

# Parametrized coinduction for logics

CALCO 2017

Ljubljana

David Sprunger\* and Lawrence Moss

Indiana University

April 12, 2018

# Overview

- Previous work (CMCS '16)
  - Logic for behavioral equivalence for finitary set functors
  - Sound and complete for weak pullback preserving functors
  - Add coinduction hypotheses only once
- Improvements
  - Precongruences: drop weak pullback preservation
  - Parametrized coinduction: add hypotheses on the fly
- Future extensions
  - Other coinductive predicates
  - Higher order schemes
  - Dualization to least fixed points

## Signature functors and finitary functors

### Definition

Let  $\Sigma$ ,  $ar : \Sigma \rightarrow \omega$  be a signature. The *signature functor*  $H_\Sigma$  is:

$$H_\Sigma X = \coprod_{n \in \omega} \Sigma_n \times X^n$$

### Definition

In a category  $\mathcal{A}$  with filtered colimits, a functor  $F : \mathcal{A} \rightarrow \mathcal{B}$  is *finitary* if it preserves filtered colimits.

When  $\mathcal{A} = \mathcal{B} = \text{Set}$  we start from the equivalent formulation:

### Theorem (Adámek, Gumm, and Trnková)

$F : \text{Set} \rightarrow \text{Set}$  is finitary if and only if  $F$  has a presentation as a quotient of  $H_\Sigma$  by an epic nat'l transformation  $\epsilon : H_\Sigma \rightarrow F$ .

We denote  $\ker(\epsilon_X)$  by  $=_\epsilon$ .

## What is finitary but does not preserve weak pullbacks?

Our running example will be  $\mathcal{W} \triangleq \mathbb{K} \times \mathbb{K}_\omega^{(-)}$  where  $\mathbb{K}$  is a ring.

$\mathbb{K}_\omega^X$  is the set of functions  $f : X \rightarrow \mathbb{K}$  with finite support.

If  $\varphi : X \rightarrow Y$ , then  $\mathbb{K}_\omega^\varphi : f \mapsto \lambda y. \sum_{x:\varphi(x)=y} f(x)$ .

One presentation for  $\mathcal{W}$  is:

$$\Sigma = \{\ell \in \mathbb{K}^* : |\ell| > 0\} \quad ar((k_0, k_1, \dots, k_n)) = n$$

with the natural transformation:

$$\epsilon_X : (k_0, k_1, \dots, k_n)(x_1, \dots, x_n) \mapsto \left( k_0, \lambda x. \sum_{i:x=x_i} k_i \right)$$

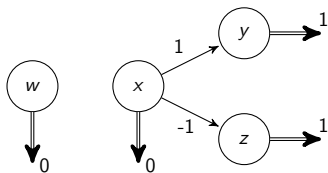
The  $=_\epsilon$  relation includes:

$$(k_0, k_1, k_2)(x, y) =_\epsilon (k_0, k_2, k_1)(y, x) \quad (\text{reorder})$$

$$(k_0, k_1, k_2)(x, x) =_\epsilon (k_0, k_1 + k_2)(x) \quad (\text{summing multiply represented})$$

$$(k_0, k_1, 0)(x, y) =_\epsilon (k_0, k_1)(x) \quad (\text{dropping weight 0})$$

## Example $\mathcal{W}$ -coalgebra: I (from Bonchi et al.)



As an  $H_\Sigma$ -coalgebra  $X \xrightarrow{d} H_\Sigma X$ ,

$$d(w) = (0) \quad d(x) = (0, 1, -1)(y, z) \quad d(y) = (1) \quad d(z) = (1)$$

*Key fact.*  $w$  and  $x$  are not bisimilar, but are behaviorally equivalent.

Previous work

## Logic (CMCS '16)

Let  $(X, d : X \rightarrow H_{\Sigma}X)$ ,  $(x, y) \in X$ , and  $(\sigma, \tau) \in H_{\Sigma}X$ .

Formulas are pairs of variables or pairs of flat terms.  $(\alpha = \beta)$

Sequents are a relation on  $X$  together with a formula.

$$\frac{R \vdash \alpha = \beta \quad \forall (x, y) \in R, R \vdash d(x) = d(y)}{\vdash \alpha = \beta} \quad b$$

$$\frac{(\sigma =_{\epsilon} \tau)}{R \vdash \sigma = \tau} \quad \epsilon$$

$$\frac{}{R \vdash \alpha = \alpha} \quad r$$

$$\frac{}{R \cup \{(x, y)\} \vdash x = y} \quad a$$

$$\frac{R \vdash \beta = \alpha}{R \vdash \alpha = \beta} \quad s$$

$$\frac{R \vdash x_1 = y_1 \cdots R \vdash x_n = y_n}{R \vdash f(x_1, \dots, x_n) = f(y_1, \dots, y_n)} \quad c$$

$$\frac{R \vdash \alpha = \beta \quad R \vdash \beta = \gamma}{R \vdash \alpha = \gamma} \quad t$$

## Soundness and completeness

### Theorem (S, 2016)

Let  $(X, d)$  be an  $H_\Sigma$ -coalgebra,  $x, y \in X$ , and  $F$  a finitary functor **which preserves weak pullbacks** presented by  $H_\Sigma$ . Then  $\vdash x = y$  if and only if  $x$  and  $y$  are  $F$ -bisimilar.



