Statistical model checking for parameterized model

Benoît Delahaye[1] Paulin Fournier[1] Didier Lime[2]

Université de Nantes - LS2N, UMR 6004 - Nantes, France

École Centrale de Nantes - LS2N, UMR 6004 - Nantes, France

SynCoP 2018

Motivation

Model-checking of pMC

- Suffers from the same problems as standard MC: state space explosion
- Produces large rational functions as the probability of satisfying a property
- Existing cannot handle large number of parameters

In some cases (large models, large number of parameters), it could be beneficial to use approximation techniques such as Statistical Model Checking, but

- SMC is limited to models without non-determinism
- Attempts to extend SMC to models with non-det have limitations
  - No precision / confidence intervals
  - Cannot be easily adapted to parameters (dependent transition probabilities)

Contribution

We propose a parametric version of SMC for parameterized models (pMC).

- Computes an approximation of the probability of satisfying a property
  - as a parametric function
  - polynomial
  - with parametric confidence intervals

- Allows to compute the value of the probability for all parameter values (with varying precision)

Outline

Introduction

Parametric Markov Chains and Properties
- Background - Properties
- Parametric Markov Chains

Monte Carlo and pMCs

Implementation

Discussion

Outline

Introduction

Parametric Markov Chains and Properties
- Background - Properties
- Parametric Markov Chains

Monte Carlo and pMCs

Implementation

Discussion

Markov Chains

Definition (Markov chain)

A *Markov chain* (MC, for short) is a tuple $\mathcal{M} = (S, s_0, P)$ where S is a denumerable set of states, $s_0 \in S$ is the initial state and $P : S \times S \to [0, 1]$ is the transition probability function.

- Finite run: $\rho = s_0 s_1 \dots s_n$ s.t. $P(s_i, s_{i+1}) > 0$
- $\Gamma(l)$: set of all runs of length l in $\mathcal{M}$
- Probability of a finite run: $\mathbb{P}_{\mathcal{M}}(\rho) = \Pi_{i=1}^{n} P(s_{i-1}, s_i)$

Properties

In the context of SMC, we only consider properties on bounded runs. Let $r : \Gamma(l) \to \mathbb{R}$ be a reward function.

Reachability $\mathbb{P}_{\mathcal{M}}(\Diamond^{\leq l} s)$. $\rho \models \Diamond^{\leq l} s$, if there exists $i \leq l$ such that $s_i = s$.

Safety $\mathbb{P}_{\mathcal{M}}(\Box^{=l} E)$. $\rho \models \Box^{=l} E$, if for all $i \leq l$, $s_i \in E$.

Expected reward $\mathbb{E}^l_{\mathcal{M}}(r)$. $\mathbb{E}^l_{\mathcal{M}}(r) = \sum_{\rho \in \Gamma(l)} \mathbb{P}_{\mathcal{M}}(\rho) r(\rho)$ is the expected value of r on the runs of length l.

Remark

For any property $\varphi \subseteq \Gamma(l)$, $\mathbb{P}_{\mathcal{M}}(\varphi) = \mathbb{E}^l_{\mathcal{M}}(\mathbb{1}_\varphi)$

$\Rightarrow$ we focus on properties of the form $\mathbb{E}^l_{\mathcal{M}}(r)$.

Outline

Introduction

Parametric Markov Chains and Properties
- Background - Properties
- Parametric Markov Chains

Monte Carlo and pMCs

Implementation

Discussion

Parametric Markov Chains (pMCs)

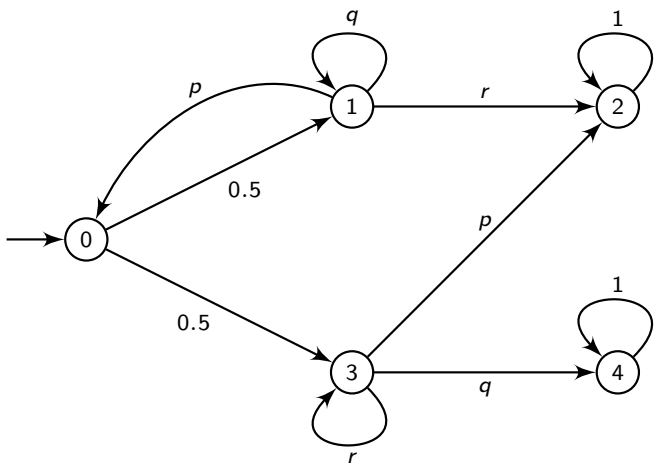
Definition (Parametric Markov chain)

A *Parametric Markov chain* is a tuple $\mathcal{M} = (S, s_0, P, \mathbb{X})$ such that S is a finite set of states, $s_0 \in S$ is the initial state, $\mathbb{X}$ is a finite set of parameters, and $P : S \times S \to Poly(\mathbb{X})$ is a parametric transition probability function.

