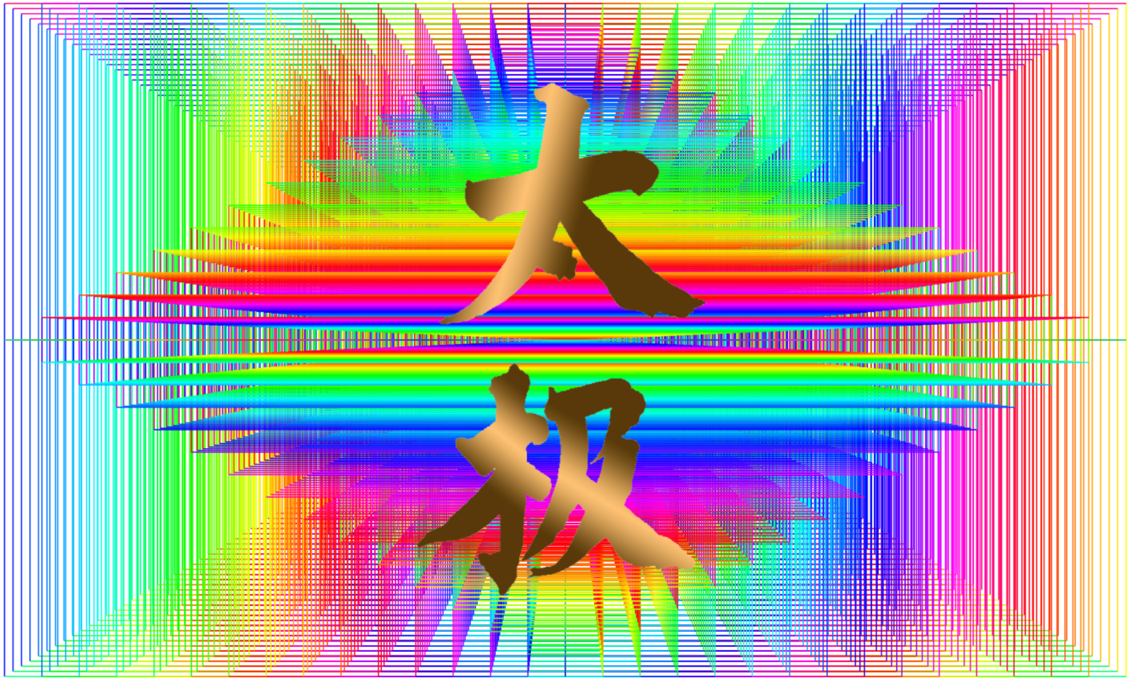


Modeling and reasoning with $\mathcal{I}$-polynomial data types

Peter Padawitz, TU Dortmund, Germany

September 1, 2017

(actual version: http://fldit-www.cs.uni-dortmund.de/∼peter/IFIP2016.pdf)

Road map

The next steps:

- First-order and modal formulas
- Congruences and invariants
- Induction and coinduction
- Varieties and covarieties
- Term monads and coterm comonads

Some examples that motivated this approach

$\Rightarrow$ points to the carrier set of a standard model of the respective signature.

Constructive signatures

- $Nat \Rightarrow \mathbb{N}$

$$S = \{nat\}, \quad \mathcal{I} = \emptyset, \quad F = \{ \begin{array}{l} zero : 1 \to nat, \\ succ : nat \to nat \ \}. \end{array}$$

- $Lists(X,Y) \Rightarrow X^* \times I$

$$S = \{list\}, \quad \mathcal{I} = \{X, Y\}, \quad F = \{ \begin{array}{l} nil : Y \to list, \\ cons : X \times list \to list \ \}. \end{array}$$

- $List(X) =_{def} Lists(X, 1) \Rightarrow X^*$,

  alternatively:

$$S = \{list\}, \quad \mathcal{I} = \{X, \mathbb{N}_{>1}\}, \quad F = \{[\dots] : X^* \to list\}.$$

- $Bintree(X)$ ⇝ binary trees of finite depth with node labels from X

$$S = \{btree\}, \quad \mathcal{I} = \{X\} \quad F = \{ \begin{array}{l} empty : 1 \to btree, \\ bjoin : btree \times X \times btree \to btree \ \}. \end{array}$$

- $Tree(X,Y)$ ⇝ finitely branching trees of finite depth with node labels from X and edge labels from Y

$$S = \{tree, trees\}, \ \mathcal{I} = \{X,Y\}, \ F = \{ \begin{array}{l} join : X \times trees \to tree, \\ nil : 1 \to trees, \\ cons : Y \times tree \times trees \to trees \ \}. \end{array}$$

- $Reg(BS)$ ⇝ regular expressions over BS

$$S = \{reg\}, \ \mathcal{I} = \{BS\}, \ F = \{ \begin{array}{ll} par : reg \times reg \to reg, & \text{(parallel composition)} \\ seq : reg \times reg \to reg, & \text{(sequential composition)} \\ iter : reg \to reg, & \text{(iteration)} \\ base : BS \to reg \ \} & \text{(embedding of base sets)} \end{array}$$

- $CCS(Act)$ ⇝ Calculus of Communicating Systems

$$
\begin{aligned}
S &= \{\ proc\ \}, \quad \mathcal{I} = \{Act\}, \\
F &= \{\ pre : Act \to proc, && \text{(prefixing by an action)} \\
&\quad\ \ cho : proc \times proc \to proc, && \text{(choice)} \\
&\quad\ \ par : proc \times proc \to proc, && \text{(parallelism)} \\
&\quad\ \ res : proc \times Act \to proc, && \text{(restriction)} \\
&\quad\ \ rel : proc \times Act^{Act} \to proc\ \}. && \text{(relabelling)}
\end{aligned}
$$

Destructive signatures

- $coNat$ ⇝ $\mathbb{N} \cup \{\infty\}$

$$S = \{nat\}, \quad \mathcal{I} = \emptyset, \quad F = \{pred : nat \to 1 + nat\}.$$

- $coList(X)$ ⇝ $X^* \cup X^{\mathbb{N}}$ $(coList(1) \mathrel{\widehat{=}} coNat)$

$$S = \{list\}, \quad \mathcal{I} = \{X\}, \quad F = \{split : list \to 1 + X \times list\}.$$

- $coBintree(X)$ ⇝ binary trees of finite or infinite depth with node labels from X

$$S = \{btree\}, \quad \mathcal{I} = \{X\}, \quad F = \{split : btree \to 1 + btree \times X \times btree\}.$$

- $coTree(X, Y)$ ⇝ finitely or infinitely branching trees of finite or infinite depth with node labels from X and edge labels from Y

$$S = \{tree\}, \quad \mathcal{I} = \{X, Y\}, \quad F = \{ \; root : tree \to X, \; subtrees : tree \to etrees, \; split : etrees \to 1 + Y \times tree \times etrees \; \}.$$

- $FBTree(X, Y)$ ⇝ finitely branching trees of finite or infinite depth with node labels from X and edge labels from Y

$$S = \{tree\}, \quad \mathcal{I} = \{X, Y, \mathbb{N}_{>1}\}, \quad F = \{ \; root : tree \to X, \; subtrees : tree \to (Y \times tree)^* \; \}.$$

- $Inftree(X, Y)$ ⇝ finitely branching trees of infinite depth with node labels from X and edge labels from Y

$$S = \{tree\}, \quad \mathcal{I} = \{X, Y, \mathbb{N}_{>1}\}, \quad F = \{ \; root : tree \to X, \; subtrees : tree \to (Y \times tree)^+ \; \}.$$

- $\mathit{DAut}(X,Y) \leadsto Y^{X^*}$ = behaviors of deterministic Moore automata with input from X and output from Y

$$S = \{\mathit{state}\}, \quad \mathcal{I} = \{X, Y\}, \quad F = \{\ \delta : \mathit{state} \to \mathit{state}^X,$$
$$\beta : \mathit{state} \to Y\ \}.$$

- $\mathit{Acc}(X) =_{\mathit{def}} \mathit{DAut}(X,2) \leadsto \mathcal{P}(X) \cong 2^{X^*}$ = behaviors of deterministic acceptors of languages over X

