Generation of Counterexamples for Synthesis in Markov Decision Processes

Chloé Capon [1] Mickael Randour [1,2]

[1]UMONS – Université de Mons, Belgium

[2]F.R.S.-FNRS, Belgium

May 30, 2024

MOVEP 2024 – Rennes (France)

Motivations

- **Reactive systems** are systems that continuously **interact** with their environment.
- We are interested in the **correctness** of critical reactive systems, e.g., ABS for cars.

Motivations

- **Reactive systems** are systems that continuously **interact** with their environment.
- We are interested in the **correctness** of critical reactive systems, e.g., ABS for cars.

Verification

Given a **formal model** of the system and a **specification**, the goal is to **check** that the system satisfies the specification.

Synthesis

Given a **system** to control trying to enforce some **specification** within an uncontrollable **environment**, it aims at the **automated construction** of provably-safe system controllers.

Motivations

- Synthesis algorithms permit to construct a suitable controller **if one exists**.
- Otherwise, they simply tell us that **no such controller exists**.

$\rightsquigarrow$ what happens in practice?

Motivations

- Synthesis algorithms permit to construct a suitable controller **if one exists**.
- Otherwise, they simply tell us that **no such controller exists**.

$\rightsquigarrow$ what happens in practice?

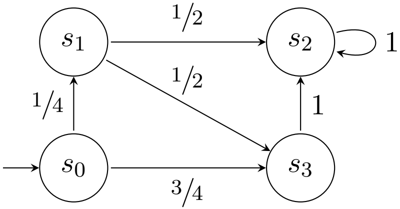
Idea

We need **refinement mechanisms** based on **counterexamples** that help practitioners understand:

1. **why** their attempt failed;
2. **how they can patch** the system – environment – specification triptych to make synthesis possible and obtain an adequate controller.

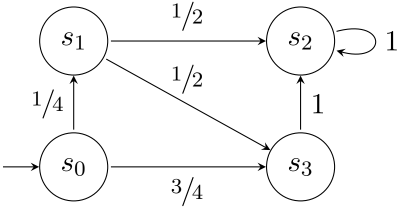
Markov Chains

- S a finite set of states
- s_0 an initial state
- $\delta : S \to \mathcal{D}(S)$ a probabilistic transition function



Markov Chains

- S a finite set of states
- s_0 an initial state
- $\delta : S \to \mathcal{D}(S)$ a probabilistic transition function

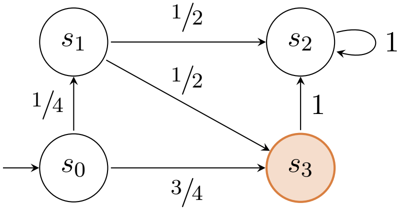


We denote by $\mathbb{P}(\Diamond T)$ the **probability to reach** a set of states T when starting in s_0.

Markov Chains

Example:

$\mathbb{P}(\Diamond\{s_3\}) =$

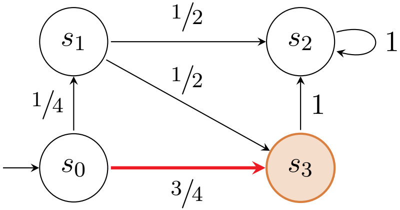


We denote by $\mathbb{P}(\Diamond T)$ the **probability to reach** a set of states T when starting in s_0.

Markov Chains

Example:

$\mathbb{P}(\Diamond\{s_3\}) = \frac{3}{4}$

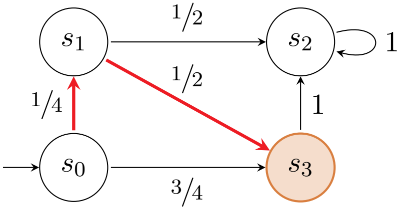


We denote by $\mathbb{P}(\Diamond T)$ the **probability to reach** a set of states T when starting in s_0.

Markov Chains

Example:

$\mathbb{P}(\Diamond\{s_3\}) = \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{2}$

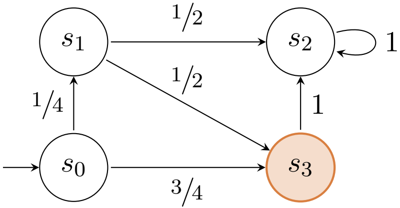


We denote by $\mathbb{P}(\Diamond T)$ the **probability to reach** a set of states T when starting in s_0.