If $v \in \mathbb{R}^{\mathbb{X}}$ is a valuation of the parameters,

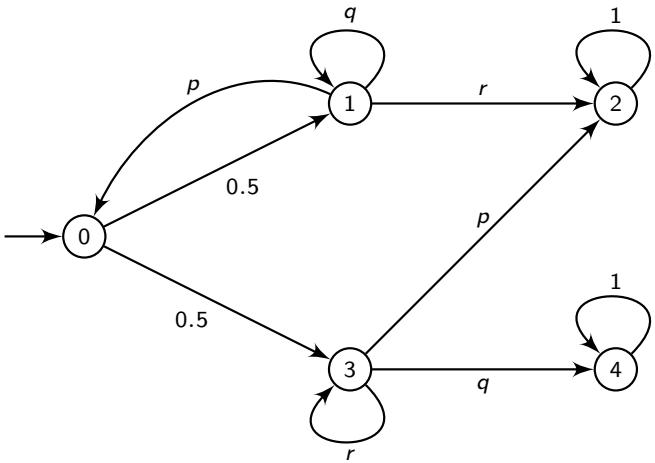
- P_v: transition probabilities under v : $P_v(s, s') = P(s, s')(v)$
- v is *valid* if (S, s_0, P_v) is a MC
- $\mathcal{M}^v = (S, s_0, P_v)$
- Runs and probabilities are similar to MC, but parametric

Example 1

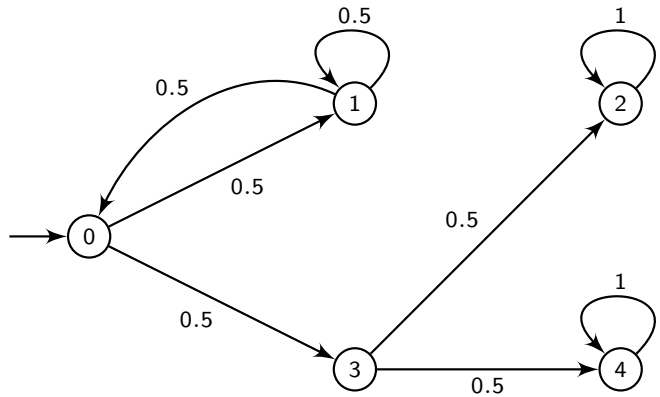


pMC $\mathcal{M}_1$

Example 1



pMC $\mathcal{M}_1$



MC $\mathcal{M}_1^v$ for parameter valuation v such that $v(p) = v(q) = 0.5$ and $v(r) = 0$

Outline

Introduction

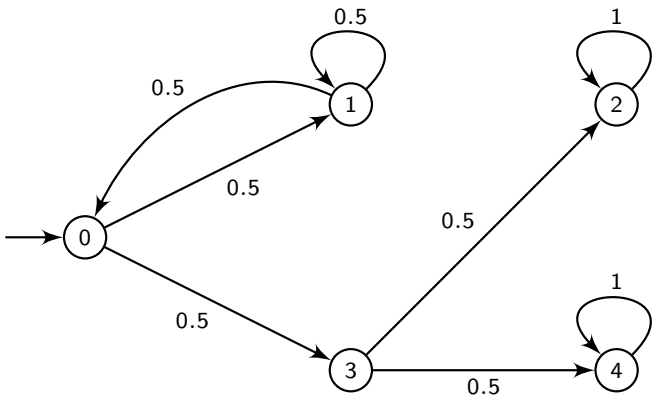
Parametric Markov Chains and Properties
- Background - Properties
- Parametric Markov Chains

