Counterexamples in Probabilistic LTL Model Checking for Markov Chains

Matthias Schmalz[1] Daniele Varacca[2] Hagen Völzer[3]

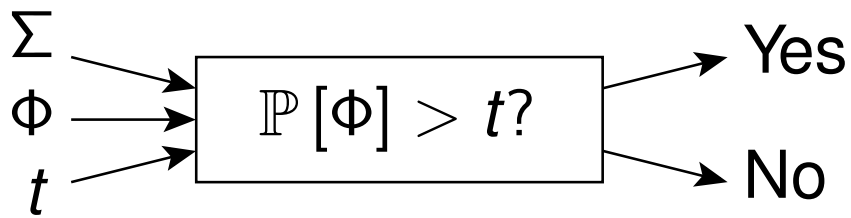
[1]ETH Zurich, Switzerland

[2]PPS - CNRS & Univ. Paris 7, France

[3]IBM Research – Zurich, Switzerland

September 1st, 2009

Probabilistic Model Checking



Σ: discrete-time finite-state Markov chain
Φ: linear-time temporal logic (LTL) formula

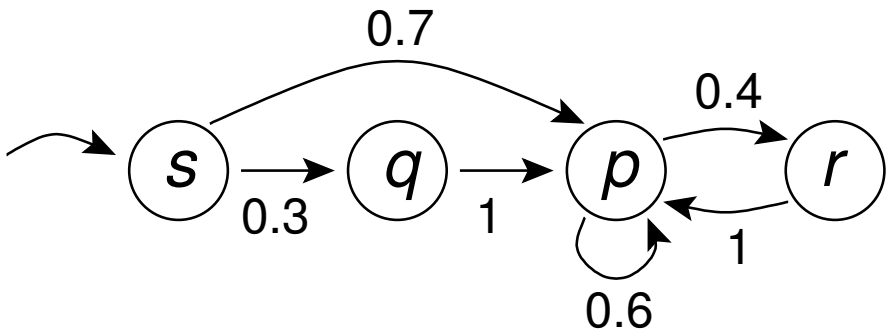
- "One of the most important advantages of model checking . . . is its counterexample facility." (Clarke et al.)

Contributions

- a way of representing counterexamples in probabilistic LTL model checking
- a method supporting the user in finding the error
- algorithms for computing our counterexample representations

Terminology

System (Markov chain) Σ:

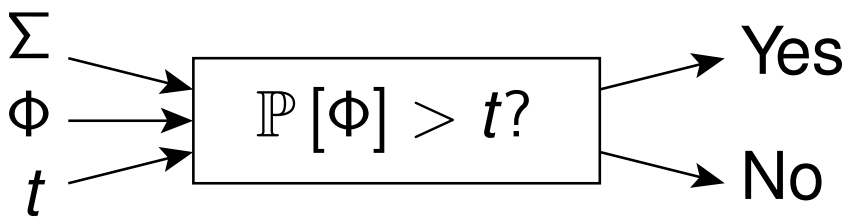


Notion:	Example:	
Path x	$s\ q\ p\ r\ p\ r\ \ldots$	
Property Y	$spr{\uparrow}$	(set of paths with prefix spr)
	$Sat(\Box\Diamond\, r)$	(set of paths infinitely often visiting r)

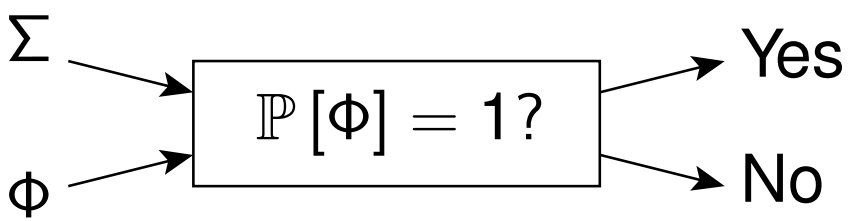
- Transition probabilities are positive.
- Paths are infinite.
- Properties are sets of paths.
- Probability of a property: $\mathbb{P}\,[spr{\uparrow}] = 0.7 \cdot 0.4$.

Quantitative and Qualitative

Quantitative Probabilistic Model Checking:



Qualitative Probabilistic Model Checking:



Outline

Validity: Counterexample

Specification: $A\Phi$

The model checker claims: $\Sigma \not\models A\Phi$

Counterexample: a path violating Φ

The user finds the bug by inspecting the counterexample.

Satisfiability: Simulation

Specification: $\mathsf{E} \Diamond \mathit{jackpot}$

The model checker claims: $\Sigma \not\models \mathsf{E} \Diamond \mathit{jackpot}$

Counterexample: set of all paths of Σ (useless)

How to find the bug?

