

EINLADUNG

Zeit: 21. Dez. 2011, 14.15 Uhr
Ort: AH 3, Ahornstr. 55
Referent: Dipl.-Inform. Carsten Fuhs,
Lehr- und Forschungsgebiet Informatik 2
Titel: SAT Encodings: From Constraint-Based
Termination Analysis to Circuit Synthesis

Abstract:

Termination is one of the most prominent undecidable problems in computer science. At the same time, the problem whether a given program terminates for all inputs is sufficiently important for the area of program verification to spur decades-long efforts in developing sufficient criteria for concluding termination. In the last decade, the focus of this research has been on automation, giving rise to several powerful fully automatic termination provers. However, the search problems that arise during the synthesis of a successful termination proof are typically NP-complete.

To tackle these algorithmic challenges, over the last years a two-stage process has turned out to be extremely successful in practice: First encode the arising problem instance to the satisfiability problem of propositional logic (SAT), and then invoke a state-of-the-art SAT solver on this SAT instance. The solution found by the SAT solver is then used in the termination proof.

While in the worst case still prohibitive due to NP-completeness of SAT, this approach has increased performance on practical problem instances for existing termination techniques by orders of magnitude. At the same time, the approach has also made new automated techniques possible that were out of reach before. This thesis contributes efficient SAT-based automation both for several existing termination techniques and also for new techniques that we have developed.

The usefulness of SAT encodings goes beyond the field of termination analysis. We have transferred the approach used for termination techniques to the---at first glance---quite distinct application domain of circuit synthesis, allowing us to obtain a provably optimal implementation of a part of the Advanced Encryption Standard.

The contributions of this thesis are implemented within our fully automated termination prover AProVE. The significance of our results is demonstrated also by AProVE reaching the highest scores in the annual International Termination Competitions of 2007 -- 2011. At these competitions, the leading automated termination analysis tools try to prove or disprove termination of programs originating from various areas of computer science.

Es laden ein: Die Dozenten der Informatik