From fixpoint to predicate co/induction and its use in standard models

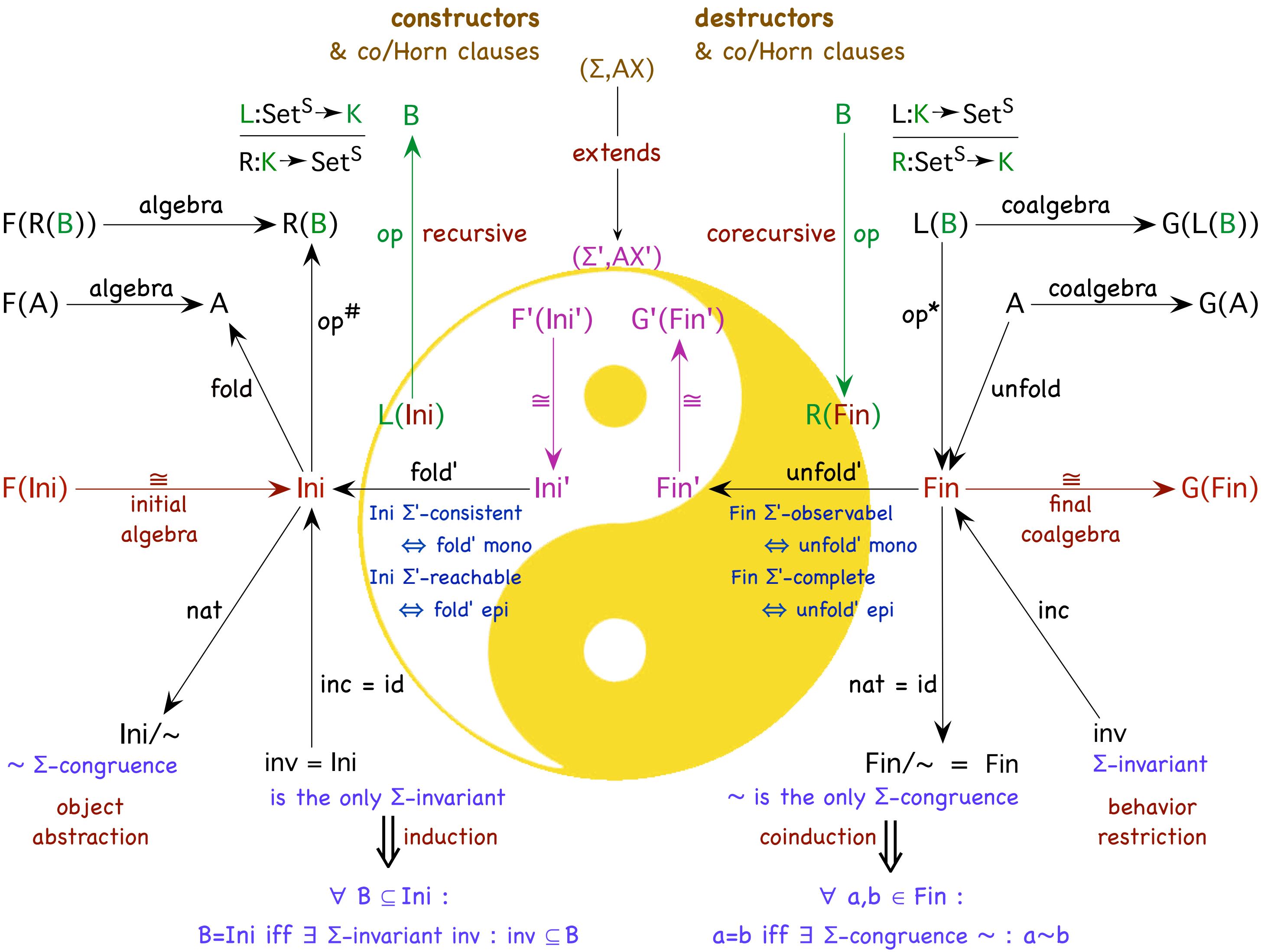
Peter Padawitz, TU Dortmund

September 1, 2017

More details in [2] and [3].

The big picture

Buy one, get one free!



Let A be a set and R be a binary relation on A.

R is a **partial order** and A is a **partially ordered set** or **poset** if R is reflexive, transitive and antisymmetric.

Let A be a poset with partial order $\leq$ and $\geq = \leq^{-1}$.

$B = \{a_i \mid i < \omega\} \subseteq A$ is an **ω-chain** of A if for all $i \in \mathbb{N}$, $a_i \leq a_{i+1}$.

$B = \{a_i \mid i < \omega\} \subseteq A$ is a **ω-cochain** of A if for all$i \in \mathbb{N}$, $a_i \geq a_{i+1}$.

A is **ω-complete** or an **ω-CPO** if A has a least element $\bot$ w.r.t. $\leq$ and for each ω-chain B of A, A contains the supremum $\sqcup B$ of B.

A is **ω-cocomplete** or a **ω-coCPO** if A has a greatest element $\top$ w.r.t. $\leq$ and for each ω-cochain B of A, A contains the infimum $\sqcap B$ of B.

