Generalized Model Checking

Patrice Godefroid
Bell Laboratories, Lucent Technologies
god@bell-labs.com

Abstract

Three-valued models, in which properties of a system are either true, false or unknown, have recently been advocated as a better representation for reactive program abstractions generated by automatic techniques such as predicate abstraction. Indeed, for the same cost, model checking three-valued abstractions (also called *may/must abstractions*) can be used to both prove and disprove any temporal-logic property, whereas traditional conservative abstractions can only prove universal properties. Also, verification results can be more precise with *generalized model checking*, which checks whether there exists a concretization of an abstraction satisfying a temporal-logic formula. Generalized model checking generalizes both model checking (when the model is complete) and satisfiability (when everything in the model is unknown), probably the two most studied problems related to temporal logic and verification.

In this talk, I will present the main ideas behind this framework, namely models for three-valued abstractions, completeness preorders (to measure the level of completeness of such models), three-valued temporal logics and generalized model checking. I will also discuss algorithms and complexity bounds for three-valued model checking and generalized model-checking for various temporal logics.

Then, I will discuss applications to program verification via automatic abstraction. I will show examples of programs and properties that can be verified by generalized model checking but not with current abstraction-based verification tools. I will also present classes of temporal-logic formulas for which model checking is guaranteed to always have the same precision as generalized model checking.

Finaly, I will briefly discuss three-valued abstractions for reasoning about open systems and about games in general, as well as completeness issues (i.e., given an infinite-state program and a property, is there a finite-state abstraction of that program that satisfies this property?).

Acknowledgements. This talk is based on results presented in several papers [1, 2, 6, 7, 8, 4, 3, 5] co-authored with Glenn Bruns, Luca de Alfaro, Michael Huth and Radha Jagadeesan.

References

[1] G. Bruns and P. Godefroid. Model Checking Partial State Spaces with 3-Valued Temporal Logics. In *Proceedings of CAV'99 (11th Conference on Computer Aided Verification)*, volume 1633 of *Lecture Notes in Computer Science*, pages 274–287, Trento, July 1999. Springer-Verlag.

[2] G. Bruns and P. Godefroid. Generalized Model Checking: Reasoning about Partial State Spaces. In *Proceedings of CONCUR'2000 (11th International Conference on Concurrency Theory)*, volume 1877 of *Lecture Notes in Computer Science*, pages 168–182, University Park, August 2000. Springer-Verlag.

[3] L. de Alfaro, P. Godefroid, and R. Jagadeesan. Three-Valued Abstractions of Games: Uncertainty, but with Precision. In *Proceedings of LICS'2004 (19th IEEE Symposium on Logic in Computer Science)*, pages 170–179, Turku, July 2004.

[4] P. Godefroid. Reasoning about Abstract Open Systems with Generalized Module Checking. In *Proceedings of EMSOFT'2003 (3rd Conference on Embedded Software)*, volume 2855 of *Lecture Notes in Computer Science*, pages 223–240, Philadelphia, October 2003. Springer-Verlag.

[5] P. Godefroid and M. Huth. Model Checking Vs. Generalized Model Checking: Semantic Minimizations for Temporal Logics. In *Proceedings of LICS'2005 (20th IEEE Symposium on Logic in Computer Science)*, Chicago, June 2005.

[6] P. Godefroid, M. Huth, and R. Jagadeesan. Abstraction-based Model Checking using Modal Transition Systems. In *Proceedings of CONCUR'2001 (12th International Conference on Concurrency Theory)*, volume 2154 of *Lecture Notes in Computer Science*, pages 426–440, Aalborg, August 2001. Springer-Verlag.

[7] P. Godefroid and R. Jagadeesan. Automatic Abstraction Using Generalized Model Checking. In *Proceedings of CAV'2002 (14th Conference on Computer Aided Verification)*, volume 2404 of *Lecture Notes in Computer Science*, pages 137–150, Copenhagen, July 2002. Springer-Verlag.

[8] P. Godefroid and R. Jagadeesan. On the Expressiveness of 3-Valued Models. In *Proceedings of VMCAI'2003 (4th Conference on Verification, Model Checking and Abstract Interpretation)*, volume 2575 of *Lecture Notes in Computer Science*, pages 206–222, New York, January 2003. Springer-Verlag.