Reachability in Stochastic Hybrid Systems [Ongoing Work]

Patricia Bouyer[1] Thomas Brihaye[2] Mickael Randour[2,3]
Cédric Rivière[2] **Pierre Vandenhove**[1,2,3]

[1]LSV, CNRS & ENS Paris-Saclay, Université Paris-Saclay, France
[2]Université de Mons, Mons, Belgium
[3]F.R.S.-FNRS

September 12, 2019 – Reachability Problems, Brussels

Outline

- **Verification** of models combining:
  - **stochastic** aspects (e.g., Markov chains);
  - **hybrid** aspects (with both discrete and continuous transitions);

  $\rightsquigarrow$ ***stochastic hybrid systems***.
- Properties about the **reachability** of states (is some set of states reached with probability 1? Can we compute the probability of reaching a set?).

Goal

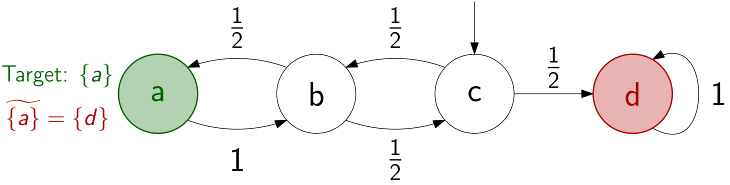
Identify a **decidability frontier** for reachability in stochastic hybrid systems.

Method

Follow an approach that has been successful for **infinite Markov chains**.

Reachability in infinite Markov chains

Let $\mathcal{M}$ be a countable Markov chain.



Let $B \subseteq S$ be a subset of states, $s \in S$ be an initial state.

Goal

Compute (or approximate) $\mathrm{Prob}_s^{\mathcal{M}}(\Diamond B)$.

We set

$$\widetilde{B} = \{s \in S \mid \mathrm{Prob}_s^{\mathcal{M}}(\Diamond B) = 0\}\,.$$

How to approximate the probability of reaching B?

Approximation procedure (for a given $\epsilon > 0$)[1]

We define

$$\begin{cases} p_n^{\mathsf{Yes}} & = \mathsf{Prob}_s^{\mathcal{M}}(\Diamond_{\leq n} B) \\ p_n^{\mathsf{No}} & = \mathsf{Prob}_s^{\mathcal{M}}(\Diamond_{\leq n} \widetilde{B}) . \end{cases}$$

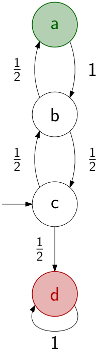
For all n, $p_n^{\mathsf{Yes}} \leq \mathsf{Prob}_s^{\mathcal{M}}(\Diamond B) \leq 1 - p_n^{\mathsf{No}}$.

We stop when

$$(1 - p_n^{\mathsf{No}}) - p_n^{\mathsf{Yes}} < \epsilon .$$

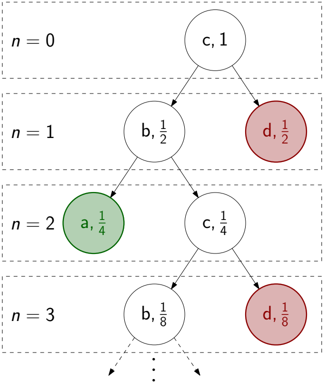
[1] Iyer and Narasimha, "Probabilistic Lossy Channel Systems", 1997.

Example



Target: $\{a\}$

$\Longrightarrow \widetilde{\{a\}} = \{d\}$.



$\rightsquigarrow p_0^{Yes} = 0,\ p_0^{No} = 0,$

$\rightsquigarrow p_1^{Yes} = 0,\ p_1^{No} = \frac{1}{2},$

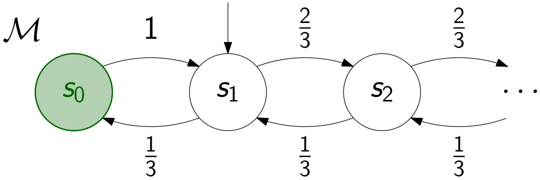
$\rightsquigarrow p_2^{Yes} = \frac{1}{4},\ p_2^{No} = \frac{1}{2},$

$\rightsquigarrow p_3^{Yes} = \frac{1}{4},\ p_3^{No} = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}.$

$\rightsquigarrow \frac{1}{4} \leq \mathrm{Prob}_c^{\mathcal{M}}(\Diamond\{a\}) \leq 1 - \frac{5}{8} = \frac{3}{8}$. $\rightsquigarrow$ **Always terminates?**

Counterexample: diverging random walk

The procedure does not terminate for this infinite Markov chain:



Initial state: s_1, target state: $B = \{s_0\} \Longrightarrow \widetilde{B} = \emptyset$. For all n,

- $p_n^{\text{Yes}} = \text{Prob}_{s_1}^{\mathcal{M}}(\Diamond_{\leq n} B) \leq \text{Prob}_{s_1}^{\mathcal{M}}(\Diamond B) = \frac{1}{2}$.
- $p_n^{\text{No}} = \text{Prob}_{s_1}^{\mathcal{M}}(\Diamond_{\leq n} \widetilde{B}) = 0$.