Monte Carlo and pMCs

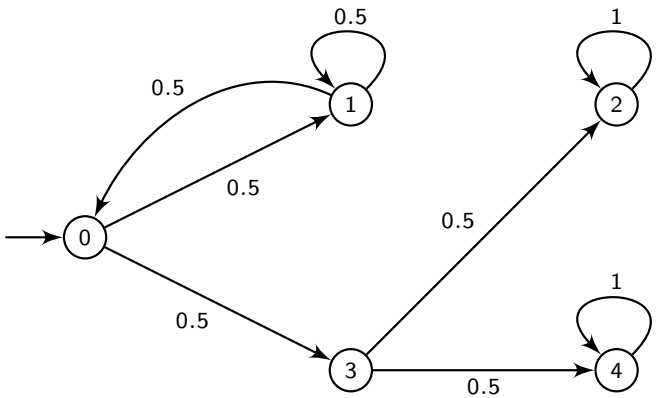
Implementation

Discussion

Monte Carlo for MCs

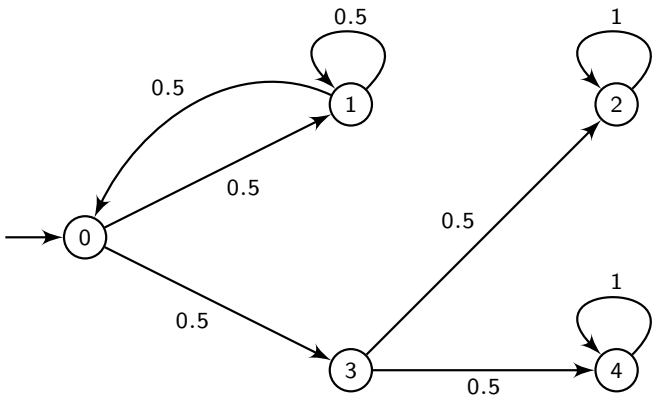


Monte Carlo for MCs



- Run n simulations ρ_i of length l

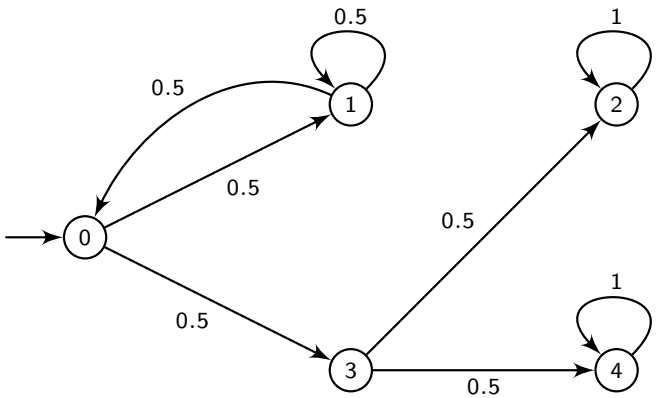
Monte Carlo for MCs



$$\rho_1 = 0 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1$$
$$\rho_2 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 4 \cdot 4$$
$$\rho_3 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$
$$\rho_4 = 0 \cdot 1 \cdot 0 \cdot 1 \cdot 0 \cdot 3$$
$$\rho_5 = 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 1$$
$$\rho_6 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$
$$\rho_7 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2$$
$$\rho_8 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 4 \cdot 4$$

- Run n simulations ρ_i of length l

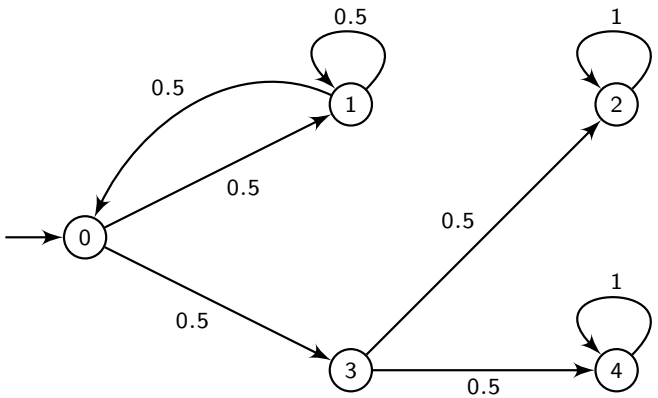
Monte Carlo for MCs



$$\rho_1 = 0 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1$$
$$\rho_2 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 4 \cdot 4$$
$$\rho_3 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$
$$\rho_4 = 0 \cdot 1 \cdot 0 \cdot 1 \cdot 0 \cdot 3$$
$$\rho_5 = 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 1$$
$$\rho_6 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$
$$\rho_7 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2$$
$$\rho_8 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 4 \cdot 4$$

- Run n simulations ρ_i of length l
- $r(\rho_i) = 1$ if ρ_i reaches 4

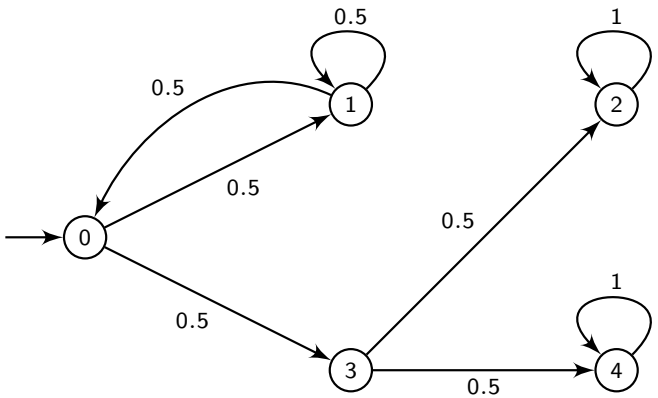
Monte Carlo for MCs



$$
\begin{aligned}
\rho_1 &= 0 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 & r(\rho_1) &= 0 \\
\rho_2 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 4 \cdot 4 & r(\rho_2) &= 1 \\
\rho_3 &= 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & r(\rho_3) &= 0 \\
\rho_4 &= 0 \cdot 1 \cdot 0 \cdot 1 \cdot 0 \cdot 3 & r(\rho_4) &= 0 \\
\rho_5 &= 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 1 & r(\rho_5) &= 1 \\
\rho_6 &= 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & r(\rho_6) &= 0 \\
\rho_7 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2 & r(\rho_7) &= 0 \\
\rho_8 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 4 \cdot 4 & r(\rho_8) &= 1
\end{aligned}
$$

- Run n simulations ρ_i of length l
- $r(\rho_i) = 1$ if ρ_i reaches 4

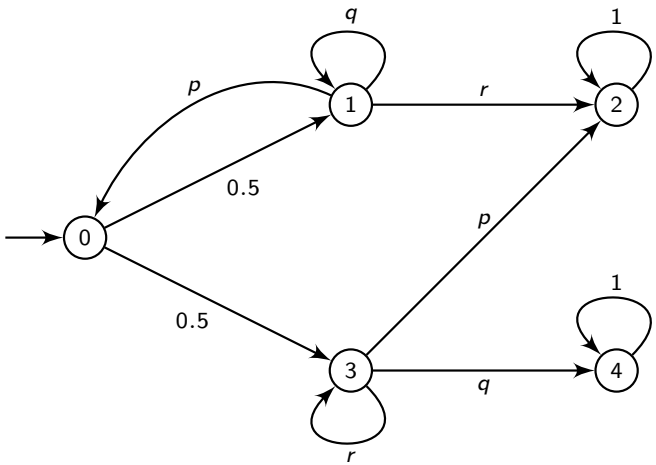
Monte Carlo for MCs



$$
\begin{array}{ll}
\rho_1 = 0 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 & r(\rho_1) = 0 \\
\rho_2 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 4 \cdot 4 & r(\rho_2) = 1 \\
\rho_3 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & r(\rho_3) = 0 \\
\rho_4 = 0 \cdot 1 \cdot 0 \cdot 1 \cdot 0 \cdot 3 & r(\rho_4) = 0 \\
\rho_5 = 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 1 & r(\rho_5) = 1 \\
\rho_6 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & r(\rho_6) = 0 \\
\rho_7 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2 & r(\rho_7) = 0 \\
\rho_8 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 4 \cdot 4 & r(\rho_8) = 1
\end{array}
$$

