Abstract Model Repair

George Chatzieleftheriou, PhD Student

Dept. Of Informatics, Aristotle University of Thessaloniki, Greece

Supervisor: Prof. Panagiotis Katsaros

• Overview

Given a Kripke structure M and a CTL formula ϕ, where M does not satisfy ϕ, the problem of Model Repair is to obtain a new model M′ such that M′ satisfies ϕ. Moreover, the changes made to M to derive M′ should be minimal with respect to all such M′. As in model checking, state explosion can make it virtually impossible to carry out model repair on models with infinite or even large state spaces. We present a framework for model repair, that uses abstraction refinement to tackle the state explosion. Our framework aims to repair Kripke Structure models based on a Kripke Modal Transition System (KMTS) and a 3-valued semantics for CTL. We introduce an abstract-model-repair algorithm for which we prove soundness and semi-completeness, and we study its complexity class. Moreover, a prototype implementation is presented to illustrate the practical utility of abstract-model-repair on an Automatic Door Opener system model and a model of the Andrew File System 1 protocol.

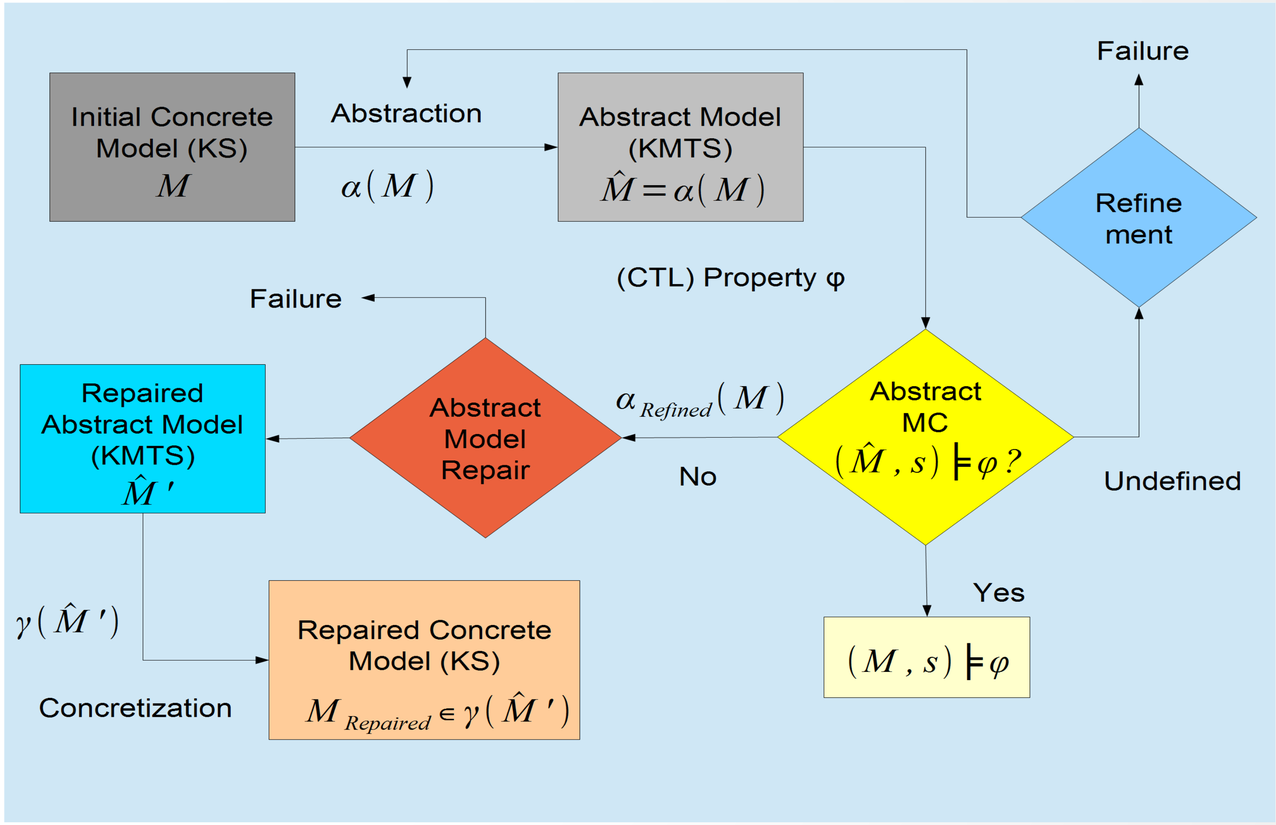
• Motivation

We are motivated by the success of abstraction-based model checking to create a model repair framework with the use of abstraction and refinement to tackle the state explosion problem which deters repaired solutions to be produced by the existing concrete model based approaches.

• The Algorithm

Our AMR algorithm is a recursive, syntax-directed algorithm, which gets as input a KMTS M and a CTL property ϕ and returns a repaired KMTS M′. AMR algorithm is sound for full CTL, complete for a major fragment of CTL and is of polynomial time with respect to the size of the abstract model.

• The AMR framework



• The distance metric

To quantify the structural differences for the possible repaired solutions in order to taking into account the minimality of changes criterion in Model Repair, we define a distance metric for KSs which counts the number of differences in state spaces, the number of differences in their transition relation and the number of common states with altered labeling.

• Experimental Results

We have implemented a prototype and compared our method with a concrete model repair approach for the Andrew File System 1 protocol and some extentions of it.

Models	Concrete Repair (Time in sec.)	AMR (Time in sec.)	Speed-up (%)
AFS1	17.4	0.14	124
AFS1-EXT1	24.9	0.14	178
AFS1-EXT2	35.0	0.14	250
AFS1-EXT3	117.0	0.14	836

• Ongoing Work

We extended our idea to the Model Repair for Probablistic Systems (DTMC M and a reachability PCTL formula ϕ). We have created a framework based on abstraction and refinement which reduces the model repair problem to a repair problem for a model with a smaller state space. We introduce an algorithm and we discuss its important properties such as soundness and complexity. As a proof of concept, we have created a prototype implementation of our method and applied it to extended versions of a probabilistic system of the well-known Craps game. .

• References

1. George Chatzieleftheriou, Borzoo Bonakdarpoor, Scott A. Smolka, and Panagiotis Katsaros. 2012. Abstract model repair. In Proceedings of the 4th international conference on NASA Formal Methods (NFM'12), Alwyn E. Goodloe and Suzette Person (Eds.). Springer-Verlag, Berlin, Heidelberg, 341-355
2. George Chatzieleftheriou, Borzoo Bonakdarpour, Panagiotis Katsaros, Scott A.Smolka, Abstract Model Repair, Logical Methods in Computer Science, Volume 11, Issue 3. doi:10.2168/LMCS-11(3:11)2015.
3. Abstract Model Repair for Probabilistic Systems, (under review)