CS 524 Lecture 10

José Meseguer

2.1 Rewriting Logic: Statics [Continued]

Definition [unsorted signature]. An [unsorted] signature of function symbols is an $\mathbb{N}$-indexed family of sets $\Sigma = \{\Sigma_n\}_{n \in \mathbb{N}}$, where $f \in \Sigma_n$ is called an n-ary function symbol, and $a \in \Sigma_0$ is called a constant symbol.

Examples. 1. The signature of monoids is Σ_{MON} with $\Sigma_{MON,0} = \{1\}$, $\Sigma_{MON,2} = \{\_\cdot\_\}$, and $\Sigma_{MON,n} = \emptyset$ otherwise.

2. Likewise, the signature of commutative monoids Σ_{CMON} has $\Sigma_{CMON,0} = \{0\}$, $\Sigma_{CMON,2} = \{\_+\_\}$, $\Sigma_{CMON,n} = \emptyset$ otherwise

3. The signature Σ_{GRP} of groups adds to Σ_{MON} a unary symbol $(\_)^{-1}$. Likewise the signature of commutative groups Σ_{CGRP} adds to Σ_{CMON} the unary symbol $-\_$ [minus].

4. The <u>signature</u> of <u>rings</u> is just $\Sigma_{RNG} = \Sigma_{CMON} \cup \Sigma_{MON}$

<u>Definition</u> [Σ-terms]. Given a signature Σ, the set of its expressions, called <u>Σ-terms</u> is defined inductively as the smallest set T_Σ such that:

1. $\forall a \in \Sigma_0, \quad a \in T_\Sigma$
2. $\forall f \in \Sigma_n,\ n \geqslant 1,\ \forall t_1, .., t_n \in T_\Sigma \Rightarrow f(t_1, .., t_n) \in T_\Sigma.$

<u>Remark</u> If X, say, $X = \{x_1, .., x_n, ...\}$ or $X = \{x, y, -\}$ is a set of variables, assumed <u>disjoint</u> from Σ_0, then the set $T_\Sigma(X)$ of <u>Σ-terms with variables in</u> X is just, by definition, $T_\Sigma(X) = T_{\Sigma[X]}$, where,

$\Sigma[X]_0 = \Sigma_0 \cup X$, and $\Sigma[X]_n = \Sigma_n$ otherwise.

Note that a signature Σ is <u>just syntax</u>! $f \in \Sigma_n$ is an <u>uninterpreted function symbol</u>, <u>not</u> <u>a</u> <u>function</u>! in any sense whatsoever, but a <u>symbol</u> <u>for</u> a <u>function</u>. In fact, we can just think of a signature Σ as a grammar specifying the Σ-expressions. For example, Σ_{RNG} is just the grammar:

$$0 \mid 1 \mid -\text{TERM} \mid \text{TERM} + \text{TERM} \mid \text{TERM} \cdot \text{TERM}$$

So, how do we interpret function symbols f in Σ as actual functions?

Of course, by Σ-algebras!

Definition [Σ-algebra]. A Σ-algebra is a pair $\mathbb{A} = (A, \{f_A\}_{f \in \Sigma})$ where, A is a set, namely, its set of elements, and for each $f \in \Sigma_n$, f_A is an n-ary function $f_A : A^n \to A$ for $n \geq 1$, and for $a \in \Sigma_0$ it is an element $a_A \in A$.

Examples 1. The multisets $M(\{a,b,c\})$ on three elements are a Σ_{CMON} algebra, where $0_{M(\{a,b,c\})} = \emptyset$ [empty multiset], and

$$+_{M(\{a,b,c\})} =_{def} \lambda(u,v) \in M(\{a,b,c\})^2.\ u\,v \text{ [multiset union]}$$

2. The integers $\mathbb{Z}$ are a Σ_{RNG}-algebra

$\mathbb{Z} = (\mathbb{Z}, \{f_{\mathbb{Z}}\}_{f \in \Sigma_{RNG}})$ where $0_{\mathbb{Z}} = 0$, $1_{\mathbb{Z}} = 1$,

$+_{\mathbb{Z}} = \lambda(n,m) \in \mathbb{Z}^2.\ x+m \in \mathbb{Z}$, with $n+m$ <u>integer</u> <u>addition</u>, $\_\cdot\__{\mathbb{Z}} = \lambda(n,m) \in \mathbb{Z}^2.\ n \cdot m \in \mathbb{Z}$, with $n \cdot m$ integer multiplication, $-_{\mathbb{Z}} = \lambda n \in \mathbb{Z}.\ -n \in \mathbb{Z}$ with $-n$ the <u>additive inverse</u> of n in $\mathbb{Z}$.