Let A, B be posets.

$f : A \to B$ is **monotone** if for all $a, b \in A$, $a \leq b$ implies $f(a) \leq f(b)$.

Let A, B be λ-CPOs.

$f : A \to B$ is ω-**continuous** if for all ω-chains B of A,

$$f(\sqcup B) = \sqcup\{f(b) \mid b \in B\}.$$

$f : A \to B$ is ω-**cocontinuous** if for all ω-cochains B of A,

$$f(\sqcap B) = \sqcap\{f(b) \mid b \in B\}.$$

If f is ω-co/continuous, then f is monotone.

If f is monotone and all ω-co/chains of A are finite, then f is ω-co/continuous.

Kleene's Fixpoint Theorem [1] (also known as Kleene's first recursion theorem)

(1) Let A be an ω-CPO and $f : A \to A$ be ω-continuous.

$lfp(f) = \sqcup_{n\in\mathbb{N}} f^n(\bot)$ is the least fixpoint of f.

(2) Let A be an ω-coCPO and $f : A \to A$ be ω-cocontinuous.

$gfp(f) = \sqcap_{n\in\mathbb{N}} f^n(\top)$ is the greatest fixpoint of f.

A poset A is a **complete lattice** if each subset B of A has a supremum $\sqcup B$ and an infimum $\sqcap B$ in A.

$\bot = \sqcup\emptyset$ is the least element and $\top = \sqcap\emptyset$ is the greatest element of A.

Let A, B be complete lattices.

$f : A \to B$ is **continuous** if for all $C \subseteq A$, $f(\sqcup C) = \sqcup_{c\in C} f(c)$.

$f : A \to B$ is **cocontinuous** if for all $C \subseteq A$, $f(\sqcap C) = \sqcap_{c\in C} f(c)$.

If f is continuous or cocontinuous, then f is monotone.

Let A be a poset and $f : A \to A$.

$a \in A$ is **f-closed** if $f(a) \leq a$. a is **f-dense** if $a \leq F(a)$.

a is a **fixpoint** of f if $f(a) = a$.

Fixpoint Theorem of Knaster and Tarski [4]

Let A be a complete lattice and $f : A \to A$ be monotone.

(1) $\mathit{lfp}(f) = \sqcap\{a \in A \mid a \text{ is } f\text{-closed}\}$ is the least fixpoint of f.

(2) $\mathit{gfp}(f) = \sqcup\{a \in A \mid a \text{ is } f\text{-dense}\}$ is the greatest fixpoint of f.

Fixpoint induction

Let

(a) A be a complete lattice and $f : A \to A$ be monotone or
(b) A be an ω-CPO and f be ω-continuous.

(1) For all f-closed $a \in A$, $\mathit{lfp}(f) \leq a$.
(2) For all $a, b \in A$, if $b \leq a$ and b is f-closed, then $\mathit{lfp}(f) \leq a$.
(3) For all $n > 0$ and f^n-closed $a \in A$, $\mathit{lfp}(f) \leq a$.

Fixpoint coinduction

Let

(a) A be a complete lattice and $f : A \to A$ be monotone or
(b) A be an ω-coCPO and f be ω-cocontinuous.

(1) For all f-dense $a \in A$, $a \leq \mathit{gfp}(f)$.
(2) For all $a, b \in A$, if $a \leq b$ and b is f-dense, then $a \leq \mathit{gfp}(f)$.
(3) For all $n > 0$ and f^n-dense $a \in A$, $a \leq \mathit{gfp}(f)$.

Co-/Horn clauses, co/resolution and predicate co/induction

A **signature** $\Sigma = (S, BS, F, P)$ consists of

- a finite set S (of **sorts**),
- a finite set BS (of **base sets**),
- a (finite) set F of **function symbols** $f : e \to e'$,
- a (finite) set P of **predicates** $p : e$,

where e, e' are **types over** S **and** BS (products, sums, base sets, function spaces, etc.).

A Σ**-algebra** A consists of

- for each $s \in S$, a set A_s, the **carrier** of A,
- for each $f : e \to e' \in F$, a function $f^A : A_e \to A_{e'}$,
- for each $p : e \in P$, a subset p^A of A_e.

An S**-sorted function** $h : A \to B$ between Σ-algebras is a Σ**-homomorphism** if

- for all $f \in F$, $h_{e'} \circ f^A = f^B \circ h_e$,
- for all $p \in P$, $h_e(p^A) \subseteq p^B$.

Set^S denotes the category of S-sorted sets and S-sorted functions.
Alg_Σ denotes the category of Σ-algebras and Σ-homomorphisms.

For any type e over S, A_e is the image of the functor $F_e : Set^S \to Set$ that builds from A an interpretation of e.

For instance, $A_{s_1 \times \dots \times s_n} = A_{s_1} \times \ldots \times A_{s_n}$ and $A_{s_1 + \dots + s_n} = A_{s_1} + \cdots + A_{s_n}$.

