# Decisiveness of Stochastic Systems and its Application to Hybrid Models

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 22, 2020 – GandALF 2020

# 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 **reachability** (is some set of states reached with probability 1? Probability of reaching a set?).

### Goal

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

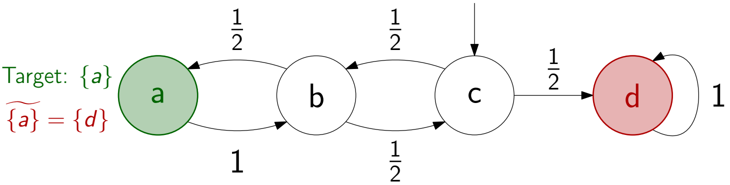
### Method

Follow an approach that has been successful for **infinite Markov chains**.[1]

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

# Reachability in infinite Markov chains

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




Let $B \subseteq S$ be target states, $s \in S$ be an initial state.

**Goal**

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

We set

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

# How to approximate the probability of reaching $B$?

## Approximation procedure (for a given $\epsilon > 0$)[2]

We define

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

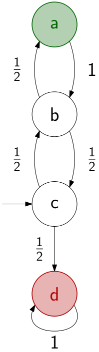
For all $n$, $p_n^{\text{Yes}} \leq \text{Prob}_s^{\mathcal{M}}(\Diamond B) \leq 1 - p_n^{\text{No}}$.

We stop when

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

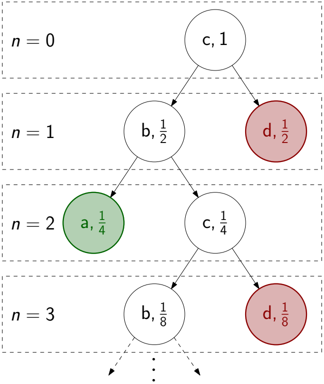
[2] Iyer and Narasimha, "Probabilistic Lossy Channel Systems", 1997.

# Example




Target: $\{a\}$

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




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

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

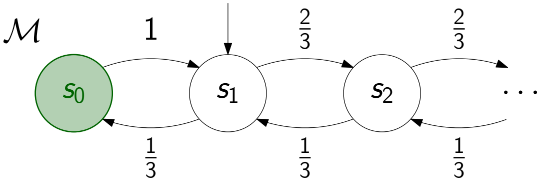
$\rightsquigarrow p_2^{Yes} = \frac{1}{4}, \; p_2^{No} = \frac{1}{2},$

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

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

# Counterexample: diverging random walk

The procedure does not terminate for this infinite Markov chain:




Initial state: $s_1$, target state: $B = \{s_0\} \implies \widetilde{B} = \emptyset$. 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[3]

$\mathcal{M}$ 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[3]

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**.

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

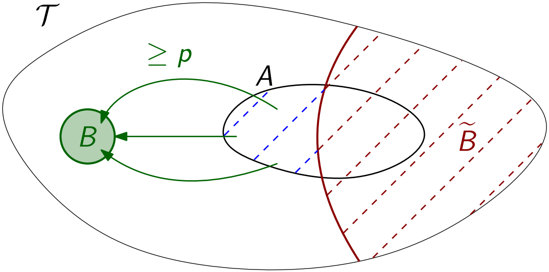
# Contribution: generalized decisiveness criterion

## Proposition

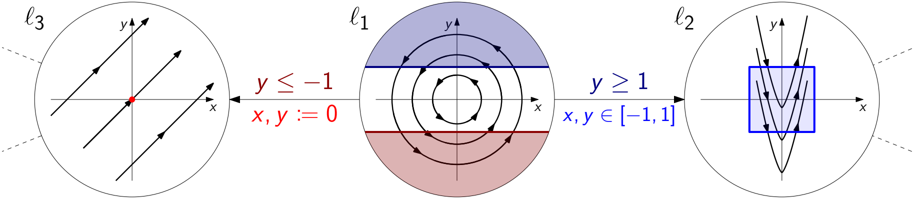
Let $\mathcal{T}$ be an stochastic transition system with an **attractor** $A \subseteq S$ and $B \subseteq S$ a set of states.
If there exists $p > 0$ such that

$$\forall s \in A \cap (\widetilde{B})^c, \mathrm{Prob}_s^{\mathcal{T}}(\Diamond B) \geq p\,,$$

then $\mathcal{T}$ is decisive w.r.t. $B$.



