Formal Methods: Lecture 3

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Indexed Families of Functions

Given two S-indexed families of sets $A = \{A_s\}$, and $B = \{B_s\}$, what is the natural generalization of the concept of function from sets to S-indexed sets?

It is the notion of an S-indexed family of functions $f = \{f_s : A_s \longrightarrow B_s\}_{s \in S}$, where for each $s \in S$ $f_s : A_s \longrightarrow B_s$ is a function in the ordinary sense. We then write $f : A \longrightarrow B$.

Mathematically, f can be described as an ordinary function $f : S \longrightarrow \mathcal{U}$ into a suitable universe $\mathcal{U}$ (set of sets) such that for each $s \in S$ we have $f(s) = f_s : A_s \longrightarrow B_s$. In the language of set theory everything can be described as a set, including a function from one set to another, so such functions can be elements of a rich enough universe $\mathcal{U}$.

Many-Sorted Homomorphisms

Given (many-sorted) Σ-algebras A and B, a Σ-homomorphism h from A to B, written $h : A \longrightarrow B$, is an S-indexed family of functions $h = \{h_s : A_s \longrightarrow B_s\}_{s \in S}$ such that:

- for each constant $a : nil \longrightarrow s$, $h_s(a_A^{nil,s}) = a_B^{nil,s}$ (preservation of constants)

- for each $f : w \longrightarrow s$ with $w = s_1 \ldots s_n$, $n \geq 1$, and each $(a_1, \ldots, a_n) \in A^w$, we have $h_s(f_A^{w,s}(a_1, \ldots, a_n)) = f_B^{w,s}(h_{s_1}(a_1), \ldots, h_{s_n}(a_n))$ (preservation of operations)

Order-Sorted Homomorphisms

For $\Sigma = (S, \{\Sigma_{w,s}\}_{(w,s)\in S^* \times S}, <)$ an order-sorted signature, and A and B order-sorted Σ-algebras, a Σ-homomorphism h from A to B, written $h : A \longrightarrow B$, is an S-indexed family of functions $h = \{h_s : A_s \longrightarrow B_s\}_{s\in S}$ such that:

- $h : A \longrightarrow B$ is a many-sorted $(S, \{\Sigma_{w,s}\}_{(w,s)\in S^* \times S})$-homomorphism; and
- if $s \equiv_{\leq} s'$ and $a \in A_s \cap A_{s'}$, then $h_s(a) = h_{s'}(a)$ (agreement on data in the same connected component)

Examples of Homomorphisms

As already mentioned, besides the term algebra $T_{\Sigma_{\texttt{NAT-PREFIX}}}$ and the natural numbers **N** (in any notation: binary, decimal, Peano, etc.) as algebras for the signature of NAT-PREFIX we also have the natural numbers modulo n, $\mathbf{N}_n$ for any $n \geq 1$. Show that we have homomorphisms:

$$T_{\Sigma_{\texttt{NAT-PREFIX}}} \stackrel{eval_{\mathbf{N}}}{\longrightarrow} \mathbf{N} \stackrel{rem_n}{\longrightarrow} \mathbf{N}_n$$

which correspond to evaluating a term to its value in $\mathbf{N}$, and to sending each number to its remainder after dividing by n. For example, we should have:

- $eval_{\mathbf{N}}(plus(s(0), s(0))) = 2$, and
- $rem_7(23) = [2]$.

Examples of Homomorphisms (II)

For Σ the signature of the theory of groups, resp. rings, resp., vector spaces, the corresponding Σ-homomorphism notion becomes that of group homomorphism, resp. ring homomorphism, resp. linear function.

In all cases, the idea is that the corresponding operations are preserved. For example, a linear function $f : \mathbf{R}^3 \longrightarrow \mathbf{R}^3$ in the 3-dimensional vector space $\mathbf{R}^3$ over the reals is typically described by a 3×3 matrix, and has two crucial properties:

- $f(\vec{v} + \vec{v'}) = f(\vec{v}) + f(\vec{v'})$, and
- $f(a.\vec{v}) = a.f(\vec{v})$,

i.e., vector addition and scalar multiplication are preserved by f. Note that Σ has two sorts: `Ring` and `Vector`.

Sensible Signatures

A signature Σ can be intrinsically ambiguous, so that a term may denote two completely different things. Consider for example the following signature:

```
sorts A B C D .
op a : -> A .
op f : A -> B .
op f : A -> C .
op g : B -> D .
op g : C -> D .
```

then the term `g(f(a))` is an ambiguous term of sort `D` denoting two completely different things.

