2.1 Rewriting Logic: Statics [Continued]

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

Examples 1. The signature of monoids is \( \Sigma_{\text{MON}} \) with \( \Sigma_{\text{MON},0} = \{ 1 \} \), \( \Sigma_{\text{MON},2} = \{ \cdot, - \} \), and
\[
\Sigma_{\text{MON},n} = \emptyset \text{ otherwise.}
\]
2. Likewise, the signature of commutative monoids \( \Sigma_{\text{CMON}} \) has \( \Sigma_{\text{CMON},0} = \{ 0, 1 \} \), \( \Sigma_{\text{CMON},2} = \{ 0, +, \cdot \} \), \( \Sigma_{\text{CMON},n} = \emptyset \) otherwise.
3. The signature \( \Sigma_{\text{GRP}} \) of groups adds to \( \Sigma_{\text{MON}} \) a unary symbol \( (\cdot)^{-1} \). Likewise, the signature of commutative groups \( \Sigma_{\text{CGRP}} \) adds to \( \Sigma_{\text{CMON}} \) the unary symbol \( - \) [minus].
4. The signature of rings is just $\Sigma_{RNG} = \Sigma_{CMON} \cup \Sigma_{MON}$

**Definition** $[\Sigma$-terms$]$. Given a signature $\Sigma$, the set of its expressions, called $\Sigma$-terms, is defined inductively as the smallest set $T_\Sigma$ such that:

1. $\forall a \in \Sigma_0, \ a \in T_\Sigma$
2. $\forall f \in \Sigma_m, m \geq 1, \forall t_1, \ldots, t_m \in T_\Sigma \Rightarrow f(t_1, \ldots, t_m) \in T_\Sigma$.

**Remark** If $X$, say, $X = \{x_1, \ldots, x_m\}$ or $X = \{x, y, \ldots\}$ in a set of variables, assumed disjoint from $\Sigma_0$, then the set $T_\Sigma(X)$ of $\Sigma$-terms with variables in $X$ is just, by definition, $T_\Sigma(X) = T_{\Sigma[X]}$, where,

$\Sigma[X]_0 = \Sigma_0 \cup X$, and $\Sigma[X]_m = \Sigma_m$ otherwise.

Note that a signature $\Sigma$ is just syntax!

$f \in \Sigma_m$ is an uninterpreted function symbol, not a function! in any sense whatsoever, but a symbol for a function. In fact,
we can just think of a signature $\Sigma$ as a grammar specifying
the $\Sigma$-expressions. For example, $\Sigma_{RNG}$ 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 $\Sigma$ as
actual functions?

Of course, by $\Sigma$-algebras!

**Definition.** [\textit{\Sigma-algebra}]. A $\Sigma$-algebra is a pair

$$A = (A, \{ f_A \}_{f \in \Sigma})$$

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 $a \in A$ it is an element $f_A(a) \in A$.

**Examples.** 1. The multisets $M(a_1, b, c)$ on three elements

are a $\Sigma_{CMON}$ algebra, where $0 = \varnothing$ [empty

multiset], and

$$\begin{align*}
+ & \quad \text{def} \sum_{(u, v) \in M(a_1, b, c)}^2, \\
\text{and} & \end{align*}$$

$U \lor V$ [multiset union]
2. The integers \( \mathbb{Z} \) are a \( \Sigma_{\text{Rng}} \)-algebra

\[
\mathbb{Z} = (\mathbb{Z}, \{ f \}_{f \in \Sigma_{\text{Rng}}}, \mathbb{Z}) \quad \text{where} \quad 0_{\mathbb{Z}} = 0, \quad 1_{\mathbb{Z}} = 1,
\]

\[
+_{\mathbb{Z}} = \lambda (m, n) \in \mathbb{Z}^2. \; x + m \in \mathbb{Z}, \quad \text{with} \quad n + m \text{ integer addition},
\]

\[
\mu_{\mathbb{Z}} = \lambda (m, n) \in \mathbb{Z}^2. \; n \cdot m \in \mathbb{Z}, \quad \text{with} \quad n \cdot m \text{ integer multiplication},
\]

\[
-_{\mathbb{Z}} = \lambda n \in \mathbb{Z}. \; -n \in \mathbb{Z}, \quad \text{with} \quad -n \text{ the additive inverse of } n \text{ in } \mathbb{Z}.
\]

