Strategy Synthesis for (Global) Window PCTL

Shibashis Guha

Tata Institute of Fundamental Research

Joint work with Benjamin Bordais, Damien Busatto-Gaston, and Jean-François Raskin

July 31, 2022

Model-checking Probabilistic Concurrent Systems

Automatic Verification of Probabilistic Concurrent Finite-State Programs

Moshe Y. Vardi[†]

Center for Study of Language and Information
Stanford University,

ABSTRACT

The *verification problem* for *probabilistic concurrent finite-state program* is to decide whether such a program satisfies its *linear temporal logic* specification. We describe an

- Concurrent Markov chains: Markov chains augmented with nondeterministic states with the nondeterminism being resolved by a scheduler.
- Markov Decision Processes (MDP) in the current literature.

Strategy Synthesis Problem

Automatic Verification of Probabilistic Concurrent Finite-State Programs

Moshe Y. Vardi[†]

Center for Study of Language and Information
Stanford University,

ABSTRACT

The *verification problem* for *probabilistic concurrent finite-state program* is to decide whether such a program satisfies its *linear temporal logic* specification. We describe an

- "...designining a correct concurrent protocol is not an easy task.".
- Here, we consider the challenging problem of designing a system which is correct by construction against a given specification.

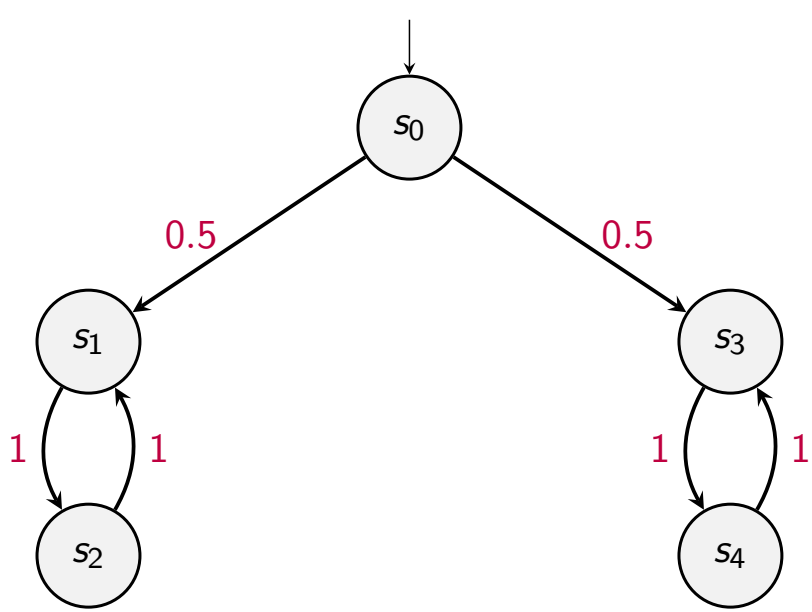
Strategy Synthesis Problem

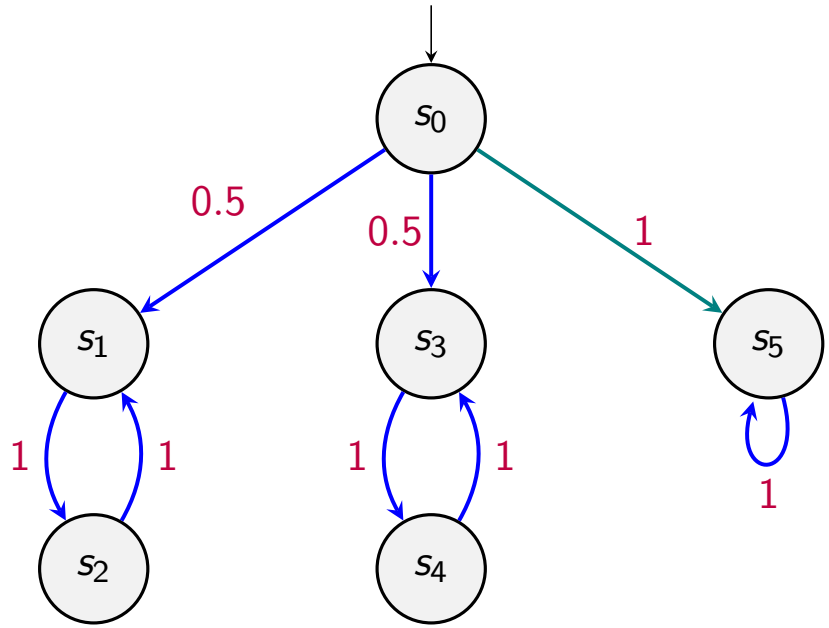
- "...designining a correct concurrent protocol is not an easy task.".
- Here, we consider the challenging problem of designing a system which is correct by construction against a given specification.

