Symbolic Execution and Software Testing

Corina Pasareanu
NASA Ames Research Center, Moffet Field, USA

Symbolic execution is a systematic program analysis technique that has become increasingly popular in recent years, due to algorithmic advances and availability of computational power and constraint solving technology.

We review different flavors of symbolic execution, ranging from generalized symbolic execution to dynamic symbolic execution or concolic testing. We also identify challenges to symbolic execution, such as dealing with: looping constructs, multi-threading, recursive data structures, and complex mathematical constraints, as well as scalability challenges due to the path explosion problem. We discuss techniques and tools that address these challenges. Finally we discuss the application of symbolic execution to software testing. If time permits, we will also review applications to: security, robustness, reliability and load testing.

We will use the Symbolic PathFinder open-source tool available from:

`http://babelfish.arc.nasa.gov/trac/jpf/wiki/projects/jpf-symbc`

References

[1] L. A. Clarke. *A System to Generate Test Data and Symbolically Execute Programs.* IEEE TSE; 1976.

[2] J. C. King. *Symbolic Execution and Program Testing.* Communications of the ACM; 1976.

[3] S. Khurshid, C. S. Pasareanu, W. Visser. *Generalized Symbolic Execution for Model Checking and Testing.* TACAS 2003.

[4] C. S. Pasareanu, W. Visser. *Verification of Java Programs Using Symbolic Execution and Invariant Generation.* SPIN 2004.

[5] P. Godefroid, N. Klarlund, K. Sen. *DART: Directed Automated Random Testing.* PLDI 2005.

[6] K. Sen, D. Marinov, G. Agha. *CUTE: a Concolic Unit Testing Engine for C.* ESEC/SIGSOFT FSE 2005.

[7] P. Godefroid. *Compositional Dynamic Test Generation.* POPL 2007.

[8] C. Cadar, D. Dunbar, D. R. Engler. *KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs.* OSDI 2008.

[9] C. S. Pasareanu, P. C. Mehlitz, D. H. Bushnell, K. Gundy-Burlet, M. R. Lowry, S. Person, M. Pape. *Combining Unit-level Symbolic Execution and System-level Concrete Execution for Testing NASA Software.* ISSTA 2008.

[10] S. Anand, C. S. Pasareanu, W. Visser. *Symbolic Execution with Abstraction.* STTT, Vol. 11(1), pp. 53-67; 2009.

[11] M. Staats, C. S. Pasareanu. *Parallel Symbolic Execution for Structural Test Generation.* ISSTA 2010.

[12] C. S. Pasareanu, N. Rungta, W. Visser. *Symbolic Execution with Mixed Concrete-symbolic Solving.* ISSTA 2011.

[13] C. Cadar, P. Godefroid, S. Khurshid, C. S. Pasareanu, K. Sen, N. Tillmann, W. Visser. *Symbolic Execution for Software Testing in Practice: Preliminary Assessment.* ICSE 2011.

Bibliography on symbolic execution: `http://sites.google.com/site/symexbib/`