CS 576 Lecture 6 2/2/17

J. Meseguer

1. Narrowing as Symbolic Execution: the Very Idea

Consider a rewrite theory. For example,

$$R = \begin{cases} x + 0 \to x \\ x + s(y) \to s(x+y) \end{cases}$$

Q: Can we rewrite $N+M$?

A: No

Q: Can we symbolically execute $N+M$?

A: Yes

Q: How?

A: By finding most general *instances* of $N+M$ that can be rewritten

Q: How?

A: By unifying a lefthand side of a rule with a non-variable subterm of the term to be symbolically executed. This is called *narrowing*.

In our example, the only non-variable subterm of $N+M$ is $N+M$ itself, which unifies with $x+0$ with $\alpha = \begin{Bmatrix} N \mapsto x' \\ M \mapsto 0 \end{Bmatrix}$, and with $x+s(y)$ with $\beta = \begin{Bmatrix} N \mapsto x' \\ M \mapsto s(y) \end{Bmatrix}$

allowing the rewrites $x'+0 \to x'$, and $x'+s(y') \longrightarrow s(x'+y')$

We write this symbolic executions as:

$$N+M \overset{\alpha}{\underset{R}{\leadsto}} x' \qquad N+M \overset{\beta}{\underset{R}{\leadsto}} s(x'+y')$$

and call them narrowing steps. Of course, we can keep going, and obtain a "narrowing tree" of symbolic executions:

$$\begin{tikzcd}[column sep=tiny]
 & N+M \arrow[dl, squiggly] \arrow[dr, squiggly] & & & & \\
x' & & s(x'+y') \arrow[dl, squiggly] \arrow[dr, squiggly] & & & \\
 & s(x'') & & s(s(x''+y'')) \arrow[dl, squiggly] \arrow[dr, squiggly] & & \\
 & & s(s(x''')) & & s(s(s(x'''+y'''))) \arrow[dl, squiggly] \arrow[dr, squiggly] & \\
 & & & s(s(s(x^{iv}))) & & \cdots
\end{tikzcd}$$

2. <u>Definition of Narrowing</u>

We may as well consider general rewrite theories of the form $\mathcal{R}=(\Sigma, B, R)$ that are strictly B-coherent, and such that B has B-unification algorithm. This will allow "symbolic execution modulo B by narrowing".

Before defining narrowing, we will make some hygiene assumptions to avoid any kind of silly "variable nonsense".

Given $\mathcal{R}=(\Sigma,B,R)$ by a rule of R <u>standardized apart</u>, denoted $(l' \to r') \ll R$ we mean that there is a variable renaming ρ and a rule $(l \to r) \in R$ such that: (i) $(l' \to r') = (l \to r)\rho$, and (ii) $vars(l \to r)$ are <u>disjoint</u> from all variables previously met in any computation. In our case, such computations will be narrowing sequences (to be defined below). Likewise, we say that a substitution θ is <u>standardized apart</u> if the variables in $ran(\theta)$ are <u>disjoint</u> from all variables previously met in any computation.

<u>Definition (Narrowing)</u>. Let $\mathcal{R}=(\Sigma, B, R)$ be a strictly B-coherent rewrite theory and $u \in T_\Sigma(X)$. Then the R,B-narrowing relation $u \overset{\eta}{\underset{R,B}{\leadsto}} v$ holds for some $v \in T_\Sigma(X)$ if there is a standardized apart $l' \to r' \ll R$ non-variable position $p \in pos_\Sigma(u)$, and standardized apart idempotent substitution $\eta \in Unif_B(l' = u|_p)$ such that $v = (u[r]_p)\eta$.

We then define a narrowing sequence as a sequence

$$u_0 \overset{\eta_1}{\underset{R,B}{\rightsquigarrow}} u_1 \overset{\eta_2}{\underset{R,B}{\rightsquigarrow}} u_2 \overset{\eta_3}{\underset{R,B}{\rightsquigarrow}} u_3 \cdots u_{n-1} \overset{\eta_n}{\rightsquigarrow} u_n$$

for $n \geq 0$, where for the case $n = 0$, we have $u_n = u_0$, and otherwise each $l_i \to r_i \ll R$ and η_i are standardize apart with respect to all variables involved in the sequence $u_0 \overset{\eta_1}{\underset{R,B}{\rightsquigarrow}} u_1 \cdots u_{i-2} \overset{\alpha_{i-1}}{\underset{R,B}{\rightsquigarrow}} u_{i-1}$, including all variables involved in the $l_j \to r_j$ and η_j, $1 \leq j < i$.

