Efficient symbolic execution for software testing

Johannes Kinder

Department of Computer Science at Royal Holloway, University of London
Email: johannes.kinder@rhul.ac.uk

Abstract of tutorial talk

Symbolic execution has proven to be a practical technique for building automated test case generation and bug finding tools. While the basic technique had been introduced already in the 70s, the advent of modern SAT and SMT solvers has lead to a surge of tools and techniques in the area over the last decade. This tutorial will introduce and compare the different approaches to using symbolic execution for testing and discuss the specific challenges and trade-offs.

A main challenge in symbolic execution is path explosion, and various proposals have been made to combat it. I will discuss how these techniques affect the number and type of solver queries that have to be made, and how this can lead to surprising effects on the efficiency of a symbolic execution engine. Going further, we will look at developments to increase the scope of symbolic execution to larger software systems. Specific topics covered include state merging, procedure summaries, abstraction, search strategies, and parallelization.

ISBN: 978-0-9835678-4-4. Copyright owned jointly by the authors and FMCAD Inc.