Statistical Model Checking

Nhat-Huy Phung

University of Constance

2021

Model checking

Definition

Model checking is an automated technique that, given a finite-state model of a system and a formal property,systematically checks whether this property holds for (a given state in) that model

Since we are interested in probabilistic model checking, our models encompasses probabilistic behaviours.

Examples (Probabilistic models)

- DTMC
- CTMC
- MDP
- etc.

Properties

Properties are specified by temporal logics

Examples

- PCTL
- CSL
- LTL
- etc.

Complexity

In general, model checking is undecidable. The verification of a model against a temporal logic formula is of *polynomial time* to the number of states on the model.

State explosion

The number of states needed to model the system increases exponentially to the state of the system.

State explosion is widely surveyed in the research of model checking. [2]

Examples (Concurrent system)

A concurrent system consists of many interacting agents. A global state is the tuple of states of all agents and communication channels, thus the number of possible global states increases exponentially to the number of agents and communication channels. In case of asynchronous channels, the number of state may increases even faster.

Statistical model checking

Statistical Model Checking (SMC) is a formal verification technique that combines simulation and statistical methods for the analysis of stochastic systems. [1] Statistical Model Checking verifies a system S property ϕ over a finite set of *traces*, acquired through simulating the system of concern S.

Advantages

- **Scalability**: avoid state space explosion issues.

1

Statistical model checking

Given a model M of a system S and a temporal property ϕ. Let $p := Pr\{M \models \phi\}$ be the probability that the model M satisfies the property ϕ. [1]

Verification

- **Quantitative**: Estimate p
- **Qualitative**: Given a threshold θ, test the hypothesis $H :=$

1

Statistical model checking

Quantitative

Estimate $p := Pr\{M \models \phi\}$ wrt. precision δ and confidence level α

The estimation is described in detail in [1]. We calculate $\hat{p}$ as an estimation of p such that

$$Pr\{|p - \hat{p}| < \delta\} = 1 - \alpha$$

$\hat{p}$ can be estimated using different bounds, such as Chernoff-Hoeffding bound [3], Okamoto bound [6] or Massart bound [5]

Statistical model checking

Quantitative

Let $p := Pr\{M \models \phi\}$ and a threshold $\theta \in [0, 1]$. Compare p and θ

The general approach is to do hypothesis test [8] given a confidential level α

- $H_0 : p >= \theta$
- $H_1 : p < \theta$

More details can be found at [7]

Case study with PRISM

PRISM [4] is a model checking tool that support discrete event simulation and statistical model checking. For an example of how to use PRISM for statistical model checking please follow this link.

References I

[1] Gul Agha and Karl Palmskog. "A survey of statistical model checking". In: *ACM Transactions on Modeling and Computer Simulation (TOMACS)* 28.1 (2018), pp. 1–39.

[2] Edmund M Clarke et al. "Model checking and the state explosion problem". In: *LASER Summer School on Software Engineering*. Springer. 2011, pp. 1–30.

[3] W Hoeffding. "Probability inequalities for sums of bounded random variables. American Statistical Association „Journal, 13–30. Katz, S.(1987). Estimation of probabilities from sparse data for the language model component of a speech recognizer". In: *IEEE Transactions on Acoustic, Speech and Signal Processing* 35 (1963), pp. 400–401.

References II

[4] Marta Kwiatkowska, Gethin Norman, and David Parker. "PRISM: Probabilistic symbolic model checker". In: *International Conference on Modelling Techniques and Tools for Computer Performance Evaluation*. Springer. 2002, pp. 200–204.

[5] Pascal Massart. "The tight constant in the Dvoretzky-Kiefer-Wolfowitz inequality". In: *The annals of Probability* (1990), pp. 1269–1283.

[6] Masashi Okamoto. "Some inequalities relating to the partial sum of binomial probabilities". In: *Annals of the institute of Statistical Mathematics* 10.1 (1959), pp. 29–35.

[7] Abraham Wald. "Sequential tests of statistical hypotheses". In: *The annals of mathematical statistics* 16.2 (1945), pp. 117–186.

References III

[8] Hakan L Younes. *Verification and planning for stochastic processes with asynchronous events*. Tech. rep. CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE, 2005.