Program Verification: Lecture 23

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Extending Narrowing-Based Infinite-State Model Checking

So far, the narrowing-based symbolic model checking of infinite-state systems applies to topmost theories of the form $\mathcal{R} = (\Sigma, B, R)$, where B is a set of equational axioms.

This leaves out topmost theories of the form, $\mathcal{R} = (\Sigma, E \cup B, R)$. But it is quite common for concurrent systems to update their states by means of auxiliary functions defined by equations E modulo B. Can we extend narrowing to richer topmost theories?

Besides symbolic verification of invariants by narrowing, since LTL allows verification of richer properties than just invariants, this raises the question: Could symbolic model checking of invariants be extended to symbolic LTL model checking of infinite-state systems?

In order to answer these two questions (in the positive), this lecture introduces a few more symbolic techniques needed for this purpose.

The Need for $E \cup B$-Unification

Symbolic model checking of a topmost rewrite theory $\mathcal{R} = (\Sigma, B, R)$ is based on the modulo B narrowing relation $\leadsto_{R,B}$. If we wish to extend this kind of symbolic model checking to admissible topmost rewrite theories of the form $\mathcal{R} = (\Sigma, E \cup B, R)$, we will need to perform narrowing modulo $E \cup B$ with a relation $\leadsto_{R,E \cup B}$. The definition of narrowing modulo in Lecture 20 remains the same, just changing B by $E \cup B$:

Given a rewrite theory $\mathcal{R} = (\Sigma, E \cup B, R)$, and a term $t \in T_{\Sigma}(X)$, an R-narrowing step modulo $E \cup B$, denoted $t \leadsto^{\theta}_{R,E \cup B} v$ holds iff there exists a non-variable position p in t, a rule $l \to r$ in R, and a B-unifier $\theta \in \mathit{Unif}_{E \cup B}(t|_p = l)$ such that $v = t[r]_p \theta$.

But the million-dolar question is: How do we compute a complete set $\mathit{Unif}_{E \cup B}(t|_p = l)$ of $E \cup B$-unifiers?

$E \cup B$-Unification

The notion of a $E \cup B$-unifier of a Σ-equation $u = v$ is as expected: it is a substitution θ such that $u\theta =_{E \cup B} v\theta$.

The notion of a complete set $\mathit{Unif}_{E \cup B}(u = v)$ of $E \cup B$-unifiers is also as expected: $\mathit{Unif}_{E \cup B}(u = v)$ is a set of $E \cup B$-unifiers of $u = v$ such that for any $E \cup B$-unifier α of $u = v$ there exists a unifier $\gamma \in \mathit{Unif}_{E \cup B}(u = v)$ of which α is an "instance modulo $E \cup B$." That is, there is a substitution δ such that $\alpha =_{E \cup B} \gamma\delta$, where, by definition, given substitutions μ, ν
$\mu =_{E \cup B} \nu \;\Leftrightarrow_{def}\; (\forall x \in \mathit{dom}(\mu) \cup \mathit{dom}(\nu))\; \mu(x) =_{E \cup B} \nu(x)$.

For $E \cup B$ an arbitrary set of equations $E \cup B$, computing such a set $\mathit{Unif}_{E \cup B}(u = v)$ is a very complex matter. But for our purposes we may assume that the oriented equations $\vec{E}$ are convergent modulo B, which makes the task much easier.

$E \cup B$-Unification for $\vec{E}$ Convergent Modulo B

For $\vec{E}$ convergent modulo B, by the Church-Rosser Theorem, for any Σ-equation $u = v$ and substitution θ we have the equivalence:

$$(\dagger) \quad u\theta =_{E \cup B} v\theta \quad \Leftrightarrow \quad (u\theta)!_{\vec{E}/B} =_B (v\theta)!_{\vec{E}/B}$$

This suggest the idea of computing $E \cup B$-unifiers by narrowing! using a theory transformation $(\Sigma, E \cup B) \mapsto (\Sigma^{\equiv}, E^{\equiv} \cup B)$, where:

1. $\Sigma^{\equiv}$ extends Σ by adding: (a) for each connected component $[s]$ in Σ not having a top sort $\top_{[s]}$, such a new top sort $\top_{[s]}$; (b) a new sort *Pred* with a constant tt; and (c) for each connected component $[s]$ in Σ a binary equality predicate $\_ \equiv \_ : \top_{[s]} \; \top_{[s]} \rightarrow \mathit{Pred}$.

