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

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

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:

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

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

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

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

For γ a ground type (i.e. nat or bool) and for all terms M of type γ and all values V of type γ, $[\![M]\!] = [\![V]\!] \Rightarrow M \Downarrow V$.

CASE $M \equiv M_1\, M_2$ $\qquad \underbrace{M_1 : \tau \to \gamma}_{\text{NOT OF GROUND TYPE!}} \qquad M_2 : \tau$

CASE $\quad M = \underline{fix}(M') \qquad M' : \gamma \to \gamma$

NOT OF GROUND TYPE!

<u>Moral</u>: We need a more general statement applicable to all types, and implying adequacy at ground types.

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.

relates

semantics & syntax

denotations

terms

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

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

- From
$$[\![M]\!] \lhd_\gamma M \quad (\gamma \in \{\underline{nat}, \underline{bool}\})$$
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.

• How should we define $\lhd_\gamma \subseteq [\![\gamma]\!] \times \underline{PCF}_\gamma$ at ground type $\gamma \in \{\underline{nat}, \underline{bool}\}$?

Requirements on the formal approximation relations, I

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

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

for $\gamma = nat$

For $d \in \mathbb{N}_\perp$, $M \in PCF_{nat}$ $\quad [\![M]\!] = n \in \mathbb{N} \Rightarrow M \Downarrow_{nat} \underline{succ}^n(\underline{0})$

$$(d \lhd_{nat} M) \overset{def}{\Longleftrightarrow} \left(d \in \mathbb{N} \Rightarrow M \Downarrow_{nat} \underline{succ}^d(\underline{0})\right).$$

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

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

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

NB. $\perp \lhd_{nat} M$ for all $M \in \mathrm{PCF}_{nat}$
$\perp \lhd_{bool} M$ for all $M \in \mathrm{PCF}_{bool}$

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.

It remains to define

$$\triangleleft_{\sigma\to\tau} \subseteq (\llbracket\sigma\rrbracket \to \llbracket\tau\rrbracket) \times PCF_{\sigma\to\tau}$$

It makes sense to do so compositionally in terms of

$$\triangleleft_{\sigma} \subseteq \llbracket\sigma\rrbracket \times PCF_{\sigma}$$

and

$$\triangleleft_{\tau} \subseteq \llbracket\tau\rrbracket \times PCF_{\tau}$$

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

CASE $M = M_1\, M_2$ $\qquad M_1 : \sigma \to \tau,\ M_2 : \sigma$

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

That is, $[\![M_1]\!]\left([\![M_2]\!]\right) \lhd_\tau M_1\, M_2$

?

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

and $[\![M_2]\!] \lhd_\sigma M_2$

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

$f \in \left([\![\sigma]\!] \to [\![\tau]\!]\right)$
$M : \sigma \to \tau$

$f \lhd_{\sigma\to\tau} M$ iff$_{\text{def}}$ whenever $d \lhd_\sigma N$ it follows that $f(d) \lhd_\tau MN$

Definition of

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

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

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

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

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

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

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

- $f \triangleleft_{\sigma \to \tau} M$ 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

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

<u>RTP</u>: $[\![\underline{fix}(M')]\!] \lhd_\tau \underline{fix}(M')$

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

?

By induction $[\![M']\!] \lhd_{\tau\to\tau} M'$

Lemma
$\{ d \in [\![\tau]\!] \mid d \lhd_\tau \underline{fix}(M') \}$
is admissible

Scott Induction

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

$$\left.\begin{array}{l} [\![M']\!] \triangleleft_{\tau\to\tau} M' \\ d \triangleleft_{\tau} \underline{fix}(M') \end{array}\right] \Longrightarrow [\![M']\!](d) \triangleleft_{\tau} M'(fix\,M')$$

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

?

<u>Lemma</u>

whenever $N \Downarrow V \Rightarrow N' \Downarrow V$

if $x \triangleleft_{\sigma} N$ then $x \triangleleft_{\sigma} N'$

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

CASE $M = \underline{fn}\, x{:}\tau.\, M'$ where $[x \mapsto \tau] \vdash M' : \tau'$

<u>RTP</u> $[\![\underline{fn}\, x{:}\tau.\, M']\!] \lhd_{\tau \to \tau'} \underline{fn}\, x{:}\tau.\, M'$

$$\| $$

$$\lambda d \in [\![\tau]\!].\ [\![[x \mapsto \tau] \vdash M']\!] [x \mapsto d]$$

that is, for all $d \lhd_\tau N$,

$[\![[x \mapsto \tau] \vdash M']\!] [x \mapsto d] \lhd_{\tau'} (\underline{fn}\, x{:}\tau.\, M')(N)$

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

Fundamental Lemma

$\|$ for all $d \lhd_\tau N$,

$[\![[x \mapsto \tau] \vdash M']\!] [x \mapsto d] \lhd_{\tau'} M'[N/x]$ $\|$

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

$$\Downarrow \; n = 0$$

$$\forall \tau . \forall M . \; [\![M]\!] \lhd_\tau M$$

$$\Downarrow \; \tau \in \{ \underline{nat}, \underline{bool} \}$$

ADEQUACY

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

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