Semantics of Programming Languages

Andrzej Murawski Nikos Tzevelekos

ESSLLI 2011

Slim PCF

Types

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

Terms

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

$$\frac{}{\Gamma \vdash \mathbf{cond} : \mathbf{nat} \to \mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}} \qquad \frac{}{\Gamma \vdash Y_A : (A \to A) \to A}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A . M : A \to B} \qquad \frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

Type order

$$\mathsf{ord}(\mathbf{nat}) = 0 \qquad \mathsf{ord}(A_1 \to A_2) = \max(\mathsf{ord}(A_1) + 1, \mathsf{ord}(A_2))$$

Examples

Order	Type
order 0	$\mathbf{nat}$
order 1	$\mathbf{nat} \to \cdots \to \mathbf{nat}$
order 2	$(\mathbf{nat} \to \cdots \to \mathbf{nat}) \to \cdots \to (\mathbf{nat} \to \cdots \to \mathbf{nat}) \to \mathbf{nat}$
order 3	$((\mathbf{nat} \to \mathbf{nat}) \to \mathbf{nat}) \to \mathbf{nat}$

“at order i”

If a property is said to apply at order i, we mean terms

$$x_1 : A_1, \cdots, x_k : A_k \vdash M : A$$

such that $\mathrm{ord}(A_1 \to \cdots \to A_k \to A) = i$.

A special case is that of $\vdash M : A$, where $\mathrm{ord}(A) = i$.

When reasoning about contextual equivalence, we shall often focus on the special case, but the results can be lifted to open terms through

$$M \cong N \iff \lambda x.M \cong \lambda x.N.$$

Full Abstraction

$$\Gamma \vdash M_1 \cong M_2 : A \quad \not\Rightarrow \quad [\![\Gamma \vdash M_1 : A]\!] = [\![\Gamma \vdash M_2 : A]\!]$$

We already know that $\mathcal{M}$ is not fully abstract.

- However, full abstraction does hold for types of low order.

  $0, 1$

- The model can be refined to regain full abstraction at higher orders.

  $2, 3$

- There exists a fundamental limitation at order 4.

Failure of full abstraction at order 2

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

- Parallel-or is undefinable: 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 $M \cong N$.

- On the other hand, $[\![\vdash M]\!](por) \neq [\![\vdash N]\!](por)$, where

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

Full abstraction fails at $(\mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}) \to \mathbf{nat}$.

What or's are definable?

Definition 1. $\vdash M : \mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}$ *represents* ***or*** *whenever*

$$M00 \Downarrow 0 \qquad M01 \Downarrow 1 \qquad M10 \Downarrow 1 \qquad M11 \Downarrow 1.$$

By Correctness, for $f = [\![\vdash M]\!]$, we then have $f00 = 0$ and $f01 = f10 = f11 = 1$. By monotonicity we must have $f0\bot = f\bot 0 = f\bot\bot = \bot$. How about $f1\bot$ and $f\bot 1$? By monotonicity neither can be 0. So each is $\bot$ or 1.

- $f1\bot = 1$ and $f\bot 1 = \bot$
- $f1\bot = \bot$ and $f\bot 1 = 1$
- $f1\bot = \bot$ and $f\bot 1 = \bot$
- $f1\bot = 1$ and $f\bot 1 = 1$

Definability of or's

- $f1\bot = 1$ and $f\bot 1 = \bot$ (left-or)

$$\lambda x^{\mathbf{nat}}.\lambda y^{\mathbf{nat}}.\mathbf{cond}\, x\, 1\, (\mathbf{cond}\, y\, 1\, 0)$$

- $f1\bot = \bot$ and $f\bot 1 = 1$ (right-or)

$$\lambda x^{\mathbf{nat}}.\lambda y^{\mathbf{nat}}.\mathbf{cond}\, y\, 1\, (\mathbf{cond}\, x\, 1\, 0)$$

- $f1\bot = \bot$ and $f\bot 1 = \bot$ (strict-or)

$$\lambda x^{\mathbf{nat}}.\lambda y^{\mathbf{nat}}.\mathbf{cond}\, x\, (\mathbf{cond}\, y\, 1\, 1)\, (\mathbf{cond}\, y\, 1\, 0)$$