Sometimes we can further decorate a narrowing step with all its ingredients as follows: $u \overset{\eta, p, l' \to r'}{\underset{R,B}{\rightsquigarrow}} v$.

We call the R,B-rewrite $u\eta \xrightarrow[R,B]{} (u[r']_p)\eta$ the rewrite induced by $u \overset{\eta, p, l' \to r'}{\underset{R,B}{\rightsquigarrow}} v$, where $v = (u[r']_p)\eta$.

A key question about narrowing as a symbolic execution method is under what conditions it can "symbolically simulate" at the level of a general pattern $u \in T_\Sigma(X)$ a more concrete R,B-rewrite $u\theta \xrightarrow[R,B]{} v'$ of a pattern instance $u\theta$. This is answered, under some conditions by the following "lifting lemma".

(with B regular & linear)

<u>Lemma</u> (Lifting Lemma). Let $\mathcal{R} = (\Sigma, B, R)$ be strictly B-coherent and such that: (i) $\forall x \in X$, x is R,B-irreducible, and (ii) $\forall\ l \to r \in R$, $l \notin X$ and $vars(r) \subseteq vars(l)$. Let $u \in T_\Sigma(X) - X$, and let θ with $dom(\theta) \subseteq vars(u)$ be an R,B-irreducible substitution, and $u' =_B u\theta$ such that $u' \to_{R,B} v'$. Then there exists a narrowing step $u \overset{\eta}{\underset{R,B}{\rightsquigarrow}} v$ and a R,B-irreducible substitution δ such that $\eta|_{vars(u)}\delta =_B \theta$ and we have

$$\begin{tikzcd} u\eta\delta \arrow[r, "R,B"'] \arrow[d, equal, "B"] & v\delta \arrow[d, equal, "B"] \\ u' \arrow[r, "R,B"'] & v' \end{tikzcd}$$

where $u\eta \to_{R,B} v$ is the R,B-rewrite induced by $u \overset{\eta}{\underset{R,B}{\rightsquigarrow}} v$.

<u>Proof</u>. By strict coherence, since we have $u' \to_{R,B} v'$ and $u' = u\theta$, we also have $u\theta \to_{R,B} v''$ with $v' =_B v''$. But since θ is R,B-irreducible, we must have a non-variable position $p \in pos_\Sigma(u)$ and a rule $l' \to r' \ll R$ standardized apart from $vars(u) \cup vars(u\theta)$ and a B-matching substitution $\alpha \in Match_B(l', u|_p\theta)$ such that $v'' = u\theta[r'\alpha]_p$.
But this means that $\theta \uplus \alpha$ is a B-unifier

of the equation $l' = u|_p$. Therefore, there is a B-unifier $\eta \in Unif_B(l' = u|_p)$, which without loss of generality we may assume: (i) idempotent (by Lemma in pg. 12 of Lecture 5), and (ii) standardized apart from $vars(u) \cup vars(u\theta)$, and a substitution δ with $dom(\delta) \subseteq ran(\eta)$ such that $\eta\delta =_B \theta \dot{\cup} \alpha$. Note, furthermore, that, since η is idempotent and $vars(l') \cap vars(u|_p) = \emptyset$, η is of the form $\eta = \gamma \dot{\cup} \beta$, with: $dom(\gamma) = vars(u|_p)$, $dom(\beta) = vars(l')$, and both γ and β idempotent, and since B is regular and $u|_p\gamma =_B l'\beta$ and η idempotent unifier, must have $ran(\eta) = ran(\beta) = ran(\gamma) \subseteq$ [illegible], and since $\eta\delta =_B \theta \dot{\cup} \alpha$ we also have $\gamma\delta =_B \theta$ with $dom(\delta) \subseteq ran(\gamma)$ and therefore, by Lemma in pg. 14 of Lecture 5 both γ and δ are R,B-irreducible. Note that we also have $\beta\delta =_B \alpha$. But since $u \overset{\eta}{\rightsquigarrow} (u[r']_p)\eta = v$, we also have:

By Lemma in pg. 13 of Lecture 5

$$
\begin{tikzcd}
u\eta\delta \arrow[r, "R,B"'] \arrow[d, equal] & v\delta = (u\gamma[r'\beta]_p)\delta \arrow[dd, equal, "B"] \\
u\gamma\delta \arrow[d, equal, "B"] & \\
u\theta \arrow[r, "R,B"'] \arrow[d, equal, "B"] & v'' = u\theta[r'\alpha]_p \arrow[d, equal, "B"] \\
u' \arrow[r, "R,B"'] & v'
\end{tikzcd}
$$

as desired. □

We then say that the rewrite $u' \to_{R,B} v'$ "lifts" to the rewrite $u\eta \to_{R,B} v$ induced by $u \overset{\eta}{\rightsquigarrow}_{R,B} v$, and that $u\eta \to_{R,B} v$ "covers" $u' \to_{R,B} v'$ as its instance $u\eta\delta \to_{R,B} v\delta$ "up to B-equality".

