

Quantitative Model-Checking of One-Clock Timed Automata under Probabilistic Semantics

Nathalie Bertrand¹, Patricia Bouyer²,
Thomas Brihaye³, Nicolas Markey²

¹INRIA Rennes, France

²LSV, CNRS & ENS Cachan, France

³Université Mons-Hainaut, Belgium

September 15th 2008

Outline

- 1 Probabilistic semantics
 - Motivations
 - Definition
 - Qualitative model-checking
- 2 Quantitative model-checking
 - Problem definition
 - Abstraction
 - Approximation method
- 3 Conclusion

Motivations

Aim: propose an alternative semantics for timed automata to measure how likely properties are satisfied.

Motivations

Aim: propose an alternative semantics for timed automata to measure how likely properties are satisfied.

- ▶ Relax the idealized semantics of timed automata
 - ▶ Only few traces may violate a property ; they might come from assumptions made in timed automata: infinite precision, instantaneous events, etc.
 - ▶ Related works: robust semantics, implementability issues, etc.

Motivations

Aim: propose an alternative semantics for timed automata to measure how likely properties are satisfied.

- ▶ Relax the idealized semantics of timed automata
 - ▶ Only few traces may violate a property ; they might come from assumptions made in timed automata: infinite precision, instantaneous events, etc.
 - ▶ Related works: robust semantics, implementability issues, etc.
- ▶ Propose a new timed and probabilistic model
 - ▶ Related models: continuous-time Markov chains, probabilistic timed automata.

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

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

Probabilistic semantics

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

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

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

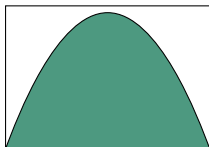
$$\mathbb{P}(\pi(s \xrightarrow{e_1} \dots \xrightarrow{e_n})) = \int_{t \in I(s, e_1)} p_{s+t}(e_1) \cdot \mathbb{P}(\pi(s_t \xrightarrow{e_2} \dots \xrightarrow{e_n})) d\mu_s(t)$$

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

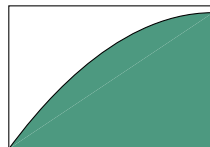
Examples of μ_s when $I(s)$ is a bounded interval



$I(s)$



$I(s)$



$I(s)$

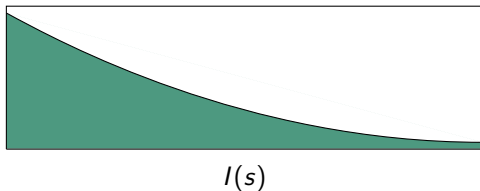
Probabilistic semantics

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

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

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

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



Probabilistic semantics

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

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

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

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

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

Probabilistic semantics

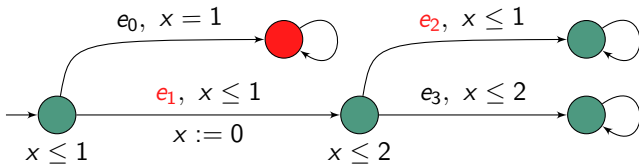
- Intuitively:** From state s ,
1. randomly choose a delay
 2. randomly select an edge

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

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

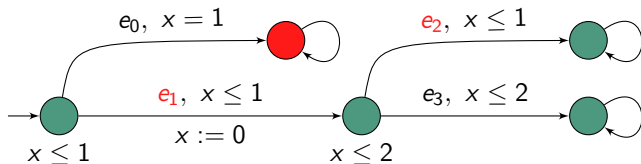
→ Extension of the probability measure to the σ -algebra generated by the cylinders.

Example



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

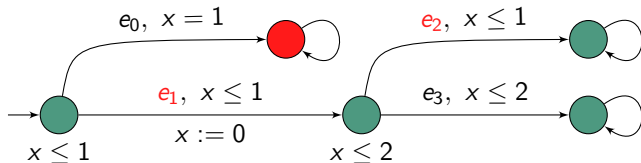
Example



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

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

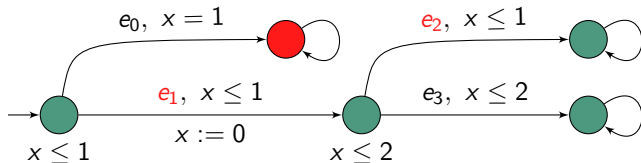
Example



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

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

Example



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

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

Almost-sure model checking

Almost-sure model-checking

Let φ be an ω -regular property. $\mathcal{A} \approx_{\mathbb{P}} \varphi \stackrel{\text{def}}{\iff} \mathbb{P}(\{\rho \mid \rho \models \varphi\}) = 1$

