Order Sorted Algebra

Daniel Găină

Japan Advanced Institute of Science and Technology

March 8, 2008

Introduction

- There are many examples where all items of one sort are necessarily also items of some other sort.
- Every natural number is an integer, and every integer is a rational. We may write this symbolically

$$\mathit{Natural} \leq \mathit{Integer} \leq \mathit{Rational}$$

- Associating to each sort name a meaning, i.e. semantic denotation, the sub-sort relations appear as set-theoretic inclusion.

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$$

Introduction

- Sort names like Natural and Rational are *syntactic*, formalized with *order sorted signatures*,
- while their interpretations $\mathbb{N}$ and $\mathbb{Q}$ are *semantic*, formalized with *order sorted algebras*.
- This area of mathematics is called **Order Sorted Algebras** (abrev. **OSA**).

Some Motivation

- A related topic is **overloading** which allows a single symbol to be used for different operations.
- we can add $2+2$ (two naturals), or $-2/3+-2$ (a rational and a integer), or $2+3/25$ (a natural and a rational).
- The flexibility comes from having both
  - an overloaded operation symbol $+$, and
  - a sub-sort relation among naturals, integers and rationals
  such that we always get the same result for the same arguments ($+$ is **sub-sort polymorphic**).

Some Motivation

- **polymorphic** express the use of the same operation symbol with different meanings in a programming language.
- One may distinguish several forms of polymorphism based on semantic relationship that holds between the different interpretations of an operation symbol

Some Motivation

- **strong ad hoc polymorphism** - an op. sym. has semantically unrelated uses.
- **multiple representation** - the uses are related semantically, but the representations may be different
- **sub-sort polymorphism** - different instances of an op. sym. are related by the subset inclusion s.t. the result does not depend on the instance used.
- **parametric polymorphism** - supported in CafeOBJ by parameterized objects, such as LIST[X].

Signatures and Terms

An order sorted signature $(S, \leq, F)$ consists of

- a many sorted signature (S, F)
- a partial ordering $\leq$ on S such that the following monotonicity condition is satisfied

$$\sigma \in F_{w_1,s_1} \cap F_{w_2,s_2} \text{ and } w_1 \leq w_2 \text{ imply } s_1 \leq s_2$$

The set T_F of terms is defines recursively by the following:

- $F_{[],s} \subseteq (T_F)_s$
- $s_1 \leq s_2$ implies $(T_F)_{s_1} \subseteq (T_F)_{s_2}$,
- $t_i \in (T_F)_{s_i}$ and $\sigma \in F_{s_1 \ldots s_n,s}$ imply $\sigma(t_1, \ldots, t_n) \in (T_F)_s$

Example in CafeOBJ

```
mod! LIST {
[ NeList < List ]
[ Nat ]
op 0 : -> Nat
op s_ : Nat -> Nat
op nil : -> List .
op cons : Nat List -> NeList .
op car : NeList -> Nat .
op cdr : NeList -> List . }
```

Models and Homomorphisms

Given an order sorted signature $(S, \leq, F)$, an **order sorted $(S, \leq, F)$-algebra** is a many sorted (S, F)-algebra M such that

- $s_1 \leq s_2$ implies $M_{s_1} \subseteq M_{s_2}$
- $\sigma \in F_{w_1,s_1} \cap F_{w_2,s_2}$ and $w_1 \leq w_2$ imply $M_\sigma^{w_1,s_1} = M_\sigma^{w_2,s_2}$ on M^{w_1}.

Given order sorted $(S, \leq, F)$-algebras M, M', an **order sorted $(S, \leq, F)$-homomorphism** $h : M \to M'$ is a many sorted (S, F)-homomorphism $h : M \to M'$ such that

- $s_1 \leq s_2$ implies $h_{s_1} = h_{s_2}$ on M_{s_1}

Regular Signatures and Initiality

An order sorted signature $(S, \leq, F)$ is **regular** iff for each $\sigma \in F_{w_1, s_1}$ and each $w_0 \leq w_1$ there is a unique least element in the set $\{(w, s) \mid \sigma \in F_{w,s}, \text{ and } w_0 \leq w\}$.

$$\begin{tikzcd}
w_1 \arrow[r, "\sigma"] \arrow[d, dash, dotted] & s_1 \arrow[d, dash, dotted] \\
w \arrow[r, "\sigma"] \arrow[d, dash, dotted] & s \\
w_0 &
\end{tikzcd}$$

Proposition

If $(S, \leq, F)$ is regular then for each $t \in T_F$ there is a least sort $s \in S$ such that $t \in (T_F)_s$. This sort is denoted $LS(t)$.