Improvements

# Precongruences

*Notation.* Given a relation  $R$ , let  $e(R)$  be its equivalence closure and  $q_R : X \rightarrow X/e(R)$  be the quotient map.

## Definition (Aczel & Mendler, 1989)

A *precongruence* on an  $F$ -coalgebra  $(X, c)$  is a relation  $R$  such that

$$R \subseteq \ker(Fq_R \circ c) = \{(x, y) \in X \times X : Fq_R(c(x)) = Fq_R(c(y))\}$$

A *congruence* is an equivalence relation and a precongruence.

Precongruences share many properties with bisimulations:

- 1 The diagonal  $\Delta_X$  is a congruence.
- 2 Arbitrary unions of precongruences are precongruences.
- 3 If a relation is a precongruence, so is its inverse.
- 4 If two relations\* are precongruences, so is their composition.
- 5  $R$  is a precongruence if and only if  $e(R)$  is a congruence.

## Congruences and kernels

### Definition (Aczel & Mendler, 1989)

A *precongruence* on an  $F$ -coalgebra  $(X, c)$  is a relation  $R$  such that

$$R \subseteq \ker(Fq_R \circ c) = \{(x, y) \in X \times X : Fq_R(c(x)) = Fq_R(c(y))\}$$

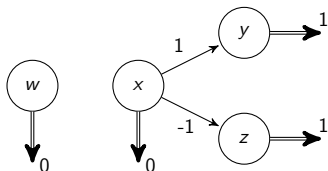
A *congruence* is an equivalence relation and a precongruence.

### Theorem (AM '89)

A relation is an  $F$ -congruence on  $(X, c)$  if and only if it is the kernel of a  $F$ -coalgebra morphism out of  $(X, c)$ .

The greatest congruence is the kernel of the final coalgebra map.

## Example $\mathcal{W}$ -coalgebra: II



As an  $F$ -coalgebra  $X \xrightarrow{c} \mathcal{W}X$ ,

$$c(w) = (0, \lambda a.0) \quad c(x) = (0, \chi_y - \chi_z)$$

$$c(y) = (1, \lambda a.0) \quad c(z) = (1, \lambda a.0)$$

*Claim.*  $R = \{(x, w), (y, z)\}$  is a precongr. ( $R \subseteq \ker(\mathcal{W}q_R \circ c)$ )

$$c(y) = c(z) = (1, \lambda a.0)$$

$$\begin{aligned} \mathcal{W}q_R(c(x)) &= \mathcal{W}q_R(0, \chi_y - \chi_z) = (0, \mathbb{K}_\omega^{qR}(\chi_y - \chi_z)) \\ &= (0, \chi_{[y]} - \chi_{[z]}) = (0, \lambda a.0) = \mathcal{W}q_r(c(w)) \end{aligned}$$

## Behavioral equivalence as a greatest fixed point

Definition (Aczel & Mendler, 1989)

A *precongruence* on an  $F$ -coalgebra  $(X, c)$  is a relation  $R$  such that

$$R \subseteq \ker(Fq_R \circ c) = \{(x, y) \in X \times X : Fq_R(c(x)) = Fq_R(c(y))\}$$

A *congruence* is an equivalence relation and a precongruence.

Given the coalgebra  $(X, c)$  we can define an operation on relations:

$$R^- \triangleq \{(x, y) \in X \times X : Fq_R(c(x)) = Fq_R(c(y))\}$$

Patently,  $R \subseteq R^-$  if and only if  $R$  is a precongruence.

$(\cdot)^-$  is a monotone function on relations on  $X$ . Its greatest fixed point is behavioral equivalence.

## Parametrized greatest fixed points

Let  $L$  be a complete lattice and  $\Phi : L \rightarrow L$  be monotone. For  $r \in L$ , define  $\Phi_r(x) \triangleq \Phi(x) \vee r$ . Knaster-Tarski says these all have greatest fixed points  $r^* = \text{gfp}(\Phi_r)$ .

We point out three useful properties:

- 1  $r \leq r^*$
- 2  $r \leq s$  implies  $r^* \leq s^*$
- 3 (discharge lemma)  $s \leq \Phi((r \vee s)^*)$  implies  $(r \vee s)^* = r^*$

Proof of 3:

$$(r \vee s)^* = \Phi((r \vee s)^*) \vee r \vee s = \Phi((r \vee s)^*) \vee r = \Phi_r((r \vee s)^*)$$

When  $\Phi = (\cdot)^-$ , behavioral equivalence is  $\perp^* = \emptyset^*$ .