- The user defined Σ and Φ.
- He has an idea how to reach the jackpot.
- The user tries to reach the jackpot.

- The user finds the bug by simulating the system.

Probabilistic Correctness: Interaction

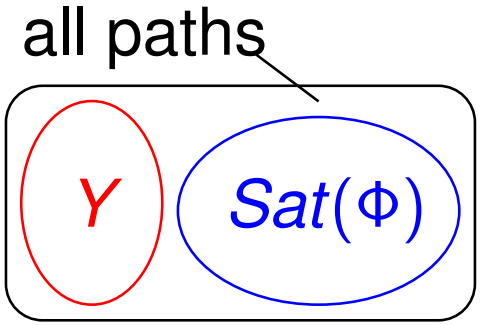
Validity		Probabilistic Correctness		Satisfiability
$\Sigma \models A\Phi$	$\Rightarrow$	$\mathbb{P}[\Phi] = 1$	$\Rightarrow$	$\Sigma \models E\Phi$
Counterexample: mc creates a path.	$\rightsquigarrow$	Interaction: both create a path.	$\leftsquigarrow$	Simulation: user creates a path.

Our Approach

Question: Why is $\mathbb{P}[\Phi] < 1$?

Counterexample: a property Y with

1. $Y \cap Sat(\Phi) = \varnothing$,
2. $\mathbb{P}[Y] > 0$.

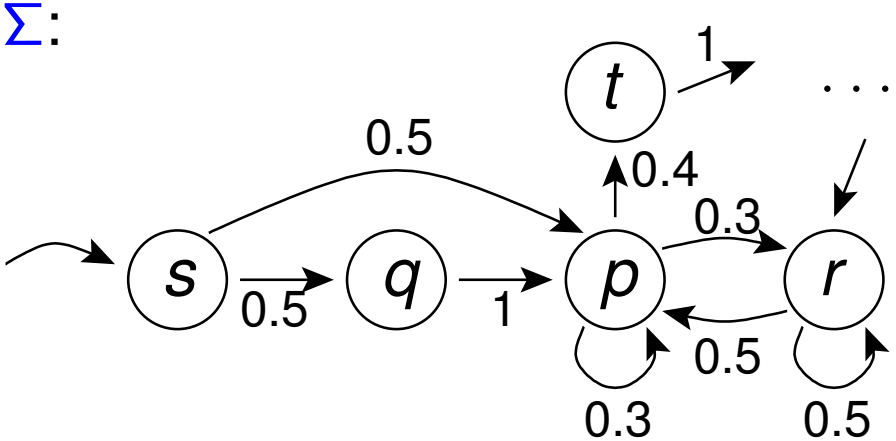


Interaction:

- The user learns why 1 and 2 hold.
- Helps the user find a bug.

An Example System

Σ:

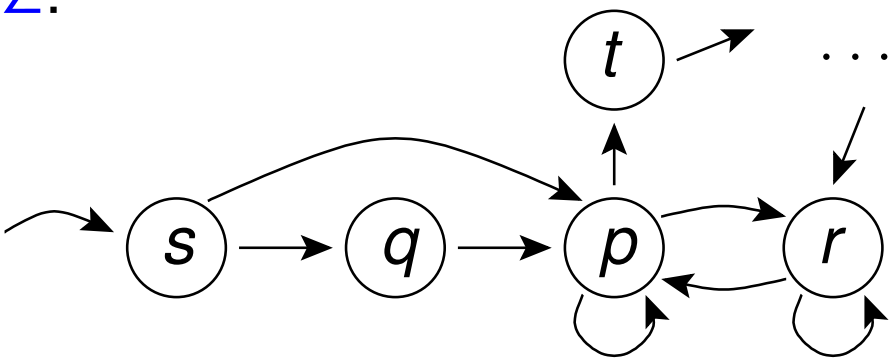


"$\mathbb{P}[\Phi] = 1$"

- is independent of precise transition probabilities!
- only depends on which states are connected by a transition.

An Example System

Σ:

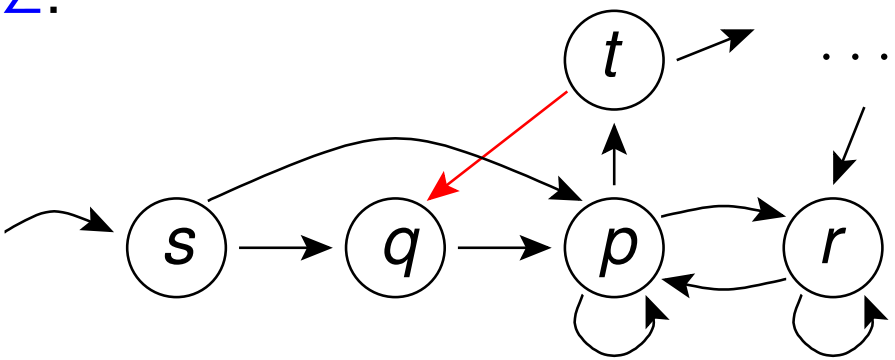


"$\mathbb{P}[\Phi] = 1$"

- is independent of precise transition probabilities!
- only depends on which states are connected by a transition.

