Logical Relations

Andrzej Murawski

University of Leicester

Part II

Midlands Graduate School 2012

Slim PCF

Types

$$\theta \quad ::= \quad \mathbf{nat} \quad | \quad \theta \to \theta$$

Terms

$$\frac{}{\Gamma \vdash n : \mathbf{nat}} \qquad \frac{}{\Gamma \vdash \mathbf{succ} : \mathbf{nat} \to \mathbf{nat}} \qquad \frac{}{\Gamma \vdash \mathbf{pred} : \mathbf{nat} \to \mathbf{nat}}$$

$$\frac{}{\Gamma \vdash \mathbf{cond} : \mathbf{nat} \to \mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}} \qquad \frac{}{\Gamma \vdash Y_\theta : (\theta \to \theta) \to \theta}$$

$$\frac{(x : \theta) \in \Gamma}{\Gamma \vdash x : \theta} \qquad \frac{\Gamma, x : \theta \vdash M : \theta'}{\Gamma \vdash \lambda x^\theta . M : \theta \to \theta'} \qquad \frac{\Gamma \vdash M : \theta \to \theta' \quad \Gamma \vdash N : \theta}{\Gamma \vdash MN : \theta'}$$

Reduction rules

Big-step semantics $M \Downarrow V$, where $\vdash M$ and $V = n, \lambda x^\theta.M$.

$$\frac{}{V \Downarrow V} \qquad \frac{M \Downarrow n}{\mathbf{succ} M \Downarrow n+1} \qquad \frac{M \Downarrow n \qquad n \neq 0}{\mathbf{pred} M \Downarrow n-1}$$

$$\frac{M \Downarrow 0 \qquad N_0 \Downarrow n}{\mathbf{cond} M N_0 N_1 \Downarrow n} \quad \frac{M \Downarrow m \qquad m \neq 0 \qquad N_1 \Downarrow n}{\mathbf{cond} M N_0 N_1 \Downarrow n}$$

$$\frac{M \Downarrow \lambda x.M' \quad M'[N/x] \Downarrow V}{MN \Downarrow V} \quad \frac{M(Y_\theta M) \Downarrow V}{Y_\theta M \Downarrow V}$$

Let $\theta \equiv \theta_1 \to \cdots \to \theta_k \to \mathbf{nat}$. Two closed terms $\vdash M : \theta$ and $\vdash N : \theta$ are equivalent (written $\vdash M \cong N : \theta$) if and only if, for all $\vdash Q_1 : \theta_1, \cdots, \vdash Q_k : \theta_k$,

$$M Q_1 \cdots Q_k \Downarrow n \iff N Q_1 \cdots Q_k \Downarrow n.$$

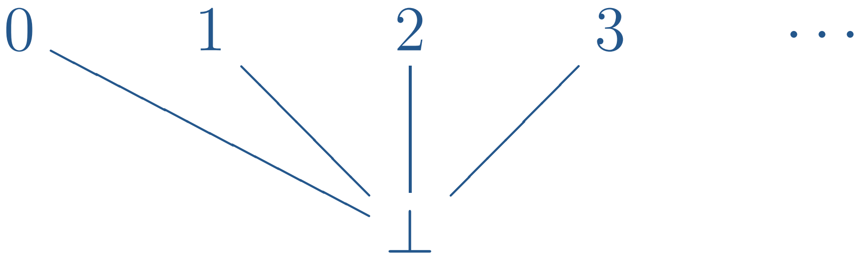
Interpretation (types)

$[\![\theta]\!]$ will be complete partial orders (cpo's).

$$\begin{aligned} [\![\mathbf{nat}]\!] &= \mathbb{N}_\perp \\ [\![\theta_1 \to \theta_2]\!] &= [\![\theta_1]\!] \Rightarrow [\![\theta_2]\!] \end{aligned}$$

$\Rightarrow$ stands for the cpo of continuous functions.

$\mathbb{N}_\perp$



Interpretation (terms)

Terms are interpreted by continuous functions.

$$\llbracket \Gamma \vdash n \rrbracket(\rho) \quad = \quad n$$

$$\llbracket \Gamma \vdash \mathbf{succ} \rrbracket(\rho)(d) \quad = \quad \begin{cases} \bot & d = \bot \\ \\ d+1 & d \neq \bot \end{cases}$$

$$\llbracket \Gamma \vdash \mathbf{pred} \rrbracket(\rho)(d) \quad = \quad \begin{cases} \bot & d = \bot, 0 \\ d-1 & d \neq 0 \end{cases}$$

$$\llbracket \Gamma \vdash \mathbf{cond} \rrbracket(\rho)(d)(e)(f) \quad = \quad \begin{cases} \bot & d = \bot \\ e & d = 0 \\ f & d \neq 0 \end{cases}$$

$$\llbracket \Gamma \vdash Y_\theta \rrbracket(\rho)(f) \quad = \quad \mathsf{lfp}(f)$$

Properties

- Computational Soundness

  If $M \Downarrow V$ then $[\![M]\!] = [\![V]\!]$

- Computational Adequacy

  If $[\![M]\!] = n$ then $M \Downarrow n$.

