Verifying Temporal Regular Properties for Abstraction of Term Rewriting Systems

Benoît Boyer
Université Rennes 1, France
Benoit.Boyer@irisa.fr

Thomas Genet
Université Rennes 1, France
Thomas.Genet@irisa.fr

The tree automaton completion is an algorithm used for proving safety properties on systems which can be modeled by a term rewriting system. This representation and verification technique works well for proving properties on infinite systems like cryptographic protocols or more recently on Java Bytecode programs. This algorithm computes a tree automaton which represents a (regular) over approximation of the set of reachable terms by rewriting initial terms. This approach is limited by the lack of information about rewriting relation between terms. Actually, terms in relation by rewriting are in the same equivalence class: there are recognized into the same state by the tree automaton.

Our objective is to produce a completed automaton embedding an abstraction of the rewriting relation sufficient to prove temporal properties on the term rewriting system.

We propose to extend the algorithm to produce a completed automaton having more equivalence classes to distinguish a term or a subterm from its successors w.r.t. rewriting. While ground transitions are used to recognize equivalence classes of terms, ε-transitions represent the rewriting relation between terms. From the completed automaton, it is possible to automatically build a Kripke structure abstracting the rewriting sequence. States of the Kripke structure are states of the tree automaton and the transition relation is given by the set of ε-transitions. States of the Kripke structure are labelled by the set of terms recognized using ground transitions. On this Kripke structure, we define the Regular Linear Temporal Logic (R-LTL) for expressing properties. Such properties can then be checked using standard model checking algorithms. The only difference between LTL and R-LTL is that predicates are replaced by a regular set of acceptable terms.

Submitted to Electronic Proceedings
in Theoretical Computer Science.