Dialgebraic Specification and Modeling

Peter Padawitz
University of Dortmund

ls5-www.cs.uni-dortmund.de/∼peter/Swinging.html
ls5-www.cs.uni-dortmund.de/∼peter/Expander2.html

September 20, 2005

Goals and characteristics of this approach

➢ *uniform syntax for algebraic and coalgebraic specifications*

signatures

(products of) sorts

functions $f : s_1 \times \cdots \times s_n \rightarrow s \qquad g : s_1 \times \cdots \times s_m \rightarrow s_1 \times \cdots \times s_n$

relations $r : s_1 \times \cdots \times s_n$

terms (conditional) equations Horn clauses first-order formulas

cosignatures ?

functors

cofunctions $f : s \rightarrow s_1 + \cdots + s_n \qquad g : s \rightarrow 1 + s_1 \times \cdots \times s_n$

corelations

coterms ? coequations ? co-Horn clauses ! modal formulas ?

What distinguishes algebras from coalgebras?

➢ *modular specifications*

chains of specifications are interpreted as a sequence of initial and final models

initial	**final**
data defined by constructors	states defined by destructors
functions defined by recursion	functions defined by corecursion
relations defined by Horn clauses	relations defined by co-Horn clauses
relations defined by co-Horn clauses	relations defined by Horn clauses
abstraction defined by a least congruence on an initial model (*variety*)	abstraction defined by a greatest congruence on an initial model (*covariety*)
restriction defined by a least invariant on an final model	restriction defined by a greatest invariant on a final model
supertyping by adding "constructors"	subtyping by adding "destructors"

➢ *Dualities admit the proof of model properties without referring to particular representations.*

➢ *proof rules that exploit initial/final semantics*

induction **coinduction**

narrowing (rewriting upon axioms + instantiation)

simplification (built-in rewriting)

Types

Let S be a set of **sorts** and $S_0 \subseteq S$. The set $\mathbb{T}(S_0, S)$ of **types over** (S_0, S) is the least set of expressions generated by the following rules:

sorts

$$\frac{}{s} \quad s \in S \qquad\qquad \frac{}{1}$$

products and sums

$$\frac{\{s_i\}_{i\in I}}{\prod_{i\in I} s_i} \qquad \frac{\{s_i\}_{i\in I}}{\coprod_{i\in I} s_i} \qquad I \neq \emptyset$$

functions

$$\frac{s_0 \quad s}{s_0 \longrightarrow s} \quad s_0 \in \mathbb{T}(S_0, S_0)$$

collections

$$\frac{s}{list(s)} \qquad \frac{s}{bag(s)} \qquad \frac{s}{set(s)}$$

The set $\mathbb{F}(S_0, S)$ of **function types** over S_0 and S consists of all expressions $s \longrightarrow s'$ such that $s, s' \in \mathbb{T}(S_0, S)$.

Signatures

A **signature** $\Sigma = (S, F, R, B)$ consists of
a finite set S of sorts,
a finite $\mathbb{F}(S_0, S)$-sorted set F of **functions**,
a finite $\mathbb{T}(S_0, S)$-sorted set R of **relations**
and an S_0-sorted set B
where $S_0 \subseteq S$ is called the set of **primitive sorts of** Σ.

Given $f : s \to s' \in F$, $dom_f =_{def} s$ and $ran_f =_{def} s'$.

$f : s \to s'$ is an s'**-constructor** if $s' \in S$.
$f : s \to s'$ is an s**-destructor** if $s \in S$.

For all $s \in S$,
R implicitly includes the s**-equality** $\equiv_s$: $s \times s$ and the s**-universe** $all_s : s$.

Terms are (representations of) functions

The $\mathbb{F}(S_0, S)$-sorted set T_Σ of **Σ-terms** is the least set of expressions t generated by the following rules:

functions of Σ and identities

$$\frac{}{f : s \to s'} \quad f : s \to s' \in F \qquad\qquad \frac{}{id_s : s \to s} \quad s \in \mathbb{T}(S_0, S)$$

Σ-projections and -injections

$$\frac{}{\pi_i : \prod_{i \in I} s_i \to s_i} \quad \frac{}{\iota_i : s_i \to \coprod_{i \in I} s_i} \quad \{s_i\}_{i \in I} \subseteq \mathbb{T}(S_0, S) \quad I \neq \emptyset$$

Σ-applications and -abstractions

$$\frac{}{apply_a : (s_x \to s) \to s} \quad a \in B_{s_x} \qquad \frac{t = \{t_a : s \to s' \mid a \in B_{s_x}\}}{\lambda x.t : s \to (s_x \to s')} \qquad s_x \in \mathbb{T}(S_0, S_0)$$

composition with functions of Σ

$$\frac{t : s \to s'}{f \circ t : s \to s''} \quad f : s' \to s'' \in F \cup \Sigma\iota \cup \Sigma\alpha \quad t \neq id_s$$

$$\frac{t : s \to s'}{t \circ f : s'' \to s'} \quad f : s'' \to s \in F \cup \Sigma\pi \cup \Sigma\beta \quad t \neq id_s$$

where $\Sigma\pi$, $\Sigma\beta$, $\Sigma\iota$ and $\Sigma\alpha$ are the sets of Σ-projections, -applications, -injections and -abstractions, respectively

tupling and selection

$$\frac{\{t_i : s \to s_i\}_{i\in I}}{tup(t_i)_{i\in I} : s \to \prod_{i\in I} s_i} \qquad \frac{\{t_i : s_i \to s\}_{i\in I}}{sel(t_i)_{i\in I} : \coprod_{i\in I} s_i \to s} \quad I \neq \emptyset$$

