Information and Computation 259 (2018) 142–160

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Abstract model repair for probabilistic systems

G. Chatzieleftheriou, P. Katsaros *

Department of Informatics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

ARTICLE INFO

Article history:
Received 19 June 2017
Received in revised form 28 June 2017
Available online 19 February 2018

Keywords:
Model repair
Abstraction
Probabilistic models

ABSTRACT

Given a Discrete Time Markov Chain M and a probabilistic temporal logic formula φ, where M violates φ, the problem of *Model Repair* is to obtain a new model M', such that M' satisfies φ. Additionally, the changes made to M in order to obtain M' should be minimum with respect to all such M'. The state explosion problem makes the repair of large probabilistic systems almost infeasible. In this paper, we use the abstraction of Discrete Time Markov Chains in order to speed-up the process of model repair for temporal logic reachability properties. We present a framework based on abstraction and refinement, which reduces the state space of the probabilistic system to repair at the price of obtaining an approximate solution. A metric space is defined over the set of DTMCs, in order to measure the differences between the initial and the repaired models. For the repair, we introduce an algorithm and we discuss its important properties, such as soundness and complexity. As a proof of concept, we provide experimental results for probabilistic systems with diverse structures of state spaces, including the well-known Craps game, the IPv4 Zeroconf protocol, a message authentication protocol and the gambler's ruin model.

1. Introduction

Given a model M and a property φ, the problem of *model checking* is to find if the property is satisfied by the model [1]. Today, a number of mature model checking algorithms exist, for probabilistic and non probabilistic models. If the property is not satisfied, some algorithms return a cause for the refutation of the property known as counterexample.

The problem of *model repair* is an extension of the model checking problem for the case where the property is refuted. More specifically, the aim of model repair is to find the minimal changes to the model, such that the property φ, which has been violated in the original model, will be satisfied. The model repair problem has been examined in the probabilistic setting for the first time in [2].

The *state space explosion* problem is inherent in model checking and makes its application infeasible to large models. This problem is also present in existing probabilistic model repair techniques, which aim to directly change the model under repair. For example, in [2] the authors transform the repair problem to a non-linear optimization problem using parametric model checking, and the time needed for computing a repaired model increases rapidly with respect to the size of the state space.

The main method for fighting the state space explosion in model checking is the use of *abstraction* techniques [3–5]. Such an approach has also been used in the non-probabilistic setting, for the repair of models with large state spaces [6,7]. Inspired from the use of abstraction in model checking and non-probabilistic model repair, we present here a framework

* Corresponding author.
E-mail addresses: gchatzie@csd.auth.gr (G. Chatzieleftheriou), katsaros@csd.auth.gr (P. Katsaros).

https://doi.org/10.1016/j.ic.2018.02.019
0890-5401/

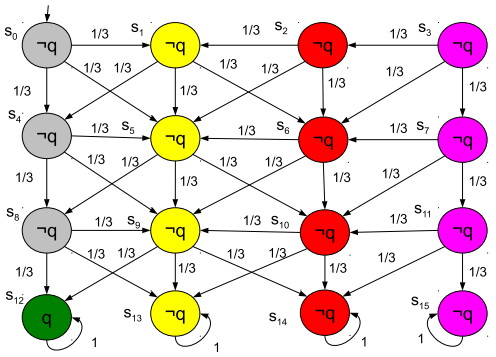

Fig. 1. A Discrete Time Markov Chain. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

based on abstraction and refinement for the repair of probabilistic models. More specifically, we focus on Discrete Time Markov Chains (DTMCs) and their repair with respect to temporal logic reachability properties.

The main contributions of our paper are:

- We introduce a framework for the repair of a DTMC with respect to a (not-nested) Probabilistic Computation Tree Logic (PCTL) reachability formula, using an Abstract Discrete Time Markov Chain (ADTMC) for the given DTMC and the 3-valued semantics of PCTL over ADTMCs. Based on a strong preservation theorem, if a PCTL property is refuted or satisfied in the ADTMC (abstract model), then the same also holds for the concrete DTMC [8].
- A metric space is defined over the DTMCs with the same state labeling, in order to measure the distance of repaired DTMCs from the original DTMC.
- We introduce a Probabilistic Abstract Model Repair (PAMR) algorithm that transforms the DTMC repair problem to a non-linear minimization problem for the state space of the abstract model, instead of the concrete one. If a solution is found, the repaired DTMC is returned, which corresponds to an approximate (not the optimal) solution; otherwise, the algorithm is iteratively applied to refined ADTMCs until a solution is found. The refinement can be potentially adapted by the analyst, for implementing alternative repair strategies.
- We analyze the PAMR computational gains and more specifically the achieved reduction in the expensive non-linear optimization and linear equation solving problems, which are involved respectively in the concrete model repair and model checking techniques.
- As a proof of concept, we provide experimental results for the DTMCs of extended versions of the Craps game, the IPv4 Zeroconf protocol, a message authentication protocol and the gambler's ruin model.

The paper is organized as follows. In Section 2, the notion of DTMC is introduced which is the formalism for the concrete model in our framework. Section 3 discusses how an ADTMC can serve as an abstraction of a DTMC and how a reachability PCTL formula can be verified in an ADTMC. In Section 4, the model repair problem for probabilistic systems is formulated together with a metric space for DTMCs. We present the abstract model repair process for probabilistic systems in Section 5 together with the basic model repair operations. The PAMR algorithm is described in Section 6. The algorithm's steps are illustrated using an application in Section 7, where we also elaborate on the method's efficiency gains, its cost in terms of the solution's optimality and its flexibility perspectives. In Section 8, we present the experimental results for extended models with progressively larger state spaces of the Craps game, the IPv4 Zeroconf protocol, a message authentication protocol and the gambler's ruin model. The related work is reviewed in Section 9 and we conclude with Section 10, where we also discuss the future work.

2. Reachability PCTL properties over DTMCs

Let AP be a set of *atomic propositions* and the set Lit of *literals* given as:

$$Lit = AP \cup \{\neg p : p \in AP\}$$

Definition 1. A (labeled) *Discrete Time Markov Chain* (DTMC) is a 4-tuple $M = (S, s_{init}, P, L)$, where:

1. S is a finite set of states;
2. $s_{init} \in S$ is the initial state;
3. $P : S \times S \to [0, 1]$ is a transition probability function with $\sum_{s' \in S} P(s, s') = 1$ for all $s \in S$;
4. $L : S \to 2^{Lit}$ is a state *labeling function* such that $\forall s \in S$, $\forall p \in AP$, $p \in L(s) \Leftrightarrow \neg p \notin L(s)$.

A DTMC is a transition system with labeled states and probabilities assigned to its transitions.