Full Abstraction fails: it is *not* the case that

$$\vdash M_1 \cong M_2 : \theta \quad \Longleftrightarrow \quad [\![\vdash M_1 : \theta]\!] = [\![\vdash M_2 : \theta]\!].$$

Failure of Full Abstraction

More precisely,

- If $[\![\vdash\ M]\!] = [\![\vdash\ N]\!]$ then $\vdash\ M \cong N$.
- But the converse fails, we can have $[\![M]\!] \neq [\![N]\!]$ and $M \cong N$.

Full abstraction at various types:

- holds for types of order 0 and 1,
- holds for $(\mathbf{nat} \to \mathbf{nat}) \to \mathbf{nat}$,
- fails for $(\mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}) \to \mathbf{nat}$.

In the following we use a divergent term: $\Omega_\theta \equiv Y_\theta(\lambda x^\theta.x)$.

Failure of full abstraction at order 2

$$M = \lambda f^{\mathbf{nat}\to\mathbf{nat}\to\mathbf{nat}}.\mathbf{cond}\,(f\,\Omega\,1)\,(\mathbf{cond}\,(f\,1\,\Omega)\,(\mathbf{cond}\,(f\,0\,0)\,\Omega\,1)\,\Omega)\,\Omega$$
$$N = \lambda f^{\mathbf{nat}\to\mathbf{nat}\to\mathbf{nat}}.\Omega$$

- $[\![\vdash\ M]\!](por) \neq [\![\vdash\ N]\!](por)$, where

$$por\,x\,y = \begin{cases} 1 & x > 0 \text{ or } y > 0 \\ 0 & x = 0 \text{ and } y = 0 \\ \bot & \text{otherwise} \end{cases}$$

- There is no PCF term Q such that

$$Q\,\Omega\,1 \Downarrow 1 \qquad Q\,1\,\Omega \Downarrow 1 \qquad Q\,0\,0 \Downarrow 0.$$

Hence $M \cong N$.

Definable elements

Full abstraction fails at $(\mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}) \to \mathbf{nat}$. It fails because of an undefinable element in the model.

We are going to refine our domain of interpretation to a setting in which, at certain types, each element can be approximated by definable ones.

- At present this is not the case already at order 1.
- We will fix that at order 1 and 2.

In addition to continuity we are going to insist on an invariance principle, to be introduced in the next few slides.

Logical Relations

Definition 1. *An n-ary* **logical relation** *is a family $\mathcal{R} = \{R_\theta\}_{\theta \in Types}$ of n-ary relations such that $R_\theta \subseteq \underbrace{[\![\theta]\!] \times \cdots \times [\![\theta]\!]}_{n}$ for any θ and*

$$R_{\theta_1 \to \theta_2}(f_1, \cdots, f_n)$$

$$\Longleftrightarrow$$

$$\textit{for all } (d_1, \cdots, d_n) \in [\![\theta_1]\!]^n,$$
$$\textit{if } R_{\theta_1}(d_1, \cdots, d_n) \textit{ then } R_{\theta_2}(f_1(d_1), \cdots, f_n(d_n)).$$

$\{R_\theta\}$ is uniquely determined by $R_{\mathbf{nat}} \subseteq [\![\mathbf{nat}]\!] \times \cdots \times [\![\mathbf{nat}]\!]$.

Fundamental Theorem

Invariance will turn out useful for tracking undefinable elements.

Theorem 2 (Plotkin). *Let* $\{R_\theta\}$ *be a logical relation such that* $R_{\theta_c}([\![\vdash c : \theta_c]\!], \cdots, [\![\vdash c : \theta_c]\!])$ *for all PCF-constants* c*. Then*

$$R_\theta([\![\vdash M : \theta]\!], \cdots, [\![\vdash M : \theta]\!]).$$

Suppose we want to show that for some $d \in [\![\theta]\!]$ there is no $\vdash M : \theta$ such that $[\![\vdash \vdash M]\!] = d$. We can try the following recipe.

