Importance Splitting for Statistical Model Checking Rare Properties

Cyrille Jegourel, Axel Legay, Sean Sedwards

Inria Rennes - Bretagne Atlantique

Statistical Model Checking, 2013

Outline

Probabilistic Model Checking

Quantify temporal logical properties of stochastic systems

- Numerical model checking
  - precise
  - exhaustive exploration of state space
  - limited model size
- Statistical model checking
  - statistical model of executions
  - results within confidence bounds
  - trades off tractability with precision

Probabilistic Model Checking

Quantify temporal logical properties of stochastic systems

- Numerical model checking
  - precise
  - exhaustive exploration of state space
  - limited model size
- Statistical model checking
  - statistical model of executions
  - results within confidence bounds
  - trades off tractability with precision

Probabilistic Model Checking

Quantify temporal logical properties of stochastic systems

- Numerical model checking
  - precise
  - exhaustive exploration of state space
  - limited model size
- Statistical model checking
  - statistical model of executions
  - results within confidence bounds
  - trades off tractability with precision

Probabilistic Model Checking

Quantify temporal logical properties of stochastic systems

- Numerical model checking
    - precise
    - exhaustive exploration of state space
    - limited model size
- Statistical model checking
    - statistical model of executions
    - results within confidence bounds
    - trades off tractability with precision

Probabilistic Model Checking

Quantify temporal logical properties of stochastic systems

- Numerical model checking
  - precise
  - exhaustive exploration of state space
  - limited model size
- Statistical model checking
  - statistical model of executions
  - results within confidence bounds
  - trades off tractability with precision

Probabilistic Model Checking

Quantify temporal logical properties of stochastic systems

- Numerical model checking
  - precise
  - exhaustive exploration of state space
  - limited model size
- Statistical model checking
  - statistical model of executions
  - results within confidence bounds
  - trades off tractability with precision

Probabilistic Model Checking

Quantify temporal logical properties of stochastic systems

- Numerical model checking
  - precise
  - exhaustive exploration of state space
  - limited model size
- Statistical model checking
  - statistical model of executions
  - results within confidence bounds
  - trades off tractability with precision

Probabilistic Model Checking

Quantify temporal logical properties of stochastic systems

- Numerical model checking
  - precise
  - exhaustive exploration of state space
  - limited model size
- Statistical model checking
  - statistical model of executions
  - results within confidence bounds
  - trades off tractability with precision

Properties

Properties specified with time bounded temporal logic:

- $\phi = \alpha \mid \phi \vee \phi \mid \phi \wedge \phi \mid \neg\phi \mid \mathbf{X}\phi \mid \mathbf{F}^{\mathbf{t}}\phi \mid \mathbf{G}^{\mathbf{t}}\phi \mid \phi\mathbf{U}^{\mathbf{t}}\phi$
  - **X** is the **next** operator,
  - $\mathbf{F}^{\mathbf{t}}$ is the **bounded eventually** operator,
  - $\mathbf{G}^{\mathbf{t}}$, is the **bounded globally** operator
  - $\mathbf{U}^{\mathbf{t}}$ is the **bounded until** operator.

Objective

- Standard Statistical technique for SMC: Monte Carlo.
- Rare events often cause serious failures but are difficult to simulate.
- Given a stochastic system, design a procedure for estimating a rare property in a reasonable time with SMC.

Monte Carlo Model Checking

- Goal: Given a Markovian system and a property φ, compute the probability γ that a path ω satisfies φ, i.e. $(\gamma = P[\omega \models \varphi])$.
- The behavior of the system with respect to the property can be modeled by a Bernoulli random variable Z.

