Program Verification: Lecture 10

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

More on $\Sigma(X)$-Algebras

Recall how we formalized the evaluation of integer arithmetic expressions with memory $m : X \to \mathbf{Z}$ as the unique $\Sigma(X)$-homomorphism:

$$\_{(\mathcal{Z},m)} : \mathcal{T}_{\Sigma(X)} \to (\mathcal{Z}, m)$$

where $(\mathcal{Z}, m)$ extends the integer Σ-algebra $\mathcal{Z} = (\mathbf{Z}, \_{\mathcal{Z}})$ by interpreting the constants X as the memory map $m : X \to \mathbf{Z}$.

This situation is completely general: For any signature Σ and any Σ-algebra $\mathcal{A} = (A, \_{\mathcal{Z}})$, given an assignment, i.e., a "memory map," $a : X \to A$, the evaluation of $\Sigma(X)$-expressions in $\mathcal{A}$ is the unique $\Sigma(X)$-homomorphism:

$$\_{(\mathcal{A},a)} : \mathcal{T}_{\Sigma(X)} \to (\mathcal{A}, a)$$

Abbreviated Notation: $\_{(\mathcal{A},a)} = \_a_{\mathcal{A}}$.

More $\Sigma(X)$-Algebras (II)

We can summarize this situation as the following:

Fact 1: Any pair $(\mathcal{A}, a)$ with $\mathcal{A} = (A, \_\mathcal{A})$ a Σ-algebra and $a : X \to A$ an assignment defines a $\Sigma(X)$-algebra $(\mathcal{A}, a)$.

Q: Are all $\Sigma(X)$-algebras of this form?

A: Yes! We just need to recall the definition of an order-sorted Σ-algebra in Lecture 3:

For $\Sigma = ((S, \leq), F))$ a signature, Σ-algebra $\mathcal{A} = (A, \_\mathcal{A})$ is just a pair with: (i) A an S-sorted set, and (ii) $\_\mathcal{A}$ a function $\_\mathcal{A} : f \mapsto f_\mathcal{A}$ interpreting each constant $c :\to s$ as an element $c_\mathcal{A} \in A_s$, and each symbol $f : w \to s$ in Σ as a function $f_\mathcal{A} \in [A^w \to A_s]$, with f overloaded agreeing on common data.

More $\Sigma(X)$-Algebras (III)

Therefore, if $\Sigma = ((S, \leq), F))$, then $\Sigma(X) = ((S, \leq), F \uplus X))$, where each new constant $x \in X_s$ has typing $x :\to s$, and $\uplus$ denotes disjoint union of sets.

Recall from STACS that if sets U and V are disjoint, any function $h : U \uplus V \to W$ decomposes uniquely as a pair $(h|_U : U \to W, h|_V : V \to W)$ of its restrictions to U and V.

Therefore, if $\mathcal{B} = (B, \_{\mathcal{B}})$ is a $\Sigma(X)$-algebra, then $\_{\mathcal{B}}$ decomposes uniquely as a pair $(\_{\mathcal{B}}|_F, \_{\mathcal{B}}|_X)$. But note that $\_{\mathcal{B}}|_X : X \to B$ is just an assignment! and $(B, \_{\mathcal{B}}|_F)$ is just a Σ-algebra! **Notation:** $(B, \_{\mathcal{B}}|_F) = \mathcal{B}|_\Sigma$, the Σ-reduct of $\mathcal{B}$.

Fact 2: $\mathcal{B} = (B, \_{\mathcal{B}})$ decomposes uniquely as $\mathcal{B} = (\mathcal{B}|_\Sigma, \_{\mathcal{B}}|_X)$.

More $\Sigma(X)$-Homomorphisms

Facts 1 and 2 tell us that any $\Sigma(X)$-algebra is exactly the same thing as a pair $(\mathcal{A}, a)$ with $\mathcal{A}$ a Σ-algebra and $a \in [X \to A]$ an assignment.

Q: What is a $\Sigma(X)$-homomorphism $h : (\mathcal{A}, a) \to (\mathcal{C}, c)$?

A: The answer is summarized in **Fact 3** below.

