Program Verification: Lecture 17

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Reachability Models

The models of equational theories are algebras. What are the models of rewrite theories? There are several answers to this question. The simplest answer, which we shall use in this course, is that they are reachability models.

By definition, given a pair (Σ, ϕ), with Σ a membership equational signature and ϕ a function specifying frozenness information for Σ, then a (Σ, ϕ)-reachability model is a pair $\mathcal{A}_{\rightarrow} = (\mathcal{A}, \rightarrow_{\mathcal{A}})$ where:

- $\mathcal{A} = (A, \_\_\_{\mathcal{A}})$ is a Σ-algebra, and
- $\rightarrow_{\mathcal{A}} = \{\rightarrow_{\mathcal{A},k}\}_{k \in K}$ a K-indexed family of binary relations, with $\rightarrow_{\mathcal{A},k} \subseteq A_k^2$ such that:

Reachability Models (II)

1. **Reflexivity and Transitivity**: for each $k \in K$ the relation $\rightarrow_{\mathcal{A},k}$ is reflexive and transitive;

2. **Congruence**: for each $f : k_1 \ldots k_n \longrightarrow k$ in Σ such that $\{1, \ldots, n\} - \phi(f) = \{i_1, \ldots, i_m\} \neq \emptyset$, whenever we have $a_1 \in \mathcal{A}_{k_1}, \ldots, a_n \in \mathcal{A}_{k_n}$ and for $1 \leq j \leq m$ we have $a_{i_j} \rightarrow_{\mathcal{A}_{k_{i_j}}} a'_{i_j}$ then we also have,

$$f_{\mathcal{A}}(a_1, \ldots, a_{i_1}, \ldots, a_{i_m}, \ldots, a_n) \rightarrow_{\mathcal{A},k} f_{\mathcal{A}}(a_1, \ldots, a'_{i_1}, \ldots, a'_{i_m}, \ldots, a_n)$$

Intuitively, $\mathcal{A}$ specifies the states plus functions between them, and $\rightarrow_{\mathcal{A}}$ specifies the reflexive-transitive closure of the transitions between states, which are concurrent because of **Congruence**. Therefore, $\mathcal{A}$ specifies the statics, and $\rightarrow_{\mathcal{A}}$ the dynamics of a concurrent system.

Satisfaction

By definition, a (Σ, ϕ)-reachability model $\mathcal{A}_{\rightarrow} = (\mathcal{A}, \rightarrow_{\mathcal{A}})$ satisfies a rewrite theory $\mathcal{R} = (\Sigma, E, \phi, R)$, written $\mathcal{A}_{\rightarrow} \models \mathcal{R}$, if an only if it satisfies each equation $e \in E$ and each rule in $r \in R$, written $\mathcal{A}_{\rightarrow} \models e$, and $\mathcal{A}_{\rightarrow} \models r$, which means:

- $\mathcal{A} \models E$, and
- for each rewrite rule in R,

  $$l : (\forall X)\, t \longrightarrow t' \;\Leftarrow\; (\bigwedge_i u_i = u_i') \wedge (\bigwedge_j v_j : s_j) \wedge (\bigwedge_l w_l \longrightarrow w_l')$$

  with, say t, t' of kind k, and w_l, w_l' of kind k_l, and for each assignment $a : X \longrightarrow A$ such that: (i) $\bigwedge_i u_i a_{\mathcal{A}} = u_i' a_{\mathcal{A}}$, (ii) $\bigwedge_j v_j a_{\mathcal{A}} : s_j$, and (iii) $\bigwedge_l w_l a_{\mathcal{A}} \rightarrow_{\mathcal{A},k_l} w_l' a_{\mathcal{A}}$, we have,

  $$t a_{\mathcal{A}} \rightarrow_{\mathcal{A},k} t' a_{\mathcal{A}}$$

Soundness and Completeness of Rewriting Logic

The following theorem can be easily proved by induction of the depth of a rewriting logic proof and is left as an exercise:

Theorem (Soundness). For each rewrite theory $\mathcal{R} = (\Sigma, E, \phi, R)$ and (Σ, ϕ)-reachability model $\mathcal{A}_{\rightarrow} = (\mathcal{A}, \rightarrow_{\mathcal{A}})$ such that $\mathcal{A}_{\rightarrow} \models \mathcal{R}$ we have:

$$\mathcal{R} \vdash (\forall X)\, t \longrightarrow t' \quad \Rightarrow \quad \mathcal{A}_{\rightarrow} \models (\forall X)\, t \longrightarrow t'.$$

Rewriting logic is also complete (Bruni and Meseguer, Theoretical Computer Science, 360, 386-414, 2006), that is, we have:

