1. ABSTRACT

Satisfiability solvers for propositional logic have had tremendous impact on hardware modeling and verification. Unfortunately, propositional logic is insufficient for reasoning about software. Precise models for software executions must cater to complex control flow (e.g., procedure calls, multithreading) and complex data manipulation (e.g., object hierarchies, pointers). To enable precise reasoning about software executions, we introduce a simple modeling language that includes features such as nondeterministic choice, loops, and (synchronous and asynchronous) procedure calls. We allow state update to be modeled using two-state predicates that relate the current and next values of program variables, requiring only that satisfiability for these predicates be efficiently decidable. For programs in this language, we refer to the problem of deciding whether a particular control location is reachable as the reachability-modulo-theories problem. We will argue that reachability-modulo-theories is a flexible foundation for building a variety of software analyzers, including tools for finding bugs, answering developer questions, and debugging crash dumps. We will describe Corral, a semi-algorithm for the reachability-modulo-theories problem. We have evaluated Corral against other related tools and found that it consistently out-performs its competitors on a variety of benchmarks.

2. SPEAKER BIOGRAPHY

Shaz Qadeer is a Senior Researcher in the RiSE group (Research in Software Engineering) at Microsoft. He received his Ph.D. from the University of California at Berkeley and worked at Compaq Systems Research Center before joining Microsoft Research. He is interested in automated reasoning, software testing and verification, and languages for parallel and distributed programming. He has spent a significant part of his professional life developing simple and practical methods for reasoning about concurrent programs. You can get more information about his activities at http://research.microsoft.com/en-us/people/qadeer/