Model Repair in Systems Design

Panagiotis Katsaros – Aristotle University of Thessaloniki (GR)

Model-Based Design for Space Systems @ AUTh

Design Validation Studies Using COMPASS

- □ Bozzano, Cimatti, Katoen, Katsaros, Mokos, Nguyen, Noll, Postmac, Roveri. ***Spacecraft early design validation using formal methods***, Reliability Engineering and System Safety, 2014
- □ Mandaras, ***Early design validation of the GOES I-M system***, Master Thesis, AUTh, 2015

Ongoing ESA TRP studies

- □ **Catalogue of System & Software Properties** with EPFL RiSD Lab and TAS
  - Requirements catalogue & formalization
  - Ontology-based semantics modeling & reasoning (Prof. Bassiliades)
  - Rigorous architecture based design (Prof. Sifakis)
- □ **Model-Based Schedulability Analysis for Cached & Multicore Processors** (working for CERTH) with Verimag Lab, Cobham Gaisler, Deimos Space

The Model Repair problem

- Extension of model checking used for ***design refinement***:

  Given a system model M and some temporal logic property φ, where M *does not satisfy* φ find a new model M′ such that M' *satisfies* φ and the *changes in M to derive M′ are minimal* with respect to all such M′.
- Variants from the bibliography:
  - with constraints (preserve properties)
  - with controllable states (repair options)

Applications

- Model Repair for incorporating fault tolerance in a distributed algorithm

  Bonakdarpour, Kulkarni, Abujarad. ***Symbolic synthesis of masking fault-tolerant programs***, 2012

- Model Repair for fault recovery in component-based models

  Bonakdarpour, Bozga, Goessler. ***A theory of fault recovery for component-based models***, 2011

- Model Repair for concurrent programs

  Attie, Cherri, Al Bab, Sakr, Saklawi. ***Model and Program Repair via SAT Solving***, 2015

- Model Repair for probabilistic systems

  Bartocci, Grosu, Katsaros, Ramakrishnan, Smolka, ***Model repair for probabilistic systems***, 2011

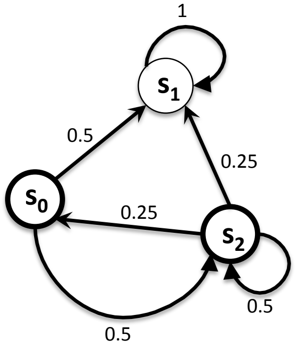
  Pathak, Abraham, Jansen, Tacchella, Katoen. ***A Greedy Approach for the Efficient Repair of Stochastic Models***, 2015

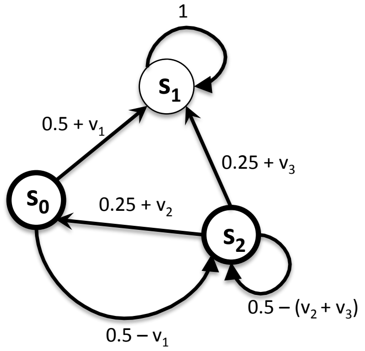
Model Repair solutions for probabilistic systems I

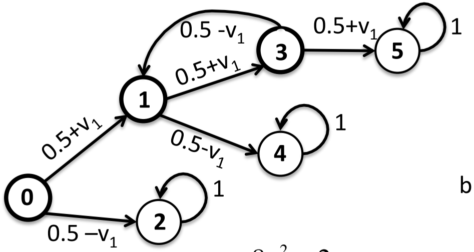
Bartocci, Grosu, Katsaros, Ramakrishnan, Smolka, ***Model repair for probabilistic systems***, TACAS, 2011

For DTMCs and CTMCs,

- using parametric probabilistic model checking ***the problem is reduced to a nonlinear optimization problem*** with a minimal-cost objective function
- solution ***feasibility*** & ***optimality conditions*** are provided
- an implementation of the solution technique is provided