Almost-sure model checking

Almost-sure model-checking

Let φ be an ω -regular property. $\mathcal{A} \approx_{\mathbb{P}} \varphi \stackrel{\text{def}}{\iff} \mathbb{P}(\{\rho \mid \rho \models \varphi\}) = 1$

Theorem [BBBBG LICS'08]

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

Almost-sure model checking

Almost-sure model-checking

Let φ be an ω -regular property. $\mathcal{A} \approx_{\mathbb{P}} \varphi \stackrel{\text{def}}{\iff} \mathbb{P}(\{\rho \mid \rho \models \varphi\}) = 1$

Theorem [BBBBG LICS'08]

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

Proof ideas:

► Complexity:

- size of single-clock region automata = polynomial [LMS04]
- consider a Markov chain version of the region graph and apply result of [CSS03] to it

Almost-sure model checking

Almost-sure model-checking

Let φ be an ω -regular property. $\mathcal{A} \approx_{\mathbb{P}} \varphi \stackrel{\text{def}}{\Leftrightarrow} \mathbb{P}(\{\rho \mid \rho \models \varphi\}) = 1$

Theorem [BBBBG LICS'08]

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

Proof ideas:

- ▶ **Complexity:**
 - ▶ size of single-clock region automata = polynomial [LMS04]
 - ▶ consider a Markov chain version of the region graph and apply result of [CSS03] to it
- ▶ **Correctness:** rather involved proof
 - ▶ 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 topological games called **Banach-Mazur games**

Outline

- 1 Probabilistic semantics
 - Motivations
 - Definition
 - Qualitative model-checking
- 2 Quantitative model-checking
 - Problem definition
 - Abstraction
 - Approximation method
- 3 Conclusion

Problems statement

Given \mathcal{A} timed automaton, φ ω -regular formula.

Quantitative MC

Compute $\mathbb{P}_{\mathcal{A}}(\varphi)$.

Problems statement

Given \mathcal{A} timed automaton, φ ω -regular formula.

Quantitative MC

Compute $\mathbb{P}_{\mathcal{A}}(\varphi)$.

Approximate quantitative MC

Given $\varepsilon > 0$, compute $p_{\varepsilon}^{-}, p_{\varepsilon}^{+} \in \mathbb{Q}$ such that
$$\begin{cases} p_{\varepsilon}^{-} \leq \mathbb{P}_{\mathcal{A}}(\varphi) \leq p_{\varepsilon}^{+} & \text{and} \\ p_{\varepsilon}^{+} - p_{\varepsilon}^{-} < \varepsilon. \end{cases}$$

Problems statement

Given \mathcal{A} timed automaton, φ ω -regular formula.

Quantitative MC

Compute $\mathbb{P}_{\mathcal{A}}(\varphi)$.

Approximate quantitative MC

Given $\varepsilon > 0$, compute $p_{\varepsilon}^{-}, p_{\varepsilon}^{+} \in \mathbb{Q}$ such that
$$\begin{cases} p_{\varepsilon}^{-} \leq \mathbb{P}_{\mathcal{A}}(\varphi) \leq p_{\varepsilon}^{+} & \text{and} \\ p_{\varepsilon}^{+} - p_{\varepsilon}^{-} < \varepsilon. \end{cases}$$

Threshold problem

Given $c \in \mathbb{Q}$ and $\sim \in \{<, \leq, =, \geq, >\}$, decide whether $\mathbb{P}_{\mathcal{A}}(\varphi) \sim c$.

Methodology

Probability values highly depend on clock valuation.

→ Region graph qualitative abstraction is no more correct.

Methodology

Probability values highly depend on clock valuation.

→ Region graph qualitative abstraction is no more correct.

Reduction to a system of differential equations.

→ (Very) Hard to solve in general, even for simple distributions, and simple properties

Methodology

Probability values highly depend on clock valuation.

→ Region graph qualitative abstraction is no more correct.

Reduction to a system of differential equations.

→ (Very) Hard to solve in general, even for simple distributions, and simple properties

→ Describe a **restricted framework** where:

\mathcal{A} can be abstracted into a **finite Markov chain**.

Methodology

Probability values highly depend on clock valuation.

→ Region graph qualitative abstraction is no more correct.

Reduction to a system of differential equations.