- $f1\bot = 1$ and $f\bot 1 = 1$ (parallel-or)

Full Abstraction at order 0

- **Context Lemma**: $\vdash M \cong N : A_1 \to \cdots \to A_k \to \mathbf{nat}$ if and only if for all $n \in \mathbb{N}$, $\vdash Q_1 : A_1, \cdots, \vdash Q_k : A_k$:

$$MQ_1 \cdots Q_k \Downarrow n \iff NQ_1 \cdots Q_k \Downarrow n.$$

- **Correctness and Computational Adequacy**: for any $\vdash M : \mathbf{nat}$

$$M \Downarrow n \iff [\![\vdash M]\!] = n.$$

Suppose $\vdash M, N : \mathbf{nat}$. By Context Lemma $M \cong N$ boils down to

$$M \Downarrow n \iff N \Downarrow n.$$

By Correctness and Adequacy this is equivalent to $[\![\vdash M]\!] = [\![\vdash N]\!]$.

So, we have full abstraction at order 0!

Full Abstraction at order 1

Let $M, N : \underbrace{\mathbf{nat} \to \cdots \to \mathbf{nat}}_{k} \to \mathbf{nat}$ such that $M \cong N$. We would like to show $[\![\vdash M]\!] = [\![\vdash N]\!]$.

- Let $y_1, \cdots, y_k \in [\![\mathbf{nat}]\!]$, i.e. $y_i \in \mathbb{N}_\perp$. Let $\vdash Q_i : \mathbf{nat}$ be such that $[\![\vdash Q_i]\!] = y_i$.

$$Q_i \equiv \begin{cases} y_i & y_i \in \mathbb{N} \\ \Omega & y_i = \perp \end{cases}$$

- Context Lemma: $MQ_1 \cdots Q_k \Downarrow n \iff NQ_1 \cdots Q_k \Downarrow n$.
- Correctness/Adequacy: $[\![\vdash MQ_1 \cdots Q_k]\!] = [\![\vdash NQ_1 \cdots Q_k]\!]$.

$$[\![\vdash M]\!]y_1 \cdots y_k = [\![\vdash M]\!][\![\vdash Q_1]\!] \cdots [\![\vdash Q_k]\!] = [\![\vdash MQ_1 \cdots Q_k]\!]$$
$$[\![\vdash N]\!]y_1 \cdots y_k = [\![\vdash N]\!][\![\vdash Q_1]\!] \cdots [\![\vdash Q_k]\!] = [\![\vdash NQ_1 \cdots Q_k]\!]$$

$[\![\vdash M]\!] = [\![\vdash N]\!]$ follows.

Full Abstraction in general

- What fails in the previous argument at higher orders?
- The passage $y_i \mapsto Q_i$ is impossible, e.g. when y_i corresponds to the parallel-or function.

General definability would be useful, but perhaps too ambitious/strong. However, if we knew that $y = \bigsqcup_i d_i$, where each d_i is definable, we could reason as follows (we assume $k = 1$ for clarity).

$$[\![\vdash M]\!]y = [\![\vdash M]\!](\bigsqcup_i d_i) = [\![\vdash M]\!](\bigsqcup_i [\![\vdash Q_{d_i}]\!]) =$$
$$\bigsqcup_i ([\![\vdash M]\!][\![\vdash Q_{d_i}]\!]) = \bigsqcup_i ([\![\vdash MQ_{d_i}]\!]).$$

So, to prove full abstraction, it suffices when each element of the domain of $[\![\vdash M]\!]$ is approximable via definable elements.

Full Abstraction at a 3rd order type

Full Abstraction failed at $(\mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}) \to \mathbf{nat}$.

Consider $(\mathbf{nat} \to \mathbf{nat}) \to \mathbf{nat}$ instead.

Any $f \in [\![\vdash \mathbf{nat} \to \mathbf{nat}]\!]$ is equal to $\bigsqcup_i g_i$ defined as follows.

$$g_i(x) = \begin{cases} f(x) & x \leq i \\ \bot & x > i \end{cases}$$

Consequenty, the method from the previous slide applies.