An Example System

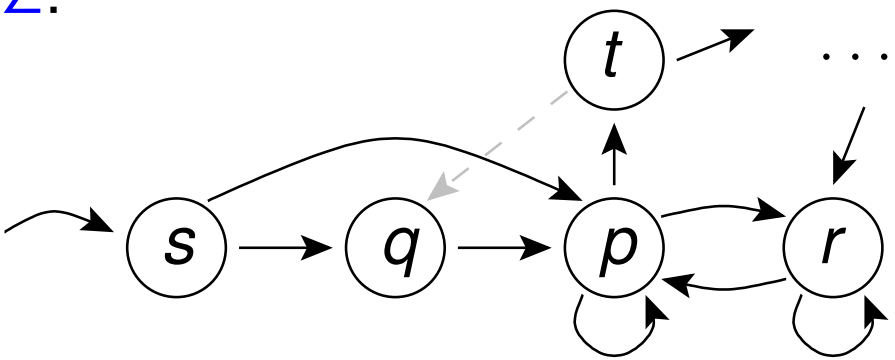
Σ:



Bug: transition $t \longrightarrow q$ is missing

An Example System

Σ:



I will . . .

- give a specification Φ,
- give a counterexample Y in our representation,
- explain the interaction helping the user find the bug.

Finitary Counterexamples

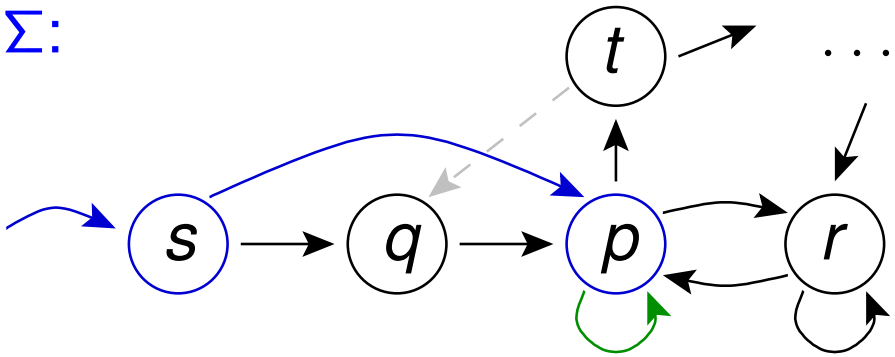
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



Try a finitary counterexample, e.g., $Y := sp\uparrow$.

- $Y \cap Sat(\Phi) \neq \varnothing$, as
  $spp^{\omega} \in Y \cap Sat(\Phi)$.

$\Rightarrow$ Y is no counterexample.

Moreover: there is no finitary counterexample!

Beyond Finitary Counterexamples

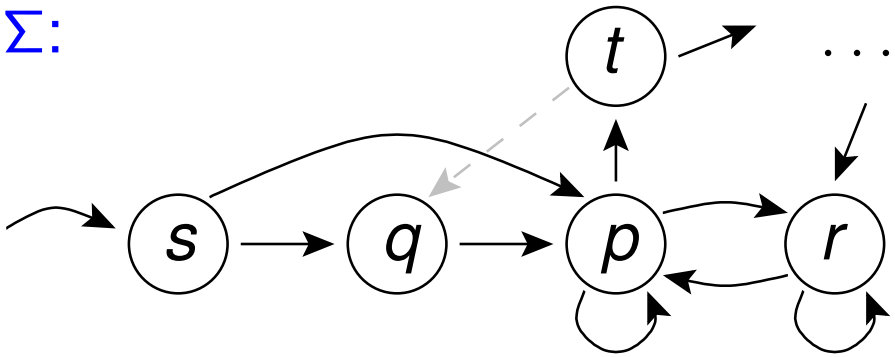
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



Counterexample: $Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$

- $Y \cap Sat(\Phi) \subseteq sp{\uparrow} \cap Sat(\Diamond\, q) = \varnothing$.
- rr belongs to a bscc reachable after sp.
- Hence, $\mathbb{P}[Y] = \mathbb{P}[sp{\uparrow}] > 0$.

