Fundamental property of the relations $\lhd_\tau$

Proposition. *If* $\Gamma \vdash M : \tau$ *is a valid PCF typing, then for all* Γ*-environments* ρ *and all* Γ*-substitutions* σ

$$\rho \lhd_\Gamma \sigma \;\Rightarrow\; [\![\Gamma \vdash M]\!](\rho) \lhd_\tau M[\sigma]$$

- $\rho \lhd_\Gamma \sigma$ means that $\rho(x) \lhd_{\Gamma(x)} \sigma(x)$ holds for each $x \in dom(\Gamma)$.
- $M[\sigma]$ is the PCF term resulting from the simultaneous substitution of $\sigma(x)$ for x in M, each $x \in dom(\Gamma)$.

NB. $M_1 \cong_{ctx} M_2$ iff $M_1 \leq_{ctx} M_2$ and $M_2 \leq_{ctx} M_1$.

Contextual preorder between PCF terms

Given PCF terms M_1, M_2, PCF type τ, and a type environment Γ, the relation $\Gamma \vdash M_1 \leq_{\mathrm{ctx}} M_2 : \tau$ is defined to hold iff

- Both the typings $\Gamma \vdash M_1 : \tau$ and $\Gamma \vdash M_2 : \tau$ hold.
- For all PCF contexts $\mathcal{C}$ for which $\mathcal{C}[M_1]$ and $\mathcal{C}[M_2]$ are closed terms of type γ, *where* $\gamma = nat$ *or* $\gamma = bool$, and for all values $V \in \mathrm{PCF}_\gamma$,

$$\mathcal{C}[M_1] \Downarrow_\gamma V \implies \mathcal{C}[M_2] \Downarrow_\gamma V \ .$$

Fact: $M_1 \leq_{ctx} M_2$ iff $[\![M_1]\!] \lhd M_2$

Cor. $M_1, M_2 : \tau_1 \to \tau_2 \to \cdots \to \tau_n \to \gamma$

Extensionality properties of $\leq_{\mathrm{ctx}}$

$M_1 \leq_{ctx} M_2$ iff $\forall N_1 \ldots N_n .\ M_1 N_1 \ldots N_n \Downarrow V \Rightarrow M_2 N_1 \ldots N_n \Downarrow V$

We need only look at APPLICATIVE contexts, i.e. $[\ ]\, N_1 \ldots N_n$

At a ground type $\gamma \in \{bool, nat\}$,

$M_1 \leq_{\mathrm{ctx}} M_2 : \gamma$ holds if and only if

$$\forall\, V \in \mathrm{PCF}_\gamma\ (M_1 \Downarrow_\gamma V \implies M_2 \Downarrow_\gamma V)\ .$$

At a function type $\tau \to \tau'$,

$M_1 \leq_{\mathrm{ctx}} M_2 : \tau \to \tau'$ holds if and only if

$$\forall\, M \in \mathrm{PCF}_\tau\ (M_1\, M \leq_{\mathrm{ctx}} M_2\, M : \tau')\ .$$

Topic 8

Full Abstraction

? Could it be that there are $M_1 \cong_{ctx} M_2$ but $[\![M_1]\!] \neq [\![M_2]\!]$?

Proof principle

For all types τ and closed terms $M_1, M_2 \in \mathrm{PCF}_\tau$,

$$[\![M_1]\!] = [\![M_2]\!] \text{ in } [\![\tau]\!] \implies M_1 \cong_{\mathrm{ctx}} M_2 : \tau \ .$$

Hence, to prove

$$M_1 \cong_{\mathrm{ctx}} M_2 : \tau$$

it suffices to establish

$$[\![M_1]\!] = [\![M_2]\!] \text{ in } [\![\tau]\!] \ .$$

Full abstraction

A denotational model is said to be *fully abstract* whenever denotational equality characterises contextual equivalence.

Full abstraction

A denotational model is said to be *fully abstract* whenever denotational equality characterises contextual equivalence.

- The domain model of PCF is *not* fully abstract.

  In other words, there are contextually equivalent PCF terms with different denotations.