→ (Very) Hard to solve in general, even for simple distributions, and simple properties

→ Describe a **restricted framework** where:

\mathcal{A} can be abstracted into a **finite Markov chain**.

Properties: first solve the problem for prefix-independent properties ; extend to ω -regular properties by product

Abstraction

Hypotheses

- ▶ for $s = (\ell, \alpha)$ and $s' = (\ell, \alpha')$ with $\alpha, \alpha' > M$, $\mu_s = \mu_{s'}$
- ▶ in every bounded cycle the clock is reset

Abstraction

Hypotheses

- ▶ for $s = (\ell, \alpha)$ and $s' = (\ell, \alpha')$ with $\alpha, \alpha' > M$, $\mu_s = \mu_{s'}$
- ▶ in every bounded cycle the clock is reset

Markov chain $MC(\mathcal{A})$

states $(\ell, 0)$ and $(\ell, x > M)$

probabilities $\mathbb{P}_{\mathcal{A}}(e_1 \cdots e_n) = \mathbb{P}(\text{Cyl}(e_1 \cdots e_n))$

Abstraction

Hypotheses

- ▶ for $s = (\ell, \alpha)$ and $s' = (\ell, \alpha')$ with $\alpha, \alpha' > M$, $\mu_s = \mu_{s'}$
- ▶ in every bounded cycle the clock is reset

Markov chain $MC(\mathcal{A})$

states $(\ell, 0)$ and $(\ell, x > M)$

probabilities $\mathbb{P}_{\mathcal{A}}(e_1 \cdots e_n) = \mathbb{P}(\text{Cyl}(e_1 \cdots e_n))$

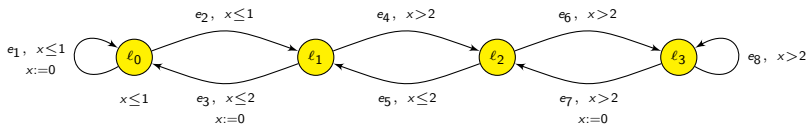
Theorem

For \mathcal{A} single-clock automaton and φ prefix-independent property,

$$\mathbb{P}_{\mathcal{A}}(\varphi) = \mathbb{P}_{MC(\mathcal{A})}(\diamond F_{\varphi})$$

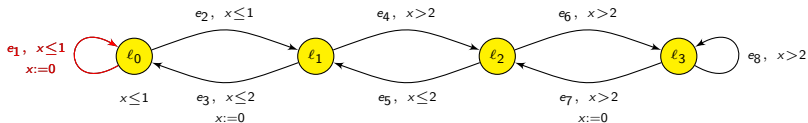
where F_{φ} is the set of BSCCs in $MC(\mathcal{A})$ that satisfy φ .

Abstraction on an example



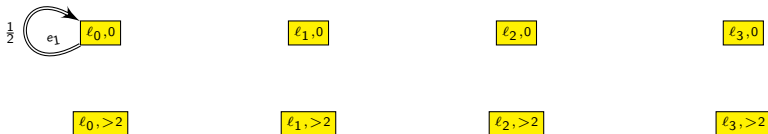
- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Abstraction on an example

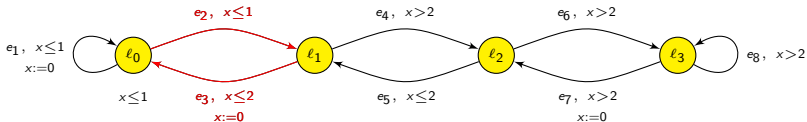


- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Construction of $MC(\mathcal{A})$ with macro-edges

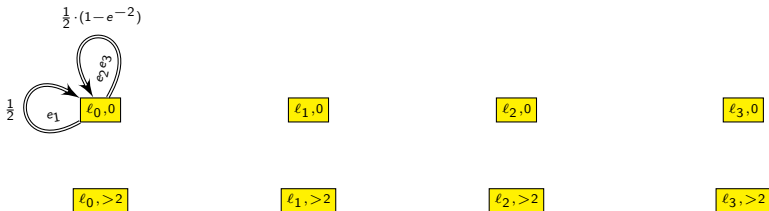


Abstraction on an example

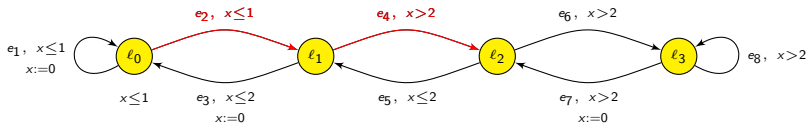


- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Construction of $MC(\mathcal{A})$ with macro-edges