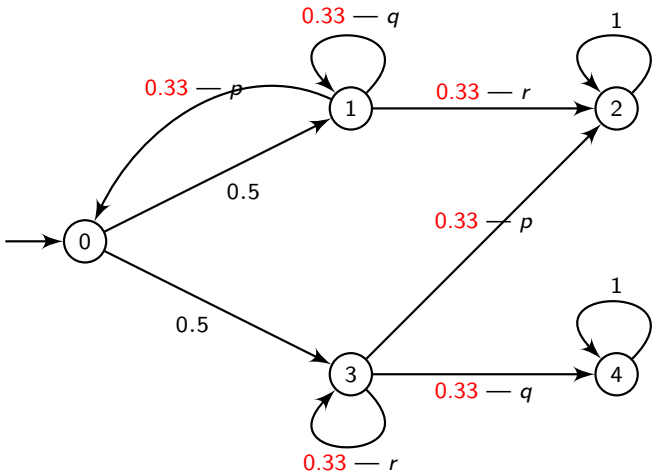
- Run n simulations ρ_i of length l
- $r(\rho_i) = 1$ if ρ_i reaches 4
- $\mathbb{E}^l_{\mathcal{M}}(r) \sim \frac{\sum r(\rho_i)}{n} \Rightarrow$ Here, $\mathbb{E}^5_{\mathcal{M}}(r) \sim 0.375$ (exact: 0.3125)

Intuition for pMCs



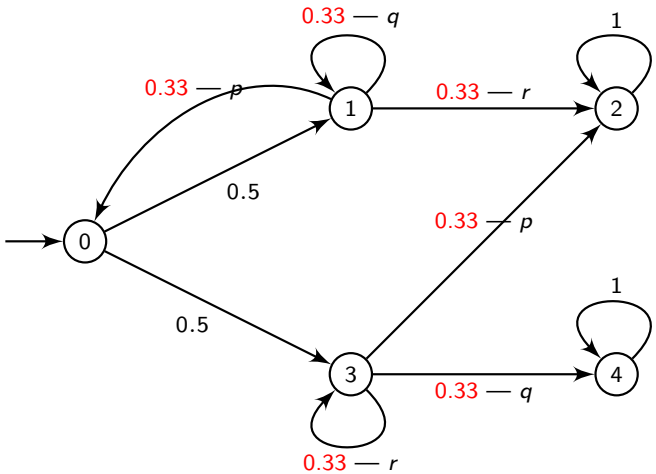
- How to run simulations?

Intuition for pMCs



- How to run simulations? Use a *normalization function* f (uniform?) $\rightarrow \mathcal{M}^f$

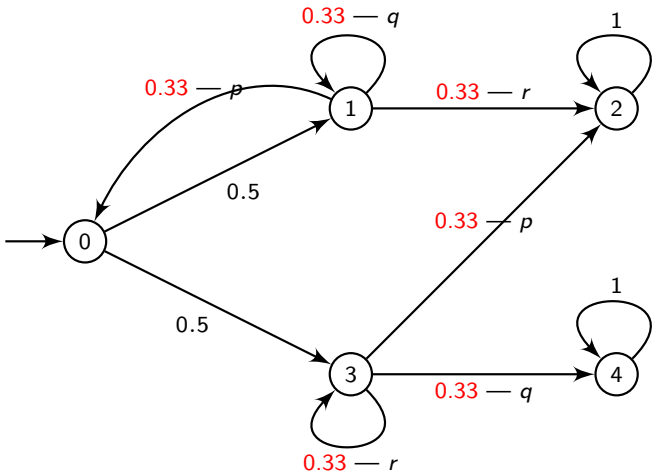
Intuition for pMCs



$$\rho_1 = 0 \cdot 1 \cdot 1 \cdot 2 \cdot 2 \cdot 2$$
$$\rho_2 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 3 \cdot 4$$
$$\rho_3 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$
$$\rho_4 = 0 \cdot 1 \cdot 0 \cdot 1 \cdot 1 \cdot 0$$
$$\rho_5 = 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 4$$
$$\rho_6 = 0 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4$$
$$\rho_7 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2$$
$$\rho_8 = 0 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$

- How to run simulations? Use a *normalization function* f (uniform?) $\rightarrow \mathcal{M}^f$

