

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

$$\llbracket M \rrbracket = \llbracket V \rrbracket \in \llbracket \gamma \rrbracket \implies M \Downarrow_\gamma V .$$

Adequacy

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

$$\llbracket M \rrbracket = \llbracket V \rrbracket \in \llbracket \gamma \rrbracket \implies M \Downarrow_\gamma V .$$

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

$$\llbracket M \rrbracket = \llbracket V \rrbracket \in \llbracket \gamma \rrbracket \implies M \Downarrow_\gamma V.$$

NB. Adequacy does not hold at function types:

$$\llbracket \mathbf{fn} \ x : \tau. (\mathbf{fn} \ y : \tau. y) \ x \rrbracket = \llbracket \mathbf{fn} \ x : \tau. x \rrbracket : \llbracket \tau \rrbracket \rightarrow \llbracket \tau \rrbracket$$

but

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

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

For τ a ground type (i.e. not or bool) and for all terms M of type τ and all values V of type τ , $\llbracket M \rrbracket = \llbracket V \rrbracket \Rightarrow M \Downarrow V$.

CASE $M \equiv M_1 M_2$ $M_1: \tau \rightarrow \tau$ $M_2: \tau$

NOT OF GROUND TYPE!

CASE $M = \underline{\text{fix}}(M')$

$M': \tau \rightarrow \tau$



NOT OF GROUND TYPE!

Moral: 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 $\{\triangleleft_z \subseteq \llbracket z \rrbracket \times PCF_z\}_{z \in \text{types}}$.

- Prove for all types z , and terms M of type z
 $\llbracket M \rrbracket \triangleleft_z M$

- From $\llbracket M \rrbracket \triangleleft_x M$ ($x \in \{\underline{\text{nat}}, \underline{\text{bool}}\}$)

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:

$$\llbracket M \rrbracket \triangleleft_{\tau} M \text{ for all types } \tau \text{ and all } M \in \text{PCF}_{\tau}$$

where the *formal approximation relations*

$$\triangleleft_{\tau} \subseteq \llbracket \tau \rrbracket \times \text{PCF}_{\tau}$$

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

- How should we define
 $\triangleleft_\gamma \subseteq \llbracket \mathcal{T} \rrbracket \times \text{PCF}_\gamma$

at ground type $\gamma \in \{\underline{\text{nat}}, \underline{\text{bool}}\}$?

Requirements on the formal approximation relations, I

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

$$\llbracket M \rrbracket \triangleleft_\gamma M \text{ implies } \underbrace{\forall V (\llbracket M \rrbracket = \llbracket V \rrbracket \Rightarrow M \Downarrow_\gamma V)}_{\text{adequacy}}$$

for $\gamma = \text{nat}$
 For $d \in \mathbb{N}_\perp, M \in \text{PCF}_{\text{nat}}$ $\llbracket M \rrbracket = n \in \mathbb{N} \Rightarrow M \Downarrow_{\text{nat}} \underline{\text{succ}}^n(\underline{0})$

$$(d \triangleleft_{\text{nat}} M) \stackrel{\text{def}}{\iff} (d \in \mathbb{N} \Rightarrow M \Downarrow_{\text{nat}} \underline{\text{succ}}^d(\underline{0})) .$$

Definition of $d \triangleleft_\gamma M$ ($d \in \llbracket \gamma \rrbracket, M \in \text{PCF}_\gamma$)
for $\gamma \in \{\text{nat}, \text{bool}\}$

$$n \triangleleft_{\text{nat}} M \stackrel{\text{def}}{\iff} (n \in \mathbb{N} \Rightarrow M \Downarrow_{\text{nat}} \mathbf{succ}^n(\mathbf{0}))$$

$$b \triangleleft_{\text{bool}} M \stackrel{\text{def}}{\iff} (b = \text{true} \Rightarrow M \Downarrow_{\text{bool}} \mathbf{true}) \\ \& (b = \text{false} \Rightarrow M \Downarrow_{\text{bool}} \mathbf{false})$$

NB. $\perp \triangleleft_{\text{nat}} M$ for all $M \in \text{PCF}_{\text{nat}}$
 $\perp \triangleleft_{\text{bool}} M$ for all $M \in \text{PCF}_{\text{bool}}$

Proof of: $\llbracket M \rrbracket \triangleleft_\gamma M$ implies adequacy

Case $\gamma = \text{nat}$.

$$\llbracket M \rrbracket = \llbracket V \rrbracket$$

$$\implies \llbracket M \rrbracket = \llbracket \text{succ}^n(\mathbf{0}) \rrbracket \quad \text{for some } n \in \mathbb{N}$$

$$\implies n = \llbracket M \rrbracket \triangleleft_\gamma M$$

$$\implies M \Downarrow \text{succ}^n(\mathbf{0}) \quad \text{by definition of } \triangleleft_{\text{nat}}$$

Case $\gamma = \text{bool}$ is similar.