$\forall M \in \mathrm{PCF}_{bool \to bool \to bool}.\ T_1 M \Downarrow V \iff T_2 M \Downarrow V.$

$\Downarrow$

Failure of full abstraction, idea

We will construct two closed terms $\forall M.\ [\![T_1]\!]([\![M]\!]) = [\![T_2]\!]([\![M]\!])$

$$T_1, T_2 \in \mathrm{PCF}_{(bool\to(bool\to bool))\to bool}$$

such that

$$T_1 \cong_{\mathrm{ctx}} T_2$$

N.B. Higher type of binary Boolean functions.

and

$$[\![T_1]\!] \neq [\![T_2]\!]$$

There will be $f \in (B_\perp \to (B_\perp \to B))$

s.t. $[\![T_1]\!] f \neq [\![T_2]\!] f$ necessarily $f \neq [\![M]\!]\ \forall M$

- We achieve $T_1 \cong_{\mathrm{ctx}} T_2$ by making sure that

$$\forall\, M \in \mathrm{PCF}_{bool \to (bool \to bool)}\, (\, T_1\, M \not\Downarrow_{bool}\ \&\ T_2\, M \not\Downarrow_{bool}\,)$$

- We achieve $T_1 \cong_{\mathrm{ctx}} T_2$ by making sure that

$$\forall\, M \in \mathrm{PCF}_{bool\to(bool\to bool)}\;(\,T_1\, M \not\Downarrow_{bool} \;\&\; T_2\, M \not\Downarrow_{bool}\,)$$

Hence,

$$[\![T_1]\!]([\![M]\!]) = \bot = [\![T_2]\!]([\![M]\!])$$

for all $M \in \mathrm{PCF}_{bool\to(bool\to bool)}$.

- We achieve $T_1 \cong_{\mathrm{ctx}} T_2$ by making sure that

$$\forall\, M \in \mathrm{PCF}_{bool \to (bool \to bool)}\ (\, T_1\, M \not\Downarrow_{bool}\ \&\ T_2\, M \not\Downarrow_{bool}\,)$$

  Hence,

$$[\![T_1]\!]([\![M]\!]) = \bot = [\![T_2]\!]([\![M]\!])$$

  for all $M \in \mathrm{PCF}_{bool \to (bool \to bool)}$.

- We achieve $[\![T_1]\!] \neq [\![T_2]\!]$ by making sure that

$$[\![T_1]\!](por) \neq [\![T_2]\!](por)$$

  for some *non-definable* continuous function

$$por \in (\mathbb{B}_\bot \to (\mathbb{B}_\bot \to \mathbb{B}_\bot))\ .$$

$\forall M : bool \to bool \to bool .\ por \neq [\![M]\!]$

Parallel-or function

is the unique continuous function $por : \mathbb{B}_\perp \to (\mathbb{B}_\perp \to \mathbb{B}_\perp)$ such that

$$\begin{array}{lcl} por\ \ true\ \ \perp & = & true \\ por\ \ \perp\ \ true & = & true \\ por\ \ false\ \ false & = & false \end{array}$$

is non-definable in PCF

Parallel-or function

is the unique continuous function $por : \mathbb{B}_\perp \to (\mathbb{B}_\perp \to \mathbb{B}_\perp)$ such that

$$
\begin{aligned}
por\ true\ \perp &= true \\
por\ \perp\ true &= true \\
por\ false\ false &= false
\end{aligned}
$$

In which case, it necessarily follows by monotonicity that

$$
\begin{aligned}
por\ true\ true &= true & \qquad por\ false\ \perp &= \perp \\
por\ true\ false &= true & \qquad por\ \perp\ false &= \perp \\
por\ false\ true &= true & \qquad por\ \perp\ \perp &= \perp
\end{aligned}
$$

Aim: Define T_1 & T_2 s.t. $[\![T_1]\!](por) \neq [\![T_2]\!](por)$

and $\forall M.\ T_1 M \not\Downarrow \Leftrightarrow T_2 M \not\Downarrow$

Undefinability of parallel-or

Proposition. *There is no closed PCF term*

$$P : bool \to (bool \to bool)$$

satisfying

$$[\![P]\!] = por : \mathbb{B}_\perp \to (\mathbb{B}_\perp \to \mathbb{B}_\perp)\ .$$

