1. Executability Conditions for Rewrite Theories

CS 524
Lecture 24
J. Meseguer

Given a rewrite theory $\mathcal{R} = (\Sigma, \phi, E \cup B, R)$ the problem we may have is that the relation $\xrightarrow{}_{\vec{R}/E\cup B}$ that faithfully describes ~~the~~ <u>one-step transitions</u> in $\mathcal{J}_{\mathcal{R}}$, in the sense that we have the equivalence

$$[u] \xrightarrow[\mathcal{R}]{} [v] \iff [u] \xrightarrow[R^{\phi}/E\cup B]{} [v]$$

may be <u>undecidable</u>: we may not be able to <u>know</u> whether a single step from u is possible with $\xrightarrow[R^{\phi}/E\cup B]{}$.

This is obviously a <u>bad</u> situation. But it is quite understandable. The problem is that we have not yet identified <u>executability</u> <u>conditions</u> for $\mathcal{R}$, similar to those for a Maude <u>functional</u> <u>module</u> where we require the <u>fmod</u> $(\Sigma, E\cup B)$ <u>endfm</u> relation $\xrightarrow[\vec{E}/B]{}$ to be [ground] <u>confluent</u>:

$$\forall \quad \exists \quad
\begin{tikzcd}
 & t \arrow[dl, "*"', "\vec{E}/B"] \arrow[dr, "*", "\vec{E}/B"'] & \\
u \arrow[dr, dashed, "\vec{E}/B"'] & & v \arrow[dl, dashed, "\vec{E}/B"] \\
 & w =_B w' &
\end{tikzcd}$$

and <u>terminating</u>.

So, the question is: are there similar executability conditions that we should require for a Maude system module of the form: mod $(\Sigma, \phi, E \cup B, R)$ endm ?

Obviously, since the equational part $(\Sigma, E \cup B)$ is just the specification of the module's auxiliary functions to perform functional computations in a state [the module's statics], we should view this part as its functional submodule, and require the same executability conditions as if we had explicitly specified as such: fmod $(\Sigma, E \cup B)$ endfm, and then imported it. That is, $\xrightarrow[\vec{E}/B]{}$ should be [ground] confluent and terminating.

But what about R? We know that $\xrightarrow[R^{\phi}/E \cup B]{}$ is too complicated. Can we simulate by some other relation that makes it decidable whether we can perform a one-step transition under suitable conditions?

A key insight comes from realizing that, thanks to the convergence [confluence + termination] of $\xrightarrow[\vec{E}/B]{}$ modulo B, because, up to B-equality, an $E \cup B$-equivalence class $[u]_{E \cup B}$ can be uniquely represented/sumarized by its <u>normal</u> <u>form</u> $u!_{E/B}$.

But computing the E/B - normal form of a term u, say, v, is a <u>relation</u> that can be denoted:

$u \xrightarrow[E/B!]{} v$, and the ~~re~~ composed relation:

$u \xrightarrow[E/B!]{} v \xrightarrow[R^{\phi}/B]{} w$ has two good properties:

(1) $\xrightarrow[E/B!]{} ; \xrightarrow[R^{\phi}/B]{}$, abbreviated to: $\xrightarrow[E/B! R^{\phi}/B]{}$

is decidable; i.e., given two terms u, and w we can <u>decide</u> in a finite number of steps whether $\exists\, w' \in [w]_B$ such that $u \xrightarrow[E/B! R^{\phi}/B]{} w'$

assuming the sets R of rules and E of equations are <u>finite</u>, and B is any combinations of A, C, and

(2) We obviously have ~~that~~ a containment of relations:

$$\xrightarrow[E/B! R^{\phi}/B]{} \subseteq \xrightarrow[\cancel{E\cup} R^{\phi}/E\cup B]{}$$

But what we, obviously would like to have is the equivalence:

$$[u] \xrightarrow[\mathcal{R}]{} [v] \Leftrightarrow [u] \xrightarrow[R^{\emptyset}/E\cup B]{} [v] \Leftrightarrow [u] \xrightarrow[E/B!\,R^{\emptyset}/B]{} [v]$$

To obtain such an equivalence it is a good idea to see clearly what we <u>want</u>, and then find a requirement for it. Notice that, pictorially, we can view successive applications of $\xrightarrow[E/B!\,R^{\emptyset}/B]{}$ as a <u>stairway</u> <u>descent</u> process:

$$\begin{tikzcd}
u_0 \arrow[d, "E/B!"'] \arrow[dr, dashed, "E/B!\,R^{\emptyset}/B"] & & \\
u_0!_{E/B} \arrow[r, "R^{\emptyset}/B"'] & u_1 \arrow[d, "E/B!"'] \arrow[dr, dashed, "E/B!\,R^{\emptyset}/B"] & \\
& u_1!_{E/B} \arrow[r, "R^{\emptyset}/B"'] & u_2 \arrow[d] \cdots \\
& & \vdots \quad \cdots
\end{tikzcd}$$

which is exactly the way the Maude interpreter computes with a system module. Obviously, we always have the implication:

$$[u] \xrightarrow[E/B!\,R^{\emptyset}/B]{} [v] \Rightarrow [u] \xrightarrow[\mathcal{R}]{} [v]$$

