The Decisiveness Property for Decidable Classes of Stochastic Systems

Pierre Vandenhove

LaBRI, Université de Bordeaux

February 29, 2024 – Liverpool Verification Seminar

LABORATOIRE BORDELAIS DE RECHERCHE EN INFORMATIQUE LaBRI

université de BORDEAUX

Outline

Verification of models:

- **stochastic** aspects (e.g., Markov chains);
- properties about **reachability** (Probability of reaching a set? Is some set of states reached with probability 0 or 1?).
  When considering infinite-state systems, often **undecidable**.

Goal

Identify **decidability frontiers** for reachability in stochastic systems.
$\rightsquigarrow$ Follow an approach using the **decisiveness** property.[1]

$\rightsquigarrow$ Illustration on **stochastic hybrid systems**.[2]

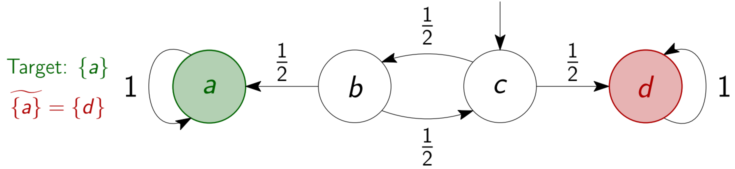
[1] Abdulla, Ben Henda, and Mayr, "Decisive Markov Chains", 2007.

[2] Bouyer, Brihaye, Randour, Rivière, and Vandenhove, "Decisiveness of stochastic systems and its application to hybrid models", 2022.

1. Stochastic systems and decisiveness

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

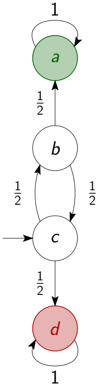
Compute (or approximate) $\mathrm{Prob}_s^{\mathcal{M}}(\Diamond B)$.

Solving a linear system may not be advised for infinite Markov chains.
Other approach: **incremental unfolding**.

We set

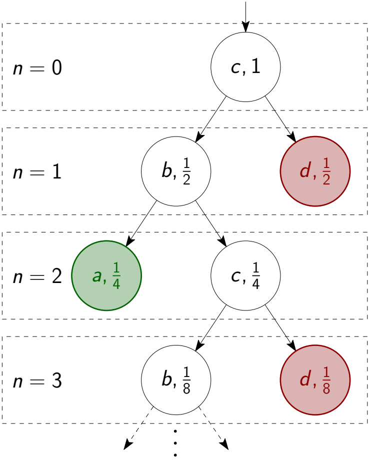
$$\widetilde{B} = \{s \in S \mid \mathrm{Prob}_s^{\mathcal{M}}(\Diamond B) = 0\}\,.$$

How to approximate the probability of reaching B?



Target: $\{a\}$

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



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

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

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

$\rightsquigarrow p_3^{Yes} = \frac{1}{4},$

$p_3^{No} = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}.$

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

Formally

Approximation procedure (for a given $\varepsilon > 0$)[3]

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 $n \geq 0$, $p_n^{\text{Yes}} \leq \text{Prob}_s^{\mathcal{M}}(\Diamond B) \leq 1 - p_n^{\text{No}}$.
We stop when

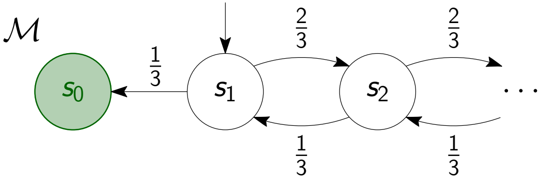
$$(1 - p_n^{\text{No}}) - p_n^{\text{Yes}} < \varepsilon \,.$$

$\rightsquigarrow$ **Always terminates?**

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

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 $n \geq 0$,

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

$\rightsquigarrow$ For all $n \geq 0$, $(1 - p_n^{\text{No}}) - p_n^{\text{Yes}} \geq \frac{1}{2} \dots$

Decisiveness

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

Decisiveness[4]

$\mathcal{M}$ 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[4]

Markov chain $\mathcal{M}$ is **decisive** w.r.t. B **if and only if** the approximation procedure **terminates**.

The diverging random walk is **not** decisive w.r.t. $B = \{s_0\}$, because

$$\mathrm{Prob}_{s_1}^{\mathcal{M}}(\Diamond B \vee \Diamond \widetilde{B}) = \mathrm{Prob}_{s_1}^{\mathcal{M}}(\Diamond B) = \frac{1}{2}.$$

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

Other reachability properties

- Decisiveness makes infinite systems behave “more like finite systems”.
- Decisiveness also helps for **almost-sure reachability** and **repeated reachability**.