2. $E^{\equiv}$ extends E by adding for each connected component $[s]$ in Σ an equation $x : \top_{[s]} \equiv x : \top_{[s]} = tt$.

$E \cup B$-Unification for $\vec{E}$ Convergent Modulo B (II)

It is easy to check (exercise!) that if $\vec{E}$ is convergent modulo B, then $\vec{E}^{\equiv}$ is convergent modulo B. But then (†) becomes:

$$u\theta =_{E\cup B} v\theta \quad \Leftrightarrow \quad (u\theta \equiv v\theta)!_{\vec{E}^{\equiv}/B} = tt.$$

Indeed, any rewriting computation from $u\theta \equiv v\theta$ such that $(u\theta \equiv v\theta)!_{\vec{E}^{\equiv}/B} = tt$ must be of the form:

$$(\ddagger) \quad u\theta \equiv v\theta \rightarrow^{*}_{\vec{E}/B} w' \equiv w' \rightarrow_{\vec{E}^{\equiv}/B} tt$$

with a rule $x{:}\top_{[s]} \equiv x{:}\top_{[s]} \rightarrow tt$ in $\vec{E}^{\equiv} \setminus \vec{E}$ used only in the last step to check $w =_B w'$, i.e., $(u\theta)!_{\vec{E}/B} =_B (v\theta)!_{\vec{E}/B}$. Thus we get:

Theorem. θ is a $E \cup B$-unifier of $u = v$ iff $(u\theta \equiv v\theta)!_{\vec{E}^{\equiv}/B} = tt$.

$E \cup B$-Unification for $\vec{E}$ Convergent Modulo B (III)

This gives us our desired $E \cup B$-unification semi-algorithm, whose proof of correctness follows easily (exercise!) by repeated application of the Lifting Lemma for the rewrite theory $(\Sigma^{\equiv}, B, \vec{E}^{\equiv})$, just by observing that θ is a $E \cup B$-unifier of $u = v$ iff its $\vec{E}/B$-normalized form $\theta!_{\vec{E}/B}$ is so.

Theorem. For $\vec{E}$ convergent modulo B, the set:

$$Unif_{E \cup B}(u = v) =_{def} \{\gamma \mid (u \equiv v) \overset{\gamma}{\leadsto}{}^{*}_{\vec{E}^{\equiv},B} tt\}$$

is a complete set of $E \cup B$-unifiers of the equation $u = v$.

For narrowing-based model checking, we obtain as an immediate corollary the following vast generalization of the Completeness of Narrowing Search Theorem in Lecture 20 for topmost theories:

Symbolic Model Checking of Topmost Rewrite Theories

For a topmost $\mathcal{R} = (\Sigma, E \cup B, R)$, narrowing with R modulo axioms $E \cup B$ supports the following symbolic reachability analysis result:

Theorem (Completeness of Narrowing Search). For a topmost and coherent $\mathcal{R} = (\Sigma, E \cup B, R)$ with $\vec{E}$ convergent modulo B, 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 $R, (E \cup B)$-narrowing sequence $t \overset{\theta}{\leadsto}^*_{R,(E \cup B)} v$ such that there is a $E \cup B$-unifier $\gamma \in \mathit{Unif}_{E \cup B}(u = v)$.

The proof, by applying the Lifting Lemma, is left as an exercise.