- $\mathit{Stream}(X) =_{\mathit{def}} \mathit{DAut}(1,X) \leadsto X^{\mathbb{N}}$

$$S = \{\mathit{stream}\}, \quad \mathcal{I} = \{X\}, \quad F = \{\ \mathit{head} : \mathit{stream} \to X,$$
$$\mathit{tail} : \mathit{stream} \to \mathit{stream}\ \},$$

alternatively:

$$S = \{\mathit{stream}\}, \quad \mathcal{I} = \{X, \mathbb{N}\}, \quad F = \{\mathit{get} : \mathit{stream} \to X^{\mathbb{N}}\}.$$

- $\mathit{Infbintree}(X) \leadsto$ binary trees of infinite depth with node labels from X

$$S = \{\mathit{btree}\}, \quad \mathcal{I} = \{X\}, \quad F = \{\ \mathit{root} : \mathit{btree} \to X,$$
$$\mathit{left}, \mathit{right} : \mathit{btree} \to \mathit{btree}\ \}.$$

- $PAut(X,Y)$ ⇝ $(1+Y)^{X^*}$ = partial automata

$$S = \{state\}, \quad \mathcal{I} = \{X, Y\}, \quad F = \{\ \delta : state \to (1 + state)^X, \\ \beta : state \to Y\ \}.$$

- $NAut(X,Y)$ ⇝ $(Y^*)^{X^*}$ = behaviors of non-deterministic image finite automata

$$S\{state\}, \quad \mathcal{I} = \{X, Y, \mathbb{N}_{>1}\}, \quad F = \{\ \delta : state \to (state^*)^X, \\ \beta : state \to Y\ \}.$$

- $WAut(X,Y,CM)$ ⇝ $((CM \times Y)^*)^{X^*}$ = behaviors of CM-weighted automata

$$S = \{state\}, \quad \mathcal{I} = \{X, Y, CM, \mathbb{N}_{>1}\}, \quad F = \{\ \delta : state \to ((state \times CM)^*)^X, \\ \beta : state \to Y\ \}.$$

- $SAut(X,Y)$ ⇝ $(([0,1] \times Y)^*)^{X^*}$ = behaviors of stochastic automata

$$S = \{state\}, \quad \mathcal{I} = \{X, Y, [0,1], \mathbb{N}_{>1}\}, \quad F = \{\ \delta : state \to ((state \times [0,1])^*)^X, \\ \beta : state \to Y\ \}.$$

- $Proctree(Act)$ ⇝ process trees whose edges are labelled with actions

$$S = \{tree\}, \quad \mathcal{I} = \{Act, \mathbb{N}_{>1}\}, \quad F = \{\ \delta : tree \to (Act \times tree)^*\ \}.$$

- $Class(\mathcal{I})$ ↬ behaviors of a class with n methods

$$
\begin{aligned}
S &= \{\ state\ \}, \quad \mathcal{I} = \{X_1, \ldots, X_n, Y_1, \ldots, Y_n, E_1, \ldots, E_n\}, \\
F &= \{\ m_i : state \to ((state \times Y_i) + E_i)^{X_i} \mid 1 \leq i \leq n\ \}.
\end{aligned}
$$

$\mathcal{I}$-polynomial types

Let S be a finite set and $\mathcal{I}$ be a set of nonempty sets (of indices), implicitly including the one-element set $1 = \{\epsilon\}$, the two-element set $2 = \{0,1\}$ and the n-element set $[n] = \{1,\dots,n\}$ for all $n > 1$. 1, 2 and [n] are omitted in the listings of index sets of sample signatures.

The set $\mathcal{T}(S,\mathcal{I})$ of **$\mathcal{I}$-polynomial types over** S is inductively defined as follows:

- $S \cup \mathcal{I} \subseteq \mathcal{T}(S,\mathcal{I})$.
- For all $I \in \mathcal{I}$ and $\{e_i\}_{i\in I} \subseteq \mathcal{T}(S,\mathcal{I})$, $\coprod_{i\in I} e_i, \prod_{i\in I} e_i \in \mathcal{T}(S,\mathcal{I})$.

For alle $I \in \mathcal{I}$, $n > 1$ and $e, e_1, \dots, e_n \in \mathcal{T}(S,\mathcal{I})$ we use the following short notations:

$$\begin{aligned}
e_1 \times \cdots \times e_n &=_{def} \prod_{i\in[n]} e_i,\\
e_1 + \cdots + e_n &=_{def} \coprod_{i\in[n]} e_i,\\
e^I &=_{def} \prod_{i\in I} e,\\
e^n &=_{def} e^{[n]},\\
e^+ &=_{def} e + \coprod_{n>1} e^n,\\
e^* &=_{def} 1 + e^+.
\end{aligned}$$

Signatures

A **signature** $\Sigma = (S, \mathcal{I}, F)$ consists of sets S and $\mathcal{I}$ as above and a finite set F of typed function symbols ("operations") $f : e \to e'$ with $e, e' \in \mathcal{T}(S, \mathcal{I})$.

$f : e \to e' \in F$ is a **constructor** if $e' \in S$ and a **destructor** if $e \in S$.

Σ is **constructive** if F consists of constructors and for all $s \in S$, $\mathcal{I}$ implicitly contains $\{f \in F \mid ran(f) = s\}$.

Σ is **destructive** if F consists of destructors and for all $s \in S$, $\mathcal{I}$ implicitly contains $\{f \in F \mid dom(f) = s\}$.

Terms and coterms

$A \multimap B$ denotes the set of partial functions from A to B.

$L \subseteq A^*$ is **prefix closed** if for all $w \in A^*$ and $a \in A$, $wa \in L$ implies $w \in L$.

A **deterministic tree** is a partial function $f : A^* \multimap B$ with prefix closed domain.

f may be written as a kind of record:

$$t_f \;=\; f(\epsilon)\{x \to t_{\lambda w.f(xw)} \mid x \in def(t) \cap A\}.$$

f is **well-founded** if there is $n \in \mathbb{N}$ with $|w| \leq n$ for all $w \in def(t)$, intuitively: all paths emanating from the root are finite.

$dtr(A, B)$ denotes the set of all deterministic trees from A^* to B.
$wdtr(A, B)$ denotes the set of all wellfounded trees of $dtr(A, B)$.

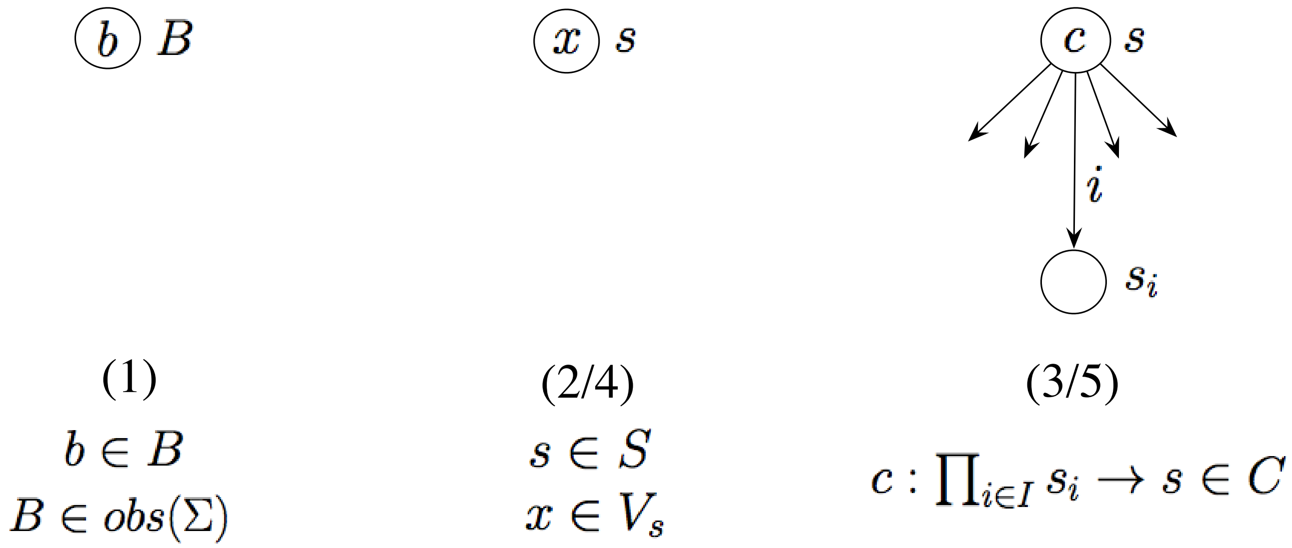
Let $\Sigma = (S, \mathcal{I}, F)$ be a signature, V be an S-sorted set,

$$\begin{aligned} EL_\Sigma &= \bigcup \mathcal{I} \cup \{sel\}, && \text{(edge labels)} \\ NL_{\Sigma,V} &= \bigcup \mathcal{I} \cup V \cup \{tup\}. && \text{(node labels)} \end{aligned}$$

Let Σ be constructive.