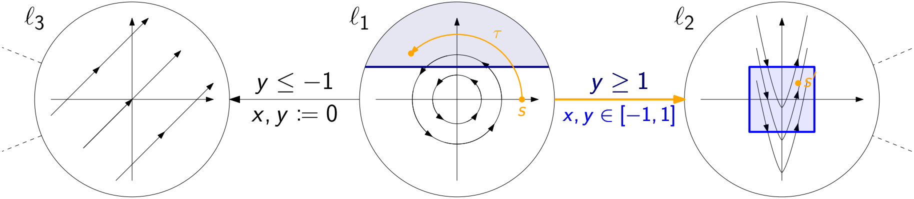
# Hybrid systems




- $(L, E)$ 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 $\ell_1$ for some **time** $\tau \geq 0$;
- we take an **edge** whose guard is satisfied;
- we take a value among the possible **resets**, e.g. $s' = (\ell_2, (\frac{1}{2}, \frac{1}{2}))$.

# Adding stochasticity

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 $\mu$ 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 $\epsilon$-close to $\mathrm{Prob}_\mu^{\mathcal{H}}(\Diamond B)$?

are **undecidable**.

$\rightsquigarrow$ inspired from an undecidability proof for hybrid systems.[4]

## Goal

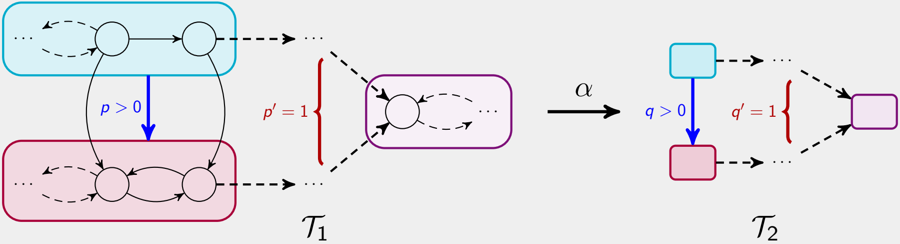
Find a setting in which reachability is decidable.

[4] 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[5] ($\dot{x} = 1, x := 0$; region graph);
- Initialized rectangular hybrid systems;[6]
- O-minimal hybrid systems[7] (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;[8]
- Reactive stochastic timed automata.[8]

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

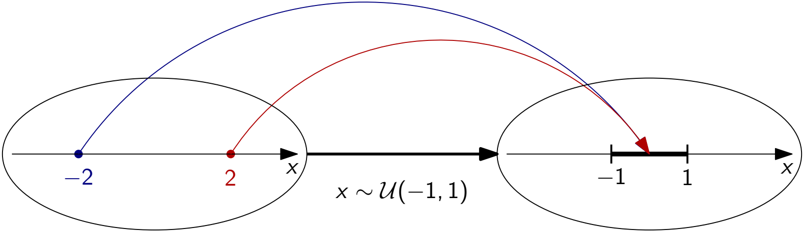
---

[5] Alur and Dill, "Automata For Modeling Real-Time Systems", 1990.
[6] Henzinger et al., "What's Decidable about Hybrid Automata?", 1998.
[7] Lafferriere, Pappas, and Sastry, "O-Minimal Hybrid Systems", 2000.
[8] 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**.[9]
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.



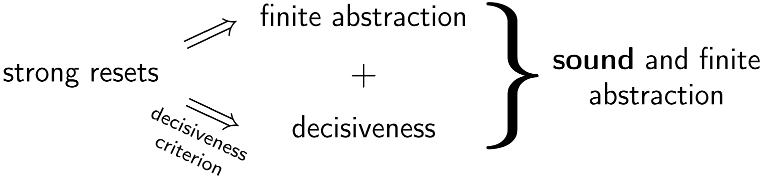

[9] Lafferriere, Pappas, and Sastry, "O-Minimal Hybrid Systems", 2000.

# 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.




⇝ Reachability is decidable when the abstraction is computable!

# Putting everything together

## Proposition

Let $\mathcal{H}$ be an SHS with one **strong reset** per cycle.
If **the sound and finite abstraction is computable**, then

- almost-sure reachability is decidable;
- adding numerical hypotheses on the distributions, we can compute an approximation of the probability to reach a set of states.

## Setting in which the abstraction is computable

- The different components (flows, guards...) are definable in an **o-minimal structure** with **decidable** theory (such as $\langle \mathbb{R}, <, +, \cdot, 0, 1 \rangle$);
- The various probability distributions are either finite or equivalent to the Lebesgue measure on their support.

# Conclusion: decidable classes of hybrid systems

## Hybrid systems: existence of a finite time-abstract bisimulation

- Timed automata;[10]
- Initialized rectangular hybrid systems;[11]
- O-minimal hybrid systems.[12]

## SHSs: existence of a sound and finite abstraction

- Single-clock stochastic timed automata;[13]
- Reactive stochastic timed automata;[13]
- **Strongly-reset stochastic hybrid systems**.

⇝ Reachability is **decidable** under effectiveness assumptions.

⇝ Soundness is shown through the **decisiveness** property.

[10] Alur and Dill, "Automata For Modeling Real-Time Systems", 1990.

[11] Henzinger et al., "What's Decidable about Hybrid Automata?", 1998.

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

[13] Bertrand et al., "When are stochastic transition systems tameable?", 2018.