$\Rightarrow$ Y is a counterexample.

Finding the Bug

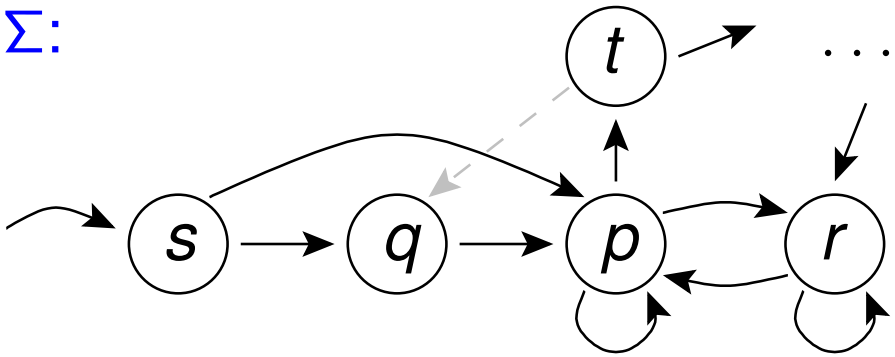
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



The model checker outputs $Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$ and explains:

1. rr is in a bscc reachable after sp.
2. $Y \cap Sat(\Phi) = \varnothing$.

$\Rightarrow\ \mathbb{P}[\Phi] < 1$.

Finding the Bug

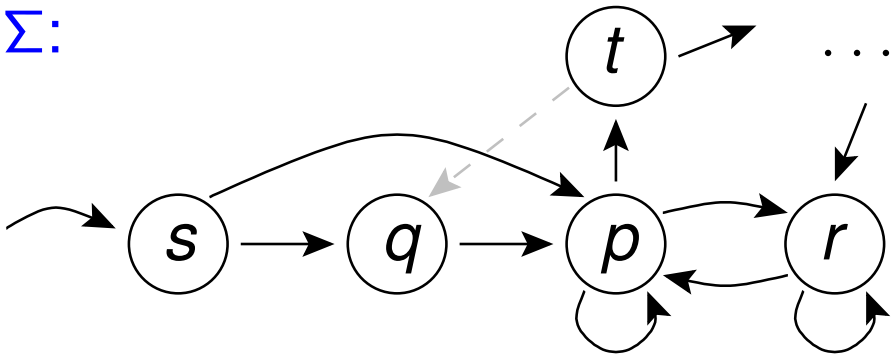
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



The model checker outputs $Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$ and explains:

1. rr is in a bscc reachable after sp. ✓
2. $Y \cap Sat(\Phi) = \varnothing$.

$\Rightarrow\ \mathbb{P}[\Phi] < 1$.

Finding the Bug

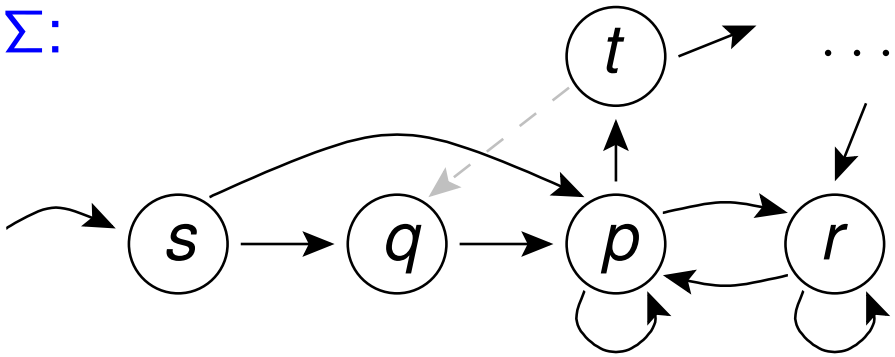
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



The model checker outputs $Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$ and explains:

1. rr is in a bscc reachable after sp. ✓
2. $Y \cap Sat(\Phi) = \varnothing$.

$\Rightarrow\ \mathbb{P}[\Phi] < 1$. ✓

Finding the Bug

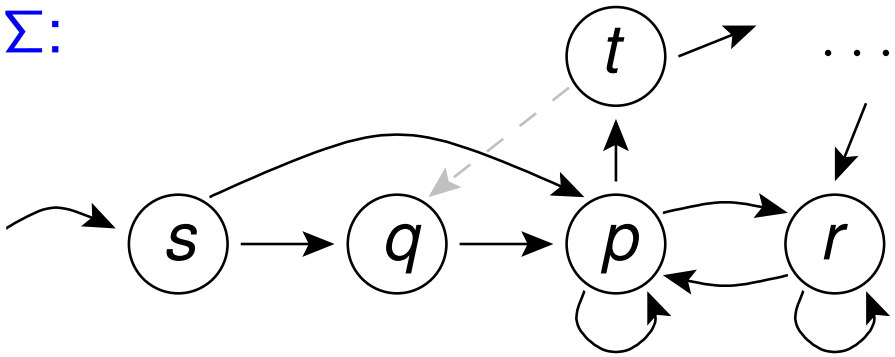
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



The model checker outputs $Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$ and explains:

1. rr is in a bscc reachable after sp. ✓
2. $Y \cap Sat(\Phi) = \varnothing$. ???

