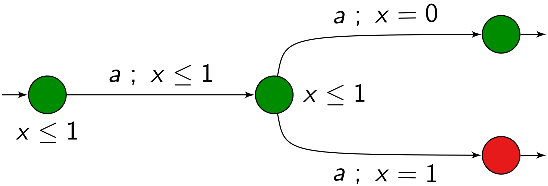
Initial example



Intuition: from the initial state,

this automaton *almost-surely* satisfies “**G** ”

The limits of intuition...



Does it *almost-surely* satisfy "$\mathbf{F}$ ●"?

Our proposition

$\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})$: symbolic path starting in s and firing edges $e_1, \dots, e_n$

Our proposition

$\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})$: symbolic path starting in s and firing edges $e_1, \dots, e_n$

$$\mathbb{P}\left(\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) = \frac{1}{2} \int_{t \in I(s,e_1)} \frac{\mathbb{P}\left(\pi(s_t \xrightarrow{e_2} \dots \xrightarrow{e_n})\right)}{\#\{I(s,e) \mid t \in I(s,e)\}} \mathrm{d}\mu_s(t)$$

where $s \xrightarrow{t,e_1} s_t$

Our proposition

$\pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n})$: symbolic path starting in s and firing edges $e_1, \ldots, e_n$

$$\mathbb{P}\left(\pi(s \xrightarrow{e_1} \ldots \xrightarrow{e_n})\right) = \frac{1}{2} \int_{t \in I(s,e_1)} \frac{\mathbb{P}\left(\pi(s_t \xrightarrow{e_2} \ldots \xrightarrow{e_n})\right)}{\#\{I(s,e) \mid t \in I(s,e)\}} \mathrm{d}\mu_s(t)$$

where $s \xrightarrow{t,e_1} s_t$

- μ_s: "reasonable" probability measure over all possible delays $I(s)$

Our proposition

$\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})$: symbolic path starting in s and firing edges $e_1, \dots, e_n$

$$\mathbb{P}\left(\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) = \frac{1}{2} \int_{t \in I(s,e_1)} \frac{\mathbb{P}\left(\pi(s_t \xrightarrow{e_2} \dots \xrightarrow{e_n})\right)}{\#\{I(s,e) \mid t \in I(s,e)\}} \mathrm{d}\mu_s(t)$$

where $s \xrightarrow{t,e_1} s_t$

- μ_s: "reasonable" probability measure over all possible delays $I(s)$
  - $\mathrm{d}\mu_s(t)$: probability of waiting t t.u.

Our proposition

$\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})$: symbolic path starting in s and firing edges $e_1, \dots, e_n$

$$\mathbb{P}\left(\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) = \frac{1}{2} \int_{t \in I(s,e_1)} \frac{\mathbb{P}\left(\pi(s_t \xrightarrow{e_2} \dots \xrightarrow{e_n})\right)}{\#\{I(s,e) \mid t \in I(s,e)\}} \mathrm{d}\mu_s(t)$$

where $s \xrightarrow{t,e_1} s_t$

- μ_s: "reasonable" probability measure over all possible delays $I(s)$
  - $\mathrm{d}\mu_s(t)$: probability of waiting t t.u.
- $\#\{I(s,e) \mid t \in I(s,e)\}$: number of transitions that can be fired after having delayed t t.u. from s

Our proposition

$\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})$: symbolic path starting in s and firing edges $e_1, \dots, e_n$

$$\mathbb{P}\left(\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) = \frac{1}{2} \int_{t \in I(s,e_1)} \frac{\mathbb{P}\left(\pi(s_t \xrightarrow{e_2} \dots \xrightarrow{e_n})\right)}{\#\{I(s,e) \mid t \in I(s,e)\}} \mathrm{d}\mu_s(t)$$

where $s \xrightarrow{t,e_1} s_t$

- μ_s: "reasonable" probability measure over all possible delays $I(s)$
  - $\mathrm{d}\mu_s(t)$: probability of waiting t t.u.
- $\#\{I(s,e) \mid t \in I(s,e)\}$: number of transitions that can be fired after having delayed t t.u. from s
- $\mathbb{P}\left(\pi(s_t \xrightarrow{e_2} \dots \xrightarrow{e_n})\right)$: probability of firing $e_2, \dots, e_n$ after s_t