Note that not all functions from

$$[\![\vdash \mathbf{nat} \to \mathbf{nat}]\!]$$

are definable. In fact some are not even computable.

The rest of the course

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

Logical relations

Definition 2. *A logical relation (of arity m) R is a family $\{R_A\}_{A \in Types}$ of relations*

$$R^A \subseteq \underbrace{[\![A]\!] \times \cdots \times [\![A]\!]}_{m}$$

such that $R^{A_1 \to A_2}(f_1, \cdots, f_m)$ if and only if $R^{A_1}(x_1, \cdots, x_m)$ entails $R^{A_2}(f_1 x_1, \cdots, f_m x_m)$ for all $(x_1, \cdots, x_m) \in [\![A_1]\!]^m$.

Slogan: related functions take related arguments to related results.

Observation 3. *A logical relation is uniquely determined by $R^{\mathbf{nat}}$: if $\{R_1^A\}_{A \in Types}$, $\{R_2^A\}_{A \in Types}$ are logical relations and $R_1^{\mathbf{nat}} = R_2^{\mathbf{nat}}$ then $R_1^A = R_2^A$ for all types A.*

Logical relations - function types

Observation 4. *Let* $A = A_1 \to \cdots \to A_n \to \mathbf{nat}$.

Then

$$R^A(g_1, \cdots, g_m)$$

if and only if, for all

$$(x_{11}, \cdots, x_{m1}) \in [\![A_1]\!]^m, \quad \cdots \quad , (x_{1n}, \cdots, x_{mn}) \in [\![A_n]\!]^m,$$

if

$$R^{A_1}(x_{11}, \cdots, x_{m1}), \cdots, R^{A_n}(x_{1n}, \cdots, x_{mn})$$

then

$$R^{\mathbf{nat}}(g_1 x_{11} \cdots x_{1n}, \cdots, g_m x_{m1} \cdots x_{mn}).$$

Logical relations - closure under lub's

Logical relationships are preserved by least upper bounds.

Lemma 5. *Let R be a logical relation and, for any $i \in \mathbb{N}$, let $(x_{1i}, \cdots, x_{mi}) \in [\![A]\!]^m$ be such that $R^A(x_{1i}, \cdots, x_{mi})$. Assume further that*

$$x_{j0} \sqsubseteq x_{j1} \sqsubseteq x_{j2} \sqsubseteq x_{j3} \sqsubseteq x_{j4} \sqsubseteq \cdots$$

for all $1 \leq j \leq m$. Then

$$R^A(\bigsqcup_i x_{1i}, \cdots, \bigsqcup_i x_{mi}).$$

Proof of Lemma 5 (nat)

If $\forall_i R^A(x_{1i}, \cdots, x_{mi})$ then $R^A(\bigsqcup_i x_{1i}, \cdots, \bigsqcup_i x_{mi})$.

By induction on the structure of A.

- $A = \mathbf{nat}$

  Observe that there exists $k \in \mathbb{N}$ such that

$$(\bigsqcup_i x_{1i}, \cdots, \bigsqcup_i x_{mi}) = (x_{1k}, \cdots, x_{mk}).$$

  By assumption $R^A(x_{1k}, \cdots, x_{mk})$ and the Lemma follows.

Proof of Lemma 5 (function types)

If $\forall_i R^A(x_{1i}, \cdots, x_{mi})$ then $R^A(\bigsqcup_i x_{1i}, \cdots, \bigsqcup_i x_{mi})$.

- $A = A_1 \to A_2$

  Assuming $R^{A_1}(y_1, \cdots, y_m)$ we need to show

  $$R^{A_2}((\bigsqcup_i x_{1i})y_1, \cdots, (\bigsqcup_i x_{mi})y_m).$$

  This is the same as $R^{A_2}(\bigsqcup_i (x_{1i}y_1), \cdots, \bigsqcup_i (x_{mi}y_m))$. Note that

  $$x_{j0}y_j \sqsubseteq x_{j1}y_j \sqsubseteq x_{j2}y_j \sqsubseteq \cdots$$

  and $R^{A_2}(x_{1i}y_1, \cdots, x_{mi}y_m)$ for all $i \in \mathbb{N}$. Hence we can use IH for A_2 and conclude exactly what we need.