$R^* = \text{gfp}((\cdot)^- \cup R)$  is very important in our soundness proof.

## Comparison with Hur et al. (POPL '13)

Let  $L$  be a complete lattice and  $\Phi : L \rightarrow L$  be monotone. For  $r \in L$ , define  $\Phi_r(x) \triangleq \Phi(x) \vee r$ . Knaster-Tarski says these all have greatest fixed points  $r^* = \text{gfp}(\Phi_r)$ .

Hur et al. considered  $\Phi'_r(x) = \Phi(x \vee r)$  and their greatest fixed points  $G_\Phi(r)$ . The slight difference leads to different properties:

- $r \leq r^*$  for all  $\Phi$
- $r \not\leq G_\Phi(r)$  for some  $\Phi$
- (discharge)  $s \leq \Phi((r \vee s)^*) \rightarrow (r \vee s)^* = r^*$
- (accumulation)  $s \leq G_\Phi(r) \leftrightarrow s \leq G_\Phi(r \vee s)$

## Logic (20167)

Let  $(X, d : X \rightarrow H_{\Sigma}X)$ ,  $(x, y) \in X$ , and  $(\sigma, \tau) \in H_{\Sigma}X$ .

Formulas are pairs of variables or pairs of flat terms.  $(\alpha = \beta)$

Sequents are a relation on  $X$  together with a formula.

$$\frac{\frac{R \vdash \alpha = \beta \quad \forall (x, y) \in R, R \vdash d(x) = d(y)}{\vdash \alpha = \beta} \quad b}{RUS \vdash \alpha = \beta \quad \forall (x, y) \in R, RUS \vdash d(x) = d(y)} \quad i$$
$$S \vdash \alpha = \beta$$

$$\frac{(\sigma =_{\epsilon} \tau)}{R \vdash \sigma = \tau} \quad \epsilon$$

$$\overline{R \vdash \alpha = \alpha} \quad r$$

$$\overline{R \cup \{(x, y)\} \vdash x = y} \quad a$$

$$\frac{R \vdash \beta = \alpha}{R \vdash \alpha = \beta} \quad s$$

$$\frac{R \vdash x_1 = y_1 \cdots R \vdash x_n = y_n}{R \vdash f(x_1, \dots, x_n) = f(y_1, \dots, y_n)} \quad c$$

$$\frac{R \vdash \alpha = \beta \quad R \vdash \beta = \gamma}{R \vdash \alpha = \gamma} \quad t$$



## Example $\mathcal{W}$ -coalgebra: III

Recall the weighted automata from above. As an  $H_\Sigma$ -coalgebra,  
 $d(w) = (0)$   $d(x) = (0, 1, -1)(y, z)$   $d(y) = (1)$   $d(z) = (1)$

Let  $R = \{(x, w), (y, z)\}$ . The following proves  $\vdash x = w$ .

$$\begin{array}{c}
 \frac{\overline{R \vdash y = z} \quad a \quad \overline{R \vdash z = z} \quad r}{\overline{R \vdash (0, 1, -1)(y, z) = (0, 1, -1)(z, z)} \quad c} \quad \overline{R \vdash (0, 1, -1)(z, z) = (0)} \quad \epsilon \\
 \hline
 R \vdash (0, 1, -1)(y, z) = (0) \quad t \\
 \\
 \uparrow \\
 \frac{\overline{(x, w) \vdash x = w} \quad a \quad \frac{\overline{R \vdash (0, 1, -1)(y, z) = (0)} \quad \overline{R \vdash (1) = (1)} \quad r}{\overline{(x, w) \vdash (0, 1, -1)(y, z) = (0)} \quad i}}{\vdash x = w} \quad i
 \end{array}$$

# Soundness & Completeness

## Theorem (Strong soundness)

Let  $(X, d)$  be an  $H_\Sigma$ -coalgebra. If  $R \vdash x = y$ , then  $(x, y) \in e(R^*)$ .  
If  $R \vdash \sigma = \tau$ , then  $(\sigma, \tau) \in \ker(Fq_{R^*} \circ \epsilon_X)$ .

## Proof.

By induction on the height of the proof tree. Interesting case is  $i$ :

$$\frac{R \cup S \vdash \alpha = \beta \quad \forall (x, y) \in R, R \cup S \vdash d(x) = d(y)}{S \vdash \alpha = \beta} \quad i$$

The IH give  $(x, y) \in \ker(Fq_{(R \cup S)^*} \circ \epsilon_X \circ d)$  for all  $(x, y) \in R$ .