Our proposition

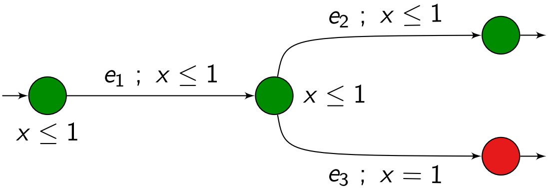
$\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})$: symbolic path starting in s and firing edges $e_1, \dots, e_n$

$$\mathbb{P}\left(\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) = \frac{1}{2}\int_{t \in I(s,e_1)} \frac{\mathbb{P}\left(\pi(s_t \xrightarrow{e_2} \dots \xrightarrow{e_n})\right)}{\#\{I(s,e) \mid t \in I(s,e)\}} \mathrm{d}\mu_s(t)$$

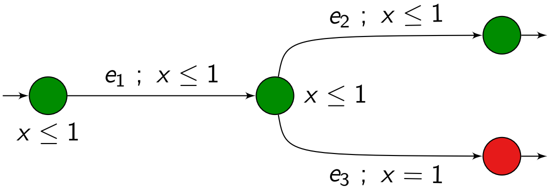
where $s \xrightarrow{t,e_1} s_t$

- μ_s: "reasonable" probability measure over all possible delays $I(s)$
  - $\mathrm{d}\mu_s(t)$: probability of waiting t t.u.
- $\#\{I(s,e) \mid t \in I(s,e)\}$: number of transitions that can be fired after having delayed t t.u. from s
- $\mathbb{P}\left(\pi(s_t \xrightarrow{e_2} \dots \xrightarrow{e_n})\right)$: probability of firing $e_2, \dots, e_n$ after s_t
- $\frac{1}{2}$: normalization factor

Back to the first example

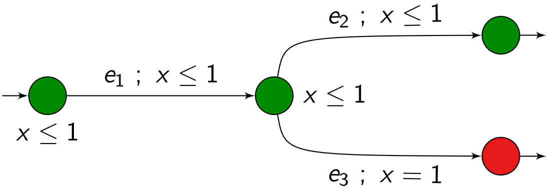


Back to the first example



The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})$ is $\frac{1}{8}$, hence > 0!

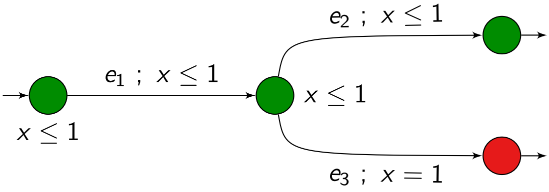
Back to the first example



The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})$ is $\frac{1}{8}$, hence > 0!

The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_3})$ is 0!

Back to the first example

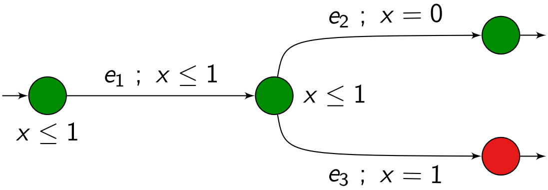


The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})$ is $\frac{1}{8}$, hence > 0!

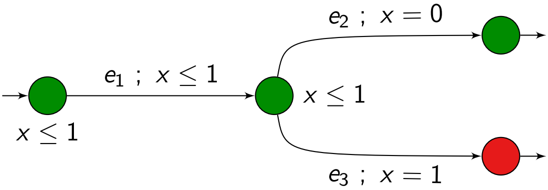
The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_3})$ is 0!

Moreover, $\mathbb{P}\Big(\mathbf{G} \mid \text{accepting}\Big) = 1$.

Back to the second example

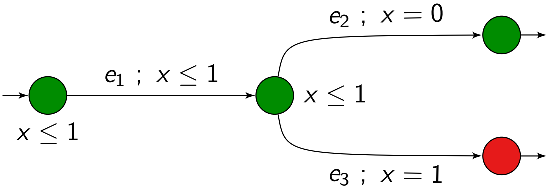


Back to the second example



The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})$ is 0!

