Topic 7

Relating Denotational and Operational Semantics

Adequacy

For any closed PCF terms M and V of *ground* type $\gamma \in \{nat, bool\}$ with V a value

$$[\![M]\!] = [\![V]\!] \in [\![\gamma]\!] \implies M \Downarrow_\gamma V \, .$$

Adequacy

For any closed PCF terms M and V of *ground* type $\gamma \in \{nat, bool\}$ with V a value

$$[\![M]\!] = [\![V]\!] \in [\![\gamma]\!] \implies M \Downarrow_\gamma V \ .$$

NB. Adequacy does not hold at function types:

$$[\![\mathbf{fn}\, x : \tau .\, (\mathbf{fn}\, y : \tau .\, y)\, x]\!] \quad = \quad [\![\mathbf{fn}\, x : \tau .\, x]\!] \quad : [\![\tau]\!] \to [\![\tau]\!]$$

but

$$\mathbf{fn}\, x : \tau .\, (\mathbf{fn}\, y : \tau .\, y)\, x \not\Downarrow_{\tau \to \tau} \mathbf{fn}\, x : \tau .\, x$$

Adequacy proof idea

1. We cannot proceed to prove the adequacy statement by a straightforward induction on the structure of terms.

   ► Consider M to be $M_1\, M_2$, $\mathbf{fix}(M')$.

RTP

$$[\![M_1\, M_2]\!] = [\![V]\!] \overset{?}{\Longrightarrow} M_1\, M_2 \Downarrow_{\gamma} V$$

$M_1 : \tau \to \gamma$ Cannot use induction

$M_2 : \tau$

Adequacy proof idea

1. We cannot proceed to prove the adequacy statement by a straightforward induction on the structure of terms.

   ► Consider M to be $M_1\, M_2$, $\mathbf{fix}(M')$.

2. So we proceed to prove a stronger statement that applies to terms of arbitrary types and implies adequacy.

   This statement roughly takes the form:

   $$[\![M]\!] \lhd_\tau M \text{ for all types } \tau \text{ and all } M \in \mathrm{PCF}_\tau$$

   where the *formal approximation relations*

   $$\lhd_\tau \subseteq [\![\tau]\!] \times \mathrm{PCF}_\tau$$

   are *logically* chosen to allow a proof by induction.

inductively

$\lhd_{nat}$

$\lhd_{bool}$

$\lhd_{\tau_1 \to \tau_2}$

Requirements on the formal approximation relations, I

We want that, for $\gamma \in \{nat, bool\}$,

$$[\![M]\!] \lhd_\gamma M \text{ implies } \underbrace{\forall V\ ([\![M]\!] = [\![V]\!] \implies M \Downarrow_\gamma V)}_{\text{adequacy}}$$

NB: $\bot \lhd_{nat} M : nat$, $\bot \lhd_{bool} M : bool$.

Definition of $d \lhd_\gamma M \;\; (d \in [\![\gamma]\!], M \in \mathrm{PCF}_\gamma)$
for $\gamma \in \{nat, bool\}$

$$n \lhd_{nat} M \quad \overset{\text{def}}{\Leftrightarrow} \quad \big(n \in \mathbb{N} \;\Rightarrow\; M \Downarrow_{nat} \mathbf{succ}^n(\mathbf{0})\big)$$

$$\begin{aligned} b \lhd_{bool} M \quad \overset{\text{def}}{\Leftrightarrow} \quad & (b = \mathit{true} \;\Rightarrow\; M \Downarrow_{bool} \mathbf{true}) \\ & \& \; (b = \mathit{false} \;\Rightarrow\; M \Downarrow_{bool} \mathbf{false}) \end{aligned}$$

Proof of: $[\![M]\!] \lhd_\gamma M$ implies **adequacy**

Case $\gamma = nat$.

$$
\begin{aligned}
& [\![M]\!] = [\![V]\!] \\
& \quad \Longrightarrow \; [\![M]\!] = [\![\mathbf{succ}^n(\mathbf{0})]\!] && \text{for some } n \in \mathbb{N} \\
& \quad \Longrightarrow \; n = [\![M]\!] \lhd_\gamma M \\
& \quad \Longrightarrow \; M \Downarrow \mathbf{succ}^n(\mathbf{0}) && \text{by definition of } \lhd_{nat}
\end{aligned}
$$

Case $\gamma = bool$ is similar.

Idea

$[\![M]\!] \lhd_\tau M \rightsquigarrow$ by induction on M.

Requirements on the formal approximation relations, II

We want to be able to proceed by induction.

- Consider the case $M = M_1 \, M_2$.

By ind

$[\![M_1]\!] \lhd_{\sigma \to \tau} M_1$

$[\![M_2]\!] \lhd_{\sigma} M_2$

$\Downarrow$?

$\rightsquigarrow$ *logical* definition

RTP

$$[\![M_1 \, M_2]\!] = [\![M_1]\!] ([\![M_2]\!]) \lhd_\tau M_1 \, M_2$$

Definition of $f \lhd_{\tau \to \tau'} M \ \big(f \in (\llbracket \tau \rrbracket \to \llbracket \tau' \rrbracket), M \in \mathrm{PCF}_{\tau \to \tau'}\big)$

$$f \lhd_{\tau \to \tau'} M$$

$$\overset{\text{def}}{\Leftrightarrow} \quad \forall\, x \in \llbracket \tau \rrbracket, N \in \mathrm{PCF}_{\tau}$$

$$(x \lhd_{\tau} N \ \Rightarrow \ f(x) \lhd_{\tau'} M\, N)$$

$\{ d \mid d \lhd_\tau \mathbf{fix}\, M' \}$ is Admissible.

