Topic 8

Full Abstraction

Recall :

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.

▶ 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

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

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

$$\forall\, M \in \mathrm{PCF}_{bool \to (bool \to bool)}\; (\, T_1\, M \Downarrow\!\!\!/_{\,bool}\; \&\; T_2\, M \Downarrow\!\!\!/_{\,bool}\,)$$

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

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

since then we have

$\forall M : bool \to bool \to bool$

$\quad \forall V : bool \, (T_1 M \Downarrow_{bool} V \iff T_2 M \Downarrow_{bool} V)$

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

$M_1 \overset{\sim}{\cong}_{\mathrm{ctx}} M_2 : \gamma$ holds if and only if

$$\forall V \in \mathrm{PCF}_\gamma \left(M_1 \Downarrow_\gamma V \iff M_2 \Downarrow_\gamma V\right).$$

(Proof uses the logical relation $\vartriangleleft$
— see Sect. 7.3.) .

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

$$\forall M \in \mathrm{PCF}_{bool \to (bool \to bool)} \left(T_1\, M \Downarrow\!\!\!\!/_{bool} \ \& \ T_2\, M \Downarrow\!\!\!\!/_{bool} \right)$$

since then we have

$\forall M : bool \to bool \to bool$

$\quad \forall v : bool \left(T_1 M \Downarrow_{bool} v \iff T_2 M \Downarrow_{bool} v \right)$

i.e.

$\quad \forall M \left(T_1 M \cong_{ctx} T_2 M \ : \ bool \right)$

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

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

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

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

(See sect. 7.3 for proof)

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

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

since then we have

$$\forall M : bool \to bool \to bool$$

$$\forall V : bool \, (\, T_1 M \Downarrow_{bool} V \iff T_2 M \Downarrow_{bool} V \,)$$

i.e. $\forall M (\, T_1 M \cong_{ctx} T_2 M \; : \; bool \,)$

hence

$$T_1 \cong_{ctx} T_2 : bool \to bool \to bool$$

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

$$\forall M \in \mathrm{PCF}_{bool \to (bool \to bool)} \, (\, T_1 \, M \, \Downarrow\!\!\!\!/_{bool} \; \& \; T_2 \, M \, \Downarrow\!\!\!\!/_{bool} \,)$$

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

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

for some *non-definable* continuous function

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

▶ 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

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

because

110

Parallel-or function

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

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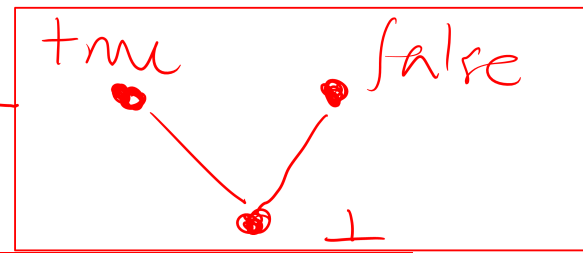por \ \ false \ \ false \ \ &= \ \ false
\end{aligned}
$$

Parallel-or function

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

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

Parallel-or function

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

$$por\ true\ \perp\ =\ true$$

$$por\ \perp\ true\ =\ true$$

$$por\ false\ false\ =\ false$$

In which case, it necessarily follows by monotonicity that

$$por\ true\ true\ =\ true \qquad por\ false\ \perp\ =\ \perp$$

$$por\ true\ false\ =\ true \qquad por\ \perp\ false\ =\ \perp$$

$$por\ false\ true\ =\ true \qquad por\ \perp\ \perp\ =\ \perp$$

Parallel-or function

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

$$por \; true \; \perp \quad = \quad true$$

$$por \; \perp \; true \quad = \quad true$$

$$por \; false \; false \quad = \quad false$$

$\underline{NB}$ $por \neq [\![fn \; x, x' : bool \; . \; if \; x \; then \; true \; else \; x']\!]$

$\qquad\qquad\quad \neq [\![fn \; x, x' : bool \; . \; if \; x' \; then \; true \; else \; x]\!]$

(left & right "sequential-or" functions)

Undefinability of parallel-or

Proposition. *There is no closed PCF term*

$$P : bool \rightarrow (bool \rightarrow bool)$$

satisfying

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

Proofs:
— Milner's "activity Lemma" (operational)
or — Berry's stable continuous fns
or — Seiber's sequential logical rel^s (denotational)

Parallel-or test functions

For $i = 1, 2$ define

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

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.

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

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

Failure of full abstraction

Proposition.