The set $CT_\Sigma(V)$ **Σ-terms over** V is the greatest $\mathcal{T}(S,\mathcal{I})$-sorted set M of subsets of $dtr(EL_\Sigma, NL_{\Sigma,V})$ with the following properties: Let $I \in \mathcal{I}$ and $\{e_i\}_{i\in I} \subseteq \mathcal{T}(S,\mathcal{I})$.

- $M_I = (1 \to I)$. (1)
- For all $s \in S$ and $t \in M_s$, $t \in V_s$ (2)
  or $t = c\{sel \to t'\}$ for some $c : e \to s \in F$ and $t' \in M_e$. (3)
- For all $t \in M_{\prod_{i\in I} e_i}$ and $i \in I$, $t = tup\{i \to t_i \mid i \in I\}$ for some $t_i \in M_{e_i}$. (4)
- For all $t \in M_{\coprod_{i\in I} e_i}$, $t = i\{sel \to t'\}$ for some $i \in I$ and $t' \in M_{e_i}$. (5)



Terms with their respective types.

The elements of $CT_\Sigma =_{def} CT_\Sigma(\emptyset)$ are called **ground Σ-terms**.

$T_\Sigma(V) =_{def} CT_\Sigma(V) \cap wdtr(EL_\Sigma, NL_{\Sigma,V})$ is the least $\mathcal{T}(S,\mathcal{I})$-sorted set M of subsets of $dtr(EL_\Sigma, NL_{\Sigma,V})$ with (1) and the following properties:

Let $I \in \mathcal{I}$ and $\{e_i\}_{i\in I} \subseteq \mathcal{T}(S,\mathcal{I})$.

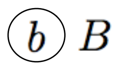
- For all $s \in S$, $V_s \subseteq M_s$. (6)
- For all $c : e \to s \in F$ and $t \in M_e$, $c\{sel \to t\} \in M_s$. (7)
- For all $t_i \in M_{e_i}$, $i \in I$, $tup\{i \to t_i \mid i \in I\} \in M_{\prod_{i\in I} e_i}$. (8)
- For all $i \in I$ and $t \in M_{e_i}$, $i\{sel \to t\} \in M_{\coprod_{i\in I} e_i}$. (9)

$T_\Sigma =_{def} T_\Sigma(\emptyset)$.

Let Σ be destructive.

The set $DT_\Sigma(V)$ of **Σ-coterms over V** is the greatest $\mathcal{T}(S,\mathcal{I})$-sorted set M of subsets of $dtr(EL_\Sigma, NL_{\Sigma,V})$ with (1), (4), (5) and the following property:

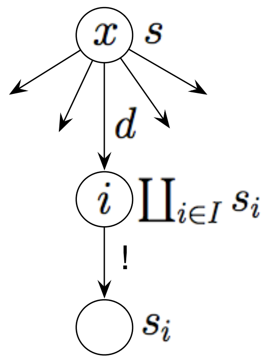
- For all $s \in S$ and $t \in M_s$ there is $x \in V_s$ and for all $d : s \to e \in F$ there is $t_d \in M_e$ with $t = x\{d \to t_d \mid d : s \to e \in F\}$. (10)



(1)

$b \in B$

$B \in obs(\Sigma)$



(6/7)

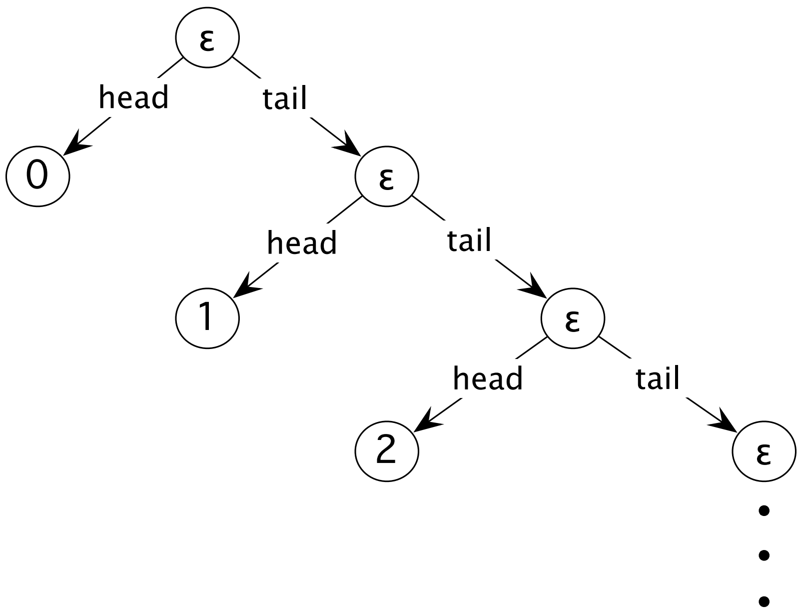
$x \in V_s$

$d : s \to \coprod_{i\in I} s_i \in D$

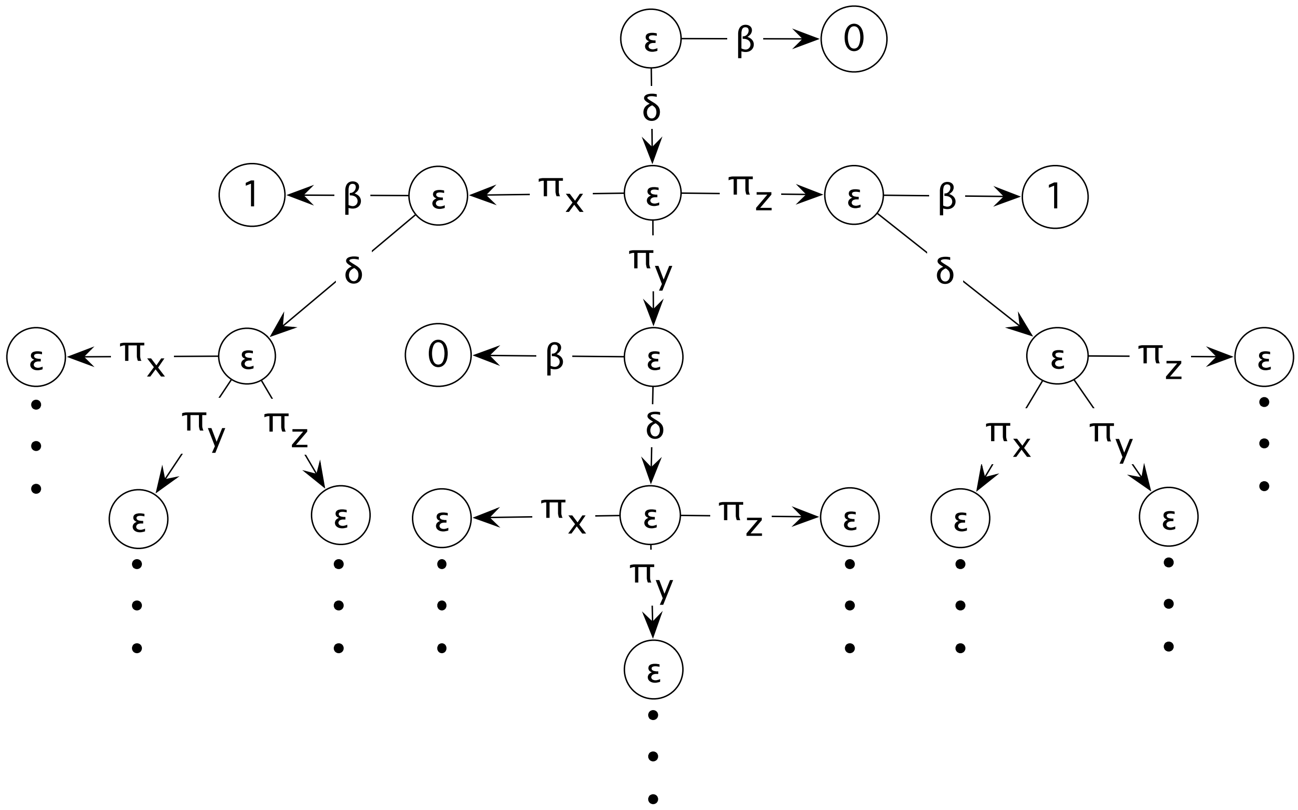
Coterms with their respective types.