A very mild condition ruling this out, yet allowing ad-hoc overloading, is the notion of a sensible signature, namely one such that whenever we have $f : w \longrightarrow s$ and $f : w' \longrightarrow s'$, with w, w' of equal length, then $w \equiv_{\leq} w' \Rightarrow s \equiv_{\leq} s'$.

Sensible Signatures (II)

Lemma. If Σ is a sensible order-sorted signature, then for any term t in T_Σ we have,

$$t \in T_{\Sigma,s} \ \wedge \ t \in T_{\Sigma,s'} \quad \Rightarrow \quad s \equiv_{\leq} s'$$

Proof: By induction on the depth of t.

We define the depth of a term as follows: constants have depth 0, and terms of the form $f(t_1, \ldots, t_n)$ have depth $1 + max(depth(t_1), \ldots, depth(t_n))$.

For depth 0, $t = a$ is a constant, and $a \in T_{\Sigma,s}$ iff there is $a : nil \rightarrow s''$ in Σ with $s'' \leq s$. Similarly, if $a \in T_{\Sigma,s'}$ there is $a : nil \rightarrow s'''$ in Σ with $s''' \leq s'$. By Σ sensible we have $s'' \equiv_{\leq} s'''$, and therefore, $s \equiv_{\leq} s'$.

Sensible Signatures (III)

Assuming the result true for depth $\leq n$, let $t = f(t_1, \ldots, t_n)$ have depth $n+1$. If we have $t \in T_{\Sigma,s} \ \wedge \ t \in T_{\Sigma,s'}$, this forces the existence of $f : w'' \longrightarrow s''$ and $f : w''' \longrightarrow s'''$, with $s'' \leq s$ and $s''' \leq s'$ and such that $(t_1, \ldots, t_n) \in T_\Sigma^{w''} \cap T_\Sigma^{w'''}$.

By the induction hypothesis this forces $w'' \equiv_\leq w'''$. And by Σ sensible this forces $s'' \equiv_\leq s'''$, and therefore, $s \equiv_\leq s'$. q.e.d.

Substitutions

Given an order-sorted signature Σ with set of sorts S and given S-indexed families of variables $X = \{X_s\}_{s \in S}$, and $Y = \{Y_s\}_{s \in S}$, a substitution is an S-indexed family of functions

$$\theta : X \longrightarrow T_{\Sigma(Y)}$$

For example, for Σ an unsorted signature of arithmetic expressions, $X = \{x, y, z\}$, and $Y = \{x, y, z, x', y', z'\}$, a particular θ can be the assignment:

- $x \mapsto (x + y') * z$
- $y \mapsto (x' - y')$
- $z \mapsto z' * z'$

Substitutions Extend to Homomorphisms

If Σ is a sensible signature, a substitution

$$\theta : X \longrightarrow T_{\Sigma(Y)}$$

extends uniquely to a Σ-homomorphism

$$\overline{\theta} : T_{\Sigma(X)} \longrightarrow T_{\Sigma(Y)}$$

defined recursively by:

- $\overline{\theta}(x) = \theta(x)$
- $\overline{\theta}(f(t_1, \ldots, t_n)) = f(\overline{\theta}(t_1), \ldots \overline{\theta}(t_n))$

For example, for the above θ we have,

$$\overline{\theta}(x + (y * z)) = ((x + y') * z) + ((x' - y') * (z' * z')).$$

Equations

What is the general notion of equation in the general setting of Σ-algebras that we are considering?

Given a signature Σ, we can define a Σ-equation as an expression of the form

$$t = t'$$

where for some variables X t, t' are terms $t \in T_{\Sigma(X)}, s$, $t' \in T_{\Sigma}(X), s'$ such that the sorts s, s' are related in the subsort ordering, i.e., $s \equiv_{\leq} s'$.

Given the above equation, we can universally quantify all its variables and get the sentence

$$(\forall X)\ t = t'$$

Conditional Equations

Sometimes equations are conditional. A cancellation law (which holds, for example, for $_ \circ _$ interpreted as: string concatenation, multiset union, or multiplication by a nonzero integer) takes the form, $x = y \Leftarrow x \circ z = y \circ z$.

In general, we may have a conjunction of several equations in the condition, with the general form,

$$t = t' \Leftarrow u_1 = v_1 \wedge \ldots \wedge u_n = v_n$$

with all the $t = t'$ and $u_i = v_i$, $1 \leq i \leq n$, Σ-equations. Again, if $t, t', u_i, v_i \in T_\Sigma(X)$, $1 \leq i \leq n$, we have the universally quantified conditional equation,

$$(\forall X)\, t = t' \Leftarrow u_1 = v_1 \wedge \ldots \wedge u_n = v_n$$

Equational Simplification

For Maude functional modules we assume that equations have been given in such a way that they can be efficiently executed by applying them from left to right.

