Topic 8

Full Abstraction

Proof principle

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

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

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.

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

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

- Recall that

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

iff

$$\forall\, M : \mathrm{PCF}_{\mathsf{bool} \to (\mathsf{bool} \to \mathsf{bool})}.\ \forall\, V : \mathrm{PCF}_{\mathsf{bool}}.$$

$$T_1\, M \Downarrow_{\mathsf{bool}} V \iff T_2\, M \Downarrow_{\mathsf{bool}} V$$

- In particular, we will achieve $T_1 \cong_{ctx} T_2$ by making sure that

$$\forall\, M : \mathrm{PCF}_{\mathsf{bool} \to (\mathsf{bool} \to \mathsf{bool})}.$$

$$T_1\, M \not\Downarrow_{\mathsf{bool}} \quad \text{and} \quad T_2\, M \not\Downarrow_{\mathsf{bool}}$$

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

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

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

iff

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

for some $f \in (\mathbb{B}_\perp \to (\mathbb{B}_\perp \to \mathbb{B}_\perp))$

that is necessarily not definable,

in the sense that

$f \neq [\![M]\!]$ $\forall M \in \mathrm{PCF}_{bool\to(bool\to bool)}$

- 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

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

In which case, it necessarily follows by monotonicity that

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

Undefinability of parallel-or

Proposition. *There is no closed PCF term*

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

satisfying

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

Remark: The definable functions have a property known as stability That, in particular, implies That, for all $M \in PCF_{bool \to (bool \to bool)}$,

$$\left(\llbracket M \rrbracket\ s_1\ t_1\right) \wedge \left(\llbracket M \rrbracket\ s_2\ t_2\right) = \llbracket M \rrbracket\ s_2\ t_1$$

for all $s_1 \sqsupseteq s_2$ and $t_1 \sqsubseteq t_2$.

- por does not here this property; so it is not stable and hence not definable

Parallel-or test functions

NB: One may define a program $T \in PCF_{(bool \to (bool \to bool)) \to bool}$ that tests whether its input behaves as por and loops otherwise.

```
T = fn f : bool → (bool → bool)
      if (f true Ω)
      then if (f Ω true)
           then if (f false false)
                then Ω
                else ... input behaves like por ...
           else Ω
      else Ω
```

In particular,

$$T\ M \not\equiv_{bool} \quad \forall M : bool \to (bool \to bool)$$

and we may define two versions of T, say T_1 and T_2, that are contextually equivalent but for which

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

by giving different outputs when the test succeeds.

Parallel-or test functions

For $i = 1, 2$ define

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

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:

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