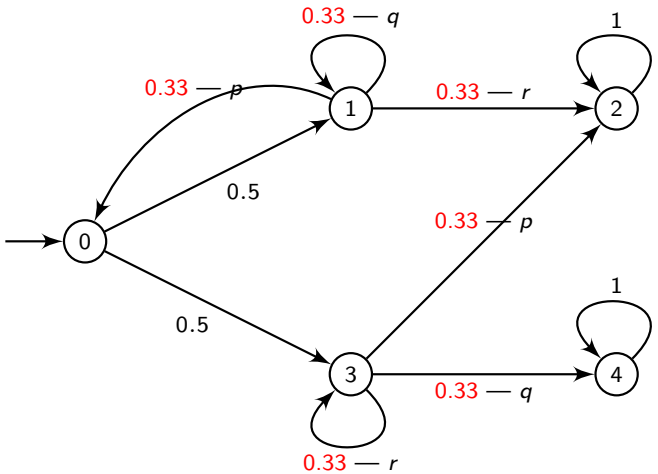
Intuition for pMCs



$$\rho_1 = 0 \cdot 1 \cdot 1 \cdot 2 \cdot 2 \cdot 2$$
$$\rho_2 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 3 \cdot 4$$
$$\rho_3 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$
$$\rho_4 = 0 \cdot 1 \cdot 0 \cdot 1 \cdot 1 \cdot 0$$
$$\rho_5 = 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 4$$
$$\rho_6 = 0 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4$$
$$\rho_7 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2$$
$$\rho_8 = 0 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$

- How to run simulations? Use a *normalization function* f (uniform?) $\rightarrow \mathcal{M}^f$
- $R(\rho_i) = \mathbb{P}_{\mathcal{M}}(\rho)$ if ρ_i reaches 4, 0 otherwise

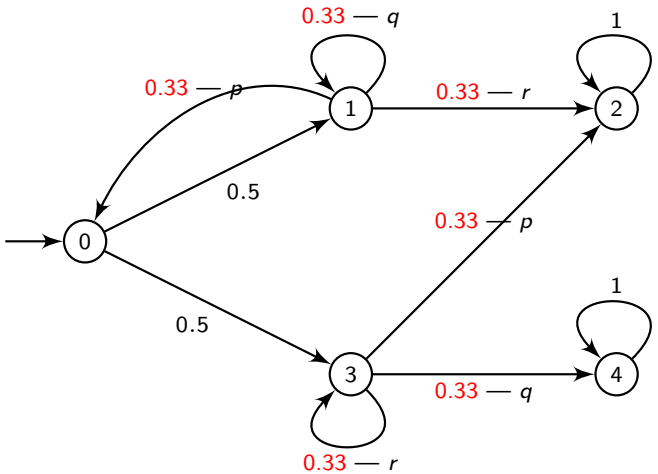
Intuition for pMCs



$$
\begin{aligned}
\rho_1 &= 0 \cdot 1 \cdot 1 \cdot 2 \cdot 2 \cdot 2 & R(\rho_1) &= 0 \\
\rho_2 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 3 \cdot 4 & R(\rho_2) &= 0.25pqr \\
\rho_3 &= 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & R(\rho_3) &= 0 \\
\rho_4 &= 0 \cdot 1 \cdot 0 \cdot 1 \cdot 1 \cdot 0 & R(\rho_4) &= 0 \\
\rho_5 &= 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 4 & R(\rho_5) &= 0.5q \\
\rho_6 &= 0 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4 & R(\rho_6) &= 0.5qr^2 \\
\rho_7 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2 & R(\rho_7) &= 0 \\
\rho_8 &= 0 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & R(\rho_8) &= 0
\end{aligned}
$$

- How to run simulations? Use a *normalization function* f (uniform?) $\rightarrow \mathcal{M}^f$
- $R(\rho_i) = \mathbb{P}_{\mathcal{M}}(\rho)$ if ρ_i reaches 4, 0 otherwise

Intuition for pMCs



$$
\begin{aligned}
\rho_1 &= 0 \cdot 1 \cdot 1 \cdot 2 \cdot 2 \cdot 2 & R(\rho_1) &= 0 \\
\rho_2 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 3 \cdot 4 & R(\rho_2) &= 0.25pqr \\
\rho_3 &= 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & R(\rho_3) &= 0 \\
\rho_4 &= 0 \cdot 1 \cdot 0 \cdot 1 \cdot 1 \cdot 0 & R(\rho_4) &= 0 \\
\rho_5 &= 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 4 & R(\rho_5) &= 0.5q \\
\rho_6 &= 0 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4 & R(\rho_6) &= 0.5qr^2 \\
\rho_7 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2 & R(\rho_7) &= 0 \\
\rho_8 &= 0 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & R(\rho_8) &= 0
\end{aligned}
$$

- How to run simulations? Use a *normalization function* f (uniform?) $\rightarrow \mathcal{M}^f$
- $R(\rho_i) = \mathbb{P}_{\mathcal{M}}(\rho)$ if ρ_i reaches 4, 0 otherwise
- $\mathbb{E}^I_{\mathcal{M}}(R)$??