Strategy synthesis problem:

Given an MDP $\mathcal{M}$, a probabilistic temporal logic formula Φ, determine if there exists a strategy σ to resolve the nondeterminism in $\mathcal{M}$ such that the resulting Markov chain (MC) $\mathcal{M}[\sigma]$ satisfies Φ,
and if so, construct one such strategy.

Markov decision process





$\mathcal{M} = \langle S, A, s_{\text{init}}, \mathbb{P}, \text{AP}, L \rangle$

$\mathbb{P} : S \times A \to \text{Dist}(S)$ is a transition function.

Strategies

Strategy in general

A (randomized memoryful/history-dependent) *strategy* is a function

$$\sigma : \mathsf{FPaths}_{\mathcal{M}} \to \mathsf{Dist}(A)$$

that maps finite paths to distributions over actions.

Strategies

Strategy in general

A (randomized memoryful/history-dependent) *strategy* is a function

$$\sigma : \mathsf{FPaths}_{\mathcal{M}} \to \mathsf{Dist}(A)$$

that maps finite paths to distributions over actions.

Deterministic (D) strategy

$\sigma : \mathsf{FPaths}_{\mathcal{M}} \to A$
(otherwise, randomized (R))

Strategies

Strategy in general

A (randomized memoryful/history-dependent) *strategy* is a function

$$\sigma : \mathsf{FPaths}_{\mathcal{M}} \to \mathsf{Dist}(A)$$

that maps finite paths to distributions over actions.

Deterministic (D) strategy

$\sigma : \mathsf{FPaths}_{\mathcal{M}} \to A$
(otherwise, randomized (R))

Memoryless (M) strategy

$\sigma : S \to \mathsf{Dist}(A)$
(otherwise, history-dependent (H))

Strategies

Strategy in general

A (randomized memoryful/history-dependent) *strategy* is a function

$$\sigma : \mathsf{FPaths}_{\mathcal{M}} \to \mathsf{Dist}(A)$$

that maps finite paths to distributions over actions.

Deterministic (D) strategy

$\sigma : \mathsf{FPaths}_{\mathcal{M}} \to A$
(otherwise, randomized (R))

Memoryless (M) strategy

$\sigma : S \to \mathsf{Dist}(A)$
(otherwise, history-dependent (H))

HR, HD, MR, MD

Probabilistic Computational Tree Logic (PCTL) for specification

$$\Phi := p \mid \neg p \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \mathbb{P}\left[\varphi\right] \succcurlyeq c$$

$$\varphi := \mathsf{X}\,\Phi \mid \Phi_1\,\mathsf{U}^{\ell}\,\Phi_2 \mid \Phi_1\,\mathsf{W}^{\ell}\,\Phi_2 \mid \Phi_1\,\mathsf{U}^{\infty}\,\Phi_2 \mid \Phi_1\,\mathsf{W}^{\infty}\,\Phi_2$$

Strategy Synthesis for PCTL

Given a PCTL formula Φ, and an MDP $\mathcal{M}$:
Does there exist a strategy σ such that $\mathcal{M}[\sigma] \models \Phi$?

Known to be highly undecidable for existence of HD strategies (Kucera et al, LICS'06)

L-PCTL specification

L-PCTL extends PCTL with *linear constraints* over probability subformulae.

$$\Phi := p \mid \neg p \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \sum_{i=1}^{n} c_i \mathbb{P}\left[\varphi_i\right] \succcurlyeq c_0$$

$$\varphi := \mathsf{X}^{\ell}\, \Phi \mid \Phi_1\, \mathsf{U}^{\ell}\, \Phi_2 \mid \Phi_1\, \mathsf{W}^{\ell}\, \Phi_2 \mid \Phi_1\, \mathsf{U}^{\infty}\, \Phi_2 \mid \Phi_1\, \mathsf{W}^{\infty}\, \Phi_2$$

The unbounded U and W are not used in *window* L-PCTL.

