Program Verification: Lecture 13

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 a mathematical, initial algebra semantics to Maude functional modules of the form $\texttt{fmod}(\Sigma, E)\texttt{endfm}$ 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 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 $\mathbb{T}_{\Sigma/E} \cong \mathbb{C}_{\Sigma/E}$. That is, the mathematical semantics of $\texttt{fmod}(\Sigma, E)\texttt{endfm}$ ($\mathbb{T}_{\Sigma/E}$) 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 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

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

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 $t\ a = t'\ a$.

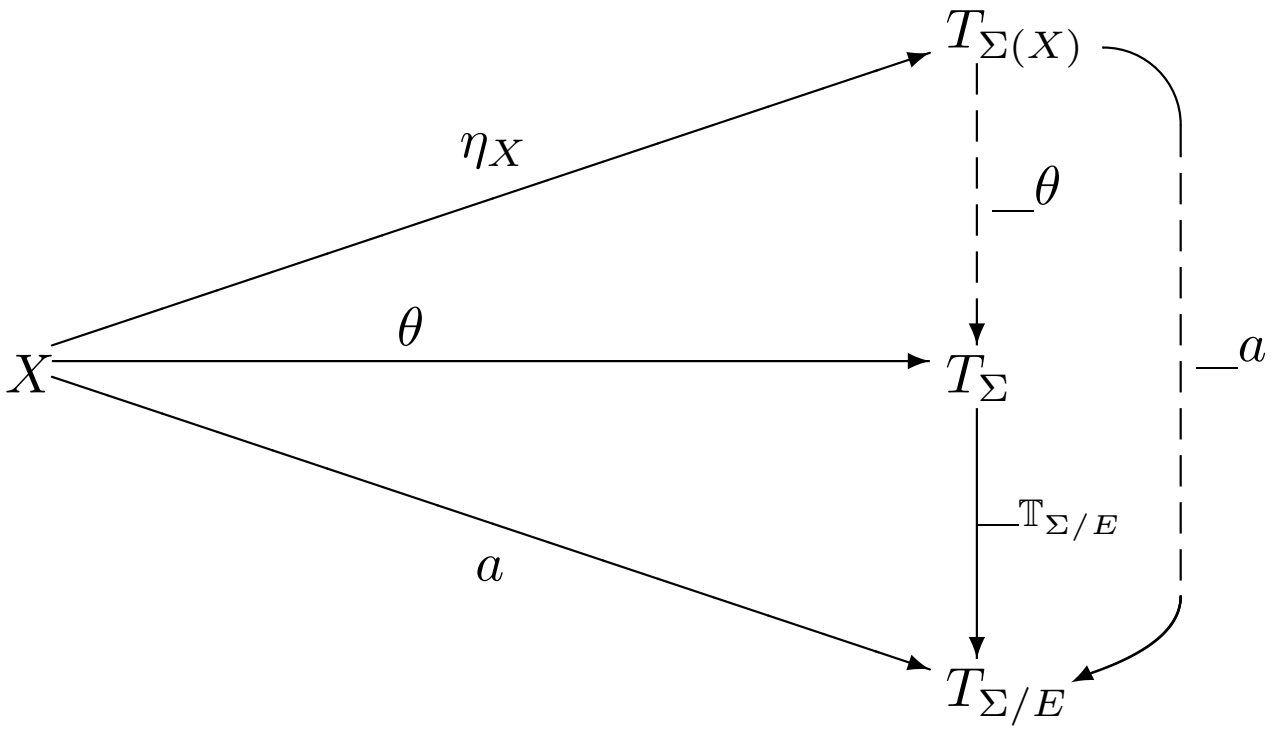
But the unique Σ-homomorphism $\_^{\mathbb{T}_{\Sigma/E}} : \mathbb{T}_{\Sigma} \longrightarrow \mathbb{T}_{\Sigma/E}$ guaranteed by $\mathbb{T}_{\Sigma}$ initial is just the passage to equivalence classes: $[\_]_E : T_\Sigma \ni t \mapsto [t]_E \in T_{\Sigma/E}$ (this has an easy proof by induction on the tree depth of 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



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 (ground) confluent, sort-decreasing, terminating and sufficiently complete w.r.t. constructors Ω. 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 $f : s_1 \dots s_n \to s$ in Σ, and $[t_i] \in T_{\Sigma/E,s_i}$, $1 \leq i \leq n$. We must show,

