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:

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

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

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

case

$$M = M_1 M_2 \qquad M_1 : \tau \to \gamma \quad M_2 : \tau$$

case

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

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.

- Define
$$\{ \triangleleft_\tau \subseteq [\![\tau]\!] \times PCF_\tau \}_{\tau \in Types}.$$

- Prove
for all types τ, and Terms M of type τ
$$[\![M]\!] \triangleleft_\tau M$$

- From
$$[\![M]\!] \triangleleft_\gamma M \quad (\gamma \in \{\underline{nat}, \underline{bool}\})$$
we will deduce
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:

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

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

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

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

Idea

$d \in \mathbb{N}_\perp$

$M \in \underline{PCF}_{nat}$

$d \lhd_{nat} M \overset{def}{\iff}$ if $[\![M]\!] = d \in \mathbb{N}$ then $M \Downarrow \underline{succ}^d(0)$

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

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

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

NB: $\perp \lhd_{nat} M$

$\perp \lhd_{bool} M$.

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

Case $\gamma = nat$.

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

$$\Longrightarrow \; [\![M]\!] = [\![\mathbf{succ}^n(\mathbf{0})]\!] \qquad \text{for some } n \in \mathbb{N}$$

$$\Longrightarrow \; n = [\![M]\!] \lhd_\gamma M$$

$$\Longrightarrow \; M \Downarrow \mathbf{succ}^n(\mathbf{0}) \qquad \text{by definition of } \lhd_{nat}$$

Case $\gamma = bool$ is similar.

It remains to define

$$\lhd_{\sigma\to\tau} \subseteq ([\![\sigma]\!] \to [\![\tau]\!]) \times PCF_{\sigma\to\tau}$$

It makes sense to do so compositionally in terms of

$$\lhd_{\sigma} \subseteq [\![\sigma]\!] \times PCF_{\sigma}$$

and

$$\lhd_{\tau} \subseteq [\![\tau]\!] \times PCF_{\tau}$$

But how?

We will proceed "logically" and shape the definition by understanding what is needed from it to be able to prove

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

by structural induction on M.

Requirements on the formal approximation relations, II

We want to be able to proceed by induction.

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

$\rightsquigarrow$ *logical* definition

RTP: $[\![M_1\, M_2]\!] \lhd_\tau M_1\, M_2$

$M_1 : \sigma \to \tau$

$M_2 : \sigma$

$$[\![M_1]\!] \lhd_{\sigma\to\tau} M_1 \qquad \overset{?}{\rightsquigarrow} \qquad [\![M_1\, M_2]\!] \lhd_\tau M_1\, M_2$$

$$[\![M_2]\!] \lhd_\sigma M_2 \qquad\qquad\qquad\qquad \| $$

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

Def (logical)

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

iff_{def}

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

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

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

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

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

Inductive definition of $\{\triangleleft_\tau\}_{\tau \in Types}$

- $n \triangleleft_{nat} M$ iff $(n \in \mathbb{N} \Rightarrow M \Downarrow \underline{\underline{succ}}^n(\underline{0}))$

- $b \triangleleft_{bool} M$ iff $(b = true \Rightarrow M \Downarrow \underline{\underline{true}})$
  $\wedge\ (b = false \Rightarrow M \Downarrow \underline{\underline{false}})$

- $f \triangleleft_{\sigma \to \tau} M$ iff $\forall d, N.$
  $d \triangleleft_\sigma N \Rightarrow f(d) \triangleleft_\tau M N$

▶ Can we now prove $\forall \tau\, \forall M.\ [\![M]\!] \triangleleft_\tau M$?

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

RTP

$$[\![\mathbf{fix}(M')]\!] \lhd_{\tau} \mathbf{fix}(M').$$

<u>RTP</u>

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

$$\|$$

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

<u>Lemma</u>

$\{d \mid d \lhd N\}$

is admissible.

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

$$d \trianglelefteq \underline{\text{fix}}(M') \overset{?}{\Longrightarrow} \underline{[\![M']\!](d) \trianglelefteq \underline{\text{fix}}(M')}$$

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

By induction $[\![M']\!] \trianglelefteq M'$

Then

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

$$\frac{M'(\underline{\text{fix}}\ M') \Downarrow V}{\underline{\text{fix}}(M') \Downarrow V}$$

<u>Lemma</u> $(N \Downarrow V \Rightarrow N' \Downarrow V)$

$$\Rightarrow \quad x \trianglelefteq N \Rightarrow x \trianglelefteq N'$$

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

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

<u>RTP</u>

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

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

TPT

$$\forall\, d \triangleleft_\tau N.\quad [\![\mathbf{fn}\, x.\, M']\!](d) \triangleleft (\mathbf{fn}\, x.\, M')\, N$$

Consider $d \triangleleft_\tau N$.

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

RTP:

$$[\![x:\tau \vdash M']\!](d) \triangleleft (\mathbf{fn}\, x:\tau.\, M')\, N \quad (*)$$

To show $(*)$, by previous lemma, it will be enough to show

Fundamental Lemma

$$[\![x:\tau \vdash M']\!](d) \triangleleft M'[N/x]$$

$$\frac{M'[N/x] \Downarrow V}{(\mathbf{fn}\, x:\tau.\, M')\, N \Downarrow V}$$

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*

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

$\Downarrow$

Case $n=0$ $\qquad [\![M]\!] \lhd_\tau M$

$\Downarrow$

Case $\tau = \gamma \in \{nat, bool\}$

$\Downarrow$

Adequacy.

Fundamental property

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

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 $x \in dom(\Gamma)$.

Implications to Contextual Equivalence

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

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

Proposition For all PCF types and all closed PCF terms M_1, M_2 of type τ,

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

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

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

m | applicative contexts [ ] M |