Program Verification: Lecture 13

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Soundness Theorem

SoundnessTheorem. For (Σ, E) an equational theory with Σ sensible, kind-complete, and with nonempty sorts, for all Σ-equations $t = t'$, we have the implication:

$$(\Sigma, E) \vdash t = t' \quad \Rightarrow \quad (\Sigma, E) \models t = t'.$$

Proof: Note that, by definition, we have

$$(\Sigma, E) \vdash t = t' \;\Leftrightarrow\; t =_E t' \;\Leftrightarrow\; (\Sigma, \overrightarrow{E} \cup \overleftarrow{E}) \vdash t \rightarrow^* t'.$$

Therefore, what we have to prove is the implication

$$(\Sigma, \overrightarrow{E} \cup \overleftarrow{E}) \vdash t \rightarrow^* t' \quad \Rightarrow \quad (\Sigma, E) \models t = t'.$$

We can do so by induction on the length of the rewrite sequence $t \rightarrow^* t'$.

Soundness Theorem (II)

Base Case. If the length of $t \to^* t'$ is 0, then t' is identical to t, so we need to prove $(\Sigma, E) \models t = t$, which trivially holds, since for any Σ-algebra $\mathbb{A}$ we have $\mathbb{A} \models t = t$. In particular, if $\mathbb{A} \models E$, then, of course, $\mathbb{A} \models t = t$.

Induction Step. Assume that if $(\Sigma, \overrightarrow{E} \cup \overleftarrow{E}) \vdash t \to^* w$ and the sequence $t \to^* w$ has length n, then the relation $(\Sigma, E) \models t = w$ holds, and consider an additional rewrite step $w \to_{\overrightarrow{E} \cup \overleftarrow{E}} t'$. We then need to prove that $(\Sigma, E) \models t = t'$. We will be done if we can prove:

Lemma. For all w, t', if $w \to_{\overrightarrow{E} \cup \overleftarrow{E}} t'$ then $(\Sigma, E) \models w = t'$.

Soundness Theorem (III)

Indeed, if this Lemma holds, then for each Σ-algebra $\mathbb{A}$ such that $\mathbb{A} \models E$ and each assignment a we have $(\mathbb{A}, a) \models t = w$ (by Ind. Hyp.), and $(\mathbb{A}, a) \models w = t'$ (by Lemma). That is,

$$t\,a = w\,a \quad \wedge \quad w\,a = t''\,a$$

and therefore $(\mathbb{A}, a) \models t = t''$, so that $(\Sigma, E) \models t = t'$.

Proof of the Lemma: We must prove the implication $w \rightarrow_{\overrightarrow{E} \cup \overleftarrow{E}} t' \Rightarrow (\Sigma, E) \models w = t'$. But the rewrite $w \rightarrow_{\overrightarrow{E} \cup \overleftarrow{E}} t'$ uses an equation $(u = v) \in E$ either from left to right or from right to left at some position p in w and with some substitution $\theta : X \rightarrow T_{\Sigma(X)}$, so that, if $u = v$ is applied left-to-right, $w = w[u\theta]_p$ and $t' = w[v\theta]_p$.

We prove the case where $u = v$ is applied from left to right. The right-to-left case is completely similar.

Soundness Theorem (IV)

The proof is by induction of the length $|p|$ of the position p.

Base Case. If $|p| = 0$, then $p = \epsilon$ is the empty string. Therefore we have $w = u\theta$ and $t' = v\theta$, and we need to prove that for each $\mathbb{A}$ such that $\mathbb{A} \models E$ and each assignment a we have $(\mathbb{A}, a) \models u\theta = v\theta$, that is, that $u\,\theta\,a = v\,\theta\,a$.

But, since $\_\theta; \_a$ is a Σ-homomorphism and $\eta_X; \_\theta; \_a = \theta; \_a$, by the Freeness Theorem we have:

$$\_\theta\,;\_a = \_(\theta\,;\_a)$$

And since $\mathbb{A} \models E$ and $(\theta; \_a) \in [X \rightarrow A]$, in particular, $(\mathbb{A}, (\theta\,; \_a)) \models u = v$, that is, $u\,\theta\,a = v\,\theta\,a$, as desired.