Requirements on the formal approximation relations, III

We want to be able to proceed by induction.

- Consider the case $M = \mathbf{fix}(M')$.

$\rightsquigarrow$ *admissibility* property

$$\frac{d \lhd_\tau \mathbf{fix}\, M' \overset{?}{\Rightarrow} [\![M']\!]\, d \lhd \mathbf{fix}\, M'}{\mathit{fix}([\![M']\!]) = [\![\mathbf{fix}\, M']\!] \lhd_\tau \mathbf{fix}\, M'}$$

Scott Ind.

RTP

$$d \lhd_{\tau} \mathit{fix}(M')$$

Log. def

Ind

$$[\![M']\!] \lhd_{\tau \to \tau} M'$$

$$[\![M']\!]\, d \lhd_{\tau} M'(\mathit{fix}\, M')$$

$$\left.\begin{array}{l} x \lhd N \\ N \Downarrow V \\ M \Downarrow V \end{array}\right\} \Longrightarrow x \lhd M$$

? Lemma

$$\frac{}{[\![M']\!]\, d \lhd_{\tau} \mathit{fix}(M')}$$

Admissibility property

Lemma. *For all types* τ *and* $M \in \mathrm{PCF}_\tau$*, the set*

$$\{\, d \in [\![\tau]\!] \mid d \lhd_\tau M \,\}$$

is an admissible subset of $[\![\tau]\!]$*.*

Further properties

Lemma. *For all types* τ, *elements* $d, d' \in [\![\tau]\!]$, *and terms* $M, N, V \in \mathrm{PCF}_\tau$,

1. *If* $d \sqsubseteq d'$ *and* $d' \lhd_\tau M$ *then* $d \lhd_\tau M$.
2. *If* $d \lhd_\tau M$ *and* $\forall V \, (M \Downarrow_\tau V \implies N \Downarrow_\tau V)$ *then* $d \lhd_\tau N$.

Requirements on the formal approximation relations, IV

We want to be able to proceed by induction.

- Consider the case $M = \mathbf{fn}\, x : \tau \,.\, M'$.

$\rightsquigarrow$ *substitutivity* property for open terms

Ind $[\![x:\tau \vdash M' : \tau']\!] \rightsquigarrow$

$[\![\mathbf{fn}\, x:\tau \,.\, M']\!] \lhd_{\tau \to \tau'} \mathbf{fn}\, x:\tau \,.\, M'$

Fundamental property

Theorem. *For all* $\Gamma = \langle x_1 \mapsto \tau_1, \ldots, x_n \mapsto \tau_n \rangle$ *and all* $\Gamma \vdash M : \tau$, *if* $d_1 \lhd_{\tau_1} M_1, \ldots, d_n \lhd_{\tau_n} M_n$ *then* $[\![\Gamma \vdash M]\!][x_1 \mapsto d_1, \ldots, x_n \mapsto d_n] \lhd_{\tau} M[M_1/x_1, \ldots, M_n/x_n]$.

NB. The case $\Gamma = \emptyset$ reduces to

$$[\![M]\!] \lhd_{\tau} M$$

for all $M \in \mathrm{PCF}_{\tau}$.

Contextual preorder between PCF terms

Given PCF terms M_1, M_2, PCF type τ, and a type environment Γ, the relation $\boxed{\Gamma \vdash M_1 \leq_{\mathrm{ctx}} M_2 : \tau}$ is defined to hold iff

- Both the typings $\Gamma \vdash M_1 : \tau$ and $\Gamma \vdash M_2 : \tau$ hold.
- For all PCF contexts $\mathcal{C}$ for which $\mathcal{C}[M_1]$ and $\mathcal{C}[M_2]$ are closed terms of type γ, *where* $\gamma = nat$ *or* $\gamma = bool$, and for all values $V \in \mathrm{PCF}_\gamma$,

$$\mathcal{C}[M_1] \Downarrow_\gamma V \implies \mathcal{C}[M_2] \Downarrow_\gamma V \ .$$

Fact

$$M_1 \leq_{ctx} M_2 \iff [\![M_1]\!] \lhd M_2$$

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

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

$\mathcal{C}_M[-] = [-] \, M \qquad \mathcal{C}_M[M_1] \qquad \mathcal{C}_M[M_2]$

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.

- The domain model of PCF is *not* fully abstract.

  In other words, there are contextually equivalent PCF terms with different denotations.

por is not definable
$\not\equiv$
[[M]] for all M

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

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

find por : $\mathbb{B}_\perp \to \mathbb{B}_\perp \to \mathbb{B}_\perp$
s.t.
$[\![T_1]\!](por) \neq [\![T_2]\!](por)$

$[\![T_i]\!] : (\mathbb{B}_\perp \to \mathbb{B}_\perp \to \mathbb{B}_\perp) \to \mathbb{B}_\perp$

- 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

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

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

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

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

For $i = 1, 2$ define

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

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.

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

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

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:

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