Window L-PCTL is a local property.

$\mathbb{P}(\mathsf{F}^{5}\, \mathrm{Good}) \geq 0.95$

The probability to reach a good state within 5 steps is at least 0.95.

L-PCTL specification

L-PCTL extends PCTL with *linear constraints* over probability subformulae.

$$\Phi := p \mid \neg p \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \sum_{i=1}^{n} c_i \mathbb{P}\left[\varphi_i\right] \succcurlyeq c_0$$

$$\varphi := \mathsf{X}^{\ell}\, \Phi \mid \Phi_1\, \mathsf{U}^{\ell}\, \Phi_2 \mid \Phi_1\, \mathsf{W}^{\ell}\, \Phi_2 \mid \Phi_1\, \mathsf{U}^{\infty}\, \Phi_2 \mid \Phi_1\, \mathsf{W}^{\infty}\, \Phi_2$$

The unbounded U and W are not used in *window* L-PCTL.

Window L-PCTL is a local property.

$\mathbb{P}(\mathsf{F}^{5}\, \mathrm{Good}) \geq 0.95$

The probability to reach a good state within 5 steps is at least 0.95.

Global window property: $AG\Phi$

Along all paths, at every state, the local window property Φ will be satisfied.

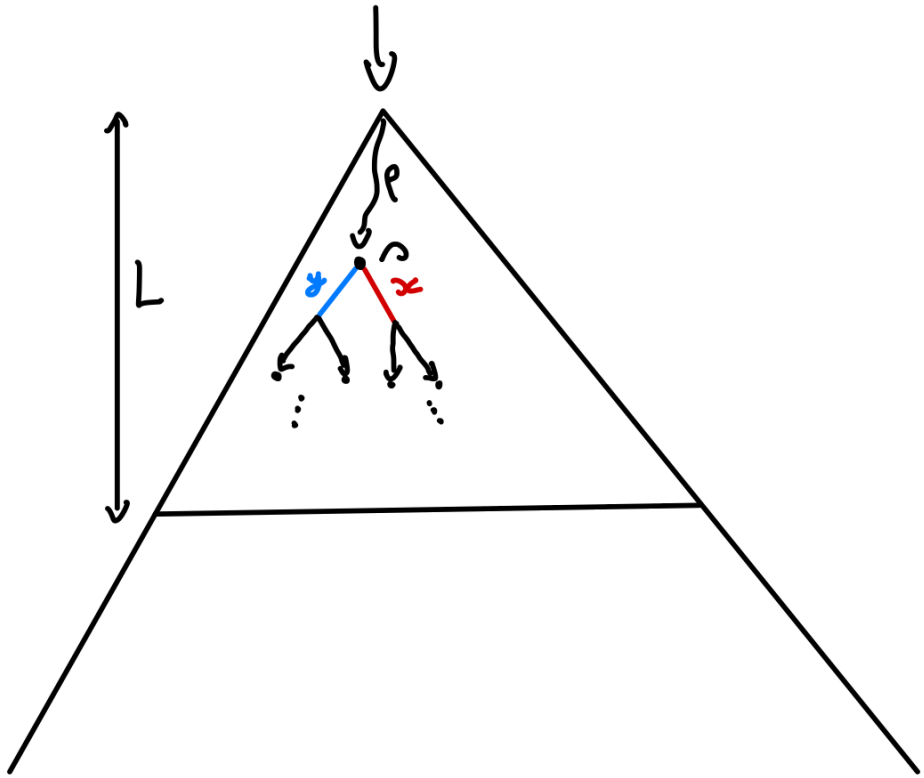
$\mathsf{A}\,\mathsf{G}\,[\mathbb{P}(\mathsf{F}^{5}\, \mathrm{Good}) \geq 2 \times \mathbb{P}(\mathsf{F}^{10}\, \mathrm{Bad}))]$

Synthesis for Window L-PCTL objective

Complexity results

	M	H
D	NP-complete (Baier et al, '04)	PSPACE-complete
R	PSPACE SQRT-SUM-hard (Kucera et al., '06)	EXPSPACE PSPACE-hard

Window L-PCTL: HR-synthesis



There is a variable corresponding to every finite path of length at most L and an action available from the last state.

$\exists$-$\mathbb{R}$ formula of exponential size: EXPSPACE procedure.