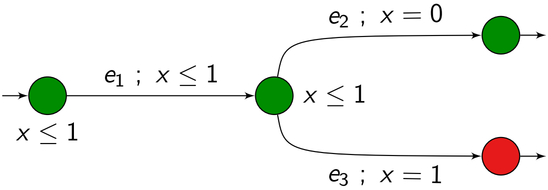
Back to the second example



The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})$ is 0!

The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_3})$ is $\frac{1}{8}$, hence > 0!

Back to the second example



The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_2})$ is 0!

The probability of the symbolic path $\pi(s_0 \xrightarrow{e_1}\xrightarrow{e_3})$ is $\frac{1}{8}$, hence > 0!

Moreover, $\mathbb{P}\Big(\mathbf{F}\ \mid \text{accepting}\Big) = 1$.

Properties of $\mathbb{P}$

Lemma

If s is a state, then $\mathbb{P}\left(\bigcup_{n\in\mathbb{N}}\bigcup_{e_1,\dots,e_n}\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) = 1$.

Properties of $\mathbb{P}$

Lemma

If s is a state, then $\mathbb{P}\left(\bigcup_{n\in\mathbb{N}}\bigcup_{e_1,\dots,e_n}\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) = 1$.

Lemma

If s and s' are region-equivalent, then

$$\mathbb{P}\left(\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) > 0 \quad\Leftrightarrow\quad \mathbb{P}\left(\pi(s' \xrightarrow{e_1} \dots \xrightarrow{e_n})\right) > 0.$$

Qualitative probabilistic model-checking

If φ is an LTL formula, then we define:

$$\begin{cases} s_0 \approx\!\!\!\!\mid_{\forall} \varphi & \overset{\text{def}}{\Leftrightarrow} \quad \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} = 1, \\ s_0 \approx\!\!\!\!\mid_{\exists} \varphi & \overset{\text{def}}{\Leftrightarrow} \quad \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} > 0. \end{cases}$$

Qualitative probabilistic model-checking

If φ is an LTL formula, then we define:

$$\begin{cases} s_0 \mathrel{|\!\!\approx_\forall} \varphi & \stackrel{\text{def}}{\Leftrightarrow} & \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} = 1, \\ s_0 \mathrel{|\!\!\approx_\exists} \varphi & \stackrel{\text{def}}{\Leftrightarrow} & \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} > 0. \end{cases}$$

This definition extends naturally to CTL* specifications...

Qualitative probabilistic model-checking

If φ is an LTL formula, then we define:

$$\begin{cases} s_0 \mathrel{|\!\!\approx_\forall} \varphi & \stackrel{\text{def}}{\Leftrightarrow} & \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} = 1, \\ s_0 \mathrel{|\!\!\approx_\exists} \varphi & \stackrel{\text{def}}{\Leftrightarrow} & \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} > 0. \end{cases}$$

This definition extends naturally to CTL* specifications...

We wish:

1. to be convinced this definition is not all nonsense,

Qualitative probabilistic model-checking

If φ is an LTL formula, then we define:

$$\begin{cases} s_0 \mathrel{|\!\!\approx_\forall} \varphi & \overset{\text{def}}{\Leftrightarrow} \quad \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} = 1, \\ s_0 \mathrel{|\!\!\approx_\exists} \varphi & \overset{\text{def}}{\Leftrightarrow} \quad \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} > 0. \end{cases}$$

This definition extends naturally to CTL* specifications...

We wish:

1. to be convinced this definition is not all nonsense,
   $\longrightarrow$ topological characterization

Qualitative probabilistic model-checking

If φ is an LTL formula, then we define:

$$\begin{cases} s_0 \approx\!\!\!\!\models_\forall \varphi & \stackrel{\text{def}}{\Leftrightarrow} \quad \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} = 1, \\ s_0 \approx\!\!\!\!\models_\exists \varphi & \stackrel{\text{def}}{\Leftrightarrow} \quad \mathbb{P}\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\} > 0. \end{cases}$$

This definition extends naturally to CTL* specifications...

