Failure of Full Abstraction

[Chapter 8, p91]

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

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

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

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

since then we have

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

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

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

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

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

- 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

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

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

ie. $\forall M\ (T_1 M \cong_{ctx} T_2 M \ : bool)$

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

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

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

- 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

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

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

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

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

- 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

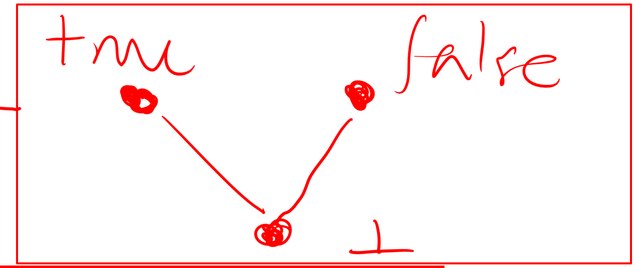
because

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

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

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

Parallel-or function

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

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

In which case, it necessarily follows by monotonicity that

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

Parallel-or function

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

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

<u>NB</u> $por \neq [\![\mathbf{fn}\ x, x' : bool .\ \mathbf{if}\ x\ \mathbf{then}\ true\ \mathbf{else}\ x']\!]$

$\neq [\![\mathbf{fn}\ x, x' : bool .\ \mathbf{if}\ x'\ \mathbf{then}\ true\ \mathbf{else}\ x]\!]$

(left & right "sequential-or" functions)

Undefinability of parallel-or

Proposition. *There is no closed PCF term*

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

satisfying

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

Proofs: – Milner's "activity lemma" (operational)
or – Berry's stable continuous fns
or – Sieber's sequential logical rel^ns (denotational)

Parallel-or test functions

For $i = 1, 2$ define

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

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.

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

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

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

Failure of full abstraction

Proposition.

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

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

because

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

Because of how T_i is defined,

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

if $T_i\, M \Downarrow_{bool} V$ (for some V) then

$$\begin{cases} M\ true\ \Omega \Downarrow true \\ M\ \Omega\ true \Downarrow true \\ M\ false\ false \Downarrow false \end{cases}$$

Because of how T_i is defined,

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

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

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

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

Because of how T_i is defined,

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

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

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

so $[\![M]\!] = \mathrm{por}$

no such M exists, so must have

$T_i M \not\Downarrow_{\mathrm{bool}}$

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:

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

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~~ that
applies to numbers

Domain equations

For example:

$$\begin{aligned} E &= S \rightharpoonup (\mathbb{N} \times S) \\ S &= \mathbb{N} \rightharpoonup E \end{aligned}$$

So E has to satisfy

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

Domain equations

For example:

$$\begin{aligned} E &= S \rightharpoonup (\mathbb{N} \times S) \\ S &= \mathbb{N} \rightharpoonup E \end{aligned}$$

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.

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

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 (~'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)