The elements of $DT_\Sigma =_{def} DT_\Sigma(1)$ are called **ground Σ-coterms**.

Examples



Stream($\mathbb{N}$)*-coterm that represents the stream of natural numbers*



Acc$(\{x, y, z\})$*-coterm that represents an acceptor of all words over* $\{x, y, z\}$ *containing* x *or* z

$coT_\Sigma(V) =_{def} DT_\Sigma(V) \cap wdtr(EL_\Sigma, NL_{\Sigma,V})$ is the least $\mathcal{T}(S,\mathcal{I})$-sorted set M of subsets of $dtr(EL_\Sigma, NL_{\Sigma,V})$ with (1), (8), (9) and the following property:

- For all $s \in S$, $x \in V_s$, $d : s \to e \in F$ and $t_d \in M_e$, $x\{d \to t_d \mid d : s \to e \in F\} \in M_s$. (11)

$coT_\Sigma =_{def} coT_\Sigma(1)$.

The set $T_\Sigma(V)$ of **well-founded Σ-terms over** V, however, is defined as if Σ were constructive:

$T_\Sigma(V)$ is the least $\mathcal{T}(S,\mathcal{I})$-sorted set M of subsets of $dtr(EL_\Sigma, NL_{\Sigma,V})$ with (1), (6), (8), (9), but the following property instead of (7):

- For all $s \in S$, $d : s \to e \in F$ and $t_d \in M_e$, $\epsilon\{d \to t_d \mid d : s \to e \in F\} \in M_s$. (12)

Type compatible $\mathcal{T}(S,\mathcal{I})$-sorted sets

A $\mathcal{T}(S,\mathcal{I})$-sorted set A is **type compatible** if for all $I \in \mathcal{I}$,

- $A_I = (1 \to I)$,
- for all $\{e_i\}_{i\in I} \subseteq \mathcal{T}(S,\mathcal{I})$
- there are

$$\pi = (\pi_i : A_{\prod_{i\in I} e_i} \to A_{e_i})_{i\in I} \quad \text{and} \quad \iota = (\iota_i : A_{e_i} \to A_{\coprod_{i\in I} e_i})_{i\in I}$$

  such that $(A_{\prod_{i\in I} e_i}, \pi)$ is a **product** and $(A_{\coprod_{i\in I} e_i}, \iota)$ is a **sum** or **coproduct** of $(A_{e_i})_{i\in I}$.

Let A be type compatible, $I \in \mathcal{I}$ and $\{e_i\}_{i\in I} \subseteq \mathcal{T}(S,\mathcal{I})$.

(1) For all $a \in A_{\coprod_{i\in I} e_i}$ there are unique $i \in I$ and $b \in A_{e_i}$ such that $\iota_i(b) = a$.

(2) For all $a, b \in A_{\prod_{i\in I} e_i}$, $a = b$ if for all $i \in I$, $\pi_i(a) = \pi_i(b)$.

Let A, B be type compatible $\mathcal{T}(S,\mathcal{I})$-sorted sets.

A $\mathcal{T}(S,\mathcal{I})$-sorted function $h : A \to B$ is **type compatible** if for all $I \in \mathcal{I}$,

- $h_I = id_I$,
- for all $\{e_i\}_{i\in I} \subseteq \mathcal{T}(S,\mathcal{I})$, $h_{\prod_{i\in I} e_i} = \prod_{i\in I} h_{e_i}$ and $h_{\coprod_{i\in I} e_i} = \coprod_{i\in I} h_{e_i}$.

$Set^{S,\mathcal{I}}$ denotes the subcategory of $Set^{\mathcal{T}(S,\mathcal{I})}$ with type compatible $\mathcal{T}(S,\mathcal{I})$-sorted sets as objects and type compatible $\mathcal{T}(S,\mathcal{I})$-sorted functions as morphisms.

$e \in \mathcal{T}(S,\mathcal{I})$ induces the projection functor $F_e : Set^{S,\mathcal{I}} \to Set$ that maps every object and morphism of $Set^{S,\mathcal{I}}$ to its respective e-component.

Lifting S-sorted to $\mathcal{T}(S,\mathcal{I})$-sorted relations

Let $A = (A_e)_{e\in\mathcal{T}(S,\mathcal{I})}$ be a type compatible $\mathcal{T}(S,\mathcal{I})$-sorted set, $n > 0$ and $R_s \subseteq A_s^n$ for all $s \in S$.

For all $I \in \mathcal{I}$, $R_I =_{def} \Delta_I^n$ and for all $\{e_i\}_{i\in I} \subseteq \mathcal{T}(S,\mathcal{I})$,

$$\begin{aligned} R_{\prod_{i\in I} e_i} &=_{def} \{(a_1,\dots,a_n) \in A^n_{\prod_{i\in I} e_i} \mid \forall\, i \in I : (\pi_i(a_1),\dots,\pi_i(a_n)) \in R_{e_i}\}, \\ R_{\coprod_{i\in I} e_i} &=_{def} \{(\iota_i(a_1),\dots,\iota_i(a_n)) \mid (a_1,\dots,a_n) \in R_{e_i},\ i \in I\} \subseteq A^n_{\coprod_{i\in I} e_i}. \end{aligned}$$

Let $\Sigma = (S, \mathcal{I}, F)$ be a signature.

A **Σ-algebra** $\mathcal{A} = (A, Op)$ consists of a type compatible $\mathcal{T}(S, \mathcal{I})$-sorted set A and an F-sorted set

$$Op \;=\; (f^{\mathcal{A}} : A_e \to A_{e'})_{f:e\to e'\in F}$$

of functions.

Let $\mathcal{A}, \mathcal{B}$ be Σ-algebras. A type compatible $\mathcal{T}(S, \mathcal{I})$-sorted function $h : \mathcal{A} \to \mathcal{B}$ is a **Σ-homomorphism** if for all $f : e \to e' \in F$,

$$h_{e'} \circ f^{A} \;=\; f^{B} \circ h_e.$$

Alg_Σ denotes the subcategory of $Set^{S,\mathcal{I}}$ with Σ-algebras as objects and Σ-homomorphisms as morphisms.

If Σ is constructive, then $CT_\Sigma(V)$ is a Σ-algebra:

Let $I \in \mathcal{I}$ and $\{e_i\} \subseteq \mathcal{T}(S, \mathcal{I})$.

- For all $c : e \to s \in C$, $t \in CT_\Sigma(V)_e$, $c^{CT_\Sigma(V)}(t) =_{def} c\{sel \to t\}$.
- For all $t_i \in CT_\Sigma(V)_{e_i}$, $i \in I$, and $k \in I$, $\pi_k(tup\{i \to t_i \mid i \in I\}) =_{def} t_k$.
- For all $i \in I$ and $t \in CT_\Sigma(V)_{e_i}$, $\iota_i(t) =_{def} i\{sel \to t\}$.

$T_\Sigma(V)$ is a Σ-subalgebra of $CT_\Sigma(V)$.

If Σ is destructive, then $DT_\Sigma(V)$ is a Σ-algebra:

Let $I \in \mathcal{I}$ and $\{e_i\} \subseteq \mathcal{T}(S,\mathcal{I})$.

