1. Why Symbolic Reachability Analysis? How?

Camilo Rocha
Escuela Colombiana de Ingeniería

7th International School on Rewriting (ISR2014)
Universidad Técnica Federico Santa María
August 25-29, 2014

Motivation

Many distributed systems such as:

- distributed cyber-physical systems, and
- secure distributed systems

are **open**, interacting with an external, possibly hostile **environment**; and are often **safety-critical**

At present, analyzing such systems with methods that are **scalable** and **amenable to (semi-)automation** is difficult because:

- they are highly **concurrent** and often **infinite-state**
- the external environment they interact with is highly **non-deterministic**

The Practical Problems

Some techniques provide certain ways to automatically analyze highly concurrent systems with varying degrees of scalability, but are, in general, limited by:

complexity: the systems can be inherently complex or have a rewrite relation that cannot be directly executed

- this is the case of many open systems that interact with an environment that is highly non-deterministic

size: the number of reachable states from an initial state or the number of initial states

- it many practical cases the sizes of such sets can be intractable or countably infinite

extensibility: the techniques and tools are hard to combine

Some Partial Answers

These techniques offer a varying degree of scalability:

- **Automata-Based Model Checking**, where possibly infinite sets of behaviors and/or states are symbolically represented by various kinds of **automata**
- **SMT Solving**, where, for domains having decidable theories, possibly infinite sets of states are symbolically represented as constraints
- **Rewriting and Narrowing Modulo Theories**, where, modulo an equational theory E, E-equivalence classes of states, or even patters defining infinite sets of such equivalence classes modulo E are represented as terms, and their transitions as rewrite rules

In These Talks

In the rest of these talks I will present some recent work towards completing, extending, and combining techniques for **symbolic reachability analysis** for rewrite theories, explaining techniques that are being developed for:

- rewriting modulo $E + SMT$, and model checking methods based on that
- rewriting and narrowing modulo E for a rich variety of equational theories, and inductive reachability analysis based on that

Main Ideas: Rewriting Modulo SMT

Using an SMT solver, rewriting can be made **executable** in a **symbolic** way by rewriting **constrained terms** of the form

$$u \mid \phi$$

with ϕ a quantifier-free formula.

I have shown that rewriting modulo SMT (as defined later) is complete with respect to reachability analysis for the ground rewrite relation

Main Ideas: Narrowing Modulo

Given a rewrite theory $\mathcal{R} = (\Sigma, G \cup B, R)$, the **narrowing modulo** $G \cup B$ relation

$$t \rightsquigarrow_{R,(G \cup B)} t'$$

is defined if there is

- a non-variable position $p \in \mathrm{Pos}(t)$
- a rule $l \longrightarrow r$ in R
- a $(G \cup B)$-**unifier** σ such that $\sigma(t|_p) =_{(G \cup B)} \sigma(l)$ and $t' = \sigma(t[r]_p)$

Meseguer and Thati have shown that, if $\mathcal{R}$ is a **topmost** rewrite theory, narrowing modulo is a **complete reachability analysis method** to solve queries fo the form

$$(\exists \vec{x}) t \rightarrow^* t'$$

Main Ideas: Bonus Feature

(Q): How can rewriting logic be used to model an **open system**, i.e., a system that interacts with a non-deterministic **environment**, modeled in the rewrite theory $\mathcal{R} = (\Sigma, G \cup B, R)$?

(A): It is modeled by the fact that the (possibly conditional) rewrite rules R may have **extra variables $\vec{y}$ in their right-hand** side

$$t(\vec{x}) \longrightarrow t'(\vec{x}, \vec{y}) \textbf{ if } cond$$

(Bonus): Rewriting modulo SMT and Narrowing Modulo can both be used to analyze open systems of this form