property indicator function $z \in \{0, 1\}$

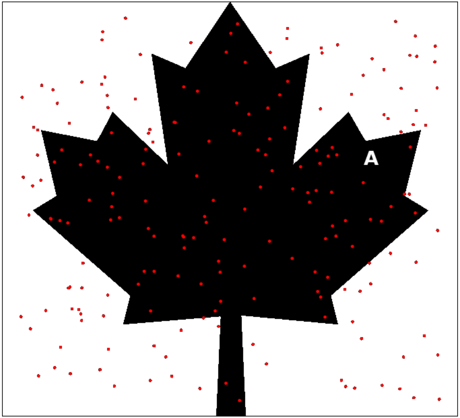
probability measure function

$$\gamma = E_f[Z] = \int_\Omega z(\omega) df$$

$$\tilde{\gamma} = \frac{1}{N} \sum_{i=1}^{N} z(\omega_i)$$

sample traces generated under f

Monte Carlo estimation



$$A = \{\omega \in \Omega \, : \, z(\omega) = 1\} \quad (1)$$

$$\tilde{\gamma} = \frac{1}{N} \sum_{i=1}^{n} z(\omega_i) \quad (2)$$

Absolute error = half the size of the confidence interval

$$AE \propto \frac{\sqrt{\gamma(1-\gamma)}}{\sqrt{N}} \quad (3)$$

Main Problems with Rare Events

- Occur with small probability (e.g. $< 10^{-6}$)
  - appear rarely in stochastic simulations
  - need very large number of trials to see single example
  - without seeing, cannot quantify how low the probability
- The absolute error is not useful: $(\gamma \pm \epsilon)$ is "large" if $\epsilon \gg \gamma$
  - Bounds (e.g. Chernoff) not useful when γ small
  - Unbounded relative error:

$$RE = \frac{\sqrt{Var(Z)}}{\sqrt{N}E[Z]} = \frac{\sqrt{\gamma(1-\gamma)}}{\sqrt{N\gamma}} \underset{\gamma \to 0}{\approx} = \frac{1}{\sqrt{N\gamma}} \tag{4}$$

Importance Sampling

Monte Carlo

- $\gamma = \int_\Omega z(\omega) df$
- $\tilde{\gamma}_{MC} = \frac{1}{N} \sum_{i=1}^{n} z(\omega_i)$
- Traces generated under f

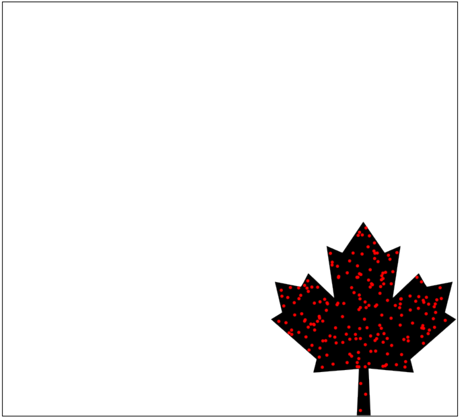
Importance Sampling

- $\gamma = \int_\Omega z(\omega) \frac{f(\omega)}{f'(\omega)} df'$
- $\tilde{\gamma}_{IS} = \frac{1}{N} \sum_{i=1}^{n} z(\omega_i) \frac{f(\omega_i)}{f'(\omega_i)}$
- Traces generated under f'

Tilted simulation

- $$\tilde{\gamma}_{IS} = \frac{1}{N} \sum_{i=1}^{n} z(\omega_i) \frac{f(\omega_i)}{f'(\omega_i)}$$
- Traces generated under f' (Importance Sampling distribution)

Optimal Importance Sampling



There exists an optimal distribution: *f* conditioned on the rare event:

$$f^{opt} = \frac{zf}{\gamma} \quad (5)$$

Limitations of Importance Sampling

- Quantifying the performance of apparently "good" distributions is an open problem.
- Problem of accuracy with long simulations: variance of the estimators increases.
- Implies the need of an alternative technique: **Importance Splitting**.

Basics of Importance Splitting

Let A be a rare event and $(A_k)_{0 \leq k \leq n}$ be a sequence of nested events:

$$A_0 \supset A_1 \supset \ldots \supset A_n = A \quad (6)$$

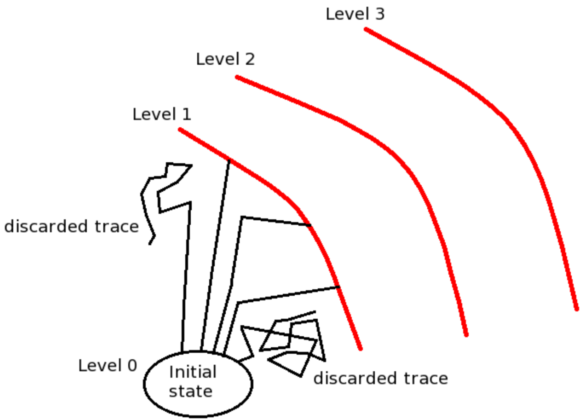
By Bayes formula,

$$\gamma \stackrel{def}{=} P(A) = P(A_0)P(A_1 \mid A_0)P(A_2 \mid A_1)\ldots P(A_n \mid A_{n-1}) \quad (7)$$

