Appendix to Lecture 24: Faithfulness of the Folding Narrowing Graph $FNG_{\mathcal{R}}(u)$

J. Meseguer

Theorem (Over-Approximation Theorem). Given a topmost $\mathcal{R} = (\Sigma, E \cup B, R)$ with $E \cup B$ FVP and a symbolic initial state u, for every narrowing path from u, $u \rightsquigarrow^*_{R,(E\cup B)} v$ there is a node w in the folding narrowing path of u $FNG_{\mathcal{R}}(u)$ such that $v \preccurlyeq_{E\cup B} w$.

Proof: By induction on the length n of the narrowing path. For $n = 0$, u itself is the desired node. Consider now a path of length $n + 1$, $u \rightsquigarrow^n_{R,(E\cup B)} v_n \rightsquigarrow_{R,(E\cup B)} v$. By the induction hypothesis we then have a node w_n in $FNG_{\mathcal{R}}(u)$ such that $v_n \preccurlyeq_{E\cup B} w_n$. Let α be a substitution such that $w_n\alpha =_{E\cup B} v_n$, and let β be the substitution associated to the narrowing step $v_n \rightsquigarrow_{R,(E\cup B)} v$. Then, $w_n\alpha\beta =_{E\cup B} v_n\beta$ and, by the definition of narrowing, we have a rewrite step $w_n\alpha\beta \rightarrow_{R/(E\cup B)} v$. Therefore, by the Lifting Lemma there is a narrowing step $w_n \rightsquigarrow_{R,(E\cup B)} w$ and a substitution γ such that $w\gamma =_{E\cup B} v$. And by the construction of $FNG_{\mathcal{R}}(u)$ there is a w' in $FNG_{\mathcal{R}}(u)$ and a substitution δ such that $w =_{E\cup B} w'\delta$ (δ could be the identity substitution if w belongs to $FNG_{\mathcal{R}}(u)$). Therefore, we have $v \preccurlyeq_{E\cup B} w'$ with w' in $FNG_{\mathcal{R}}(u)$, as desired. $\square$

Theorem (Faithfulness Theorem). For $\mathcal{R} = (\Sigma, E \cup B, R)$ and u as above, $FNG_{\mathcal{R}}(u)$ is a *faithful* over-approximation of the narrowing tree of u in the sense that for any set of states of $\mathcal{R}$ described symbolically by a pattern term p, an instance of p can be reached by a narrowing path $u \rightsquigarrow^*_{R,(E\cup B)} v$ such that $Unif_{E\cup B}(v = p) \neq \emptyset$ iff there is a node w in $FNG_{\mathcal{R}}(u)$ such that $Unif_{E\cup B}(w = p) \neq \emptyset$.

In particular, if p is the negation of an invariant, any counterexample found in $FNG_{\mathcal{R}}(u)$ is a true counterexample and therefore *proves* the invariant's violation (i.e., $FNG_{\mathcal{R}}(u)$ has *no spurious* counterexamples).

Proof: The ($\Leftarrow$) implication follows from the fact that, by construction, for each node w in $FNG_{\mathcal{R}}(u)$ there is a narrowing path $u \rightsquigarrow^*_{R,(E\cup B)} w$. The ($\Rightarrow$) implication follows from the Over Approximation Theorem, since if there is a narrowing path $u \rightsquigarrow^*_{R,(E\cup B)} v$ such that $Unif_{E\cup B}(v = p) \neq \emptyset$, then there is a node w in $FNG_{\mathcal{R}}(u)$ such that $v \preccurlyeq_{E\cup B} w$, which forces $Unif_{E\cup B}(w = p) \neq \emptyset$. $\square$