Software Model Checking via Systematic Testing

Patrice Godefroid
Microsoft Research, Redmond, USA

Model checking and testing have a lot in common. Over the last two decades, significant progress has been made on how to broaden the scope of model checking from finite-state abstractions to actual software implementations. One way to do this consists of adapting model checking into a form of systematic testing that is applicable to industrial-size software. The aim of these lectures is to present a comprehensive overview of this strand of software model checking, by describing the main ideas, techniques and results obtained in this area, including combinations with static program analysis.

Further Reading:
General [3, 4, 6], on dealing with concurrency [2], on dealing with data inputs [5], on may/must abstractions [1], on combining with static softwaremodel checking [7]

All available at `http://research.microsoft.com/ pg/`

References

[1] G. Bruns, P. Godefroid. *Generalized Model Checking: Reasoning about Partial State Spaces.* In: Procs. of CONCUR2000; LNCS 1877; pp. 168–182; Springer; 2000.

[2] P. Godefroid. *Software Model Checking: The VeriSoft Approach.* Formal Methods in System Design, Vol. 26(2); pp. 168–182; 2005.
Also available as Bell Labs Technical Memorandum ITD-03-44189G, 2003.

[3] P. Godefroid. *The Soundness of Bugs is What Matters* (Position Paper). In: Procs. of BUGS05 (PLDI05 Workshop on the Evaluation of Software Defect Detection Tools); 2005.

[4] P. Godefroid, P. de Halleux, M. Y. Levin, A. V. Nori, S. K. Rajamani, W. Schulte, N. Tillmann. *Automating Software Testing Using Program Analysis.* IEEE Software, Vol. 25(5); pp.3037; 2008.

[5] P. Godefroid, N. Klarlund, K. Sen. *DART: Directed Automated Random Testing.* In: Procs. of PLDI05; pp. 213-223; 2005.

[6] P. Godefroid, M.Y. Levin, D. Molnar. *SAGE: Whitebox Fuzzing for Security Testing.* Communications of the ACM, Vol. 55(3); pp. 40-44; 2012.

[7] P. Godefroid, A.V. Nori, S.K. Rajamani, S.D. Tetali. *Compositional May-Must Program Analysis: Unleashing The Power of Alternation.* In: Procs. of POPL10; pp. 43-55; 2010.