$\Rightarrow\ \mathbb{P}[\Phi] < 1$. ✓

Finding the Bug

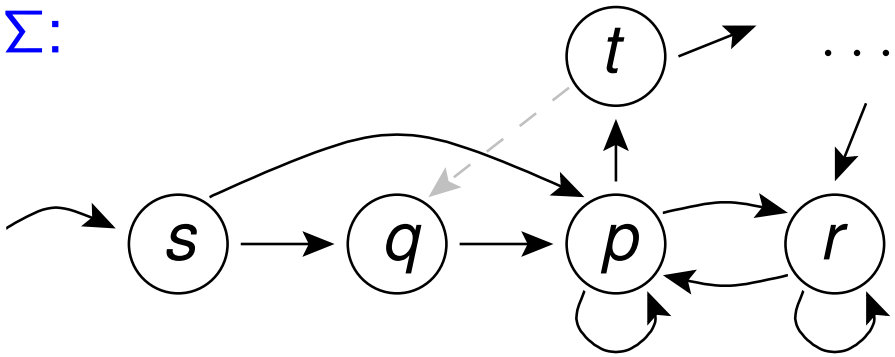
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



$Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$

Why is $Y \cap Sat(\Phi) = \varnothing$?

- User and MC create a path x.
- MC ensures $x \in Y$.
- User aims for $x \models \Phi$.
- By failing the user finds the bug!

Finding the Bug

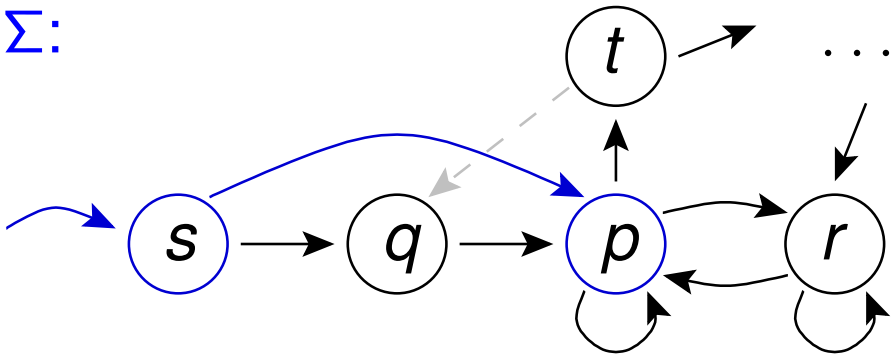
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



$Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$ $\quad s\ p$

Why is $Y \cap Sat(\Phi) = \varnothing$?

- User and MC create a path x.
- MC ensures $x \in Y$.
- User aims for $x \models \Phi$.
- By failing the user finds the bug!

Finding the Bug

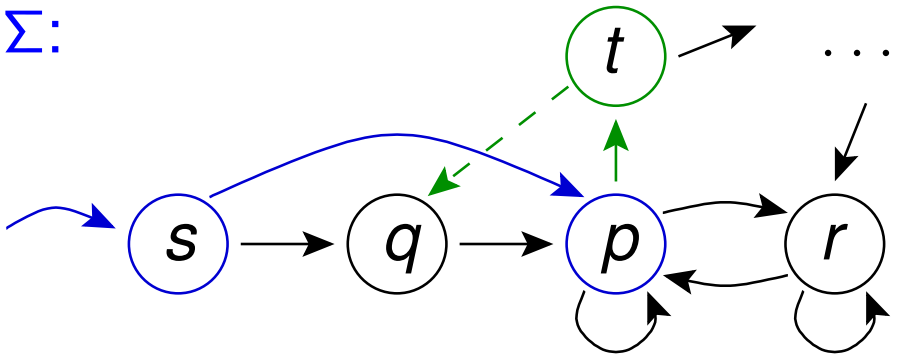
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



$Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$

s p t q

Why is $Y \cap Sat(\Phi) = \varnothing$?

- User and MC create a path x.
- MC ensures $x \in Y$.
- User aims for $x \models \Phi$.
- By failing the user finds the bug!