I.e.  $R \subseteq ((R \cup S)^*)^-$ . Discharge lemma gives  $S^* = (R \cup S)^*$ .  $\square$

## Theorem (Completeness)

Let  $(X, d)$  be an  $H_\Sigma$ -coalgebra. If  $(x, y) \in R \subseteq R^-$ , then  $\vdash x = y$ .

## Soundness and completeness

### Theorem (S, 2016)

Let  $(X, d)$  be an  $H_\Sigma$ -coalgebra,  $x, y \in X$ , and  $F$  a finitary functor **which preserves weak pullbacks** presented by  $H_\Sigma$ .  
Then  $\vdash x = y$  if and only if  $x$  and  $y$  are  $F$ -**bisimilar**.

## Soundness and completeness

Theorem (S & Moss, 2017)

*Let  $(X, d)$  be an  $H_\Sigma$ -coalgebra,  $x, y \in X$ , and  $F$  a finitary functor presented by  $H_\Sigma$ .*

*Then  $\vdash x = y$  if and only if  $x$  and  $y$  are  $F$ -congruent.*

Future work

## Categorizing rules

Take  $FX = A \times X$ , let  $(X, d)$  be an  $F$ -coalgebra and  $R \subseteq X \times X$ .

$$R^F = \{(a :: x, a :: y) \in FX \times FX : x R y\}$$

$$\Phi(R) = R^- = R^F \circ (d \times d)$$

### Hypothesis introduction and elimination

$$\frac{R \cup S \vdash \varphi \quad \forall (x, y) \in R, R \cup S \vdash d(x) = d(y)}{S \vdash \varphi} \quad i$$

$$\frac{}{R \cup \{(x, y)\} \vdash x = y} \quad a$$

### Lifting rules

$$\frac{R \vdash x = y}{R \vdash a :: x = a :: y} \quad c$$

### Up-to rules

$$\frac{}{R \vdash \alpha = \alpha} \quad r$$

$$\frac{R \vdash \beta = \alpha}{R \vdash \alpha = \beta} \quad s$$

$$\frac{R \vdash \alpha = \beta \quad R \vdash \beta = \gamma}{R \vdash \alpha = \gamma} \quad t$$

## Future work: other predicates

$FX = A \times X$  and  $(X, d)$  is an  $F$ -coalgebra. Let  $\leq$  order  $A$ .

$R^F = \{(a :: x, b :: y) \in FX \times FX : a \leq b \text{ and } x R y\}$

$\Phi(R) = R^F \circ (d \times d)$

### Hypothesis introduction and elimination

$$\frac{R \cup S \vdash \varphi \quad \forall (x, y) \in R, R \cup S \vdash d(x) \leq d(y)}{S \vdash \varphi} \quad i$$

$$\frac{}{R \cup \{(x, y)\} \vdash x \leq y} \quad a$$

### Lifting rules

$$\frac{R \vdash x \leq y}{R \vdash a :: x \leq b :: y} \quad c, a \leq b$$

### Up-to rules

$$\frac{\frac{}{R \vdash \alpha \leq \alpha} \quad r}{R \vdash \alpha \leq \beta \quad R \vdash \beta \leq \gamma} \quad t}{R \vdash \alpha \leq \gamma}$$

## Future work: other predicates

$FX = A \times X$  and  $(X, d)$  is an  $F$ -coalgebra. Let  $\leq$  order  $A$ .

$R^F = \{(a :: x, b :: y) \in FX \times FX : a < b \text{ or } a = b \text{ and } x R y\}$

$\Phi(R) = R^F \circ (d \times d)$

### Hypothesis introduction and elimination

$$\frac{RUS \vdash \varphi \quad \forall (x, y) \in R, RUS \vdash d(x) \leq d(y)}{S \vdash \varphi} \quad i$$

$$\frac{}{RU\{(x, y)\} \vdash x \leq y} \quad a$$

### Lifting rules

$$\frac{R \vdash x \leq y}{R \vdash a :: x \leq a :: y} \quad c_1$$
$$\frac{}{R \vdash a :: x \leq b :: y} \quad c_2, a < b$$

### Up-to rules

$$\frac{}{R \vdash \alpha \leq \alpha} \quad r$$
$$\frac{R \vdash \alpha \leq \beta \quad R \vdash \beta \leq \gamma}{R \vdash \alpha \leq \gamma} \quad t$$



## Future work

### Higher order schemes (with S. Bhaskar)

$X \xrightarrow{d} FX$  gives a 0-order recursion scheme.

Coalgebraic proof techniques also seem to work for some 1-order schemes.

### Dualizing for least fixed points (with I. Hasuo, S. Katsumata)

The *behavioral distance* between two points is given by the least pseudometric satisfying certain conditions.

Parametrized fixed point work dualizes to least fixed points, can follow a similar scheme to get a proof system.

Thanks!