product and sum

$$\frac{\{t_i : s_i \to s_i'\}_{i\in I}}{\prod_{i\in I} t_i : \prod_{i\in I} s_i \to \prod_{i\in I} s_i'} \qquad \frac{\{t_i : s_i \to s_i'\}_{i\in I}}{\coprod_{i\in I} t_i : \coprod_{i\in I} s_i \to s_i'} \quad I \neq \emptyset$$

function lifting

$$\frac{t : s \to s'}{(s_0 \to t) : (s_0 \to s) \to (s_0 \to s')} \quad s_0 \in \mathbb{T}(S_0, S_0)$$

collection building

$$\frac{\{t_i : s \to s'\}_{i=1}^{n}}{list_n(t_1, \ldots, t_n) : s \to list(s')} \quad \frac{\{t_i : s \to s'\}_{i=1}^{n}}{bag_n(t_1, \ldots, t_n) : s \to bag(s')} \quad n > 0$$

$$\frac{\{t_i : s \to s'\}_{i=1}^{n}}{set_n(t_1, \ldots, t_n) : s \to set(s')} \quad n > 0$$

collection lifting

$$\frac{t : s \to s'}{list(t) : list(s) \to list(s')} \quad \frac{t : s \to s'}{bag(t) : bag(s) \to bag(s')}$$

$$\frac{t : s \to s'}{set(t) : set(s) \to set(s')}$$

$$\prod_{i \in I} t_i \ = \ tup(t_i \circ \pi_i)_{i \in I} \qquad \coprod_{i \in I} t_i \ = \ tsel(\iota_i \circ t_i)_{i \in I}$$

$t : dom \to s$ is a **Σ-generator** if $dom \in \mathbb{T}(S_0, S_0)$ and either $s \in \mathbb{T}(S_0, S_0)$ and $t = id_s$ or $s \in S \setminus S_0$ and all function symbols of t are constructors, injections or abstractions.

$t : s \to ran$ is a **Σ-observer** if $ran \in \mathbb{T}(S_0, S_0)$ and either $s \in \mathbb{T}(S_0, S_0)$ and $t = id_s$ or $s \in S \setminus S_0$ and function symbols of t are destructors, projections or applications.

Formulas are (representations of) relations

The $\mathbb{T}(S_0, S)$-sorted set F_Σ of **Σ-formulas** is the least set of expressions φ generated by the following rules:

relations of Σ, tautology and contradiction

$$\frac{}{r : s} \quad r : s \in R \qquad \frac{}{True : s} \quad \frac{}{False : s} \quad s \in \mathbb{T}(S_0, S)$$

Σ-atoms and negation

$$\frac{t : s \to s'}{r \circ t : s} \quad r : s' \in R,\ t \neq id_s \qquad \frac{\varphi : s}{\neg\varphi : s}$$

conjunction and disjunction

$$\frac{\{\varphi_j : \prod_{i \in I_j} s_i\}_{j \in J}}{\bigwedge_{j \in J} \varphi_j : \prod_{i \in \cup\{I_j | j \in J\}} s_i} \quad \frac{\{\varphi_j : \prod_{i \in I_j} s_i\}_{j \in J}}{\bigvee_{j \in J} \varphi_j : \prod_{i \in \cup\{I_j | j \in J\}} s_i} \quad J \neq \emptyset,\ \forall\ j \in J : I_j \neq \emptyset$$

quantification

$$\frac{\varphi : \prod_{i\in I} s_i}{\forall k\varphi : \prod_{i\in I\setminus\{k\}} s_i} \qquad \frac{\varphi : \prod_{i\in I} s_i}{\exists k\varphi : \prod_{i\in I\setminus\{k\}} s_i} \quad k \in I,\ I \neq \emptyset$$

$$False \;=\; \neg True \qquad \bigvee_{j\in J}\varphi_j \;=\; \neg(\bigwedge_{j\in J}\neg\varphi_j) \qquad \varphi \Rightarrow \psi \;=\; \neg\varphi \vee \psi$$

$$\varphi \Leftrightarrow \psi \;=\; (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi) \qquad \exists k\varphi \;=\; \neg\forall k\neg\varphi$$

Let $p : s$ be a Σ-atom and $\varphi : s$ be a Σ-formula.

$p \Leftarrow \varphi$ is a **Horn clause over Σ**.
$p \Rightarrow \varphi$ is called a **co-Horn clause over Σ**.

If $p = r \circ t$ for some logical $r \in R$,
then $p \Leftarrow \varphi$ resp. $p \Rightarrow \varphi$ is a Horn resp. co-Horn clause **for r**.

If $p = f \circ t \equiv u$ for some $f \in F$,
then $p \Leftarrow \varphi$ is a Horn clause **for f**.

A Σ-formula φ is **normalized** if φ consists of literals, quantifiers and conjunction or disjunction symbols.

Given $R_1 \subseteq R$, a normalized Σ-formula φ is **R_1-positive** if all negative literals of φ are $(R \setminus R_1)$-literals.

A Horn clause $p \Leftarrow \varphi$ or co-Horn clause $p \Rightarrow \varphi$ is **R_1-positive** if φ is R_1-positive.

Given $S_1 \subseteq S$, a Σ-formula φ is **S_1-restricted** if
for all subformulas $\forall k\psi$ of φ such that $s_k \in S_1$, $\neg all_{s_k} \circ \pi_k$ is a summand of ψ, and
for all subformulas $\exists k\psi$ of φ such that $s_k \in S_1$, $all_{s_k} \circ \pi_k$ is a factor of ψ.