Finding the Bug

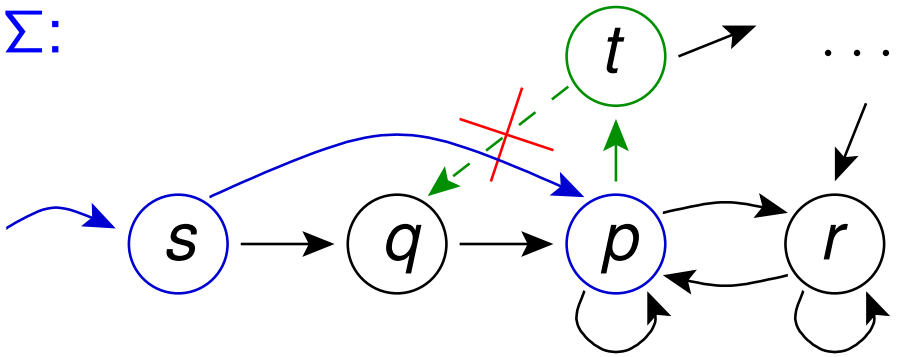
Specification:

$\Phi := \Box\Diamond\, rr \Rightarrow \Diamond\, q$

Question:

Why is $\mathbb{P}[\Phi] < 1$?

Σ:



$Y := sp{\uparrow} \cap Sat(\Box\Diamond\, rr)$

$s\ p\ t\ \cancel{q}$

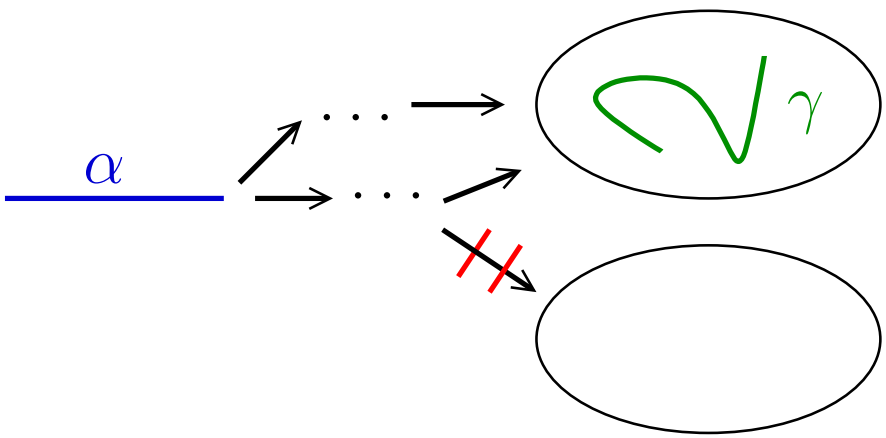
Why is $Y \cap Sat(\Phi) = \varnothing$?

- User and MC create a path x.
- MC ensures $x \in Y$.
- User aims for $x \models \Phi$.
- By failing the user finds the bug!

Finite Path Leading to a Recurrent Word

Definition

- Recurrent word $:=$ finite path fragment belonging to a bscc
- A finite path α (almost surely) leads to a recurrent word $\gamma \neq \lambda$. $\iff$ The bscc of γ is the only bscc reachable after α.



Qualitative Counterexamples

Question: Why is $\mathbb{P}[\Phi] < 1$?
Counterexample: $Y := \alpha\uparrow \cap \mathit{Sat}(\Box\Diamond\gamma)$, where

1. γ recurrent
2. α (almost surely) leads to γ
3. $Y \cap \mathit{Sat}(\Phi) = \varnothing$

Theorem (Soundness)

(a) *1, 2* $\Longrightarrow \mathbb{P}[\Box\Diamond\gamma \mid \alpha\uparrow] = 1$ *and hence* $\mathbb{P}[Y] > 0$

(b) *1, 2, 3* $\Longrightarrow \mathbb{P}[\Phi \mid \alpha\uparrow] = 0$ *and hence* $\mathbb{P}[\Phi] \leq 1 - \mathbb{P}[\alpha\uparrow] < 1$

- α explains how much probability is lost.
- α explains where the probability is lost.
- γ explains why the probability is lost.

Qualitative Counterexamples

Question: Why is $\mathbb{P}[\Phi] < 1$?
Counterexample: $Y := \alpha\uparrow \cap \mathit{Sat}(\Box\Diamond\gamma)$, where

1. γ recurrent
2. α (almost surely) leads to γ
3. $Y \cap \mathit{Sat}(\Phi) = \varnothing$

Theorem (Soundness)

(a) *1, 2* $\Longrightarrow \mathbb{P}[\Box\Diamond\gamma \mid \alpha\uparrow] = 1$ *and hence* $\mathbb{P}[Y] > 0$

(b) *1, 2, 3* $\Longrightarrow \mathbb{P}[\Phi \mid \alpha\uparrow] = 0$ *and hence* $\mathbb{P}[\Phi] \leq 1 - \mathbb{P}[\alpha\uparrow] < 1$

- α explains how much probability is lost.
- α explains where the probability is lost.
- γ explains why the probability is lost.