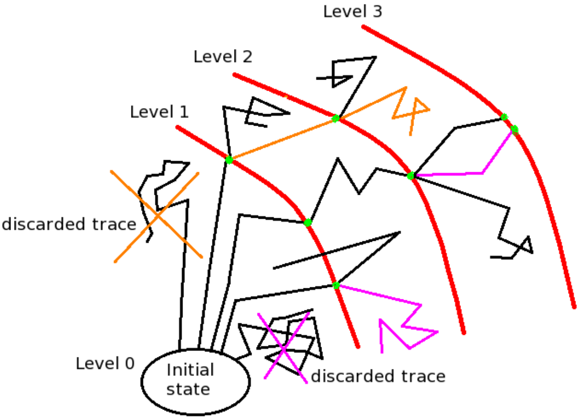
implying that every conditionnal probability is less rare:

$$\forall k, \; P(A_k \mid A_{k-1}) = \gamma_k \geq \gamma \quad (8)$$

Example: Reaching Level 3 in finite time



Example: Reaching Level 3 in finite time



P(reaching Level 3)=3/5*2/5*2/5

Importance Splitting in a Model Checking Context

Idea: given a rare property φ, define a set of levels based on a sequence of temporal properties such that:

$$(\varphi_k)_{0 \leq k \leq n} \ : \ \varphi_0 \Leftarrow \varphi_1 \Leftarrow \ldots \Leftarrow \varphi_n = \varphi \tag{9}$$

Thus,

$$\gamma = P(\omega \models \varphi_0) \prod_{k=1}^{n} P(\omega \models \varphi_k \mid \omega \models \varphi_{k-1}) \tag{10}$$

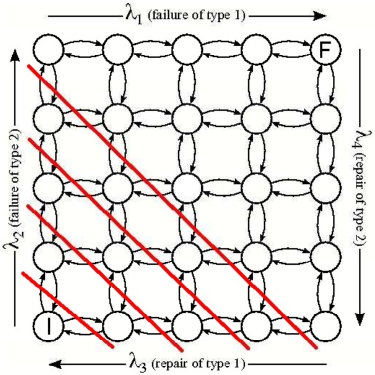
Simple Decomposition

- When $\varphi = \bigwedge_{j=1}^{n} \psi_j$, a decomposition into nested properties is: $\varphi_i = \bigwedge_{i=1}^{j} \psi_j \, , \forall i \in \{1, ..., n\}$ with $\varphi_0 = \top$
- Possibility to choose an arbitrary order of sub-formulae:
- Ex: Given $\varphi \; = \; a \wedge b \wedge c$,
  - $\varphi_3 \; = \; a \wedge b \wedge c$, $\varphi_2 \; = \; a \wedge b$, $\varphi_1 \; = \; c$
  - $\varphi_3 \; = \; a \wedge b \wedge c$, $\varphi_2 \; = \; b \wedge c$, $\varphi_1 \; = \; a$
  - Both decompositions are valid.

Natural Decomposition

- Many rare events are defined with a natural notion of level, when some quantity of the system reaches a particular value.
- In Computational systems: might refer to a loop counter, a number of software objects, etc...
- In physical systems: might refer to a temperature, a distance, a number of molecules...
- Natural levels defined by nested atomic properties: $\varphi_i = (x > x_i)$ with x a state variable and $\omega \models \varphi_n \Leftrightarrow x \geq x_n$.