Parallel-or test functions

Parallel-or test functions

For $i = 1, 2$ define

$$
\begin{aligned}
T_i \stackrel{\text{def}}{=}\ & \mathbf{fn}\ f : bool \to (bool \to bool)\ . \\
& \quad \mathbf{if}\ (f\ \mathbf{true}\ \Omega)\ \mathbf{then} \\
& \qquad \mathbf{if}\ (f\ \Omega\ \mathbf{true})\ \mathbf{then} \\
& \qquad\quad \mathbf{if}\ (f\ \mathbf{false}\ \mathbf{false})\ \mathbf{then}\ \Omega\ \mathbf{else}\ B_i \\
& \qquad \mathbf{else}\ \Omega \\
& \quad \mathbf{else}\ \Omega
\end{aligned}
$$

where $B_1 \stackrel{\text{def}}{=} \mathbf{true}$, $B_2 \stackrel{\text{def}}{=} \mathbf{false}$,

and $\Omega \stackrel{\text{def}}{=} \mathbf{fix}(\mathbf{fn}\ x : bool\ .\ x)$. ~ The divergent computation

$[\![\Omega]\!] = fix(id) = \bot$ $\qquad$ $\Omega \Downarrow\!\!\!\!/$

$\mathbf{fix}\,(\mathbf{fn}\ x.\ x) \not\Downarrow$

Suppose by contradiction $\mathbf{fix}\,(\mathbf{fn}\ x.\ x) \Downarrow V$

Take the minimal derivation for it:

$$\dfrac{(\mathbf{fn}\ x.x) \Downarrow (\mathbf{fn}\ x.x) \qquad \dfrac{↯}{x\left[{}^{\mathbf{fix}(\mathbf{fn}\ x.x)}/_{x}\right] \Downarrow V}\ \ \Omega = \mathbf{fix}(\mathbf{fn}\ x.x)}{(\mathbf{fn}\ x.x)\ (\mathbf{fix}(\mathbf{fn}\ x.x)) \Downarrow V}$$

$$\overline{\Omega = \mathbf{fix}\,(\mathbf{fn}\ x.\ x) \Downarrow V}$$

Failure of full abstraction

Proposition.

$$T_1 \cong_{\text{ctx}} T_2 : (bool \to (bool \to bool)) \to bool$$

$$[\![T_1]\!] \neq [\![T_2]\!] \in (\mathbb{B}_\perp \to (\mathbb{B}_\perp \to \mathbb{B}_\perp)) \to \mathbb{B}_\perp$$

PCF+por

Expressions $M ::= \cdots \mid \mathbf{por}(M, M)$

Typing

$$\frac{\Gamma \vdash M_1 : bool \quad \Gamma \vdash M_2 : bool}{\Gamma \vdash \mathbf{por}(M_1, M_2) : bool}$$

Evaluation

$$\frac{M_1 \Downarrow_{bool} \mathbf{true}}{\mathbf{por}(M_1, M_2) \Downarrow_{bool} \mathbf{true}} \qquad \frac{M_2 \Downarrow_{bool} \mathbf{true}}{\mathbf{por}(M_1, M_2) \Downarrow_{bool} \mathbf{true}}$$

$$\frac{M_1 \Downarrow_{bool} \mathbf{false} \quad M_2 \Downarrow_{bool} \mathbf{false}}{\mathbf{por}(M_1, M_2) \Downarrow_{bool} \mathbf{false}}$$

Plotkin's full abstraction result

The denotational semantics of PCF+por is given by extending that of PCF with the clause

$$[\![\Gamma \vdash \mathbf{por}(M_1, M_2)]\!](\rho) \stackrel{\text{def}}{=} por\big([\![\Gamma \vdash M_1]\!](\rho)\big)\big([\![\Gamma \vdash M_2]\!](\rho)\big)$$

This denotational semantics is fully abstract for contextual equivalence of PCF+por terms:

$$\Gamma \vdash M_1 \cong_{\mathrm{ctx}} M_2 : \tau \;\Leftrightarrow\; [\![\Gamma \vdash M_1]\!] = [\![\Gamma \vdash M_2]\!].$$

(*ii*) For PCF terms M and N with respective typings $\Gamma \vdash M : \tau \to \alpha$ and $\Gamma \vdash N : \alpha \to \sigma$, let $N \circ M$ be the PCF term $\mathbf{fn}\ x : \tau.\ N\,(M\,x)$, where $x \notin \mathrm{dom}(\Gamma)$, with typing $\Gamma \vdash N \circ M : \tau \to \sigma$.