Example for repeated reachability

Let $\mathcal{M} = (S, P)$ be an infinite Markov chain.
If $\mathcal{M}$ is **decisive** w.r.t. $B \subseteq S$, then

$$\mathrm{Prob}_s^{\mathcal{M}}(\Box\Diamond B) = 1 \iff s \models \forall\Box\exists\Diamond B.$$

$\Longleftarrow$ is not true without decisiveness.

Decidability

Along with **effectiveness assumptions**, e.g.,

- finite branching and computability of successors,
- computability of $\widetilde{B}$,

decisiveness is very useful to decide reachability problems.

- Used to show that *probabilistic lossy channel systems*, *probabilistic VASSs* (with B upwards closed) are decidable.[5]
- Multiple **sufficient conditions** for decisiveness in the literature.

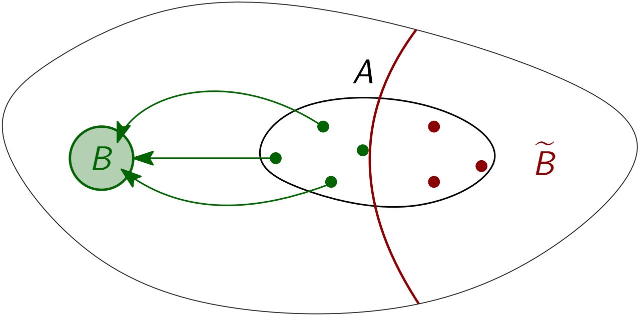
[5] Abdulla, Ben Henda, and Mayr, "Decisive Markov Chains", 2007.

Criterion

An **attractor** is a set $A \subseteq S$ such that for all $s \in S$, $\mathrm{Prob}_s^{\mathcal{M}}(\Diamond A) = 1$.

Sufficient condition

A Markov chain with a **finite attractor** is decisive w.r.t. **all sets**.



In particular, **finite Markov chains** are decisive w.r.t. all sets.

Summary for decisiveness

- Useful property for verification of reachability in stochastic systems.
- Hard to check directly, but multiple easier **criteria**.
- Has been extended to **uncountable** stochastic systems.[6]

Definition

A **stochastic transition system** is a tuple $\mathcal{T} = (S, \Sigma, \kappa)$ where:

- (S, Σ) is a measurable space, and
- $\kappa\colon S \times \Sigma \to [0, 1]$ is a function such that for each $s \in S$, $\kappa(s, \cdot)$ is a distribution over S and for $A \in \Sigma$, $\kappa(\cdot, A)$ is measurable.

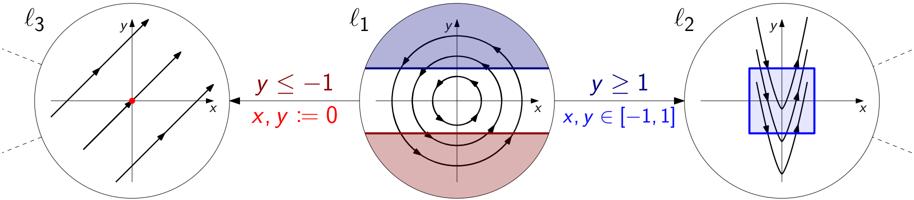
Rest of the talk: application of decisiveness to **hybrid systems** (joint work with P. Bouyer, T. Brihaye, C. Rivière and M. Randour).

[6] Bertrand, Bouyer, Brihaye, and Carlier, "When are stochastic transition systems tameable?", 2018.

2. Stochastic hybrid systems

Hybrid systems

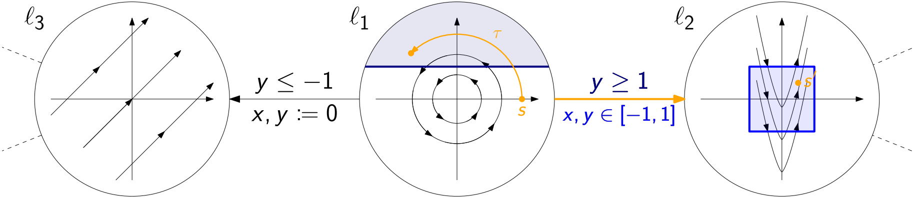
Hybrid systems combine **discrete** and **continuous** transitions.



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

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: 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. $s' = (\ell_2, (\frac{1}{2}, \frac{1}{2}))$.

Decidable hybrid systems

Undecidable classes

The reachability problem in **hybrid systems** is **undecidable**:

- already with variables using **two** linear rates ($\dot{x} \in \{a, b\}$ with $a \neq b$),[7]
- in a *robust* fashion.[8]

Decidable classes: trade-off between **dynamics** and **resets**.