<u>Theorem</u>. (Lifting Theorem for R,B-rewrite sequences). Let $\mathcal{R} = (\Sigma, B, R)$, $u \in T_\Sigma(X) - X$, and θ satisfy the assumptions in the Lifting Lemma, and let

$$u' \to_{R,B} v'_1 \to_{R,B} v'_2 \cdots v'_{n-1} \to_{R,B} v'_n \quad \text{with } u' =_B u\theta$$

be a rewrite sequence, $n \geq 0$. Then there is a narrowing sequence $u \overset{\eta_1}{\rightsquigarrow} v_1 \overset{\eta_2}{\rightsquigarrow} v_2 \cdots v_{n-1} \overset{\eta_n}{\rightsquigarrow} v_n$ inducing a rewrite $u\eta_1 \cdots \eta_n \to_{R,B} v_1\eta_2 \cdots \eta_n \cdots v_{n-1}\eta_n \to v_n$, and there is an R,B-normalized substitution δ_n such that $(\eta_1 \cdots \eta_n)|_{vars(u)}\delta_n =_B \theta$, and such that, applying δ_n to such an induced rewrite we get:

$$(\star) \quad \begin{tikzcd} u\eta_1 \cdots \eta_n \delta_n \arrow[r, "*", "R,B"'] \arrow[d, no head, "B"] & v_n\delta_n \arrow[d, no head, "B"] \\ u' \arrow[r, "*", "R,B"'] & v'_n \end{tikzcd}$$

<u>Proof</u>. By induction on n. For $n = 0$, $u' = v'_0$, $u = v$, and $\delta_0 = \theta$, and we are done. Assume the result holds

For n, and let us prove it for $n+1$. By the induction hypothesis we have an induced rewrite sequence and an R,B-irreducible δ_n such that (✡) holds. But by the Lifting Lemma we then have $v_n \overset{\eta_{n+1}}{\rightsquigarrow} v_{n+1}$

$$\begin{cases} \text{with } \eta_{n+1} = \gamma_{n+1} \overset{+}{\cup} \beta_{n+1} \\ \text{and } \delta_{n+1} \ R,B\text{-irred.} \\ \quad \text{with } dom(\delta_{n+1}) \subseteq vars(v_{n+1}) \\ \text{and } \alpha_{n+1} \in Match_B(l'^{n+1}, v_n|_p \delta_n) \end{cases}$$

s.t. $$\begin{cases} \delta_n =_B \gamma_{n+1}\delta_{n+1} \\ \alpha_{n+1} =_B \beta_{n+1}\delta_{n+1} \\ \eta_{n+1}\delta_{n+1} =_B \delta_n \overset{+}{\cup} \alpha_{n+1} \end{cases}$$

Therefore we have an induced rewrite $v_n\eta_{n+1} \xrightarrow[R,B]{} v_{n+1}$ ($\boxtimes$)

such that

$$\begin{tikzcd} v_n\eta_{n+1}\delta_{n+1} \arrow[r, "R,B"'] \arrow[d, equal, "B"] \arrow[dr, phantom, "(\otimes)"] & v_{n+1}\delta_{n+1} \arrow[d, equal, "B"] \\ v'_n \arrow[r, "R,B"'] & v'_{n+1} \end{tikzcd}$$