It remains to define

$$\Delta_{\sigma \rightarrow \tau} \subseteq ([\![\sigma]\!] \rightarrow [\![\tau]\!]) \times \text{PCF}_{\sigma \rightarrow \tau}$$

It makes sense to do so compositionally
in terms of

and $\Delta_{\sigma} \subseteq [\![\sigma]\!] \times \text{PCF}_{\sigma}$

$$\Delta_{\tau} \subseteq [\![\tau]\!] \times \text{PCF}_{\tau}$$

But how?

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

$$\llbracket M \rrbracket \triangleleft_c M$$

by structural induction on M .

Requirements on the formal approximation relations, II

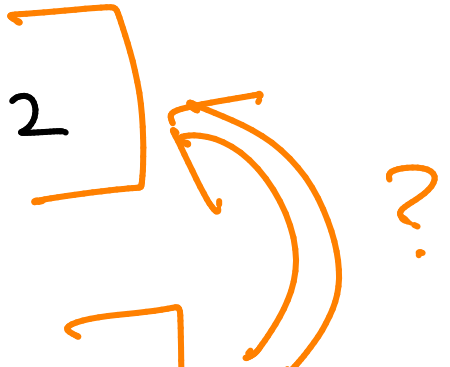
We want to be able to proceed by induction.

► Consider the case $M = M_1 M_2$.

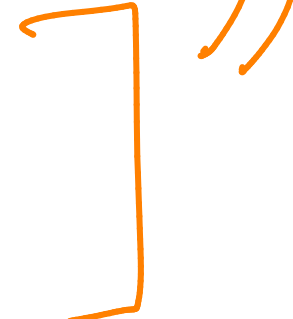
\rightsquigarrow *logical* definition

CASE $M = M_1 M_2$ $M_1: \sigma \rightarrow \tau, M_2: \sigma$

RTP $\llbracket M_1 M_2 \rrbracket \triangleleft_\tau M_1 M_2$

That is, $\llbracket M_1 \rrbracket (\llbracket M_2 \rrbracket) \triangleleft_\tau M_1 M_2$ 

By induction

$\llbracket M_1 \rrbracket \triangleleft_{\sigma \rightarrow \tau} M_1$
and $\llbracket M_2 \rrbracket \triangleleft_\sigma M_2$ 

Define $\triangleleft_{\sigma \rightarrow \tau} \subseteq (\llbracket \sigma \rrbracket \rightarrow \llbracket \tau \rrbracket) \times \text{PCF}_{\sigma \rightarrow \tau}$
 $f \in (\llbracket \sigma \rrbracket \rightarrow \llbracket \tau \rrbracket)$
 $M: \sigma \rightarrow \tau$ $f \triangleleft_{\sigma \rightarrow \tau} M$ iff def whenever $d \triangleleft_\sigma N$ it follows that $f(d) \triangleleft_\tau MN$

Definition of

$$f \triangleleft_{\tau \rightarrow \tau'} M \quad (f \in ([\tau] \rightarrow [\tau']), M \in \text{PCF}_{\tau \rightarrow \tau'})$$

$$f \triangleleft_{\tau \rightarrow \tau'} M$$

$$\stackrel{\text{def}}{\Leftrightarrow} \quad \forall x \in [\tau], N \in \text{PCF}_{\tau}$$

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

Inductive definition of $\{\Delta_z\}_{z \in \text{types}}$

- $n \Delta_{nat} M$ iff $(n \in \mathbb{N} \Rightarrow M \Downarrow \underline{\underline{succ^n(0)}})$
- $b \Delta_{bool} M$ iff $\wedge \begin{cases} (b = \text{true} \Rightarrow M \Downarrow \underline{\underline{true}}) \\ (b = \text{false} \Rightarrow M \Downarrow \underline{\underline{false}}) \end{cases}$
- $f \Delta_{\sigma \rightarrow \tau} M$ iff $\forall d, N.$
 $d \Delta_{\sigma} N \Rightarrow f(d) \Delta_{\tau} MN$

► Can we now prove $\forall z \forall M. \llbracket M \rrbracket \Delta_z M$?

Requirements on the formal approximation relations, III

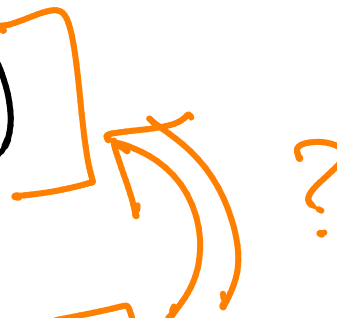
We want to be able to proceed by induction.