- Timed automata: $\dot{x} = 1$, $x := 0$.[9]
- Rectangular automata: arbitrary **linear** dynamics ($\dot{x} \in \mathbb{Z}$), but **reset** whenever **change in dynamics**.[10]
- **O-minimal** hybrid systems: rich dynamics, but **all variables** have to be "**strongly reset**" at every discrete transition.[11]

[7] Alur, Courcoubetis, et al., "The Algorithmic Analysis of Hybrid Systems", 1995.

[8] Henzinger and Raskin, "Robust Undecidability of Timed and Hybrid Systems", 2000.

[9] Alur and Dill, "A Theory of Timed Automata", 1994.

[10] Henzinger, Kopke, Puri, and Varaiya, "What's Decidable about Hybrid Automata?", 1998.

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

Adding stochasticity

Hybrid systems are qualitative; we want a stochastic model here.
We replace the three sources of nondeterminism:

- **waiting time** from a given state,
- **edge choice**, and
- choice of a **reset value**

with **probability distributions**.

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

Undecidability

Undecidability of reachability for SHSs

Given an SHS $\mathcal{H}$, an initial state and a target set $B \subseteq L \times \mathbb{R}^n$, the **reachability problems**

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

are **undecidable**.

$\rightsquigarrow$ inspired from an undecidability proof for hybrid systems.[12]

Goal

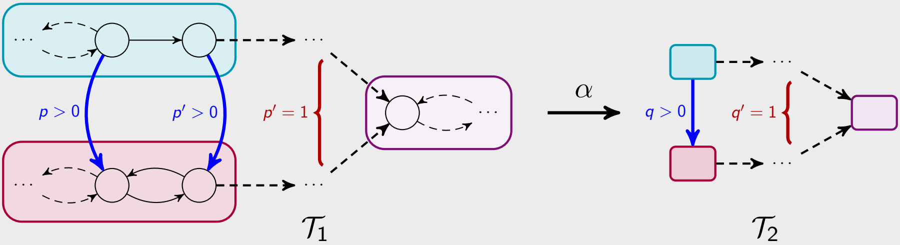
Find a setting in which reachability is decidable.

[12] Henzinger, Kopke, Puri, and Varaiya, "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 $p > 0 \iff q > 0$.
- For **almost-sure reachability**: an **abstraction** is **sound** if

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

Decidable classes for reachability

Hybrid systems: existence of a **finite abstraction**

- Timed automata (*region graph*)[13]
- Rectangular hybrid systems[14]
- O-minimal hybrid systems[15]

$\rightsquigarrow$ Decidability is a by-product of **a finite abstraction**.

Stochastic HSs: existence of a finite and **sound** abstraction

- Single-clock stochastic timed automata[16]
- Reactive stochastic timed automata[17]

$\rightsquigarrow$ Decidability is a by-product of **a sound and finite abstraction**.

[13] Alur and Dill, "A Theory of Timed Automata", 1994.

[14] Henzinger, Kopke, Puri, and Varaiya, "What's Decidable about Hybrid Automata?", 1998.

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

[16] Bertrand, Bouyer, Brihaye, Menet, et al., "Stochastic Timed Automata", 2014.

[17] Bertrand, Bouyer, Brihaye, and Carlier, "When are stochastic transition systems tameable?", 2018.

Soundness vs. decisiveness

Summary: properties that help for **decidability** are

- **decisiveness**,
- the existence of a **sound and finite abstraction**.

They are strongly **linked**.

Let $\mathcal{T}_2$ be an abstraction of $\mathcal{T}_1$ through function α.

Lemma[18]

- If $\mathcal{T}_1$ is **decisive**, then α is a **sound** abstraction.
- If α is **sound** and $\mathcal{T}_2$ is decisive, then $\mathcal{T}_1$ is **decisive**.

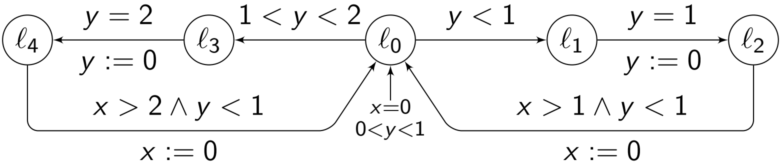
[18] Bertrand, Bouyer, Brihaye, and Carlier, “When are stochastic transition systems tameable?”, 2018.

How to make SHSs decidable?

We mentioned three classes of hybrid systems with finite abstraction:

- Timed automata,
- Rectangular hybrid systems,
- O-minimal hybrid systems with strong resets.

Which ideas could lead to a **sound** abstraction for **stochastic** HSs?



