

Model Checking

Motivation

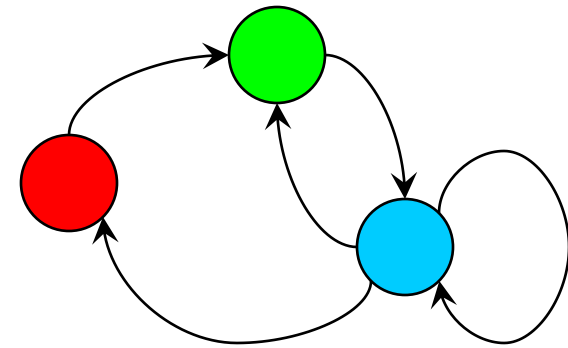
With testing, you can never be sure that you did not miss a bug. Model checking is a more rigorous approach where you actually proof that a system cannot violate a given formal specification. We have a tool named RATSU which is able to do synthesize a system from its specification. We want to extend it with model checking capabilities.

Project description

- Goal
 - Implement a model checking algorithm in RATSU.
- Tasks
 - Read into the topic: understand the basics of automata, games, and model checking.
 - Think of a model checking algorithm for so-called GR(1) specifications.
 - Implement it using the existing infrastructure of RATSU.
 - Evaluate the performance.

Literature

- Baier, Katoen: "*Principles of Model Checking*", MIT Press, 2008. ISBN 978-0-262-02649-9
- Piterman et al., "*Synthesis of Reactive(1) Designs*", LNCS 3855, 2006.
- <http://rat.fbk.eu/ratsy/>



Deliverables

- Source Code (commit to SVN repository)
- Documentation (~10-15 pages)
- Presentation (~10 slides)

Project schedule

- Start Immediately
- Month 1 Familiarize with theory, think of an algorithm
- Month 2 Familiarize with RATSU, Implementation, Evaluation
- Month 3 Final deliverables

Scope and Credits

Studies: INF SEW TEL MATH
 The scope, effort, and credits of this project are scalable.

Prerequisites

- Interest in formal methods
- Basic programming skills

Advisor / contact

Roderick.Bloem@iaik.tugraz.at
Robert.Koenighofer@iaik.tugraz.at

SCOS