The Marriage of Exploration and Deduction

Rupak Majumdar

Max-Planck Institute for Software Systems, Germany
rupak@mpi-sws.org

State space exploration based on abstraction and refinement has been the cornerstone of several successful software verification tools from the last decade. While these tools have made impressive progress in verifying control-dominant properties of code, most prominently in the domain of device drivers, their applications to more data-intensive properties have been limited. In particular, we focus on *parameterized systems*, which define infinite families of systems, one for each value of the parameter. Many real-life software systems, for example, memory management units or cache coherence protocols can be modeled as parameterized systems (parameterized, e.g., by the number of processes and memory locations), We want to perform *uniform verification* of parameterized systems, where we show a formula is an invariant of every member in the parameterized family.

The primary verification strategy for parameterized systems is *deduction*. For safety verification, the user guesses an inductive invariant for the parameterized family, and uses decision procedures to check that the guess is indeed correct. The deductive approach has the advantage of better scalability (through reducing the problem to a few SMT queries), expressiveness (invariants are usually quantified, and modern decision procedures have good quantifier instantiation heuristics), and avoids unbounded refinement loops that plague abstraction-refinement based model checkers. However, it depends on the ingenuity of the user to provide appropriate inductive invariants.

We shall show how combinations of deductive and explorative techniques can lead to automatic verification for parameterized systems, or at least, reduce the manual effort required to come up with appropriate inductive invariants. We demonstrate the applicability of the technique through two case studies: the verification of transactional memories and of cache coherence protocols. We also outline some challenges in applying the methods, and directions which require further research.

R. Joshi, P. Müller, and A. Podelski (Eds.): VSTTE 2012, LNCS 7152, p. 162, 2012.