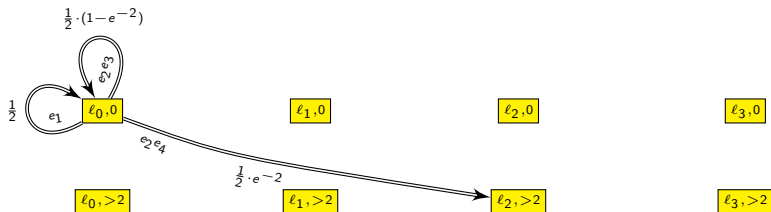


Abstraction on an example

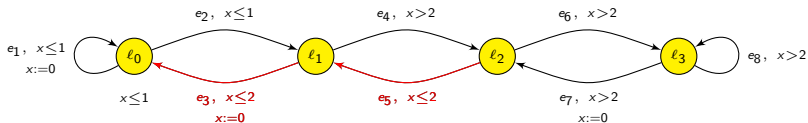


- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Construction of $MC(\mathcal{A})$ with macro-edges

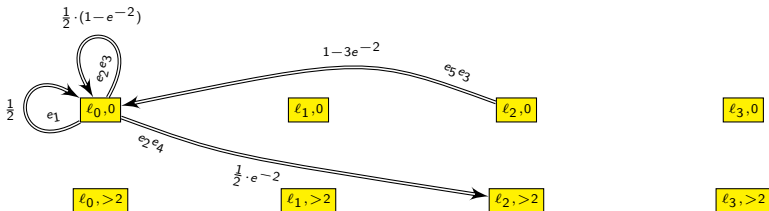


Abstraction on an example

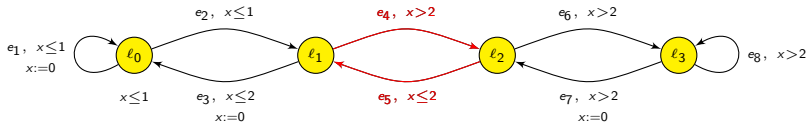


- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Construction of $MC(\mathcal{A})$ with macro-edges

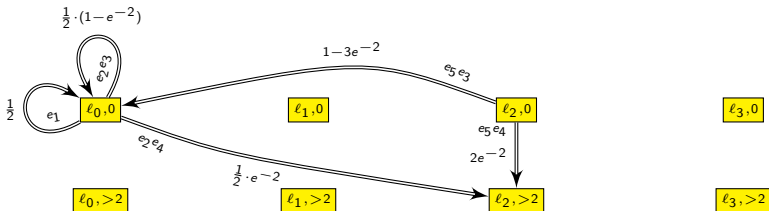


Abstraction on an example

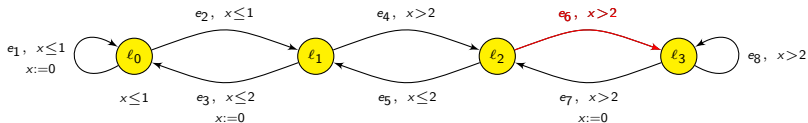


- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Construction of $MC(\mathcal{A})$ with macro-edges

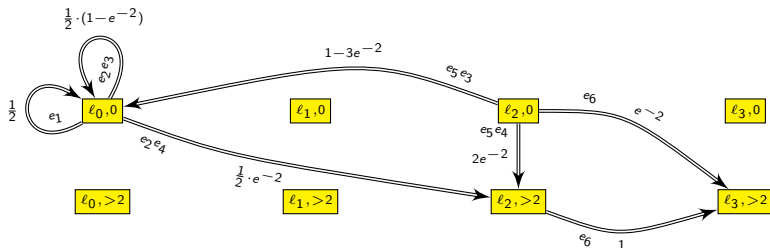


Abstraction on an example

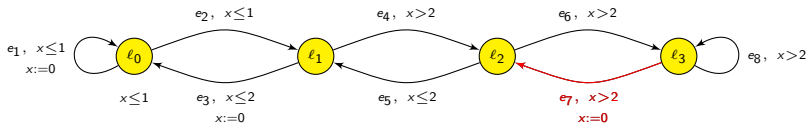


- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Construction of $MC(\mathcal{A})$ with macro-edges