Fact 3: Since h must preserve both the Σ-symbols F and the constants X but $F \cap X = \emptyset$, h is exactly:

1. a Σ-homomorphism $h : \mathcal{A} \to \mathcal{C}$ such that

2. for each $s \in S$, $x \in X_s$, $h_s(a(x)) = c(x)$, i.e., $a; h = c$.

Example: Substitutions Revisited

Let us apply **Fact 2** to the initial $\Sigma(X)$-algebra $\mathcal{T}_{\Sigma(X)} = (T_{\Sigma(X)}, \_\mathcal{T}_{\Sigma(X)})$. What unique decomposition do we get for $\mathcal{T}_{\Sigma(X)}$? We get a pair $(\mathcal{T}_{\Sigma(X)}|_{\Sigma}, \eta_X)$, where:

1. $\mathcal{T}_{\Sigma(X)}|_{\Sigma} = (T_{\Sigma(X)}, \_\mathcal{T}_{\Sigma(X)}|_F)$, that is, the elements $t \in T_{\Sigma(X)}$ are the same: (Σ-terms with variables in X), but only the Σ-operations are considered; and

2. $\eta_X : X \to T_{\Sigma(X)} : x \mapsto x$ is the identity interpretation for each variable x in X, that is, the identity substitution.

To simplify the notation, we will denote $\mathcal{T}_{\Sigma(X)}|_{\Sigma}$ by $\mathcal{T}_{\Sigma}(X)$, and will call it the free Σ-algebra on the variables X.

Example: Substitutions Revisited (II)

Consider now another S-sorted set Y of variables and a substitution $\theta : X \to T_{\Sigma(Y)}$.

Q: how can we model the extension of θ to the map on terms $\_\theta : T_{\Sigma(X)} \to T_{\Sigma(Y)}$ defined in Lecture 3?

A: Easy! Consider the $\Sigma(X)$-algebra $(\mathcal{T}_\Sigma(Y), \theta)$. Then $\_\theta$ is just the unique $\Sigma(X)$-homomorphism:

$$\_\theta = \_\theta_{\mathcal{T}_\Sigma(Y)} : \mathcal{T}_{\Sigma(X)} \to (\mathcal{T}_\Sigma(Y), \theta),$$

which decomposing $\mathcal{T}_{\Sigma(X)}$ as $\mathcal{T}_{\Sigma(X)} = (\mathcal{T}_\Sigma(X), \eta_X)$, is the unique $\Sigma(X)$-homomorphism:

$$\_\theta : (\mathcal{T}_\Sigma(X), \eta_X) \to (\mathcal{T}_\Sigma(Y), \theta).$$

Example: Substitutions Revisited (III)

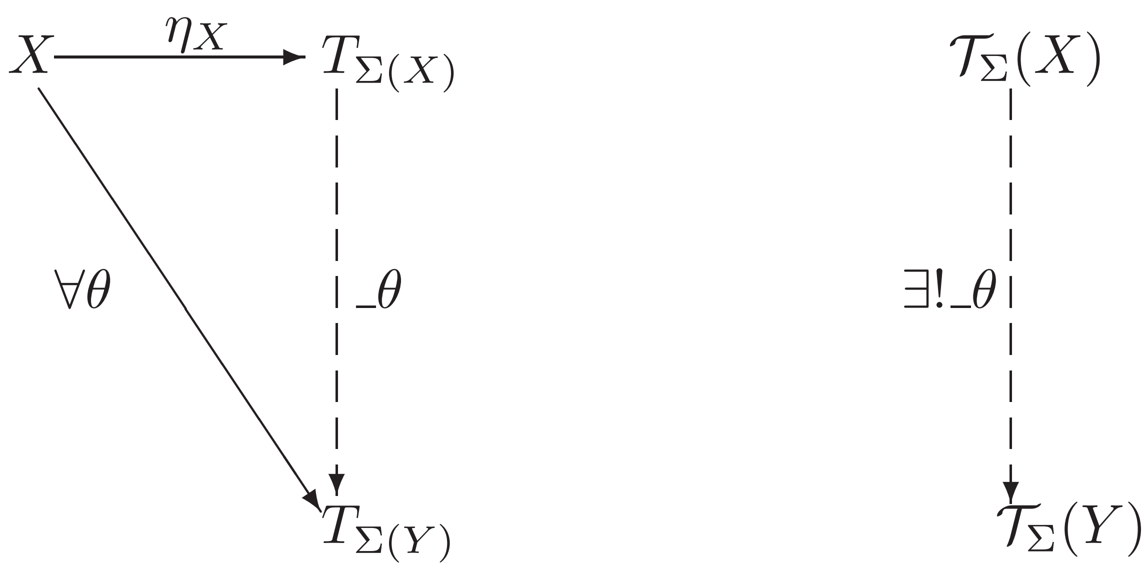
But by **Fact 3**, $\_\theta : (\mathcal{T}_\Sigma(X), \eta_X) \to (\mathcal{T}_\Sigma(Y), \theta)$ is a $\Sigma(X)$-homomorphism iff:

1. $\_\theta : \mathcal{T}_\Sigma(X) \to \mathcal{T}_\Sigma(Y)$ is a Σ-homomorphism, and

2. $\eta_X ; \_\theta = \theta$

Therefore, each substitution θ has a unique extension to a Σ-homomorphism $\_\theta$ such that the following diagram commutes:

Homomorphic Extension of Substitutions



$\mathbf{Set}^S$: S-Indexed Families and S-Indexed Functions

$\mathbf{Alg}_\Sigma$: Σ-Algebras and Σ-Homomorphism

Freeness Theorem

The extension $\theta \mapsto \_\theta$ is an instance of the more general:

Theorem (Freeness Theorem). For each Σ-algebra $\mathcal{A} = (A, \_\mathcal{A})$, and assignment $a : X \longrightarrow A$ there exists a unique Σ-homomorphism $\_a_{\mathcal{A}} : \mathcal{T}_{\Sigma}(X) \longrightarrow \mathcal{A}$ such that $\eta_X ; \_a_{\mathcal{A}} = a$.

Proof: Since $(\mathcal{A}, a)$ is a $\Sigma(X)$-algebra, by the initiality of $\mathcal{T}_{\Sigma(X)}$ there is a unique $\Sigma(X)$-homomorphism

$$\_a_{\mathcal{A}} : \mathcal{T}_{\Sigma(X)} \to (\mathcal{A}, a),$$

which decomposing $\mathcal{T}_{\Sigma(X)}$ as $\mathcal{T}_{\Sigma(X)} = (\mathcal{T}_{\Sigma}(X), \eta_X)$, is the same thing as a unique $\Sigma(X)$-homomorphism:

$$\_a_{\mathcal{A}} : (\mathcal{T}_{\Sigma}(X), \eta_X) \to (\mathcal{A}, a),$$

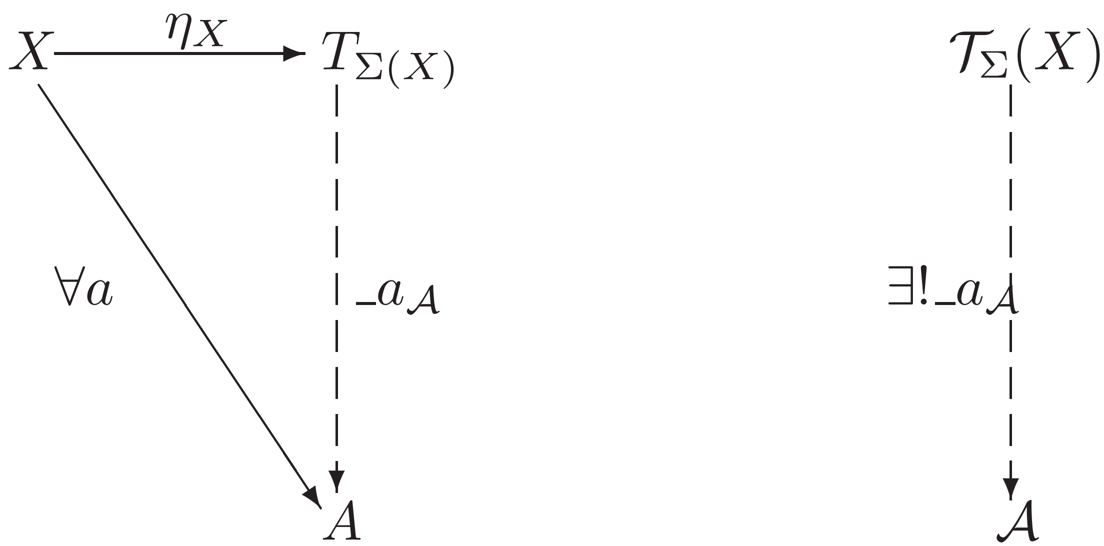
which by the definition of $\Sigma(X)$-homomorphism is the same thing as a unique Σ-homomorphism