An Example of Non-Regular Signature

mod! TEST {
[$s_1 < s_3$]
[$s_2 < s_4$]
[s_5]
op $a : -> s_1$
op $b : -> s_2$
op $f : s_1\ s_4 -> s_5$.
op $f : s_3\ s_2 -> s_5$. }

Locally Filtered Signatures and Congruence Relations

- s_1 and s_2 are in the same **connected component** of S iff $s_1 \equiv s_2$, where $\equiv$ is the least equivalence relation on S that contains $\leq$.
- A partial ordering $(S, \leq)$ is **filtered** iff for all $s_1, s_2 \in S$ there is some $s \in S$ such that $s_1 \leq s$ and $s_2 \leq s$.
- A partial ordering $(S, \leq)$ is **locally filtered** iff every connected component of it is filtered.
- An order sorted signature $(S, \leq, F)$ is **locally filtered** iff $(S, \leq)$ is locally filtered.

Locally Filtered Signatures and Congruence Relations

- An **order sorted** $(S, \leq, F)$**-congruence** on a $(S, \leq, F)$-algebra M is a many-sorted (S, F)-congruence such that if $s \leq s'$ and $a, a' \in M_s$ then $a \equiv_s a'$ iff $a \equiv_{s'} a'$.
- Constr. of the **quotient** of M by $\equiv$. For each C we define:
  - $M_C = \bigcup_{s \in C} M_s$
  - the equiv. rel. $\equiv_C$ by $a \equiv_C a'$ iff $a \equiv_s a'$ for some $s \in C$.
  - $(M/_{\equiv})_s = q_C(M_s)$ where $q_C : M_C \to (M_C)/_{\equiv_C}$, $q_C(a) = [a]$
  - $(M/_{\equiv})_\sigma = ([a_1], \ldots, [a_n]) = [M_\sigma(a_1, \ldots, a_n)]$

Example

mod! TEST {
[$s_1 < s_3$]
[$s_2 < s_3$]
ops $a\ b : -> s_1$
op $c : -> s_3$
op $f : s_1 -> s_1$.
eq $c = a$.
eq $c = b$.
}
$[a]_{s_1} = [a]_{s_3} = \{a, b, c\}$, $[b]_{s_1} = [b]_{s_3} = \{a, b, c\}$, $[c]_{s_1} = \{a, b, c\}$
$(T_{TEST}/_{\equiv})_{s_3} = \emptyset$
$f([a]) = [f(a)] = \{f(a), f(b)\}$

Coherent signatures and Equations

- A signature is **coherent** iff it is both locally filtered and regular.
- An order sorted $(S, \leq, F)$-**equation** is a triple $\langle X, t_1, t_2 \rangle$ where X is an S-indexed set and $t_1, t_2 \in T_{F \cup X}$ such that $LS(t_1)$ and $LS(t_2)$ are in the same connected component of $(S, \leq)$. We will write $(\forall X) t_1 = t_2$.
- A **conditional** $(S, \leq, F)$**-equation** is a quadruple $\langle X, t_1, t_2, C \rangle$, where $\langle X, t_1, t_2 \rangle$ is a $(S, \leq, F)$ equation and C is a (finite) set of pairs $\langle u, v \rangle$ such that $\langle X, u, v \rangle$ is a $(S, \leq, F)$-equation. We will write $(\forall X) t_1 = t_2 if C$.

