ISR: Lecture 9

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Executing Rewrite Theories

Rewriting logic's rules of deduction allow us to reason correctly. But because they are based on the general equational deduction relation, which in general is undecidable, it may be undecidable whether an inference step can be taken. Consider, for example, the inference rule:

Equality. $$\frac{(\forall X)\ u \longrightarrow v \quad E \vdash (\forall X) u = u' \quad E \vdash (\forall X) v = v'}{(\forall X)\ u' \longrightarrow v'}$$

In general it may undecidable whether E can prove u and u' equal. Furthermore, even if E is decidable, there may be an infinite number of terms in E-equivalence classes; so we may need to start an infinite search for a term u we can rewrite. Therefore, to effectively decide whether the **Equality** rule can be applied we need stronger assumptions on E.

Executing Rewrite Theories (II)

The best possible situation is assuming that E is a collection B of equational axioms, such as associativity, commutativity, and identity, for which we have an B-matching algorithm, so that given a rewrite rule $t \longrightarrow t'$ and terms u', v' it becomes decidable whether we can perform a one-step rewrite $u \longrightarrow v$ using $t \longrightarrow t'$ with $u =_B u'$ and $v =_B v'$. Recall Lecture 5, where (changing E there by R here) the analogue of the **Equality** inference step was achieved with the decidable relation $\longrightarrow_{R/B}$.

In practice, what may be reasonable to have as equations in a rewrite theory $\mathcal{R}$ is a disjoint union $E \cup B$ with B as above and E ground confluent, sort-decreasing, and terminating modulo B, that is, the usual executability assumptions for functional modules.

Executing Rewrite Theories (III)

The key idea is now the following. Given a rewrite theory $\mathcal{R} = (\Sigma, E \cup B, \phi, R)$ with $E \cup B$ having the just-mentioned executability assumptions we can simulate it and make it decidable by means of the rewrite theory $\hat{\mathcal{R}} = (\Sigma, B, \phi, \vec{E} \cup R)$, where, by definition, $\vec{E} = \{t \longrightarrow t' \mid (t = t') \in E\}$.

In what follows we will assume that both the equations E and the rules R are unconditional, and that for each rule $t \longrightarrow t'$ in R, $vars(t') \subseteq vars(t)$. The ideas can be generalized to the conditional case but this requires a somewhat more complex transformed theory $\hat{\mathcal{R}}$. The equivalence we want is:

$$\mathcal{R} \vdash t \longrightarrow t' \quad \Leftrightarrow \quad \hat{\mathcal{R}} \vdash can_{E/B}(t) \longrightarrow can_{E/B}(t')$$

Executing Rewrite Theories (IV)

It is easy to prove by induction on the depth of rewrite proofs that we always have the implication

$$\mathcal{R} \vdash t \longrightarrow t' \quad \Leftarrow \quad \hat{\mathcal{R}} \vdash can_{E/B}(t) \longrightarrow can_{E/B}(t')$$

The hard part is the reverse implication, which in general may fail to hold. For example, if we have $B = \emptyset$, $E = \{a = c\}$, and $R = \{a \longrightarrow b\}$, we obviously have $\mathcal{R} \vdash a \longrightarrow b$, but we cannot prove $\hat{\mathcal{R}} \vdash c \longrightarrow b$.

The question then becomes one of finding suitable checkable conditions under which the above implication becomes an equivalence. This is to the topic of coherence, a property studied by P. Viry (TCS 285, 487–517, 2002), and extended to the conditional order-sorted case by Durán&Meseguer (JLAP, 81, 816–850, 2012).

