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


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