Topic 8

Full Abstraction

Proof principle

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

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

Is this complete?

Hence, to prove

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

No!

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.

There are τ_1 and τ_2 such that

$\tau_1 \leq_{ctx} \tau_2$ but $[\![\tau_1]\!] \neq [\![\tau_2]\!]$

We are looking for τ_1, τ_2 s.t.

$$\tau_1 \cong_{ctx} \tau_2 \quad \& \quad [\![\tau_1]\!] \neq [\![\tau_2]\!]$$

Can we find such τ_1, τ_2 of ground type?
(bool or nat)

Recall

$$M_1 \cong_{ctx} M_2 : \gamma \text{ iff } \forall v.\ M_1 \Downarrow v \Leftrightarrow M_2 \Downarrow v$$

Every higher PCF type is of the form

$$\tau_1 \to \tau_2 \to \dots \to \tau_n \to \gamma$$

Can we find such T_1, T_2 of type $\gamma' \to \gamma$?

Recall

$$M_1 \leq_{ctx} M_2 : \tau_1 \to \tau_2 \to \cdots \to \tau_n \to \gamma$$

iff $\forall N_1, N_2, \ldots, N_n$

$$M_1\ N_1\ N_2 \ldots N_n \Downarrow \checkmark$$

$$\Longleftrightarrow$$

$$M_2\ N_1\ N_2 \ldots N_n \Downarrow \checkmark$$

Can we find such $T_1, T_2 : bool \to bool$?

Want $\tau_1 \cong_{ctx} \tau_2 : bool \to bool$

$\iff \forall N : bool.\ \tau_1 N \Downarrow V \iff \tau_2 N \Downarrow V$

Can we have $[\![\tau_1]\!] \neq [\![\tau_2]\!] : B_\perp \to B_\perp$?

Ie can we have $[\![\tau_1]\!](d) \neq [\![\tau_2]\!](d)$ for some $d \in B_\perp$.

Let's try with $d = true \in B$.

But $true = [\![true]\!]$

Every element of $B_\perp$ is PCF definable

$false = [\![false]\!]$

$\perp = [\![fix(fn\ x.x)]\!]$

So $[\![\tau_1]\!](d) = [\![\tau_1]\!]\,[\![\text{true}]\!] = [\![\tau_1\,(\text{true})]\!]$

$$\|$$

$[\![\tau_2]\!](d) = [\![\tau_2]\!]\,[\![\text{true}]\!] = [\![V]\!]$

?

for $\tau_1 \Downarrow V$ and

$\tau_2 \Downarrow V$

We try higher types one level up:

$$(\text{bool} \to \text{bool} \to \text{bool}) \to \text{bool}$$

And aim at finding a non-definable element of $(B_\bot \to (B_\bot \to B_\bot))$?

say d.

$\forall M \in PCF_{bool \to bool \to bool} \,.\, [\![M]\!] \neq d$.

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

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

- 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

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

Parallel-or function

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

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

Parallel-or function

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

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

In which case, it necessarily follows by monotonicity that

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

Claim por is not PCF-definable

$\forall M.\ [\![M]\!] \neq por$

Define a **STABLE** function model

→ continuity

+ minimal input for output required.

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

Define T_1, T_2 s.t. $[\![T_1]\!](por) \neq [\![T_2]\!](por)$

$$\Downarrow$$

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

and $T_1\, M \not\Downarrow$ & $T_2\, M \not\Downarrow$ $\forall M$.

Parallel-or test functions

For $i = 1, 2$ define

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

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

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

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

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

otherwise $[\![T_i]\!](d) = \bot$

$T_1\, M \Downarrow$ & $T_2\, M \Downarrow$

$[\![\Omega]\!] = \bot$

$\Downarrow$

$T_1 \not\cong_{ctx} T_2$

Failure of full abstraction

Proposition.

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

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

PCF+por

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

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:

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