A Horn clause $p \Leftarrow \varphi$ or co-Horn clause $p \Rightarrow \varphi$ is **S_1-restricted** if φ is S_1-restricted.

Signature morphism

Let $\Sigma = (S, F, R, B)$ and $\Sigma' = (S', F', R', B')$ be signatures with primitive sort sets S_0 and S_0', respectively.

A **signature morphism** $\sigma : \Sigma \longrightarrow \Sigma'$ consists of

a function from $\mathbb{T}(S_0, S)$ to $\mathbb{T}(S_0', S')$,
an $\mathbb{F}(S_0, S)$-sorted function $\{\sigma_s : F_s \longrightarrow F_{\Sigma,\sigma(s)}\}_{s \in \mathbb{F}(S_0,S)}$ and
a $\mathbb{T}(S_0, S)$-sorted function $\{\sigma_s : R_s \longrightarrow T_{\Sigma,\sigma(s)}\}_{s \in \mathbb{T}(S_0,S)}$.

Swinging type

Given a signature Σ and a set AX of Σ-formulas, called **axioms**, the pair $SP = (\Sigma, AX)$ is a **specification**.

A specification $SP' = (\Sigma', AX')$ is a **swinging type (ST)** with **base type** $SP = (\Sigma, AX)$ and **primitive subtype** $SP_0 = (\Sigma_0, AX_0)$
if SP_0 and SP are swinging types

and $SP' = SP = SP_0 = (\emptyset, \emptyset)$ or one of the following conditions holds true.

Let $\Sigma_0 = (S_0, F_0, R_0, B_0)$, $\Sigma = (S, F, R, B)$, $\Sigma' = (S', F', R', B')$ and $S_1 = S \setminus S_0$.

(1) **Data.** $SP = SP_0$ and $AX' = AX$.
$\Sigma' \setminus \Sigma$ consists of a set S_{new} of sorts and a set of constructors $c : s \to s'$ such that $s' \in S_{new}$ and $s \in \mathbb{T}(S, S')^{<2}$. $AX' = AX$.

(2) **States.** $SP = SP_0$ and $AX' = AX$.
$\Sigma' \setminus \Sigma$ consists of of a set S_{new} of sorts and a set of destructors $d : s \to s'$ such that $s \in S_{new}$ and $s' \in \mathbb{T}(S, S')^{<2}$.

(3) **Recursion.** SP satisfies (1).
$\Sigma' \setminus \Sigma$ is a set of functions $f : s \to s'$ such that $s \in S_1$.
For all $s \in S_1$, let $F(s) = \{f \in F' \setminus F \mid dom_f = s\}$.
$AX' \setminus AX$ consists of an equation

$$f \circ c \equiv t_{f,c} \odot (dom_c \lhd T)$$

for each $f \in \Sigma' \setminus \Sigma$, each dom_f-constructor c and some Σ-term

$$t_{f,c} : dom_c[(\prod_{f \in F(s)} ran_f)/s \mid s \in S_1] \to ran_f$$

where $T_s = \begin{cases} id_s & \text{if } s \in S_0 \\ tup(F(s)) & \text{if } s \in S_1 \end{cases}$

(4) **Corecursion.** SP satisfies (2).
$\Sigma' \setminus \Sigma$ is a set of functions $f : s \to s'$ such that $s' \in S_1$.
For all $s \in S_1$, let $F(s) = \{f \in F' \setminus F \mid ran_f = s\}$.
$AX' \setminus AX$ consists of an equation

$$d \circ f \equiv (ran_d \lhd T) \odot t_{f,d}$$

for each $f \in \Sigma' \setminus \Sigma$, each ran_f-destructor d and some Σ-term

$$t_{f,d} : dom_f \to ran_d[(\coprod_{f \in F(s)} dom_f)/s \mid s \in S_1]$$

where $T_s = \begin{cases} id_s & \text{if } s \in S_0 \\ sel(F(s)) & \text{if } s \in S_1 \end{cases}$

(5) **Least relations.** $\Sigma' \setminus \Sigma$ is a set R_1 of logical relations.
$AX' \setminus AX$ consists of R_1-positive Horn clauses for R_1.

(6) **Greatest relations.** $\Sigma' \setminus \Sigma$ is a set R_1 of logical relations.
$AX' \setminus AX$ consists of R_1-positive co-Horn clauses for R_1.

(7) **Visible abstraction.** SP is visible.
$R \subseteq \Sigma_0 \cup equals$ where $equals = \{\equiv_s \mid s \in S \setminus S_0\}$.
$\Sigma' \setminus \Sigma$ is a set R_1 of logical relations.
$AX' \setminus AX$ consists of $(R_1 \cup equals)$-positive Horn clauses for $R_1 \cup equals$ and includes CONH.

(8) **Hidden abstraction.** SP is visible.
$R \subseteq \Sigma_0 \cup equals$ where $equals = \{\equiv_s \mid s \in S \setminus S_0\}$.
$\Sigma' \setminus \Sigma$ is a set R_1 of logical relations.
$AX' \setminus AX$ consists of $(R_1 \cup equals)$-positive co-Horn clauses for $R_1 \cup equals$ and includes CONC.

(9) **Hidden restriction.** SP is hidden.

$R \subseteq \Sigma_0 \cup univs$ where $univs = \{all_s \mid s \in S \setminus S_0\}$.

$\Sigma' \setminus \Sigma$ is a set R_1 of logical relations.

$AX' \setminus AX$ consists of $(R_1 \cup univs)$-positive and S_1-restricted co-Horn clauses for $R_1 \cup univs$ and includes INVC.

