

Developing an Open-Source, State-of-the-Art Symbolic Model-Checking Framework for the Model-Checking Research Community

Kristin Y. Rozier
Iowa State University
Ames, IA, USA
kyrozier@iastate.edu

Natarajan Shankar
SRI
Menlo Park, CA, USA
shankar@cs.sri.com

Cesare Tinelli
University of Iowa
Iowa City, IA, USA
cesare-tinelli@uiowa.edu

Moshe Vardi
Rice University
Houston, TX, USA
vardi@cs.rice.edu

Abstract—As model checking becomes more integrated into the standard design and verification process for safety-critical systems, the platforms for model checking research have become more limited. Previous options have become closed-source or industry tools; current research platforms don't have support for expressive specification languages needed for verifying real systems. Our goal is to fill the current gap in model checking research platforms: building a freely-available, open-source, scalable model checking infrastructure that accepts expressive models and efficiently interfaces with the currently-maintained state-of-the-art back-end algorithms to provide an extensible research and verification tool. With extensive involvement from the research community, we have been creating a community resource with a well-documented intermediate representation to enable extensibility, and a web portal, facilitating new modeling languages and back-end algorithmic advances. To add new modeling languages or algorithms, researchers need only to develop a translator to/from the new intermediate language, and will then be able to integrate each advance with the full state-of-the-art in model checking. This tutorial will include an overview of the model checking intermediate language semantics and demonstrations of (provably correct) translators to and from that representation.