$F_{e,\Sigma}$ denotes the restriction of F_e to Alg_Σ. For all $f : e \to e' \in F$, the interpretations f^A of f, $A \in Alg_\Sigma$, form a natural transformation from $F_{e,\Sigma}$ to $F_{e',\Sigma}$. Each natural transformations from $F_{e,\Sigma}$ to $F_{e',\Sigma}$ is called a **Σ-term** of type $e \to e'$.

Σ-formulas built up on P and Σ-terms are usual predicate-logic formulas. As function symbols are terms, so predicates are formulas. Every formula φ has a type that denotes the domain of its solutions: Given a Σ-algebra A, the interpretation φ^A of $\varphi : e$ in A is a subset of A_e.

If $\varphi : e$ has variables from a set V, e is supposed to be of the form $\prod_{x \in V} e_x$, i.e., variables are indices of a product. Accordingly, variable occurrences in φ stand for the respective projections.

Let Σ be a subsignature of a signature Σ' and A be a Σ'-algebra.

The **Σ-reduct** $A|_\Sigma$ **of** A is the Σ-algebra defined as follows:

- For all $s \in S$, $(A|_\Sigma)_s = A_s$.
- For all $f \in F \cup P$, $f^{A|_\Sigma} = f^A$.

Let $\Sigma = (S, BS, F, P)$ and $\Sigma' = (S, BS, F, P \uplus P')$ be signatures and C be a Σ-algebra.

$Alg_{\Sigma',C}$ denotes the category of all Σ'-algebras A with $A|_\Sigma = C$.

$Alg_{\Sigma',C}$ is a complete lattice:

For all $A, B \in Alg_{\Sigma',C}$,

$$A \leq B \iff \forall\, p \in P : p^A \subseteq p^B.$$

For all $\mathcal{A} \subseteq Alg_{\Sigma',C}$ and $p : e \in P$,

$$p^\perp = \emptyset, \quad p^\top = A_e, \quad p^{\sqcup\mathcal{A}} = \bigcup_{A\in\mathcal{A}} p^A \;\text{ and }\; p^{\sqcap\mathcal{A}} = \bigcap_{A\in\mathcal{A}} p^A.$$

Given a set AX of Σ'-formulas, $Alg_{\Sigma',AX}$ denotes the category of all Σ-algebras A that satisfy AX.

$Alg_{\Sigma',C,AX} = Alg_{\Sigma',AX} \cap Alg_{\Sigma',C}$.

A **Horn clause for** $p \in P'$ is a Σ'-formula of the form $pt \Leftarrow \varphi$ such that $\vee$, $\wedge$ and $\forall$ are the only logical operators of φ.

A **co-Horn clause for** $p \in P'$ is a Σ'-formulas of the form $pt \Rightarrow \varphi$ such that $\vee$, $\wedge$ and $\exists$ are the only logical operators of φ.

Let $A, B \in Alg_{\Sigma',C}$ and $pt \Leftarrow \varphi$ resp. $pt \Rightarrow \varphi$ be a Horn resp. co-Horn clause. Since φ is negation-free,

$$A \leq B \quad \text{implies} \quad \varphi^A \subseteq \varphi^B. \tag{3}$$

A Σ'-formula φ is **finitely branching** if for all $A \in Alg_{\Sigma',C}$ and subformulas $\exists x(\psi : e)$ or $\forall x(\psi : e)$ of φ and $a \in A_e$, the set $\{b \mid a[b/x] \in \psi^A\}$ is finite.

If φ is negation-free and finitely branching, then for all ω-chains $\{A_i \in Alg_{\Sigma',C} \mid i < \omega\}$ and ω-cochains $\{A_i \in Alg_{\Sigma',C} \mid i < \omega\}$ of $Alg_{\Sigma',C}$,

$$\varphi^{\sqcup_{i\in\mathbb{N}} A_i} \subseteq \bigcup_{i\in\mathbb{N}} \varphi^{A_i} \quad \text{and} \quad \bigcap_{i\in\mathbb{N}} \varphi^{A_i} \subseteq \varphi^{\sqcap_{i\in\mathbb{N}} A_i}.$$

For all $p \in P'$, let AX_p be a set of Horn clauses for p. Then $AX = \cup_{p\in P'} AX_p$ is a **Horn specification for** P' and the elements of P' are called **least predicates**.

The **step function** $\Phi = \Phi_{\Sigma',C,AX} : Alg_{\Sigma',C} \to Alg_{\Sigma',C}$ is defined as follows: For all $A \in Alg_{\Sigma',C}$ and $p : e \in P'$,

$$p^{\Phi(A)} \;=\; \{t^C(a) \mid pt \Leftarrow \varphi \in AX,\; a \in \varphi^A\}.$$

By (3), Φ is monotone and thus by the Fixpoint Theorem of Knaster and Tarski, Φ has the least fixpoint

$$lfp(\Phi) \;=\; \sqcap\{A \in Alg_{\Sigma',C} \mid \Phi(A) \leq A\}.$$

Moreover,

$$Alg_{\Sigma',C,AX} = \{A \in Alg_{\Sigma',C} \mid \Phi(A) \leq A\}. \tag{4}$$

Proof. Let $A \in Alg_{\Sigma',C,AX}$ and $b \in p^{\Phi(A)}$. Then $b = t^A(a)$ for some $pt \Leftarrow \varphi \in AX$ and $a \in \varphi^A$. Since A satisfies $pt \Leftarrow \varphi$, $a \in (pt)^A$ and thus $b = t^C(a) \in p^A$. Hence A is Φ-closed.