Markov Chains

Example:

$\mathbb{P}(\Diamond\{s_3\}) = \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{2} = \frac{7}{8}$

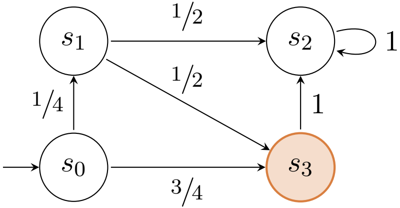


We denote by $\mathbb{P}(\Diamond T)$ the **probability to reach** a set of states T when starting in s_0.

Markov Chains

Example:

$\mathbb{P}(\Diamond\{s_3\}) = \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{2} = \frac{7}{8}$

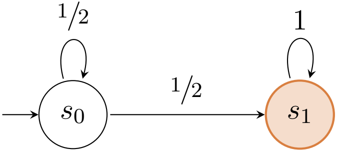


> We denote by $\mathbb{P}(\Diamond T)$ the **probability to reach** a set of states T when starting in s_0.

We consider properties of the form: $\mathcal{P}_{\leq\lambda}[\Diamond T]$ for $\lambda \in [0, 1]$.

Counterexamples for MCs

A counterexample is **a set of paths** with a **sufficient** probability mass.

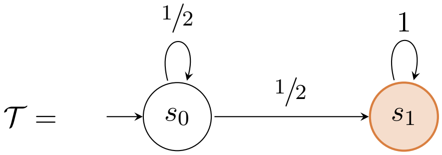
$\mathcal{T} =$ 

We have that $\mathcal{T} \not\models \mathcal{P}_{\leq 3/5}[\Diamond\{s_1\}]$

$\{s_0 s_1, s_0 s_0 s_1\}$ is a counterexample with a probability mass of $3/4$.

Counterexamples for MCs

A counterexample is **a set of paths** with a **sufficient** probability mass.

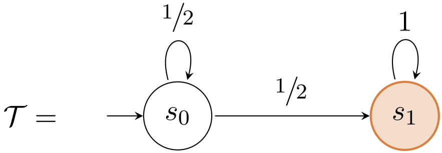


However: Quickly very large $\rightsquigarrow$ **hard** to understand and manipulate.

A counterexample for $\mathcal{P}_{<1}[\Diamond\{s_1\}]$ must be of infinite size.

Counterexamples for MCs

A counterexample is **a set of paths** with a **sufficient** probability mass.



However: Quickly very large $\rightsquigarrow$ **hard** to understand and manipulate.

A counterexample for $\mathcal{P}_{<1}[\Diamond\{s_1\}]$ must be of infinite size.

$\rightsquigarrow$ compact representation via **subsystems**[1]

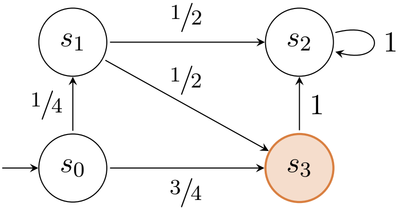
[1] Ábrahám et al., "Counterexample Generation for Discrete-Time Markov Models: An Introductory Survey".

Critical subsystems for MCs

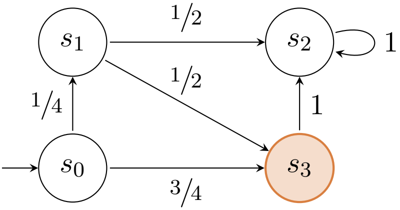
Example

We have that $\mathbb{P}(\Diamond\{s_3\}) = \frac{7}{8}$, therefore both specifications are **false**.

- $\mathcal{P}_{\leq 1/5}[\Diamond\{s_3\}]$



- $\mathcal{P}_{\leq 3/4}[\Diamond\{s_3\}]$

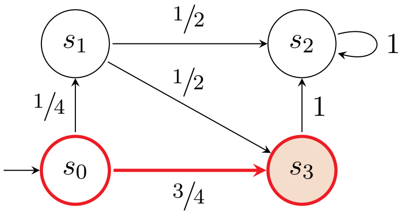


Critical subsystems for MCs

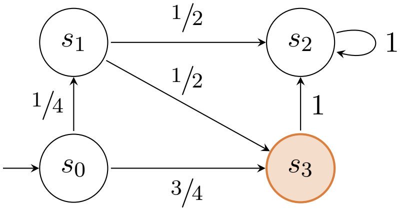
Example

We have that $\mathbb{P}(\Diamond\{s_3\}) = \frac{7}{8}$, therefore both specifications are **false**.