Coherence

Assuming E confluent (resp. ground confluent), sort-decreasing and terminating modulo B, we say that the rules R are coherent (resp. ground coherent) with E modulo B relative to ϕ if for each Σ-term t (resp. ground Σ-term t) such that $t \longrightarrow^{1}_{R^{\phi}/B} t'$ and $u = can_{E/B}(t)$ we have:

$$\begin{tikzcd}
t \arrow[r, "1", "R^{\phi}/B"'] \arrow[dd, "E/B"', "!"] & t' \arrow[dr, dotted, "!", "E/B"'] & \\
 & & w \\
u \arrow[r, dotted, "1", "R^{\phi}/B"'] & u' \arrow[ur, dotted, "!", "E/B"'] &
\end{tikzcd}$$

Coherence (II)

Throughout we will assume that B is any combination of associativity, commutativity, and identity axioms, and that Σ is preregular modulo B. The relation $\longrightarrow_{E/B}$ is the relation of rewriting with E modulo B zero, one, or more steps, denoted $\longrightarrow^{*}_{E/B}$ in Lecture 5. The symbol "!" indicates a terminating rewrite. The one-step rewriting relation $\longrightarrow^{1}_{R^{\phi}/B}$ with R modulo B is the restriction to frozennes conditions ϕ of what would be denoted $\longrightarrow_{R/B}$ in Lecture 5.

The Viry paper (TCS 285, 487–517, 2002) gives "critical pair-like" conditions to check coherence. The Maude Coherence Checker Tool checks coherence of conditional rules modulo combinations of associativity, commutativity and identity, except associativity without commutativity.

More on Rewriting Proofs

We want to prove that coherence implies our desired equivalence

$$\mathcal{R} \vdash t \longrightarrow t' \quad \Leftrightarrow \quad \hat{\mathcal{R}} \vdash can_{E/B}(t) \longrightarrow can_{E/B}(t')$$

In order to prove this result, it will be technically convenient to use a somewhat more restrictive set of inference rules, yet the proof system $\vdash'$ thus obtained will be equivalent in proving power to the original one. The key point is to make explicit the one-step rewriting relation $\longrightarrow^1$ as a subrelation of $\longrightarrow$. For this we have the rules:

- **Reflexivity**. For each $t \in T_\Sigma(X)$, $\dfrac{}{(\forall X)\ t \longrightarrow t}$
- **Equality**.
$$\frac{(\forall X)\ u \longrightarrow v \quad E \vdash (\forall X) u = u' \quad E \vdash (\forall X) v = v'}{(\forall X)\ u' \longrightarrow v'}$$

- **Congruence'**. For each $f : k_1 \ldots k_n \longrightarrow k$ in Σ, with $j \in \{1, \ldots, n\} - \phi(f)$, with $t_i \in T_\Sigma(X)_{k_i}$, $1 \leq i \leq n$, and with $t'_j \in T_\Sigma(X)_{k_j}$,

$$\frac{(\forall X)\, t_j \longrightarrow^1 t'_j}{(\forall X)\; f(t_1, \ldots, t_j, \ldots, t_n) \longrightarrow^1 f(t_1, \ldots, t'_j, \ldots, t_n)}$$

- **Replacement'**. For each rule in R of the form,

$$l : (\forall X)\, t \longrightarrow t' \;\Leftarrow\; (\bigwedge_i u_i = u'_i) \wedge (\bigwedge_j w_j \longrightarrow w'_j)$$

  and finite substitution $\theta : X \longrightarrow T_\Sigma(Y)$,

$$\frac{(\bigwedge_i (\forall Y)\; u_i\theta = u'_i\theta) \quad \wedge (\bigwedge_j (\forall Y)\; w_j\theta \longrightarrow w'_k\theta)}{(\forall Y)\; t\theta \longrightarrow^1 t'\theta}$$

- **Transitivity'**

$$\frac{(\forall X)\; t_1 \longrightarrow^1 t_2 \qquad (\forall X)\; t_2 \longrightarrow t_3}{(\forall X)\; t_1 \longrightarrow t_3}$$

More on Rewriting Proofs (II)

The two main lemmas below about this equivalent inference system have somewhat tedious but essentially unproblematic proofs by induction, that are left as exercises.