Soundness Theorem (V)

Induction Step. We assume that the Lemma holds for $|p| = n$. Consider now $w = w[u\theta]_{i.p}$ and $t' = w[v\theta]_{i.p}$, with $|i.p| = n + 1$. This means that, for some f, $w = f(w_1, \ldots, w_n)$, $1 \leq i \leq n$, $w = f(w_1, \ldots, w_i[u\theta]_p, \ldots, w_n)$ and $t' = f(w_1, \ldots, w_i[v\theta]_p, \ldots, w_n)$.

But by the Ind. Hyp., if $\mathbb{A} \models E$ then $\mathbb{A} \models w_i[u\theta]_p = w_i[v\theta]_p$. Therefore, for any assignment $a \in [X \to A]$ we have:

$$w\,a = f_{\mathbb{A}}(w_1 a, \ldots, w_i[u\theta]_p a, \ldots, w_n a) = f_{\mathbb{A}}(w_1 a, \ldots, w_i[v\theta]_p a, \ldots, w_n a) = t'\,a$$

as desired. q.e.d.

This also concludes the proof of the Soundness Theorem. q.e.d.

Construction of the Initial Algebra $\mathbb{T}_{\Sigma/E}$

$\mathbb{T}_{\Sigma}$ is initial in the class $\mathbf{Alg}_{\Sigma}$ of all Σ-algebras. To give a mathematical, initial algebra semantics to Maude functional modules of the form `fmod`(Σ, E)`endfm` we need an initial algebra in the class $\mathbf{Alg}_{(\Sigma,E)}$ of all (Σ, E)-algebras, with Σ sensible, kind complete, and with nonempty sorts, denoted $\mathbb{T}_{\Sigma/E}$.

We shall define $\mathbb{T}_{\Sigma/E}$ and show that it is initial in $\mathbf{Alg}_{(\Sigma,E)}$, i.e., (i) $\mathbb{T}_{\Sigma/E} \models E$, and (ii) for any (Σ, E)-algebra $\mathbb{A}$ there is a unique Σ-homomorphism $\_^{E}_{\mathbb{A}} : \mathbb{T}_{\Sigma/E} \longrightarrow \mathbb{A}$.

If the equations E are sort-decreasing, confluent, terminating and sufficiently complete, will also show that there is an isomorphism $\mathbb{T}_{\Sigma/E} \cong \mathbb{C}_{\Sigma/E}$. That is, the mathematical semantics of `fmod`(Σ, E)`endfm` ($\mathbb{T}_{\Sigma/E}$) and its operational semantics ($\mathbb{C}_{\Sigma/E}$) coincide.

Construction of $\mathbb{T}_{\Sigma/E}$ (II)

We construct $\mathbb{T}_{\Sigma/E}$ out of the provability relation $(\Sigma, E) \vdash t = t'$; that is, out of the E-equality relation $t =_E t'$. But, by definition $t =_E t' \Leftrightarrow (\Sigma, \overrightarrow{E} \cup \overleftarrow{E}) \vdash t \rightarrow^* t'$. Therefore, $=_E$, besides being reflexive and transitive is symmetric, and therefore is an equivalence relation on terms. But since if $t =_E t'$, then there is a connected component $[s]$ such that $t, t' \in T_{\Sigma,[s]}$, in particular $=_E$ is also an equivalence relation on $T_{\Sigma,[s]}$. Therefore, we have a quotient set $T_{\Sigma/E,[s]} = T_{\Sigma,[s]}/{=_E}$.

We can then define the S-indexed family of sets $T_{\Sigma/E} = \{T_{\Sigma/E,s}\}_{s \in S}$, where, by definition,

$$T_{\Sigma/E,s} = \{[t] \in T_{\Sigma/E,[s]} \mid (\exists t')\ t' \in [t] \wedge t' \in T_{\Sigma,s}\},$$

where $[t]$, or $[t]_E$, abbreviate $[t]_{=_E}$.

Construction of $\mathbb{T}_{\Sigma/E}$ (III)

To make $T_{\Sigma/E}$ into a Σ-algebra $\mathbb{T}_{\Sigma/E} = (T_{\Sigma/E}, \_{\mathbb{T}_{\Sigma/E}})$, interpret a constant $a : nil \longrightarrow s$ in Σ by its equivalence class $[a]$.