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

Reachabilty Homomorphisms

Given two (Σ, ϕ)-reachability models $\mathcal{A}_{\rightarrow} = (\mathcal{A}, \rightarrow_{\mathcal{A}})$, and $\mathcal{B}_{\rightarrow} = (\mathcal{B}, \rightarrow_{\mathcal{B}})$, a (Σ, ϕ)-reachability homomorphism $h : \mathcal{A}_{\rightarrow} \longrightarrow \mathcal{B}_{\rightarrow}$ is a Σ-homomorphism $h : \mathcal{A} \longrightarrow \mathcal{B}$ such that "preserves reachability," that is, for each $k \in K$, $a \rightarrow_{\mathcal{A},k} a'$ implies $h_k(a) \rightarrow_{\mathcal{B},k} h_k(a')$.

Intuitively, we can think of h as an algebraic (because it preserves the algebraic structure) (stuttering) simulation, because, via h, $\mathcal{B}_{\rightarrow}$ can mimic or simulate any move that $\mathcal{A}_{\rightarrow}$ can make. The "stuttering" qualification indicates the fact that an atomic transition in $\mathcal{A}_{\rightarrow}$ may be simulated by a sequence of zero, one, or more atomic transitions in $\mathcal{B}_{\rightarrow}$.

The Initial Model $\mathcal{T}_{\mathcal{R}}$

The most obvious reachabilty model for a rewrite theory $\mathcal{R} = (\Sigma, E, \phi, R)$ is the model $\mathcal{T}_{\mathcal{R}} = (\mathcal{T}_{\Sigma/E}, \rightarrow_{\mathcal{R}})$, where, by definition,

$$[t] \rightarrow_{\mathcal{R}} [t'] \quad \Leftrightarrow \quad \mathcal{R} \vdash t \longrightarrow t'$$

This is indeed a reachability model, and $\mathcal{T}_{\mathcal{R}} \models \mathcal{R}$, because (exercise) all the requirements are guaranteed by $\mathcal{T}_{\Sigma/E}$ being a (Σ, E)-algebra and by the inference rules of rewriting logic.

Using the Soundness Theorem and the initiality theorem for membership equational logic it is then nontrivial but relatively easy to prove (exercise) that we have:

The Initial Model $\mathcal{T}_{\mathcal{R}}$ (II)

Theorem. (Initiality Theorem). Assuming that Σ is sensible, $\mathcal{T}_{\mathcal{R}}$ is initial in the class of reachability models that satisfy $\mathcal{R}$. That is, if $\mathcal{A}_{\rightarrow} \models \mathcal{R}$, then there is a unique (Σ, ϕ)-reachability homomorphism

$$-_{\mathcal{A}_{\rightarrow}}^{\mathcal{R}} : \mathcal{T}_{\mathcal{R}} \longrightarrow \mathcal{A}_{\rightarrow}$$

Therefore, when reasoning about a concurrent system specified by a rewrite theory $\mathcal{R}$, for example as a system module in Maude, we will view $\mathcal{T}_{\mathcal{R}}$ as the standard model specified by $\mathcal{R}$, that is, as the mathematical model denoted by the specification $\mathcal{R}$. In other words, the initial algebra semantics of equational logic generalizes in a natural way to an initial reachability model semantics for rewriting logic.

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 A of equational axioms, such as associativity, commutativity, and identity, for which we have an A-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 $u =_A u'$ and $v =_A v'$. Recall Lecture 5, where (changing E there by R here) the analogue of the **Equality** inference step was achieved with the decidable relation $\longrightarrow_{R/A}$.

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

Executing Rewrite Theories (III)

The key idea is now the following. Given a rewrite theory $\mathcal{R} = (\Sigma, E \cup A, \phi, R)$ with $E \cup A$ having the just-mentioned executability assumptions we can simulate it and make it decidable by means of the rewrite theory $\hat{\mathcal{R}} = (\Sigma, A, \phi, \vec{E} \cup R)$, 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:

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

Executing Rewrite Theories (IV)