1. Find a logical relation $\mathcal{R}$ (this amounts to exhibiting $R_{\mathbf{nat}}$).

2. Check that $R_{\theta_c}([\![\vdash c]\!], \cdots, [\![\vdash c]\!])$.

3. Check that $R_\theta(d, \cdots, d)$ fails.

By Theorem 2, d is not definable.

Proving $R_{(\theta\to\theta)\to\theta}(\llbracket Y_\theta \rrbracket, \cdots, \llbracket Y_\theta \rrbracket)$

It suffices to show that $R_{\mathbf{nat}}(\bot_{\llbracket \mathbf{nat} \rrbracket}, \cdots, \bot_{\llbracket \mathbf{nat} \rrbracket})$!

- The above turns out to imply $R^\theta(\bot_{\llbracket \theta \rrbracket}, \cdots, \bot_{\llbracket \theta \rrbracket})$ for any θ (induction on θ).
  - $R_{\mathbf{nat}}(\bot_{\llbracket \mathbf{nat} \rrbracket}, \cdots, \bot_{\llbracket \mathbf{nat} \rrbracket})$
  - $R_{\theta_1\to\theta_2}(\bot_{\llbracket \theta_1\to\theta_2 \rrbracket}, \cdots, \bot_{\llbracket \theta_1\to\theta_2 \rrbracket})$ follows from $R_{\theta_2}(\bot_{\llbracket \theta_2 \rrbracket}, \cdots, \bot_{\llbracket \theta_2 \rrbracket})$.
- Now suppose $R_{\theta\to\theta}(f_1, \cdots, f_m)$. Because $R_\theta(\bot_{\llbracket \theta \rrbracket}, \cdots, \bot_{\llbracket \theta \rrbracket})$, we obtain $R_\theta(f_1 \bot_\theta, \cdots, f_m \bot_\theta)$ and, more generally, $R_\theta(f_1^i \bot_\theta, \cdots, f_m^i \bot_\theta)$.

  Then $R^\theta(\bigsqcup_i (f_1^i \bot_\theta), \cdots, \bigsqcup_i (f_m^i \bot_\theta))$, i.e.

$$R_\theta(\llbracket Y_\theta \rrbracket\, f_1, \cdots, \llbracket Y_\theta \rrbracket\, f_m).$$

Parallel-or is undefinable

Lemma 3. *There is no definable function* $f \in [\![\mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}]\!]$ *such that*

$$\begin{array}{cccccc} f & 1 & \bot & = & 1 \\ f & \bot & 1 & = & 1 \\ f & 0 & 0 & = & 0. \end{array}$$

Let us define $R_{\mathbf{nat}}(x, y, z)$ to be $(x = y = z) \vee (x = \bot) \vee (y = \bot)$. Note that $R_{\mathbf{nat}}(1, \bot, 0)$ and $R_{\mathbf{nat}}(\bot, 1, 0)$. However, $R_{\mathbf{nat}}(1, 1, 0)$ does not hold. Because

$$(f1\bot, f\bot1, f00) = (1, 1, 0)$$

we do *not* have $R(f, f, f)$. If we can show that all interpretations of PCF constants are invariant under R, we will be entitled to conclude that f is indeed undefinable.

All PCF constants are invariant under R

$$\boxed{R_{\mathbf{nat}}(x,y,z) \quad \equiv \quad (x=y=z) \vee (x=\bot) \vee (y=\bot)}$$

- $R_{\mathbf{nat}}(\bot,\bot,\bot)$ ✓
- $R_{\mathbf{nat}}(n,n,n)$ ✓
- $R_{\mathbf{nat}\to\mathbf{nat}}(\llbracket\mathbf{succ}\rrbracket, \llbracket\mathbf{succ}\rrbracket, \llbracket\mathbf{succ}\rrbracket)$

  If $R_{\mathbf{nat}}(x,y,z)$ then $R_{\mathbf{nat}}(\llbracket\mathbf{succ}\rrbracket\, x, \llbracket\mathbf{succ}\rrbracket\, y, \llbracket\mathbf{succ}\rrbracket\, z)$.