Conversely, let A be Φ-closed, $pt \Leftarrow \varphi \in AX$ and $a \in \varphi^A$. Then $t^C(a) \in p^{\Phi(A)}$. Since A is Φ-closed, $t^C(a) \in p^A$ and thus $a \in (pt)^A$. Hence A satisfies $pt \Leftarrow \varphi$. ❏

Hence for all $A \in Alg_{\Sigma',C,AX}$,

$$lfp(\Phi) \leq A. \tag{5}$$

If the premises of all Horn clauses of AX are finitely branching, then Φ is ω-continuous.

For all $p \in P'$, let AX_p be a set of co-Horn clauses for p. Then $AX = \cup_{p \in P'} AX_p$ is a **co-Horn specification for** P' and the elements of P' are called **greatest predicates**.

The **step function** $\Phi = \Phi_{\Sigma',C,AX} : Alg_{\Sigma',C} \to Alg_{\Sigma',C}$ is defined as follows: For all $A \in Alg_{\Sigma',C}$ and $p : e \in P'$,

$$p^{\Phi(A)} = C_e \setminus \{t^C(a) \mid pt \Rightarrow \varphi : e' \in AX,\ a \in C_{e'} \setminus \varphi^A\}.$$

By (3), Φ is monotone and thus by the Fixpoint Theorem of Knaster and Tarski, Φ has the greatest fixpoint

$$gfp(\Phi) \;=\; \sqcup\{A \in Alg_{\Sigma',C} \mid A \leq \Phi(A)\}.$$

Moreover,

$$Alg_{\Sigma',C,AX} = \{A \in Alg_{\Sigma',C} \mid A \leq \Phi(A)\}. \tag{6}$$

Proof. Let $A \in Alg_{\Sigma',C,AX}$ and $b \not\in p^{\Phi(A)}$. Then $b = t^C(a)$ for some $pt \Rightarrow \varphi \in AX$ and $a \not\in \varphi^A$. Since A satisfies $pt \Rightarrow \varphi$, $a \not\in (pt)^A$ and thus $b = t^C(a) \not\in p^A$. Hence A is Φ-dense.

Conversely, let A be Φ-dense, $pt \Rightarrow \varphi \in AX$ and $a \not\in \varphi^A$. Then $t^C(a) \not\in p^{\Phi(A)}$. Since A is Φ-dense, $t^C(a) \not\in p^A$ and thus $a \not\in (pt)^A$. Hence A satisfies $pt \Rightarrow \varphi$. ❑

Hence for all $A \in Alg_{\Sigma',C,AX}$,

$$A \leq gfp(\Phi). \tag{7}$$

If the conclusions of all co-Horn clauses of AX are finitely branching, then Φ is ω-cocontinuous.

Computation and proof in $lfp(\Phi)$ resp. $gfp(\Phi)$

- **Resolution** Let p be a least predicate. AX_p is applied to an atom pt:

$$\frac{pt}{\bigvee_{i=1}^{k} \exists Z_i : (\varphi_i\sigma_i \wedge \vec{x} = \vec{x}\sigma_i)} \Updownarrow$$

where $AX_p = \{pt_1 \Leftarrow \varphi_1, \ldots, pt_n \Leftarrow \varphi_n\}$,

$(*)$ $\vec{x}$ is a list of the variables of t,
for all $1 \leq i \leq k$, $t\sigma_i = t_i\sigma_i$ and $Z_i = var(t_i, \varphi_i)$,
for all $k < i \leq n$, t is not unifiable with t_i.

- **Coresolution** Let p be a greatest predicate. AX_p is applied to an atom pt:

$$\frac{pt}{\bigwedge_{i=1}^{k} \forall Z_i : (\varphi_i\sigma_i \vee \vec{x} \neq \vec{x}\sigma_i)} \Updownarrow$$

where $AX_p = \{pt_1 \Rightarrow \varphi_1, \ldots, pt_n \Rightarrow \varphi_n\}$ and $(*)$ holds true.

Let $p : e$ be a least predicate of P' and $\psi_p : e$ be a Σ-formula that shall be proved to follow from p.

- **Predicate induction** A goal $p \Rightarrow \psi_p$ is applied to AX_p:

$$\frac{p \Rightarrow \psi_p}{\bigwedge_{pt \Leftarrow \varphi \in AX}(\varphi[\psi_p/p \mid p \in P'] \Rightarrow \psi_p t)} \;\Uparrow\; by\ (5)$$

Let $p : e$ be a greatest predicate of P' and $\psi_p : e$ be a Σ-formula that shall be proved to imply p.