We wish:

1. to be convinced this definition is not all nonsense,
   $\longrightarrow$ topological characterization
2. to decide qualitative model-checking.

Some topology

Which notion of topology is suitable?

Some topology

Which notion of topology is suitable?

- we need a property *toto* such that if A is *toto*, then A^c is not *toto* (because $\mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\}) = 1 - \mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \not\models \varphi\})$)

Some topology

Which notion of topology is suitable?

- we need a property *toto* such that if A is *toto*, then A^c is not *toto* (because $\mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\}) = 1 - \mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \not\models \varphi\})$)
- that cannot be density [VV06]

Some topology

Which notion of topology is suitable?

- we need a property *toto* such that if A is *toto*, then A^c is not *toto* (because $\mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\}) = 1 - \mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \not\models \varphi\})$)
- that cannot be density [VV06]
  ex: $\mathbb{Q}$ is dense in $\mathbb{R}$, and $\mathbb{R} \setminus \mathbb{Q}$ is also dense in $\mathbb{R}$

Some topology

Which notion of topology is suitable?

- we need a property *toto* such that if A is *toto*, then A^c is not *toto*
  (because $\mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\}) = 1 - \mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \not\models \varphi\})$)
- that cannot be density [VV06]
  ex: $\mathbb{Q}$ is dense in $\mathbb{R}$, and $\mathbb{R} \setminus \mathbb{Q}$ is also dense in $\mathbb{R}$
- that can be **largeness** and **meagerness**!

Some topology

Which notion of topology is suitable?

- we need a property *toto* such that if A is *toto*, then A^c is not *toto* (because $\mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\}) = 1 - \mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \not\models \varphi\})$)

- that cannot be density [VV06]
  ex: $\mathbb{Q}$ is dense in $\mathbb{R}$, and $\mathbb{R} \setminus \mathbb{Q}$ is also dense in $\mathbb{R}$

- that can be **largeness** and **meagerness**!
  - a set B is nowhere dense if $\mathring{\overline{B}} = \emptyset$,
  - a set B is meager if it is a countable union of nowhere dense sets,
  - a set B is large if its complement is meager.

Some topology

Which notion of topology is suitable?

- we need a property *toto* such that if A is *toto*, then A^c is not *toto* (because $\mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\}) = 1 - \mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \not\models \varphi\})$)

- that cannot be density [VV06]
  ex: $\mathbb{Q}$ is dense in $\mathbb{R}$, and $\mathbb{R} \setminus \mathbb{Q}$ is also dense in $\mathbb{R}$

- that can be **largeness** and **meagerness**!
  - a set B is nowhere dense if $\mathring{\overline{B}} = \emptyset$,
  - a set B is meager if it is a countable union of nowhere dense sets,
  - a set B is large if its complement is meager.

  ex: $\mathbb{Q}$ is meager and $\mathbb{R} \setminus \mathbb{Q}$ is large in $\mathbb{R}$

Some topology

Which notion of topology is suitable?

- we need a property *toto* such that if A is *toto*, then A^c is not *toto* (because $\mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \models \varphi\}) = 1 - \mathbb{P}(\{\varrho \in \mathsf{Runs}(s_0) \mid \varrho \not\models \varphi\})$)
- that cannot be density [VV06]
  ex: $\mathbb{Q}$ is dense in $\mathbb{R}$, and $\mathbb{R} \setminus \mathbb{Q}$ is also dense in $\mathbb{R}$
- that can be **largeness** and **meagerness**!
  - a set B is nowhere dense if $\mathring{\overline{B}} = \emptyset$,
  - a set B is meager if it is a countable union of nowhere dense sets,
  - a set B is large if its complement is meager.

  ex: $\mathbb{Q}$ is meager and $\mathbb{R} \setminus \mathbb{Q}$ is large in $\mathbb{R}$

These notions are abstract but enjoy a very nice characterization using Banach-Mazur games!