- For all $d : s \to e \in D$, $x \in V_s$ and $t'_d \in DT_\Sigma(V)_e$, $d' : s \to e' \in D$,
$$d^{DT_\Sigma(V)}(x\{d \to t'_d \mid d' : s \to e' \in D\}) =_{def} t_d.$$
- For all $t_i \in DT_\Sigma(V)_{e_i}$, $i \in I$, and $k \in I$, $\pi_k(tup\{i \to t_i \mid i \in I\}) =_{def} t_k$.
- For all $i \in I$ and $t \in DT_\Sigma(V)_{e_i}$, $\iota_i(t) =_{def} i\{sel \to t\}$.

$coT_\Sigma(V)$ is a Σ-subalgebra of $DT_\Sigma(V)$.

Let $e \in \mathcal{T}(S,\mathcal{I})$, $I \in \mathcal{I}$ and $\{e_i\}_{i\in I} \subseteq \mathcal{T}(S,\mathcal{I})$.

$\{c_i : A_{e_i} \to A_e \mid i \in I\}$ is a **set of constructors for** e if $[c_i]_{i\in I} : \coprod_{i\in I} A_{e_i} \to A_e$ is iso.

$\{d_i : A_e \to A_{e_i} \mid i \in I\}$ is a **set of destructors for** e if $\langle d_i\rangle_{i\in I} : A_e \to \prod_{i\in I} A_{e_i}$ is iso.

- The injections of A for a sum type form a set of constructors for this type.
- The projections of A for a product type form a set of destructors for this type.
- If Σ is constructive and $\mathcal{A}$ is initial in Alg_Σ, then for all $s \in S$, $\{f^\mathcal{A} \mid f : e \to s \in F\}$ is a set of constructors for s.
- If Σ is destructive and $\mathcal{A}$ is final in Alg_Σ, then for all $s \in S$, $\{f^\mathcal{A} \mid f : s \to e \in F\}$ is a set of destructors for s.

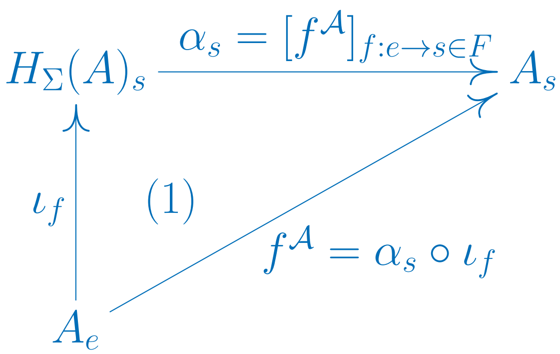
Let $\Sigma = (S, \mathcal{I}, F)$ be a constructive signature.

Σ induces the functor $H_\Sigma : Set^S \to Set^S$:

For all $A, B \in Set^S$, $h \in Set^S(A, B)$ and $s \in S$,

$$\begin{aligned} H_\Sigma(A)_s &= \coprod_{f:e\to s\in F} A_e, \\ H_\Sigma(h)_s &= \coprod_{f:e\to s\in F} h_e. \end{aligned}$$

For all $s \in S$ and $f : e \to s \in F$,



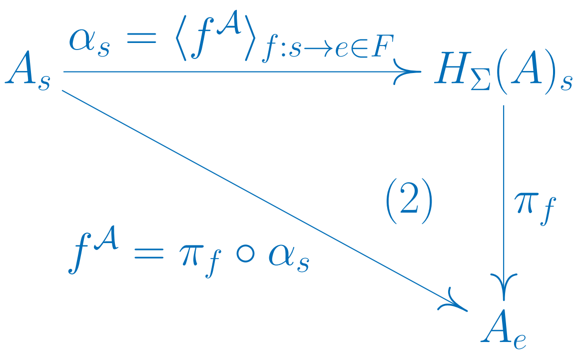
Let $\Sigma = (S, \mathcal{I}, F)$ be a destructive signature.

Σ induces the functor $H_\Sigma : Set^S \to Set^S$:

For all $A, B \in Set^S$, $h \in Set^S(A, B)$ and $s \in S$,

$$
\begin{aligned}
H_\Sigma(A)_s &= \prod_{f:s\to e\in F} A_e, \\
H_\Sigma(h)_s &= \prod_{f:s\to e\in F} h_e.
\end{aligned}
$$

For all $s \in S$ and $f : s \to e \in F$,



$$
\begin{aligned}
H_{NAut(X,Y)}(A)_{state} &= (A^*_{state})^X \times Y, \\
H_{WAut(X,Y,CM)}(A)_{state} &= ((A_{state} \times CM)^*)^X \times Y, \\
H_{SAut(X,Y)}(A)_{state} &= ((A_{state} \times [0,1])^*)^X \times Y.
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{W}_{fin}(A, CM) &= \{f : A \to CM \mid |supp(f)| < \omega\}, \\
\mathcal{D}_{fin}(A) &= \{f : A \to [0,1] \mid |supp(f)| < \omega, \ \sum f(supp(f)) = 1\}.
\end{aligned}
$$

$$
\begin{aligned}
B_{NAut(X,Y)}(A)_{state} &= \mathcal{P}_{fin}(A_{state})^X \times Y, \\
B_{WAut(X,Y,CM)}(A)_{state} &= \mathcal{W}_{fin}(A_{state}, CM)^X \times Y, \\
C_{SAut(X,Y)}(A)_{state} &= (\{((a_i, p_i))_{i=1}^n \in (A_{state} \times [0,1])^* \mid \textstyle\sum_{i=1}^n p_i = 1\})^X \times Y, \\
B_{SAut(X,Y)}(A)_{state} &= \mathcal{D}_{fin}(A_{state})^X \times Y.
\end{aligned}
$$

Do exist surjective natural transformations

$$
\begin{aligned}
\tau_1 : H_{NAut(X,Y)} &\to B_{NAut(X,Y)}, \\
\tau_2 : H_{WAut(X,Y,CM)} &\to B_{WAut(X,Y,CM)}, \\
\tau_3 : C_{SAut(X,Y)} &\to B_{SAut(X,Y)}
\end{aligned}
$$

and an injective natural transformation $\tau_4 : C_{SAut(X,Y)} \to H_{SAut(X,Y)}$?

Term folding und state unfolding

Let $\Sigma = (S, \mathcal{I}, C)$ be a constructive signature, $\mathcal{A} = (A, Op)$ be a Σ-algebra, V be an S-sorted set of "variables" and $g : V \to A$ be an S-sorted **valuation** of V.

The **extension** of g,

$$g^* : T_\Sigma(V) \to A,$$

is the $\mathcal{T}(S, \mathcal{I})$-sorted function that is inductively defined as follows:

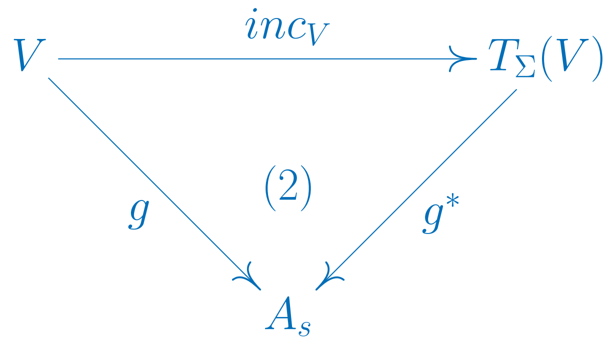
Let $I \in \mathcal{I}$ and $\{e_i\}_{i \in I} \subseteq \mathcal{T}(S, \mathcal{I})$.

- $g^*_I = id_I$. (1)
- For all $s \in S$ and $x \in V_s$, $g^*_s(x) = g_s(x)$. (2)
- For all $c : e \to s \in F$ and $t \in T_\Sigma(V)_e$, $g^*_s(c\{sel \to t\}) = c^{\mathcal{A}}(g^*_e(t))$. (3)
- For all $t_i \in T_\Sigma(V)_{e_i}$, $i \in I$, and $k \in I$, $\pi_k(g^*_{\prod_{i \in I} e_i}(\{tup \to t_i \mid i \in I\})) = g^*_{e_k}(t_k)$. (4)
- For all $k \in I$ and $t \in T_\Sigma(V)_{e_k}$, $g^*_{\coprod_{i \in I} e_i}(k\{sel \to t\}) = \iota_k(g^*_{e_k}(t))$. (5)

Intuitively, g^* evaluates each wellfounded Σ-term over V in $\mathcal{A}$.

