Proving Reachability Modulo Theories (extended abstract)

Ștefan Ciobâcă

Faculty of Computer Science
Alexandru Ioan Cuza University
stefan.ciobaca@info.uaic.ro

We consider transition systems generated by constrained rewrite rules of the form $l \twoheadrightarrow r \texttt{ if } \phi$, where l and r are terms and ϕ is a logical constraint. The terms l, r can contain both uninterpreted symbols and symbols interpreted in a builtin model such as the model of booleans and integers. The constraint ϕ is a first-order formula which limits the application of the rule. The intuitive meaning of a constrained rule $l \twoheadrightarrow r \texttt{ if } \phi$ is that any instance of l that satisfies ϕ transitions into the corresponding instance of r in one step.

Given a constrained rule system, which serves as a specification for a transition system, it is natural to define the notion of constrained term $\varphi = (t \,|\, \phi)$, where t is an ordinary term (with variables) and ϕ is a logical constraint. The intuitive meaning of such a term is the set of ground instances of t that satisfy ϕ.

A reachability formula is a pair of constrained terms $(t \,|\, \phi) \Rightarrow (t' \,|\, \phi')$. The intuitive meaning of a reachability formula is that any instance of $(t \,|\, \phi)$ reaches, along all terminating paths of the transition system, an instance of $(t' \,|\, \phi')$ that agrees with $(t \,|\, \phi)$ on the set of shared variables.

We provide a proof system for deriving valid reachability formulae from transition systems specified by a set of constrained rules. We present our proof system in two steps. In the first step, we provide a three-rule proof system for *symbolic execution of constrained terms*:

$$[\mathsf{axiom}]\ \frac{}{(t \,|\, \phi) \Rightarrow \varphi'}\ M^{\Sigma} \models \phi \iff \bot$$

$$[\mathsf{subs}]\ \frac{(t'' \,|\, \phi'' \wedge \neg\phi''') \Rightarrow (t' \,|\, \phi')}{(t \,|\, \phi) \Rightarrow (t' \,|\, \phi')}\quad \begin{array}{l} (t'' \,|\, \phi'') \Rightarrow \varphi' \equiv (t \,|\, \phi) \Rightarrow \varphi', \text{ and} \\ M^{\Sigma} \models \phi''' \iff (\exists X)(t'' =^{?} t' \wedge \phi'), \text{ and} \\ X \triangleq var(t', \phi') \setminus var(t'', \phi'') \end{array}$$

$$[\mathsf{der}^{\forall}]\ \frac{\{(t^j \mid \phi^j) \Rightarrow \varphi' \mid (t^j \mid \phi^j) \in \Delta_{\mathcal{R}}((t'' \mid \phi''))\}}{(t \mid \phi) \Rightarrow \varphi'}$$

$(t \mid \phi)$ $\mathcal{R}-$derivable, and
$(t'' \mid \phi'') \Rightarrow \varphi' \equiv (t \mid \phi) \Rightarrow \varphi'$, and
$\phi'' \wedge \bigwedge \left\{ \neg(\exists Y)\phi^j \;\middle|\; \begin{array}{l} (t^j \mid \phi^j) \in \Delta_{\mathcal{R}}((t'' \mid \phi'')), \\ Y \triangleq var(t^j, \phi^j) \setminus var(t'', \phi'') \end{array} \right\}$ not satisfiable

The set $\Delta_{\mathcal{R}}((t'' \mid \phi''))$ denotes the symbolic successors of the constrained term $(t'' \mid \phi'')$ and a constrained term $(t \mid \phi)$ is $\mathcal{R}$-derivable if it has at least such a successor.

When interpreting the proof system coinductively, its proof tress can be finite or infinite. The finite proof trees allow to derive reachability formulae $(t \mid \phi) \Rightarrow (t' \mid \phi')$ when there is a bounded number of steps between $(t \mid \phi)$ and $(t' \mid \phi')$. The infinite proof trees correspond to proofs of reachability formulae $(t \mid \phi) \Rightarrow (t' \mid \phi')$ that hold for an unbounded number of steps between $(t \mid \phi)$ and $(t' \mid \phi')$. Unfortunately, the infinite proof trees are not too useful in practice because they cannot be obtained in finite time.

In order to allow the derivation of reachability formulae that require an unbounded number of steps, we introduce a fourth proof rule to the system that we call *circularity*:

$$[\mathsf{circ}]\ \frac{\begin{array}{l}(t'_c \mid \phi'_c \wedge \phi \wedge \phi'')) \Rightarrow \varphi', \\ (t \mid \phi \wedge \neg\phi'') \Rightarrow \varphi'\end{array}}{(t \mid \phi) \Rightarrow \varphi'} \quad \begin{array}{l} M^{\Sigma} \models \phi'' \iff (\exists var(t_c, \phi_c))(t =^{?} t_c \wedge \phi_c), \\ (t_c \mid \phi_c) \Rightarrow (t'_c \mid \phi'_c) \in G \end{array}$$

The circularity proof rule can be used to compress infinite proof trees into finite proof trees by first identifying a set G of *circularities*, which are simply patterns of reachability formulae that are repeatedly used in the infinite proof tree. The set G includes the reachability formulas to be proved. The circularity proof rule allows to use G as axioms to prove the formulae in G, thereby reducing infinite trees to finite trees. As expected, using the circularity rule in an unrestricted fashion can quickly lead to unsoundness. We provide a *syntactic criterion for using circularity in a sound manner*, by requiring that each use of the rule is preceded by a proper step in the transition system (using the $[\mathsf{der}^{\forall}]$ rule). This syntactic criterion selects sound proof trees out of the entire set of trees. In order to validate the proof system, we have implemented it in the `RMT` tool and tested it on some non-trivial examples.

This is joint work with Dorel Lucanu. Partially, this work was supported by a grant of the Romanian National Authority for Scientific Research and Innovation, CNCS/CCCDI UEFISCDI, project number PN-III-P2-2.1-BG-2016-0394, within PNCDI III.