Performance Barriers for Symbolic Reachability

In the above, generalized Completeness of Narrowing Search Theorem, narrowing happens at two levels: (i) with R modulo $E \cup B$ for reachability analysis, and (ii) with $\vec{E}^{\equiv}$ modulo B for computing $E \cup B$-unifiers.

From a performance point of view this is very challenging, since this gives us what we might describe as a "nested narrowing tree," wich can by infinite at each of its levels and therefore huge.

To overcome this performance barrier, the technique of folding an infinite narrowing tree into a (hopefully finite) narrowing graph can be applied at both levels. For the symbolic reachability level with $\rightsquigarrow^*_{R,(E \cup B)}$ we have already seen this in Lecture 20. Likewise, for $\vec{E}, B$-narrowing with $\vec{E}$ convergent modulo B ($\vec{E}^{\equiv}, B$-narrowing is just a special case), folding variant narrowing delivers the goods:

Folding Variant Narrowing

Folding Variant Narrowing, proposed by S. Escobar, R. Sasse and J. Meseguer[a] for theories $(\Sigma, E \cup B)$ with $\vec{E}$ convergent modulo B, folds the $\vec{E}, B$-narrowing tree of t into a graph in a breadth first manner as follows:

1. It considers only paths $t \overset{\theta}{\leadsto}{}^{n}_{\vec{E},B} u$ in the narrowing tree such that u and θ are $\vec{E}, B$-normalized.
2. For any such path $t \overset{\theta}{\leadsto}{}^{n}_{\vec{E},B} u$, if there is another such different path $t \overset{\theta'}{\leadsto}{}^{m}_{\vec{E},B} u'$ with $m \leq n$ and a B-matching substitution γ such that: (i) $u =_B u'\gamma$, and (ii) $\theta =_B \theta'\gamma$, then the node u is folded into the more general node u'.

[a]"Folding variant narrowing and optimal variant termination", J. Alg. & Log. Prog., 81, 898–928, 2012.

Folding Variant Narrowing (II)

The pairs (u, θ) associated to paths $t \overset{\theta}{\leadsto}{}^{n}_{\vec{E},B}\ u$ in such a graph are called the $\vec{E}, B$-variants of t; and the graph thus obtained is called the folding variant narrowing graph of t.

Maude supports the enumeration of all variants in the narrowing graph of t by the `get variants :` t `.` command (§14.4, Maude Manual). It also supports variant-based $E \cup B$-unification when $\vec{E}$ is convergent modulo B with the `variant unify` command (§14.9, Maude Manual).

$(\Sigma, E \cup B)$ enjoys the finite variant property (FVP) iff for any Σ-term t its folding variant graph is finite. This property holds iff for each $f : s_1 \ldots s_n \to s$ in Σ the folding variant graph of $f(x_1 \!:\! s_1, \ldots, x_n \!:\! s_n)$ is finite, which can be checked in Maude.

Symbolic Model Checking for $\mathcal{R} = (\Sigma, E \cup B, R)$ when $E \cup B$ is FVP

It is easy to check (exercise!) that if $(\Sigma, E \cup B)$ is FVP, then $(\Sigma^{\equiv}, E^{\equiv} \cup B)$ is also FVP. This means that when $(\Sigma, E \cup B)$ is FVP variant unification provides an effectively computable finite and complete set of $E \cup B$-unifiers for any unification problem.

Thus, for $(\Sigma, E \cup B)$ FVP, the Completeness of Narrowing Search Theorem for a rewrite theory $\mathcal{R} = (\Sigma, E \cup B, R)$ makes symbolic model checking tractable. In fact, it is supported by the same `fvu-narrow` command already discussed in Lecture 20.

In summary, we have generalized the symbolic model checking results from Lecture 20 to: (i) any topmost rewrite theory $\mathcal{R} = (\Sigma, E \cup B, R)$ with $\vec{E}$ convergent modulo B, and (ii) made it tractable when $E \cup B$ is FVP. For symbolic model checking examples when $E \cup B$ is FVP, see §15 of the The Maude Manual.