Denotational semantics of PCF

Proposition. *For all typing judgements* $\Gamma \vdash M : \tau$, *the denotation*

$$[\![\Gamma \vdash M]\!] : [\![\Gamma]\!] \to [\![\tau]\!]$$

is a well-defined continous function.

Denotations of closed terms

For a closed term $M \in \mathrm{PCF}_\tau$, we get

$$[\![\emptyset \vdash M]\!] : [\![\emptyset]\!] \to [\![\tau]\!]$$

and, since $[\![\emptyset]\!] = \{\perp\}$, we have

$$[\![M]\!] \stackrel{\text{def}}{=} [\![\emptyset \vdash M]\!](\perp) \in [\![\tau]\!] \qquad (M \in \mathrm{PCF}_\tau)$$

Compositionality

Proposition. *For all typing judgements* $\Gamma \vdash M : \tau$ *and* $\Gamma \vdash M' : \tau$*, and all contexts* $\mathcal{C}[-]$ *such that* $\Gamma' \vdash \mathcal{C}[M] : \tau'$ *and* $\Gamma' \vdash \mathcal{C}[M'] : \tau'$*,*

if $[\![\Gamma \vdash M]\!] = [\![\Gamma \vdash M']\!] : [\![\Gamma]\!] \to [\![\tau]\!]$

then $[\![\Gamma' \vdash \mathcal{C}[M]]\!] = [\![\Gamma' \vdash \mathcal{C}[M]]\!] : [\![\Gamma']\!] \to [\![\tau']\!]$

by induction $[\![M_1]\!] = [\![\mathbf{fn}\, x . M]\!] \overset{*}{=} \lambda d.\, [\![x \mapsto M]\!](d)$

substitution lemma

$? = [\![M[M_2/x]]\!] = [\![V]\!]$

$[\![M_1(M_2)]\!] = [\![M_1]\!]([\![M_2]\!]) \overset{\text{by } *}{=} [\![x \mapsto M]\!]([\![M_2]\!]) =$

Soundness

Proposition. *For all closed terms* $M, V \in \mathrm{PCF}_\tau$,

if $M \Downarrow_\tau V$ *then* $[\![M]\!] = [\![V]\!] \in [\![\tau]\!]$.

$$\frac{M_1 \Downarrow \mathbf{fn}\, x . M \qquad M[M_2/x] \Downarrow V}{M_1(M_2) \Downarrow V}$$

Substitution property

Proposition. *Suppose that* $\Gamma \vdash M : \tau$ *and that* $\Gamma[x \mapsto \tau] \vdash M' : \tau'$*, so that we also have* $\Gamma \vdash M'[M/x] : \tau'$*.*

Then,

$$\begin{aligned} &[\![\Gamma \vdash M'[M/x]]\!](\rho) \\ &\quad = [\![\Gamma[x \mapsto \tau] \vdash M']\!]\big(\rho[x \mapsto [\![\Gamma \vdash M]\!]]\big) \end{aligned}$$

for all $\rho \in [\![\Gamma]\!]$*.*

Substitution = application

Substitution property

Proposition. *Suppose that* $\Gamma \vdash M : \tau$ *and that* $\Gamma[x \mapsto \tau] \vdash M' : \tau'$*, so that we also have* $\Gamma \vdash M'[M/x] : \tau'$*.*

Then,

$$\llbracket \Gamma \vdash M'[M/x] \rrbracket (\rho)$$
$$= \llbracket \Gamma[x \mapsto \tau] \vdash M' \rrbracket \big(\rho\big[x \mapsto \llbracket \Gamma \vdash M \rrbracket\big]\big)$$

for all $\rho \in \llbracket \Gamma \rrbracket$*.*

In particular when $\Gamma = \emptyset$, $\llbracket \langle x \mapsto \tau \rangle \vdash M' \rrbracket : \llbracket \tau \rrbracket \to \llbracket \tau' \rrbracket$ and

$$\llbracket M'[M/x] \rrbracket = \llbracket \langle x \mapsto \tau \rangle \vdash M' \rrbracket (\llbracket M \rrbracket)$$

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

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:

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

$$\lambda d.\, [\![x \vdash (\mathrm{fn}\, y.\, y)\, x]\!](d) \qquad \lambda d.\, [\![x \vdash x]\!](d) = \lambda d.\, d$$

$$= \lambda d.\, [\![x \vdash \mathrm{fn}\, y.\, y]\!](d)\,([\![x \vdash x]\!]\, d) = \lambda d\, (\lambda e.\, e)\, d = \lambda d.\, d$$

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

$$[\![M]\!] = [\![V]\!] \Rightarrow M \Downarrow_{\gamma} V$$

$$M = M_1(M_2) \quad \leadsto \quad M_1 : \tau \to \sigma \qquad M_2 : \tau$$

τ not of ground type, so cannot proceed.

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

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.

   logical relation

   This statement roughly takes the form:

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

   where the *formal approximation relations*

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

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

$[\![M]\!] \lhd_\tau M$
⇓ WANT
Adequacy

Requirements on the formal approximation relations, I

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

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

$\lhd_{nat} \subseteq \mathbb{N}_\perp \times PCF_{nat}$

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

$n \neq \perp$

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

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

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.

Ind $[\![M_1]\!] \triangleleft_{\tau' \to \tau} M_1$

$[\![M_2]\!] \triangleleft_{\tau'} M_2$

Requirements on the formal approximation relations, II

We want to be able to proceed by induction.

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

WANT — to get it we define $\triangleleft_{\tau' \to \tau}$ in a manner that it will work; namely

$\rightsquigarrow$ *logical* definition

$$[\![M_1]\!]([\![M_2]\!]) = [\![M_1(M_2)]\!] \triangleleft_{\tau} M_1(M_2)$$

LOGICALLY

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

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

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

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

by ind $[\![M']\!] \lhd_{\tau\to\tau'} M'$

WANT ~ idea is to use

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

$\{x \mid x \lhd_\tau M\}$ admissible.

$\bigsqcup_n [\![M']\!]^n(\bot)$

$= \mathrm{fix}\, [\![M']\!]$

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

— $\lhd_{\tau \to \tau'}^{M}$ admissible

$f_0 \subseteq f_1 \subseteq \cdots \subseteq f_n \subseteq \cdots$? $\quad f_n \lhd M \Rightarrow \bigsqcup f_n \lhd M$

Assume $f_n \lhd M$ $\quad$ RTP $x \lhd N \Rightarrow (\bigsqcup f_n)(x) \lhd M(N)$

Admissibility property

$f_n(x) \lhd M(N) \xRightarrow{\text{ind}}$ $\quad \bigsqcup_n (f_n(x))$

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* $d \lhd_\tau N$.

crucial to get the induction for

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

Requirements on the formal approximation relations, IV

We want to be able to proceed by induction.

- Consider the case $M = \mathbf{fn}\, x : \tau \,.\, M'$.

$\leadsto$ *substitutivity* property for open terms

$$[\![x \vdash M]\!](e)$$

$$\forall e \lhd N.\ (\lambda d\, [\![x \vdash M]\!](d))(e) \lhd (\mathbf{fn}\, x . M)\, N$$

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

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

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 $x \in dom(\Gamma)$.