Qualitative Counterexamples

Question: Why is $\mathbb{P}[\Phi] < 1$?
Counterexample: $Y := \alpha\uparrow \cap \mathit{Sat}(\Box\Diamond\gamma)$, where

1. γ recurrent
2. α (almost surely) leads to γ
3. $Y \cap \mathit{Sat}(\Phi) = \varnothing$

Theorem (Soundness)

(a) *1, 2* $\Longrightarrow \mathbb{P}[\Box\Diamond\gamma \mid \alpha\uparrow] = 1$ *and hence* $\mathbb{P}[Y] > 0$

(b) *1, 2, 3* $\Longrightarrow \mathbb{P}[\Phi \mid \alpha\uparrow] = 0$ *and hence* $\mathbb{P}[\Phi] \leq 1 - \mathbb{P}[\alpha\uparrow] < 1$

- α explains how much probability is lost.
- α explains where the probability is lost.
- γ explains why the probability is lost.

Qualitative Counterexamples

Question: Why is $\mathbb{P}[\Phi] < 1$?
Counterexample: $Y := \alpha\uparrow \cap \mathit{Sat}(\Box\Diamond\gamma)$, where

1. γ recurrent
2. α (almost surely) leads to γ
3. $Y \cap \mathit{Sat}(\Phi) = \varnothing$

Theorem (Soundness)

(a) *1, 2* $\Longrightarrow \mathbb{P}[\Box\Diamond\gamma \mid \alpha\uparrow] = 1$ *and hence* $\mathbb{P}[Y] > 0$

(b) *1, 2, 3* $\Longrightarrow \mathbb{P}[\Phi \mid \alpha\uparrow] = 0$ *and hence* $\mathbb{P}[\Phi] \leq 1 - \mathbb{P}[\alpha\uparrow] < 1$

- α explains how much probability is lost.
- α explains where the probability is lost.
- γ explains why the probability is lost.

Qualitative Counterexamples

Question: Why is $\mathbb{P}[\Phi] < 1$?

Counterexample: $Y := \alpha\uparrow \cap \mathit{Sat}(\Box\Diamond\gamma)$, where

1. γ recurrent
2. α (almost surely) leads to γ
3. $Y \cap \mathit{Sat}(\Phi) = \varnothing$

Theorem (Completeness)

$\mathbb{P}[\Phi] < 1 \Longrightarrow$ *there are* α, γ *such that 1, 2, 3 hold.*

Interaction

Conditions 1, 2, 3 can be expressed in terms of path games between the user and the model checker.

Condition *i* holds $\iff$ the model checker has a winning strategy in the respective path game.

- To understand why a condition holds, the user plays the respective path game against the model checker.
- By losing the user finds the error in the system.

Interaction

Disjointness – $Y \cap Sat(\Phi) = \varnothing$

The path game:

- The model checker ensures $x \in Y$.
- The user wins iff $x \models \Phi$.
- The model checker has a winning strategy $\Longleftrightarrow$

  The user is unable to establish $x \models \Phi$ $\Longleftrightarrow$

  $Y \cap Sat(\Phi) = \varnothing$

- The game corresponds to the Banach-Mazur game.

Interaction

Disjointness – $Y \cap Sat(\Phi) = \varnothing$

The path game:

$x = \alpha$

- The model checker ensures $x \in Y$.
- The user wins iff $x \models \Phi$.
- The model checker has a winning strategy $\Longleftrightarrow$

  The user is unable to establish $x \models \Phi$ $\Longleftrightarrow$

  $Y \cap Sat(\Phi) = \varnothing$

- The game corresponds to the Banach-Mazur game.

Interaction

Disjointness – $Y \cap Sat(\Phi) = \varnothing$

The path game:

$x = \alpha$ 

- The model checker ensures $x \in Y$.
- The user wins iff $x \models \Phi$.
- The model checker has a winning strategy $\iff$

  The user is unable to establish $x \models \Phi$ $\iff$

  $Y \cap Sat(\Phi) = \varnothing$

- The game corresponds to the Banach-Mazur game.

Interaction

Disjointness – $Y \cap Sat(\Phi) = \varnothing$

The path game:

$x = \alpha$  γ

- The model checker ensures $x \in Y$.
- The user wins iff $x \models \Phi$.
- The model checker has a winning strategy $\iff$

  The user is unable to establish $x \models \Phi$ $\iff$

  $Y \cap Sat(\Phi) = \varnothing$

- The game corresponds to the Banach-Mazur game.