$\rightsquigarrow$ For all n, $(1 - p_n^{\text{No}}) - p_n^{\text{Yes}} \geq \frac{1}{2} \ldots$

Decisiveness

Let $\mathcal{M} = (S, P)$ be a countable Markov chain, $B \subseteq S$.

Decisiveness[2]

$\mathcal{M}$ is **decisive** w.r.t. $B \subseteq S$ if for all $s \in S$, $\mathrm{Prob}_s^{\mathcal{M}}(\Diamond B \vee \Diamond \widetilde{B}) = 1$.

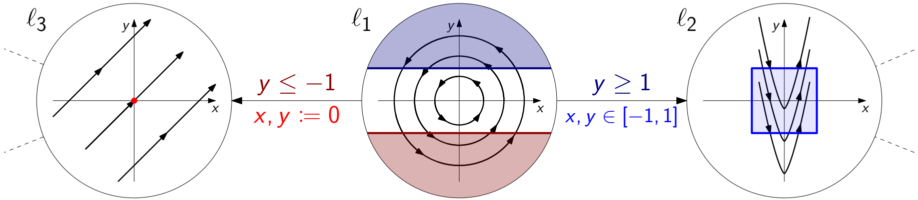
Theorem[2]

If $\mathcal{M}$ is decisive w.r.t. B, then the approximation procedure is correct and **terminates**.

- The diverging random walk is not decisive w.r.t. $B = \{s_0\}$.
- Decisiveness also allows for a procedure to verify **almost-sure reachability**.

[2] Abdulla, Ben Henda, and Mayr, "Decisive Markov Chains", 2007.

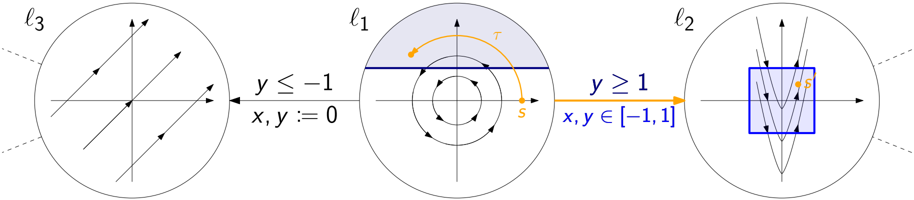
Hybrid systems



- (L, E) is a **finite graph**.
- A number n of **continuous variables** $\rightsquigarrow$ states of the system are in $L \times \mathbb{R}^n$ $\rightsquigarrow$ **uncountable**!
- For each $\ell \in L$, $\gamma_\ell : \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^n$ is a **continuous dynamics**.
- For each edge $e \in E$, $\mathcal{G}(e) \subseteq \mathbb{R}^n$ is a **guard**.
- For each edge $e \in E$, $\mathcal{R}(e) : \mathbb{R}^n \to 2^{\mathbb{R}^n}$ is a **reset map**.

Transitions of hybrid systems

States: $L \times \mathbb{R}^n$ (discrete location $\times$ value of the continuous variables).



A transition combines a **continuous evolution** and a **discrete transition**.
Example: initial state is $s = (\ell_1, (2, 0))$;

- we stay in ℓ_1 for some **time** $\tau \geq 0$;
- we take an **edge** whose guard is satisfied;
- we take a value among the possible **resets**, e.g. $s' = (\ell_2, (\frac{1}{2}, \frac{1}{2}))$.

We replace the nondeterminism of hybrid systems with probability distributions on the:

- waiting time from a given state;
- edge choice;
- choice of a reset value.

$\rightsquigarrow$ **Stochastic** hybrid systems (**SHSs**)

Undecidability

Undecidability of reachability for SHSs

Given an SHS $\mathcal{H}$, an initial distribution μ on the states of $\mathcal{H}$ and a target set $B \subseteq L \times \mathbb{R}^n$, the reachability problems

- $\mathrm{Prob}_{\mu}^{\mathcal{H}}(\Diamond B) = 1$?
- $\mathrm{Prob}_{\mu}^{\mathcal{H}}(\Diamond B) = 0$?
- is a value ϵ-close to $\mathrm{Prob}_{\mu}^{\mathcal{H}}(\Diamond B)$?

are **undecidable**.

