Abstract

09/03/2015

Modern software analysis and model-based tools are increasingly complex and multi-faceted software systems. However, at their core is invariably a component using logical formulas for describing states and transformations between system states. In a nutshell, symbolic logic is the calculus of computation. The state-of-the art Satisfiability Modulo Theories (SMT) solver, Z3, from Microsoft Research, can be used to check the satisfiability of first-order formulas containing operations from various theories such as the Booleans, bit-vectors, arithmetic, arrays, and recursive data types. SMT solvers are extensions of Boolean satisfiability solvers (SAT solvers) that check the satisfiability of formulas built from Boolean variables and operations. SMT solvers have a wide range of applications in hardware and software verification, extended static checking, constraint solving, planning, scheduling, test case generation, and computer security. In this doctoral seminar we briefly survey the theory of SAT and SMT solving, and present some of the key algorithms (for instance DPLL and other incomplete algorithms) and later we will discuss various theories, applications and extensions i.e. programmatic APIs (especially using Python) to Z3.

Keywords: First order logic, SAT, SMT, Z3.