Banach-Mazur games

$(A, \mathcal{T})$ topological space, $\mathcal{B}$ a family of subsets of A such that:

- for all $B \in \mathcal{B}$, $\mathring{B} \neq \emptyset$,
- if O is a non-empty open set, there exists $B \in \mathcal{B}$ s.t. $B \subseteq O$.

Banach-Mazur games

$(A, \mathcal{T})$ topological space, $\mathcal{B}$ a family of subsets of A such that:

- for all $B \in \mathcal{B}$, $\mathring{B} \neq \emptyset$,
- if O is a non-empty open set, there exists $B \in \mathcal{B}$ s.t. $B \subseteq O$.

We fix $C \subseteq A$. The game is then as follows:

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

Banach-Mazur games

$(A, \mathcal{T})$ topological space, $\mathcal{B}$ a family of subsets of A such that:

- for all $B \in \mathcal{B}$, $\mathring{B} \neq \emptyset$,
- if O is a non-empty open set, there exists $B \in \mathcal{B}$ s.t. $B \subseteq O$.

We fix $C \subseteq A$. The game is then as follows:

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

Banach-Mazur games

$(A, \mathcal{T})$ topological space, $\mathcal{B}$ a family of subsets of A such that:

- for all $B \in \mathcal{B}$, $\mathring{B} \neq \emptyset$,
- if O is a non-empty open set, there exists $B \in \mathcal{B}$ s.t. $B \subseteq O$.

We fix $C \subseteq A$. The game is then as follows:

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

Banach-Mazur games

$(A, \mathcal{T})$ topological space, $\mathcal{B}$ a family of subsets of A such that:

- for all $B \in \mathcal{B}$, $\mathring{B} \neq \emptyset$,
- if O is a non-empty open set, there exists $B \in \mathcal{B}$ s.t. $B \subseteq O$.

We fix $C \subseteq A$. The game is then as follows:

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

Banach-Mazur games

$(A, \mathcal{T})$ topological space, $\mathcal{B}$ a family of subsets of A such that:

- for all $B \in \mathcal{B}$, $\mathring{B} \neq \emptyset$,
- if O is a non-empty open set, there exists $B \in \mathcal{B}$ s.t. $B \subseteq O$.

We fix $C \subseteq A$. The game is then as follows:

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

Player 1 wins the game whenever $\bigcap_{i=1}^{\infty} B_i \cap C \neq \emptyset$. Otherwise Player 2 wins the game.

Banach-Mazur games

$(A, \mathcal{T})$ topological space, $\mathcal{B}$ a family of subsets of A such that:

- for all $B \in \mathcal{B}$, $\mathring{B} \neq \emptyset$,
- if O is a non-empty open set, there exists $B \in \mathcal{B}$ s.t. $B \subseteq O$.

We fix $C \subseteq A$. The game is then as follows:

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

Player 1 wins the game whenever $\bigcap_{i=1}^{\infty} B_i \cap C \neq \emptyset$. Otherwise Player 2 wins the game.

Theorems

- Banach-Mazur games are not determined.
- [Oxtoby57] Player 2 has a winning strategy iff C is meager.

Let's play Banach-Mazur games!

- Classical topology on $\mathbb{R}$,
  $\mathcal{B} = \{$all non-empty intervals with rational bounds$\}$.
  Take $C = (0, 1)$.

Let's play Banach-Mazur games!

- Classical topology on $\mathbb{R}$,
  $\mathcal{B} = \{$all non-empty intervals with rational bounds$\}$.
  Take $C = (0, 1)$.

  Then Player 1 has a winning strategy! Hence, C is not meager.

Let's play Banach-Mazur games!

- Classical topology on $\mathbb{R}$,
  $\mathcal{B} = \{$all non-empty intervals with rational bounds$\}$.
  Take $C = (0, 1)$.

  Then Player 1 has a winning strategy! Hence, C is not meager.

- Topological space $(\mathbb{R}, \mathcal{T})$ with
  $$\text{basis}(\mathcal{T}) = \{\emptyset\} \cup \{(i, i + 2^{-n}) \mid i \in \mathbb{Z},\ n \in \mathbb{N}\} \cup \{\mathbb{R}\},$$
  $\mathcal{B} = \text{basis}(\mathcal{T}) \setminus \{\emptyset\}$.
  Take $C = (0, 1)$.