System of (Proof) Rules and Entailment Systems

A **system of (proof) rules** $(\mathbf{Sig}, \mathbf{Sen}, Rl)$ consists of

- a category of "signatures" **Sig**,
- a "sentence functor" $\mathbf{Sen} : \mathbf{Sig} \to \mathbb{S}et$
- a family of relations $Rl = (Rl_\Sigma)_{\Sigma \in |\mathbf{Sig}|}$ between sets of sentences $\vdash_\Sigma \subseteq \mathcal{P}(\mathbf{Sen}(\Sigma)) \times \mathcal{P}(\mathbf{Sen}(\Sigma))$ for all $\Sigma \in |\mathbf{Sig}|$.

An entailment system $(\mathbf{Sig}, \mathbf{Sen}, \vdash)$ is just a systems of rules s. t. for each $\Sigma \in |\mathbf{Sig}|$, $\vdash_\Sigma$ has the following prop.:

- *anti-monotonicity:* $E_1 \vdash_\Sigma E_2$ if $E_2 \subseteq E_1$,
- *transitivity:* $E_1 \vdash_\Sigma E_3$ if $E_1 \vdash_\Sigma E_2$ and $E_2 \vdash_\Sigma E_3$, and
- *unions:* $E_1 \vdash_\Sigma E_2 \cup E_3$ if $E_1 \vdash_\Sigma E_2$ and $E_1 \vdash_\Sigma E_3$

We call $\vdash_\Sigma$ the entailment relation associated to the signature Σ.

Proof rules for **AOSA**

- $(R)\emptyset \vdash t = t$ for each term t
- $(S) t = t' \vdash t' = t$ for any terms t, t'
- $(T)\{t = t', t' = t''\} \vdash t = t''$ for any terms t, t', t''
- $(F)\{t_i = t'_i | 1 \leq i \leq n\} \vdash \sigma(t_1, ..., t_n) = \sigma(t'_1, ..., t'_n)$ for any $\sigma \in F$

Proposition

For each set E of quantifier free $(S, \leq, F)$-equations we have that $(T_F)/_{\equiv_E} \models t = t'$ iff $E \vdash t = t'$ and **AOSA** *with the above system of proof rules is sound and complete.*

Entailment Systems with Implications

An entailment system $(\mathbf{Sig}, \mathbf{Sen}, \vdash)$ has (finitary) implications if for each set of Σ-sentences E and any Σ-sentence e if C,

$$E \vdash e \text{ if } C \text{ iff } E \cup C \vdash e$$

Proposition

The entailment system with implications freely generated by the systems of rules for **AOSA** *is sound and complete for the quantifier free part of* **OSA**.

Entailment Systems with Universal Quantification

An entailment system $(\mathbf{Sig}, \mathbf{Sen}, \vdash)$ has universal $\mathcal{D}$-quantification, for a sub-category $\mathcal{D} \subseteq \mathbf{Sig}$ of signature morphisms if the entailment system satisfies the following property (also called the meta-rule of 'Generalization').

$$\Gamma \vdash_{\Sigma} (\forall \chi) e' \text{ iff } \chi(\Gamma) \vdash_{\Sigma'} e'$$

for each set of sentences $\Gamma \subseteq \mathbf{Sen}(\Sigma)$ and any sentence $(\forall \chi) e' \in \mathbf{Sen}(\Sigma)$, where $\chi : \Sigma \to \Sigma' \in \mathcal{D}$.

Proof Rules for **OSA**

Theorem

Entailment system for **OSA** *is obtained as the free entailment system*

- *with universal quantification and*
- *with implication at the quantifier-free level*

generated by

- $(R) \emptyset \vdash t = t$ *for each term* t
- $(S) t = t' \vdash t' = t$ *for any terms* t, t'
- $(T) \{t = t', t' = t''\} \vdash t = t''$ *for any terms* t, t', t''
- $(F) \{t_i = t_i' | 1 \leq i \leq n\} \vdash \sigma(t_1, ..., t_n) = \sigma(t_1', ..., t_n')$ *for any* $\sigma \in F$
- $(Subst)(\forall Y)\rho \vdash (\forall X)\theta(\rho)$ *for any* $(S, \leq, F)$*-sentence* $(\forall Y)\rho$ *and for any substitution* $\theta : Y \to T_F(X)$.