Appendix 2 to Lecture 23: 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 a car, the transitions of $\mathcal{R}^{-1}$ are just those of $\mathcal{R}$ *in reverse*. This has, as an immediate consequence of the Completeness of Narrowing Search Theorem in pg. 9 of Lecture 23, the following useful corollary:

Theorem (Completeness of Backwards Narrowing Search). For $\mathcal{R} = (\Sigma, B, R)$ topmost, t a non-variable term of sort *State* with variables $\vec{x}$, and u a term of sort *State* with variables $\vec{y}$, the FOL existential formula:

$$\exists \vec{x}, \vec{y}.\ t \to^{*} u$$

is satisfied in $\mathbb{C}_{\mathcal{R}}$ iff there is an R^{-1}, B-narrowing sequence $u \overset{\theta}{\rightsquigarrow}{}^{*}_{R^{-1},B} v$ such that there is a B-unifier $\gamma \in \mathit{Unif}_{B}(t = v)$.

The symbolic search method based on performing narrowing search backwards from the target term u to the term t 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, whose completeness was proved in the Completeness of Narrowing Search Theorem.

The advantage of having both the forwards and the backwards narrowing options available to prove reachability properties of the form $\exists \vec{x}, \vec{y}.\ t \to^{*} u$ resides in the fact that, in some cases, the symbolic search may be much easier backwards than forwards. For example, our initial state t may be a *ground term*, for which we know *a priori* (see the remark in Lecture 20, pg. 14) that the narrowing relation $\rightsquigarrow^{*}_{R,B}$ *becomes* the rewrite relation $\to_{R/B}$, making truly symbolic search impossible, whereas this problem completely evaporates by performing backwards narrowing search from u to t 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 $\mathit{vars}(r) \subseteq \mathit{vars}(t)$, $\mathcal{R}^{-1}$ *need not be executable by rewriting*, since such a variable containment property may fail to hold. 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 compared 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 backwards narrowing search.