Automata and Equations based Approximations for Reachability Analysis

Thomas Genet
Univ Rennes/Inria/CNRS/IRISA,
Campus Beaulieu, 35042 Rennes Cedex, France

Term Rewriting Systems (TRSs for short) are a convenient formal model for software systems. This formalism is expressive enough to model in a simple and accurate way many aspects of computation such as: recursivity, non-determinism, parallelism, distribution, communication. On such models, verification is facilitated by the large collection of proof techniques of rewriting: termination, non-termination, confluence, non-confluence, reachability, unreachability, inductive properties, etc. This talk focuses on unreachability properties of a TRS, which entails safety properties on the modeled software system.

Starting from a single term \( s \), proving that \( t \) is unreachable, i.e., \( s \not \rightarrow^* R t \) is straightforward if \( R \) is terminating. This problem is undecidable if \( R \) is not terminating or if we consider infinite sets of initial terms \( s \) and infinite sets of “Bad” terms \( t \). There exists TRSs classes for which those problems are decidable. For those classes, decidability comes from the fact that the set of reachable terms is regular, i.e., it can be recognized by a tree automaton [5]. Those classes are surveyed in [7].

However, TRSs modeling software systems do not belong to those “decidable classes”; in general. The rewriting and tree automata community have proposed different techniques to over-approximate the set of reachable terms. Over-approximating reachable terms provide a criterion for unreachability on TRSs and, thus, a criterion for safety of the modeled systems. Those approximation techniques range from TRSs transformation [11], ad hoc automata transformations [6,10], CounterExample-Guided Abstraction Refinement (CEGAR) [4,2,1], and abstraction by equational theories [12,9]. I will present the principles underlying those techniques, discuss their pros and cons, and recall some of their applications. Then, I will present a recent attempt to combine abstraction by equational theories and CEGAR to infer accurate over-approximations for TRSs modeling higher-order functional programs [8].

References


