Formal Methods: Lecture 5

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Assignments

Given variables in $X = \{X_s\}$ we will often be interested in assignments (also called valuations) of data elements in a given Σ-algebra A to those variables. Of course, if $x \in X_s$ then the value, say $a(x)$, assigned to x should be an element of A_s. That is the assignments should be well-sorted. All this can be made precise by defining an assignment as an S-indexed family of functions, $a = \{a_s : X_s \longrightarrow A_s\}_{s \in S}$, denoted $a : X \longrightarrow A$.

Often what we want to do with such assignments is to extend them from variables to terms on such variables in the obvious, homomorphic way. That leads us to the algebra $T_{\Sigma(X)}$.

Extending Assignments Homomorphically

The point now is to extend and assignment $a : X \longrightarrow A$ to a Σ-homomorphism

$$\overline{a} : T_{\Sigma(X)} \longrightarrow A$$

Assuming that Σ is sensible and that the variables X are disjoint from the constants in Σ, then $\Sigma(X)$ is also sensible and this makes terms in $T_{\Sigma(X)}$ unambiguos. This allows us to define $\overline{a} : T_{\Sigma(X)} \longrightarrow A$ recursively as follows:

- $\overline{a}(x) = a(x)$ for x a variable
- $\overline{a}(b) = b_A$ for b a constant in Σ
- $\overline{a}(f(t_1, \ldots, t_n) = f_A(\overline{a}(t_1), \ldots, \overline{a}(t_n))$

Extending Assignments Homomorphically (II)

Note that $\overline{a}$ extends a, since both agree on the variables in X. Furthermore, it is not hard to check that $\overline{a}$ is:

1. well-defined, because $\Sigma(X)$ is sensible and A is an order-sorted algebra (so that terms and unambiguous, and the various subsort-overloaded versions $f_A^{w,s}$ agree on common data, so their qualification in the above definition is immaterial);
2. a Σ-homomorphism by construction, and
3. the unique possible extension of a to a Σ-homomorphism.

In fact, all these properties are a special case of a more general initiality property that we shall discuss.

A Homomorphic Extension Example

A good example of Σ-homomorphic extension of an assignment is provided by the evaluation of expressions in a programming language. For integer expressions, Σ could be chosen to have two sorts, say, `Int` and `Exp`, with a subsort inclusion, `Int < Exp`, and with constants $0, 1$ of sort `Int`, and overloaded operators,

```
op _+_ : Exp Exp -> Exp .
op _+_ : Int Int -> Int .
op _-_ : Exp Exp -> Exp .
op _-_ : Int Int -> Int .
op _*_ : Exp Exp -> Exp .
op _*_ : Int Int -> Int .
```

A Homomorphic Extension Example (II)

The set X of variables is precisely the set of variables in the programming language. The expressions in this language are precisely the elements of the initial $\Sigma(X)$-algebra $T_{\Sigma(X)}$. Expression evaluation is then relative to a given store, that is, to a given assignment function $a : X \longrightarrow \mathbf{Z}$, where we denote by $\mathbf{Z}$ the Σ-algebra of arbitrary precision integers, and adopt the convention that an uninitialized variable x always has the value $a(x) = 0$.

Then the unique Σ-homomorphism $\overline{a} : T_{\Sigma(X)} \longrightarrow \mathbf{Z}$ is just the function evaluating each arithmetic expression to its value, given the store a. For example, if $a(x) = 2$, $a(y) = 3$, and $a(z) = 4$, then, for example, $\overline{a}((x * y) - z) = 2$.

Substitutions as Homomorphic Extensions

Notice that the notion of substitution is a special case of the notion of assignment, namely it is an assignment of terms in a term algebra $T_{\Sigma(Y)}$ to the variables in X

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

Of course, what we are interested in is its unique extension to a Σ-homomorphism

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

guaranteed by the general definition of extension, and already defined earlier (in Lecture 3) for the special case of substitutions,

Satisfaction of Equations

Given a Σ-algebra A, an assignment $a : X \longrightarrow A$, and an equation $t = t'$ with $t, t' \in T_{\Sigma(X)}$, we define the satisfaction relation $A, a \models t = t'$ by means of the equivalence,

$$A, a \models t = t' \quad \Leftrightarrow \quad \overline{a}(t) = \overline{a}(t')$$

Similarly, given a Σ-algebra A, and an equation $t = t'$ with $t, t' \in T_{\Sigma(X)}$, we define the satisfaction relation $A \models (\forall X)\, t = t'$ iff for all assignments $a : X \longrightarrow A$ we have $A, a \models t = t'$.