By applying η_{n+1} to the induced rewrite from the I.H. and composing with $\boxtimes$ we get: $u\eta_1 \cdots \eta_n\eta_{n+1} \xrightarrow[R,B]{*} v_n\eta_{n+1} \xrightarrow[R,B]{} v_{n+1}$. By $\eta_{n+1}\delta_{n+1} =_B \delta_n \overset{+}{\cup} \alpha_{n+1}$ and $l'^{n+1} \to r'^{n+1} \in R$ we get:

$$\begin{tikzcd} u\eta_1\cdots\eta_n\eta_{n+1}\delta_{n+1} \arrow[r, "*", "R,B"'] \arrow[d, equal, "B"] & v_n\eta_{n+1}\delta_{n+1} \arrow[r, "R,B"'] \arrow[d, equal, "B"] & v_{n+1}\delta_{n+1} \arrow[ddd, equal, "B"] \\ u\eta_1\cdots\eta_n(\delta_n \overset{+}{\cup} \alpha_{n+1}) \arrow[d, equal] & v_n(\delta_n \overset{+}{\cup} \alpha_{n+1}) \arrow[d, equal] \arrow[ddr, phantom, "\otimes"] & \\ u\eta_1\cdots\eta_n\delta_n \arrow[r, "*", "R,B"'] \arrow[d, equal, "B"] \arrow[dr, phantom, "✡ \ \mathrm{I.H.}"] & v_n\delta_n \arrow[d, equal, "B"] & \\ u' \arrow[r, "*", "R,B"'] & v'_n \arrow[r, "R,B"'] & v'_{n+1} \end{tikzcd}$$

The last thing that needs to be checked is that

$$(\eta_1 \cdots \eta_{n+1})|_{vars(u)}\, \delta_{n+1} =_B \theta$$

But note that by the induction hypothesis we have $(\eta_1 \cdots \eta_n)|_{vars(u)}\, \delta_n =_B \theta$,

that $(\eta_1 \cdots \eta_n\, \eta_{n+1})|_{vars(u)} = (\eta_1 \cdots \eta_n)|_{vars(u)}\, \gamma_{n+1}$

and therefore, $(\eta_1 \cdots \eta_n \eta_{n+1})|_{vars(u)}\, \delta_{n+1} =$

$$= (\eta_1 \cdots \eta_n)|_{vars(u)}\, \gamma_{n+1}\, \delta_{n+1} =_B (\eta_1 \cdots \eta_n)|_{vars(u)}\, \delta_n =_B \theta. \quad \square$$

we then say that the rewrite sequence $u \xrightarrow[R,B]{*} v'_n$ "lifts" to the induced rewrite $u\eta_1 \cdots \eta_n \xrightarrow[R,B]{*} v_n$ induced by

$u \overset{\eta_1 \cdots \eta_n}{\underset{R,B}{\curvearrowright^*}} v_n$ and that such an induced rewrites "covers" $u \xrightarrow[R,B]{*} v'_n$ as an instance $u\eta_1 \cdots \eta_n \delta_n \rightarrow v_n \delta_n$ up to B-equality.

3. The $(\Sigma, B, \vec{E}) \mapsto (\Sigma^{\equiv}, B, \vec{E}^{\equiv})$ Transformation

Let $(\Sigma, B, \vec{E})$ be a decomposition of $(\Sigma, B \cup E)$.

We can extend Σ to $\Sigma^{\equiv}$ by: (i) adding a fresh new kind Eq with constant tt, (ii) adding for each top sort s of each connected component of sorts in Σ an operator $\_\equiv\_ : s\ s \rightarrow Eq$. Likewise, we can extend E to $E^{\equiv}$ adding to E the equations $(x:s \equiv x:s) = tt$, for each top sort s of each connected components of sorts in Σ.

Lemma $(\Sigma^{\equiv}, B, \vec{E}^{\equiv})$ is a decomposition of $(\Sigma, B \cup E^{\equiv})$.

Proof. B-coherence of $\vec{E}^{\equiv}$ follows easily from that of $\vec{E}$. For confluence we just need to prove that each term of the form $u \equiv v$ is confluent. But there are two possibilities: $u!_{E,B} =_B v!_{E,B}$, in which case any rewrite sequence $u \equiv v \xrightarrow[\vec{E}^{\equiv},B]{*} u' \equiv v'$

can be extended to $u \equiv v \xrightarrow[\vec{E}^{\equiv},B]{*} tt$, with $(u \equiv v)!_{\vec{E}^{\equiv},B} = tt$,

or $u!_{E,B} \neq_B v!_{E,B}$, in which it can be extended to

$$u \equiv v \xrightarrow{*} u!_{\vec{E},B} \equiv v!_{\vec{E},B} \quad \text{with} \quad (u \equiv v)!_{\vec{E}^{\equiv},B} = u!_{\vec{E},B} \equiv v!_{\vec{E},B}$$

in either case, we get confluence.