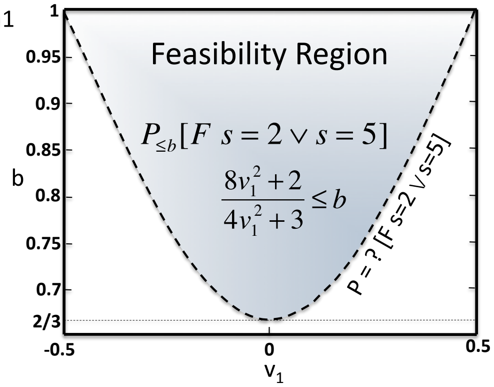






$$P_{\leq 0.3}[F\ s=2 \vee s=5] \Leftrightarrow \frac{8v_1^2+2}{4v_1^2+3} \leq 0.3$$

is infeasible



Model Repair solutions for probabilistic systems II

For MDPs,

Chen, Hahn, Han, Kwiatkowska, Qu, Zhang, ***Model Repair for Markov Decision Processes,*** TASE, 2013

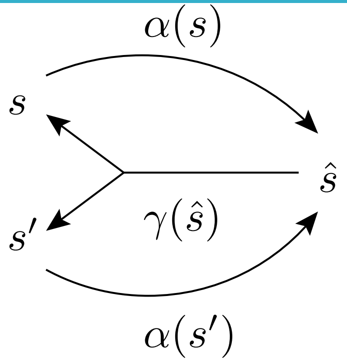
- Region refinement through the parameter space (approximation)
- Sampling-based search through the parameter space

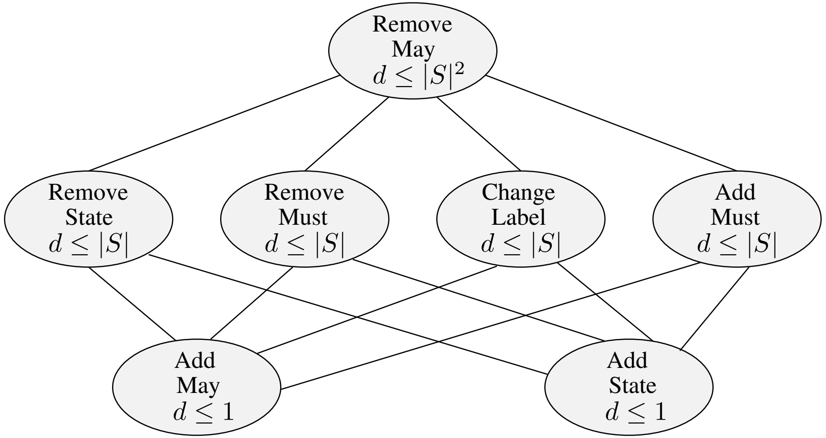
For DTMCs + CTMCs,

Pathak, Abraham, Jansen, Tacchella, Katoen. ***A Greedy Approach for the Efficient Repair of Stochastic Models***, 2015

- From initial parameter assignment, iteratively changes the parameter values by local repair steps