State whether or not if $\Gamma \vdash M \cong_{\mathrm{ctx}} M' : \tau \to \alpha$ and $\Gamma \vdash N \cong_{\mathrm{ctx}} N' : \alpha \to \sigma$ then $\Gamma \vdash N \circ M \cong_{\mathrm{ctx}} N' \circ M' : \tau \to \sigma$. Justify your answer. [5 marks]

$M \cong M' \iff \forall \mathcal{C}.\ \mathcal{C}[M] \Downarrow V$
$\iff \mathcal{C}[M'] \Downarrow V$

$M \circ N = \lambda x.\ M(Nx)$

$M \cong M' \ \&\ N \cong N' \overset{?}{\Longrightarrow} M \circ N \cong M' \circ N'$

Let $\mathcal{C}$ and consider $\mathcal{C}[\lambda x. M(Nx)] \Downarrow V \overset{?}{\Longrightarrow} \mathcal{C}[\lambda x M'(N'x)] \Downarrow V$

$= \mathcal{C}'[M]$

$\mathcal{C}' = \mathcal{C}[\lambda x. [\,](Nx)]$

$\Downarrow\ \mathcal{C}'[M'] \Downarrow V$

$= \mathcal{C}[\lambda x\, M'(Nx)] = \mathcal{C}''[N]$

$\mathcal{C}'' = \mathcal{C}[\lambda x. M'([\,]x)]$

$\Downarrow\ \mathcal{C}''[N'] \Downarrow V$

$= \mathcal{C}[\lambda x. M'(N'x)]$

or otherwise, show that the function ε from $(\mathbb{N}_\perp \to \mathbb{B}_\perp)$ to $\mathbb{B}_\perp$ given by

$$\varepsilon(P) \stackrel{\text{def}}{=} \begin{cases} \mathit{true} & \text{if } \exists\, n \in \mathbb{N}.\ P(n) = \mathit{true} \\ \mathit{false} & \text{if } \forall\, n \in \mathbb{N}.\ P(n) = \mathit{false} \\ \perp & \text{otherwise} \end{cases} \qquad \big(P \in (\mathbb{N}_\perp \to \mathbb{B}_\perp)\big)$$

is not continuous. Argue as to whether or not ε is definable by a closed term of type $(\mathit{nat} \to \mathit{bool}) \to \mathit{bool}$ in both PCF and PCF+por. [5 marks]

$$\mathcal{E} : \underbrace{(N_\bot \to B_\bot)}_{P_n} \to B_\bot$$

$$\mathcal{E}\left(\bigsqcup_n P_n\right) \neq \bigsqcup_n \mathcal{E}(P_n)$$

	$\bot$	0	1	$\dots$	n	$\dots$
$P \in (N_\bot \to B_\bot)$	$P(\bot)$	$P(0)$	$P(1)$	$\dots$	$P(n)$	$\dots$

	$\bot$	0	1	2	$\dots$	n	$\dots$		$\mathcal{E}(P_i)$
P_0	$\bot$	$\bot$	$\bot$	$\bot$	$\dots$				$\bot$
$\sqsubseteq$									
P_1	$\bot$	false	$\bot$	$\bot$	$\dots$				$\bot$
$\sqsubseteq$									
P_2	$\bot$	false	false	$\bot$	$\dots$				$\bot$
$\sqsubseteq$									
P_n	$\bot$	false	$\dots$			false	$\bot$ $\dots$	$\bot$	
$\bigsqcup_n P_n =$	$\bot$	false	false		$\dots$	false	$\dots$		

$$\bigsqcup_i \mathcal{E}(P_i) = \bigsqcup_i \bot = \bot$$

$$\neq$$

$$\mathcal{E}\left(\bigsqcup_n P_n\right) = \text{false}$$

(c) Let M be the $\mathsf{PCF{+}por}$ term

$$\begin{aligned}&\mathbf{fn}\ f : (nat \to bool) \to bool\,.\\ &\quad \mathbf{fn}\ P : nat \to bool\,.\\ &\qquad \mathbf{por}\Big(P\,\mathbf{0}\,,\ f\ \big(\mathbf{fn}\ n : nat\,.\ P\,(\mathbf{succ}(n))\big)\Big)\end{aligned}$$

Give an explicit description of $[\![\,\mathbf{fix}(M)\,]\!] \in \big((\mathbb{N}_\perp \to \mathbb{B}_\perp) \to \mathbb{B}_\perp\big)$. [7 marks]