Interaction

Disjointness – $Y \cap Sat(\Phi) = \varnothing$

The path game:

$x = \alpha$  γ

- The model checker ensures $x \in Y$.
- The user wins iff $x \models \Phi$.
- The model checker has a winning strategy $\iff$

  The user is unable to establish $x \models \Phi$ $\iff$

  $Y \cap Sat(\Phi) = \varnothing$

- The game corresponds to the Banach-Mazur game.

Interaction

Disjointness – $Y \cap Sat(\Phi) = \varnothing$

The path game:

$x = \alpha$  $\cdots$

- The model checker ensures $x \in Y$.
- The user wins iff $x \models \Phi$.
- The model checker has a winning strategy $\iff$

  The user is unable to establish $x \models \Phi$ $\iff$

  $Y \cap Sat(\Phi) = \varnothing$

- The game corresponds to the Banach-Mazur game.

Interaction

Disjointness – $Y \cap Sat(\Phi) = \varnothing$

The path game:

$x = \alpha$  $\gamma \cdots \models \Phi$

- The model checker ensures $x \in Y$.
- The user wins iff $x \models \Phi$.
- The model checker has a winning strategy $\iff$

  The user is unable to establish $x \models \Phi$ $\iff$

  $Y \cap Sat(\Phi) = \varnothing$

- The game corresponds to the Banach-Mazur game.

Outline

Quantitative Counterexamples

Quantitative Counterexample: $Y := W{\uparrow} \cap Fair_\Sigma(R)$

- W: set of finite paths
- R: set of recurrent words
- $Y \cap Sat(\Phi) = \varnothing$, $\mathbb{P}[Y]$ "sufficiently" large

Theorem (Soundness)

- $\mathbb{P}[\Phi] \leq 1 - \mathbb{P}[W{\uparrow}]$
- $\mathbb{P}[\Phi \mid W{\uparrow}] = 0$

Theorem (Completeness)

$\mathbb{P}[\Phi] \leq 1 - t \implies$ *There is a counterexample* $W{\uparrow} \cap Fair_\Sigma(R)$, *where* R *contains one rec. word per bscc, and* W *is regular.*

Interaction: as W is regular, various techniques from the literature can be applied for presenting W to the user.

Computing Counterexamples

We have developed non-trivial extensions of an algorithm of Courcoubetis and Yannakakis (1995).

	Complexity in $\lvert\Sigma\rvert$	Complexity in $\lvert\Phi\rvert$
α, γ	$\lvert\Sigma\rvert$	exonential
α of max. probability	$\lvert\Sigma\rvert \cdot \log \lvert\Sigma\rvert$	doubly exp.
W	$\lvert\Sigma\rvert$	doubly exp.
R	$\lvert\Sigma\rvert \cdot \#\text{bsccs}$	exponential

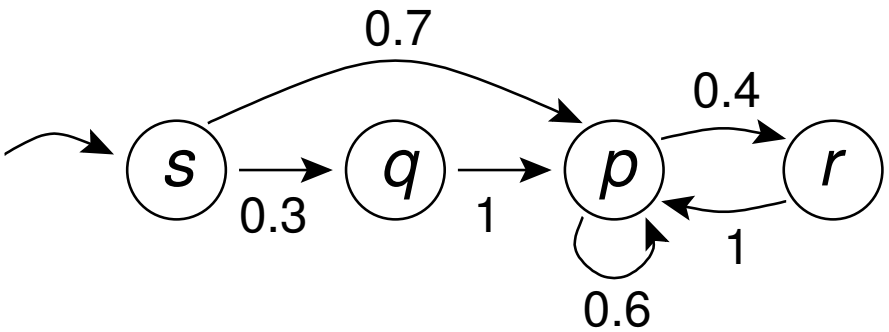
Summary

- A qualitative counterexample can be represented as $\alpha\uparrow \cap Sat(\Box \diamond \gamma)$.
- A quantitative counterexample can be represented as $W\uparrow \cap Fair_{\Sigma}(R)$, where W is regular.
- We describe an interactive game that supports the user in finding the error.
- We have developed algorithms computing our counterexample representations.

Future directions:

- Generalize results for Markov Decision Processes.
- Case studies

Periodic Counterexamples



- Each periodic path has probability zero, e.g., $\mathbb{P}[\{s(pr)^\omega\}] = 0$.
- The set of all periodic paths is countable.

$\Rightarrow$ The set of all periodic paths has probability zero.

Sets of periodic paths can in general not be used as counterexamples!