On Techniques for Formal Verification

Olga Tveretina

Аннотация

Techniques for formal verification provide a guarantee that a design is free of specific flaws. Formal verification can be helpful in proving the correctness of systems such as cryptographic protocols, combinational circuits, digital circuits with internal memory, and software expressed as source code. Examples of mathematical models used to describe such systems include various logics and automata.

Many verification problems can be reduced to propositional satisfiability checking. Moreover, the classical propositional calculus presents some of the most challenging and intriguing problems in modern logic. And in the first part of my talk I will concentrate on key advances of propositional SAT solving/solvers.

In the second part of my talk I will present current challenges in the verification of hybrid systems. A hybrid system is a dynamic system that exhibits both continuous and discrete behaviour. Examples of such systems come from robotics, avionics, air traffic management and automated highway management. Most of the hybrid systems are safety critical and errors can have serious consequences. Latest progress include theoretical results and tools for the safety verification of such systems. However, a large number of challenging problems has to be solved before these techniques can be applied to applications of industrial size.