Similarly, given $f : s_1 \dots s_n \to s$ in Σ, and given $[t_i] \in T_{\Sigma/E,s_i}$, $1 \leq i \leq n$, define

$$f^{s_1 \dots s_n, s}_{\mathbb{T}_{\Sigma/E}}([t_1], \dots, [t_n]) = [f(t'_1, \dots, t'_n)],$$

where $t'_i \in [t_i] \wedge t'_i \in T_{\Sigma,s_i}$, $1 \leq i \leq n$.

Checking that the above definition does not depend on either: (1) the choice of the $t'_i \in [t_i]$, or (2) the choice of the subsort-overloaded operator $f : s_1 \dots s_n \to s$ in Σ, so that it is well-defined and indeed defines an order-sorted Σ-algebra is left as an easy exercise.

Initiality Theorem for $\mathbb{T}_{\Sigma/E}$

Theorem: For (Σ, E) with Σ sensible, kind complete, and with nonempty sorts, $\mathbb{T}_{\Sigma/E} \models E$. Furthermore, $\mathbb{T}_{\Sigma/E}$ is initial in the class $\mathbf{Alg}_{(\Sigma,E)}$. That is, for any $\mathbb{A} \in \mathbf{Alg}_{(\Sigma,E)}$ there is a unique Σ-homomorphism $\_^E_{\mathbb{A}} : \mathbb{T}_{\Sigma/E} \longrightarrow \mathbb{A}$.

Proof: We first need to show that $\mathbb{T}_{\Sigma/E} \models E$, i.e., that $\mathbb{T}_{\Sigma/E} \models t = t'$ for each $(t = t') \in E$. That is, for each assignment $a : X \longrightarrow T_{\Sigma/E}$ we must show that $t\, a = t'\, a$.

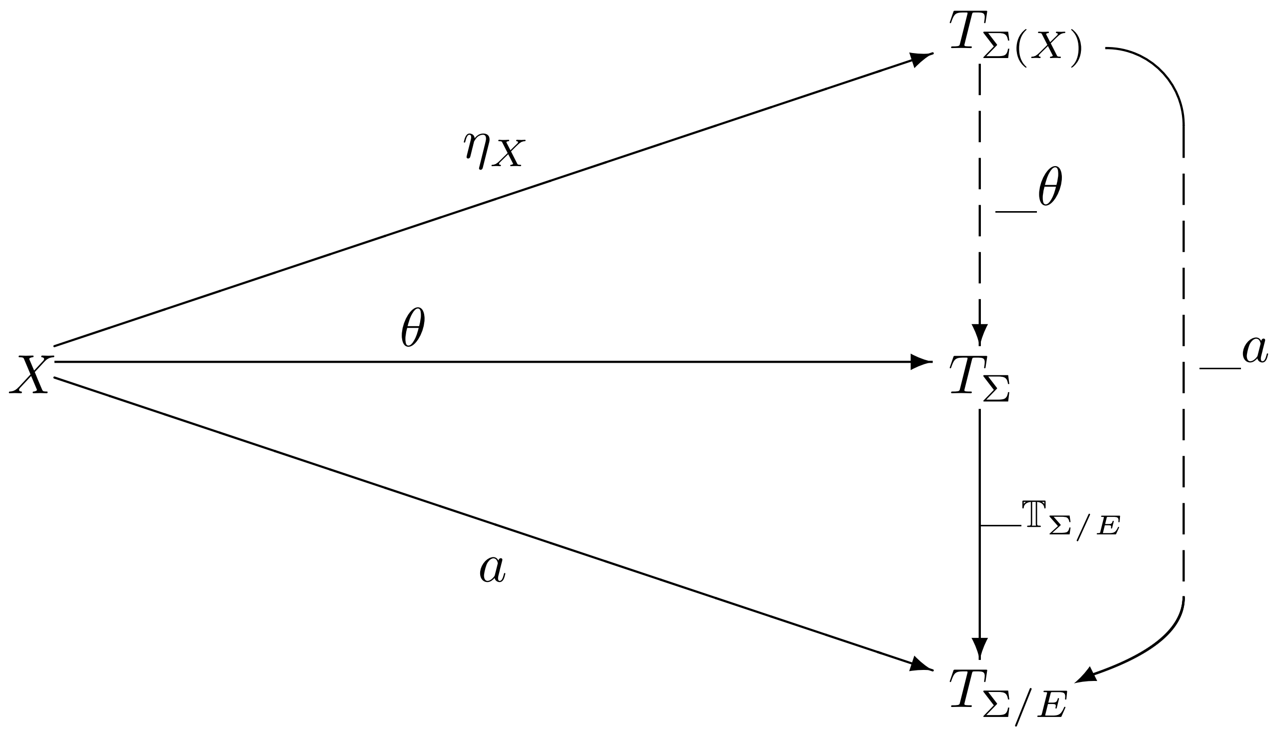
But (see **Ex**.13.1) the unique Σ-homomorphism $\__{\mathbb{T}_{\Sigma/E}} : \mathbb{T}_{\Sigma} \longrightarrow \mathbb{T}_{\Sigma/E}$ guaranteed by $\mathbb{T}_{\Sigma}$ initial is just the passage to equivalence classes: $[\_]_E : T_{\Sigma} \ni t \mapsto [t]_E \in T_{\Sigma/E}$ and is therefore surjective.