To see termination, again it is enough to show that any term $u \equiv v$ terminates, but this has just been shown above. More precisely, any non-terminating sequence must be of the form

$$u \equiv v \to_{\vec{E},B} u_1 \equiv v_1 \to_{\vec{E},B} u_2 \equiv v_2 \cdots \to_{\vec{E},B} u_n \equiv v_n \to \cdots$$

so that there must be a non-terminating sequence on the left or on the right, contradicting $\to_{\vec{E},B}$ terminating. □

<u>Lemma</u>. $u =_{E \cup B} v$ iff $(u \equiv v)!_{\vec{E}^{\equiv},B} = tt$

<u>Proof</u>. From the Church-Rosser Theorem for $(\Sigma, B, \vec{E})$ plus the above proof of confluence of $(\Sigma^{\equiv}, B, \vec{E}^{\equiv})$. □

4. A Narrowing-Based Unification Semi-Algorithm

<u>Theorem</u> Let (Σ, B, R) be a decomposition of $(\Sigma, E \cup B)$ where (Σ, B, R) satisfies the conditions in the Lifting Lemma and B has a finitary B-unification algorithm. Then

The recursively enumerable set

$$Unif_{E\cup B}(u=v) = \{ \eta_1 \cdots \eta_n \mid u \equiv v \overset{\eta_1 \cdots \eta_n}{\rightsquigarrow}{}^{+}_{\vec{E}^{\equiv},B}\ tt \}$$

provides a complete set of $E \cup B$-unifiers for the equation $u = v$, and therefore a semi-algorithm.

<u>Proof</u>. By the Church-Rosser Theorem, θ is a $E\cup B$-unifier of $u = v$ iff $\theta!_{E,B}$ is

iff $$u\theta \equiv v\theta \xrightarrow[\vec{E},B]{*} u(\theta!_{E,B}) \equiv v(\theta!_{E,B}) \xrightarrow[\vec{E},B]{*} u!_{\vec{E},B} \equiv v!_{\vec{E},B} \rightarrow_{E^{\equiv},B} tt.$$

Therefore, by the Lifting Theorem applied to $u \equiv v$ and the normalized substitution $\theta!_{E,B}$ there is a narrowing sequence $u \equiv v \overset{\eta_1 \cdots \eta_n}{\rightsquigarrow}{}^{+}\ tt$ and a $\vec{E}^{\equiv},B$-normalized substitution δ_n such that $(\eta_1 \cdots \eta_n)|_{vars(u\equiv v)}\delta_n =_B \theta!_{\vec{E},B}$ and

$$\begin{array}{ccc}
(u \equiv v)\eta_1 \cdots \eta_m \delta_n & \xrightarrow[E^{\equiv},B]{+} & tt = tt\delta_n \\
\|_B & & \| \\
(u \equiv v)\theta!_{\vec{E},B} & \xrightarrow[E^{\equiv},B]{+} & tt
\end{array}$$

But this shows that: (i) $(\eta_1 \cdots \eta_n)|_{vars(u\equiv v)}$ is a $E\cup B$-unifier of $u = v$, and (ii) that $(\eta_1 \cdots \eta_n)|_{vars(u\equiv v)} \sqsupseteq_{E\cup B} \theta$, as desired. $\square$

<u>Remark</u>. It might seem that this approach is <u>not sufficiently general</u>, since it does not explicitly handle the case of a system of Σ-equations

$$\varphi = \bigwedge_{j=1}^{n} u_j = v_j$$

But this is essentially an optical illusion: if $s_1, .., s_n$ are the top sorts of $u_1, .., u_n$, we just need to add a tupling operator $\langle \_, \_, \ldots, \_ \rangle : s_1 \ldots s_n \to Tuple$ to $\Sigma^{\equiv}$ and observe that θ is an $E \cup B$ - unifier of φ iff θ is an $E \cup B$ - unifier of $\langle u_1, .., u_n \rangle = \langle v_1, .., v_n \rangle$, so that $E \cup B$ - unifiers of φ can be computed by $\vec{E}^{\equiv}, B$ - narrowing sequences

$$\langle u_1, .., u_n \rangle \equiv \langle v_1, .., v_n \rangle \overset{\eta_1 \cdots \eta_n}{\rightsquigarrow}{}^{*} tt .$$

<u>Remark</u>. In the $E \cup B$ - unification theorem of pg. 10, the requirement that B has a <u>finitary</u> B-unification algorithm is not really needed: one can also recursively enumerate all $\eta_1 \ldots \eta_n$ such that $u \equiv v \overset{+}{\rightsquigarrow}_{\vec{E}^{\equiv}, B} tt$ when B has an infinitary unification algorithm.