A SAT/SMT-based CEGAR Framework

Á. Hajdu, T. Tóth, A. Vörös, Z. Micskei, I. Majzik

Budapest University of Technology and Economics
Fault Tolerant Systems Research Group
http://inf.mit.bme.hu/en

Overview

Abstraction
Build and check abstract model with a given precision

Refinement
Check counterexample and refine precision if needed

Counterexample-Guided Abstraction Refinement (CEGAR)

Motivation

Formal verification

<table>
<thead>
<tr>
<th>Formal model</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Image]</td>
<td>Never „Green“ and „Red“ at the same time</td>
</tr>
</tbody>
</table>

Challenges

- Large set of states and behaviors
- Possible solution is abstraction
- CEGAR method: start with coarse abstraction and refine until sufficient precision is reached
- Various abstract domains and refinement strategies exist

Goal

- Finding efficient combinations of abstractions and refinements for analyzing various models
- Evaluating heuristics for selecting the most efficient combination

Configurable framework required

Counterexample

- Feasible
- Spurious

Use SMT solver: extract refutation from UNSAT formula (interpolant, unsat core, etc.), and refine precision based on the refutation

Advantages

- Configurable
  - Formalisms
  - Abstract domains
  - Refinement strategies
- Novel combinations of abstractions and refinements
- Allows using heuristics for selecting the most efficient configuration based on input

Reference