- $\mathcal{P}_{\leq 1/5}[\Diamond\{s_3\}]$



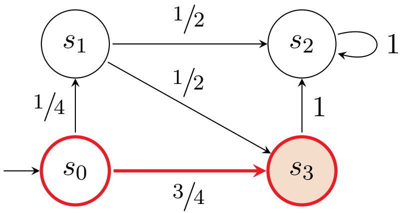
- $\mathcal{P}_{\leq 3/4}[\Diamond\{s_3\}]$



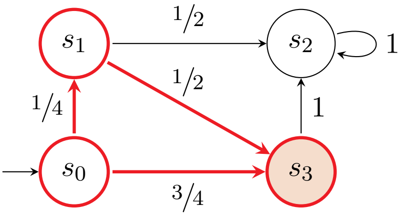
Critical subsystems for MCs
Example

We have that $\mathbb{P}(\Diamond\{s_3\}) = \frac{7}{8}$, therefore both specifications are **false**.

- $\mathcal{P}_{\leq 1/5}[\Diamond\{s_3\}]$



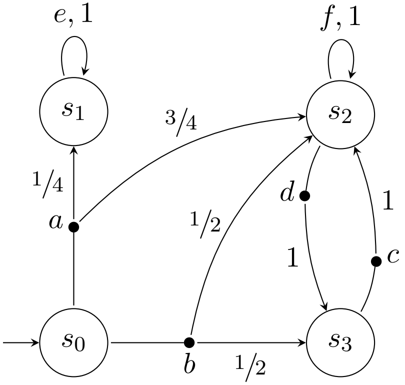
- $\mathcal{P}_{\leq 3/4}[\Diamond\{s_3\}]$



Markov Decision Processes

Models with probabilistic transitions and **non-deterministic choices**:

- Finite set of actions A
- Probabilistic transition function $\delta : S \times A \to \mathcal{D}(S)$



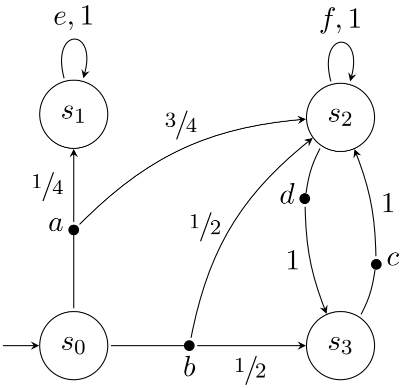
Markov Decision Processes

Models with probabilistic transitions and **non-deterministic choices**:

- Finite set of actions A
- Probabilistic transition function $\delta : S \times A \to \mathcal{D}(S)$

Strategy

A function $\sigma : S \to A$ that, given a current state, returns an available action.



Motivations

Counterexamples for MDPs

- For probabilistic systems with non-determinism, the behavior under the **strategies** is examined.

Verification:

$\mathcal{P}^{\forall}_{\leq\lambda}[\Diamond T]$: **every** strategy has a probability smaller than λ to reach T.

Counterexamples : Need to show that

$$\exists\sigma\,,\mathbb{P}^{\sigma}(\Diamond T) > \lambda$$

Done in [WJÁ+14][2]

[2] Wimmer et al.,“Minimal counterexamples for linear-time probabilistic verification”.

Motivations

Counterexamples for MDPs

- For probabilistic systems with non-determinism, the behavior under the **strategies** is examined.

Verification:

$\mathcal{P}^{\forall}_{\leq\lambda}[\Diamond T]$: **every** strategy has a probability smaller than λ to reach T.

Synthesis:

$\mathcal{P}^{\exists}_{\leq\lambda}[\Diamond T]$: there **exists** a strategy with probability smaller than λ to reach T.

Counterexamples : Need to show that

$$\exists\sigma\,,\mathbb{P}^{\sigma}(\Diamond T) > \lambda$$

Done in [WJÁ+14][2]

[2]Wimmer et al.,"Minimal counterexamples for linear-time probabilistic verification".

Motivations

Counterexamples for MDPs

- For probabilistic systems with non-determinism, the behavior under the **strategies** is examined.

Verification:

$\mathcal{P}^{\forall}_{\leq\lambda}[\Diamond T]$: **every** strategy has a probability smaller than λ to reach T.

Counterexamples : Need to show that

$$\exists\sigma\,,\mathbb{P}^{\sigma}(\Diamond T) > \lambda$$

Done in [WJÁ+14][2]

Synthesis:

$\mathcal{P}^{\exists}_{\leq\lambda}[\Diamond T]$: there **exists** a strategy with probability smaller than λ to reach T.

