

Topic 8

Full Abstraction

Proof principle

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

$$\llbracket M_1 \rrbracket = \llbracket M_2 \rrbracket \text{ in } \llbracket \tau \rrbracket \implies M_1 \cong_{\text{ctx}} M_2 : \tau .$$

Hence, to prove

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

it suffices to establish

$$\llbracket M_1 \rrbracket = \llbracket M_2 \rrbracket \text{ in } \llbracket \tau \rrbracket .$$

Is this complete?
No!

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 T_1 and T_2 such that

$T_1 \leq_{\text{ctx}} T_2$ but $\llbracket T_1 \rrbracket \neq \llbracket T_2 \rrbracket$

We are looking for T_1, T_2 s.t.

$$T_1 \cong_{\text{ctx}} T_2 \quad \& \quad [T_1] \neq [T_2]$$

Can we find such T_1, T_2 of ground type?

bool or not

Recall

$$M_1 \underset{\text{ctx}}{\cong} M_2 : \gamma \text{ iff } \forall V. M_1[V] \leftrightarrow M_2[V]$$

Every higher PCF type is of the form

$$T_1 \rightarrow T_2 \rightarrow \dots \rightarrow T_n \rightarrow \gamma$$

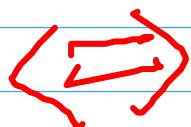
Can we find such T_1, T_2 of type $\gamma' \rightarrow \delta'$?

Recall

$$M_1 \leq_{\text{ctx}} M_2 : T_1 \rightarrow T_2 \rightarrow \dots \rightarrow T_n \rightarrow \delta'$$

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

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



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

Can we find such $T_1, T_2 : \text{bool} \rightarrow \text{bool}$?

Want $T_1 \cong_{\text{ctx}} T_2 : \text{bool} \rightarrow \text{bool}$

$\exists N : \text{bool}. \quad T_1 \nVdash N \vee \top \Leftrightarrow T_2 \nVdash N \vee \top$

Can we have $\llbracket T_1 \rrbracket \neq \llbracket T_2 \rrbracket : B_1 \rightarrow B_\perp$?

It can we have $\llbracket T_1 \rrbracket(d) \neq \llbracket T_2 \rrbracket(d)$ for some $d \in B_1$.

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

But

$$\boxed{\text{true} = \llbracket \text{true} \rrbracket}$$

Every element of B_\perp is PCF definable
 $\text{false} = \llbracket \text{false} \rrbracket$
 $\perp = \llbracket \text{fix } (\lambda x. x) \rrbracket$

$$\text{So } \llbracket T_1 \rrbracket(d) = \llbracket T_1 \rrbracket \llbracket \text{true} \rrbracket = \llbracket T_1(\text{true}) \rrbracket$$

$$\llbracket T_2 \rrbracket(d) = \llbracket T_2 \rrbracket \llbracket \text{true} \rrbracket = \llbracket V \rrbracket$$

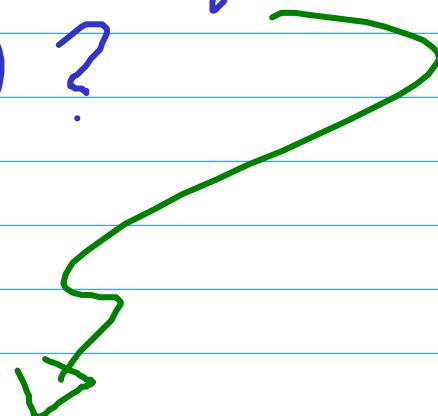
for $T_1 \Downarrow V$ and

$T_2 \Downarrow V$

We try higher types one level up:

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

And aim at finding a non-definable element of $(B_1 \rightarrow (B_1 \rightarrow B_1))$?



Say d.

$\forall M \in \text{PCF}_{\text{bool} \rightarrow \text{bool} \rightarrow \text{bool}} . \exists N \nexists d .$

Failure of full abstraction, idea

We will construct two closed terms

$$T_1, T_2 \in \text{PCF}_{(bool \rightarrow (bool \rightarrow bool)) \rightarrow bool}$$

such that

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

and

$$\llbracket T_1 \rrbracket \neq \llbracket T_2 \rrbracket$$

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

$$\forall M \in \text{PCF}_{\text{bool} \rightarrow (\text{bool} \rightarrow \text{bool})} (T_1 M \not\models_{\text{bool}} \& T_2 M \not\models_{\text{bool}})$$

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

$$\forall M \in \text{PCF}_{\text{bool} \rightarrow (\text{bool} \rightarrow \text{bool})} (T_1 M \not\downarrow_{\text{bool}} \& T_2 M \not\downarrow_{\text{bool}})$$

Hence,

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

for all $M \in \text{PCF}_{\text{bool} \rightarrow (\text{bool} \rightarrow \text{bool})}$.