The burning question is the <u>completeness</u> question: are we missing something with $\xrightarrow[E/B!R^{\emptyset}/B]{}$? that is, are we missing <u>reachable states</u>? Do we really also have an implication the other way?, i.e.,

$$[u] \xrightarrow[E/B!R^{\emptyset}/B]{} [v] \Leftarrow [u] \xrightarrow[R]{} [v]$$

In general we may not. Suppose Σ has just three constants, a, b, c, $E = \{a = b\}$, which is confluent and terminating!, and $R = \{a \to c\}$. We of course have $[a] \xrightarrow[R]{} [c]$, but we do <u>not</u> have $[a] \xrightarrow[E/B!R^{\emptyset}/B]{} [c]$. In fact,

$\xrightarrow[E!R]{}$ is the <u>empty relation</u>!

This failure of completeness looks like this:

$$\begin{tikzcd} a \arrow[r, "R"'] \arrow[d, "E!"'] & c \\ b & ?? \end{tikzcd}$$

So we just should <u>require</u> that b should <u>simulate</u> a.

This is the so-called coherence property:

$$\forall \quad \begin{tikzcd}
u \arrow[r, "R\emptyset/B"] \arrow[d, "E/B!"'] & w \arrow[r, dashed, "E/B!"] & w!E/B \arrow[d, dotted, no head, "B"] \\
v \arrow[r, dashed, "R\emptyset/B"] & w' \arrow[r, dashed, "E/B!"] & w'!E/B
\end{tikzcd} \quad \exists$$

Or, put even more compactly, but, equivalently:

$$\forall \quad \begin{tikzcd}
u \arrow[r, "R\emptyset/B"] \arrow[d, "E/B"'] & w \arrow[d, dotted, no head, "E\cup B"] \\
v \arrow[r, dashed, "R\emptyset/B"] & w'
\end{tikzcd} \quad \exists$$

We call the property ground coherence if we only require this for ground terms, which is quite enough for our purposes, since $\mathcal{T}_{\mathcal{R}}$ is a model where the states are concrete states, i.e., of the form $[u]_{E\cup B}$ with $u \in T_\Sigma$ a ground term.

And, of course, what we want to prove is:

<u>Main Theorem</u>. If $\mathcal{R} = (\Sigma, \emptyset, E \cup B, R)$ is <u>ground coherent</u>, then we have the equivalence:

$$[u] \xrightarrow[\mathcal{R}]{} [v] \iff [u] \xrightarrow[E/B!R^{\emptyset}/B]{} [v].$$

<u>Proof</u>. We only need to prove the $(\Rightarrow)$ part. But this follows from the following diagram:

$$[u] \xrightarrow[\mathcal{R}]{} [v]$$

$$\iff$$

$\exists u', v'$

$$\begin{tikzcd}
u \arrow[r, equal, "E\cup B"'] \arrow[ddr, "E/B!"', "\text{confl.}"] & u' \arrow[r, "R^{\emptyset}"'] \arrow[d, "E/B!"'] \arrow[dr, phantom, "\text{coh.}"] & v' \arrow[r, equal, "E\cup B"'] \arrow[d, dashed, equal, "E\cup B"] \arrow[dr, phantom, "\text{trans.}"] & v \arrow[dl, dotted, equal, "E\cup B"] \\
& u_0' \arrow[r, dashed, "R^{\emptyset}/B"'] \arrow[d, equal, "B"] & v_0' & \\
& u_0 \arrow[ur, dashed, "R^{\emptyset}/B"'] & &
\end{tikzcd}$$

That is, we have $u \xrightarrow[E/B!R^{\emptyset}/B]{} v_0$ with $v_0 =_{E\cup B} v$

and therefore, $[u] \xrightarrow[E/B!R^{\emptyset}/B]{} [v]$, as desired! $\square$

<u>The big picture</u>! What have we accomplished?

A no mean feat! Namely, to tame the beast of the generally hopeless and undecidable rewriting modulo $E \cup B$ relation $\xrightarrow[R^{\emptyset}/E\cup B]{}$ by a <u>much simpler</u>

<u>relation</u> $\xrightarrow[E/B!\,R^{\emptyset}/B]{}$ under the assumptions that $\xrightarrow[\vec{E}/B]{}$ is <u>convergent</u> and $R^{\emptyset}$ is [ground] <u>coherent</u> with $\vec{E}$ <u>modulo</u> B.