(10) **Visible restriction.** SP is hidden.

$R \subseteq \Sigma_0 \cup univs$ where $univs = \{all_s \mid s \in S \setminus S_0\}$.

$\Sigma' \setminus \Sigma$ is a set R_1 of of logical relations.

$AX' \setminus AX$ consists of $(R_1 \cup univs)$-positive and S_1-restricted Horn clauses for $R_1 \cup univs$ and includes INVH.

(11) **Supertyping.** SP is visible.

$\Sigma' \setminus \Sigma$ consists of constructors $c : dom \rightarrow ran$ and logical relations $r : s$ such that $ran \in S \setminus S_0$ and $dom, s \in \mathbb{T}(S_0, S)$.

R and $AX' \setminus AX$ satisfy the conditions of (7) or (8).

(12) **Subtyping.** SP is hidden.

$\Sigma' \setminus \Sigma$ consists of destructors $d : dom \rightarrow ran$ and logical relations $r : s$ such that $dom \in S' \setminus S_0$ and $ran, s \in \mathbb{T}(S_0, S)$.

R and $AX' \setminus AX$ satisfy the conditions of (9) or (10).

In cases (1), (3), (7) and (10), SP' is **visible**.
In cases (2), (4), (8) and (9), SP' is **hidden**.
In cases (5) and (6), SP' is **visible** resp. **hidden** if SP is visible resp. hidden.
In cases (11) and (12), SP' is **visible** resp. **hidden** if $AX' \setminus AX$ consists of Horn resp. co-Horn clauses.

In cases (3) to (12), SP_0 is also the primitive subtype of SP.

Structures and the interpretation of terms and formulas

Let $\Sigma = (S, F, R, C)$ be a signature with primitive set of sorts S_0.

A **Σ-structure** A consists of an S-sorted set, for all $f : s \to s' \in F$, a function $f^A : A_s \to A_{s'}$, and for all $r : s \in R$, a relation $r^A \subseteq A_s$, such that for all $s \in S_0$, $A_s = B_s$.

Mod(Σ) denotes the category of Σ-structures and Σ-homomorphisms.
$\mathbf{Mod}_{EU}(\Sigma)$ denotes the full subcategory of $Mod(\Sigma)$ whose objects are Σ-structures with equality and universe.

Given $S_1 \subseteq S$ and an S_1-sorted set B, **Mod(B,Σ)** denotes the subcategory of **Σ-structures A over B**, i.e. for all $s \in S_0$, $A_s = B_s$. The morphisms of this category are restricted to the Σ-homomorphisms h with $h_s = id_s^B$ for all $s \in S_0$.

The interpretation of a Σ-term $t : s \rightarrow s'$ in A is a function $t^A : A_s \rightarrow A_{s'}$.

The interpretation of a Σ-formula $\varphi : s$ in A is a subset of A_s that is inductively defined as follows:

- For all $t : s \rightarrow s' \in T_\Sigma \setminus \{id_s\}$ and $r : s' \in R$, $(r \circ t)^A = (t^A)^{-1}(r^A)$.
- For all $s \in \mathbb{T}(S_0, S)$, $True_s^A = A_s$ and $False_s^A = \emptyset$.
- For all $\varphi : s \in F_\Sigma$, $(\neg\varphi)^A = A_s \setminus \varphi^A$.
- For all $\{\varphi_j : \prod_{i \in I_j} s_i\}_{j \in J} \subseteq F_\Sigma$, $(\bigwedge_{j \in J} \varphi_j)^A = \bigcap_{j \in J} \pi_{I_j}^{-1}(\varphi_j^A)$.[1]
- For all $\varphi : \prod_{i \in I} s_i \in F_\Sigma$ and $k \in I$, $(\forall k \varphi)^A = \bigcap_{b \in s_k^A}(\varphi^A \div_k b)$.

[1] π_{I_j} maps from $\prod_{\cup\{i \in I_j | j \in J\}} s_i^A$ to $\prod_{i \in I_j} s_i^A$.

$a \in A_s$ **satisfies** $\varphi : s$ if $a \in \varphi^A$. A **satisfies** $\varphi : s$ if $\varphi^A = A_s$.

Let $SP = (\Sigma, AX)$ be a specification. A is an **SP-model** if A satisfies AX. **Mod(SP)** denotes the category of SP-models and Σ-homomorphisms.

Let $\Sigma = (S, F, R, C)$, $\Sigma = (S', F', R', C')$ be signatures, S_0 be the set of primitive sorts of Σ and A be a Σ'-structure.

Given a signature morphism $\sigma : \Sigma \to \Sigma'$, the **$\sigma$-reduct of A**, $A|_\sigma$, is the Σ-structure defined by $(A|_\sigma)_s = A_{\sigma(s)}$ for all $s \in \mathbb{T}(S_0, S)$ and $f^{A|_\sigma} = \sigma(f)^A$ for all $F \cup R$.

Congruences and invariants

Let $SP = (\Sigma, AX)$ be a specification, $\Sigma = (S, F, R)$, A be a Σ-structure, $\sim$ be an S-sorted binary relation on A and inv be an S-sorted subset of A.

$\sim$ is **Σ-congruent** if for all $f : s \to s' \in F$ and $a, b \in A_s$,

$$a \sim_s b \quad \text{implies} \quad f^A(a) \sim_{s'} f^A(b).$$

$\sim$ extends to a Σ-structure:

- For all $f : s \to s' \in F$, $a \sim_s b$ implies $f^\sim(a, b) = (f^A(a), f^A(b))$,
- for all $r : s \in R$, $r^\sim = (r^A \times r^A) \cap \sim_s$.

