Topic 7

Relating Denotational and Operational Semantics

Soundness :

$$M \Downarrow V \Rightarrow [\![M]\!] = [\![V]\!]$$

Adequacy

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

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

equivalently

$\forall M \in PCF_{nat} . \; [\![M]\!] = n \in \mathbb{N} \Rightarrow M \Downarrow succ^n(0)$

& $\forall M \in PCF_{bool} . \; [\![M]\!] = true \in \mathbb{B} \Rightarrow M \Downarrow \underline{true}$

& $[\![M]\!] = false \in \mathbb{B} \Rightarrow M \Downarrow \underline{false}$.

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

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:

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

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

Adequacy proof idea

$M' : \sigma \to \sigma$

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

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

$[\![M]\!] = [\![V]\!] \Rightarrow M \Downarrow V$

$M = M_1(M_2)$ ——— $M_1 : \tau \to \sigma$

$M_2 : \tau$

Assume

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

want to show $M_1(M_2) \Downarrow V$

~~By "induction"~~

~~$[\![M_1]\!] = [\![V_1]\!] \Rightarrow \ldots$~~

~~$[\![M_2]\!] = [\![V_2]\!] \Rightarrow \text{--}$~~

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 $\boxed{\text{stronger statement}}$ that applies to terms of arbitrary types and implies adequacy.

because we are interested in doing an inductive proof.

Adequacy proof idea

at ground type should imply adequacy

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* ~ Key idea

construct

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

RELATING DENOTATION AND SYNTAX

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

Requirements on the formal approximation relations, I

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

DESIDERATA

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

idea

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

defined as

$n \lhd_{nat} M \quad \text{iff}_{def} \quad \underbrace{M \Downarrow succ^n(0)}_{\text{adequacy statement at ground type.}}$

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

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

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

$[\![M]\!] \lhd_\gamma M \Rightarrow$ adequacy.

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.

Want to show $[\![M]\!] \vartriangleleft_\tau M$ for all τ

Choose the def. of $\vartriangleleft_{\sigma\to\tau}$ carefully

Requirements on the formal approximation relations, II

We want to be able to proceed by induction.

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

I want

$\rightsquigarrow$ *logical* definition

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

By induction, I will have $[\![M_1]\!] \vartriangleleft_{\sigma\to\tau} M_1$ and

$[\![M_2]\!] \vartriangleleft_\sigma M_2$

$$[\![M_1]\!]([\![M_2]\!]) \overset{?}{\lhd}_\tau M_1(M_2)$$ by logical definition

By induction $[\![M_1]\!] \lhd_{\sigma\to\tau} M_1$, $[\![M_2]\!] \lhd_\sigma M_2$

Def $f \lhd_{\sigma\to\tau} M$

iff $\forall d \lhd_\sigma N.\ f(d) \lhd_\tau M(N)$ logical def.

We've defined $\lhd_\tau$ for all τ.

Definition of

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

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

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

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

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

We want $[\![\mathbf{fix}(M')]\!] \lhd_\tau \mathbf{fix}(M')$?

$$\mathbf{fix}\,[\![M']\!] = \bigsqcup_n [\![M']\!]^n(\perp)$$

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

We want

$$\bigsqcup_n [\![M']\!]^n(\bot) \trianglelefteq_\tau \underline{\mathrm{fix}}(M')$$

It would be nice if $P(x) \equiv \left(x \trianglelefteq_\tau \underline{\mathrm{fix}}(M')\right)$ is admissible because then it would be enough to show

$$[\![M']\!]^n(\bot) \trianglelefteq_\tau \underline{\mathrm{fix}}(M')$$

In fact it is true!

How would we show

$$[\![M']\!]^n(\perp) \lhd \mathit{fix}(M') \quad ?$$

(1) $\perp \lhd \mathit{fix}(M')$. ~

$$\frac{M'(\mathit{fix}\, M') \Downarrow v}{\mathit{fix}(M') \Downarrow v}$$

(2) $[\![M']\!](\perp) \lhd \mathit{fix}(M')$?

[By induction $[\![M']\!] \lhd M'$
By admissibility $\perp \lhd \mathit{fix}(M')$]

log. def

$\Longrightarrow [\![M']\!](\perp) \lhd M'(\mathit{fix}\, M')$

We want yet another lemma

$$\frac{d \triangleleft M \quad \& \quad (M \Downarrow V \Rightarrow N \Downarrow V)}{d \triangleleft N}$$

and apply it to the case

$$M = M'(\underline{\text{fix}}\ M'), \quad N = \underline{\text{fix}}(M')$$

$$d = [\![M']\!](\bot)$$

Chain closure

$$f_n \lhd_{\sigma\to\tau} M \implies \bigsqcup f_n \lhd_{\sigma\to\tau} M$$

$$\bigsqcup_n f_n \lhd_{\sigma\to\tau} M \text{ iff } \forall d \lhd_\sigma N.\ \underbrace{\left(\bigsqcup_n f_n\right)(d)}_{=\ \bigsqcup_n (f_n\, d)} \lhd_\tau M(N)$$

assume $f_n \lhd_{\sigma\to\tau} M$
and $d \lhd_\sigma N$ $\Rightarrow$ ~~log rel~~

$$f_n(d) \lhd_\tau M(N) \implies \bigsqcup (f_n d) \lhd_\tau M(N)$$

admiss
induction

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* $d \lhd_\tau N$ *.*

Want $\Pi[\![\mathbf{fn}\, x . M]\!] \lhd_{\sigma \to \tau}$ fn $x . M$, inductively from ... a generalisation of the statement that works on OPEN terms.

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

$$\frac{x : \sigma \vdash M : \tau}{\vdash \mathbf{fn}\, x . M : \sigma \to \tau}$$

The statement for closed terms

$$[\![M]\!] \triangleleft M$$

How do we generalise it to open terms

$$\Gamma \vdash M : \tau \qquad \Gamma \equiv (x_1 : \tau_1, \ldots x_n : \tau_n)$$

$\forall \; d_i \triangleleft_{\tau_i} M_i$.

$$[\![\Gamma \vdash M]\!](d_1 \ldots d_n) \triangleleft_\tau M[M_1/x_1, \ldots, M_n/x_n]$$

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*
$[\![\Gamma \vdash M]\!][x_1 \mapsto d_1, \ldots, x_n \mapsto d_n] \lhd_\tau M[M_1/x_1, \ldots, M_n/x_n]$.

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

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

Thm $[\![M_1]\!] \lhd_2 M_2$ 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

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