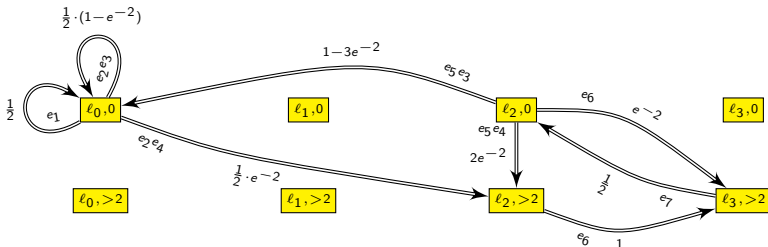


Abstraction on an example

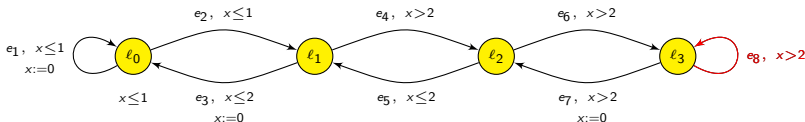


- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Construction of $MC(\mathcal{A})$ with macro-edges

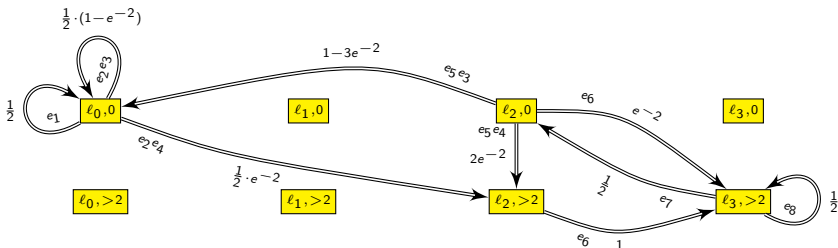


Abstraction on an example

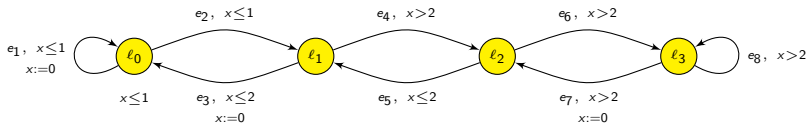


- ▶ distributions $\mu_s: t \mapsto e^{-t}$ when $I(s) = \mathbb{R}_+$
 μ_s uniform distribution when $I(s)$ is bounded
- ▶ uniform weights on transitions

Construction of $MC(\mathcal{A})$ with macro-edges

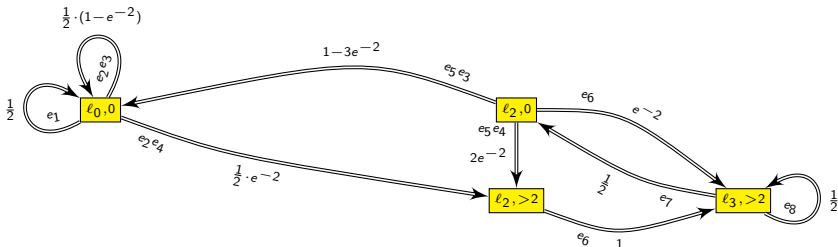


Abstraction on an example



- ▶ 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

Construction of $MC(\mathcal{A})$ with macro-edges



Probability expression

Limits of the abstraction:

there might be no closed form for the labels values in $MC(\mathcal{A})$.

Probability expression

Limits of the abstraction:

there might be no closed form for the labels values in $MC(\mathcal{A})$.

- ▶ We assume furthermore that:
 - ▶ for every state s , $I(s) = \mathbb{R}_+$
(the timed automaton is 'reactive')

Probability expression

Limits of the abstraction:

there might be no closed form for the labels values in $MC(\mathcal{A})$.

- ▶ 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 $\lambda_\ell \in \mathbb{Q}_+$

Probability expression

Limits of the abstraction:

there might be no closed form for the labels values in $MC(\mathcal{A})$.

- ▶ 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]

Probability expression

Limits of the abstraction:

there might be no closed form for the labels values in $MC(\mathcal{A})$.

