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:

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

   where the *formal approximation relations*

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

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

Requirements on the formal approximation relations, I

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

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

We define $\lhd_{nat} \subseteq \mathbb{N}_\perp \times \underline{PCF}_{nat}$ and

$\lhd_{bool} \subseteq \mathbb{B}_\perp \times \underline{PCF}_{bool}$ such that (*) holds

Check $[\![M]\!] \lhd_{nat} M$ implies adequacy for M

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

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

$\mathbb{B}_\perp \ni b \lhd_{bool} M \overset{\text{def}}{\Leftrightarrow} (b = true \;\Rightarrow\; M \Downarrow_{bool} \mathbf{true})$
$\& \; (b = false \;\Rightarrow\; M \Downarrow_{bool} \mathbf{false})$

<u>NB</u>: $\perp \lhd_{nat} M$

$\perp \lhd_{bool} M$

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.

2 How do we define $\lhd_{\tau_1 \to \tau_2}$?

And can show $[\![M]\!] \lhd_{\tau_1 \to \tau_2} M$?

Requirements on the formal approximation relations, II

We want to be able to proceed by induction.

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

$\leadsto$ *logical* definition

$M = M_1 M_2$

$M_1 : \tau \to \tau'$ $M_2 : \tau$

$[\![M_1]\!] \in ([\![\tau]\!] \to [\![\tau']\!])$

$[\![M_2]\!] \in [\![\tau]\!]$

$[\![M]\!] \vartriangleleft_{\tau'} M$?

$[\![M]\!] = [\![M_1 M_2]\!] = [\![M_1]\!]([\![M_2]\!])$

$M = M_1 M_2$

?

By induction,

$[\![M_1]\!] \vartriangleleft_{\tau \to \tau'} M_1$

and

$[\![M_2]\!] \vartriangleleft_{\tau} M_2$

?

$f \vartriangleleft_{\tau \to \tau'} F$

$\Longleftrightarrow_{\text{def}} \forall d \vartriangleleft_{\tau} A . \ f(d) \vartriangleleft_{\tau'} F A$

LOGICAL

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

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

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

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

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

$M = \underline{\underline{fix}}(M') \qquad M' : \tau \to \tau$

$$[\![M]\!] \overset{?}{\lhd_\tau} \underline{\underline{fix}}(M')$$

$$\|$$

$$[\![\underline{\underline{fix}}(M')]\!]$$

$$\|$$

$$\underline{fix}([\![M']\!])$$

use Scott induction

need an admissible property.

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

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 $[\![\tau]\!]$.

$$\frac{x \in S \Rightarrow f(x) \in S}{\underline{fix}(f) \in S}$$

Assume

$$d \trianglelefteq \underline{\underline{fix}}(M')$$

By induction

$$[\![M']\!] \trianglelefteq_{\mathbb{Z}\to\mathbb{Z}} M'$$

By the logical definition

$$[\![M']\!](d) \trianglelefteq_{\mathbb{Z}} M'(\underline{\underline{fix}}(M'))$$

$$? \Downarrow$$

$$[\![M']\!](d) \trianglelefteq_{\mathbb{Z}} \underline{fix}(M')$$

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* $d \lhd_\tau N$.

use it with $M = M'(\underline{\mathbf{fix}}(M'))$

and $N = \underline{\mathbf{fix}}(M')$

Requirements on the formal approximation relations, IV

We want to be able to proceed by induction.

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

$\leadsto$ *substitutivity* property for open terms

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

Fundamental property of the relations $\lhd_\tau$

Proposition. *If* $\Gamma \vdash M : \tau$ *is a valid PCF typing, then for all* Γ*-environments* ρ *and all* Γ*-substitutions* σ

$$\rho \lhd_\Gamma \sigma \;\Rightarrow\; [\![\Gamma \vdash M]\!](\rho) \lhd_\tau M[\sigma]$$

- $\rho \lhd_\Gamma \sigma$ means that $\rho(x) \lhd_{\Gamma(x)} \sigma(x)$ holds for each $x \in dom(\Gamma)$.
- $M[\sigma]$ is the PCF term resulting from the simultaneous substitution of $\sigma(x)$ for x in M, each $x \in dom(\Gamma)$.

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 $V \in \mathrm{PCF}_\gamma$,

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

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

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

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

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.

Failure of full abstraction, idea

We will construct two closed terms

$$T_1, T_2 \in \mathrm{PCF}_{(bool \to (bool \to bool)) \to bool}$$

Type of binary boolean functions.

such that

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

and

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

$$\exists f \in (B_\perp \to (B_\perp \to B_\perp)).\ [\![T_1]\!](f) \neq [\![T_2]\!](f) \in B_\perp$$

__NB__: If $T_1 \cong_{ctx} T_2$

Then $\forall F \in \underline{PCF}_{(bool \to (bool \to bool))}$

$$[\![T_1\, F]\!] = [\![T_2\, F]\!] \quad \text{in } \mathbb{B}_\perp$$

$$[\![T_1]\!]([\![F]\!]) = [\![T_1\, F]\!] = [\![T_2\, F]\!] = [\![T_2]\!]([\![F]\!])$$

So to show failure of full abstraction there need be a <u>non-definable</u> binary boolean function in the model.

- 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 $por : \mathbb{B}_\bot \to (\mathbb{B}_\bot \to \mathbb{B}_\bot)$ such that

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

In which case, it necessarily follows by monotonicity that

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

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

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

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.

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

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

PCF+por

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

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:

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