  - ○ $x=y=z$
  - ○ $x=\bot$
  - ○ $y=\bot$

  In each case $R_{\mathbf{nat}}(\llbracket\mathbf{succ}\rrbracket\, x, \llbracket\mathbf{succ}\rrbracket\, y, \llbracket\mathbf{succ}\rrbracket\, z)$, because $\llbracket\mathbf{succ}\rrbracket\, \bot = \bot$. ✓

All PCF constants are invariant under R

$$\boxed{R_{\mathbf{nat}}(x, y, z) \quad \equiv \quad (x = y = z) \vee (x = \bot) \vee (y = \bot)}$$

- $R_{\mathbf{nat}\to\mathbf{nat}}([\![\mathbf{pred}]\!], [\![\mathbf{pred}]\!], [\![\mathbf{pred}]\!])$ (same as $\mathbf{succ}$) ✓
- $R_{\mathbf{nat}\to\mathbf{nat}\to\mathbf{nat}\to\mathbf{nat}}([\![\mathbf{cond}]\!], [\![\mathbf{cond}]\!], [\![\mathbf{cond}]\!])$

  If $R_{\mathbf{nat}}(x, y, z)$, $R_{\mathbf{nat}}(x_L, y_L, z_L)$ and $R_{\mathbf{nat}}(x_R, y_R, z_R)$ then $R_{\mathbf{nat}}([\![\mathbf{cond}]\!]xx_Lx_R, [\![\mathbf{cond}]\!]yy_Ly_R, [\![\mathbf{cond}]\!]zz_Lz_R)$.

  - $x = y = z$: reduces to $R_{\mathbf{nat}}(\bot_{[\![\mathbf{nat}]\!]}, \bot_{[\![\mathbf{nat}]\!]}, \bot_{[\![\mathbf{nat}]\!]})$, $R_{\mathbf{nat}}(x_L, y_L, z_L)$ or $R_{\mathbf{nat}}(x_R, y_R, z_R)$
  - $x = \bot$: $[\![\mathbf{cond}]\!]xx_Lx_R = \bot$
  - $y = \bot$: $[\![\mathbf{cond}]\!]yy_Ly_R = \bot$

✓

Sequentiality relations

Definition 4. *Let* R *be a logical relation.* R *is called a* sequentiality relation *whenever* $R([\![\vdash c]\!], \cdots, [\![\vdash c]\!])$ *for all PCF constants.*

Let $m \in \mathbb{N}$. Suppose

$$A \subseteq B \subseteq \{1, \cdots, m\}.$$

Let

$$S^m_{A,B} \subseteq \underbrace{[\![\mathbf{nat}]\!] \times \cdots \times [\![\mathbf{nat}]\!]}_{m}$$

be defined by

$$S^m_{A,B}(x_1, \cdots, x_m) \iff (\exists i \in A.\ x_i = \bot) \vee (\forall i, j \in B.\ x_i = x_j).$$

Sequentiality relations

Theorem 5. *An m-ary logical relation R is a sequentiality relation if and only if $R_{\mathbf{nat}}$ is an intersection of relations of the form $S^m_{A,B}$.*

Now let us try to prove the Fundamental Theorem.

Let $\{R_\theta\}$ be a logical relation such that $R_{\theta_c}(\llbracket \vdash\ c : \theta_c \rrbracket, \cdots, \llbracket \vdash \vdash c : \theta_c \rrbracket)$ for all PCF-constants c. Then

$$R_\theta(\llbracket \vdash\ M : \theta \rrbracket, \cdots, \llbracket \vdash\ M : \theta \rrbracket).$$

We shall reason by structural induction on closed terms using the alternative (but equivalent) typing rules for closed terms (next slide).

Alternative typing rules for closed terms

$$\frac{}{\lambda x_1^{\theta_1} \cdots x_k^{\theta_k}.x_i : \theta_1 \to \cdots \to \theta_k \to \theta_i}$$

$$\frac{x_1 : \theta_1, \cdots , x_n : \theta_n \vdash \ c : \theta_c}{\lambda x_1^{\theta_1} \cdots x_k^{\theta_k}.c : \theta_1 \to \cdots \to \theta_k \to \theta_c}$$

$$\frac{\lambda x_1^{\theta_1} \cdots x_j^{\theta_j} x_{j+1}^{\theta_{j+1}} \cdots x_k^{\theta_k}.M : \theta_1 \to \cdots \theta_j \to \theta_{j+1} \to \cdots \to \theta_k \to \theta}{\lambda x_1^{\theta_1} \cdots x_{j+1}^{\theta_{j+1}} x_j^{\theta_j} \cdots x_k^{\theta_k}.M : \theta_1 \to \cdots \theta_{j+1} \to \theta_j \to \cdots \to \theta_k \to \theta}$$

$$\frac{\begin{array}{c}\lambda x_1^{\theta_1} \cdots x_k^{\theta_k}.M : \theta_1 \to \cdots \to \theta_k \to \theta \to \theta' \\ \lambda x_1^{\theta_1} \cdots x_k^{\theta_k}.N : \theta_1 \to \cdots \to \theta_k \to \theta\end{array}}{\lambda x_1^{\theta_1} \cdots x_k^{\theta_k}.MN : \theta_1 \to \cdots \to \theta_k \to \theta'}$$

We have $M : \theta$ (according to the above rules) if and only if $\vdash \ M : \theta$.