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

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

because $\begin{cases} [\![T_1]\!](por) = true \\ [\![T_2]\!](por) = false \end{cases}$

114

Failure of full abstraction

Proposition.

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

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

because

$$\forall M : bool \rightarrow bool \rightarrow bool \; (T_1 M \not\Downarrow_{bool} \quad \& \quad T_2 M \not\Downarrow_{bool})$$

Because of how T_i is defined,

for any $M : bool \to bool \to bool$,

if $T_i M \Downarrow_{bool} V$ then $\begin{cases} M \; true \; \Omega \Downarrow true \\ M \; \Omega \; true \Downarrow true \\ M \; false \; false \Downarrow false \end{cases}$

(for some V)

Because of how T_i is defined,

for any $M : \text{bool} \to \text{bool} \to \text{bool}$,

if $T_i M \Downarrow_{\text{bool}} V$ then
$$\begin{cases} M \text{ true } \Omega \Downarrow \text{ true} \\ M \Omega \text{ true } \Downarrow \text{ true} \\ M \text{ false false } \Downarrow \text{ false} \end{cases}$$

so
$$\begin{cases} [\![M]\!] (\text{true})(\bot) = \text{true} \\ [\![M]\!] (\bot)(\text{true}) = \text{true} \\ [\![M]\!] (\text{false})(\text{false}) = \text{false} \end{cases}$$

so $\quad [\![M]\!] = \text{por}$

Because of how T_i is defined,

for any $M : bool \to bool \to bool$,

if $T_i M \Downarrow_{bool} V$ then $\begin{cases} M \text{ true } \Omega \Downarrow \text{ true} \\ M \; \Omega \text{ true } \Downarrow \text{ true} \\ M \text{ false false } \Downarrow \text{ false} \end{cases}$

so $\begin{cases} [\![M]\!] (\text{true})(\bot) = \text{true} \\ [\![M]\!] (\bot)(\text{true}) = \text{true} \\ [\![M]\!] (\text{false})(\text{false}) = \text{false} \end{cases}$

so $[\![M]\!] = por$

no such M exists, so must have $T_i M \cancel{\Downarrow}_{bool}$

PCF+por

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

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

Evaluation

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

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

Plotkin's full abstraction result

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

$$\llbracket \Gamma \vdash \mathbf{por}(M_1, M_2) \rrbracket(\rho) \overset{\mathrm{def}}{=} por\big(\llbracket \Gamma \vdash M_1 \rrbracket(\rho)\big)\big(\llbracket \Gamma \vdash M_2 \rrbracket(\rho)\big)$$

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

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

Fully abstract den. sem. of PCF

- Sieber, O'Hearn–Riecke ('95)
  "Kripke logical relations of varying arity"

- Abramsky et al / Hyland–Ong (~'95)
  GAME SEMANTICS

Domain equations

For example:

denotations of numerical expressions
whose evaluation side-effects state

$$E = S \rightharpoonup (\mathbb{N} \times S)$$

$$S = \mathbb{N} \rightharpoonup E$$

states that store a mutable method that applies to numbers

Domain equations

For example:

$$E = S \rightharpoonup (\mathbb{N} \times S)$$
$$S = \mathbb{N} \rightharpoonup E$$

So E has to satisfy

$$E = (\mathbb{N} \rightharpoonup E) \rightharpoonup (\mathbb{N} \times (\mathbb{N} \rightharpoonup E))$$

Domain equations

For example:

$$E = S \rightharpoonup (\mathbb{N} \times S)$$
$$S = \mathbb{N} \rightharpoonup E$$

So E has to satisfy

$$E = (\mathbb{N} \rightharpoonup E) \rightharpoonup (\mathbb{N} \times (\mathbb{N} \rightharpoonup E))$$

Cantor: there are no such <u>sets</u> E.

$$\text{card}(RHS) \geq 2^{\text{card}(LHS)} > \text{card}(LHS)$$

Domain equations

For example:

$$E = S \rightharpoonup (\mathbb{N} \times S)$$
$$S = \mathbb{N} \rightharpoonup E$$

So E has to satisfy

$$E = (\mathbb{N} \rightharpoonup E) \rightharpoonup (\mathbb{N} \times (\mathbb{N} \rightharpoonup E))$$

Cantor: there are no such <u>sets</u> E.

Scott & Plotkin ($\sim$'79): there <u>are</u> domains satisfying

$$E = (\mathbb{N}_{\perp} \to E) \to (\mathbb{N}_{\perp} \times (\mathbb{N}_{\perp} \to E))$$

(Can solve fixpoint equations for domains)