$$\_a_{\mathcal{A}} : \mathcal{T}_{\Sigma}(X) \to \mathcal{A}$$

such that $\eta_X ; \_a_{\mathcal{A}} = a$, as desired. q.e.d.

This theorem can be summarized in the following diagram:

$\mathcal{T}_\Sigma(X)$ as a Free Σ-Algebra on X



$\mathbf{Set}^S$: S-Indexed Families and S-Indexed Functions $\mathbf{Alg}_\Sigma$: Σ-Algebras and Σ-Homomorphism

Useful Corollary on Free Σ-Algebras

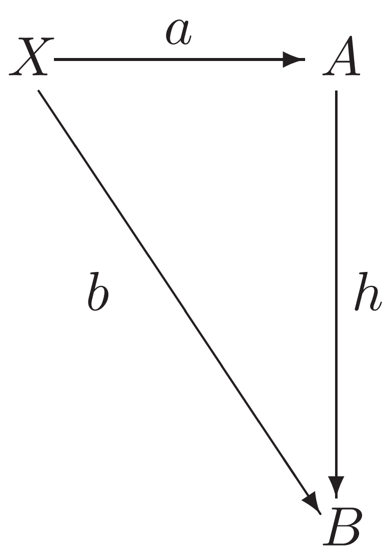
Corollary (Freeness Corollary). For any Σ-homomorphism $h : \mathcal{A} \longrightarrow \mathcal{B}$, and assignments $a : X \longrightarrow A$, $b : X \longrightarrow B$ such that $a; h = b$, the following identity between Σ-homomorphisms holds:

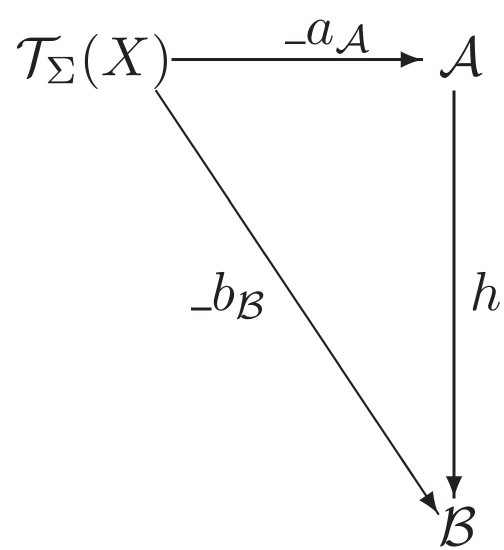
$$\_a_{\mathcal{A}}; h = \_b_{\mathcal{B}}$$

Proof: $\_a_{\mathcal{A}}; h$ is a Σ-homomorphism $\_a_{\mathcal{A}}; h : \mathcal{T}_{\Sigma}(X) \longrightarrow \mathcal{B}$. But since, by hypothesis, we have $a; h = b$, we must also have: $\eta_X; \_a_{\mathcal{A}}; h = a; h = b$, which by the Freeness Theorem forces $\_a_{\mathcal{A}}; h = \_b_{\mathcal{B}}$, as desired. q.e.d.

The corollary can be summarized in the following diagram:

Useful Corollary on Free Σ-Algebras (II)





$\mathbf{Set}^S$: S-Indexed Families and S-Indexed Functions

$\mathbf{Alg}_\Sigma$: Σ-Algebras and Σ-Homomorphism

What is "free" about a Free Algebra?