Examples of Satisfaction

Consider, for example, a signature Σ with just one sort `Natural`, with constants $0, 1$, and operations of addition $_ + _$, and multiplication $_ * _$. Let $\mathbf{N}$ denote the natural numbers. Then we have $\mathbf{N} \models t = t'$ for the following equations $t = t'$:

- $(\forall x)\ \ x + 0 = x$
- $(\forall x, y)\ \ x + y = y + x$
- $(\forall x, y, z)\ \ x + (y + z) = (x + y) + z$
- $(\forall x)\ \ x * 1 = x$
- $(\forall x, y)\ \ x * y = y * x$
- $(\forall x, y, z)\ \ x * (y * z) = (x * y) * z$

Examples of Satisfaction (II)

A permutation on n elements is a bijective function $\pi : [n] \longrightarrow [n]$, where $[n] = \{1, \ldots, n\}$. The set of all such permutations is denoted S_n and has function composition as a binary operation $_ \circ _$ for which the identity permutation $1_{[n]} : [n] \longrightarrow [n]$ is an identity element. Also, for each $\pi \in S_n$ the inverse function π^{-1} is another permutation such that, $\pi \circ \pi^{-1} = 1_{[n]} = \pi^{-1} \circ \pi$. S_n is called the symmetric group on n elements, because it satisfies the group theory axioms,

$(\forall x, y, z)\ \ x \circ (y \circ z) = (x \circ y) \circ z$ (associativity)
$(\forall x)\ \ x \circ 1 = x = 1 \circ x$ (identity)
$(\forall x)\ \ x \circ x^{-1} = 1 = x^{-1} \circ x$ (inverse)

Similarly, given a set X of elements, the set X^* of its strings with the concatenation operation is a monoid, because it satisfies the above associativity and identity axioms.

Satisfaction of Conditional Equations

A Σ-algebra A satisfies the universally quantified conditional equation,

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

written,

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

iff for all assignments $a : X \longrightarrow A$ such that $A, a \models u_i = v_i$, $1 \leq i \leq n$, we have $A, a \models t = t'$.

Models and Theorems of Theories

Given an order-sorted equational theory $T = (\Sigma, E)$, where E may contain conditional equations, and given a Σ-algebra A we write $A \models T$, or, equivalently, $A \models E$, if A satisfies all the equations in E. We then call A a model of T, or a T-algebra. For example, for T the theory groups (resp. monoids), a model of T is called a group (resp. a monoid).

Given a theory T, what other equations, besides those in T, does a T-algebra satisfy? We call an equation $(\forall X)\, t = t'$ a theorem of T iff for each T-algebra A we have, $A \models (\forall X)\, t = t'$. For example, the equations $1^{-1} = 1$ and $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$ are satisfied by any group and are therefore theorems in group theory. Can we derive all such theorems logically from the axioms of T?

Equational Deduction

How can we prove that a given equation e is a theorem of an equational theory T? We can do so by giving appropriate inference rules.

Given an equational theory $T = (\Sigma, E)$, with Σ as always assumed sensible, and a set E of possibly conditional Σ-equations, we say that an unconditional equation $(\forall X)\, t = t'$ is derivable from E, written $E \vdash (\forall X)\, t = t'$, iff it can be obtained by finite application of the following rules:

- **Reflexivity**. For each family of variables X with $t \in T_\Sigma(X)$,

$$\frac{}{(\forall X)\, t = t}$$

Equational Deduction (II)

- **Symmetry**.

$$\frac{(\forall X)\ t = t'}{(\forall X)\ t' = t}$$

- **Transitivity**.

$$\frac{(\forall X)\ t = t' \qquad (\forall X)\ t' = t''}{(\forall X)\ t = t''}$$

- **Congruence**. For $f : s_1 \dots s_n \to s$, $f : s'_1 \dots s'_n \to s'$ in Σ with $s_1 \dots s_n s \equiv_{\leq} s'_1 \dots s'_n s'$, and for $t_i \in T_\Sigma(X)_{s_i}$, $t'_i \in T_\Sigma(X)_{s'_i}$, $1 \leq i \leq n$,

$$\frac{(\forall X)\ t_1 = t'_1 \quad \dots \quad (\forall X)\ t_n = t'_n}{(\forall X)\ f(t_1, \dots, t_n) = f(t'_1, \dots, t'_n)}$$

Equational Deduction (III)

- **Modus ponens**. For families of variables X, Y, a substitution $\theta : X \to T_\Sigma(Y)$, and a conditional equation in E

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

$$\frac{(\forall Y)\ \overline{\theta}(u_1) = \overline{\theta}(v_1) \quad \ldots \quad (\forall Y)\ \overline{\theta}(u_n) = \overline{\theta}(v_n)}{(\forall Y)\ \overline{\theta}(t) = \overline{\theta}(t')}$$

We call $\vdash$ the provability relation, and define $T \vdash (\forall X)\ t = t'$ iff $E \vdash (\forall X)\ t = t'$.