Logical invariance

Definition 6. *Let R be a logical relation, A - a type and $d \in [\![A]\!]$. Then d is invariant under R iff $R^A(\underbrace{d, \cdots, d}_{m})$.*

The concept of invariance will turn out useful for tracking undefinable elements. This is thanks to the following result.

Lemma 7 (Main Logical Relations Lemma)**.** *Let R be a logical relation such that $R([\![\vdash\ c]\!], \cdots, [\![\vdash\ c]\!])$ for all PCF-constants c. Then*

$$R([\![\vdash\ M]\!], \cdots, [\![\vdash\ M]\!]).$$

An approach to undefinability

Suppose we want to show that for some $d \in [\![A]\!]$ there is no $\vdash M : A$ such that $[\![\vdash M]\!] = d$.

We can try the following recipe.

1. Find a logical relation R. By Observation 3 this amounts to exhibiting $R^{\mathbf{nat}}$.
2. Check that $R([\![\vdash c]\!], \cdots, [\![\vdash c]\!])$.
3. Check that $R(d, \cdots, d)$ fails.

By Lemma 7, d cannot then be definable.

This approach will turn out very fruitful!

Proving $R^{(A\to A)\to A}([\![Y_A]\!],\cdots,[\![Y_A]\!])$

It suffices to show that $R^{\mathbf{nat}}(\bot_{[\![\mathbf{nat}]\!]},\cdots,\bot_{[\![\mathbf{nat}]\!]})$!

- The above turns out to imply $R^A(\bot_{[\![A]\!]},\cdots,\bot_{[\![A]\!]})$ for any A (induction on A).
  - $R^{\mathbf{nat}}(\bot_{[\![\mathbf{nat}]\!]},\cdots,\bot_{[\![\mathbf{nat}]\!]})$
  - $R^{A_1\to A_2}(\bot_{[\![A_1\to A_2]\!]},\cdots,\bot_{[\![A_1\to A_2]\!]})$ follows from $R^{A_2}(\bot_{[\![A_2]\!]},\cdots,\bot_{[\![A_2]\!]})$.
- Now suppose $R^{A\to A}(f_1,\cdots,f_m)$. Because $R^A(\bot_{[\![A]\!]},\cdots,\bot_{[\![A]\!]})$, we obtain $R^A(f_1\bot_A,\cdots,f_m\bot_A)$ and, more generally, $R^A(f_1^i\bot_A,\cdots,f_m^i\bot_A)$.

  By Lemma 5, $R^A(\bigsqcup_i(f_1^i\bot_A),\cdots,\bigsqcup_i(f_m^i\bot_A))$, i.e. $R^A([\![Y_A]\!]\,f_1,\cdots,[\![Y_A]\!]\,f_m)$.

Parallel-or is undefinable

Lemma 8. *There is no definable function* $f \in [\![\mathbf{nat} \to \mathbf{nat} \to \mathbf{nat}]\!]$ *such that*

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

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

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

- $R^{\mathbf{nat}}(\bot,\bot,\bot)$ ✓
- $R^{\mathbf{nat}}(n,n,n)$ ✓
- $R^{\mathbf{nat}\to\mathbf{nat}}([\![\mathbf{succ}]\!],[\![\mathbf{succ}]\!],[\![\mathbf{succ}]\!])$

  If $R^{\mathbf{nat}}(x,y,z)$ then $R^{\mathbf{nat}}([\![\mathbf{succ}]\!]\,x,[\![\mathbf{succ}]\!]\,y,[\![\mathbf{succ}]\!]\,z)$.