Let's play Banach-Mazur games!

- Classical topology on $\mathbb{R}$,
  $\mathcal{B} = \{$all non-empty intervals with rational bounds$\}$.
  Take $C = (0, 1)$.

  Then Player 1 has a winning strategy! Hence, C is not meager.

- Topological space $(\mathbb{R}, \mathcal{T})$ with
  $$\text{basis}(\mathcal{T}) = \{\emptyset\} \cup \{(i, i + 2^{-n}) \mid i \in \mathbb{Z},\ n \in \mathbb{N}\} \cup \{\mathbb{R}\},$$
  $\mathcal{B} = \text{basis}(\mathcal{T}) \setminus \{\emptyset\}$.
  Take $C = (0, 1)$.

  Then Player 2 has a winning strategy! Hence, C is meager.

Some remarks

- There is no relation between open and meager sets.

Some remarks

- There is no relation between open and meager sets.
- A topological space where every non-empty open set is not meager is called a Baire space.

Some remarks

- There is no relation between open and meager sets.
- A topological space where every non-empty open set is not meager is called a Baire space.

  ex: $\mathbb{R}$ is a Baire space, $\mathbb{Q}$ is not a Baire space.

Topology over timed automata

- Notion of dimension (on blackboard).

Topology over timed automata

- Notion of dimension (on blackboard).
- This notion is region-invariant.

Topology over timed automata

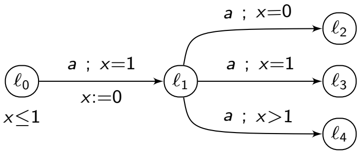
- Notion of dimension (on blackboard).
- This notion is region-invariant.
- We define a topology on a timed automaton, whose basic open sets are symbolic paths π such that $\dim(\pi)$ is defined and the set of all paths.

Topology over timed automata

- Notion of dimension (on blackboard).
- This notion is region-invariant.
- We define a topology on a timed automaton, whose basic open sets are symbolic paths π such that $\dim(\pi)$ is defined and the set of all paths.
- NB: this topological space is a Baire space.

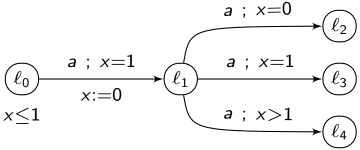
Topology over timed automata

- Notion of dimension (on blackboard).
- This notion is region-invariant.
- We define a topology on a timed automaton, whose basic open sets are symbolic paths π such that $\dim(\pi)$ is defined and the set of all paths.
- NB: this topological space is a Baire space.
- **ex:**



Topology over timed automata

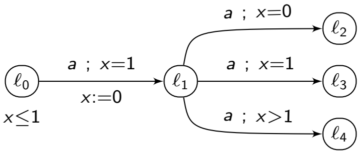
- Notion of dimension (on blackboard).
- This notion is region-invariant.
- We define a topology on a timed automaton, whose basic open sets are symbolic paths π such that $\dim(\pi)$ is defined and the set of all paths.
- NB: this topological space is a Baire space.
- **ex:**



  - only π_0, π_1 and π_4 have a dimension, they are thus open sets,

Topology over timed automata

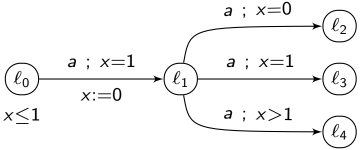
- Notion of dimension (on blackboard).
- This notion is region-invariant.
- We define a topology on a timed automaton, whose basic open sets are symbolic paths π such that $\dim(\pi)$ is defined and the set of all paths.
- NB: this topological space is a Baire space.
- **ex:**



  - only π_0, π_1 and π_4 have a dimension, they are thus open sets,
  - $\pi_2 \cup \pi_3$ is a closed set,