Proof of Theorem 2

If $R_{\theta_c}([\![\vdash c]\!], \cdots, [\![\vdash c]\!])$ then $R_\theta([\![\vdash M]\!], \cdots, [\![\vdash M]\!])$.

1. $\lambda x_1 \cdots x_k . x_i$ ✓
2. $\lambda x_1 \cdots x_k . c$ (assumption) ✓
3. $\lambda x_1 \cdots x_{j+1} x_j \cdots . M$

   Follows immediately from IH for $\lambda x_1 \cdots x_j x_{j+1} \cdots . M$.

Proof of Theorem 2 (ii)

4. $\lambda x_1 \cdots x_k.MN$

Let us write Q, Q_f, Q_a for $\lambda x_1 \cdots x_k.MN$, $\lambda x_1 \cdots x_k.M$ and $\lambda x_1 \cdots x_k.N$ respectively.

Assuming $R_{\theta_i}(x_1^i, \cdots, x_m^i)$ for $i = 1, \cdots, k$ we should show

$$R^{\theta'}([\![Q]\!]x_1^1 \cdots x_1^k, \cdots, [\![Q]\!]x_m^1 \cdots x_m^k).$$

By IH for Q_f and Q_a

$$R_{\theta \to \theta'}([\![Q_f]\!]x_1^1 \cdots x_1^k, \cdots, [\![Q_f]\!]x_m^1 \cdots x_m^k),$$
$$R_{\theta}([\![Q_a]\!]x_1^1 \cdots x_1^k, \cdots, [\![Q_a]\!]x_m^1 \cdots x_m^k).$$

Observe that $[\![Q]\!]x_j^1 \cdots x_j^k = ([\![Q_f]\!]x_j^1 \cdots x_j^k)([\![Q_a]\!]x_j^1 \cdots x_j^k)$, so $R_{\theta'}([\![Q]\!]x_1^1 \cdots x_1^k, \cdots, [\![Q]\!]x_m^1 \cdots x_m^k)$ follows.

Sequentiality relations

We have seen that denotations of PCF terms are invariant under all logical relations under which the constants are invariant.

Definition 6. $f \in [\![\theta]\!]$ *is a* logically sequential function *whenever* $R_\theta(f, \cdots, f)$ *for all sequentiality relations* R*.*

What we have learnt can now be summarised as follows: all denotations of PCF terms are logically sequential.

Are all logically sequential functions definable? No, but it will turn out that at order 1 and 2 they can be approximated by definable elements (as lubs of chains of definable elements).

Coverability

Lemma 7. *Let θ be a type order 1 or 2, i.e. $\theta = \theta_1 \to \cdots \to \theta_n \to \mathbf{nat}$, where $\theta_1, \cdots, \theta_n$ are of order at most 1. Let $f \in [\![\theta]\!]$ be a logically sequential function. Suppose*

$$(x_1^i, \cdots, x_n^i) \in [\![\theta_1]\!] \times \cdots \times [\![\theta_n]\!]$$

for $i = 1, \cdots, m$. Then there exists a PCF term $\vdash M : \theta$ such that

$$\begin{array}{rcl} [\![\vdash M]\!] x_1^1 \cdots x_n^1 & = & f x_1^1 \cdots x_n^1 \\ & \vdots & \\ [\![\vdash M]\!] x_1^m \cdots x_n^m & = & f x_1^m \cdots x_n^m \end{array}$$

for all $1 \leq i \leq m$.

In short, M coincides with f on m selected points.

Proof of Lemma 7

Define $R_{\mathbf{nat}}(e_1, \cdots, e_m)$ as $\exists_{M:\theta} \forall_{1 \leq i \leq m} [\![\vdash M]\!] x_1^i \cdots x_n^i = e_i$.

The lemma amounts to showing $R_{\mathbf{nat}}(f x_1^1 \cdots x_n^1, \cdots, f x_1^m \cdots x_n^m)$.

- First one proves that R is a sequentiality relation (deferred).
- Because f is logically sequential, we have $R_\theta(f, \cdots, f)$.