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

\rightsquigarrow *admissibility* property

CASE $M = \underline{\text{fix}}(M')$ $M' : \tau \rightarrow \tau$

RTP: $\llbracket \underline{\text{fix}}(M') \rrbracket \triangleq_{\tau} \underline{\text{fix}}(M')$

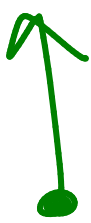
that is, $\underline{\text{fix}} \llbracket M' \rrbracket \triangleq_{\tau} \underline{\text{fix}}(M')$ 

By induction

$\llbracket M' \rrbracket \triangleq_{\tau \rightarrow \tau} M'$ 

Scott Induction

Lemma
 $\{d \in \llbracket \tau \rrbracket \mid d \triangleq_{\tau} \underline{\text{fix}}(M')\}$
is admissible

$d \triangleq_{\tau} \underline{\text{fix}}(M') \stackrel{?}{\Rightarrow} \llbracket M' \rrbracket(d) \triangleq_{\tau} \underline{\text{fix}}(M')$
 $\underline{\text{fix}} \llbracket M' \rrbracket \triangleq_{\tau} \underline{\text{fix}}(M')$ 

$$\begin{array}{l}
 \left[\begin{array}{l} \llbracket M' \rrbracket \trianglelefteq_{\mathcal{Z}} M' \\ d \trianglelefteq_{\mathcal{Z}} \text{fix}(M') \end{array} \right] \Rightarrow \llbracket M' \rrbracket(d) \trianglelefteq_{\mathcal{Z}} M'(\text{fix } M') \\
 \stackrel{?}{\Rightarrow} \llbracket M' \rrbracket(d) \trianglelefteq_{\mathcal{Z}} \text{fix}(M') \quad \swarrow \quad ?
 \end{array}$$

Lemma

whenever $N \Downarrow V \Rightarrow N' \Downarrow V$
 if $x \trianglelefteq_{\delta} N$ Then $x \trianglelefteq_{\delta} N'$

Admissibility property

Lemma. *For all types τ and $M \in \text{PCF}_\tau$, the set*

$$\{ d \in \llbracket \tau \rrbracket \mid d \triangleleft_\tau M \}$$

is an admissible subset of $\llbracket \tau \rrbracket$.

Further properties

Lemma. For all types τ , elements $d, d' \in \llbracket \tau \rrbracket$, and terms $M, N, V \in \text{PCF}_\tau$,

1. If $d \sqsubseteq d'$ and $d' \triangleleft_\tau M$ then $d \triangleleft_\tau M$.
2. If $d \triangleleft_\tau M$ and $\forall V (M \Downarrow_\tau V \implies N \Downarrow_\tau V)$ then $d \triangleleft_\tau N$.

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

$$\underline{R\tau P} \quad \llbracket \underline{\text{fn}} x: \tau. M' \rrbracket \triangleleft_{\tau \rightarrow \tau'} \underline{\text{fn}} x: \tau. M'$$

$$\parallel \lambda d \in \llbracket \tau \rrbracket. \llbracket [x \mapsto \tau] \vdash M' \rrbracket [x \mapsto d] \parallel$$

that is, for all $d \triangleleft_{\tau'} N$,

$$\llbracket [x \mapsto \tau] \vdash M' \rrbracket [x \mapsto d] \triangleleft_{\tau'} (\underline{\text{fn}} x: \tau. M')(N)$$

$\nearrow M'[N/x] \Downarrow \checkmark$ implies $(\underline{\text{fn}} x: \tau. M')(N) \Downarrow \checkmark$
Fun denotational Lemma

$$\parallel \text{for all } d \triangleleft_{\tau'} N, \llbracket [x \mapsto \tau] \vdash M' \rrbracket [x \mapsto d] \triangleleft_{\tau'} M'[N/x] \parallel$$

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 $d_1 \triangleleft_{\tau_1} M_1, \dots, d_n \triangleleft_{\tau_n} M_n$ then $\llbracket \Gamma \vdash M \rrbracket [x_1 \mapsto d_1, \dots, x_n \mapsto d_n] \triangleleft_{\tau} M[M_1/x_1, \dots, M_n/x_n]$.

$\Downarrow n=0$

$\forall z. \forall M. \llbracket M \rrbracket \triangleleft_z M$

$\Downarrow z \in \{\underline{nat}, \underline{bool}\}$

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 $\Gamma \vdash M_1 \leq_{\text{ctx}} M_2 : \tau$ 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 $\gamma = \text{nat}$ or $\gamma = \text{bool}$, and for all values $V \in \text{PCF}_\gamma$,

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

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

$$M_1 \leq_{ctx} M_2 : \tau \quad \text{iff} \quad \llbracket M_1 \rrbracket \triangleleft_{\tau} M_2$$

Extensionality properties of \leq_{ctx}

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 $\tau \rightarrow \tau'$,

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

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