- **Predicate coinduction** A goal $\psi_p \Rightarrow p$ is applied to AX_p:

$$\frac{\psi_p \Rightarrow p}{\bigwedge_{pt \Rightarrow \varphi \in AX}(\psi_p t \Rightarrow \varphi[\psi_p/p \mid p \in P'])} \;\Uparrow\; by\ (7)$$

Incremental versions

Let $p : e$ be a least predicate of P' and $\psi_p : e$ be a Σ-formula that shall be proved to follow from p.

- **Predicate induction**

$$(1) \qquad \frac{p \Rightarrow \psi_p}{\bigwedge_{pt \Leftarrow \varphi \in AX}(\varphi[q_p/p \mid p \in P'] \Rightarrow \psi_p t)} \qquad q_p \Rightarrow \psi_p \textit{ is added to } AX$$

$$(2) \qquad \frac{q_p \Rightarrow \delta_p}{\bigwedge_{pt \Leftarrow \varphi \in AX}(\varphi[q_p/p \mid p \in P'] \Rightarrow \delta_p t)} \qquad q_p \Rightarrow \delta_p \textit{ is added to } AX$$

The proof starts by adding to P a predicate q_p, first for ψ_p and – when the second rule is applied – for a generalization $\psi_p \wedge \delta_p$ of ψ_p.

Between the applications of (1) resp. (2), coresolution steps upon the added axiom $q_p \Rightarrow \psi_p$ must be confined to redex positions with negative polarity, i.e., the number of preceding negation symbols in the entire formula must be odd. Otherwise the axiom added when (2) is applied might violate the soundness of the coresolution steps.

Coresolution upon q_p at any redex position becomes sound as soon as the set of axioms for q_p is not extended any more.

By inferring *True* from the conclusions of (1) and (2) one shows, roughly speaking, that the predicate $\psi_p \wedge \delta_p$ solves the axioms for p. Since p itself represents the least solution, we conclude $p \Rightarrow \psi_p \wedge \delta_p$, in particular the original goal $p \Rightarrow \psi_p$.

Let $p : e$ be a greatest predicate of P' and $\psi_p : e$ be a Σ-formula that shall be proved to imply p.

- **Predicate coinduction**

(1) $$\frac{\psi_p \Rightarrow p}{\bigwedge_{pt\Rightarrow\varphi\in AX}(\psi_p t \Rightarrow \varphi[q_p/p \mid p \in P'])}$$

$q_p \Leftarrow \psi_p$ and – only if p denotes a congruence relation – equivalence axioms for q_p are added to AX

(2) $$\frac{\delta_p \Rightarrow q_p}{\bigwedge_{pt\Rightarrow\varphi\in AX}(\delta_p t \Rightarrow \varphi[q_p/p \mid p \in P'])}$$

$q_p \Leftarrow \delta_p$ is added to AX

The proof starts by adding to P a predicate q_p, first for ψ_p and – when the second rule is applied – for a generalization $\psi_p \vee \delta_p$ of ψ_p.

Between the applications of (1) resp. (2), resolution steps upon the added axiom $q_p \Leftarrow \psi_p$ must be confined to redex positions with positive polarity, i.e., the number of preceding negation symbols in the entire formula must be even. Otherwise the axiom added when (2) is applied might violate the soundness of the resolution steps.

Resolution upon q_p at any redex position becomes sound as soon as the set of axioms for q_p is not extended any more.

By inferring *True* from the conclusions of (1) and (2) one shows, roughly speaking, that the predicate $\psi_p \vee \delta_p$ (or its equivalence closure if p denotes a congruence relation) solves the axioms for p. Since p itself represents the greatest solution, we conclude $\psi_p \vee \delta_p \Rightarrow p$, in particular the original goal $\psi_p \Rightarrow p$.