We call this process equational simplification, because intuitively the expressions get progressively simpler, until getting to their simplest possible result.

This is of course a special form of equational deduction, replacing equals by equals.

Equational Simplification (II)

Let $T = (\Sigma, E)$ be an equational theory. We say that the equations in E are admissible as equational simplification rules if each equation $(\forall X)\, t = t' \Leftarrow u_1 = v_1 \wedge \ldots \wedge u_n = v_n$ in E satisfies the following two properties:

- *fewer variables on the right side and condition*, that is, the families of variables $\mathrm{vars}(t')$, $\mathrm{vars}(u_i)$, and $\mathrm{vars}(v_i)$, $1 \leq i \leq n$, are all contained in $\mathrm{vars}(t) = X$, where, $\mathrm{vars}(t)$ denotes the family of variables actually appearing in t.

- *sort decreasingness*, that is, for any substitution $\theta : X \longrightarrow T_\Sigma(Y)$, and any $s \in S$, if $\overline{\theta}(t) \in T_\Sigma(Y)_s$, then $\overline{\theta}(t') \in T_\Sigma(Y)_s$.

Term Positions and Subterm Occurences

Each Σ-term can be viewed as a tree in the obvious way. Each position in the tree can be denoted by a string of natural numbers, indicating the path that we must follow to go down in the tree and reach the position.

At each level, the corresponding number in the string indicates the argument position on which we must go down, to finally reach the desired position. For example, the term $f(h(d), q(b, a), g(a, k(c)))$ has the subterm $k(c)$ at position 3.2.

Given a Σ-term t and a position π we denote by t/π the subterm occuring at that position; thus, $f(h(d), q(b, a), g(a, k(c)))/3.2 = k(c)$.

Term Replacement

Given a Σ-term t, a position π in it, and another Σ-term u we denote by

$$t[\pi \leftarrow u]$$

the replacement of t/π by u in t at position π. For example, consider the term $t = s(x) + s(s(y))$, its 2.1 position, and the term $u = x + z$. Then $t[2.1 \leftarrow u] = s(x) + s(x + z)$.

Note that, in general, $t[\pi \leftarrow u]$ need not be a well-formed Σ-term. However, it is a well-formed Σ-term if, for any $s \in S$,

$$t/\pi \in T_\Sigma(\mathsf{vars}(u) \cup \mathsf{vars}(t/\pi))_s \quad \Rightarrow \quad u \in T_\Sigma(\mathsf{vars}(u) \cup \mathsf{vars}(t/\pi))_s.$$

The Equational Rewriting Relation

Let $T = (\Sigma, E)$ be a theory whose equations E are admissible as equational simplification rules. Then we can use them from left to right to hopefully bring terms to a simpler form which can be interpreted as their evaluation.

This process is called equational simplification, or equational rewriting. For any S-indexed family X of variables, this defines two binary relations on $T_{\Sigma(X)}$, $\longrightarrow_E$, and its reflexive and transitive closure $\overset{*}{\longrightarrow}_E$. $\longrightarrow_E$ is defined recursively as follows:

For $t, t' \in T_{\Sigma(X)}$, we have $t \longrightarrow_E t'$ iff, either:

The Equational Rewriting Relation (II)

- there is an equation $(\forall \text{vars}(u))\ u = v$ in E, a position π in t, and a substitution $\theta : \text{vars}(u) \longrightarrow T_{\Sigma(X)}$ such that, $t/\pi = \overline{\theta}(u)$, and $t' = t[\pi \leftarrow \overline{\theta}(v)]$, or

- there is a conditional equation $(\forall \text{vars}(u))\ u = v \Leftarrow u_1 = v_1 \wedge \ldots \wedge u_n = v_n$ in E, a position π in t, a substitution $\theta : \text{vars}(u) \longrightarrow T_{\Sigma(X)}$, and terms $w_i \in T_{\Sigma(X)}$, $1 \leq i \leq n$, such that:

  1. (*satisfaction of the condition*) $\overline{\theta}(u_i) \stackrel{*}{\longrightarrow}_E w_i$ and $\overline{\theta}(v_i) \stackrel{*}{\longrightarrow}_E w_i$, $1 \leq i \leq n$, and

  2. (*matching and replacement*) $t/\pi = \overline{\theta}(u)$, and $t' = t[\pi \leftarrow \overline{\theta}(v)]$.