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

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

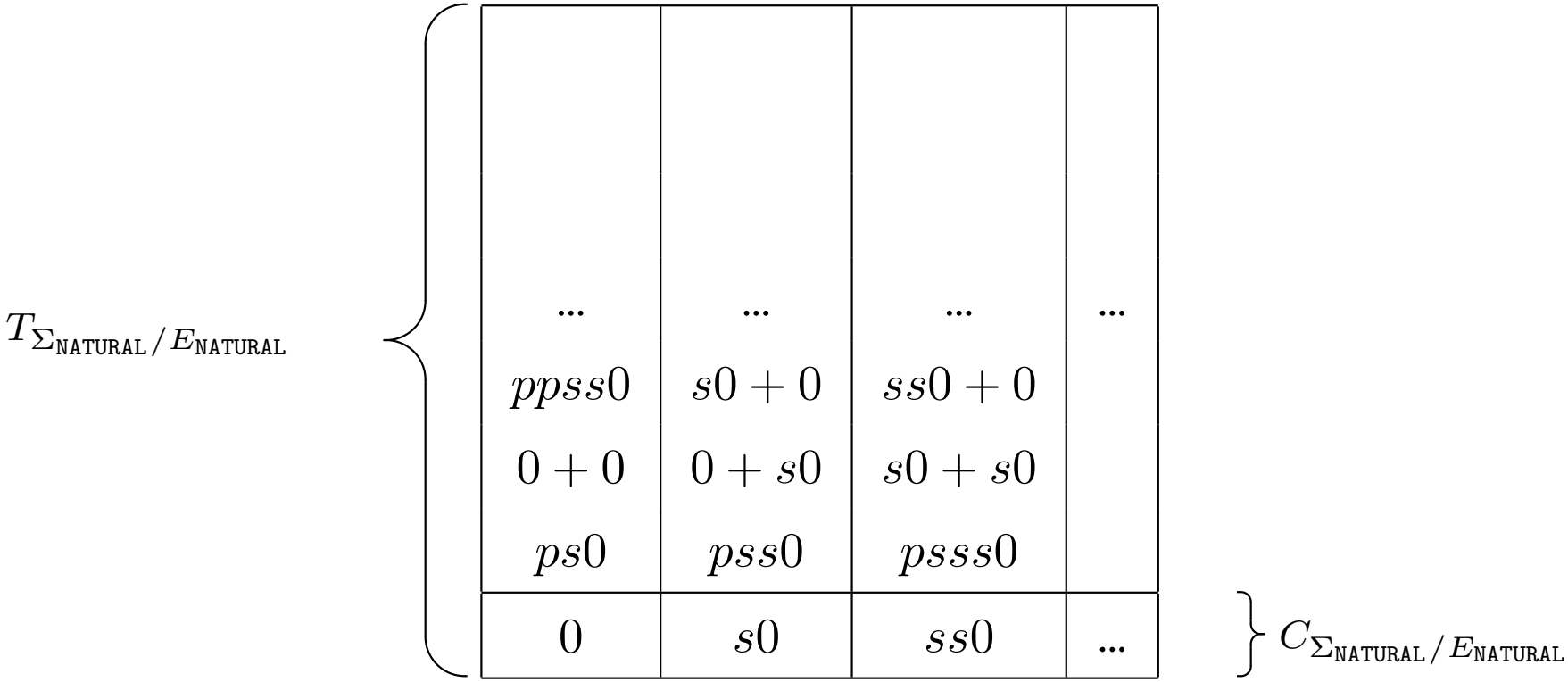
Math. Sems. = Operatl. Sems.: An Example

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 $E_{\texttt{NATURAL}}$ 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 $f^{s_1 \cdots s_n, s}_{\mathbb{C}_{\Sigma/E}}$ 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)



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.

Provable Theorems and Theorems of an Equational Theory (Σ, E)

For $\Sigma = ((S, \leq), \Sigma)$ and order-sorted signature, define the set of Σ-equations in the obvious way (where X has a countably infinite set X_s of variables for each sort $s \in S$):

$$\Sigma.Eq = \{u = v \mid \exists s, s' \in S.\ u \in T_\Sigma(X)_s \wedge v \in T_\Sigma(X)_{s'} \wedge [s] = [s']\}.$$

Given any set of Σ-equations $E \subseteq \Sigma.Eq$, define the set of its provable theorems as:

$$PThm(E) = \{u = v \in \Sigma.Eq \mid u =_E v\}.$$

Likewise, for any $E \subseteq \Sigma.Eq$, define the set of its theorems as:

$$Thm(E) = \{u = v \in \Sigma.Eq \mid \forall \mathbb{A} \in \mathbf{Alg}_{(\Sigma,E)},\ \mathbb{A} \models u = v\}.$$

The Soundness and Completeness Theorems show that we have:

$$PThm(E) = Thm(E).$$

Inductive Theorems of an Equational Theory (Σ, E)

Given any Σ-algebra $\mathbb{A}$, define its set of theorems as:

$$Thm(\mathbb{A}) = \{u = v \in \Sigma.Eq \mid \mathbb{A} \models u = v\}.$$

Then, given an equational theory (Σ, E) define its set of inductive theorems $IndThm(\Sigma, E)$ by the set-theoretic equality:

$$IndThm(\Sigma, E) =_{def} Thm(\mathbb{T}_{\Sigma/E}).$$

In particular, when a functional module $\texttt{fmod}(\Sigma, E \cup B)\texttt{endfm}$ is (ground) confluent, terminating and sufficiently complete w.r.t. constructors Ω, since $\mathbb{T}_{\Sigma/E \cup B} \cong \mathbb{C}_{\Sigma, E/B}$, and by Ex.12.2 we know that $Thm(\mathbb{T}_{\Sigma/E}) = Thm(\mathbb{C}_{\Sigma, E/B})$, in this case $IndThm(\Sigma, E)$ are the equational properties satisfied by the program $\texttt{fmod}(\Sigma, E \cup B)\texttt{endfm}$. Thus $IndThm(\Sigma, E)$ is a crucial concept in program verification.