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

  In each case $R^{\mathbf{nat}}([\![\mathbf{succ}]\!]\,x,[\![\mathbf{succ}]\!]\,y,[\![\mathbf{succ}]\!]\,z)$, because $[\![\mathbf{succ}]\!]\,\bot = \bot$. ✓

All PCF constants are invariant under R

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

- $R^{\mathbf{nat}\to\mathbf{nat}}([\![\mathbf{pred}]\!],[\![\mathbf{pred}]\!],[\![\mathbf{pred}]\!])$ (same as **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 $R^{\mathbf{nat}}(x_R,y_R,z_R)$
  - $x=\bot$: $[\![\mathbf{cond}]\!]xx_Lx_R=\bot$
  - $y=\bot$: $[\![\mathbf{cond}]\!]yy_Ly_R=\bot$

✓

Logical Relations Lemma

Let R be a logical relation, A - a type and $d \in [\![\vdash\ A]\!]$. Then d is invariant under R iff $R^A(\underbrace{d, \cdots, d}_{m})$.

Lemma (Main Logical Relations Lemma)**.** *Let R be a logical relation. Assume that for all constants $\vdash\ c : A_c$ we have*

$$R^{A_c}([\![\vdash\ c]\!], \cdots, [\![\vdash\ c]\!]).$$

Then for any closed term $\vdash\ M : A$

$$R^A([\![\vdash\ M]\!], \cdots, [\![\vdash\ M]\!]).$$

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

$$\frac{}{\lambda x_1^{A_1} \cdots x_k^{A_k}.x_i : A_1 \to \cdots \to A_k \to A_i}$$

$$\frac{\vdash\ c : A_c}{\lambda x_1^{A_1} \cdots x_k^{A_k}.c : A_1 \to \cdots \to A_k \to A_c}$$

$$\frac{\lambda x_1^{A_1} \cdots x_j^{A_j} x_{j+1}^{A_{j+1}} \cdots x_k^{A_k}.M : A_1 \to \cdots A_j \to A_{j+1} \to \cdots \to A_k \to A}{\lambda x_1^{A_1} \cdots x_{j+1}^{A_{j+1}} x_j^{A_j} \cdots x_k^{A_k}.M : A_1 \to \cdots A_{j+1} \to A_j \to \cdots \to A_k \to A}$$

$$\frac{\begin{array}{c}\lambda x_1^{A_1} \cdots x_k^{A_k}.M : A_1 \to \cdots \to A_k \to A \to B \\ \lambda x_1^{A_1} \cdots x_k^{A_k}.N : A_1 \to \cdots \to A_k \to A\end{array}}{\lambda x_1^{A_1} \cdots x_k^{A_k}.MN : A_1 \to \cdots \to A_k \to B}$$

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

Proof of Lemma 6

If $R^{A_c}([\![\vdash\ c]\!], \cdots, [\![\vdash\ c]\!])$ then $R^{A}([\![\vdash\ M]\!], \cdots, [\![\vdash\ M]\!])$.

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 Lemma 6 (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 $R^{A_i}(x_1^i, \cdots, x_m^i)$ for $i = 1, \cdots, k$ we should show

$$R^B([\![Q]\!]x_1^1 \cdots x_1^k, \cdots, [\![Q]\!]x_m^1 \cdots x_m^k).$$

By IH for Q_f and Q_a

$$R^{A \to B}([\![Q_f]\!]x_1^1 \cdots x_1^k, \cdots, [\![Q_f]\!]x_m^1 \cdots x_m^k),$$
$$R^A([\![Q_a]\!]x_1^1 \cdots x_1^k, \cdots, [\![Q_a]\!]x_m^1 \cdots x_m^k).$$

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 $R^B([\![Q]\!]x_1^1 \cdots x_1^k, \cdots, [\![Q]\!]x_m^1 \cdots x_m^k)$ follows.

Sequentiality relations

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

Definition 9. *Let R be a logical relation. R is called a* sequentiality relation *whenever $R([\![\vdash c]\!], \cdots, [\![\vdash c]\!])$ for all PCF constants.*

Definition 10. *$f \in [\![A]\!]$ is a* logically sequential function *whenever $R^A(f, \cdots, f)$ 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 11. *Let A be a type order 1 or 2, i.e. $A = A_1 \to \cdots \to A_n \to \mathbf{nat}$, where $A_1, \cdots, A_n$ are of order at most 1. Let $f \in [\![A]\!]$ be a logically sequential function. Suppose*

$$(x_1^i, \cdots, x_n^i) \in [\![A_1]\!] \times \cdots \times [\![A_n]\!]$$

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

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

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

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

Proof of Lemma 11

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

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 $R^A(f, \cdots, f)$.