Proof Trees

Note that proofs in this inference system can always be displayed as proof trees, with the theorem proved as the root of the tree and all leaves closed (no premisses left). An incomplete proof tree will have some pending goals to be closed in its leaves. For example, in the theory of groups (see Lecture 3, page 36) the theorem $1^{-1} = 1$ has the following (complete) proof tree, where on the left subtree we have used modus ponens and symmetry, on the right subtree modus ponens, and at the bottom transitivity):

$$\dfrac{\dfrac{\dfrac{}{1 \circ 1^{-1} = 1^{-1}}}{1^{-1} = 1 \circ 1^{-1}} \qquad \dfrac{}{1 \circ 1^{-1} = 1}}{1^{-1} = 1}$$

Soundness and Completeness

Given these rules of inference we can ask two fundamental questions:

- (**Soundness**): are they correct? that is, if T proves a given equation e is then e always a theorem of T? Mathematically this is the implication

$$T \vdash (\forall X)\, t = t' \quad \Rightarrow \quad T \models (\forall X)\, t = t'.$$

- (**Completeness**): are they powerful enough to prove all the theorems of T? Mathematically this is the implication

$$T \vdash (\forall X)\, t = t' \quad \Leftarrow \quad T \models (\forall X)\, t = t'.$$

Soundness and Completeness (II)

The answer to these two questions are both on the affirmative, so that we have indeed the following equivalece

$$T \vdash (\forall X)\, t = t' \quad \Leftrightarrow \quad T \models (\forall X)\, t = t'.$$

The proof of soundness is given in detail in the electronic lecture notes of CS 476; the proof of completeness is left for a sequence of exercises in that same course. Due to time limitations we will not give such proofs in this course.

Initiality of T_Σ

We say that a Σ-algebra I is initial iff for every Σ-algebra A there is a unique Σ-homorphism from I to A.

It is not hard to prove by induction on the depth of terms that given a sensible order-sorted signature Σ for any Σ-algebra A the recursive definitions

- $eval_A(a) = a_A$, for a a constant in Σ
- $eval_A(f(t_1, \ldots, t_n)) = f_A(eval_A(t_1), \ldots, eval_A(t_n))$, for f a nonconstant operator in Σ

indeed define a Σ-homomorphism $eval_A : T_\Sigma \longrightarrow A$, and that there is no other homomorphism possible from T_Σ to A. Therefore T_Σ is indeed initial. A detailed proof can again be found in the electronic lecture notes of CS 476.

Construction of the Initial Algebra $T_{\Sigma/E}$

We have already shown the initiality of T_Σ for the class of all Σ-algebras, that we shall denote by $\mathbf{Alg}_\Sigma$. What we are really interested in is the more general construction of an initial algebra in the class of all models of a given equational theory $T = (\Sigma, E)$. That is, of an algebra that is initial in the class,

$$\mathbf{Alg}_{(\Sigma,E)} = \{A \in \mathbf{Alg}_\Sigma \mid A \models E\}.$$

We shall construct such an initial T-algebra, denoted $T_{\Sigma/E}$. If the equations E are confluent and terminating there will be an isomorphism $T_{\Sigma/E} \cong Can_{\Sigma/E}$.

Remark: A Maude functional module `fmod`(Σ, E)`endfm`, has an initial algebra semantics, given by $T_{\Sigma/E}$.

Construction of $T_{\Sigma/E}$ (II)

We can construct $T_{\Sigma/E}$ out of the provability relation. First of all, note that, for terms without variables $t, t' \in T_\Sigma$ that have sorts related by $\equiv_\leq$, our general notation for quantified equations specializes to the notation $(\forall \emptyset)\ t = t'$, where $\emptyset$ denotes the empty family of variables (that is, for each $s \in S$ the set of variables is empty). Note that we have, $\Sigma(\emptyset) = \Sigma$, and therefore $T_\Sigma(\emptyset) = T_\Sigma$.

Then, for each conected component C in the poset of sorts $(S, \leq)$ consider the set $T_{\Sigma,C} = \cup_{s \in C} T_{\Sigma,s}$. We can define an equivalence relation $\equiv_E$ on any such $T_{\Sigma,C}$ as follows:

$$t \equiv_E t' \quad \Leftrightarrow \quad E \vdash (\forall \emptyset)\ t = t'.$$

Construction of $T_{\Sigma/E}$ (III)

Note that $\equiv_E$ is indeed an equivalence relation because of the **Reflexivity**, **Symmetry** and **Transitivity** rules in our inference system. Denote by $T_{\Sigma/E,C}$ the quotient set $T_{\Sigma,C}/\equiv_E$.

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

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

We can then make $T_{\Sigma/E}$ into a Σ-algebra as follows. We interpret a constant $a : nil \longrightarrow s$ in Σ by its equivalence class $[a]$, which obviously does not depend on our choice of the subsort-overloaded declaration $a : nil \longrightarrow s$ for a.

