Building a Software Model-Checker

Javier Esparza
Technische Universität München, Germany

Model-checking techniques are being increasingly applied to software. In this course I will start by introducing jMoped, a tool for the analysis of Java programs. I will then proceed to explain the theory and algorithms behind the tool.

In jMoped we assume that variables have a finite range. I will start by considering the computational complexity of verifying different classes of programs satisfying this constraint. As we shall see, even in this case many verification problems can be undecidable. After choosing a reasonable class of programs, I will introduce a model-checking algorithm based on pushdown automata. Then I will address the problem of data: while variables have a finite range, this range may be large. I will present an approach to this problem based on BDDs and counterexample-based abstraction refinement with interpolants (here there will probably be a significant overlap with Orna Grumberg's course, but the approach will be a bit different).

The course will be based on the following papers (in the order in which they will be used in the course):

References

1. A. Bouajjani and J. Esparza. *Rewriting Models of Boolean Programs*. Proceedings of RTA '06, F. Pfenning (ed.), LNCS 4098, pp. 136–150, 2006.
2. J. Esparza, D. Hansel, P. Rossmanith and S. Schwoon. *Efficient Model Checking Algorithms for Pushdown Systems*. Proceedings of CAV '00, E.A. Emerson and A.P. Sistla (eds.) , LNCS 1855, pp. 232–247, 2000.
3. J. Esparza and S. Schwoon. *A BBD-Based Model Checker for Recursive Programs*. Proceedings of CAV '01, G. Berry, H. Comon, and A. Finkel (eds.), LNCS 2102, pp. 324–336, 2001.
4. J. Esparza, S. Kiefer, and S. Schwoon. *Abstraction Refinement with Craig Interpolation and Symbolic Pushdown Systems*. Proceedings of TACAS '06, LNCS 3920, 489–503, 2006.
5. D. Suwimonteerabuth, S. Schwoon and J. Esparza. *jMoped: A Java Bytecode Checker Based on Moped*. Proceedings of TACAS '05, N. Halbwachs and L. Zuck (eds.), LNCS 3440, pp. 541–545, 2005.

The papers are available online at my home page.