Program Verification: Lecture 12

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

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 an initial algebra semantics to Maude functional modules of the form $\mathtt{fmod}(\Sigma, E)\mathtt{endfm}$ 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.

We shall construct such an algebra, denoted $\mathbb{T}_{\Sigma/E}$, and show that it is indeed 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 show that there is an isomorphism $\mathbb{T}_{\Sigma/E} \cong \mathbb{C}_{\Sigma/E}$, a very intuitive semantics.

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 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 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 $t \mapsto [t]$ 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

$$
\begin{tikzcd}
 & T_{\Sigma(X)} \arrow[d, dashed, "\_\theta"] \arrow[dd, dashed, bend left=60, "\_a"] \\
X \arrow[ur, "\eta_X"] \arrow[r, "\theta"] \arrow[dr, "a"'] & T_{\Sigma} \arrow[d, "\_\mathbb{T}_{\Sigma/E}"] \\
 & T_{\Sigma/E}
\end{tikzcd}
$$

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 surjecive, and therefore (**Ex.**10.8) 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 $\texttt{fmod}(\Sigma, E)\texttt{endfm}$ 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 $\texttt{fmod}(\Sigma, E)\texttt{endfm}$: it can be defined for any equational theory (Σ, E).

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

The Canonical Term Algebra is Initial

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

Proof: An easy generalization of **Ex.**10.10 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 (**Ex.**11.2) $\mathbf{Alg}_{(\Sigma,E)}$ 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 $t'_i \equiv_E t_i$ with $t'_i \in T_{\Sigma,s_i}$, $1 \leq i \leq n$; and
- by the sort-decreasingness assumption for E, since $t'_i \stackrel{*}{\longrightarrow}_E t'_i!_E = t_i!_E$, 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:

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

as desired.

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

Lemma. The bijective S-sorted map $\_!^{-1}_E : C_{\Sigma/E} \to T_{\Sigma/E}$ 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 $E_{\mathtt{NATURAL}}$ 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, $n +_{\mathbb{C}_{\mathtt{NATURAL}}} m = (n + m)!_{E_{\mathtt{NATURAL}}}$, so that $\_ +_{\mathbb{C}_{\mathtt{NATURAL}}} \_$ is the addition function.

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

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

$\ldots$	$\ldots$	$\ldots$	$\ldots$
$ppss0$	$s0+0$	$ss0+0$	
$0+0$	$0+s0$	$s0+s0$	
$ps0$	$pss0$	$psss0$	
0	$s0$	$ss0$	$\ldots$

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

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 $\mathbf{Alg}_{(\Sigma,E\cup B)}$.

Verification of Maude Functional Modules

We are now ready to begin discussing program verification for deterministic declarative programs, and, more specifically, for Maude functional modules of the form $\texttt{fmod}(\Sigma, E \cup B)\texttt{endfm}$, where we assume E confluent, sort-decreasing, terminating and sufficiently complete modulo B, and Σ preregular modulo B. Their mathematical semantics is given by the initial algebra $\mathbb{T}_{\Sigma/E\cup B}$.

Their (concrete) operational semantics is given by equational simplification with $\vec{E}$ modulo B. Both semantics coincide in the canonical term algebra, since we have the Σ-isomorphism,

$$\mathbb{T}_{\Sigma/E\cup B} \cong \mathbb{C}_{\Sigma,E/B}.$$

Verification of Maude Functional Modules (II)

What are properties of a module $\texttt{fmod}(\Sigma, E \cup B)\texttt{endfm}$?

They are sentences φ, perhaps in equational logic, or, more generally, in first-order logic, in the language of a signature containing Σ.

When do we say that the above module satisfies property φ?

When we have,

$$\mathbb{T}_{\Sigma/E \cup B} \models \varphi.$$

How do we verify such properties?