Remarks on the Equational Rewriting Relation

- Note that, because of our assumption about sort-decreasingness of the equational simplification rules in E, whenever we have an equation $u = v$, with or without a condition, in E, and a term $t \in T_{\Sigma(X)}$ such that $t/\pi = \overline{\theta}(u)$, then $t[\pi \leftarrow \overline{\theta}(v)]$ is a well-formed Σ-term.

- Note also that $\mathsf{vars}(t[\pi \leftarrow \overline{\theta}(v)]) \subseteq \mathsf{vars}(t)$, and therefore, whenever $t \longrightarrow_E^* t'$ we have $\mathsf{vars}(t') \subseteq \mathsf{vars}(t)$.

Notation: We define the binary relation $t \downarrow_E t'$ on pairs of terms $t, t' \in T_{\Sigma(X)}$ by,

$$t \downarrow_E t' \quad \Leftrightarrow \quad (\exists w \in T_{\Sigma(X)})\ t \longrightarrow_E^* w \ \wedge\ t' \longrightarrow_E^* w.$$

Confluence

Suppose we have a theory $T = (\Sigma, E)$ whose equations are admissible as equational simplification rules. Then we can do sound inference by equational simplification with E, but the equations E may still be quite unusable, because depending on the order and place of equation application we may get different and unrelatable results. That is, in general, equational simplification can be nondeterministic.

The minimum requirement to make equational simplification deterministic is confluence, also called the Church-Rosser property. We say that E is confluent iff whenever we have $t \xrightarrow{*}_E u$ and $t \xrightarrow{*}_E v$, then $u \downarrow_E v$. We call E ground confluent iff the above property is guaranteed only for terms without variables $t \in T_\Sigma$.

Termination

Equational theories $T = (\Sigma, E)$ whose equations are ground confluent can be viewed as equational programs, and support a style of functional programming in which expresions are evaluated by simplification. This is what Maude functional modules are: equational programs evaluated by simplification.

In general, however, such programs can be nonterminating. Terminating equational programs are obtained when the rewriting relation is terminating.

We say that the equations E are terminating as simplification rules when there is no infinite chain of rewrites

$$t \longrightarrow_E t_1 \longrightarrow_E t_2 \ldots t_{n-1} \longrightarrow_E t_n \longrightarrow \ldots$$

Canonical Forms

If the equations in $T = (\Sigma, E)$ are confluent (resp. ground confluent) and terminating, then for each term $t \in T_{\Sigma(X)}$ (resp. $t \in T_\Sigma$) there is a unique term $can_E(t) \in T_{\Sigma(X)}$ (resp. $can_E(t) \in T_\Sigma$) called its canonical form such that:

- $t \longrightarrow^*_E can_E(t)$, and
- $can_E(t)$ cannot be further rewritten.

Indeed, by the termination assumption, we can always simplify t to such a term; and uniqueness is then forced by the confluence (resp. ground confluence) property. The term $can_E(t)$ should be understood as the value returned by the equational program $T = (\Sigma, E)$ for the input expression t.

The Canonical Term Algebra

If the equations in $T = (\Sigma, E)$ are ground confluent and terminating, then the S-indexed family of terms $Can_{\Sigma/E}$ with

$$Can_{\Sigma/E,s} = \{can_E(t) \mid t \in T_{\Sigma,s}\}$$

can be made into a Σ-algebra as follows:

- for each constant $a : nil \longrightarrow s$ in Σ, we define $a_{Can_{\Sigma/E}} = can_E(a)$, and
- for each $f : s_1 \dots s_n \to s$ in Σ, and $t_i \in Can_{\Sigma/E,s_i}$, $1 \leq i \leq n$, we define $f^{s_1 \dots s_n, s}_{Can_{\Sigma/E}}(t_1, \dots, t_n) = can_E(f(t_1, \dots, t_n))$.