Examples

$$
\begin{array}{lcll}
AX_q & = & \{q(0),\ q(1)\} & \text{What is } q^{lfp(\Phi)}? \\
AX_{NOTr} & = & \{NOTr(suc(suc(x)))\} & \text{What is } NOTr^{lfp(\Phi)}? \\
AX_r & = & \{q(suc(suc(x))) \Rightarrow False\} & \text{What is } q^{gfp(\Phi)}? \\
AX_{NOTq} & = & \{NOTq(0) \Rightarrow False,\ NOTq(1) \Rightarrow False\} & \text{What is } NOTq^{gfp(\Phi)}?
\end{array}
$$

```
q$0                        --> True                       -- resolution
q$suc$suc$x ==> False      --> True                       -- induction
NOTq(0)                    --> False                      -- coresolution
NOTq(suc(suc(x)))          --> True                       -- coinduction

r$0                        --> True                       -- coinduction
r$suc$suc$x ==> False      --> True                       -- coresolution
NOTr(0) ==> False          --> True                       -- induction
NOTr(suc(suc(x)))          --> True                       -- resolution
```

```
q$x                     --> x = 0 | x = 1               -- resolution
q$!x ==> False          --> !x =/= 0 & !x =/= 1         -- induction
NOTq(x) ==> False       --> x = 0 | x = 1               -- coresolution
NOTq(!x)                --> !x =/= 0 & !x =/= 1         -- coinduction

r$!x                    --> All y: !x =/= suc(suc(y)) -- coinduction
r$x ==> False           --> Any y: x = suc(suc(y))    -- coresolution
NOTr(!x) ==> False      --> All y: !x =/= suc(suc(y)) -- induction
NOTr(x)                 --> Any y: x = suc(suc(y))    -- resolution
```

```
   F(P)$s <=== P$s | F(P)$tail$s                         -- finally
   G(P)$s ===> P$s & G(P)$tail$s                         -- generally
   NatStream(x:s) ===> Nat(x) & NatStream(s)
   s ~ s' ===> head(s) = head(s') & tail(s) ~ tail(s')
                                                         -- stream equality
-- simplifications
   head$blink == 0
   tail$blink == 1:blink
   head$x:s == x
   tail$x:s == s
   head(zip(s,s')) == head(s)
   tail(zip(s,s')) == zip(s',tail(s))
   head(evens(s)) == head(s)
   tail(evens(s)) == evens(tail(tail(s)))
   odds == evens.tail
   blink = 1:blink <==> False
   not(F(P)) <==> G(not(P))
   not(G(P)) <==> F(not(P))
```

```
conjectures:

   G(F$(=0).head)(blink)           --> True
   Not(G(F$(=0).head)(blink))      --> True
   G(F$(=2).head)(blink)           --> False
   Not(G(F$(=2).head)(blink))      --> True
   G(F$(=!x).head)(blink)          --> !x=0 | !x=1
   G(F$(=0).head)(mu s.(0:1:s))    --> True

   NatStream(mu s.(1:2:3:s))       --> True
   NatStream(1:2:3:!s)             --> !s = (3:!s) | !s = (2:(3:!s)) |
                                       !s = (1:(2:(3:!s)))

   blink ~ zip(zero,one)           --> True
   evens$x:s ~ x:odds$s            --> True
   evens$zip(s,s') ~ s             --> True
   odds$zip(s,s') ~ s'             --> True
   zip(evens$s,odds$s) ~ s         --> True
```

Co/induction in standard models

Let $\Sigma = (S, BS, F, P)$ be a signature.

Σ is **constructive** if all $f : e \to e'$ are **constructors**, i.e., $e' \in S$.

Σ is **destructive** if all $f : e \to e'$ are **destructors**, i.e., $e \in S$.

Three examples Let X and Y be sets, Z be a finite set and CS be a finite set of sets.

- $DAut(X, Y)$ ⧟ deterministic Moore automata

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

$Stream(Y) = DAut(1, Y)$. Acceptors of $L \subseteq X^*$ are $DAut(X, 2)$-algebras.

- $Reg(Z, CS)$ ⧟ regular operators

$$\begin{array}{lcl} S & = & \{ \ reg \ \}, \\ BS & = & \{ \ Z \ \} \cup CS, \\ F & = & \{ \ \emptyset, \ \epsilon : 1 \to reg, \quad \_ : Z \to reg, \quad star : reg \to reg, \\ & & \quad \_|\_, \ \_ \cdot \_ : reg \times reg \to reg \ \} \cup \\ & & \{ \ C : 1 \to reg \mid C \in CS \ \}. \end{array}$$

- $\Sigma(G)$ ⇝ abstract syntax of a context-free grammar $G = (S, BS, Z, R)$ with nonterminals S, base sets BS, terminals Z and rules $R \subseteq S \times (S \cup BS \cup Z)^*$

$$F = \{f_r : e_1 \times \cdots \times e_n \to s \mid \begin{array}{l} r = (s, w_0 e_1 w_1 \dots e_n w_n) \in R, \\ w_0, \dots, w_n \in Z^*,\ e_1, \dots, e_n \in S \cup BS \end{array} \}$$

Under certain (weak) conditions on the types used in Σ,

- Alg_Σ has an initial object if Σ is constructive,
- Alg_Σ has a final object if Σ is destructive.

A Σ-algebra A is **initial** in a full subcategory $\mathcal{K}$ of Alg_Σ if for all $B \in \mathcal{K}$ there is exactly one Σ-homomorphism $fold^B : A \to B$.

A Σ-algebra A is **final** in a full subcategory $\mathcal{K}$ of Alg_Σ if for all $B \in \mathcal{K}$ there is exactly one Σ-homomorphism $unfold^B : B \to A$.

Initial and final Σ-algebras are unique up to isomorphism.

The initial resp. final Σ-algebra is denoted by $\mu\Sigma$ resp. $\nu\Sigma$.

Let $\Sigma = (S, BS, F, P)$ be constructive and $s \in S$. All s-constructors can be combined into a single one with domain $e = \coprod_{f:e_f \to s \in F} e_f$.