Inductive Theorems of an Equational Theory (Σ, E) (II)

By definition, given a Σ-equation $u = v$, we write $E \models_{ind} u = v$ and say that $u = v$ is an inductive consequence of E iff $(u = v) \in \mathit{IndThm}(\Sigma, E)$.

But since $\mathit{IndThm}(\Sigma, E) = \mathit{Thm}(\mathbb{T}_{\Sigma/E})$ and $\mathbb{T}_{\Sigma/E} \models E$, we have an inclusion $\mathit{Thm}(E) \subseteq \mathit{IndThm}(\Sigma, E)$, and therefore an implication:

$$E \models u = v \quad \Rightarrow \quad E \models_{ind} u = v$$

In general, however, the converse implication does not hold: there are theories (Σ, E) and Σ-equations $u = v$ such that $\mathbb{T}_{\Sigma/E} \models u = v$ but $E \not\models u = v$, so that, by Soundness and Completeness, $E \nvdash u = v$. Let us see some examples.

Can have $\mathbb{T}_{\Sigma/E} \models u = v$ but $E \not\vdash u = v$

Consider the unsorted signature $\Sigma = \{0, s, \_ + \_\}$ with $E = \{x + 0 = x, x + s(y) = s(x + y)\}$. We have already proved that $\vec{E}$ is confluent and terminating, and (in a Homework assignment) that $\mathbb{C}_{\Sigma,E/B}$ is the addition function on the natural numbers, which is well-known to be associative and commutative. Therefore, $\mathbb{T}_{\Sigma/E} \models x + y = y + x$, and $\mathbb{T}_{\Sigma/E} \models (x + y) + x = x + (y + z)$. However,

$$E \not\vdash x + y = y + x \quad \textit{and} \quad E \not\vdash (x + y) + z = x + (y + z)$$

since, by the Church-Rosser Theorem, $x + y =_E y + x$ iff $(x + y)!_{\vec{E}} = (y + x)!_{\vec{E}}$, and $(x + y) + z =_E x + (y + z)$ iff $((x + y) + z)!_{\vec{E}} = (x + (y + z))!_{\vec{E}}$. But, those canonical forms are all different, because the terms involved, $x + y$, $y + x$, $(x + y) + z$ and $x + (y + z)$ are all in $\vec{E}$-canonical form: no $\vec{E}$ rules apply to them.

Characterizing the Inductive Theorems of (Σ, E)

Can we say something about when $(u = v) \in IndThm(\Sigma, E)$? Yes, we can characterize all inductive theorems as follows:

Theorem (Characterization of Inductive Theorems):

1. $(u = v) \in IndThm(\Sigma, E)$ iff $\forall \theta \in [X \to T_\Sigma], E \vdash u\theta = v\theta$, where $X = vars(u) \cup vars(v)$.
2. If, in addition, the rules $\vec{E}$ are ground confluent, terminating and sufficiently complete w.r.t. Ω, then $(u = v) \in IndThm(\Sigma, E)$ iff $\forall \rho \in [X \to T_\Omega], E \vdash u\rho = v\rho$.

Proof Hints: The proof of (1) follows from the notion of satisfaction $\mathbb{T}_{\Sigma/E} \models u = v$, since any assignment $a \in [X \to T_{\Sigma/E}]$ is of the form $a = \theta; [\_]_E$ for some $\theta \in [X \to T_\Sigma]$. The proof of (2) is a variant of that of (1) using the (ground) Church-Rosser Theorem and sufficient completeness.

Exercises

Ex.13.1 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.

Ex.13.2. Prove in detail the theorem characterizing the inductive theorems of a theory (Σ, E) stated in pg. 22 of this lecture.

Exercises (II)

Ex.13.3. Consider the equational theory (Σ, E) defined by the functional module:

```
fmod PEANO-p is
sorts NzNat Nat .   subsorts NzNat < Nat .
op 0 : -> Nat [ctor] .
op s : Nat -> NzNat [ctor] .
op p : NzNat -> Nat .
eq p(s(N:Nat)) = N:Nat .
endfm
```

which defines the predecessor function `p`. Do the following:

1. Prove that $(\Sigma, \vec{E})$ is sort-decreasing, confluent, terminating, and sufficiently complete w.r.t. $\Omega = \{0, s\}$ by either using tools in Maude's Formal Environment, or giving a hand proof.

2. Prove that $E \not\vdash s(p(y:NzNat)) = y:NzNat$.

3. Prove that $(\Sigma, E) \models_{ind} s(p(y:NzNat)) = y:NzNat$ by applying Part (2) of the theorem characterizing the inductive theorems of a theory (Σ, E) stated in pg. 22 of this lecture.