Construction of $T_{\Sigma/E}$ (IV)

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

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

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

Checking that (assuming as always Σ sensible) 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 a Σ-algebra is left as an easy exercise.

Initiality Theorem for $T_{\Sigma/E}$

Theorem: $T_{\Sigma/E} \models E$. Furthermore, $T_{\Sigma/E}$ is initial in the class $\mathbf{Alg}_{(\Sigma,E)}$. That is, for any $A \in \mathbf{Alg}_{(\Sigma,E)}$ there is a unique Σ-homomorphism $eval_A^E : T_{\Sigma/E} \longrightarrow A$.

Again , the detailed proof of this theorem is given in the CS 476 electronic lecture notes.

The key intuition behid this proof is that if $A \models E$, the defining equality

$$eval_A^E([t]) = evalA(t)$$

is indeed independent of the choice of t, and therefore it correctly defines an S-indexed family of functions $eval_A^E : T_{\Sigma/E} \longrightarrow A$ which is a Σ-homomorphism and is indeed unique.

The Canonical Term Algebra is Initial

Theorem: Assume that the equations in $T = (\Sigma, E)$ are ground confluent and terminating. Then, $Can_{\Sigma/E}$ is isomorphic to $T_{\Sigma/E}$ and is therefore initial in $\mathbf{Alg}_{(\Sigma,E)}$.

Proof: It is easy to see that if A is initial for a given class of algebras and B is isomorphic to A, then B is also initial for that class. We just have to show the isomorphism.

Define for each $s \in S$ a function $can_{E,s} : T_{\Sigma/E,s} \longrightarrow Can_{\Sigma/E,s}$ by, $can_{E,s}[t] = can_E(t)$. This is independent of the choice of t and therefore well-defined because, by definition of $\equiv_E$, we have $t \equiv_E t'$ iff $E \vdash (\forall \emptyset)\ t = t'$ iff (by E confluent) $t \downarrow_E t'$, iff $can_E(t) = can_E(t')$. Furthermore, $can_{E,s}$ is surjective by construction and injective because of the above chain of equivalences; therefore it is bijective.

The Canonical Term Algebra is Initial (II)

Let us see that $can_E : T_{\Sigma/E} \longrightarrow Can_{\Sigma/E}$ 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,

$$can_{E,s}(f^{s_1 \dots s_n,s}_{T_{\Sigma/E}}([t_1], \dots, [t_n])) = f^{s_1 \dots s_n,s}_{Can_{\Sigma/E}}(can_E(t_1), \dots, can_E(t_n)).$$

The key observation is that $can_E(t_i) \in T_{\Sigma,s_i}$, $1 \leq i \leq n$. 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 $t'_i \stackrel{*}{\longrightarrow}_E can(t'_i) = can(t_i)$, if $t'_i \in T_{\Sigma,s_i}$, $1 \leq i \leq n$, then $can_E(t_i) \in T_{\Sigma,s_i}$, $1 \leq i \leq n$.

The Canonical Term Algebra is Initial (III)

Therefore, we have:

$can_{E,s}(f^{s_1 \ldots s_n, s}_{T_{\Sigma/E}}([t_1], \ldots, [t_n])) =$ (by definition of $f^{s_1 \ldots s_n, s}_{T_{\Sigma/E}}$)
$can_{E,s}([f(can_E(t_1), \ldots, can_E(t_n))]) =$ (by definition of $can_{E,s}$)
$can_E(f(can_E(t_1), \ldots, can_E(t_n))) =$ (by definition of $f^{s_1 \ldots s_n, s}_{Can_{\Sigma/E}}$)
$f^{s_1 \ldots s_n, s}_{Can_{\Sigma/E}}(can_E(t_1), \ldots, can_E(t_n))$

as desired.

Checking that the inverse family of functions
$can^{-1}_E = \{can^{-1}_{E,s}\}_{s \in S}$ defines also a Σ-homomorphism is easy.
For $f : s_1 \ldots s_n \to s$ in Σ and $t_i = can_E(t_i) \in Can_{\Sigma/E,s_i}$,
$1 \leq i \leq n$ we have,

The Canonical Term Algebra is Initial (IV)

$$can^{-1}_{E,s}(f^{s_1 \ldots s_n, s}_{Can_{\Sigma/E}}(t_1, \ldots, t_n)) =$$
$$[can_E(f(t_1, \ldots, t_n))] =$$
$$[f(t_1, \ldots, t_n)] =$$
$$f^{s_1 \ldots s_n, s}_{T_{\Sigma/E}}([t_1], \ldots, [t_n]) =$$
$$f^{s_1 \ldots s_n, s}_{T_{\Sigma/E}}(can^{-1}_E(t_1), \ldots, can^{-1}_E(t_n))$$

as desired. q.e.d.