Theorem FREE

g^* is the only Σ-homomorphism from $T_\Sigma(V)$ to $\mathcal{A}$ that satisfies (2):



The restriction of g^* to ground terms does not depend on g and is denoted by

$$fold^{\mathcal{A}}: T_\Sigma \to \mathcal{A}.$$

Since g^* is the only Σ-homomorphism from $T_\Sigma(V)$ to $\mathcal{A}$ that satisfies (2), $fold^{\mathcal{A}}$ is the only Σ-homomorphism from T_Σ to $\mathcal{A}$, i.e., T_Σ is initial in Alg_Σ.

$\mathcal{A}$ is **reachable** (or **generated**) if $fold^{\mathcal{A}}$ is epi.

$\mathcal{A}$ is **equationally consistent** if $fold^{\mathcal{A}}$ is mono.

Let $\Sigma = (S, \mathcal{I}, D)$ be a destructive signature, $\mathcal{A} = (A, Op)$ be a Σ-algebra, V be an S-sorted set of "colors" and $g : A \to V$ be an S-sorted **coloring** of A.

The **coextension** of g,

$$g^{\#} : A \to DT_{\Sigma}(V),$$

is the $\mathcal{T}(S, \mathcal{I})$-sorted function that is inductively defined as follows:

Let $I \in \mathcal{I}$ and $\{e_i\}_{i \in I} \subseteq \mathcal{T}(S, \mathcal{I})$.

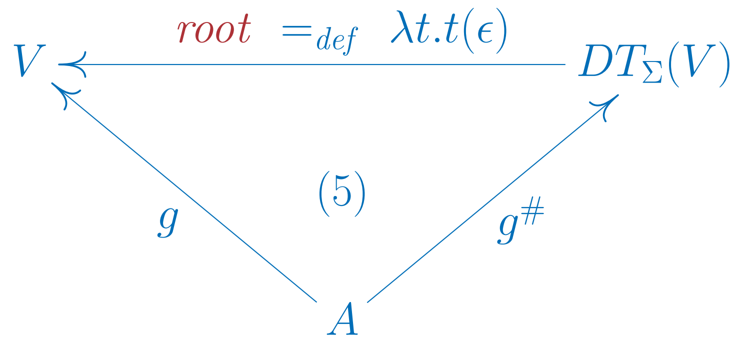
- $g_I^{\#} = id_I$. (1)
- For all $s \in S$ and $a \in A_s$, $g_s^{\#}(a) = g_s(a)\{d \to g_e^{\#}(d^{\mathcal{A}}(a)) \mid d : s \to e \in D\}$. (2)
- For all $a \in A_{\prod_{i \in I} e_i}$, $g^{\#}_{\prod_{i \in I} e_i}(a) = tup\{i \to g_{e_i}^{\#}(\pi_i(a)) \mid i \in I\}$. (3)
- For all $k \in I$ and $a \in A_{e_k}$, $g^{\#}_{\coprod_{i \in I} e_i}(\iota_k(a)) = k\{sel \to g_{e_k}^{\#}(a)\}$. (4)

Intuitively, $g^{\#}$ unfolds each "state" $a \in A$ into the Σ-coterm that represents the "behavior" of a w.r.t. $\mathcal{A}$.

In particular, the coextension $id_A^{\#} : A \to DT_{\Sigma}(A)$ "runs" (the destructors of) $\mathcal{A}$ on its arguments.

Theorem COFREE

$g^\#$ is the only Σ-homomorphism from $\mathcal{A}$ to $DT_\Sigma(V)$ that satisfies (5):



The restriction of $g^\#$ to ground coterms does not depend on g and is denoted by

$$unfold^{\mathcal{A}}: \mathcal{A} \to DT_\Sigma.$$

Since $g^\#$ is the only Σ-homomorphism from $\mathcal{A}$ to $DT_\Sigma(V)$ that satisfies (5), $unfold^{\mathcal{A}}$ is the only Σ-homomorphism from $\mathcal{A}$ to DT_Σ, i.e., DT_Σ is final in Alg_Σ.

$\mathcal{A}$ is **observable** (or **cogenerated**) if $unfold^{\mathcal{A}}$ is mono.

$\mathcal{A}$ is **behaviorally complete** if $unfold^{\mathcal{A}}$ is epi.

From constructors to destructors and backwards

Lambek's Lemma

(1) Suppose that Alg_F has an initial object $\alpha : F(A) \to A$. α is iso.

(2) Suppose that $coAlg_F$ has a final object $\beta : A \to F(A)$. β is iso.

Lambek's Lemma allows us to transform every constructive or destructive signature Σ into a destructive resp. constructive signature $co\Sigma$ such that

$$DT_{co\Sigma} \cong CT_{\Sigma} \quad \text{resp.} \quad T_{co\Sigma} \cong coT_{\Sigma}.$$

Here are the details:

Let $\Sigma = (S, \mathcal{I}, C)$ be a constructive signature,

$$\begin{aligned} D &= \{s : s \to \coprod_{c:e\to s\in C} e \mid s \in S\}, \\ co\Sigma &= (S, \mathcal{I}, D). \end{aligned}$$

By Lambek's Lemma (1), the initial H_Σ-algebra

$$\alpha = \{\alpha_s : H_\Sigma(T_\Sigma)_s \stackrel{[c^{T_\Sigma}]_{c:e\to s\in C}}{\longrightarrow} T_{\Sigma,s} \mid s \in S\}$$

is iso. Hence there is the H_Σ-coalgebra

$$\{\alpha_s^{-1} : T_{\Sigma,s} \to H_\Sigma(T_\Sigma)_s \mid s \in S\}$$

that corresponds to the $co\Sigma$-algebra $\mathcal{A} = (T_\Sigma, Op)$ with $s^{\mathcal{A}} = \alpha_s^{-1}$ for all $s \in S$.

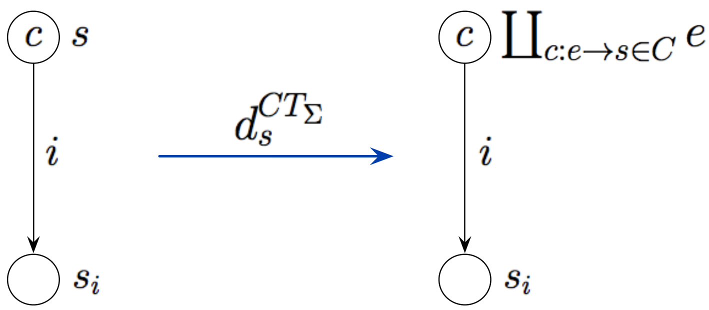
Since $co\Sigma$ is destructive, Theorem COFREE implies that $DT_{co\Sigma}$ is final in $Alg_{co\Sigma}$.

CT_Σ is also final in $Alg_{co\Sigma}$:

CT_Σ is a $co\Sigma$-algebra: Let $I \in \mathcal{I}$ and $\{e_i\} \subseteq \mathcal{T}(S, \mathcal{I})$.

- For all $c : e \to s \in C$, $t \in CT_{\Sigma,e}$,

$$s^{CT_\Sigma}(c\{sel \to t\}) =_{def} c\{sel \to t\}.$$

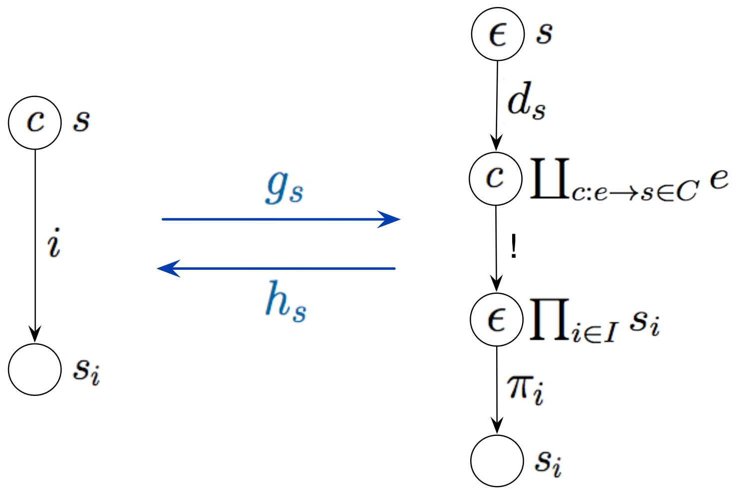


- For all $t_i \in CT_{\Sigma,e_i}$, $i \in I$, and $k \in I$, $\pi_k(tup\{i \to t_i \mid i \in I\}) =_{def} t_k$.
- For all $i \in I$ and $t \in CT_{\Sigma,e_i}$, $\iota_i(t) =_{def} i\{sel \to t\}$.