Abstract Model Repair for transition systems I

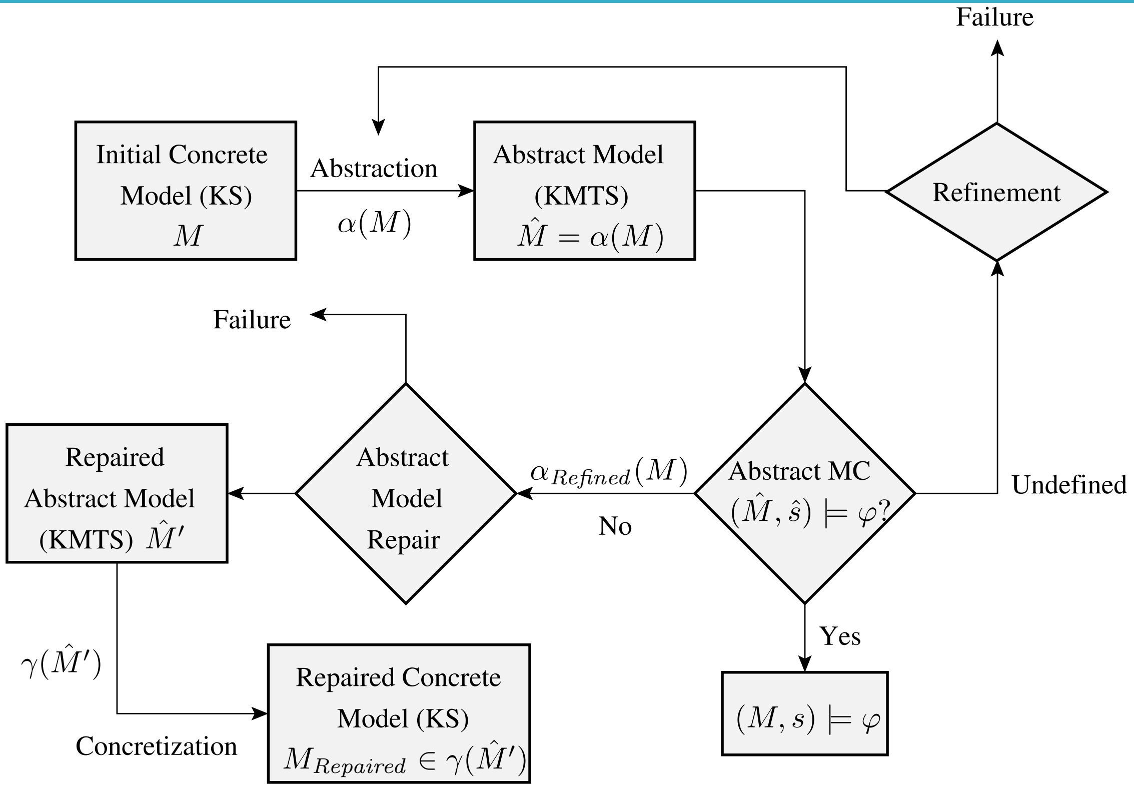




Chatzieleftheriou, Bonakdarpour, Katsaros, Smolka. ***Abstract Model Repair***, NASA Formal Methods 2012 + Logical Methods in Computer Science 2015

- Model Repair CTL properties using **abstraction & refinement** to tackle state space explosion:
  - Concrete model is a Kripke Structure
  - Abstract model is a (Kripke) Modal Transition System
  - A pair of abstraction & concretization functions (α, γ) is defined
- A **metric space over Kripke structures** is defined to quantify their structural differences.
- Partial ordering of basic **abstract repair operations** in terms of the structural changes implied for the concrete model.

Abstract Model Repair for transition systems II


Failure
Initial Concrete Model (KS) M
Abstraction
$\alpha(M)$
Abstract Model (KMTS) $\hat{M} = \alpha(M)$
Refinement
Failure
Repaired Abstract Model (KMTS) $\hat{M}'$
Abstract Model Repair
$\alpha_{Refined}(M)$
No
Abstract MC $(\hat{M}, \hat{s}) \models \varphi?$
Undefined
$\gamma(\hat{M}')$
Concretization
Repaired Concrete Model (KS) $M_{Repaired} \in \gamma(\hat{M}')$
Yes
$(M, s) \models \varphi$

Conclusions

- Model Repair solutions for probabilistic systems
- Abstract Model Repair framework & algorithm
  - proved **sound for the full CTL** and **complete for a subset of CTL** (excluding only the AND operator)
  - complexity: upper bounded by a polynomial expression in the size of the abstract model
  - constraints in model repair undermine completeness
- Towards **Design Repair**
  - better criteria for quantifying changes and minimality (structural differences, only good for abstract repair)
  - define basic repair operations in rigorous system design languages (e.g. SLIM, BIP) and assess their cost
  - introduce architecture specific repair options in the design/verification front-end

THANK YOU!

katsaros@csd.auth.gr