Results

Let $r'(\rho) = \frac{R(\rho)}{P_{\mathcal{M}^f}(\rho)} r(\rho)$. Due to the central limit theorem:

- $\mathbb{E}^I_{\mathcal{M}}(r')(v) = \mathbb{E}^I_{\mathcal{M}^v}(r)$ for all valid parameter valuation v
- Condition: Under v, $\mathcal{M}$ must conserve the same structure as under f

Results

Let $r'(\rho) = \frac{R(\rho)}{P_{\mathcal{M}^f}(\rho)} r(\rho)$. Due to the central limit theorem:

- $\mathbb{E}^I_{\mathcal{M}}(r')(v) = \mathbb{E}^I_{\mathcal{M}^v}(r)$ for all valid parameter valuation v
- Condition: Under v, $\mathcal{M}$ must conserve the same structure as under f

- Moreover, the confidence interval can be expressed as a polynomial function of the parameters. For n large enough and an error rate of 5%, its size is $3.92\widehat{\sigma}/\sqrt{n}$ where

$$\widehat{\sigma^2} = \frac{1}{(n-1)} \sum_{i=1}^{n} (r'(\rho_i))^2 - \frac{(\sum_{i=1}^{n} r'(\rho_i))^2}{n(n-1)}.$$

Results

Let $r'(\rho) = \frac{R(\rho)}{P_{\mathcal{M}^f}(\rho)} r(\rho)$. Due to the central limit theorem:

- $\mathbb{E}^I_{\mathcal{M}}(r')(v) = \mathbb{E}^I_{\mathcal{M}^v}(r)$ for all valid parameter valuation v
- Condition: Under v, $\mathcal{M}$ must conserve the same structure as under f

- Moreover, the confidence interval can be expressed as a polynomial function of the parameters. For n large enough and an error rate of 5%, its size is $3.92\widehat{\sigma}/\sqrt{n}$ where

$$\widehat{\sigma^2} = \frac{1}{(n-1)} \sum_{i=1}^{n} (r'(\rho_i))^2 - \frac{(\sum_{i=1}^{n} r'(\rho_i))^2}{n(n-1)}.$$

- Here, $\mathbb{E}^5_{\mathcal{M}}(r') \sim 3.48pqr + 0.38q + 3.47qr^2$.

Results

Let $r'(\rho) = \frac{R(\rho)}{P_{\mathcal{M}^f}(\rho)} r(\rho)$. Due to the central limit theorem:

- $\mathbb{E}^I_{\mathcal{M}}(r')(v) = \mathbb{E}^I_{\mathcal{M}^v}(r)$ for all valid parameter valuation v
- Condition: Under v, $\mathcal{M}$ must conserve the same structure as under f

- Moreover, the confidence interval can be expressed as a polynomial function of the parameters. For n large enough and an error rate of 5%, its size is $3.92\widehat{\sigma}/\sqrt{n}$ where

$$\widehat{\sigma^2} = \frac{1}{(n-1)} \sum_{i=1}^{n} (r'(\rho_i))^2 - \frac{(\sum_{i=1}^{n} r'(\rho_i))^2}{n(n-1)}.$$

- Here, $\mathbb{E}^5_{\mathcal{M}}(r') \sim 3.48pqr + 0.38q + 3.47qr^2$.
- For $v(p) = v(q) = 0.25, v(r) = 0.5$: $\mathbb{E}^5_{\mathcal{M}}(r')(v) \sim 0.42$ (exact: 0.261..)

Application to Example 1

For 1000 runs, we get

$$\mathbb{E}^5_{\mathcal{M}}(r') \sim 0.189 * p * q^2 + 0.405 * p * q * r + 0.252 * p * q + 0.729 * q * r^3 + 0.567 * q * r^2 + 0.54 * q * r + 0.492 * q$$

Application to Example 1

For 1000 runs, we get

$$\mathbb{E}^5_{\mathcal{M}}(r') \sim 0.189 * p * q^2 + 0.405 * p * q * r + 0.252 * p * q + 0.729 * q * r^3$$
$$+ 0.567 * q * r^2 + 0.54 * q * r + 0.492 * q \sim 0.2801$$

Application to Example 1

For 1000 runs, we get

$$\mathbb{E}^5_{\mathcal{M}}(r') \sim 0.189 * p * q^2 + 0.405 * p * q * r + 0.252 * p * q + 0.729 * q * r^3 + 0.567 * q * r^2 + 0.54 * q * r + 0.492 * q \sim 0.2801$$

and the size of the CI is

$$(0.062 * (5.108 * p^2 * q^4 + 10.946 * p^2 * q^2 * r^2 + 2.27 * p^2 * q^2 + 59.108 * q^2 * r^6 + 15.324 * q^2 * r^4 + 4.865 * q^2 * r^2 + 1.478 * q^2 - 1.0 * (0.189 * p * q^2 + 0.405 * p * q * r + 0.252 * p * q + 0.729 * q * r^3 + 0.567 * q * r^2 + 0.54 * q * r + 0.492 * q)^2))^{\frac{1}{2}}$$

Application to Example 1

For 1000 runs, we get

$$\mathbb{E}^5_{\mathcal{M}}(r') \sim 0.189 * p * q^2 + 0.405 * p * q * r + 0.252 * p * q + 0.729 * q * r^3 + 0.567 * q * r^2 + 0.54 * q * r + 0.492 * q \sim 0.2801$$

and the size of the CI is

$$(0.062 * (5.108 * p^2 * q^4 + 10.946 * p^2 * q^2 * r^2 + 2.27 * p^2 * q^2 + 59.108 * q^2 * r^6 + 15.324 * q^2 * r^4 + 4.865 * q^2 * r^2 + 1.478 * q^2 - 1.0 * (0.189 * p * q^2 + 0.405 * p * q * r + 0.252 * p * q + 0.729 * q * r^3 + 0.567 * q * r^2 + 0.54 * q * r + 0.492 * q)^2))^{\frac{1}{2}} \sim 0.0296$$

Outline

Introduction

Parametric Markov Chains and Properties
- Background - Properties
- Parametric Markov Chains