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

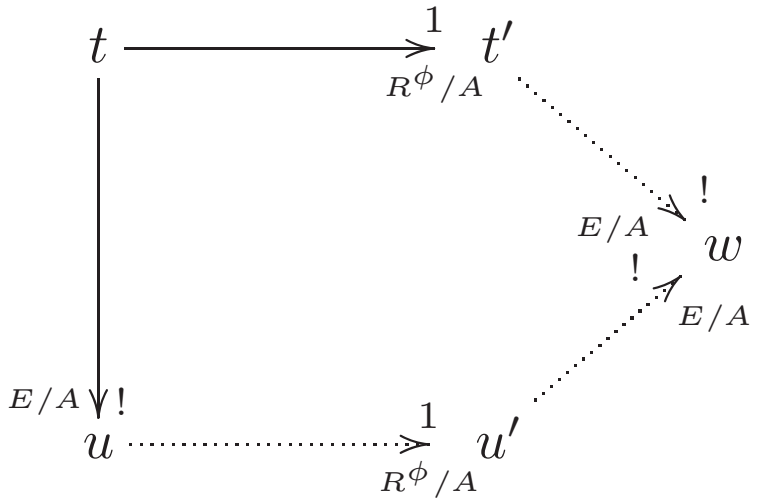
$$\mathcal{R} \vdash t \longrightarrow t' \quad \Leftarrow \quad \hat{\mathcal{R}} \vdash can_{E/A}(t) \longrightarrow can_{E/A}(t')$$

The hard part is the reverse implication, which in general may fail to hold. For example, if we have $A = \emptyset$, $E = \{a = c\}$, 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 A, we say that the rules R are coherent (resp. ground coherent) with E modulo A relative to ϕ if for each Σ-term t (resp. ground Σ-term t) such that $t \longrightarrow^{1}_{R^{\phi}/A} t'$ and $u = can_{E/A}(t)$ we have:



Coherence (II)

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

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

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,

$$l : (\forall X)\ t \longrightarrow t' \ \Leftarrow\ (\bigwedge_i u_i = u'_i) \wedge (\bigwedge_j v_j : s_j) \wedge (\bigwedge_k w_k \longrightarrow w'_k)$$

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

$$\frac{(\bigwedge_i (\forall Y)\ \theta(u_i) = \theta(u'_i)) \wedge (\bigwedge_j (\forall Y)\ \theta(v_j) : s_j) \wedge (\bigwedge_k (\forall Y)\ \theta(w_k) \longrightarrow \theta(w'_k)}{(\forall Y)\ \theta(t) \longrightarrow^1 \theta(t')}$$

- **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, A, and R already mentioned, and such that R is coherent with E modulo A w.r.t. ϕ we have:

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

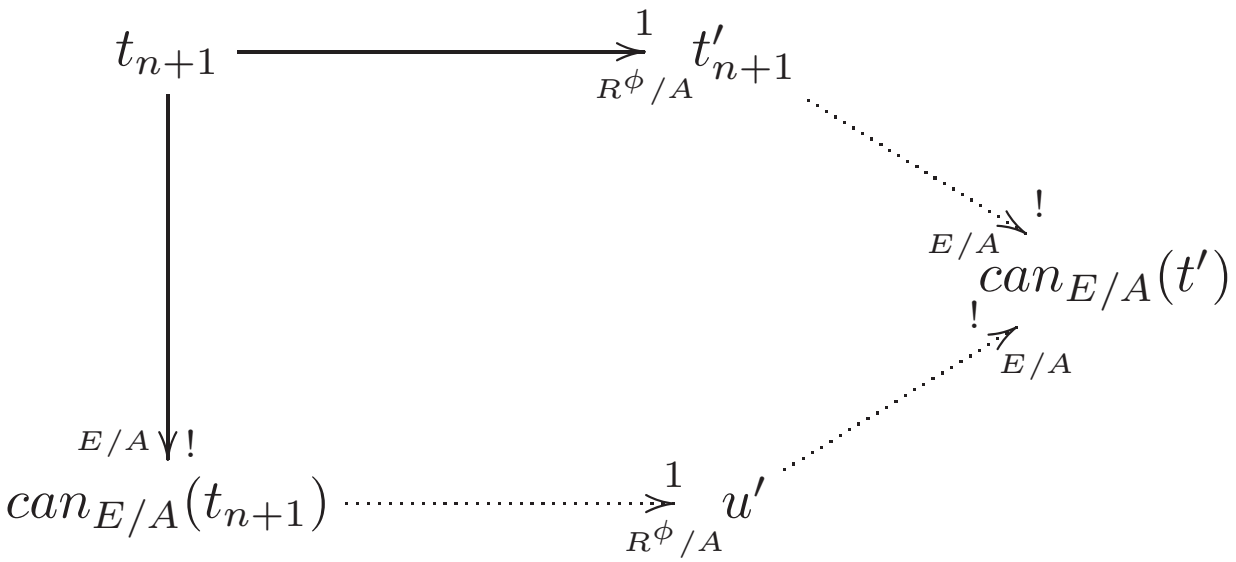
Proof: We only need to prove the implication $(\Rightarrow)$. By the Equivalence and Sequentialization Lemmas there is an $n \geq 0$ and proofs $\mathcal{R} \vdash' (\forall X)\, t_i \longrightarrow^1 t'_i$, $1 \leq i \leq n$, such that: $E \vdash (\forall X)\, t = t_1$, $E \vdash (\forall X)\, t'_i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

