Contextual preorder between PCF terms

Given PCF terms M_1, M_2, PCF type τ, and a type environment Γ, the relation $\boxed{\Gamma \vdash M_1 \leq_{\mathrm{ctx}} M_2 : \tau}$ 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 $V \in \mathrm{PCF}_\gamma$,

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

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

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

consider $M_1 N_1 N_2 \ldots N_n \Downarrow V \Longrightarrow M_2 N_1 N_2 \ldots N_n \Downarrow V$

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

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

Applicative contexts

$\mathcal{C}_M[\,] \equiv [\,]M$

Topic 8

Full Abstraction

Proof principle

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

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

$$\overset{?}{\Longleftarrow}$$

Hence, to prove

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

it suffices to establish

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

NB: Failure of definability: ⇝ At higher type

For all $d \in [\![\tau]\!]$, does there exists $M \in PCF_\tau$ s.t. $[\![M]\!] = d$?

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.

Failure of full abstraction, idea

We will construct two closed terms

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

such that

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

and

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

because there is an undefinable: $por \in (\mathbb{B}_\perp \to (\mathbb{B}_\perp \to \mathbb{B}_\perp))$ s.t. $[\![T_1]\!](por) \neq [\![T_2]\!](por)$

- 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

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

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

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

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

For $i = 1, 2$ define $\forall p.\ T_1\,p \not\Downarrow \wedge T_2\,p \not\Downarrow$

$\Downarrow$

$T_1 \cong_{ctx} T_2$

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

NB $[\![T_1]\!](por) = true$

$[\![T_2]\!](por) = false$

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

where $B_1 \stackrel{\text{def}}{=} \mathbf{true}$, $B_2 \stackrel{\text{def}}{=} \mathbf{false}$,
and $\Omega \stackrel{\text{def}}{=} \mathbf{fix}(\mathbf{fn}\, x : bool\,.\, x)$.

Failure of full abstraction

Proposition.

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

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

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:

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