  If we knew that

  $$R_{\theta_1}(x_1^1, \cdots, x_1^m), \cdots, R_{\theta_n}(x_n^1, \cdots, x_n^m)$$

  we could derive $R_{\mathbf{nat}}(f x_1^1 \cdots x_n^1, \cdots, f x_1^m \cdots x_n^m)$.
- So, let us prove that $R_{\theta_j}(x_j^1, \cdots, x_j^m)$.

Proof of Lemma 7 (ii)

$$\boxed{R^{\mathbf{nat}}(e_1, \cdots, e_m) \equiv \exists_{M:\theta} \forall_{1 \leq i \leq m} [\![\vdash M]\!] x_1^i \cdots x_n^i = e_i}$$

We want to show $R^{\theta_j}(x_j^1, \cdots, x_j^m)$.
Note that θ_j is of order at most 1, so we have two cases only.

- $\theta_j = \mathbf{nat}$
- $\theta_j = \underbrace{\mathbf{nat} \to \cdots \to \mathbf{nat}}_{k} \to \mathbf{nat}$

Suppose $\theta_j = \mathbf{nat}$. It suffices to find $M : \theta$ such that

$$[\![\vdash M]\!] x_1^i \cdots x_n^i = x_j^i.$$

We can simply take M to be the jth projection $\lambda x_1 \cdots x_n . x_j$.

Proof of Lemma 7 (iii)

$$\boxed{R_{\mathbf{nat}}(e_1, \cdots, e_m) \equiv \exists_{M:\theta} \forall_{1 \le i \le m} [\![\vdash\ M]\!] x_1^i \cdots x_n^i = e_i}$$

Suppose $\theta_j = \underbrace{\mathbf{nat} \to \cdots \to \mathbf{nat}}_{k} \to \mathbf{nat}$. Assuming

$$R_{\mathbf{nat}}(y_1^1, \cdots, y_m^1), \cdots, R_{\mathbf{nat}}(y_1^k, \cdots, y_m^k)$$

we need to show $R_{\mathbf{nat}}(x_j^1 y_1^1 \cdots y_1^k, \cdots, x_j^m y_m^1 \cdots y_m^k)$.
By definition this amounts to finding M such that

$$M x_1^i \cdots x_n^i = x_j^i y_i^1 \cdots y_i^k.$$

By assumption we already have terms M_h ($h = 1, \cdots, k$) such that

$$M_h x_1^i \cdots x_n^i = y_i^h.$$

We can take M to be $\lambda x_1 \cdots x_n . x_j (M_1 x_1 \cdots x_n) \cdots (M_k x_1 \cdots x_n)$.

Some comments

It is really instructive to understand why the argument above cannot be repeated at order 3!

- $\theta_j = (\mathbf{nat} \to \mathbf{nat}) \to \mathbf{nat}$

  We want to show $R_{\theta_j}(x_j^1, \cdots, x_j^m)$. Thus, assuming $R_{\mathbf{nat}\to\mathbf{nat}}(y_1, \cdots, y_m)$ we should show $R_{\mathbf{nat}}(x_j^1 y_1, \cdots, x_j^m y_m)$, i.e. that there exists M such that

  $$[\![\vdash M]\!] x_1^i \cdots x_n^i = x_j^i y_i.$$

  How do we extract M for y_i's from $R^{\mathbf{nat}\to\mathbf{nat}}(y_1, \cdots, y_m)$?

Let us not forget that we have not yet proved that the relation R from the proof is a sequentiality relation.

R is a sequentiality relation

$$R^{\mathbf{nat}}(e_1, \cdots, e_m) \equiv \exists_{M:A} \forall_{1 \leq i \leq m} [\![\vdash M]\!] x_1^i \cdots x_n^i = e_i$$

We should prove that $R([\![\vdash c]\!], \cdots, [\![\vdash c]\!])$ for each constant.

- $R^{\mathbf{nat}}(\bot, \cdots, \bot)$
$$M \equiv \lambda x_1 \cdots x_n . \Omega_{\mathbf{nat}}$$
- $R^{\mathbf{nat}}(u, \cdots, u)$
$$M \equiv \lambda x_1 \cdots x_n . u$$
- $R^{\mathbf{nat} \rightarrow \mathbf{nat}}([\![\vdash \mathbf{succ}]\!], \cdots, [\![\vdash \mathbf{succ}]\!])$

  Assume $R^{\mathbf{nat}}(y_1, \cdots, y_m)$, i.e. there exists M such that $[\![\vdash M]\!] x_1^i \cdots x_n^i = y_i$. Then

  $$[\![\vdash (\lambda x_1 \cdots x_n . \mathbf{succ}(M x_1 \cdots x_n))]\!] x_1^i \cdots x_n^i = [\![\vdash \mathbf{succ}]\!] y_i .$$

  So $R^{\mathbf{nat}}([\![\vdash \mathbf{succ}]\!] y_1, \cdots, [\![\vdash \mathbf{succ}]\!] y_m)$.