CT_Σ and $DT_{co\Sigma}$ are $co\Sigma$-isomorphic. Equivalently,

$$unfold^{CT_\Sigma} : CT_\Sigma \to DT_{co\Sigma}$$

is bijective.



Let $\Sigma = (S, \mathcal{I}, D)$ be a destructive signature,

$$\begin{array}{lll} C & = & \{s : \prod_{d:s\to e\in D} e \to s \mid s \in S\}, \\ co\Sigma & = & (S, \mathcal{I}, C). \end{array}$$

By Lambek's Lemma (2), the final H_Σ-coalgebra

$$\alpha = \{\alpha_s : DT_{\Sigma,s} \stackrel{\langle d^{DT_\Sigma}\rangle_{d:s\to e\in D}}{\longrightarrow} H_\Sigma(DT_\Sigma)_s \mid s \in S\}$$

is iso. Hence there is the H_Σ-algebra

$$\{\alpha_s^{-1} : H_\Sigma(DT_\Sigma)_s \to DT_{\Sigma,s} \mid s \in S\}$$

that corresponds to the $co\Sigma$-algebra $\mathcal{A} = (DT_\Sigma, Op)$ with $s^\mathcal{A} = \alpha_s^{-1}$ for all $s \in S$.

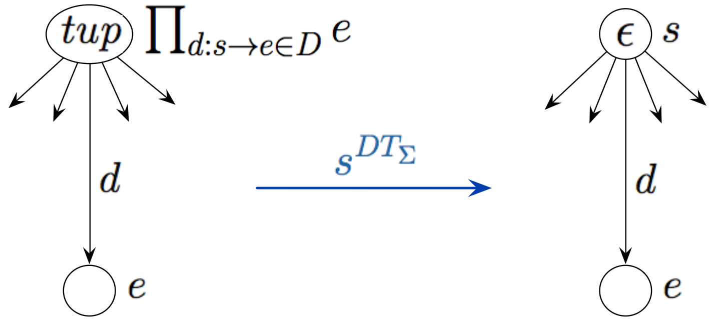
Since $co\Sigma$ is constructive, Theorem FREE implies that $T_{co\Sigma}$ is initial in $Alg_{co\Sigma}$.

coT_Σ is also initial in $Alg_{co\Sigma}$:

coT_Σ is a $co\Sigma$-algebra: Let $I \in \mathcal{I}$ and $\{e_i\} \subseteq \mathcal{T}(S, \mathcal{I})$.

- For all $s \in S$, $d : s \to e \in D$ and $t_d \in coT_{\Sigma,e}$,

$$s^{coT_\Sigma}(tup\{d \to t_d \mid d : s \to e \in D\}) =_{def} \epsilon\{d \to t_d \mid d : s \to e \in D\}.$$

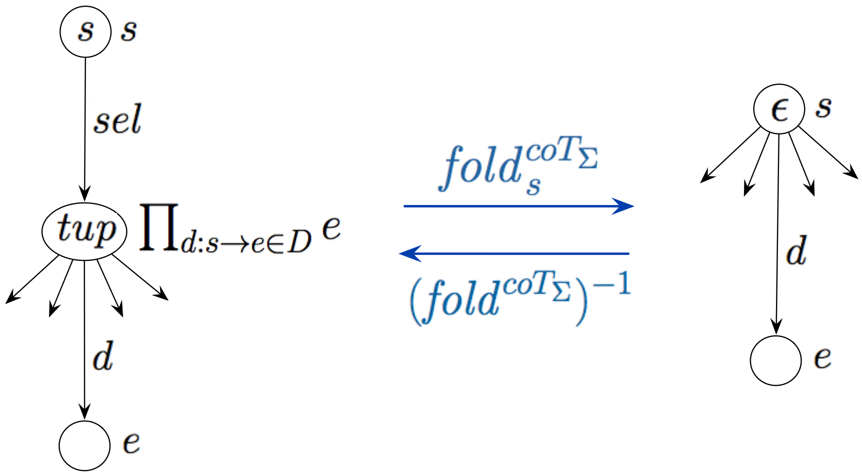


- For all $t_i \in coT_{\Sigma,e_i}$, $i \in I$, and $k \in I$, $\pi_k(tup\{i \to t_i \mid i \in I\}) =_{def} t_k$.
- For all $i \in I$ and $t \in coT_{\Sigma,e_i}$, $\iota_i(t) =_{def} i\{sel \to t\}$.

$T_{co\Sigma}$ and coT_Σ are $co\Sigma$-isomorphic. Equivalently,

$$fold^{coT_\Sigma} : T_{co\Sigma} \to coT_\Sigma$$

is bijective.



Iterative Σ-equations

Let $\Sigma = (S, \mathcal{I}, F)$ be a constructive or destructive signature and V be a finite S-sorted set. An S-sorted function

$$E : V \to T_\Sigma(V)$$

with $img(E) \cap V = \emptyset$ is called a **system of iterative Σ-equations**.

E is usually written as $\{x = E(x) \mid x \in V\}$.

Let Σ be constructive, $\mathcal{A} = (A, Op)$ be a Σ-algebra and A^V be the set of S-sorted functions from V to A.

$g \in A^V$ **solves** E **in** $\mathcal{A}$ if $g^* \circ E = g$.

E turns $T_\Sigma(V)$ into a *co*Σ-algebra: Let $s \in S$, $I \in \mathcal{I}$ and $\{e_i\} \subseteq \mathcal{T}(S, \mathcal{I})$.

- For all $x \in V_s$, $s^{T_\Sigma(V)}(x) =_{def} s^{T_\Sigma(V)}(E(x))$.
- For all $c : e \to s \in F$, $t \in T_\Sigma(V)_e$, $s^{T_\Sigma(V)}(c\{sel \to t\}) =_{def} c\{sel \to t\}$.
- For all $t_i \in T_\Sigma(V)_{e_i}$, $i \in I$, and $k \in I$, $\pi_k(tup\{i \to t_i \mid i \in I\}) =_{def} t_k$.
- For all $i \in I$ and $t \in T_\Sigma(V)_{e_i}$, $\iota_i(t) =_{def} i\{sel \to t\}$.

Theorem SOL

$$V \stackrel{inc_V}{\to} T_\Sigma(V) \stackrel{unfold^{T_\Sigma(V)}}{\to} DT_{co\Sigma} \stackrel{(unfold^{CT_\Sigma})^{-1}}{\to} CT_\Sigma$$

solves E in CT_Σ uniquely.

Proof. See Theorem SOL (coalgebraic version) in Fixpoints, Categories, and (Co)Algebraic Modeling. ❑

Example

Let $V = \{blink, blink'\}$. The following system of $List(\mathbb{Z})$-equations over V has a unique solution in $CT_{List(\mathbb{Z})}$ and thus defines two elements of $CT_{List(\mathbb{Z})}$:

$$\begin{aligned} blink &= cons\{sel \to tup\{1 \to 0, 2 \to blink'\}\}, \\ blink' &= cons\{sel \to tup\{1 \to 1, 2 \to blink\}\}. \end{aligned} \tag{1}$$

Infinite terms that are representable as unique solutions of iterative equations are called **rational**. A Σ-term is rational iff it has only finitely many subterms.

Let Σ be destructive and h be the bijection between $T_\Sigma(V)$ and $T_{co\Sigma}(V)$ that is the identity on V and agrees with $(fold^{coT_\Sigma})^{-1}$ on $T_\Sigma = coT_\Sigma$.

Corollary $h \circ E$ has a unique solution in DT_Σ.