For Combinatory logic we saw that any CL term $t = t(x_1, \ldots, x_n)$ defines a <u>function</u>

$$t : CL^n \longrightarrow CL$$
$$(u_1, \ldots, u_n) \longmapsto t\{x_1 \mapsto u_1, \ldots, x_n \mapsto u_n\}$$

But this is just an instance of a much more general phenomenon:

<u>Definition</u> [Function defined by a term $t \in T_\Sigma(X)$ on a Σ-algebra]. Let $X = \{x_1, x_2, \ldots, x_n, \ldots\}$, $n \in \mathbb{N}$, be a countable set of variables, and let $t \in T_\Sigma(X)$. By notational

<u>convention</u> we write $t = t(x_1, \dots, x_n)$ to <u>mean</u> that the variables <u>appearing</u> in t [there could be <u>none</u>, i.e., t could be a constant symbol] are <u>among</u> the $x_1, \dots, x_n$.

Then, given $t = t(x_1, \dots, x_n)$ and a Σ-algebra $A = (A, \{f_A\}_{f \in \Sigma})$, t defines an <u>n-ary function</u> $t_A : A^n \longrightarrow A$ defined inductively as follows:

1. If t is a constant $a \in \Sigma_0$, then
$$a_A = \lambda(a_1, \dots, a_n) \in A^n.\ a_A \in A$$
2. If $t = f(t_1, \dots, t_n)$, then
$$t_A = \lambda(a_1, \dots, a_n) \in A^n.\ f_A(t_{1_A}(a_1, \dots, a_n), \dots, t_{m_A}(a_1, \dots, a_n)) \in A$$

<u>Definition</u> [Equation and Satisfaction of an Equation in an Algebra].

1. A <u>Σ-equation</u> is a formula $t = t'$ with $t, t' \in T_\Sigma(X)$.
2. A Σ-algebra $A = (A, \{f_A\}_{f \in \Sigma})$ <u>satisfies</u> a Σ-equation $t = t'$, written $A \models t = t'$ <u>iff</u> $t_A = t'_A$, both viewed as n-ary functions if x_n is the biggest variable in

either t, or t' [the biggest of all variables in both].

3. An <u>equational theory</u> is a pair (Σ, E), where Σ is a signature and E is a <u>set</u> of Σ-equations.

4. A Σ-algebra $A = (A, \{f_A\}_{f \in \Sigma})$ is a (Σ, E)-<u>algebra</u> iff $\forall\, (u = v) \in E \quad A \models u = v$, abbreviated $A \models E$.

<u>Examples</u>. 1. The theory of <u>monoids</u> is $(\Sigma_{MON}, \{lid_{MON}, rid_{MON}, assoc_{MON}\})$-

where $lid_{MON} =_{def} (1 \cdot x_1 = x_1)$, $rid_{MON} =_{def} (x_1 \cdot 1 = x_1)$,

and $assoc_{MON} =_{def} ((x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3))$

For any alphabet Λ, the set of strings Λ^* is a Σ_{MON}-algebra with $1_{\Lambda^*} = \varepsilon$ (empty string), and with

$\_ \cdot \_{}_{\Lambda^*} = \lambda (u,v) \in \Lambda^*.\ uv \in \Lambda^*$ [string concatenation]

Furthermore, $(\Lambda^*, \{f_{\Lambda^*}\}_{f \in \Sigma_{MON}})$ is a $(\Sigma_{MON}, \{lid_{MON}, rid_{MON}, assoc_{MON}\})$-algebra, that is, a <u>monoid</u>.

2. The theory of <u>commutative monoids</u> is $(\Sigma_{CMON}, \{id_{CMON}, com_{CMON}, assoc_{CMON}\})$,

where $id_{CMON} =_{def.} (x_1 + 0 = x_1)$, and $com_{CMON} =_{def} (x_1 + x_2 = x_2 + x_1)$

$assoc_{CMON} =_{def} ((x_1 + x_2) + x_3 = x_1 + (x_2 + x_3))$

The Σ_{CMON}-algebra $\mathcal{M}(B) = (M(B), \{f_{M(B)}\}_{f \in \Sigma_{CMON}})$

of multisets is in fact a $(\Sigma_{CMON}, \{id_{CMON}, assoc_{CMON}\})$-algebra, i.e., a <u>commutative monoid</u>.

3. The <u>theory of commutative rings</u> is $(\Sigma_{RNG}, \{id_{CMON}, com_{CMON}, assoc_{CMON}, inv-,$

$idl_{MON}, comm_{MON}, assoc_{MON}, dist\})$, where

$comm_{MON} =_{def} (x_1 \cdot x_2 = x_2 \cdot x_1)$

$inv- =_{def} (x_1 + -x_1 = 0)$

$dist =_{def} (x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3))$

The integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are <u>all</u> (with the standard interpretations of $0, 1, +, -$ and $- \cdot -$) <u>commutative rings</u>, i.e., they <u>satisfy</u> all the above equations.