Semantic Equivalence through Coherence (II)

For $n = 0$ we have $can_{E/A}(t) = can_{E/A}(t')$ 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 $\hat{\mathcal{R}} \vdash can_{E/A}(t) \longrightarrow can_{E/A}(t_{n+1})$. So we will be done by repeatedly using **Transitivity'** if we can show $\hat{\mathcal{R}} \vdash can_{E/A}(t_{n+1}) \longrightarrow can_{E/A}(t')$. 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 $t_{n+1} \longrightarrow^1_{R^\phi/A} t'_{n+1}$.

Semantic Equivalence through Coherence (III)

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



The Canonical Reachability Model $\mathcal{C}_{\mathcal{R}}$

Given a system module `mod` $\mathcal{R}$ `endm`, with, say, $\mathcal{R} = (\Sigma, E \cup A, \phi, R)$, Maude assumes the following executability conditions: (i) Σ is preregular modulo A; (ii) E is ground confluent, sort-decreasing, and terminating modulo A; and (iii) R is ground coherent with E modulo A relative to ϕ. By the semantic equivalence theorem we have just proved, Maude can then essentially use $\hat{\mathcal{R}}$ to compute in $\mathcal{R}$ (we have seen the case when $\mathcal{R}$ is unconditional, but this generalizes to the conditional case).

Under these circumstances we can define a very intutive reachability model that exactly corresponds to the computational behavior experienced by a Maude user.

The Canonical Reachability Model $\mathcal{C}_{\mathcal{R}}$ (II)

Given a rewrite theory $\mathcal{R} = (\Sigma, E \cup A, \phi, R)$ satisfying the above executability conditions, we can define the canonical reachability model $\mathcal{C}_{\mathcal{R}} = (\mathcal{C}_{\Sigma,E/A}, \rightarrow_{\mathcal{C}_{\mathcal{R}}})$, were $\mathcal{C}_{\Sigma,E/A}$ is the canonical term algebra modulo A for $(\Sigma, E \cup A)$ as defined in Lecture 5, and $\rightarrow_{\mathcal{C}_{\mathcal{R}}}$ is the reflexive and transitive closure of the relation $\rightarrow^1_{\mathcal{C}_{\mathcal{R}}}$ where, by definition, given $[t], [t'] \in C_{\Sigma.E/A,k}$ for some kind k we have $[t] \rightarrow^1_{\mathcal{C}_{\mathcal{R}}} [t']$ if and only if there is a ground Σ-term u such that $t \longrightarrow^1_{R^{\phi}/A} u$ and $[can_{E/A}(u)] = [t']$.

The result of a Maude `rewrite` command, beginning with a term t in canonical form, is always a term t' such that $t \rightarrow_{\mathcal{C}_{\mathcal{R}}} t'$. Similarly, the nodes of the search graph computed by a `search` command are exactly elements of $\mathcal{C}_{\Sigma,E/A}$ and the edges are exactly $\rightarrow^1_{\mathcal{C}_{\mathcal{R}}}$-edges.

The Canonical Reachability Model $\mathcal{C}_{\mathcal{R}}$ (III)

The importance of $\mathcal{C}_{\mathcal{R}}$is that it provides a perfect agreement between mathematical and operational semantics, since we have,

Theorem. Under the above executability assumptions (i)–(iii) we have an isomorphism of reachability models

$$\mathcal{T}_{\mathcal{R}} \cong \mathcal{C}_{\mathcal{R}}$$

Proof: We already have an isomorphism $\mathcal{T}_{\Sigma/E \cup A} \cong \mathcal{C}_{\Sigma,E/A}$, mapping $[t]$ to $can_{E/A}(t)$. The remaining part of the proof boils down to proving that $[t] \rightarrow_{\mathcal{R}} [t']$ iff $[can_{E/A}(t)] \rightarrow_{\mathcal{C}_{\mathcal{R}}} [can_{E/A}(t')]$, which by the definition of $\rightarrow_{\mathcal{C}_{\mathcal{R}}}$ follows easily from the proof of semantic equivalence between $\mathcal{R}$ and $\hat{\mathcal{R}}$. q.e.d.

Verification of Declarative Concurrent Programs

We are now ready to discuss the subject of verification of declarative concurrent programs, and, more specifically, the verification of properties of Maude system modules, that is, of declarative concurrent programs that are rewrite theories.