$\mu\Sigma$ is a fixpoint of F_e: $\mu\Sigma \cong F_e(\mu\Sigma)$.

Given a signature $\Sigma' = (S, BS, F, P \uplus P')$ and a Horn specification AX, $lfp(\Phi_{\Sigma',\mu\Sigma,AX})$ is initial in $Alg_{\Sigma',C,AX}$.

Let $\Sigma = (S, BS, F, P)$ be destructive and $s \in S$. All s-destructors can be combined into a single one with range $e = \prod_{f:s \to e_f \in F} e_f$.

$\nu\Sigma$ is a fixpoint of F_e: $\nu\Sigma \cong F_e(\nu\Sigma)$.

Given a signature $\Sigma' = (S, BS, F, P \uplus P')$ and a co-Horn specification AX, $gfp(\Phi_{\Sigma',\nu\Sigma,AX})$ is final in $Alg_{\Sigma',C,AX}$.

Examples

- The set $T_{Reg(Z,CS)}$ of regular expressions over X together with the *free* interpretation of the regular operators is initial in $Alg_{Reg(Z,CS)}$.

- Let $Z_{CS} = Z \cup \bigcup CS$.
  The set $Lang(Z, CS) = \mathcal{P}(Z_{CS}^*)$ of languages over Z and CS together with the following interpretation of δ and β is final in $Alg_{DAut(Z_{CS},2)}$:
  For all $L \subseteq Z_{CS}^*$ and $x \in Z_{CS}$,

$$\delta^{Lang}(L)(x) = \{w \in Z'^* \mid xw \in L\}, \qquad \beta^{Lang}(L) = 1 \Leftrightarrow \epsilon \in L.$$

- $T = T_{Reg(Z,CS)}$ is also a $DAut(Z',2)$-algebra: For all $x, y \in X$ und $t, t' \in T$,

$$
\begin{array}{lcl}
\delta^T(\epsilon)(x) & = & \emptyset, \\
\delta^T(\emptyset)(x) & = & \emptyset, \\
\delta^T(x,y) & = & \begin{cases} \epsilon & \mathit{if} \ \ x = y, \\ \emptyset & \mathit{if} \ \ x \neq y, \end{cases} \\
\delta^T(t|t')(x) & = & \delta^T(t)(x) \mid \delta^T(t')(x), \\
\delta^T(t \cdot t')(x) & = & \begin{cases} \delta^T(t)(x) \cdot t' | \delta^T(t')(x) & \mathit{if} \ \ \beta^T(t) = 1, \\ \delta^T(t)(x) \cdot t' & \mathit{if} \ \ \beta^T(t) = 0, \end{cases} \\
\delta^T(star(t))(x) & = & \delta^T(t)(x) \cdot star(t), \\
\beta^T(\epsilon) & = & 1, \\
\beta^T(\emptyset) & = & 0, \\
\beta^T(x) & = & 0, \\
\beta^T(t|t') & = & \beta^T(t) + \beta^T(t'), \\
\beta^T(t \cdot t') & = & \beta^T(t) * \beta^T(t'), \\
\beta^T(star(t)) & = & 1.
\end{array}
$$

$\delta^T(t)(x)$ is called the x-**derivative** of t.

- $Lang(Z,CS)$ is also a $Reg(Z,CS)$-algebra (the usual semantics of regular expressions). Hence there is a unique $Reg(Z,CS)$-homomorphism

$$fold^{Lang} : T_{Reg(Z,CS)} \to Lang(Z,CS).$$

$fold^{Lang}$ is also $DAut(Z',2)$-homomorphic.
This makes $T_{Reg(Z,CS)}$ into a parser for regular expressions: For all $w = x_1 \dots x_n \in Z^*_{CS}$,

$$parse(t,w) =_{def} \beta^T(\delta^T(\dots\delta^T(t)(x_1)\dots)(x_n)) = 1 \iff w \in fold^{Lang}(t).$$

- Let $G = (S, BS, Z, R)$ be a context-free grammar. The set $T_{\Sigma(G)}$ of ground $\Sigma(G)$-terms together with the free interpretation of all f_r, $r \in R$, is initial in $Alg_{Reg(Z,BS)}$.
The $\Sigma(G)$-algebra $Word(G)$ is defined as follows:
For all $s \in N$,$r = (s, w_0s_1w_1 \dots s_nw_n) \in R$ and $v_1, \dots, v_n \in Z^*_{BS}$,

$$\begin{array}{lcl} Word(G)_s & = & Z^*_{BS}, \\ f_r^{Word(G)}(v_1,\dots,v_n) & = & w_0v_1w_1\dots v_nw_n. \end{array}$$

The **language of** G, $L(G)$, is the image algebra $fold^{Word(G)}(T_{\Sigma(G)})$.

Let A be a Σ-algebra.

An S-sorted binary relation $\sim$ on A is a **Σ-congruence** if for all $f : e \to e' \in F$ and $a, b \in A_e$,

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

$$\Delta_{\nu\Sigma} = \{(a,a) \mid a \in \nu\Sigma\} \text{ is the only (and thus the greatest) } \Sigma\text{-congruence on } \nu\Sigma. \qquad (1)$$

Hence $\nu\Sigma$ has no proper Σ-quotients.