Stochastic timed automaton (simple dynamics and resets), simple guards, rectangular.[19]

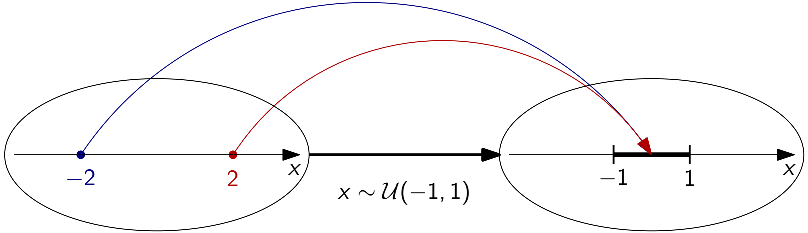
Not decisive (w.r.t. $\{\ell_2\} \times \mathbb{R}^2$)! So not the **first two**...

[19] Bertrand, Bouyer, Brihaye, Menet, et al., "Stochastic Timed Automata", 2014.

How to make SHSs decidable? Strong resets

We restrict our focus to SHSs with **strong resets**.[20]
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.



Frequent idea in the literature about hybrid systems.[21,22]

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

[21] Bertrand, Bouyer, Brihaye, and Markey, "Quantitative Model-Checking of One-Clock Timed Automata under Probabilistic Semantics", 2008.

[22] Gentilini, "Reachability Problems on Extended O-Minimal Hybrid Automata", 2005.

Why strong resets?

In **non-stochastic** **hybrid systems**,

$$\text{strong resets} \Longrightarrow \text{finite abstraction.}$$

Proof idea: the classical "bisimulation algorithm" terminates.

- Here, we want a **sound** abstraction.
- We can show this by proving **decisiveness of strongly-reset SHSs**.
- However, the previous criteria (e.g., finite attractor) do not hold here.

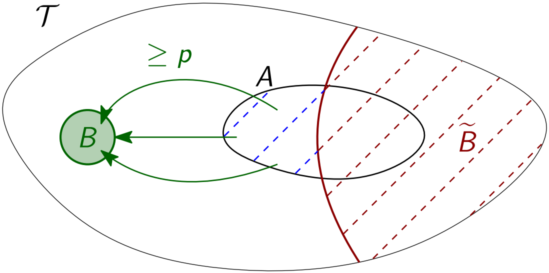
Generalized decisiveness criterion

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.



Consequences of strong resets

Proposition

A **stochastic hybrid system with only strong resets**

- has a **finite abstraction** (classic proof, bisimulation algorithm),
- is **decisive** w.r.t. any set of states.

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

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

$\rightsquigarrow$ “Only strong resets” can be generalized to “one strong reset per cycle”.

Final piece: When is the abstraction computable?

- The different components (dynamics, guards...) are definable in an **structure** with **decidable** theory (such as $\mathbb{R}_{\mathsf{alg}} = \langle \mathbb{R}, <, +, \cdot, 0, 1 \rangle$).
- Suffices for **nondeterministic HSs**, but not **stochastic ones**: probabilities may not be definable! E.g., $x \mapsto \frac{1}{x}$ is definable in $\mathbb{R}_{\mathsf{alg}}$, but

$$\int_1^t \frac{1}{x} \mathrm{d}x = \log(t)$$

  is not.

How to proceed?

Final piece: o-minimal structures

$\mathbb{R}_{\mathsf{alg}} = \langle \mathbb{R}, <, +, \cdot, 0, 1 \rangle$ is not only decidable but also *o-minimal*.

Lemma[23]

In an *o-minimal* structure, for a definable set $A \subseteq \mathbb{R}^n$,

$$\lambda(A) > 0 \iff \mathrm{int}(A) \neq \emptyset,$$

where λ is the Lebesgue measure.

So we restrict the probability distributions to ones **equivalent to the Lebesgue measure** on a **definable set**.

$\rightsquigarrow$ **Abstraction is computable**!

Note: $\mathbb{R}_{\mathsf{exp}} = \langle \mathbb{R}, <, +, \cdot, 0, 1, e^x \rangle$ is also o-minimal, but decidability is open.

[23] Kaiser, "First order tameness of measures", 2012.

Summing up

Putting it all together

For **stochastic hybrid systems** with

- one strong reset per cycle,
- every component (resets, guards, dynamics) definable in a decidable and o-minimal theory (e.g., $\mathbb{R}_{\mathsf{alg}}$),
- distributions either finite or equivalent to the Lebesgue measure,

almost-sure reachability problems are decidable.

Ongoing work: POMDPs

Adapting the **reset** ideas to **partially observable Markov decision processes**, a large class of undecidable infinite stochastic systems. Main change: there is a "**control**" part!

Thanks!