Proof. DT_Σ is a $co\Sigma$-algebra: For all $s \in S$,

$$s^{DT_\Sigma}(\epsilon\{d \to t_d \mid d : s \to e \in F\}) \ =_{def} \ s\{sel \to tup\{d \to t_d \mid d : s \to e \in F\}\}.$$

By Theorem SOL, $h \circ E$ has a unique solution in $CT_{co\Sigma}$. Since $CT_{co\Sigma}$ is final in $Alg_{coco\Sigma}$, $CT_{co\Sigma}$ is $coco\Sigma$-isomorphic to $A =_{def} DT_{coco\Sigma}$. A is a Σ-algebra: For all $s \in S$ and $d : s \to e$ and $t_d \in A_e$, $d : s \to e \in F$,

$$d^A(\epsilon\{s \to s\{sel \to tup\{d \to t_d \mid d : s \to e \in F\}\}\}) \ =_{def} \ t_d.$$

$unfold^A : A \to DT_\Sigma$ is bijective: The inverse maps $\epsilon\{d \to t_d \mid d : s \to e \in F\} \in DT_\Sigma$ to

$$\epsilon\{s \to s\{sel \to tup\{d \to t_d \mid d : s \to e \in F\}\}\}.$$

Hence $CT_{co\Sigma} \cong A \cong DT_\Sigma$ and thus the solutions of $h \circ E$ in $CT_{co\Sigma}$ and DT_Σ, respectively, coincide up to isomorphism. ❏

Example

Let $V = \{esum, osum\}$. Given the following system E of $Acc(\mathbb{Z})$-equations over V, $h \circ E$ has a unique solution in $DT_{Acc(\mathbb{Z})}$ and thus defines two elements of $DT_{Acc(\mathbb{Z})}$:

$$\begin{aligned} esum &= \epsilon\{\delta \to tup(\{x \to esum \mid x \in even\} \cup \{x \to osum \mid x \in odd\}), \beta \to 1\}, \\ osum &= \epsilon\{\delta \to tup\{x \to osum \mid x \in even\} \cup \{x \to esum \mid x \in odd\}), \beta \to 0\}. \end{aligned} \tag{2}$$

Typed theories

Let $\Sigma = (S, \mathcal{I}, F)$ be a signature.

The set der_Σ of **derived Σ-operations** is inductively defined as follows:

Let $I \in \mathcal{I}$ and $\{e_i\} \subseteq \mathcal{T}(S, \mathcal{I})$.

- $F \subseteq der_\Sigma$.
- For all $e \in \mathcal{T}(S, \mathcal{I})$ and $i \in I$, $\bar{i} : e \to I \in der_\Sigma$.
- For all $f : e \to e',\ g : e' \to e'' \in der_\Sigma$, $g \circ f : e \to e'' \in der_\Sigma$.
- $\pi_i : \prod_{i \in I} e_i \to e_i,\ \ \iota_i : e_i \to \coprod_{i \in I} e_i \in der_\Sigma$ (also written as id if I is a singleton).
- For all $f_i : e \to e_i \in der_\Sigma$, $i \in I$, $\langle f_i \rangle : e \to \prod_{i \in I} e_i \in der_\Sigma$.
- For all $f_i : e_i \to e \in der_\Sigma$, $i \in I$, $[f_i] : \coprod_{i \in I} e_i \to e \in der_\Sigma$.
- **λ-abstraction**:
  For all $c_i : e_i \to e,\ \ f_i : e_i \to e' \in der_\Sigma$, $i \in I$, $\lambda\{c_i.f_i\}_{i \in I} : e \to e' \in der_\Sigma$.
- **κ-abstraction**:
  For all $d_i : e \to e_i,\ \ f_i : e' \to e_i \in der_\Sigma$, $i \in I$, $\kappa\{d_i.f_i\}_{i \in I} : e' \to e \in der_\Sigma$.

$Th(\Sigma) = (S, \mathcal{I}, der_\Sigma)$ is called the (algebraic) **Σ-theory**.

Let $\mathcal{A} = (A, Op)$ be a Σ-algebra.

The $Th(\Sigma)$-algebra $\mathcal{B} = Th(\mathcal{A})$ with $\mathcal{B}|_\Sigma = \mathcal{A}$ and the following interpretation of der_Σ is called the **theory of** $\mathcal{A}$.

Let $I \in \mathcal{I}$ and $\{e_i\} \subseteq \mathcal{T}(S, \mathcal{I})$.

- For all $e \in \mathcal{T}(S, \mathcal{I})$, $id^{\mathcal{B}} = id_A$.
- For all $e \in \mathcal{T}(S, \mathcal{I})$, $i \in I$ and $a \in A_e$, $\bar{i}^{\mathcal{B}} = \lambda x.i$.
- Compositions, projections, injections, product and coproduct extensions are defined as usually.
- For all $c_i : e_i \to e,\ f_i : e_i \to e' \in der_\Sigma$, $i \in I$, such that $\{c_i^{\mathcal{B}} \mid i \in I\}$ is a set of constructors for e, for all $k \in I$,

$$(\lambda\{c_i.f_i\}_{i\in I})^{\mathcal{B}} \circ c_k^{\mathcal{B}} \; = \; f_k^{\mathcal{B}}.$$

- For all $d_i : e \to e_i,\ f_i : e' \to e_i \in der_\Sigma$, $i \in I$, such that $\{d_i^{\mathcal{B}} \mid i \in I\}$ is a set of destructors for e, for all $k \in I$,

$$d_k^{\mathcal{B}} \circ (\kappa\{d_i.f_i\}_{i\in I})^{\mathcal{B}} \; = \; f_k^{\mathcal{B}}.$$

The following lemma implies that λ- and κ-abstractions are well-defined:

(1) Let $\{f_i : A_{e_i} \to A_e \mid i \in I\}$ be a set of constructors for e.
For all $a \in A_e$ there are unique $i \in I$ and $b \in A_{e_i}$ such that $f_i^A(b) = a$.

(2) Let $\{f_i : A_e \to A_{e_i} \mid i \in I\}$ be a set of destructors for e.
For all $a, b \in A_e$, $a = b$ if $f_i(a) = f_i(b)$ for all $i \in I$.

For ease of notation, $Th(\mathcal{A})$ may be regarded as the category with $\mathcal{T}(S,\mathcal{I})$ as the set of objects and the operations of $Th(\mathcal{A})$ as morphisms:

Every $Th(\mathcal{A})$-morphism $f : e \to e'$ denotes the interpretation of some derived Σ-operation in $\mathcal{A}$.

Example

Let $p : e \to 2$ and $f, g : e \to e'$ be $Th(\mathcal{A})$-morphisms. The conditional

$$\mathit{if}\ p\ \mathit{then}\ f\ \mathit{else}\ g : e \to e'$$

can be derived as follows:

$$\mathit{if}\ p\ \mathit{then}\ f\ \mathit{else}\ g \quad = \quad e \xrightarrow{\langle id,p\rangle} e \times 2 \xrightarrow{\lambda\{\langle id,\overline{1}\rangle.f,\langle id,\overline{0}\rangle.g\}} e'.$$

Recursive equations

$$factorial : \mathbb{N} \to \mathbb{N}$$

$$factorial \;=\; \lambda\{\overline{0}.\overline{1},\; (+1).(*) \circ \langle id, factorial \circ (-1)\rangle\}$$

$$factorial : \mathbb{N}^2 \to \mathbb{N}^2$$

$$factorial \;=\; [id,\; factorial \circ (x \leftarrow x - 1) \circ (y \leftarrow x * y)] \circ (x = 0) \qquad \text{or}$$

$$factorial \;=\; if\;\; x \equiv 0\; then\; id\; else\; factorial \circ (x \leftarrow x - 1) \circ (y \leftarrow x * y)$$

$$\text{where } (x = 0)(m, n) = if\;\; m = 0\; then\; \iota_1(m, n)\; else\; \iota_2(m, n)$$

$$(x \equiv 0)(m, n) = if\;\; m = 0\; then\; 1\; else\; 0$$

$$(x \leftarrow x - 1)(m, n) = (m - 1, n)$$

$$(y \leftarrow x * y)(m, n) = (m, m * n)$$

$$zip : X^{\mathbb{N}} \times X^{\mathbb{N}} \to X^{\mathbb{N}}$$

$$zip \;=\; \kappa\{head.head \circ \pi_1,\; tail.tail \circ zip \circ \langle \pi_2, tail \circ \pi_1\rangle\}$$

Where do such equations have unique solutions?