Clearly, the concept of a free Σ-algebra $\mathcal{T}_\Sigma(X)$ generalizes the case of an initial algebra, since when $X = \emptyset$, where $\emptyset$ here denotes the S-indexed set having all its components empty, we have $\mathcal{T}_\Sigma(\emptyset) = \mathcal{T}_\Sigma$. As in the case of initial algebras, free algebras have (provided Σ is sensible) no confusion. Therefore, the first meaning of "free" is that no equalities force terms in $\mathcal{T}_\Sigma(X)$ to become equal: they are all different, unconstrained, and in this sense "free."

Note that if X is nonempty $\mathcal{T}_\Sigma(X)$ has junk! (even though, $\mathcal{T}_{\Sigma(X)}$, with the same data elements, doesn't!). Which junk? Well, X, of course, and all the junk spread by X when building terms with variables. However, this "junk" is very well-behaved.

What is "free" about a Free Algebra? (II)

X is well-behaved: we can feely interpret the variables in X as data elements in any Σ-algebra $\mathcal{B}$ by any assignment $b : X \longrightarrow B$ with the guarantee that b will always extend to a unique Σ-homomorphism $\_b_{\mathcal{B}}$. This free interpretation and free extensibility is the second meaning of "free."

This freedom is not enjoyed by other algebras. Let Σ be the unsorted signature with constant 0 and unary s. $\mathcal{T}_\Sigma$ is the natural numbers in Peano notation. Define $\mathcal{T}_\Sigma \cup \{x, y, z\}$ with elements $T_\Sigma \cup \{x, y, z\}$, with 0 and s interpreted as before on the T_Σ part, and with $s(x) = y$, $s(y) = z$, and $s(z) = x$. Now the junk $X = \{x, y, z\}$ is badly behaved. Let $\mathbb{N}$ be the natural numbers in decimal notation with 0 and succesor. There is no assignment at all $b : X \longrightarrow \mathbb{N}$ that can be extended to a Σ-homomorphism $\mathcal{T}_\Sigma \cup \{x, y, z\} \longrightarrow \mathbb{N}$.

Satisfaction of Equations

Let $X = \{X_s\}$ be such that for each $s \in S$, X_s is a countably infinite set. Given a Σ-algebra $\mathcal{A}$, an assignment $a : X \longrightarrow A$, and a Σ-equation $t = t'$ with variables in X, we define the satisfaction relation $(\mathcal{A}, a) \models t = t'$ by means of the equivalence,

$$(\mathcal{A}, a) \models t = t' \quad \Leftrightarrow \quad t\, a_{\mathcal{A}} = t'\, a_{\mathcal{A}}.$$

We then define the satisfaction relation $\mathcal{A} \models t = t'$ iff for all assignments $a : X \longrightarrow A$ we have $(\mathcal{A}, a) \models t = t'$.

Note that, since each $(\mathcal{A}, a)$ is a $\Sigma(X)$-algebra, we have defined the satisfaction of $\mathcal{A} \models t = t'$ as the satisfaction of the ground $\Sigma(X)$-equation $t = t'$ by each $(\mathcal{A}, a)$, denoted $(\mathcal{A}, a) \models t = t'$, for all assignments a.

Examples of Satisfaction

Consider the unsorted signature Σ with constants $0, 1$, and operations of addition $\_ + \_$, and multiplication $\_ * \_$. Then all the algebras $\mathbb{N}$, $\mathbb{N}_k$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, in Lecture 2, pp. 27-28, satisfy the equations:

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

Examples of Satisfaction (II)

Consider the signature Σ for Boolean operations in page 29 of Lecture 2. Then all Σ-algebras $\mathbf{B}$, $\mathcal{P}(X)$, $\mathbf{B}^X$, and $[0,1]$ satisfy the equations:

- $x\ and\ true = x \qquad (\forall x)\ \ x\ or\ false = x$
- $x\ and\ y = y\ and\ x \qquad (\forall x, y)\ \ x\ or\ y = y\ or\ x$
- $x\ and\ (y\ and\ z) = (x\ and\ y)\ and\ z$
- $x\ or\ (y\ or\ z) = (x\ or\ y)\ or\ z$
- $x\ and\ x = x \qquad x\ or\ x = x$

Examples of Satisfaction (III)

Consider the `NAT-LIST` signature in Lecture 2, and the two algebras for it defined in Lecture 2, pages 34–35. Show that the first algebra (where the sort `List` is interpreted as finite strings of natural numbers) satisfies all the equation in the module `NAT-LIST`.

