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., $s \not\rightarrow^*_{\mathcal{R}} t$ is straightforward if $\mathcal{R}$ is terminating. This problem is undecidable if $\mathcal{R}$ 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 [6,10,3], 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

1. Y. Boichut, B. Boyer, T. Genet, and A. Legay. Equational Abstraction Refinement for Certified Tree Regular Model Checking. In *ICFEM'12*, volume 7635 of *LNCS*. Springer, 2012.
2. Y. Boichut, R. Courbis, P.-C. Héam, and O. Kouchnarenko. Finer is better: Abstraction refinement for rewriting approximations. In A. Voronkov, editor, *Rewriting Techniques and Applications, 19th International Conference, RTA-08*, LNCS 5117, pages 48–62, Hagenberg, Austria, 2008. Springer.

3. Y. Boichut, P.-C. Héam, and O. Kouchnarenko. Automatic Approximation for the Verification of Cryptographic Protocols. In *Proc. AVIS'2004, joint to ETAPS'04, Barcelona (Spain)*, 2004.
4. A. Bouajjani, P. Habermehl, A. Rogalewicz, and T. Vojnar. Abstract regular tree model checking. *ENTCS*, 149(1):37–48, 2006.
5. H. Comon, M. Dauchet, R. Gilleron, F. Jacquemard, D. Lugiez, C. Löding, S. Tison, and M. Tommasi. Tree Automata Techniques and Applications. `http://tata.gforge.inria.fr`, 2008.
6. T. Genet. Decidable Approximations of Sets of Descendants and Sets of Normal Forms. In *RTA'98*, volume 1379 of *LNCS*, pages 151–165. Springer, 1998.
7. T. Genet. Reachability analysis of rewriting for software verification. Université de Rennes 1, 2009. Habilitation document, `http://people.irisa.fr/Thomas.Genet/publications.html`.
8. T. Genet, T. Haudebourg, and T. Jensen. Verifying higher-order functions with tree automata. In *FoSSaCS'18*, LNCS. Springer, 2018. To be published.
9. T. Genet and R. Rusu. Equational tree automata completion. *Journal of Symbolic Computation*, 45:574–597, 2010.
10. T. Genet and Valérie Viet Triem Tong. Reachability Analysis of Term Rewriting Systems with *timbuk*. In *Proc. 8th LPAR Conf., Havana (Cuba)*, volume 2250 of *LNAI*, pages 691–702. Springer-Verlag, 2001.
11. F. Jacquemard. Decidable approximations of term rewriting systems. In H. Ganzinger, editor, *Proc. of RTA'96*, volume 1103 of *LNCS*, pages 362–376. Springer, 1996.
12. J. Meseguer, M. Palomino, and N. Martí-Oliet. Equational abstractions. *TCS*, 403(2-3):239–264, 2008.