Lemma (Equivalence)

$$\mathcal{R} \vdash (\forall X)\, t \longrightarrow t' \quad \Leftrightarrow \quad \mathcal{R} \vdash' (\forall X)\, t \longrightarrow t'$$

Lemma (Sequentialization) Wenever we have $\mathcal{R} \vdash' (\forall X)\, t \longrightarrow t'$ there is an $n \geq 0$ and proofs $\mathcal{R} \vdash' (\forall X)\, t_i \longrightarrow^1 t'_i$, $1 \leq i \leq n$, such that: $E \vdash (\forall X)\, t = t_1$, $E \vdash (\forall X)\, t'_i = t_{i+1}$, $1 \leq i \leq n$, and $E \vdash (\forall X)\, t'_n = t'$.

Semantic Equivalence through Coherence

We are now ready to prove our main result about the semantic equivalence of $\mathcal{R}$ and $\hat{\mathcal{R}}$.

Theorem. For $\mathcal{R}$ an unconditional rewrite theory satisfying the assumptions on Σ, E, B, and R already mentioned, and such that R is coherent with E modulo B w.r.t. ϕ we have:

$$\mathcal{R} \vdash t \longrightarrow t' \quad \Leftrightarrow \quad \hat{\mathcal{R}} \vdash can_{E/B}(t) \longrightarrow can_{E/B}(t')$$

Proof: We only need to prove the implication $(\Rightarrow)$. By the Equivalence and Sequentialization Lemmas there is an $n \geq 0$ and proofs $\mathcal{R} \vdash' (\forall X)\, t_i \longrightarrow^1 t'_i$, $1 \leq i \leq n$, such that:
$E \cup B \vdash (\forall X)\, t = t_1$, $E \cup B \vdash (\forall X)\, t'_i = t_{i+1}$, $1 \leq i \leq n$, and
$E \cup B \vdash (\forall X)\, t'_n = t'$. We can now proceed by induction on n.

Semantic Equivalence through Coherence (II)

For $n = 0$ we have $can_{E/B}(t) = can_{E/B}(t')$ and a proof in $\hat{\mathcal{R}}$ can be found by **Reflexivity** and **Equality**. Let us assume that the result holds for n and let us prove it for $n+1$. The point is then that, by repeated application of **Equality** and **Transitivity**, we can build proofs $\mathcal{R} \vdash' (\forall X)\, t \longrightarrow t_{n+1}$ and $\mathcal{R} \vdash' (\forall X)\, t_{n+1} \longrightarrow t'$, where the first proof can be sequentialized with n 1-step rewrites, and the second with only one 1-step rewrite. By the induction hypothesis we then have $\hat{\mathcal{R}} \vdash can_{E/B}(t) \longrightarrow can_{E/B}(t_{n+1})$. So we will be done by repeatedly using **Transitivity'** if we can show $\hat{\mathcal{R}} \vdash can_{E/B}(t_{n+1}) \longrightarrow can_{E/B}(t')$. Note that we have a proof $\mathcal{R}(\forall X)\ \vdash' t_{n+1} \longrightarrow^{1} t'_{n+1}$, which by its very definition makes no use of **Equality**. Therefore we have a one-step rewrite $t_{n+1} \longrightarrow^{1}_{R^{\phi}} t'_{n+1}$, and a fortiori $t_{n+1} \longrightarrow^{1}_{R^{\phi}/B} t'_{n+1}$.

Semantic Equivalence through Coherence (III)

We also have a proof $E \cup B \vdash (\forall X)\, t'_{n+1} = t'$; therefore $can_{E/B}(t'_{n+1}) = can_{E/B}(t')$. The desired proof of $\hat{\mathcal{R}} \vdash can_{E/B}(t_{n+1}) \longrightarrow can_{E/B}(t')$ then follows by Coherence (see diagram) by repeated application of **Equality** and **Transitivity**. q.e.d.

$$\begin{tikzcd}
t_{n+1} \arrow[rr, "1", "R^{\phi}/B"'] \arrow[dd, "E/B"', "!"] & & t'_{n+1} \arrow[dr, dotted, "!", "E/B"'] & \\
 & & & can_{E/A}(t') \\
can_{E/A}(t_{n+1}) \arrow[rr, dotted, "1", "R^{\phi}/B"'] & & u' \arrow[ur, dotted, "!", "E/B"'] &
\end{tikzcd}$$