Coinduction for proving equality

Let $P' = \{\sim_s : s \times s \mid s \in S\}$, $\Sigma' = (S, F, P \uplus P')$,

$$AX \;=\; \{x \sim_e y \Rightarrow fx \sim_{e'} fy \mid f : e \to e' \in F\},$$

R be an S-sorted binary relation on $\nu\Sigma$ and ψ be an S-sorted set of Σ-formulas such that for all $s \in S$, $\psi_s^{\nu\Sigma} = R_s$. By (1),

$$\begin{array}{rcl} R \subseteq \Delta_{\nu\Sigma} & \iff & \text{the greatest } \Sigma\text{-congruence} \sim \text{contains } R \\ & \Longleftarrow & \text{the succedent of predicate coinduction is valid} \\ & & \text{for } P',\ AX \text{ and } \psi \text{ defined as above.} \end{array}$$

An S-sorted subset inv of A is a **Σ-invariant** or **Σ-subalgebra** of A if for all $f : e \to e' \in F$ and $a \in A_e$,

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

$\mu\Sigma$ is the only (and thus the least) Σ-invariant of $\mu\Sigma$. (2)

Hence $\mu\Sigma$ has no proper Σ-subalgebras.

Induction for proving membership

Let $P' = \{inv_s : s \mid s \in S\}$, $\Sigma' = (S, F, P \uplus P')$,

$$AX \;=\; \{inv_{e'}(fx) \Leftarrow inv_e(x) \mid f : e \to e' \in F\},$$

R be an S-sorted subset of $\mu\Sigma$ and ψ be an S-sorted set of Σ-formulas such that for all $s \in S$, $\psi_s^{\mu\Sigma} = R_s$. By (2),

$$\begin{array}{rcl} R = \mu\Sigma & \Longleftrightarrow & R \text{ contains the least } \Sigma\text{-invariant of } \mu\Sigma \\ & \Longleftarrow & \text{the succedent of predicate induction is valid} \\ & & \text{for } P',\ AX \text{ and } \psi \text{ defined as above.} \end{array}$$

Examples

Induction: A partial function $f : T_{Reg(Z,CS)} \to A$ is total iff the domain of f contains a $Reg(X)$-invariant of $T_{Reg(Z,CS)}$ iff f is defined inductively.

Coinduction: $L = L' \in Z^*_{CS}$ iff some $DAut(Z_{CS}, 2)$-congruence on $Lang(Z, CS)$ contains (L, L').

Further impacts of initiality and finality

- A function f in an initial model is defined in terms of equations, which express that its extension f^* – with respect to an appropriate adjunction – is a fold (unique homomorphism from the initial model).

- A function f in a final model is defined in terms of equations, which express that its extension $f^\#$ – with respect to an appropriate adjunction – is an unfold (unique homomorphism to the final model).

- Each constructive signature Σ induces a destructive signature $co\Sigma$ such that **recursive** (also called guarded or iterative) **Σ-equations** have unique solutions in the final $co\Sigma$-algebra (whose carriers consist of all finite or infinite Σ-terms).

- Each context-free grammar $G=(S,BS,Z,R)$ induces a set of recursive $Reg(Z,BS)$-equations with variables from S, given as a function $E(G):S\to T_{Reg(Z,BS)}(S)$: For all $s\in S$,
$$E(G)(s)=\sum\{w\mid (s,w)\in R\}.$$
Given a $Reg(Z,BS)$-algebra A, a **solution** of $E(G)$ in A is a function $f:S\to A$ such that $f=f^*\circ E$.
$L(G)$ is the least solution of $E(G)$ in $Lang(Z,CS)$.
Suppose that the interpretations of δ^T and β^T in $T_{Reg(Z,BS)}$ can be extended to interpretations in $T_{Reg(Z,BS)}(S)$ – and thus *parse* to a parser for G – such that for all $s\in S$,
$$\delta^T(s)=\delta^T(E(G)(s))\ \text{ and }\ \beta^T(s)=\beta^T(E(G)(s)).$$
(We conjecture that this is possible if and only if G is not left-recursive.)
Then all solutions of $E(G)$ in $Lang(Z,BS)$ coincide.

References

[1] S.C. Kleene, *Introduction to Metamathematics*, Van Nostrand 1952

[2] P. Padawitz, *(Co)Algebraic Modeling and Reasoning*, slides, TU Dortmund 2014, fldit-www.cs.tu-dortmund.de/∼peter/DialgSlides.pdf

[3] P. Padawitz, *From grammars and automata to algebras and coalgebras*, Proc. CAI 2011, Springer LNCS 6742 (2011) 21-43, revised version: fldit-www.cs.tu-dortmund.de/∼peter/CAI.pdf

[4] A. Tarski, *A lattice-theoretical fixpoint theorem and its applications*, Pacific J. Math. 5 (1955), 285-309