  If we knew that

  $$R^{A_1}(x_1^1, \cdots, x_1^m), \cdots, R^{A_n}(x_n^1, \cdots, x_n^m)$$

  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 $R^{A_j}(x_j^1, \cdots, x_j^m)$.

Proof of Lemma 11 (ii)

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

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

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

Suppose $A_j = \mathbf{nat}$. It suffices to find $M : A$ 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 11 (iii)

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

Suppose $A_j = \underbrace{\mathbf{nat} \to \cdots \to \mathbf{nat}}_{k} \to \mathbf{nat}$. 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!

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

  We want to show $R^{A_j}(x_j^1, \cdots, x_j^m)$. 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.

- $R^{\mathbf{nat}}(\bot, \cdots, \bot)$

  $$M \equiv \lambda x_1 \cdots x_n . \Omega_{\mathbf{nat}}$$

- $R^{\mathbf{nat}}(u, \cdots, u)$

  $$M \equiv \lambda x_1 \cdots x_n . u$$

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

  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 logically sequential (ii)

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

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

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

The first step will be to prove that identity functions can be approximated in this way.

Lemma 12. *For any A, there exists a chain $\{d_i^A\}$ in $[\![A \to A]\!]$ such that each d_i is definable and $\bigsqcup_i d_i^A = \mathsf{id}_A$. Moreover, $\mathsf{Im}(d_i^A)$ is finite.*

$$d_i^{\mathbf{nat}}(x) = \begin{cases} x & x \leq i \\ \bot & x > i \end{cases} \qquad d_i^{A_1 \to A_2}(x) = d_i^{A_2} \circ x \circ d_i^{A_1}$$

It is easy to see that $\mathsf{Im}(d_i^A)$ is always finite.

Proof of Lemma 12

- definability

$$\begin{array}{rcl} M^i_{\mathbf{nat}} & = & \lambda x^{\mathbf{nat}}.\mathbf{cond}\, x\ \cdots \\ M^i_{A_1 \to A_2} & = & \lambda f^{A_1 \to A_2}.\lambda x^{A_1}.M^i_{A_2}(f(M^i_{A_1} x)) \end{array}$$

- $\bigsqcup_i d^A_i = id_A$
  - $A = \mathbf{nat}$

$$d^{\mathbf{nat}}_i(x) = \begin{cases} x & x \leq i \\ \bot & x > i \end{cases}$$

Proof of Lemma 12 (ii)

$$\bigsqcup_i d_i^A = id_A$$

- $A = A_1 \to A_2$

$$\begin{array}{rcl} L(x) & = & (\bigsqcup_i d^i_{A_1 \to A_2})(x) = \bigsqcup_i (d^i_{A_2} \circ x \circ d^i_{A_1}) \\ R(x) & = & id_{A_1 \to A_2}(x) = (id_{A_1} \circ x \circ id_{A_2}) = \\ & = & (\bigsqcup_i d^i_{A_2}) \circ x \circ (\bigsqcup_j d^j_{A_1}) = \bigsqcup_i \bigsqcup_j (d^i_{A_2} \circ x \circ d^j_{A_1}) \end{array}$$

Because $L \sqsupseteq d^i_{A_2} \circ f \circ d^j_{A_1}$, we have $L \sqsupseteq R$.
Because $R \sqsupseteq d^i_{A_2} \circ x \circ d^i_{A_1}$ we have $R \sqsupseteq L$.