$\sim$ is **R-compatible** if for all $r : s \in R$ and $a, b \in A_s$, $a \in r^A$ and $a \sim b$ imply $b \in r^A$.

Given a Σ-congruent and R-compatible equivalence relation $\sim$ on A, the **$\sim$-quotient** of A, $A/\!\sim$, is the Σ-structure that is defined as follows:

- For all $s \in S$, $(A/\!\sim)_s = \{[a] \mid a \in A_s\}$,
- for all $f : s \to s' \in F$ and $a \in A_s$, $f^{A/\sim}([a]) = f^A(a)$,
- for all $r \in R$, $r^{A/\sim} = \{[a] \mid a \in r^A\}$,

inv is a **Σ-invariant** if for all $f : s \rightarrow s' \in F$ and $a \in A_s$,

$$a \in inv_s \quad \text{implies} \quad f^A(a) \in inv_{s'}.$$

inv extends to a Σ-structure:

- For all $f : s \rightarrow s' \in F$ and $a \in inv_s$, $f^{inv}(a) = f^A(a)$,
- for all $r : s \in R$, $r^{inv} = r^A \cap inv_s$.

The initial model

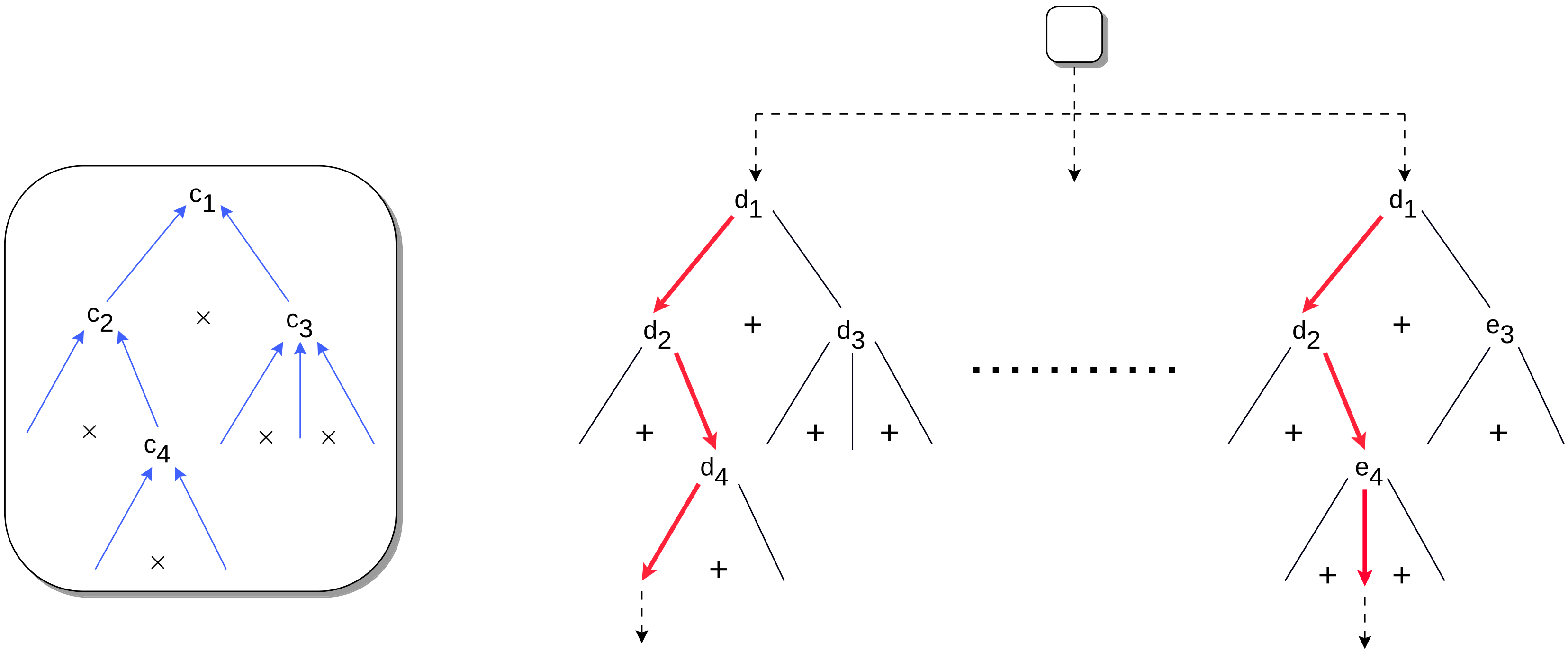
Let $SP' = (\Sigma', AX')$ be a swinging type with base type $SP = (\Sigma, AX)$ such that SP satisfies (1).
Given an SP-model A, a $poly(\Sigma')$-structure Ini with equality and universe is defined as follows:
For all $s \in S'$, let $Gen(s)$ be the set of all Σ'-generators $t : dom \to s$.

- $Ini|_\Sigma = A$.
- For all $s \in S_{new}$, $Ini_s = \coprod_{t \in Gen(s)} dom_t^A$.