For Combinatory logic we saw that any CL term

\[
t = t(x_1, \ldots, x_n) \quad \text{defines a function}
\]

\[
t : \text{CL}^n \longrightarrow \text{CL}
\]

\[
(u_1, \ldots, u_n) \longmapsto t\{x_1 \mapsto u_1, \ldots, x_n \mapsto u_n\}
\]

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

**Definition** [Function defined by a term \( t \in T_{\Sigma}(X) \) on a \( \Sigma \)-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
convention we write \( t = t(x_1, \ldots, x_n) \) to mean that the variables appearing in \( t \) [there could be none, i.e., \( t \) could be a constant symbol] are among the \( x_1, \ldots, x_n \).

Then, given \( t = t(x_1, \ldots, x_n) \) and a \( \Sigma \)-algebra \( A = (A, \{ f_A \}_{f \in \Sigma}) \), \( t \) defines an \( n \)-ary function \( t_A : A^n \rightarrow A \) defined inductively as follows:

1. If \( t \) is a constant \( a \in \Sigma_0 \), then
   \[ a_A = \lambda (a_1, \ldots, a_n) \in A^n. \quad a_A \in A \]

2. If \( t = f(t_1, \ldots, t_n) \), then
   \[ t_A = \lambda (a_1, \ldots, a_n) \in A^n. \quad f_A(t_1, a_1, \ldots, a_n), \ldots, t_n(a_1, \ldots, a_n) \in A \]

**Definition** [Equation and Satisfaction of an Equation in an Algebra]

1. A \( \Sigma \)-equation is a formula \( t = t' \) with \( t, t' \in T_\Sigma(X) \).
2. A \( \Sigma \)-algebra \( A = (A, \{ f_A \}_{f \in \Sigma}) \) satisfies a \( \Sigma \)-equation \( t = t' \), written \( A \models t = t' \) if \( t_A = t'_A \), 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 \underline{equational theory} is a pair \((\Sigma, E)\), where \(\Sigma\) is a signature and \(E\) is a set of \(\Sigma\)-equations.

4. A \(\Sigma\)-\underline{algebra} \(A = (A, \{f_A\}_{f \in \Sigma})\) is a \((\Sigma, E)\)-\underline{algebra} iff \(\forall (u = v) \in E\) \(A \models u = v\), abbreviated \(A \models E\).

**Example 1.** The theory of monoids \(\Sigma_{\text{MON}}\) \((\Sigma_{\text{MON}}, \{\text{rid}_\text{MON}, \text{ass}_\text{MON}\})\) -

\[
\begin{align*}
\text{id}_{\text{MON}} & \overset{\text{def}}{=} (1 \cdot x_1 = x_1), \\
\text{rid}_{\text{MON}} & \overset{\text{def}}{=} (x_1 \cdot 1 = x_1), \\
\text{ass}_{\text{MON}} & \overset{\text{def}}{=} ((x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3))
\end{align*}
\]

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

\[
\Lambda^* = \varepsilon (u \cdot v) \in \Lambda^*, \quad u, v \in \Lambda^* \quad \text{[string concatenation]}
\]

Furthermore, \((\Lambda^*, \{f_{\Lambda^*}\}_{f \in \Sigma_{\text{MON}}})\) is a \((\Sigma_{\text{MON}}, \{\text{rid}_{\text{MON}}^\Lambda, \text{ass}_{\text{MON}}^\Lambda\})\)-algebra, that is, a \underline{monoid}. 
2. The theory of commutative monoids is \( \Sigma_{CMON}, \{ \text{id}_{CMON}, \text{comm}_{CMON}, \text{assoc}_{CMON} \} \), where

\[ \text{id}_{CMON} \overset{\text{def.}}{=} (x_1 + 0 = x_1), \quad \text{comm}_{CMON} \overset{\text{def.}}{=} (x_1 + x_2 = x_2 + x_1) \]

\[ \text{assoc}_{CMON} \overset{\text{def.}}{=} \left( (x_1 + x_2) + x_3 = x_1 + (x_2 + x_3) \right) \]

The \( \Sigma_{CMON} \)-algebra \( M(B) = \{ (M(B), \{ f \in M(B) \in CMON \}) \} \) of monoids is in fact a \( (\Sigma_{CMON}, \{ \text{id}_{CMON}, \text{comm}_{CMON}, \text{assoc}_{CMON} \}) \)-algebra, i.e., a commutative monoid.