Counterexamples : Need to show that

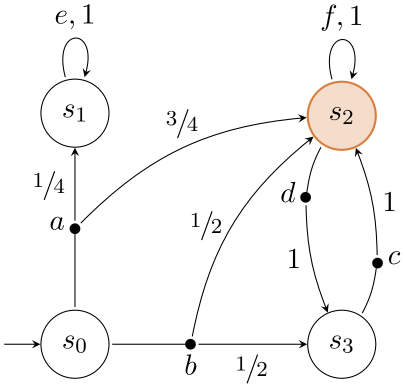
$$\forall\sigma\,,\mathbb{P}^{\sigma}(\Diamond T) > \lambda$$

Our ongoing work

[2] Wimmer et al.,"Minimal counterexamples for linear-time probabilistic verification".

Counterexample for synthesis

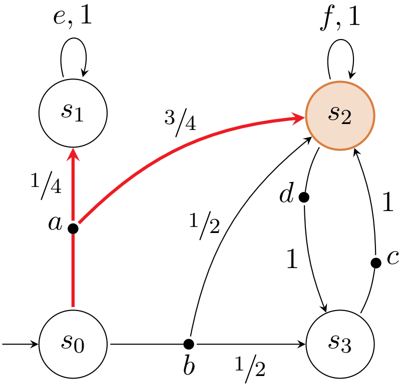
Example



Specification $\mathcal{P}^{\exists}_{\leq 1/4}[\Diamond\{s_2\}]$ is false :

Counterexample for synthesis

Example

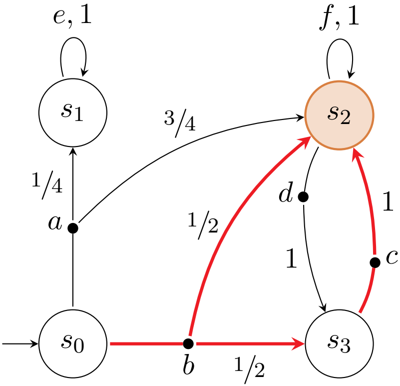


Specification $\mathcal{P}^{\exists}_{\leq 1/4}[\Diamond\{s_2\}]$ is false :

- $\mathbb{P}^{\sigma_1}(\Diamond\{s_2\}) = 3/4$

Counterexample for synthesis

Example



Specification $\mathcal{P}^{\exists}_{\leq 1/4}[\Diamond\{s_2\}]$ is false :

- $\mathbb{P}^{\sigma_1}(\Diamond\{s_2\}) = 3/4$
- $\mathbb{P}^{\sigma_2}(\Diamond\{s_2\}) = 1$

Therefore, we cannot find a strategy that has $\mathbb{P}(\Diamond\{s_2\}) \leq 1/4$.

Counterexample for synthesis

Example

In the case of synthesis, we need to keep the **structure** of the original MDP:

- Keep **every action** of each taken state

Counterexample for synthesis

Example

In the case of synthesis, we need to keep the **structure** of the original MDP:

- Keep **every action** of each taken state
- The missing probability is sent to a **sink** state

Counterexample for synthesis

Example

In the case of synthesis, we need to keep the **structure** of the original MDP:

- Keep **every action** of each taken state
- The missing probability is sent to a **sink** state
- **Minimize** the number of states

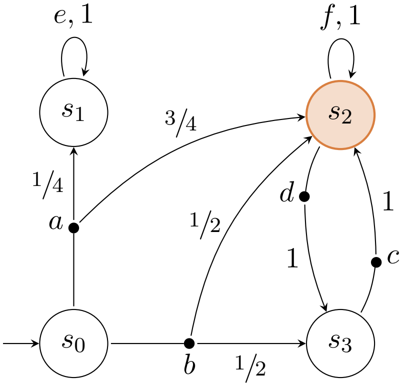
Counterexample for synthesis

Example

In the case of synthesis, we need to keep the **structure** of the original MDP:

- Keep **every action** of each taken state
- The missing probability is sent to a **sink** state
- **Minimize** the number of states

For $\mathcal{P}^{\exists}_{\leq 1/4}[\Diamond\{s_2\}]$:



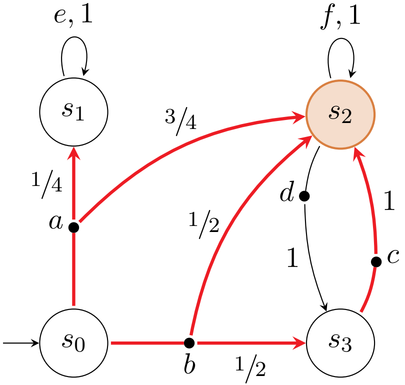
Counterexample for synthesis

Example

In the case of synthesis, we need to keep the **structure** of the original MDP:

- Keep **every action** of each taken state
- The missing probability is sent to a **sink** state
- **Minimize** the number of states

For $\mathcal{P}^{\exists}_{\leq 1/4}[\Diamond\{s_2\}]$:



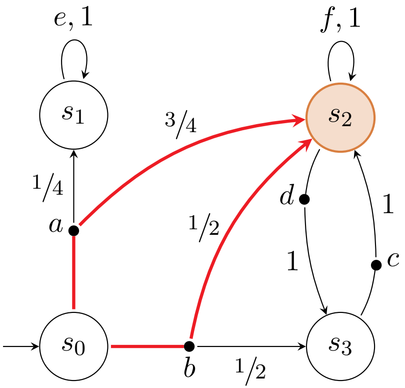
Counterexample for synthesis

Example

In the case of synthesis, we need to keep the **structure** of the original MDP:

- Keep **every action** of each taken state
- The missing probability is sent to a **sink** state
- **Minimize** the number of states

For $\mathcal{P}^{\exists}_{\leq 1/4}[\Diamond\{s_2\}]$:



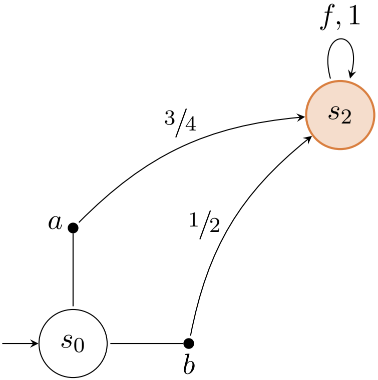
Counterexample for synthesis

Example

In the case of synthesis, we need to keep the **structure** of the original MDP:

- Keep **every action** of each taken state
- The missing probability is sent to a **sink** state
- **Minimize** the number of states

For $\mathcal{P}^{\exists}_{\leq 1/4}[\lozenge\{s_2\}]$:



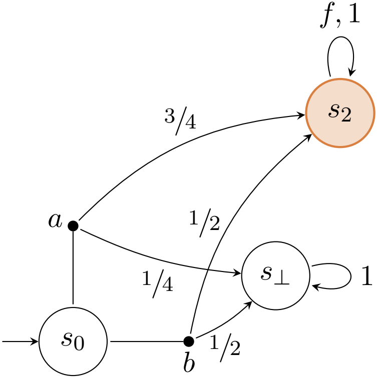
Counterexample for synthesis

Example

In the case of synthesis, we need to keep the **structure** of the original MDP:

For $\mathcal{P}^{\exists}_{\leq 1/4}[\lozenge\{s_2\}]$:

- Keep **every action** of each taken state
- The missing probability is sent to a **sink** state
- **Minimize** the number of states



Conclusion

For now:

- Works for specifications: $\mathcal{P}^{\exists}_{\sim\lambda}[\Diamond T]$ where $\sim \in \{\leq, <, \geq, >\}$
- **Generation** of counterexamples for synthesis through a Mixed Integer Linear Program (MILP)
- Used the tool **STORM** to implement our MILP
- Able to minimize on the **number of commands** when the input is in PRISM

Conclusion

For now:

- Works for specifications: $\mathcal{P}^{\exists}_{\sim\lambda}[\Diamond T]$ where $\sim \in \{\leq, <, \geq, >\}$
- **Generation** of counterexamples for synthesis through a Mixed Integer Linear Program (MILP)
- Used the tool **STORM** to implement our MILP
- Able to minimize on the **number of commands** when the input is in PRISM

Ongoing/Future work:

- Assess the perfomance of our method on **benchmarks**
- Use the information given by counterexamples for when the synthesis process **fails**

Thank you for your attention!

Bibliography I

Ábrahám, Erika et al. "Counterexample Generation for Discrete-Time Markov Models: An Introductory Survey". In: *Formal Methods for Executable Software Models - 14th International School on Formal Methods for the Design of Computer, Communication, and Software Systems, SFM 2014, Bertinoro, Italy, June 16-20, 2014, Advanced Lectures*. Ed. by Marco Bernardo et al. Vol. 8483. Lecture Notes in Computer Science. Springer, 2014, pp. 65–121. DOI: 10.1007/978-3-319-07317-0_3. URL: https://doi.org/10.1007/978-3-319-07317-0_3.

Wimmer, Ralf et al. "Minimal counterexamples for linear-time probabilistic verification". In: *Theor. Comput. Sci.* 549 (2014), pp. 61–100. DOI: 10.1016/j.tcs.2014.06.020. URL: https://doi.org/10.1016/j.tcs.2014.06.020.