$\rightsquigarrow$ inspired from an undecidability proof for hybrid systems.[3]

Goal

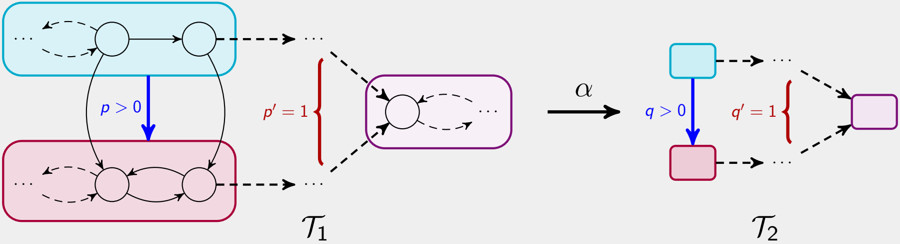
Find a setting in which reachability is decidable.

[3] Henzinger et al., “What’s Decidable about Hybrid Automata?”, 1998.

Reachability problems in **stochastic** systems

To deal with an uncountable number of states $\rightsquigarrow$ "**finite abstraction**".

Abstraction of a **stochastic** hybrid system



- **Abstraction** whenever $p > 0 \Leftrightarrow q > 0$.
- **Sound** abstraction whenever

$$\mathrm{Prob}^{\mathcal{T}_2}(\Diamond B) = 1 \implies \mathrm{Prob}^{\mathcal{T}_1}(\Diamond \alpha^{-1}(B)) = 1 \, .$$

Decidable classes for reachability

Hybrid systems: existence of a finite time-abstract bisimulation

- Timed automata[4] ($\dot{x} = 1, x := 0$; region graph);
- Initialized rectangular hybrid systems;[5]
- O-minimal hybrid systems[6] (rich dynamics, all variables have to be reset at every discrete transition).

SHSs: existence of a finite and **sound** abstraction

- Single-clock stochastic timed automata;[7]
- Reactive stochastic timed automata.[7]

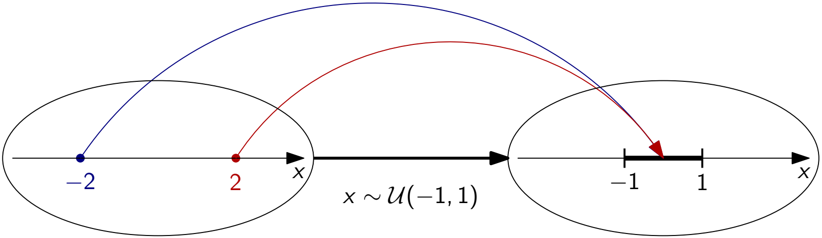
$\rightsquigarrow$ Proof of soundness: **finite abstraction** + **decisiveness**.

[4] Alur and Dill, "Automata For Modeling Real-Time Systems", 1990.
[5] Henzinger et al., "What's Decidable about Hybrid Automata?", 1998.
[6] Lafferriere, Pappas, and Sastry, "O-Minimal Hybrid Systems", 2000.
[7] Bertrand et al., "When are stochastic transition systems tameable?", 2018.

Plan to make reachability decidable: strong resets

We restrict our focus to SHSs with **strong resets**.[8]
Strong reset = reset that does not depend on the value of the variables.

Example: x follows a uniform dist. in $[x-1, x+1]$ **is not** a strong reset.
x follows a uniform distribution in $[-1, 1]$ **is** a strong reset.



[8] Lafferriere, Pappas, and Sastry, "O-Minimal Hybrid Systems", 2000.

Consequences of strong resets

Proposition

If an SHS has (at least) one **strong reset** per cycle of the discrete graph, it

- has a **finite abstraction**;
- is **decisive** w.r.t. any set of states.

$$\text{strong resets} \;\begin{array}{l} \Nearrow \\ \\ \Searrow \end{array}\; \left.\begin{array}{c} \text{finite abstraction} \\ + \\ \text{decisiveness} \end{array}\right\} \begin{array}{c} \textbf{sound} \text{ and finite} \\ \text{abstraction} \end{array}$$

$\rightsquigarrow$ Reachability is decidable when the abstraction is computable!

Conclusion: decidable classes of hybrid systems

Hybrid systems: existence of a finite time-abstract bisimulation

- Timed automata;[9]
- Initialized rectangular hybrid systems;[10]
- O-minimal hybrid systems.[11]

SHSs: existence of a sound and finite abstraction

- Single-clock stochastic timed automata;[12]
- Reactive stochastic timed automata;[12]
- **Strongly-reset stochastic hybrid systems**.

$\rightsquigarrow$ Reachability is **decidable** under effectiveness assumptions.

[9] Alur and Dill, "Automata For Modeling Real-Time Systems", 1990.
[10] Henzinger et al., "What's Decidable about Hybrid Automata?", 1998.
[11] Lafferriere, Pappas, and Sastry, "O-Minimal Hybrid Systems", 2000.
[12] Bertrand et al., "When are stochastic transition systems tameable?", 2018.