Hence $L = R$ and

$$id_A = \bigsqcup_i d_i^A.$$

Definability for logically sequential functions

Lemma 13. *Let A be a type of order 1 or 2. Let $f \in [\![A]\!]$ be a logically sequential element. Then there exists a chain $\{f_i\}$ in $[\![A]\!]$ of definable elements such that $f = \bigsqcup_i f_i$.*

Observe that

$$f = id_A(f) = (\bigsqcup_i d^i_A)(f) = \bigsqcup_i d^i_A(f)$$

so we could take $f_i = d^i_A(f)$. But is f_i definable?

f_i is definable

Suppose $A = A_1 \to \cdots \to A_n \to \mathbf{nat}$. Let

$$(x_1, \cdots, x_n) \in [\![A_1]\!] \times \cdots \times [\![A_n]\!].$$

Then

$$f_i x_1 \cdots x_n = (d^i_A f) x_1 \cdots x_n = d^i_{\mathbf{nat}}(f(d^i_{A_1} x_1) \cdots (d^i_{A_n} x_n)).$$

Invoke Lemma 11 for all

$$(y_1, \cdots, y_n) \in d^i_{A_1}([\![A_1]\!]) \times \cdots \times d^i_{A_n}([\![A_n]\!]).$$

to obtain M such that

$$[\![\vdash M]\!] y_1 \cdots y_n = f\, y_1 \cdots y_n.$$

Note that we exploit the finiteness of images of d^i_A.

f_i is definable (ii)

Known:

$$\begin{array}{rcll} f_i x_1 \cdots x_n & = & d^i_{\mathbf{nat}}(f(d^i_{A_1} x_1) \cdots (d^i_{A_n} x_n)) & x_j \in [\![A_j]\!] \\ [\![\vdash M]\!] y_1 \cdots y_n & = & f y_1 \cdots y_n & y_j \in d^i_{A_j}([\![A_j]\!]) \end{array}$$

Then

$$\begin{aligned} f_i x_1 \cdots x_n &= d^i_{\mathbf{nat}}([\![\vdash M]\!](d^i_{A_1} x_1) \cdots (d^i_{A_n} x_n)) \\ &= (d^i_A [\![\vdash M]\!]) x_1 \cdots x_n \\ &= ([\![\vdash M^i_A M]\!]) x_1 \cdots x_n. \end{aligned}$$

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

Full Abstraction at order 2 and 3

Let $A = A_1 \to \cdots \to A_n \to \mathbf{nat}$ be a type of order at most 3 and $\vdash M, N : A$. Recall that the following failed.

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

$[\![\vdash M]\!] = [\![\vdash N]\!]$ means $[\![\vdash M]\!]x_1 \cdots x_n = [\![\vdash N]\!]x_1 \cdots x_n$ for all $x_1 \in [\![A_1]\!], \cdots, x_n \in [\![A_n]\!]$. Now we can repair the above failure!

Theorem 14. *$M \cong N$ if and only if*

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

for all **logically sequential** $x_1 \in [\![A_1]\!], \cdots, x_n \in [\![A_n]\!]$.

Proof of Theorem 14

$M \cong N$ iff $[\![\vdash\ M]\!]x_1 \cdots x_n = [\![\vdash\ N]\!]x_1 \cdots x_n$ **for LS** $x_1, \cdots, x_n$

$\Leftarrow$

We use the Context Lemma. Take $\vdash\ Q_1 : A_1, \cdots, \vdash\ Q_n : A_n$. Then:

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

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 14

$M \cong N$ iff $[\![\vdash\ M]\!]x_1 \cdots x_n = [\![\vdash\ N]\!]x_1 \cdots x_n$ **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 13 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. $M \not\cong N$.

Full Abstraction summary

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

Such results are known as *full abstraction* theorems.

- At order 0 and 1 it sufficed 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 $[\![A_1 \to \cdots \to A_n \to \mathbf{nat}]\!]$, arity of $[\![A_1]\!] \times \cdots \times [\![A_n]\!]$ 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 A, we can determine the logically sequential elements of $[\![A]\!]$ (and there will be finitely many of them).

Finite types at order 2 and 3

Theorem. *Let* $A = A_1 \to \cdots \to A_n \to \mathbf{nat}$ *be a type of order at most* 3 *and* $\vdash M, N : A$. $M \cong N$ *if and only if*

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

for all **logically sequential** $x_1 \in [\![A_1]\!], \cdots, x_n \in [\![A_n]\!]$.

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 for order 4 because of the following result.

Theorem 15 (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 13 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.

Sequentiality relations explicitly

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

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

Theorem 16. *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 $S^m_{A,B}$.*

References

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

[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.