Monte Carlo and pMCs

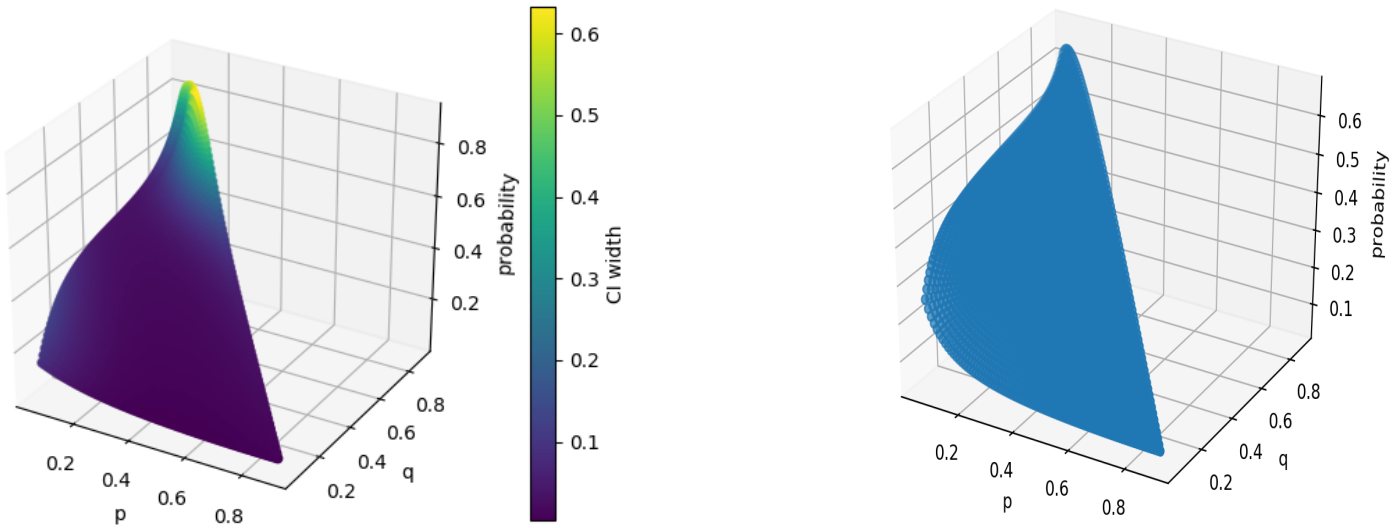
Implementation

Discussion

Implementation

- In Python (not optimized)
- Input: text format similar to prism
- Output: Polynomial, graph...

Exemple 1



(a) With 10 000 simulations and uniform normalization

(b) Theoretical probability

Figure: Results on pMC $\mathcal{M}_1$ ($\mathbb{E}^{100}_{\mathcal{M}}(r')$)

Exemple 2

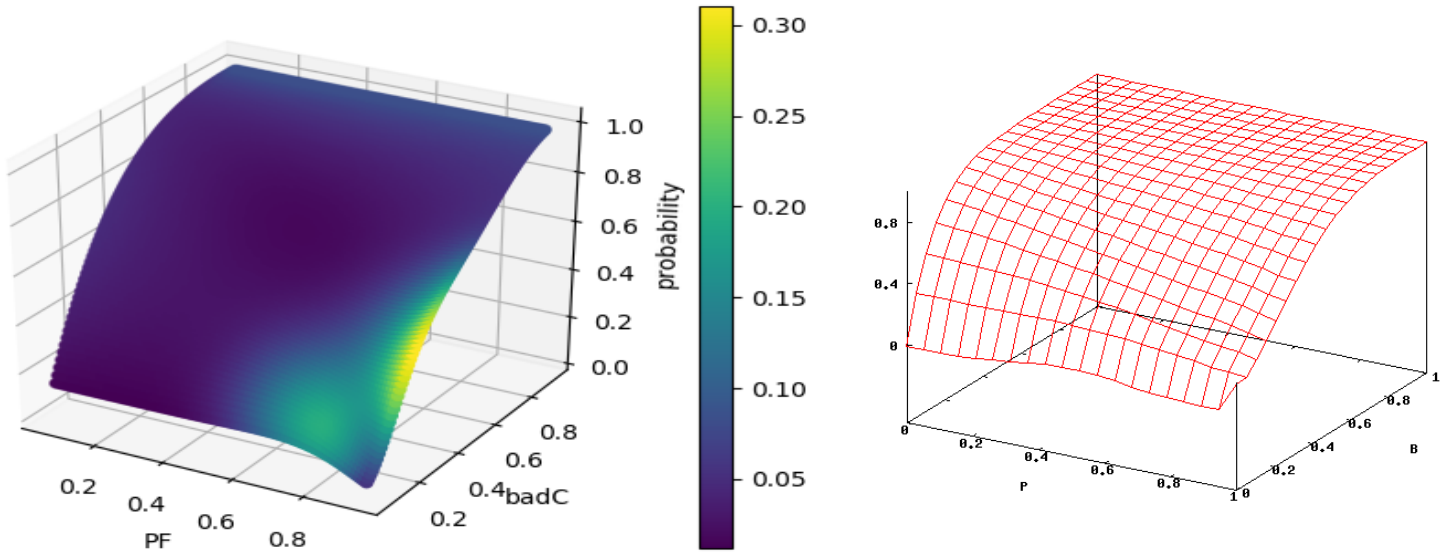


Figure: Results on the Crowds protocol model for our implementation (left) and from the PARAM website (right).

