Lecture 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 $M_1 M_2$, $\mathbf{fix}(M')$, $\mathbf{fn}\, x : \tau . M'$.

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

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

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

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

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

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

Case $\gamma = nat$.

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

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

$$\implies n = [\![M]\!] \vartriangleleft_\gamma M$$

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

Case $\gamma = bool$ is similar.

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

Definition of

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

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

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

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

Requirements on the formal approximation relations, III

We want to be able to proceed by induction.

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

$$\leadsto \textit{admissibility} \text{ property}$$

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 $M = \mathbf{fn}\, x : \tau \,.\, M'$.

$$\rightsquigarrow \textit{substitutivity} \text{ property for open terms}$$

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*

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

NB. The case $\Gamma = \emptyset$ reduces to

$$\llbracket M \rrbracket \lhd_\tau M$$

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

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

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

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 $\tau \to \tau'$,

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

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