Initiality Theorem for $\mathbb{T}_{\Sigma/E}$ (II)

Therefore, since by the Axiom of Choice any surjective function is a right inverse (STACS, Ch. 10, Thm. 9, pg. 80), we can always choose a substitution $\theta : X \longrightarrow T_\Sigma$ such that $a = \theta; \_{\mathbb{T}_{\Sigma/E}}$. Therefore, by the Freeness Corollary we have $\_a = \_\theta; \_{\mathbb{T}_{\Sigma/E}}$ (see diagram next page).

Therefore, $t\ a = t'\ a$ is just the equality $[t\theta]_E = [t'\theta]_E$, which holds iff $t\theta =_E t'\theta$, which itself holds by $(t = t') \in E$ and the Lemma in the proof of the Soundness Theorem. Therefore, $\mathbb{T}_{\Sigma/E} \models E$.

Lifting of a to a Substitution θ



Initiality Theorem for $\mathbb{T}_{\Sigma/E}$ (III)

Let us now show that for each $\mathbb{A} \in \mathbf{Alg}_{(\Sigma,E)}$ there is a unique Σ-homomorphism $\_^{E}_{\mathbb{A}} : \mathbb{T}_{\Sigma/E} \longrightarrow \mathbb{A}$.

We first prove uniqueness. Suppose that we have two homomorphisms $h, h' : \mathbb{T}_{\Sigma/E} \longrightarrow \mathbb{A}$. Then, composing with $\__{\mathbb{T}_{\Sigma/E}} : \mathbb{T}_{\Sigma} \longrightarrow \mathbb{T}_{\Sigma/E}$ on the left we get, $\__{\mathbb{T}_{\Sigma/E}}; h, \__{\mathbb{T}_{\Sigma/E}}; h' : T_{\Sigma} \longrightarrow \mathbb{A}$, and by the initiality of $\mathbb{T}_{\Sigma}$ we must have, $\__{T_{\Sigma/E}}; h = \__{T_{\Sigma/E}}; h' = \__{\mathbb{A}}$. But recall that $\__{\mathbb{T}_{\Sigma/E}} : \mathbb{T}_{\Sigma} \longrightarrow \mathbb{T}_{\Sigma/E}$ is surjective, and therefore (**Ex**.11.9) epi, which forces $h = h'$, as desired.

Initiality Theorem for $\mathbb{T}_{\Sigma/E}$ (IV)

To show existence of $\_^E_{\mathbb{A}} : \mathbb{T}_{\Sigma/E} \longrightarrow \mathbb{A}$, given $[t] \in T_{\Sigma/E,s}$, define $[t]^E_{\mathbb{A},s} = t'_{\mathbb{A},s}$, where $t' \in [t] \wedge t' \in T_{\Sigma,s}$. Then show (exercise) that:

- $[t]^E_{\mathbb{A},s}$ is independent of the choice of t' because of the hypothesis $\mathbb{A} \models E$ and the Soundness Theorem; and

- the family of functions $\_^E_{\mathbb{A}} = \{\_^E_{\mathbb{A},s}\}_{s \in S}$ thus defined is indeed a Σ-homomorphism.

q.e.d.

