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

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

NB. Adequacy does not hold at function types:

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

Two different values with the same denotation

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

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

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

$\boxed{\text{Adequacy}}$ proof idea

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

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

by ind.

$[\![M_1]\!] = [\![\mathrm{fn}\, x. M]\!] \Rightarrow \cdots$

We cannot do induction

$$\frac{M_1 \Downarrow \mathrm{fn}\, x. M \quad M[M_2/x] \Downarrow V}{M_1\, M_2 \Downarrow V}$$

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

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

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

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:

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

For τ = nat or bool ⇒ Adequacy

   where the *formal approximation relations*

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

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

proved by induction on the structure of terms.

$\gamma = bool \quad \mathbb{B}_\perp \ni true \lhd_{bool} M \iff M \Downarrow_{bool} \underline{\underline{true}}$

$\mathbb{B}_\perp \ni false \lhd_{bool} M \iff M \Downarrow_{bool} \underline{false}$

Requirements on the formal approximation relations, I

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

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

If $[\![M]\!] \lhd_{bool} M$ then $\underbrace{\forall V.\ [\![M]\!] = [\![V]\!] \Rightarrow M \Downarrow V}_{\text{Adequacy}}$.

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

for $\gamma \in \{nat, bool\}$

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

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

$\boxed{?}$ $\lhd_{\tau \to \tau'}$?

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 | define $\lhd_{\tau \to \tau'}$
| have $[\![M_1 M_2]\!] \lhd_{\tau'} M_1(M_2)$

$\parallel$

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

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 induction, $[\![M_1]\!] \lhd_{\tau\to\tau'} M_1$ and $[\![M_2]\!] \lhd_{\tau} M_2$

$\rightsquigarrow$ *logical* definition

$[\![\tau]\!] \to [\![\tau']\!]$

$\Downarrow$

$f \lhd_{\tau\to\tau'} M_1 \overset{?}{\iff} \forall x \in [\![\tau]\!].\ x \lhd_{\tau} M_2 .\ f(x) \lhd_{\tau'} M_1(M_2)$

?

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

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

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

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

Want that $[\![\underline{\mathbf{fix}}(M')]\!] \vartriangleleft_\tau \underline{\mathbf{fix}}(M')$

$$\| $$

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

Need to prove a property of a fixed point

Requirements on the formal approximation relations, III

We want to be able to proceed by induction. We do it by Scott Induction

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

$\leadsto$ *admissibility* property

which requires

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

admissible

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

$\bot \lhd_\tau M$

and

$(n \in \mathbb{N})$

$d_0 \sqsubseteq d_1 \sqsubseteq \cdots \sqsubseteq d_n \sqsubseteq \cdots$

$(\forall i \;\; d_i \lhd_\tau M) \Rightarrow \bigsqcup_i d_i \lhd_\tau M$

$\{ d \in [\![\tau]\!] \mid d \lhd_\tau M \}$ is downwards closed

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

$//$

$f = \lambda d \in [\![\tau]\!].\, [\![x:\tau \vdash M]\!][x \mapsto d]$

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

Iff $\forall d \lhd_\tau N.\ f(d) \lhd_{\tau'} (\mathbf{fn}\, x.M)(N)$

$\|$

$[\![x:\tau \vdash M]\!][x \mapsto d]$

by previous lemma we want

$[\![x \vdash M]\!][x \mapsto d] \lhd M[N/x]$

$M[N/x] \Downarrow V \Rightarrow (\mathbf{fn}\, x.M)(N) \Downarrow V$

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

$\Downarrow$ take τ = nat or bool

Adequacy

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

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

<u>In fact:</u> $M_1 \leq_{ctx} M_2 \iff [\![M_1]\!] \lhd M_2$

$M_1, M_2 : \tau_1 \to \tau_2 \to \cdots \to \tau_n \to \gamma$

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

$M_1 \leq_{ctx} M_2$ iff $\forall N_1 N_2 \ldots N_n$. $M_1 N_1 N_2 \cdots N_n \Downarrow \checkmark \Rightarrow M_2 N_1 N_2 \cdots N_n \Downarrow \checkmark$

At a ground type $\gamma \in \{bool, nat\}$,

$M_1 \leq_{\text{ctx}} M_2 : \gamma$ holds if and only if

$$\forall V \in \text{PCF}_\gamma \; (M_1 \Downarrow_\gamma V \implies M_2 \Downarrow_\gamma V) \;.$$

At a function type $\tau \to \tau'$,

$M_1 \leq_{\text{ctx}} M_2 : \tau \to \tau'$ holds if and only if

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

<u>Applicative contexts</u>: $[-] N_1 \cdots N_n$