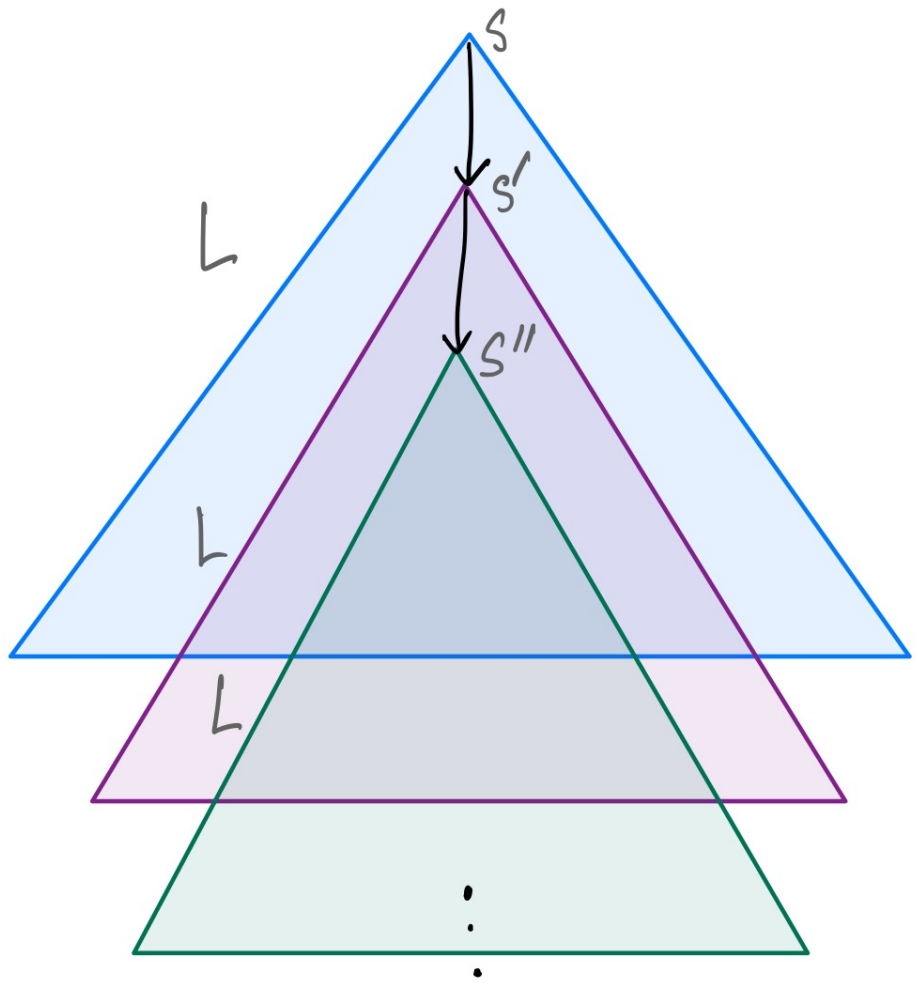
Synthesis for global window L-PCTL objective

A G Φ, where Φ is a window L-PCTL formula.

Complexity results

	M	H
D	NP-complete (Baier et al, '04)	2EXPTIME EXPTIME-hard
R	PSPACE SQRT-SUM-hard (Kucera et al., '06)	*coRE*-complete (for flat and non-strict) Σ_1^1-hard (for flat)

Global window L-PCTL: HR-synthesis



Fixed-point characterization: There exists a strategy σ so that $s \models_\sigma \mathsf{A}\,\mathsf{G}\,\Phi$ if and only if the greatest fixed point is non-empty.

Synthesis for global window L-PCTL objective

Complexity results

	M	H
D	NP-complete (Baier et al, '04)	2EXPTIME EXPTIME-hard
R	PSPACE SQRT-SUM-hard (Kucera et al., '06)	*coRE*-complete (for flat and non-strict) Σ_1^1-hard (for flat)

The first decidability result for HD strategies and quantitative probabilistic temporal properties.

Synthesis for global window L-PCTL objective

Complexity results

	M	H
D	NP-complete (Baier et al, '04)	2EXPTIME EXPTIME-hard
R	PSPACE SQRT-SUM-hard (Kucera et al., '06)	*coRE*-complete (for flat and non-strict) Σ_1^1-hard (for flat)

The first decidability result for HD strategies and quantitative probabilistic temporal properties.

Thank you for your attention!