In other words, what the relation $\xrightarrow[E/B!\,R^{\emptyset}/B]{}$ efficiently <u>implements</u> is <u>rewriting modulo</u> $E \cup B$.

<u>A very practical question</u>: Assume that E is already convergent modulo B. How can we:

1) check that $R^{\emptyset}$ is $\boxed{\text{ground}}$ coherent with $\vec{E}$ modulo B?

2) <u>make</u> $R^{\emptyset}$ so in case the check fails?

The answer to 1 is provided by Maude's

Church-Rosser Checker and Coherence Checker tool, whose theoretical foundations are explained in the Durán-Meseguer paper available in the course web page.

A recent answer to (2) has been given by defining an automatable method of <u>coherence completion</u> that makes a rewrite theory $\mathcal{R}$ coherent by a transformation process $\mathcal{R} \mapsto \hat{\mathcal{R}}$, where $\hat{\mathcal{R}}$ is ground coherent and semantically equivalent to $\mathcal{R}$, i.e.

$$[u] \xrightarrow[\mathcal{R}]{} [v] \iff [u] \xrightarrow[\hat{\mathcal{R}}]{} [v]$$

This is also described in a paper by Meseguer on coherence completion also available in the course web page.

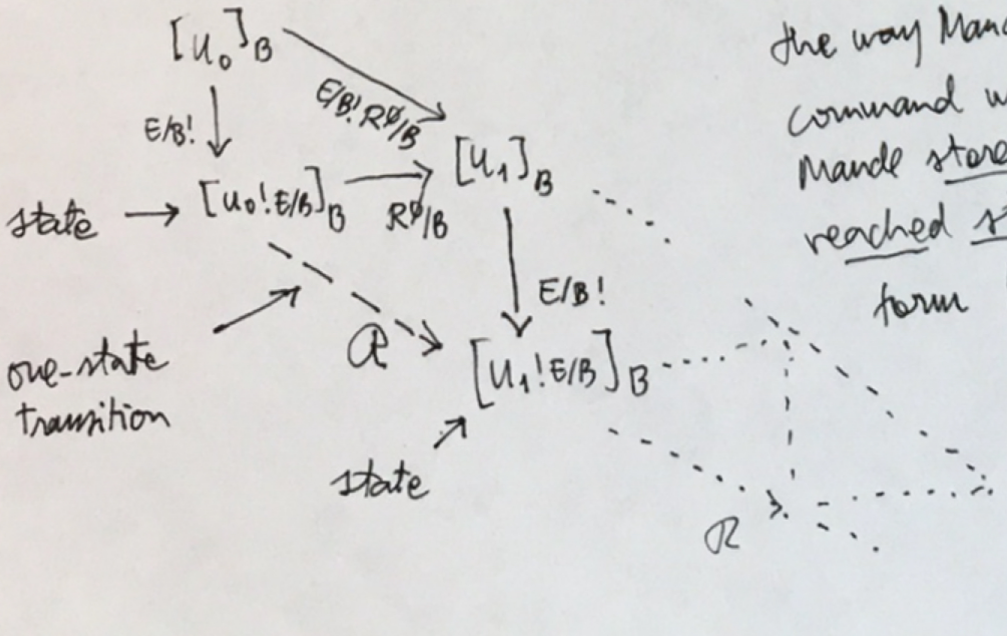
<u>An even more concrete model of $\mathcal{T}_{\mathcal{R}}$</u>

The category $\mathcal{T}_{\mathcal{R}}$ is of course a good <u>mathematical</u> <u>model</u> of the concurrent computations of the system specified by $\mathcal{R}$. But it does not take account of any executability requirements.

But if $\mathcal{R} = (\Sigma, \phi, E \cup B, R)$ has all the good properties of (1) ground convergence of E modulo B, and (2) ground coherence of R^{ϕ} with E modulo B, a much more concrete model of $\mathcal{R}$ is possible, namely the one implicitly used by Maude. In this model states are B-equivalence classes of terms in normal form, i.e., $[u!_{E/B}]_B$ and transitions hold between such states, denoted $[u]_B \xrightarrow[\mathcal{R}]{} [v]_B$ iff $u \xrightarrow[R^{\phi}/B]{} w \xrightarrow[E/B!]{} w_0 =_B v$. That is,

$$[u]_B \xrightarrow[\mathcal{R}]{} [v]_B \iff [u]_B \xrightarrow[R^{\phi}/B;\, E/B!]{} [v]_B$$

This completes the picture in fig. 4 as follows:



This is, for example, the way Maude's search command works: what Maude stores are the reached states of the form $[u_n!_{E/B}]_B$