- For all $s \in S_{new}$, s-constructors c and $a \in Ini_{dom_c}$,

$$c^{Ini}(a) = \begin{cases} (b, c \odot t) & \text{if } dom_c = s' \in S' \\ & \text{and } a = (b,t) \in Ini_{s'} = Ini_{dom_c}, \\ ((a_i)_{i\in I}, c \odot \prod_{i\in I} t_i) & \text{if } dom_c = \prod_{i\in I} s_i \\ & \text{and } a = (a_i, t_i)_{i\in I} \in \prod_{i\in I} Ini_{s_i} = Ini_{dom_c}, \\ (a, c \odot \iota_k \odot t) & \text{if } dom_c = \coprod_{i\in I} s_i \\ & \text{and } a = ((a,t),k) \in \coprod_{i\in I} Ini_{s_i} = Ini_{dom_c}, \\ (\lambda x.a_x, c \odot \lambda x.t_x) & \text{if } dom_c = (s_0 \to s') \\ & \text{and } a = \lambda x.(a_x, t_x) \in [A_{s_0} \to Ini_{s'}] = Ini_{dom_c}, \\ ([a_1, \dots, a_n], & \\ \quad c \odot list_n(t_1, \dots, t_n)) & \text{if } dom_c = list(s') \\ & \text{and } a = [(a_1,t_1), \dots, (a_n,t_n)] \in Ini^+_{s'} = Ini_{dom_c}. \end{cases}$$

Let $\sim$ be the least interpretation of $\equiv$ in $Ini|_{poly}$ that satisfies CONH. Then $Ini/{\sim}$ is initial in $Mod_{EU}(A, SP')$.



An element of the initial model for constructors $c_i : s_{i,1} \times \ldots \times s_{i,n_i} \rightarrow s_i$ (left) versus an element of the final model for destructors $d_i : s_i \rightarrow s_{i,1} + \cdots + s_{i,n_i}$ (right).

The final model

Let $SP' = (\Sigma', AX')$ be a swinging type with base type $SP = (\Sigma, AX)$ such that SP satisfies (2).

Given an SP-model A, a $poly(\Sigma')$-structure Fin with equality and universe is defined as follows:

For all $s \in S'$, let $Obs(s)$ be the set of all Σ'-observers $t : s \to ran$.

- $Fin|_\Sigma = A$.
- For all $s \in S_{new}$,

$$Fin_s = \{a \in \prod_{t \in Obs(s)} ran_t^A \mid \left\{ \begin{array}{l} \forall\ destructors\ d : s \to \coprod_{i \in I} s_i\ \exists\ k \in I \\ \forall\ (t_i : s_i \to s'_i)_{i \in I} \in \prod_{i \in I} D(s_i) \\ \exists\ b \in A_{s'_k} : a_{(\coprod_{i \in I} t_i) \odot d} = (b, k), \\ \forall\ destructors\ d : s \to list(s')\ \exists\ n \in \mathbb{N} \\ \forall\ t : s' \to s'' \in D(s') \\ \exists\ a_1, \ldots, a_n \in A_{s''} : a_{list(t) \odot d} = [a_1, \ldots, a_n] \end{array} \right\} \}.$$

- For all $s \in S_{new}$, s-destructors d and $a \in Fin_s$,

$$d^{Fin}(a) = \begin{cases} (a_{t \odot d})_{t \in Obs(s')} \in Fin_{s'} = Fin_{ran_d} & \text{if } ran_d = s' \in S', \\ ((a_{t \odot \pi_i \odot d})_{t \in Obs(s_i)})_{i \in I} \in \prod_{i \in I} Fin_{s_i} = Fin_{ran_d} & \text{if } ran_d = \prod_{i \in I} s_i, \\ (a_{(\coprod_{i \in I} t_i) \odot d})_{(t_i)_{i \in I} \in \prod_{i \in I} Obs(s_i)} \in \coprod_{i \in I} Fin_{s_i} = Fin_{ran_d} & \text{if } ran_d = \coprod_{i \in I} s_i \\ \lambda x.(a_{t \odot apply_x \odot d})_{t \in Obs(s')} \in [A_{s_0} \to Fin_{s'}] = Fin_{ran_d} & \text{if } ran_d = (s_0 \to s'), \\ (a_{list(t) \odot d})_{t \in Obs(s')} \in Fin_{s'}^{+} = Fin_{ran_d} & \text{if } ran_d = list(s'). \end{cases}$$

Let $\sim$ be the greatest interpretation of $\equiv$ in $Fin|_{poly}$ that satisfies CONC. Then $Fin/\sim$ is final in $Mod_{EU}(A, SP')$.

Axiomatizing relations

Let $\Sigma = (S, F, R, C)$ be a signature, AX be a finite set of either only Horn or only co-Horn clauses over Σ, A be a Σ-structure with equality and $r : s_x \in R$.

(1) Let $AX_r = \{(r(t_i) \Leftarrow \varphi_i) : s_i\}_{i=1}^n$ be the set of Horn clauses for r among the clauses of AX. The Σ-formula

$$\varphi_r(AX) \quad =_{def} \quad r(x) \Leftarrow \bigvee_{i=1}^{n} \exists i(x \equiv t_i(i) \wedge \varphi_i) : s_x$$

is called the **AX-definition of r**.

(2) Let $AX_r = \{(r(t_i) \Rightarrow \varphi_i) : s_i\}_{i=1}^n$ be the set of co-Horn clauses for r among the clauses of AX. The Σ-formula

$$\varphi_r(AX) \quad =_{def} \quad r(x) \Rightarrow \bigwedge_{i=1}^{n} \forall i(\neg x \equiv t_i(i) \vee \varphi_i) : s_x$$

is called the **AX-definition of r**.

A satisfies AX_r iff A satisfies $\varphi_r(AX)$.