There are two levels of specification involved: (1) a system specification level, provided by the rewrite theory and yielding an initial model for our program; and (2) a property specification level, given by some property (or properties) φ that we want to prove about our program. To say that our program satisfies the property φ then means exactly to say that its initial model does.

Verification of Declarative Concurrent Programs (II)

Specifically, we have considered the reachability initial model, $\mathcal{T}_{\mathcal{R}}$ of a rewrite theory $\mathcal{R}$.

The question then becomes, which language shall we use to express the properties φ that we want to prove hold in the model $\mathcal{T}_{\mathcal{R}}$? That is, how should we express relevant properties φ such that,

$$\mathcal{T}_{\mathcal{R}} \models \varphi.$$

The first, most obvious possibility is to use a first-order language based on the signature Σ together with a family of binary transition relations $\{\rightarrow_k\}_{k \in K}$.

Verification of Declarative Concurrent Programs (IV)

In particular, we can consider a modal logic $\mathcal{M}(\Sigma, \phi)$, expressing properties based on necessity, $\Box\varphi$, and possibility, $\Diamond\varphi$, which can be regarded as a sublanguage of such a first-order language. We will focus on properties $\Box I$, with I a predicate on states, stating that I is an invariant.

But not all properties of interest are expressible in $\mathcal{M}(\Sigma, \phi)$. For example, properties involving fairness, and other properties related to the infinite behavior of a system typically are not expressible in $\mathcal{M}(\Sigma, \phi)$. For such properties we can use some kind of temporal logic. We will give particular attention to linear temporal logic (LTL) because of its intuitive appeal, widespread use, and well-developed proof methods and decision procedures.

Invariants

Rather than developing in full detail the logic $\mathcal{M}(\Sigma, \phi)$, we will focus on invariants. Invariants specify safety properties, that is, properties guaranteeing that nothing "bad" can happen or, equivalently, that the system will always be in a "good" state. Given a rewrite theory $\mathcal{R}$, a chosen kind k of states, and an equationally-defined Boolean predicate I on states of kind k, we say that I is an invariant for $\mathcal{T}_{\mathcal{R}}$ beginning in an initial state $[t]$, written

$$\mathcal{T}_{\mathcal{R}}, [t] \models \Box I$$

if and only if $\mathcal{T}_{\mathcal{R}}$ satisfies the following first-order formula:

$$(\forall x : k)\ (t \rightarrow x) \Rightarrow I(x) = true.$$

Invariants (II)

Since the reachability relation is reflexive and transitive this exactly means that: (i) $I(t) = true$, and (ii) for any state x reachable from t we have $I(x) = true$. Therefore the predicate I specifies some good property that our system must always satisfy; and the fact that we have $\mathcal{T}_{\mathcal{R}}, [t] \models \Box I$ means that our system is I-safe, in the sense that the bad thing, namely $\neg I$, will never happen in any state reachable from our initial state $[t]$.

Given any (Σ, ϕ)-reachability model $\mathcal{A}_{\rightarrow} = (\mathcal{A}, \rightarrow_{\mathcal{A}})$ a kind k and an element $a \in A_k$, we define $Reach_{\mathcal{A}_{\rightarrow}}(a) = \{x \in A_k \mid a \rightarrow_{\mathcal{A}} x\}$. Similarly, given a Boolean predicate I with arguments of kind k we define $[|I|]_{\mathcal{A}_{\rightarrow}} = \{x \in A_k | I_{\mathcal{A}}(x) = true_{\mathcal{A}}\}$.

Invariants (III)

Therefore, we have,

$$\mathcal{T}_{\mathcal{R}}, [t] \models \Box I \quad \Leftrightarrow \quad Reach_{\mathcal{T}_{\mathcal{R}}}([t]) \subseteq [|I|]_{\mathcal{T}_{\mathcal{R}}}$$

More generally, given any (Σ, ϕ)-reachability model $\mathcal{A}_{\rightarrow} = (\mathcal{A}, \rightarrow_{\mathcal{A}})$ we can define the invariant satisfaction relation $\mathcal{A}_{\rightarrow}, a \models \Box I$ as the containment $Reach_{\mathcal{A}_{\rightarrow}}(a) \subseteq [|I|]_{\mathcal{A}_{\rightarrow}}$.

In other words, the predicate I carves out a set $[|I|]_{\mathcal{A}_{\rightarrow}}$ of "good" states. Satisfying the invariant I just means that our set $Reach_{\mathcal{A}_{\rightarrow}}(a)$ of reachable states is always inside the "safe envelope" $[|I|]_{\mathcal{A}_{\rightarrow}}$. An interesting question is how to verify such invariants.