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

Approximation scheme

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

Approximation scheme

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

- ▶ Compute sequences $(a_i)_i$ and $(b_i)_i$ with
 - ▶ $\lim_i a_i = \lim_i b_i = e^{-r}$
 - ▶ $a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i$
 - use e.g. Maclaurin series of exp

Approximation scheme

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

- ▶ Compute sequences $(a_i)_i$ and $(b_i)_i$ with
 - ▶ $\lim_i a_i = \lim_i b_i = e^{-r}$
 - ▶ $a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i$
 - use e.g. Maclaurin series of exp
- ▶ Compute an interval $(\alpha, \beta) \ni e^{-r}$ over which f is monotonic:
 - possible since e^{-r} is transcendental

Approximation scheme

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

- ▶ Compute sequences $(a_i)_i$ and $(b_i)_i$ with
 - ▶ $\lim_i a_i = \lim_i b_i = e^{-r}$
 - ▶ $a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i$
 - use e.g. Maclaurin series of exp

- ▶ Compute an interval $(\alpha, \beta) \ni e^{-r}$ over which f is monotonic:
 - possible since e^{-r} is transcendental
 - ▶ writing $f = P/Q$, we have that $f' = (P'Q - PQ')/Q^2$

Approximation scheme

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

- ▶ Compute sequences $(a_i)_i$ and $(b_i)_i$ with
 - ▶ $\lim_i a_i = \lim_i b_i = e^{-r}$
 - ▶ $a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i$
 - use e.g. Maclaurin series of exp

- ▶ Compute an interval $(\alpha, \beta) \ni e^{-r}$ over which f is monotonic:
 - possible since e^{-r} is transcendental
 - ▶ 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)

Approximation scheme

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

- ▶ Compute sequences $(a_i)_i$ and $(b_i)_i$ with
 - ▶ $\lim_i a_i = \lim_i b_i = e^{-r}$
 - ▶ $a_i \leq a_{i+1} \leq e^{-r} \leq b_{i+1} \leq b_i$
 - use e.g. Maclaurin series of exp

- ▶ Compute an interval $(\alpha, \beta) \ni e^{-r}$ over which f is monotonic:
 - possible since e^{-r} is transcendental
 - ▶ 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)

- ▶ For N large enough, $(a_N, b_N) \subseteq (\alpha, \beta)$, sequences $(f(a_i))_{i \geq N}$ and $(f(b_i))_{i \geq N}$ are monotonic and converge to $f(e^{-r})$

Results

Framework:

- ▶ single-clock timed automaton
- ▶ reset on every bounded cycle
- ▶ reactive timed automaton ($I(s) = \mathbb{R}_+$)
- ▶ exponential distributions on delays

Results

Framework:

- ▶ single-clock timed automaton
- ▶ reset on every bounded cycle
- ▶ reactive timed automaton ($I(s) = \mathbb{R}_+$)
- ▶ exponential distributions on delays

Quantitative approximation

Given φ an ω -regular formula, one can decide whether $\mathbb{P}_{\mathcal{A}}(\varphi) \in \mathbb{Q}$. If so $\mathbb{P}_{\mathcal{A}}(\varphi)$ can be computed, otherwise it is of the form $f(e^{-1/q})$ with $f \in \mathbb{Q}(X)$ and $q \in \mathbb{N}$ and can be approximated.

Results

Framework:

- ▶ single-clock timed automaton
- ▶ reset on every bounded cycle
- ▶ reactive timed automaton ($I(s) = \mathbb{R}_+$)
- ▶ exponential distributions on delays

Quantitative approximation

Given φ an ω -regular formula, one can decide whether $\mathbb{P}_{\mathcal{A}}(\varphi) \in \mathbb{Q}$. If so $\mathbb{P}_{\mathcal{A}}(\varphi)$ can be computed, otherwise it is of the form $f(e^{-1/q})$ with $f \in \mathbb{Q}(X)$ and $q \in \mathbb{N}$ and can be approximated.

Threshold problem

Given φ an ω -regular formula, \sim a comparison relation, and c a rational number, one can decide whether $\mathbb{P}_{\mathcal{A}}(\varphi) \sim c$.

Outline

- 1 Probabilistic semantics
 - Motivations
 - Definition
 - Qualitative model-checking
- 2 Quantitative model-checking
 - Problem definition
 - Abstraction
 - Approximation method
- 3 Conclusion

Conclusion and further works

Recap

study of (restricted) single-clock automata under probabilistic semantics

- ▶ approximation scheme for the quantitative model-checking problem
- ▶ algorithm for the threshold problem

Conclusion and further works

Recap

study of (restricted) single-clock automata under probabilistic semantics

- ▶ approximation scheme for the quantitative model-checking problem
- ▶ algorithm for the threshold problem

Further works

- ▶ define approximation schemes for other frameworks
 - e.g. bounded automata
- ▶ handle several clocks (even in the qualitative case)
- ▶ compute expected time