The Mathematical and Operational Semantics Coincide

As stated in pg. 2, the semantics of a Maude functional module `fmod`(Σ, E)`endfm` is an initial algebra semantics, given by $\mathbb{T}_{\Sigma/E}$. Let us call $\mathbb{T}_{\Sigma/E}$ the module's mathematical semantics. This sematics does not depend on any executability assumptions about `fmod`(Σ, E)`endfm`: it can be defined for any equational theory (Σ, E).

Call `fmod`(Σ, E)`endfm` admissible if the equations E are (ground) confluent, sort-decreasing and terminating and sufficiently complete w.r.t. constructors Ω. Under these executabilty requirements we have another semantics for `fmod`(Σ, E)`endfm`: the canonical term algebra $\mathbb{C}_{\Sigma/E}$ defined in Lecture 4. This is the most intuitive computational model for `fmod`(Σ, E)`endfm`. Call it its operational semantics, since $\mathbb{C}_{\Sigma/E}$ is defined by the `reduce` command. But both semantics coincide!

The Canonical Term Algebra is Initial

Theorem: If the rules $\vec{E}$ are sort-decreasing, confluent and terminating, then, $\mathbb{C}_{\Sigma/E}$ is isomorphic to $\mathbb{T}_{\Sigma/E}$ and is therefore initial in $\mathbf{Alg}_{(\Sigma,E)}$.

Proof: A slight extension of the proof of **Ex**.11.11 shows that if $\mathbb{I}$ is initial for a given class of algebras closed under isomorphisms and $\mathbb{J}$ is isomorphic to $\mathbb{I}$, then $\mathbb{J}$ is also initial for that class. Since by (**Ex**.12.2) $\mathbf{Alg}_{(\Sigma,E)}$ is closed under isomorphisms, we just have to show $\mathbb{T}_{\Sigma/E} \cong \mathbb{C}_{\Sigma/E}$.

Define $\_!_E = \{\_!_{E,s} : T_{\Sigma/E,s} \longrightarrow C_{\Sigma/E,s}\}_{s \in S}$ by, $[t]!_{E,s} = t!_E$. This is independent of the choice of t, since $t =_E t'$ iff $E \vdash t = t'$ iff (by E confluent) $t \downarrow_E t'$, iff $t!_E = t'!_E$. $\_!_{E,s}$ is surjective by construction and injective by these equivalences; therefore $\_!_E$ is bijective.

The Canonical Term Algebra is Initial (II)

Let us see that $\_!_E : \mathbb{T}_{\Sigma/E} \longrightarrow \mathbb{C}_{\Sigma/E}$ is a Σ-homomorphism. Preservation of constants is trivial. Let $f : s_1 \ldots s_n \to s$ in Σ, and $[t_i] \in T_{\Sigma/E,s_i}$, $1 \leq i \leq n$. We must show,

$$f^{s_1 \ldots s_n, s}_{\mathbb{T}_{\Sigma/E}}([t_1], \ldots, [t_n])!_{E,s} = f^{s_1 \ldots s_n, s}_{\mathbb{C}_{\Sigma/E}}(t_1!_E, \ldots, t_n!_E).$$

The key observation is that $t_i!_E \in T_{\Sigma,s_i}$, $1 \leq i \leq n$. This is because:

- by definition of $[t_i]$ there must be a $t_i' =_E t_i$ with $t_i' \in T_{\Sigma,s_i}$, $1 \leq i \leq n$; and
- by the sort-decreasingness assumption for E, since $t_i' \overset{*}{\longrightarrow}_E t_i'!_E = t_i!_E$, if $t_i' \in T_{\Sigma,s_i}$, $1 \leq i \leq n$, then $t_i!_E \in T_{\Sigma,s_i}$, $1 \leq i \leq n$.