μ- and ν-extensions

Let $\Sigma = (S, F, R, C)$, $\Sigma' = (S, F, R', C)$ and $SP = (\Sigma, AX)$ and $SP' = (\Sigma', AX \uplus AX_1)$ be specifications such that $R \subseteq R'$ and AX_1 consists of

(1) R_1-positive Horn clauses for $R_1 =_{def} (R' \setminus R) \cup \{\equiv_s \mid s \in S_1\}$ or

(2) R_1-positive co-Horn clauses for $R_1 =_{def} (R' \setminus R) \cup \{all_s \mid s \in S_1\}$

where S_1 is the set of non-primitive sorts of Σ. R_1 is called the set of **relations defined by SP'**.

In case (1), SP' is a **μ-extension of SP**.
In case (2), SP' is a **ν-extension of SP**.

The signature morphism $\sigma : \Sigma' \rightarrow \Sigma'$ that is the identity on Σ and maps $r \in R_1$ to the AX_1-definition of r is called the **relation transformer of SP'**.

Relation transformer are monotone functions on $Mod(A,\Sigma')$

For all $B, C \in Mod(A,\Sigma')$,

$$B \leq C \iff \forall\, r \in R_1 : r^B \subseteq r^C.$$

For all $r : s \in R_1$ and $\mathcal{B} \subseteq Mod(A,\Sigma')$,
$r^{\perp} = \emptyset$, $r^{\top} = A_s$, $r^{\sqcup\mathcal{B}} = \bigcup_{B\in\mathcal{B}} r^B$ and $r^{\sqcap\mathcal{B}} = \bigcap_{B\in\mathcal{B}} r^B$.

Let R_1 be an S-sorted set of binary relations $r_s : s \times s$. For all $B, C \in Mod(A,\Sigma')$, $B \cdot C \in Mod(A,\Sigma')$ is defined as follows: For all $r \in R_1$, $r^{B\cdot C} = r^B \cdot r^C$.

$\sigma : Mod(A,\Sigma') \to Mod(A,\Sigma')$ maps B to $B|_\sigma$.

$B \in Mod(A,\Sigma')$ is **σ-closed** if $\sigma(B) \leq B$.
$B \in Mod(A,\Sigma')$ is **σ-dense** if $B \leq \sigma(B)$.

σ is **monotone** if for all $B, C \in Mod(A,\Sigma')$, $B \leq C$ implies $\sigma(B) \leq \sigma(C)$.

σ is **continuous** if for all increasing chains $B_0 \leq B_1 \leq B_2 \leq \dots$ of elements of $Mod(A,\Sigma')$, $\sigma(\sqcup_{i\in\mathbb{N}} a_i) \leq \sqcup_{i\in\mathbb{N}} \sigma(a_i)$.

σ is **cocontinuous** if for all decreasing chains $B_0 \geq B_1 \geq B_2 \geq \dots$ of elements of $Mod(A,\Sigma')$, $\sqcap_{i\in\mathbb{N}} \sigma(a_i) \leq \sigma(\sqcap_{i\in\mathbb{N}} a_i)$.

- If SP' is a μ-extension of SP, then

$$B \in Mod(A,\Sigma') \models AX_1 \quad \text{iff} \quad B \models \bigwedge_{r \in R_1} (r \Leftarrow \sigma(r)) \quad \text{iff } B \text{ is } \sigma\text{-closed.}$$

- If SP' is a ν-extension of SP, then

$$B \in Mod(A,\Sigma') \models AX_1 \quad \text{iff} \quad B \models \bigwedge_{r \in R_1} (r \Rightarrow \sigma(r)) \quad \text{iff } B \text{ is } \sigma\text{-dense.}$$

- If SP' is a μ- or ν-extension of SP, then

$$B \in Mod(A,\Sigma') \models AX_1 \quad \text{iff} \quad B \models \bigwedge_{r \in R_1} (r \Leftrightarrow \sigma(r)) \quad \text{iff } B \text{ is a fixpoint of } \sigma.$$

- $B \in Mod(A,\Sigma')$ is a fixpoint of σ iff for all Σ'-formulas ψ, $B \models \psi \Leftrightarrow \sigma(\psi)$.

(Iterative/circular/strong) induction and coinduction

Let $SP = (\Sigma, AX)$,
$SP_1 = (\Sigma_1, AX \uplus AX_1)$ and $SP_2 = (\Sigma_2, AX \uplus AX_2)$ be specifications such that both SP_1 and SP_2 are either μ- or ν-extensions of SP and the set R_1 of relations defined by SP_1 is contained in the set of relations defined by SP_2.

For $i = 1, 2$, let σ_i be the relation transformer of SP_i.
Let $\tau : \Sigma' \to \Sigma'$ be a signature morphism that is the identity on Σ.

Induction. Suppose that $lfp(\sigma_1) \leq lfp(\sigma_2)$.

$$lfp(\sigma_1) \models \bigwedge_{r \in R_1} (r \Rightarrow \tau(r)) \quad \text{if} \quad \exists\, n > 0 : lfp(\sigma_1) \models \bigwedge_{r \in R_1} (\tau(\sigma_2^n(r)) \Rightarrow \tau(r)).$$

Coinduction. Suppose that $gfp(\sigma_2) \leq gfp(\sigma_1)$.

$$gfp(\sigma_1) \models \bigwedge_{r \in R_1} (\tau(r) \Rightarrow r) \quad \text{if} \quad \exists\, n > 0 : gfp(\sigma_1) \models \bigwedge_{r \in R_1} (\tau(r) \Rightarrow \tau(\sigma_2^n(r))).$$

Abstraction and restriction

Let $SP' = (\Sigma', AX')$ be a swinging type with base type $SP = (\Sigma, AX)$ and primitive subtype $SP_0 = (\Sigma_0, AX_0)$, σ be the relation transformer of SP' and A be an SP_0-model.