Show also that the second algebra (where the sort `List` is interpreted as finite sets of natural numbers) does not satisfy the equation

```
eq length(N . L) = s length(L) .
```

Examples of Satisfaction (IV)

Consider all the examples 1–6, and the first version of example 7, of algebras for the "vector-space-like" signature of Picture 2.4 defined in pages 35–38 of Lecture 2. Prove that, for x, y variables of sort `Scalar`, and v, v' variables of sort `Vector`, all these algebras satisfy the equations:

- $(x + y).v = (x.v) + (y.v)$
- $x.(v + v') = (x.v) + (x.v')$
- $0.v = \vec{0}$
- $1.v = v$

Examples of Satisfaction (V)

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,

$x \circ (y \circ z) = (x \circ y) \circ z \quad$ (associativity)
$x \circ 1 = x = 1 \circ x \quad$ (identity)
$x \circ x^{-1} = 1 = x^{-1} \circ x \quad$ (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.

Models and Theorems of Theories

Given an order-sorted equational theory (Σ, E) and a Σ-algebra $\mathcal{A}$, we write $\mathcal{A} \models (\Sigma, E)$, or, equivalently, $\mathcal{A} \models E$, iff $\mathcal{A}$ satisfies all the equations in E. We then call $\mathcal{A}$ a model of (Σ, E), or a (Σ, E)-algebra. For example, for (Σ, E) the theory groups (resp. monoids), a model of (Σ, E) is called a group (resp. a monoid).

Given a theory (Σ, E), what other equations, besides those in E, does any (Σ, E)-algebra satisfy? We call an equation $t = t'$ a theorem of (Σ, E) iff for each (Σ, E)-algebra $\mathcal{A}$ we have, $\mathcal{A} \models t = t'$. We then write $(\Sigma, E) \models t = t'$.

We have now two different relations: (i) $(\Sigma, E) \vdash t = t'$, telling us which equations we can mechanically prove, and (ii) $(\Sigma, E) \models t = t'$, telling us which equations are theorems.

Soundness and Completeness

There are now two obvious questions:

Soundness: Does the implication

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

always hold? That is, is anything we can prove always true, i.e., always a theorem? For example, we can prove the equations $1^{-1} = 1$ and $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$ from the theory of groups, but are they really theorems of group theory?

Completeness: Does the implication

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

always hold? That is, can we prove all the equations that are theorems of (Σ, E)?

Soundness Theorem

Soundness Theorem. For (Σ, E) an equational theory with Σ sensible, kind-complete, and with nonempty sorts, and 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

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

Therefore, what we have to prove is the implication

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

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

Soundness Theorem (II)

Base Case. If the length of $t \rightarrow^* t'$ 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 $\mathcal{A}$ we have $\mathcal{A} \models t = t$. In particular, if $\mathcal{A} \models E$, then, of course, $\mathcal{A} \models t = t$.

Induction Step. Assume that if $(\Sigma, \overrightarrow{E} \cup \overleftarrow{E}) \vdash t \rightarrow^* w$ and the sequence $t \rightarrow^* w$ has length n, then the relation $(\Sigma, E) \models t = w$ holds, and consider an additional rewrite step $w \rightarrow_{\overrightarrow{E} \cup \overleftarrow{E}} t'$. 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 $w \rightarrow_{\overrightarrow{E} \cup \overleftarrow{E}} t'$ then $(\Sigma, E) \models w = t'$.