The Canonical Term Algebra is Initial (III)

Therefore, we have:

$f^{s_1 \dots s_n, s}_{\mathbb{T}_{\Sigma/E}}([t_1], \dots, [t_n])!_E = [f(t_1!_E, \dots, t_n!_E)]!_E$
(by definition of $f^{s_1 \dots s_n, s}_{\mathbb{T}_{\Sigma/E}}$)
$= f(t_1!_E, \dots, t_n!_E)!_E$ (by definition of $\_!_E$)
$= f^{s_1 \dots s_n, s}_{\mathbb{C}_{\Sigma/E}}(t_1!_E, \dots, t_n!_E)$
(by definition of $f^{s_1 \dots s_n, s}_{\mathbb{C}_{\Sigma/E}}$)

as desired.

All now reduces to proving the following easy lemma, which is left as an exercise:

Lemma. The bijective S-sorted map
$\{\_!^{-1}_{E,s} : C_{\Sigma/E,s} \ni u \mapsto [u] \in T_{\Sigma/E,s}\}_{s \in S}$ is a Σ-homomorphism
$\_!^{-1}_{E} : \mathbb{C}_{\Sigma/E} \to \mathbb{T}_{\Sigma/E}$.

q.e.d

Math. Sems. = Operatl. Sems.: An Example

The canonical term algebra $\mathbb{C}_{\Sigma/E}$ is in some sense the most intuitive representation of the initial algebra from a computational point of view. Let us see in a simple example what the coincidence beteen mathematical and operational semantics means.

For example, the equations $E_{\texttt{NATURAL}}$ in the `NATURAL` module are confluent and terminating. Its canonical forms are the natural numbers in Peano notation. And its operations are the successor and addition functions.

Indeed, given two Peano natural numbers n, m the general definition of $f^{s_1 \ldots s_n, s}_{\mathbb{C}_{\Sigma/E}}$ specializes for $f = \_+\_$ to the definition of addition, $n +_{\mathbb{C}_{\texttt{NATURAL}}} m = (n+m)!_{E_{\texttt{NATURAL}}}$, so that $\_ +_{\mathbb{C}_{\texttt{NATURAL}}} \_$ is the addition function.

Math. Sems. = Operatl. Sems.: An Example (II)

$T_{\Sigma_{\mathtt{NATURAL}}/E_{\mathtt{NATURAL}}}$

...	...	...	...
$ppss0$	$s0+0$	$ss0+0$	
$0+0$	$0+s0$	$s0+s0$	
$ps0$	$pss0$	$psss0$	
0	$s0$	$ss0$	...

$C_{\Sigma_{\mathtt{NATURAL}}/E_{\mathtt{NATURAL}}}$

All Generalizes Modulo Axioms B

More generally, we are interested in the agreement between the mathematical and operational semantics of an admissible Maude module of the form $\texttt{fmod}(\Sigma, E \cup B)\texttt{endfm}$, with B a (possibly empty) set of associativity, commutativity, and identity axioms. The, following, easy but nontrivial, generalization of the above theorem is left as an exercise.

Theorem: Let the equations E in $(\Sigma, E \cup B)$ be sort-decreasing, confluent, terminating and sufficiently complete modulo B; and let Σ be preregular modulo B. Then, $\mathbb{C}_{\Sigma,E/B}$ is isomorphic to $\mathbb{T}_{\Sigma/E \cup B}$ and is therefore initial in $\mathbf{Alg}_{(\Sigma,E \cup B)}$.

The Completeness Theorem for Equational Logic

The construction of the initial algebra $\mathbb{T}_{\Sigma/E}$ together with the Freeness Theorem proved in Lecture 12 are the two ingredients allowing a very short (less than one page) proof of The Completeness Theorem:

Teorem (Completeness). For any equational theory (Σ, E) and Σ-equation $u = v$, the following implication holds:

$$E \models u = v \quad \Rightarrow \quad E \vdash u = v$$

That is, any theorem of (Σ, E) is provable in equational logic.

The short proof of this important theorem can be found in an Appendix to this lecture.

Exercises

Ex.13.1. Prove that for any equational theory (Σ, E) with Σ sensible and having $(S, <)$ as poset of sorts, the unique Σ-homomorphism $\_{\mathbb{T}_{\Sigma/E}} : \mathbb{T}_\Sigma \longrightarrow \mathbb{T}_{\Sigma/E}$ is exactly the S-sorted function of passage to equivalence classes:
$\{[\_]_{E,s} : T_{\Sigma,s} \ni t \mapsto [t]_E \in T_{\Sigma/E,s}\}_{s \in S}$.