Decomposition of Temporal Operators



- Repair model
- $\varphi = \text{init} \wedge \mathbf{X}\left(\neg\text{init}\,\mathbf{U}^{\mathbf{t}}\,\text{fail}\right)$ with init $\Leftrightarrow (x = 0)$ and fail $\Leftrightarrow (x = n)$.
- Decomposition: $\forall k \in \{1, ..., n\}$, $\varphi_k =$ init $\wedge\ \mathbf{X}\left(\neg\text{init}\,\mathbf{U}^{\mathbf{t}}\,(x \geq k)\right)$

Fluctuation Analysis

- $(1-\alpha)$ Confidence Interval based on the relative variance σ: $\left[\tilde{\gamma}\left(\frac{1}{1+\frac{z_\alpha \sigma}{\sqrt{N}}}\right) ; \tilde{\gamma}\left(\frac{1}{1-\frac{z_\alpha \sigma}{\sqrt{N}}}\right)\right]$ with $\sigma^2 \geq \sum_{k=1}^{m} \frac{1-\gamma_k}{\gamma_k}$
- Inequality arises because the independence of initial states diminishes with increasing levels.
- Several possibilities minimise this dependence effect.

Idealized Version

- Relative variance of the estimator: $\sigma^2 = \sum_{k=1}^{m} \frac{1-\gamma_k}{\gamma_k}$
- For a fixed number of levels, this variance is minimal if all the conditional probabilities are equal ($\exists p \in]0;1[\ s.t. \forall k,\ \gamma_k = p$)
- Problem: levels might be too coarse.

Score functions

- Score function goal: increase the resolution of levels.
- Level-based score functions: Mapping from logical properties to $\mathbb{R}$ which give information on the number of satisfied sub-formulae.

$$S(\omega) = \max_k \{k \mid \omega \models \varphi_k\} \tag{11}$$

- General score functions: Mapping from sets of paths to $\mathbb{R}$ s.t. higher scores assigned to paths that satisfy the overall property.

$$S(\omega) = \max_{\omega_{\leq j}} P\left(\varphi \mid \omega_{\leq j}\right) \tag{12}$$

Use of heuristics

- Level-based score functions correlate logic to score.
- General score functions requires:
  - higher scores assigned to paths that satisfy the overall property.
  - $P(\phi \mid \omega') \geq P(\phi \mid \omega) \Rightarrow S(\omega') \geq S(\omega)$
- In some case, the shortest paths satisfying a rare property are the most likely => possibility to exploit the length of a path to improve a score function based on coarse logical levels.

Dining Philosophers Problem

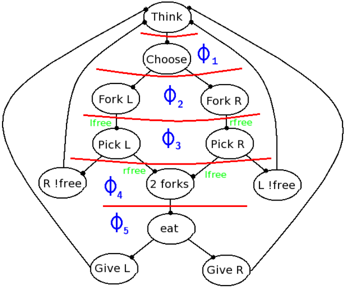


Figure: Automata modelling a philosopher

- 150 philosophers
- more than 2^{144} states
- property of interest: $\varphi = \mathbf{F}^{30}$ (Phil i eat)

Experimental Results given by an adaptive algorithm

- based on A. Guyader, F. Cérou, T. Furon, Del Moral work (2007)
- predefined $\gamma_k \approx 0.85$,
- The algorithm finds adaptively around 96 iterations,
- gain of time: between 800 and 5000 times faster than Monte Carlo

Experimental Results given by an adaptive algorithm

	Importance Splitting					MC
number of experiments	100	100	100	100	1	1
nb of paths	50	100	200	500	1000	10 million
time (seconds)	0,66	1,73	4,08	11,64	24,17	>5 hours
estimate (average)	1,42	1,52	1,59	1,58	1,53	1,2
standard deviation	1,63	1,02	0,87	0,5	-	0,35
Relative Error (average)	0,72	0,45	0,31	0,19	0,13	0,29
95%-CI lower bound	0,82	1,04	1,22	1,33	1,35	0,52
95%-CI upper bound	5,08	2,76	2,29	1,95	1,76	1,88

Results are times 10^6   *6% wrong

Summary

- Rare events are often critical.
- Importance splitting is a rare event technique that admits a confidence bound and is applicable to many systems.
- We have defined how importance splitting may be combined with temporal logic to apply SMC to rare events.
- Score functions generalise the notion of levels required by importance splitting
- Heuristics may be used to increase the granularity of score functions to improve performance.

Ongoing work

- Improved confidence bounds
- Integration in Statistical Model Checker PLASMA
- Case studies: false alarm of derailment, collision of particles?