Topology over timed automata

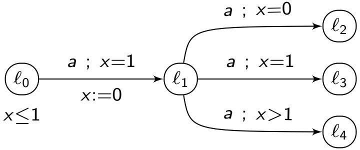
- Notion of dimension (on blackboard).
- This notion is region-invariant.
- We define a topology on a timed automaton, whose basic open sets are symbolic paths π such that $\dim(\pi)$ is defined and the set of all paths.
- NB: this topological space is a Baire space.
- **ex:**



  - only π_0, π_1 and π_4 have a dimension, they are thus open sets,
  - $\pi_2 \cup \pi_3$ is a closed set,
  - π_2 is nowhere dense, and so is π_3,

Topology over timed automata

- Notion of dimension (on blackboard).
- This notion is region-invariant.
- We define a topology on a timed automaton, whose basic open sets are symbolic paths π such that $\dim(\pi)$ is defined and the set of all paths.
- NB: this topological space is a Baire space.
- **ex:**



  - only π_0, π_1 and π_4 have a dimension, they are thus open sets,
  - $\pi_2 \cup \pi_3$ is a closed set,
  - π_2 is nowhere dense, and so is π_3,
  - $\pi_2 \cup \pi_3$ is meager, and $\pi_0 \cup \pi_1 \cup \pi_4$ is large.

Probabilistic semantics *vs* topology

- If π is a symbolic path in $R(\mathcal{A})$, then

$$\mathbb{P}_{R(\mathcal{A})}(\pi) > 0 \Leftrightarrow \mathsf{dim}_{R(\mathcal{A})}(\pi) \text{ defined}$$

Probabilistic semantics *vs* topology

- If π is a symbolic path in $R(\mathcal{A})$, then

$$\mathbb{P}_{R(\mathcal{A})}(\pi) > 0 \Leftrightarrow \mathsf{dim}_{R(\mathcal{A})}(\pi) \text{ defined}$$

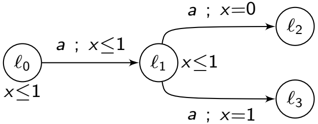
- If π is a symbolic path in $\mathcal{A}$, $\mathbb{P}_{\mathcal{A}}(\pi) = \sum_{\varsigma \in \iota(\pi)} \mathbb{P}_{R(\mathcal{A})}(\varsigma)$

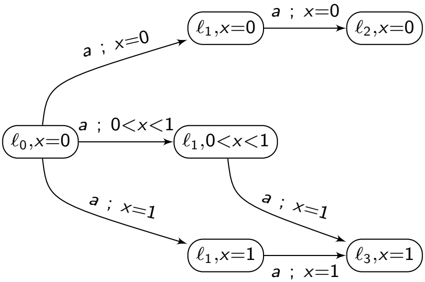
Probabilistic semantics *vs* topology

- If π is a symbolic path in $R(\mathcal{A})$, then

$$\mathbb{P}_{R(\mathcal{A})}(\pi) > 0 \Leftrightarrow \dim_{R(\mathcal{A})}(\pi) \text{ defined}$$

- If π is a symbolic path in $\mathcal{A}$, $\mathbb{P}_{\mathcal{A}}(\pi) = \sum_{\varsigma \in \iota(\pi)} \mathbb{P}_{R(\mathcal{A})}(\varsigma)$





Probabilistic semantics *vs* topology (2)

Theorem

Let $\mathcal{A}$ be a timed automaton, s_0 a state of $\mathcal{A}$, and φ an LTL formula. Then,

$$\begin{array}{rcl} \mathcal{A}, s_0 \mathrel{|}\!\!\approx_\forall \varphi & \stackrel{\text{def}}{\Leftrightarrow} & \text{w.r.t. } \mathbb{P}\text{, almost all paths from } s_0 \text{ in } \mathcal{A} \text{ satisfy } \varphi \\ & \Leftrightarrow & \text{the paths of } R(\mathcal{A}) \text{ from } s_0 \text{ not satisfying } \varphi \text{ have an undefined dimension} \\ & \Leftrightarrow & \text{the set of paths of } R(\mathcal{A}) \text{ from } s_0 \text{ satisfying } \varphi \text{ is (topologically) large} \end{array}$$

(simple application of Banach-Mazur games)

From an algorithmic point-of-view

Theorem

Over finite timed words, the almost-sure ($\models\!\!\!\approx_\forall$) and the positive ($\models\!\!\!\approx_\exists$) LTL model-checking problems over non-blocking timed automata are PSPACE-Complete.