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

$$\forall M \in \text{PCF}_{\text{bool} \rightarrow (\text{bool} \rightarrow \text{bool})} (T_1 M \not\downarrow_{\text{bool}} \& T_2 M \not\downarrow_{\text{bool}})$$

Hence,

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

for all $M \in \text{PCF}_{\text{bool} \rightarrow (\text{bool} \rightarrow \text{bool})}$.

- We achieve $\llbracket T_1 \rrbracket \neq \llbracket T_2 \rrbracket$ by making sure that

$$\llbracket T_1 \rrbracket(\text{por}) \neq \llbracket T_2 \rrbracket(\text{por})$$

for some *non-definable* continuous function

$$\text{por} \in (\mathbb{B}_\perp \rightarrow (\mathbb{B}_\perp \rightarrow \mathbb{B}_\perp)) .$$

Parallel-or function

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

$$\text{por } \text{true } \perp = \text{true}$$

$$\text{por } \perp \text{ true} = \text{true}$$

$$\text{por } \text{false } \text{ false} = \text{false}$$

Parallel-or function

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

$$\text{por } \text{true } \perp = \text{true}$$

$$\text{por } \perp \text{ true} = \text{true}$$

$$\text{por } \text{false } \text{ false} = \text{false}$$

In which case, it necessarily follows by monotonicity that

$$\text{por } \text{true } \text{ true} = \text{true}$$

$$\text{por } \text{false } \perp = \perp$$

$$\text{por } \text{true } \text{ false} = \text{true}$$

$$\text{por } \perp \text{ false} = \perp$$

$$\text{por } \text{false } \text{ true} = \text{true}$$

$$\text{por } \perp \perp = \perp$$

Claim

par is not PCF-definable

$\forall M. \quad [M] \neq \text{par}$

Define a STABLE functional model

↓ continuity

+ minimal effort for output
representation.

Undefinability of parallel-or

Proposition. *There is no closed PCF term*

$$P : \text{bool} \rightarrow (\text{bool} \rightarrow \text{bool})$$

satisfying

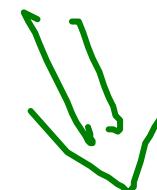
$$\llbracket P \rrbracket = \text{por} : \mathbb{B}_\perp \rightarrow (\mathbb{B}_\perp \rightarrow \mathbb{B}_\perp) .$$

Parallel-or test functions

Define T_1, T_2 s.t. $[T_1](\text{par}) \neq [T_2](\text{par})$

and

$T_1 \text{ Mst} \wedge T_2 \text{ Mst } \forall n.$



$[T_1] \neq [T_2]$

Parallel-or test functions

For $i = 1, 2$ define

$$T_i \stackrel{\text{def}}{=} \text{fn } f : \text{bool} \rightarrow (\text{bool} \rightarrow \text{bool}) . \begin{array}{l} \text{if } (f \text{ true } \Omega) \text{ then} \\ \quad \text{if } (f \Omega \text{ true}) \text{ then} \\ \quad \quad \text{if } (f \text{ false } \text{false}) \text{ then } \Omega \text{ else } B_i \\ \quad \text{else } \Omega \\ \text{else } \Omega \end{array}$$

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

$$\boxed{[T_1]Y(\text{for}) = \text{true}} \quad \boxed{[T_2]Y(\text{for}) = \text{false}}$$

otherwise

$$T_1 M \not\models \& T_2 M \not\models$$

$[\Omega]Y = \perp$

↑
 $T_1 \models \neg \Omega$

Failure of full abstraction

Proposition.

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

$$\llbracket T_1 \rrbracket \neq \llbracket T_2 \rrbracket \in (\mathbb{B}_\perp \rightarrow (\mathbb{B}_\perp \rightarrow \mathbb{B}_\perp)) \rightarrow \mathbb{B}_\perp$$

PCF+por

Expressions $M ::= \dots \mid \text{por}(M, M)$

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

Evaluation

$$\frac{\begin{array}{c} M_1 \Downarrow_{\text{bool}} \text{true} \\[1ex] M_2 \Downarrow_{\text{bool}} \text{true} \end{array}}{\text{por}(M_1, M_2) \Downarrow_{\text{bool}} \text{true}} \qquad \frac{\begin{array}{c} M_1 \Downarrow_{\text{bool}} \text{false} \quad M_2 \Downarrow_{\text{bool}} \text{false} \end{array}}{\text{por}(M_1, M_2) \Downarrow_{\text{bool}} \text{false}}$$

Plotkin's full abstraction result

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

$$\llbracket \Gamma \vdash \mathbf{por}(M_1, M_2) \rrbracket(\rho) \stackrel{\text{def}}{=} \text{por}\left(\llbracket \Gamma \vdash M_1 \rrbracket(\rho)\right)\left(\llbracket \Gamma \vdash M_2 \rrbracket(\rho)\right)$$

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

$$\Gamma \vdash M_1 \cong_{\text{ctx}} M_2 : \tau \Leftrightarrow \llbracket \Gamma \vdash M_1 \rrbracket = \llbracket \Gamma \vdash M_2 \rrbracket.$$