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 proof idea

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

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

We cannot directly proceed by induction: In particular the adequacy statement only applies to ground types and so gives no information for higher-order programs.

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 $M_1\, M_2$, $\mathbf{fix}(M')$.

   by induction on the type structure

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*

Define a good family of relations

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

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

$[\![M]\!] \lhd_\tau M \Rightarrow$ adequacy holds for M.

NB $\lhd_{nat} = \{(\perp, M) \mid M \in PCF_{nat}\}$
$\cup \{(n, M) \mid n \in \mathbb{N} \wedge M \Downarrow \underline{succ}^n(0)\}$

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

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

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

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

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.

By ind: $[\![M_1]\!] \triangleleft_{\sigma\to\tau} M_1$, $[\![M_2]\!] \triangleleft_\sigma M_2$

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

$=$

$[\![M_1 M_2]\!] \triangleleft_\tau M_1 M_2$ $\Longleftarrow$?

Requirements on the formal approximation relations, II

We want to be able to proceed by induction.

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

$\rightsquigarrow$ *logical* definition

$$f \triangleleft_{\sigma\to\tau} M \text{ iff}_{\text{def}} \ \forall d \triangleleft_\sigma N.\ f(d) \triangleleft_\tau M\,N$$

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

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

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

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

hypothesis: $\{d \in [\![\tau]\!] \mid d \triangleleft_\tau N\}$ is admissible.

$\underline{\mathrm{fix}}\,[\![M]\!] = [\![\underline{\mathrm{fix}}(M)]\!] \triangleleft_\tau \underline{\mathrm{fix}}(M)$

Requirements on the formal approximation relations, III

We want to be able to proceed by induction.

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

$\leadsto$ *admissibility* property

Scott Ind.

$$\frac{d \in S \Rightarrow f(d) \in S}{\underline{\mathrm{fix}}(f) \in S} \quad (S \text{ admissible})$$

$$[d \lhd \underline{\mathrm{fix}}\, M]$$

$$\frac{}{[\![M]\!] \lhd_{\tau\to\tau} M}\ \text{by ind}$$

$$\frac{[\![M]\!] \lhd_{\tau\to\tau} M}{[\![M]\!]\, d \lhd_\tau M(\underline{\mathrm{fix}}\, M)}\ \text{by log. def}$$

$$[\![M]\!]\, d \lhd \underline{\mathrm{fix}}\, M$$

we have a gap!

$$\frac{[\![M]\!]\, d \lhd \underline{\mathrm{fix}}\, M}{d \lhd \underline{\mathrm{fix}}\, M \Rightarrow [\![M]\!]\, d \lhd \underline{\mathrm{fix}}(M)}$$

Assume admissibility

$$\frac{d \lhd \underline{\mathrm{fix}}\, M \Rightarrow [\![M]\!]\, d \lhd \underline{\mathrm{fix}}(M)}{\mathrm{fix}\, [\![M]\!] = [\![\underline{\mathrm{fix}}\, M]\!] \lhd_\tau \underline{\mathrm{fix}}\, M}$$

$$\frac{M(\underline{\mathrm{fix}}\, M) \Downarrow V}{\underline{\mathrm{fix}}(M) \Downarrow V}$$

We need: $x \lhd M(\underline{\mathrm{fix}}\, M) \Rightarrow x \lhd \underline{\mathrm{fix}}(M)$

We show: $x \lhd N \wedge (N \Downarrow V \Rightarrow N' \Downarrow V) \Rightarrow x \lhd N'$

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* $d \lhd_\tau N$.

We were looking at $\llbracket M \rrbracket \lhd_\tau M$ for closed M.

NOT ENOUGH!

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

by induction M' is open

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

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

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

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

enough to check in the empty context $\mathcal{C}[-] = [-]$

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

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

enough to check in applicative contexts $\mathcal{C}[-] = [-](M)$

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.

(*) essentially because por is not PCF definable; that is, cannot be implemented by a PCF program.

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

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

Will happen because there will be some input por in $(\mathbb{B}_\perp \to (\mathbb{B}_\perp \to \mathbb{B}_\perp))$ s.t. $[\![T_1]\!](por) \neq [\![T_2]\!](por)$ but nevertheless this cannot be seen operationally (*)

$[\![T_1]\!] \neq [\![T_2]\!]$ because $[\![T_1]\!](\underline{por}) \neq [\![T_2]\!](\underline{por})$

but this is not the case!

$T_1 \equiv_{ctx} T_2$

If there is a program P s.t. $[\![P]\!] = por$ then I can consider the context $C[-] = [-]\,P$ and it will happen that

$$C[T_1] \text{ and } C[T_2]$$

have different operational behaviour.