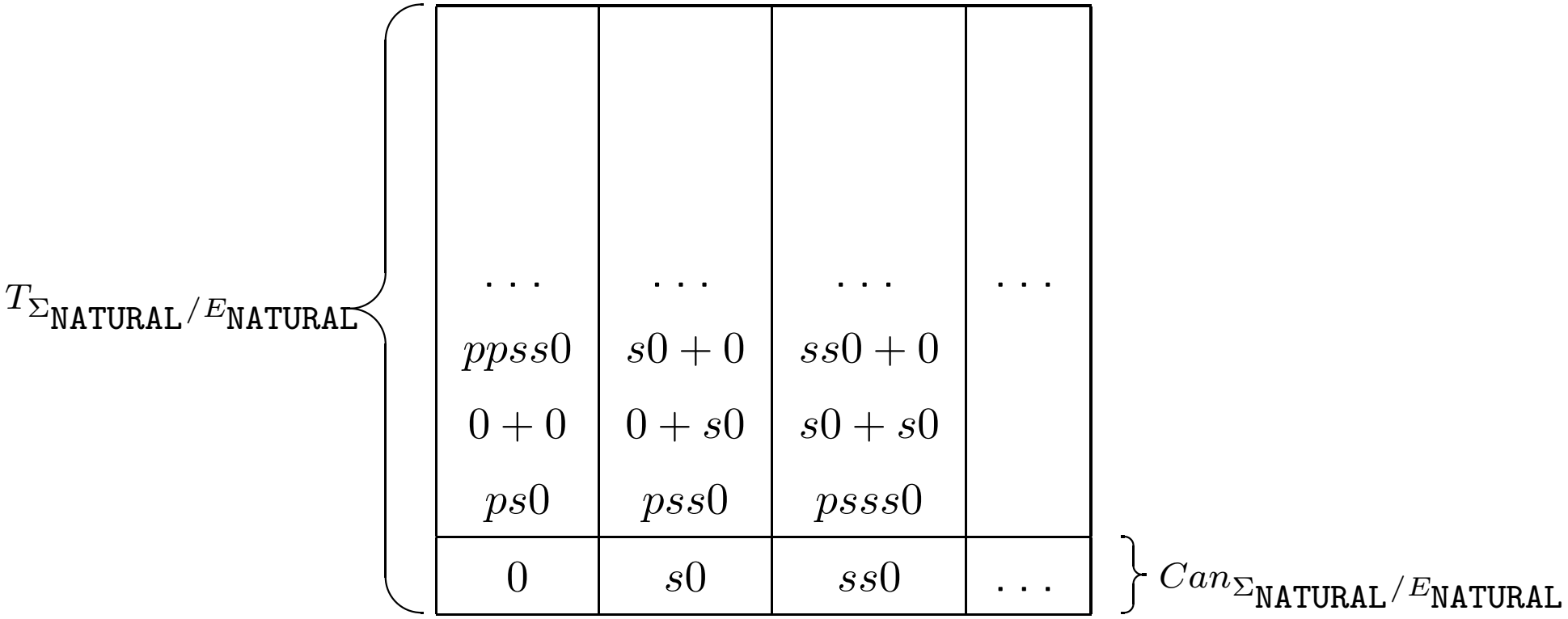
Example of Canonical Term Algebra

We shall see that the canonical term algebra satisfies the equations E and is the simplest possible model (called initial) among those satisfying the equations E. We will interpret the meaning of a Maude functional module `fmod` (Σ, E) `endfm` which is assumed to be confluent and terminating as its canonical term algebra $Can_{\Sigma/E}$.

For example, the equations in the `NATURAL` module are ground 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 $f^{s_1 \cdots s_n, s}_{Can_{\Sigma/E}}$ specializes for $f = _ + _$ to the definition of addition, $n +_{Can_{\texttt{NATURAL}}} m = can_{\texttt{NATURAL}}(n + m)$, so that $_ +_{Can_{\texttt{NATURAL}}} _$ is the addition function.

Example of Canonical Term Algebra (II)



Exercises

Ex. 5.1 Call an ordered set $(A, \leq)$ noetherian iff any nonempty subset $B \subseteq A$ has a minimal element, that is, an element $x \in B$ such that $\forall y \in B\ x \geq y \Rightarrow x = y$.

- prove that the following principle of noetherian induction is correct:

  "If $(A, \leq)$ is noetherian, then any $B \subseteq A$ such that for any $a \in A$ if $a{\downarrow} \subseteq B$ then $a \in B$ must be $B = A$, where, by definition, $a{\downarrow} = \{x \in A \mid x < a\}$."

- Show that if a set of equations E is terminating, then for any $s \in S$, the relation $\stackrel{*}{\longrightarrow}_E$ defines a noetherian partial order on $T_{\Sigma(X),s}$.

Exercises (II)

Ex. 5.2 Call a set E of equations locally confluent iff whenever we have $t \longrightarrow_E u$ and $t \longrightarrow_E v$, then $u \downarrow_E v$.

- prove that if E is terminating and locally confluent, then E is confluent (Hint: use noetherian induction)

- exhibit a set of equations that are localy confluent but not confluent.

Exercises (III)

Ex. 5.3 Call E weakly terminating if any term t can be rewritten by E to a term t' that cannot be further rewritten.

- show that if E is weakly terminating and confluent, there is a unique canonical form $can_E(t)$ for any t

- exhibit a set of equations E that is weakly terminating and confluent, but not terminating.