<u>Definition</u> [Σ-congruence on a Σ-algebra and quotient]

Given a Σ-algebra $A = (A, \{f_A\}_{f \in \Sigma})$, a <u>congruence</u> on A is an <u>equivalence relation</u> $\equiv \subseteq A^2$ such that for each $n \geq 1$ and each $f \in \Sigma_n$

($\ddagger$) If $a_1 \equiv a'_1$ and $\ldots$, $a_n \equiv a'_n$, then $f_A(a_1, \ldots, a_n) \equiv f_A(a'_1, \ldots, a'_n)$.

The quotient set $A = A/_{\equiv}$ of $\equiv$-equivalence classes <u>is</u> a Σ-algebra if $\equiv$ is a Σ-congruence. Namely,

1. For each $a \in \Sigma_0$, $a_{A/\equiv} = [a_A]_{\equiv}$

2. For $n \geq 1$, $f \in \Sigma_n$,

$$f_{A/\equiv} =_{def} \lambda([a_1]_{\equiv}, \ldots, [a_n]_{\equiv}) \in A/_{\equiv}^{n} . \ [f(a_1, \ldots, a_n)]_{\equiv} \in A/_{\equiv}$$

which is <u>well defined</u>, i.e., does <u>not</u> <u>depend</u> on the choice of $a_i \in [a_i]$, precisely because of ($\ddagger$).

<u>The term algebra.</u> The set T_Σ of Σ-terms has a natural Σ-algebra structure $\mathbb{T}_\Sigma = (T_\Sigma, \{f_{\mathbb{T}_\Sigma}\}_{f \in \Sigma})$ defined as follows:

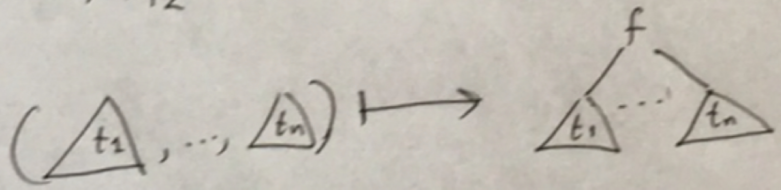
1. For $a \in \Sigma_0$, $a_{\mathbb{T}_\Sigma} = a$

2. For $n \geq 1$, $f \in \Sigma_n$,

$$f_{\mathbb{T}_\Sigma} = \lambda(t_1, \ldots, t_n) \in T_\Sigma^n .\ f(t_1, \ldots, t_n)$$

that is, $f_{\mathbb{T}_\Sigma}$ is a <u>tree building operation</u>:

$f_{\mathbb{T}_\Sigma}$:



<u>The Initial Algebra $\mathbb{T}_{\Sigma/E}$.</u> For any equational theory (Σ, E) let $\equiv_E$ be the <u>smallest congruence</u> on $\mathbb{T}_{\Sigma/E}$ generated by the set of pairs

$$\equiv_E^0 = \left\{ u\{x_1 \mapsto v_1, \ldots, x_n \mapsto v_n\} \equiv v\{x_1 \mapsto v_1, \ldots, x_n \mapsto v_n\} \;\middle|\; \begin{array}{l} (u(x_1, \ldots, x_n) = v(x_1, \ldots, x_n)) \in E \\ v_1, \ldots, v_n \in T_\Sigma \end{array} \right\}$$

that is by the set $\equiv_E^0$ of all <u>ground instances</u> of <u>the equations</u> E. Then $\mathbb{T}_{\Sigma/E} =_{def} \mathbb{T}_\Sigma / \equiv_E$ is called the <u>initial algebra</u> of (Σ, E).

<u>Examples</u> 1. <u>Strings</u> $\{a,b,c\}^*$ on the alphabet $\{a,b,c\}$ are the initial algebra of the theory $(\Sigma_{MON} \cup \{a,b,c\}, \{lde, rid, assoc\})$.

2. <u>Multisets</u> $M(\{a,b,c\})$ are the initial algebra of the theory $(\Sigma_{CMON} \cup \{a,b,c\}, \{id_+, comm_+, assoc_+\})$

3. The <u>integers</u> $\mathbb{Z}$ are the <u>initial algebra of the theory of commutative rings</u>. You can implement them in Maude that way as a functional module.

Better notation [already defined]:

$\Sigma_{MON}[\{a,b,c\}]$

$\Sigma_{CMON}[\{a,b,c\}]$

Rewriting logic statics at last!

~~Definition~~.

A <u>concurrent data structure</u> <u>is</u> an element $[u]_{=_E} \in T_{\Sigma/E}$ of an <u>initial algebra</u> for an equational theory (Σ, E), i.e., of an <u>algebraic data type</u>.

<u>Remarks</u>

1. As already mentioned, Σ can, more generally, be many-sorted, order-sorted, or membership equatl. signat.

Recall the <u>Bergstra-Tucker Meta-Theorem</u> in Lecture 9

2. Since we want the data structures to be <u>computable</u>, we assume that $T_{\Sigma/E}$ is a <u>computable</u> <u>algebra</u>, i.e., all $f_{T_{\Sigma/E}}$ <u>are</u> <u>computable functions</u>, $f \in \Sigma$.