R is a sequentiality relation (ii)

$$R^{\mathbf{nat}}(e_1, \cdots, e_m) \equiv \exists_{M:A} \forall_{1 \le i \le m} [\![\vdash M]\!] x_1^i \cdots x_n^i = e_i$$

- $R^{\mathbf{nat} \to \mathbf{nat}}([\![\vdash \mathbf{pred}]\!], \cdots, [\![\vdash \mathbf{pred}]\!])$ (analogous)
- $R^{\mathbf{nat} \to \mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}}([\![\vdash \mathbf{cond}]\!], \cdots, [\![\vdash \mathbf{cond}]\!])$

  Assume $R^{\mathbf{nat}}(g_1, \cdots, g_m)$, $R^{\mathbf{nat}}(l_1, \cdots, l_m)$, $R^{\mathbf{nat}}(r_1, \cdots, r_m)$, i.e. there exist M_g, M_l, M_r s.t.

$$[\![\vdash M_g]\!] x_1^i \cdots x_n^i = g_i \qquad [\![\vdash M_l]\!] x_1^i \cdots x_n^i = l_i \qquad [\![\vdash M_r]\!] x_1^i \cdots x_n^i = r_i.$$

  Take M to be
  $\lambda x_1 \cdots x_n.\mathbf{cond}(M_g x_1 \cdots x_n)(M_l x_1 \cdots x_n)(M_r x_1 \cdots x_n)$.
  Then

$$[\![\vdash M]\!] x_1^i \cdots x_n^i = [\![\vdash \mathbf{cond}]\!] g_i l_i r_i,$$

  i.e. $R^{\mathbf{nat}}([\![\vdash \mathbf{cond}]\!] g_1 l_1 r_1, \cdots, [\![\vdash \mathbf{cond}]\!] g_n l_n r_n)$.

Summary

So, at order 1 and 2 each finite part of a logically sequential element can be “covered” by a definable element.

One can prove a bit more: each logically sequential element at order 1 and 2 is the lub of a chain of definable elements.

Lemma 8. *Let θ be a type of order 1 or 2. Let $f \in [\![\theta]\!]$ be a logically sequential element. Then there exists a chain $\{f_i\}$ in $[\![\theta]\!]$ of definable elements such that $f = \bigsqcup_i f_i$.*

Full Abstraction at order 2 and 3

Let $\theta = \theta_1 \to \cdots \to \theta_n \to \mathbf{nat}$ be a type of order at most 3 and $\vdash M, N : \theta$. Recall that the following failed.

$$\vdash M \cong N \iff [\![\vdash M]\!] = [\![\vdash N]\!]$$

$[\![\vdash M]\!] = [\![\vdash N]\!]$ means $[\![\vdash M]\!](x_1)\cdots(x_n) = [\![\vdash N]\!](x_1)\cdots(x_n)$ for all $x_1 \in [\![\theta_1]\!], \cdots, x_n \in [\![\theta_n]\!]$. Now we can repair the above failure!

Theorem 9. *For all types θ of order at most* three, $\vdash M \cong N : \theta$ *if and only if*

$$[\![\vdash M]\!](x_1)\cdots(x_n) = [\![\vdash N]\!](x_1)\cdots(x_n)$$

for all **logically sequential** $x_1 \in [\![\theta_1]\!], \cdots, x_n \in [\![\theta_n]\!]$.

Proof of Theorem 9

$$M \cong N \quad \text{iff} \quad [\![\vdash M]\!](x_1)\cdots(x_n) = [\![\vdash N]\!](x_1)\cdots(x_n)$$
$$\textbf{for LS } x_1, \cdots, x_n$$

$(\Leftarrow)$ Take $\vdash Q_1 : \theta_1, \cdots, \vdash Q_n : \theta_n$. Then:

$$\begin{aligned} [\![\vdash MQ_1\cdots Q_n]\!] &= [\![\vdash M]\!][\![\vdash Q_1]\!]\cdots[\![\vdash Q_n]\!] \\ &= [\![\vdash N]\!][\![\vdash Q_1]\!]\cdots[\![\vdash Q_n]\!] \\ &= [\![\vdash NQ_1\cdots Q_n]\!] \end{aligned}$$

because $[\![\vdash Q_i]\!]$ is logically sequential for each i. Hence

$$MQ_1\cdots Q_n \Downarrow m \iff NQ_1\cdots Q_n \Downarrow m$$

and $M \cong N$.