3. The theory of rings is \( \Sigma_{RNG}, \{ \text{id}_{RNG}, \text{comm}_{RNG}, \text{assoc}_{RNG}, \text{inv}_{RNG}, \text{dist}_{RNG} \} \), where

\[ \text{comm}_{RNG} \overset{\text{def.}}{=} (x_1 \cdot x_2 = x_2 \cdot x_1) \]

\[ \text{inv}_{RNG} \overset{\text{def.}}{=} (x_1 + -x_1 = 0) \]

\[ \text{dist}_{RNG} \overset{\text{def.}}{=} (x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)) \]

The integers \( \mathbb{Z} \), the rationals \( \mathbb{Q} \), the reals \( \mathbb{R} \), and the complex numbers \( \mathbb{C} \) are all (with the standard interpretations of 0, 1, +, - and \(-\cdot\)) commutative rings, i.e., they satisfy all the above equations.
Definition [\(\Sigma\)-congruence on a \(\Sigma\)-algebra and quotient]

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

(+) If \(a_1 \equiv a_1', \ldots, a_n \equiv a_n'\), 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 is a \(\Sigma\)-algebra if \(\equiv\) is a \(\Sigma\)-congruence. Namely,

1. For each \(a \in \Sigma_0\), \(a_{A/\equiv} = [\sigma_A]_{\equiv}\)

2. For \(n \geq 1\), \(f \in \Sigma^n\),

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

which is well defined, i.e., does not depend on the choice of \(a_i \in [\sigma_i]\), precisely because of (+).
The term algebra. The set $T_{\Sigma}$ of $\Sigma$-terms has a natural $\Sigma$-algebra structure $T_{\Sigma} = (T_{\Sigma}, \{f_{T_{\Sigma}}\}_{f \in \Sigma})$ defined as follows:

1. For $a \in \Sigma_0$, $a_{T_{\Sigma}} = a$

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

$$f_{T_{\Sigma}} = \lambda (t_1, \ldots, t_n) \in T_{\Sigma}^n \cdot f(t_1, \ldots, t_n)$$

That is, $f_{T_{\Sigma}}$ is a tree build up operation:

$$f_{T_{\Sigma}} : (\triangle t_1, \ldots, \triangle t_n) \mapsto \triangle t_1 \ldots \triangle t_n$$

The Initial Algebra $T_{\Sigma/E}$. For any equational theory $(\Sigma, E)$ let $\equiv_E$ be the smallest congruence on $T_{\Sigma/E}$ generated by the set of pairs

$$\equiv^0_E = \{ (v(x_1, \ldots, x_n), v(x_1', \ldots, x_n')) \mid \forall i \in \{1, \ldots, n\} \cdot (v_i(x_1, \ldots, x_n) = v_i(x_1', \ldots, x_n') \in E) \}$$

that is, by the set $\equiv^0_E$ of all ground instances of the equations $E$. Then $T_{\Sigma/E} \equiv \{ T_{\Sigma} / \equiv_E \} \equiv E$ is called the initial algebra of $(\Sigma, E)$. 
Examples 1. Strings $\{a, b, c\}$ on the alphabet $\{a, b, c\}$ are the initial algebra of the theory $(\Sigma_{\text{MON}} U\{a, b, c\}, \{\text{id}, \text{id}, \text{assoc}\})$.

2. Multisets $M(\{a, b, c\})$ are the initial algebra of the theory $(\Sigma_{\text{CHON}} U\{a, b, c\}, \{\text{id}_+, \text{comm}_+, \text{assoc}_+\})$.

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

Rewriting logic statics at last!

Better notation (already defined):

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

$$\Sigma_{\text{CHON}}[\{a, b, c\}]$$

Definition

A concurrent data structure is an element $[\pi]_e \in T_{\Sigma/E}$ of an initial algebra for an equational theory $(\Sigma, E)$, i.e., of an algebraic data type.

Remarks

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

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

Recall the Bongio-Szabó, Moller-Thomson