Outline

Introduction

Parametric Markov Chains and Properties
- Background - Properties
- Parametric Markov Chains

Monte Carlo and pMCs

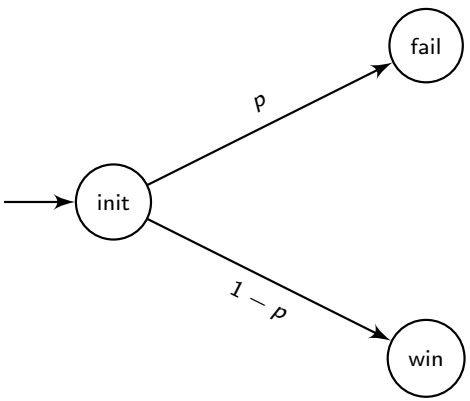
Implementation

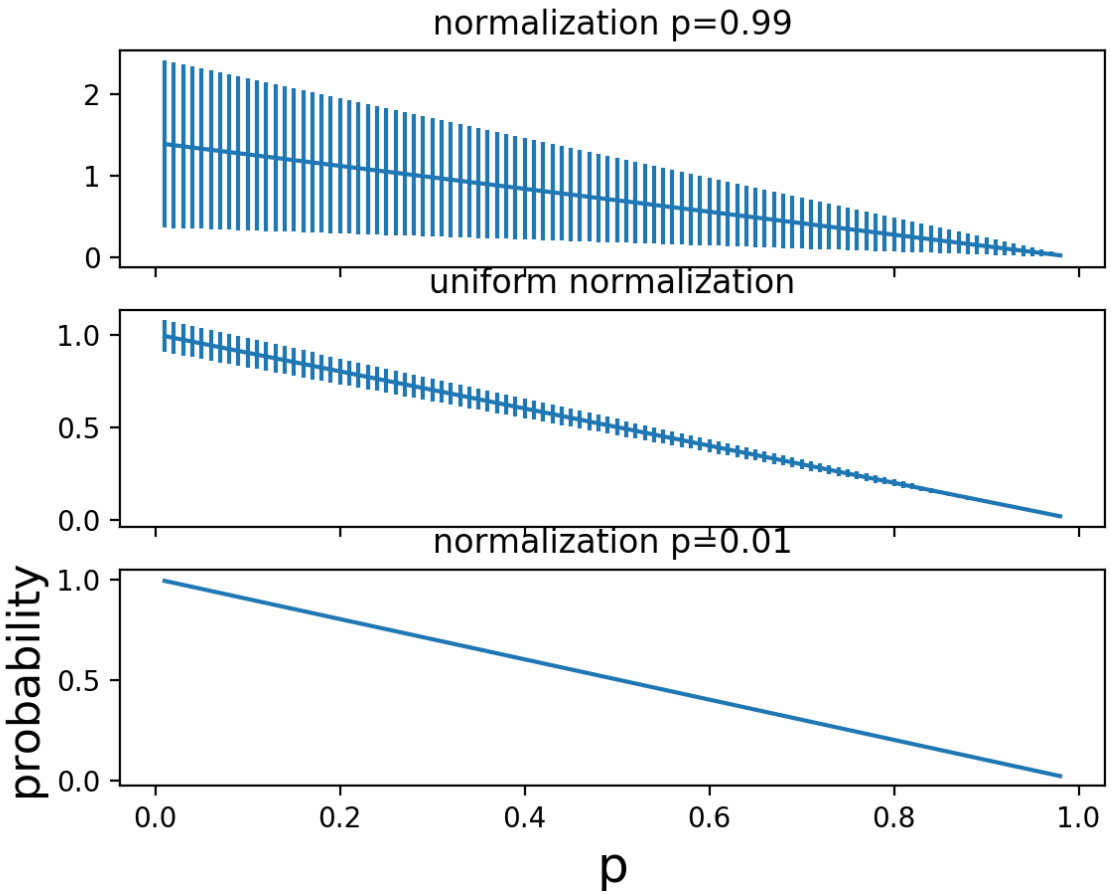
Discussion

Improvements

- Choice of normalization function
  Depending on this choice, the size of the confidence interval may vary drastically
- Structure of the pMC
  If the structure is different under valuation and normalization, the estimated number of runs may change
- Complement property
  Only for probability (not expected value): Evaluating the property and its negation in parallel may improve precision

Impact of normalization function





Impact of the choice of the normalization function f on the size of confidence intervals.

- **Summary**:
  - Parametric Monte Carlo procedure for pMC
  - Polynomial funtions instead of rational;
  - Polynomial parametric confidence interval;
  - Prototype implementation

- **Summary**:
  - Parametric Monte Carlo procedure for pMC
  - Polynomial funtions instead of rational;
  - Polynomial parametric confidence interval;
  - Prototype implementation

- **Future work**:
  - Test and implement improvements
  - Comparison/Integration(?) to existing tools
  - Extension to parametric timed systems (Non trivial)

- **Summary**:
  - Parametric Monte Carlo procedure for pMC
  - Polynomial funtions instead of rational;
  - Polynomial parametric confidence interval;
  - Prototype implementation

- **Future work**:
  - Test and implement improvements
  - Comparison/Integration(?) to existing tools
  - Extension to parametric timed systems (Non trivial)

Thank you for your Attention