Soundness Theorem (III)

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

$$t\, a_{\mathcal{A}} = w\, a_{\mathcal{A}} \quad \wedge \quad w\, a_{\mathcal{A}} = t''\, a_{\mathcal{A}}$$

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

Proof of the Lemma. We must prove the implication $w \to_{\overrightarrow{E} \cup \overleftarrow{E}} t' \Rightarrow (\Sigma, E) \models w = t'$. But the rewrite $w \to_{\overrightarrow{E} \cup \overleftarrow{E}} t'$. 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 $\theta : X \to T_{\Sigma(X)}$, 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 $\mathcal{A}$ such that $\mathcal{A} \models E$ and each assignment a we have $(\mathcal{A}, a) \models u\theta = v\theta$, that is, that $u\,\theta\,a_{\mathcal{A}} = v\,\theta\,a_{\mathcal{A}}$.

But by the Freeness Corollary and definition of $\_\theta$ we have:

$$\_\theta\,;\,\_a_{\mathcal{A}} = (\eta_X; \_\theta; \_a_{\mathcal{A}})_{\mathcal{A}} = (\theta\,;\,\_a_{\mathcal{A}})_{\mathcal{A}}$$

And since $\mathcal{A} \models E$ and $(\theta; \_a_{\mathcal{A}}) \in [X \to A]$, in particular, $(\mathcal{A}, (\theta\,;\,\_a_{\mathcal{A}})) \models u = v$, that is, $u\,\theta\,a_{\mathcal{A}} = v\,\theta\,a_{\mathcal{A}}$, as desired.

Soundness Theorem (V)

Induction Hypothesis. 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 $\mathcal{A} \models E$ then $\mathcal{A} \models w_i[u\theta]_p = w_i[v\theta]_p$. Therefore, for any assignment $a \in [X \to A]$ we have:

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

as desired. q.e.d.

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

Exercises

Ex.10.1 For a subsignature $\Sigma = ((S, \leq), F) \subseteq \Sigma' = ((S, \leq), F')$ and $\mathcal{A} = (A, \_\mathcal{A})$ a Σ'-algebra, define its Σ-reduct $\mathcal{A}|_\Sigma$ as the Σ-algebra $\mathcal{A}|_\Sigma = (A, \_\mathcal{A}|_F)$. Prove that for any Σ-equation $u = v$ we have the equivalence:

$$\mathcal{A} \models u = v \quad \Leftrightarrow \quad \mathcal{A}|_\Sigma \models u = v.$$

Ex.10.2 (i) Let $h : \mathcal{A} \longrightarrow \mathcal{B}$ be a Σ-isomorphism, and $u = v$ a Σ-equation. Prove that

$$\mathcal{B} \models u = v \quad \Leftrightarrow \quad \mathcal{A} \models u = v.$$

(ii) Give an example of a bijective Σ-homomorphism h such that the above equivalence does not hold (**Hint**: Consider order-sorted signatures Σ that are not kind-complete).

Exercises (II)

Ex.10.3 Call a Σ-algebra $\mathcal{A}$ a subalgebra of a Σ-algebra $\mathcal{B}$ iff for each sort $s \in S$ we have $A_s \subseteq B_s$, and the S-family of inclusion functions $j = \{j_s : A_s \longrightarrow B_s\}_{s \in S}$, with $j_s : a \mapsto a$ mapping each element $a \in A_s$ identically to itself is a Σ-homomorphism $j : \mathcal{A} \longrightarrow \mathcal{B}$. We then write: $\mathcal{A} \subseteq \mathcal{B}$. Show that if $\mathcal{A} \subseteq \mathcal{B}$, for any Σ-equation $u = v$ we have:

$$\mathcal{B} \models u = v \quad \Rightarrow \quad \mathcal{A} \models u = v$$

Give an example showing that the implication in the other direction in general does not hold.

Exercises (II)

Ex.10.4 Let $h : \mathcal{A} \longrightarrow \mathcal{B}$ be a surjective Σ-homomorphism, and $u = v$ a Σ-equation. Prove that

$$\mathcal{A} \models u = v \quad \Rightarrow \quad \mathcal{B} \models u = v$$

Show, by giving a counterexample, that the implication in the other direction in general does not hold.