A Simple Example: Associativity of Addition

Consider the module,

```
fmod NATURAL is
  sort Natural .
  op 0 : -> Natural [ctor] .
  op s : Natural -> Natural [ctor] .
  op _+_ : Natural Natural -> Natural .
  vars N M L : Natural .
  eq N + 0 = N .
  eq N + s(M) = s(N + M) .
endfm
```

A property φ satisfied by this module is the associativity of addition, that is, the equation,

$$(\forall \mathtt{N}, \mathtt{M}, \mathtt{L})\ \mathtt{N\ +\ (M\ +\ L)} = \mathtt{(N\ +\ M)\ +\ L}.$$

Need More than Equational Deduction

Since the initial algebra $\mathbb{T}_{\Sigma/E\cup B}$ associated to a module $\texttt{fmod}(\Sigma, E \cup B)\texttt{endfm}$ satisfies the equations $E \cup B$, by the **Soundness Theorem** for equational deduction, whenever we can prove an equation φ by $E \cup B \vdash \varphi$, we must have $\mathbb{T}_{\Sigma/E\cup B} \models \varphi$, and therefore the module satisfies φ.

Therefore, equational deduction is always a sound proof method to verify properties of functional modules. However, it is quite limited, and generally insufficient for many properties.

In particular, for φ the associativity of addition and E the equations in `NATURAL` (in this case $A = \emptyset$) we cannot prove $E \vdash (x + y) + z = x + (y + z)$.

Need More than Equational Deduction (II)

This is easy to see, since the equations in the module `NATURAL` are terminating (there is an easy proof using an RPO order) and confluent (automatically checkable using the Church-Rosser Checker). Therefore, by the **Church-Rosser Theorem** we have:

$$E \vdash (x+y)+z = x+(y+z) \quad \Leftrightarrow \quad ((x+y)+z)!_E = (x+(y+z))!_E$$

But $(x+y)+z$ and $x+(y+z)$ are terms in E-normal form. Therefore, $E \not\vdash (x+y)+z = x+(y+z)$. The same argument also proves, for example, that $E \not\vdash x+y = y+x$.

However, we shall see that the initial model of `NATURAL` satisfies in fact the associativity and commutativity of $+$

Inductive Properties

The point is that associativity and commutativity are inductive properties of natural number addition; that is, properties satisfied by the initial model of E, but not in general by other models of E.

What we need are inductive proof methods based on a more powerful proof system $\vdash_{ind}$, satisfying the soundness requirement,

$$E \cup B \vdash_{ind} \phi \quad \Rightarrow \quad \mathbb{T}_{\Sigma/E \cup B} \models \phi.$$

Also, it should prove all that equational deduction can prove and more. That is, for formulas ϕ that are equations it should satisfy,

$$E \cup B \vdash \phi \quad \Rightarrow \quad E \cup B \vdash_{ind} \phi.$$

Inductive Properties (II)

Because of Gödel's Incompleteness Theorem, in general we cannot hope to have completeness of inductive inference, that is, to have an equivalence

$$E \cup B \vdash_{ind} \phi \quad \Leftrightarrow \quad \mathbb{T}_{\Sigma/E \cup B} \models \phi$$

although this may be possible for some very specific theories (Σ, E) for which a complete proof system, or even an algorithm (a decision procedure), providing this equivalence exists.

The inductive inference system that we will justify and use generalizes the usual proofs by natural number induction. In fact, in our example of associativity of natural number addition it actually specializes to the usual proof method by natural number induction.

Sufficient Completeness is Crucial for Inductive Proofs

```
fmod NON-STANDARD-NAT is
  sort Natural .
  op 0 : -> Natural [ctor] .
  op s : Natural -> Natural [ctor] .
  op a : -> Natural .
  op _+_ : Natural Natural -> Natural .
  vars N M L : Natural .
  eq N + 0 = N .
  eq N + s(M) = s(N + M) .
endfm
```

In this module, $T_{\Sigma/E} \not\models$ `a +(a + a)` $=$ `(a + a)+ a`, since both terms are in normal form and the equations are confluent and terminating. However, natural number induction on the declared constructors easily proves associativity of $+$. Therefore, induction without sufficient completeness is unsound.

Exercises

- **Ex.**12.1 Consider the `NAT-PREFIX` specification of Lecture 2. Prove that the natural numbers $\mathbb{N}$, with zero, successor and the addition function are isomorphic to the initial algebra of that specification.

- **Ex.**12.2 Give your own algebraic specification of the Booleans in Maude (use a sort, say `Truth`, and constants `tt`, `ff`, to avoid any confusion with the built-in module `BOOL` in Maude) with disjunction, conjunction, and negation, and prove that the standard Booleans are isomorphic to the initial algebra of your specification.