Proof of Theorem 9

$$M \cong N \quad \text{iff} \quad [\![\vdash M]\!](x_1)\cdots(x_n) = [\![\vdash N]\!](x_1)\cdots(x_n)$$

for LS $x_1, \cdots, x_n$

$(\Rightarrow)$ Suppose $[\![\vdash M]\!]x_1 \cdots x_n \neq [\![\vdash N]\!]x_1 \cdots x_n$ for some LS $x_1, \cdots, x_n$. By Lemma 8 each $x_i = \bigsqcup_j x_i^j$, where x_i^j are definable. Because of continuity, there must exist j such that

$$[\![\vdash M]\!]x_1^j \cdots x_n^j \neq [\![\vdash N]\!]x_1^j \cdots x_n^j.$$

Because x_i^j are definable (let Q_i^j be the corresponding term) we have

$$[\![\vdash MQ_1^j \cdots Q_n^j]\!] \neq [\![\vdash MQ_1^j \cdots Q_n^j]\!].$$

This implies that $MQ_1^j \cdots Q_n^j \Downarrow m \iff MQ_1^j \cdots Q_n^j \Downarrow m$ is violated, i.e. $M \ncong N$.

Full Abstraction summary

Altogether we have found a mathematical characterisation of program equivalence in a restricted case.

Such results are known as *full abstraction* theorems.

- At order 0 and 1 it suffices to compare the corresponding continuous functions.
- At order 2 and 3 the comparison had to be restricted to logically sequential arguments.

How about order 4? Do our methods apply?

Finite types

Imagine that $\mathbf{nat}$ is finite, i.e. $0, \cdots, N$. The resultant language is then called *finitary PCF*.

We can still interpret finitary PCF according to our recipe. Observe that for any type the functions involved will be finite!

Recall that a logically sequential function needs to be invariant under all sequentiality relations. The arity of these relations can be arbitrary but, if we are testing finite functions, say, from $[\![\theta_1 \to \cdots \to \theta_n \to \mathbf{nat}]\!]$, arity of $[\![\theta_1]\!] \times \cdots \times [\![\theta_n]\!]$ will suffice to explore all possibilities and, consequently, detect any possible violation of invariance.

In the finite case, there are finitely many relations of bounded arity. Consequently, testing for logical sequentiality becomes effective! For any type θ, we can determine the logically sequential elements of $[\![\theta]\!]$ (and there will be finitely many of them).

Finite types at order 2 and 3

Theorem. *Let* $\theta = \theta_1 \to \cdots \to \theta_n \to \mathbf{nat}$ *be a type of order at most* 3 *and* $\vdash M, N : \theta$*.* $M \cong N$ *if and only if*

$$[\![\vdash M]\!] x_1 \cdots x_n = [\![\vdash N]\!] x_1 \cdots x_n$$

for all **logically sequential** $x_1 \in [\![\theta_1]\!], \cdots, x_n \in [\![\theta_n]\!]$*.*

In finitary PCF the above result gives us a way of deciding program equivalence at orders up to 3. This is because there are finitely many tuples to explore and we can determine them all.

Finite types at order 4

The approach must fail at order 4 because of the following result.

Theorem 10 (Loader 2001)**.** *Program equivalence in finitary PCF is undecidable (at order 4).*

- The result also means that definability in finitary PCF is undecidable (at order 3), even though the sets involved are finite.
- By Lemma 8 definability is decidable at order $0, 1, 2$ (in finitary PCF). This is because in the finite setting each chain must stabilise. Hence, being logically sequential (at orders 0-2) coincides with being definable.

Loader's result places a limitation on concrete presentations of fully abstract models of PCF (not only the logical relations method).

References

The results we discussed (and more) can be found in [3, 2, 1].

[1] R. Loader. Finitary PCF is not decidable. *Theoretical Computer Science*, 266(1-2):341–364, 2001.

[2] J. C. Mitchell. *Foundations for Programming Languages*. MIT Press, 2000.

[3] K. Sieber. Reasoning about sequential functions via logical relations. In M. P. Fourman *et al*, editor, *Applications of Categories in Computer Science*, volume 177 of *London Mathematical Society Lecture Note Series*, pages 258–269. Cambridge University Press, 1992.