Suppose that SP' satisfies (7). Let Ini be initial in $Mod_{EU}(A, SP)$.
If σ is continuous, then $lfp(\sigma)/\equiv^{lfp(\sigma)}$ is initial in $Mod_{EU}(A, SP')$.

Suppose that SP' satisfies (8). Let Ini be initial in $Mod_{EU}(A, SP)$.
If σ is cocontinuous, then $gfp(\sigma)/\equiv^{gfp(\sigma)}$ is final in $RMod_{EU}(A, SP')$.

Suppose that SP' satisfies (9). Let Fin be final in $Mod_{EU}(A, SP)$.
If σ is continuous, then $all^{gfp(\sigma)}$ is final in $Mod_{EU}(A, SP')$.

Suppose that SP' satisfies (10). Let Fin be final in $Mod_{EU}(A, SP)$.
If σ is cocontinuous, then $all^{lfp(\sigma)}$ is initial in $OMod_{EU}(A, SP')$.

Supertyping and subtyping I

Let $SP' = (\Sigma', AX')$ be a swinging type with base type $SP = (\Sigma, AX)$ and primitive subtype SP_0 and A be an SP_0-model.

(1) Suppose that SP' satisfies (11). Let Ini and Ini' be initial in $Mod_{EU}(A, SP)$ resp. $Mod_{EU}(A, SP')$.
The unique Σ-homomorphism $h : Ini \to Ini'|_\Sigma$ is an isomorphism iff h can be extended to a Σ'-homomorphism in which case Ini is initial in $Mod_{EU}(A, SP')$.

(2) Suppose that SP' satisfies (12). Let Fin and Fin' be final in $Mod_{EU}(A, SP)$ resp. $Mod_{EU}(A, SP')$.
The unique Σ-homomorphism $h : Fin'|_\Sigma \to Fin$ is an isomorphism iff h can be extended to a Σ'-homomorphism in which case Fin is final in $Mod_{EU}(A, SP')$.

Reachability and observability

Let $\Sigma_0 = (S_0, F_0, R_0, B_0)$ and $\Sigma = (S, F, R, B)$ be signatures such that $\Sigma_0 \subseteq \Sigma$, $S_1 = S \setminus S_0$ and $A \in Mod(\Sigma)$.

The **reachability invariant** of A is the S-sorted set that is defined as follows:

$$reach_s^A \ =_{def} \ \begin{cases} A_s & \text{if } s \in S_0 \\ \{a \in A_s \mid \exists\, t{:}dom \to s \in Gen_\Sigma,\ b \in A_{dom} : t^A(b) = a\} & \text{if } s \in S_1 \end{cases}$$

A is **reachable** if $reach^A = A$.

The **observability congruence** of A is the S-sorted set that is defined as follows:

$$obs_s^A \ =_{def} \ \begin{cases} \Delta_s^A & \text{if } s \in S_0 \\ \{(a,b) \in A_s^2 \mid \forall\, t{:}s \to ran \in Obs_\Sigma : t^A(a) = t^A(b)\} & \text{if } s \in S_1 \end{cases}$$

A is **observable** if $obs^A = \Delta^A$.

Consistency and completeness

Let $\Sigma = (S, F, R, B)$ be a signature, $A \in Mod(\Sigma)$, $S_0 \subseteq S$ and $S_1 = S \setminus S_0$.

A set C of constructors of F is **consistent for A**
if for all $s \in S_1$, $f : dom \to s, g : dom' \to s \in C$, $a \in A_{dom}$ and $b \in A_{dom'}$,
$f^A(a) = g^A(b)$ implies $f = g$ and $a = b$.

A set D of destructors of F is **complete for A**
if for all $s \in S_1$ and $a, b \in A_s$, $a \neq b$ implies $f^A(a) \neq f^A(b)$ for some $f \in D$.

Supertyping and subtyping II

Let $SP' = (\Sigma', AX')$ be a swinging type with base type $SP = (\Sigma, AX)$ and primitive subtype $SP_0 = (\Sigma_0, AX_0)$, $\Sigma' = (S', F', R', B')$, $\Sigma = (S, F, R, B)$, $\Sigma_0 = (S_0, F_0, R_0, B_0)$ and A be an SP_0-model.

(1) Suppose that SP satisfies (1) and $SP = SP'$ or SP' satisfies (11).
Let Ini and Ini' be initial in $Mod_{EU}(A, SP)$ resp. $Mod_{EU}(A, SP')$.
If $Ini \cong Ini'|_\Sigma$, then $F \setminus F_0$ is a consistent for Ini'.

(2) Suppose that SP satisfies (2) and $SP = SP'$ or SP' satisfies (12).
Let Fin and Fin' be final in $Mod_{EU}(A, SP)$ resp. $Mod_{EU}(A, SP')$.
If If $Fin \cong Fin'|_\Sigma$, then $F \setminus F_0$ is complete for Fin'.

Perfect model of a swinging type

Let $SP' = (\Sigma', AX')$ be a swinging type with base type $SP = (\Sigma, AX)$ and primitive subtype SP_0.

If $SP' = SP = SP_0 = (\emptyset, \emptyset)$, then $Per(SP)$ is the empty Σ-structure. Otherwise

- SP is visible $\Longrightarrow Per(SP')$ is initial $Mod_{EU}(Per(SP_0), SP')$
- SP is hidden $\Longrightarrow Per(SP')$ is final of $Mod_{EU}(Per(SP_0), SP')$
- (5) $\Longrightarrow Per(SP')$ is the least fixpoint of the relation transformer of SP'
- (6) $\Longrightarrow Per(SP')$ is the greatest fixpoint of the relation transformer of SP'