Some remarks

- the probabilistic semantics can be defined for a larger class of systems, for instance hybrid systems with a finite bisimulation quotient

Related works

- Other "probabilistic and timed" (automata-)based models

Related works

- Other “probabilistic and timed” (automata-)based models
  - probabilistic timed automata *à la* PRISM [KNSS02]

Related works

- Other "probabilistic and timed" (automata-)based models
  - probabilistic timed automata *à la* PRISM [KNSS02]
  - real-time probabilistic systems [ACD91,ACD92]

Related works

- Other "probabilistic and timed" (automata-)based models
  - probabilistic timed automata *à la* PRISM [KNSS02]
  - real-time probabilistic systems [ACD91,ACD92]
  - dense-time Markov chains [BHHK03]

Related works

- Other "probabilistic and timed" (automata-)based models
  - probabilistic timed automata *à la* PRISM [KNSS02]
  - real-time probabilistic systems [ACD91,ACD92]
  - dense-time Markov chains [BHHK03]

NB: our model is more general than dense-time Markov chains, and by slightly extending our model, our model becomes more general than probabilistic timed automata

Related works

- Other “probabilistic and timed” (automata-)based models
  - probabilistic timed automata *à la* PRISM [KNSS02]
  - real-time probabilistic systems [ACD91,ACD92]
  - dense-time Markov chains [BHHK03]

  NB: our model is more general than dense-time Markov chains, and by slightly extending our model, our model becomes more general than probabilistic timed automata

- Labelled Markov processes over a continuum [DGJP03,04]

Related works

- Other "probabilistic and timed" (automata-)based models
  - probabilistic timed automata *à la* PRISM [KNSS02]
  - real-time probabilistic systems [ACD91,ACD92]
  - dense-time Markov chains [BHHK03]

  NB: our model is more general than dense-time Markov chains, and by slightly extending our model, our model becomes more general than probabilistic timed automata

- Labelled Markov processes over a continuum [DGJP03,04]

- Strong relation with robustness

Related works

- Other "probabilistic and timed" (automata-)based models
  - probabilistic timed automata *à la* PRISM [KNSS02]
  - real-time probabilistic systems [ACD91,ACD92]
  - dense-time Markov chains [BHHK03]

  NB: our model is more general than dense-time Markov chains, and by slightly extending our model, our model becomes more general than probabilistic timed automata

- Labelled Markov processes over a continuum [DGJP03,04]

- Strong relation with robustness
  - robust timed automata [GHJ97,HR00]
  - robust model-checking [Puri98,DDR04,DDMR04,ALM05,BMR06]

Conclusions

Conclusion

- a probabilistic semantics for timed automata which removes "unlikely" events,
- qualitative model-checking has a topological interpretation,
- decidability of qualitative LTL model-checking.

Conclusions

Conclusion

- a probabilistic semantics for timed automata which removes "unlikely" events,
- qualitative model-checking has a topological interpretation,
- decidability of qualitative LTL model-checking.

Further work

- extend to infinite paths,
- quantitative analysis,
- timed objectives,
- ...

Conclusions

Conclusion

- a probabilistic semantics for timed automata which removes "unlikely" events,
- qualitative model-checking has a topological interpretation,
- decidability of qualitative LTL model-checking.

Further work

- extend to infinite paths,
- quantitative analysis,
- timed objectives,
- ...

Some possible improvements?

- handle accepting states,
- the normalization factor $\frac{1}{2}$ is not completely satisfactory,
- discount time, not the number of transitions,
- ...

Extension to infinite timed words

- definition: straightforward extension to cylinders
- non-trivial to decide...

Extension to infinite timed words

- definition: straightforward extension to cylinders
- non-trivial to decide...

For one-clock timed automata,

- we can decide qualitative LTL model-checking
- we have properties like

$$\mathbb{P}(\text{Zeno behaviours}) = 0$$

if the automaton is not "degenerated"