Appendix 2 to Lecture 21: Backwards Symbolic Reachability Analysis

J. Meseguer

Given a topmost rewrite theory $\mathcal{R} = (\Sigma, B, R)$, define its *inverse* theory $\mathcal{R}^{-1}$ as the theory $\mathcal{R}^{-1} = (\Sigma, B, R^{-1})$, where $R^{-1} =_{def} \{r \to l \mid (l \to r) \in R\}$. Then, by the very definition of the rewriting relation $\to_{R/B}$ we have for any Σ-terms t, t' the equivalence:

$$t \to_{R/B} t' \quad \Leftrightarrow \quad t' \to_{R^{-1}/B} t.$$

That is, like with driving a car, the transitions of $\mathcal{R}^{-1}$ are just those of $\mathcal{R}$ *in reverse*. This has, as an immediate consequence of the Symbolic Verification of $\Diamond$ Properties Theorem in pg. 11 of Lecture 21, the following useful corollary:

Corollary (Backwards Symbolic Verification of $\Diamond$ properties). For $\mathcal{R} = (\Sigma, B, R)$ topmost, and $u_1 \vee \ldots \vee u_n$ and $v_1 \vee \ldots \vee v_m$ constructor pattern disjunctions,

$$\mathbb{C}_{\mathcal{R}}, (u_1 \vee \ldots \vee u_n) \models_{S4} \Diamond(v_1 \vee \ldots \vee v_m)$$

iff

$$\mathbb{C}_{\mathcal{R}^{-1}}, (v_1 \vee \ldots \vee v_m) \models_{S4} \Diamond(u_1 \vee \ldots \vee u_n)$$

iff there exist i, j, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$ and an R, B-narrowing sequence $v_j \overset{\theta}{\leadsto}{}^{*}_{R^{-1},B}\, w$ such that there is a B-unifier $\gamma \in \mathit{Unif}_B(u_i = w)$.

The symbolic search method based on performing narrowing search backwards from the target term v_j to the term u_i symbolically describing a (typically infinite) set of concrete initial states by performing narrowing with $\mathcal{R}^{-1}$ is called *backwards symbolic reachability analysis*, and, as the above corollary shows, is completely equivalent to its forwards version.

The advantage of having both the forwards and the backwards narrowing options available to prove $\Diamond$ properties $\mathbb{C}_{\mathcal{R}}, (u_1 \vee \ldots \vee u_n) \models_{S4} \Diamond(v_1 \vee \ldots \vee v_m)$ resides in the fact that, in some cases, the symbolic search may be much easier backwards than forwards. For example, our initial state may be a single *ground term*, for which we know *a priori* (see the remark in Lecture 21, pg. 18) that the narrowing relation $\leadsto^{*}_{R,B}$ *becomes* the rewrite relation $\to_{R/B}$, making truly symbolic search impossible, whereas this problem may completely evaporate by performing backwards narrowing search from the v_j to the u_i with $\mathcal{R}^{-1}$.

Note, finally, that, even assuming that $\mathcal{R}$ is, as usual, *executable* by rewriting, that is, that for each $(l \to r) \in R$ we have $\mathit{vars}(r) \subseteq \mathit{vars}(l)$, $\mathcal{R}^{-1}$ *need not be executable by rewriting*, since such a variable containment property will only hold in the opposite direction if $\mathit{vars}(r) = \mathit{vars}(l)$. However, $\mathcal{R}^{-1}$ *is perfectly well executable by narrowing.* This shows the greater generality of narrowing symbolic computation as compared to rewriting computation, as well as the considerably greater range of rewrite theories $\mathcal{R}$ that can be *symbolically* executed by narrowing, when compare to those executable by rewriting. Maude's `fvu-narrow` search command is fully general: it also applies to non-executable topmost rewrite theories $\mathcal{R}^{-1}$, thus supporting symbolic backwards narrowing search.