Topic 7

Relating Denotational and Operational Semantics

Recall:

PCF denotational semantics — aims

- PCF types $\tau \;\mapsto\;$ domains $[\![\tau]\!]$.
- Closed PCF terms $M : \tau \;\mapsto\;$ elements $[\![M]\!] \in [\![\tau]\!]$.

  Denotations of open terms will be continuous functions.
- Compositionality.

  In particular: $[\![M]\!] = [\![M']\!] \;\Rightarrow\; [\![\mathcal{C}[M]]\!] = [\![\mathcal{C}[M']]\!]$.
- Soundness.

  For any type τ, $M \Downarrow_\tau V \;\Rightarrow\; [\![M]\!] = [\![V]\!]$.
- Adequacy.

  For $\tau = bool$ or nat, $[\![M]\!] = [\![V]\!] \in [\![\tau]\!] \implies M \Downarrow_\tau V$.

e.g. if $M : nat$ & $[\![M]\!] = n \in \mathbb{N}$, then $M \Downarrow_{nat} succ^n(0)$

Recall:

Theorem. *For all types* τ *and closed terms* $M_1, M_2 \in \mathrm{PCF}_\tau$, *if* $[\![M_1]\!]$ *and* $[\![M_2]\!]$ *are equal elements of the domain* $[\![\tau]\!]$, *then* $M_1 \cong_{\mathrm{ctx}} M_2 : \tau$.

Proof.

$$\mathcal{C}[M_1] \Downarrow_{nat} V \Rightarrow [\![\mathcal{C}[M_1]]\!] = [\![V]\!] \quad \text{(soundness)}$$

$$\Rightarrow [\![\mathcal{C}[M_2]]\!] = [\![V]\!] \quad \text{(compositionality on } [\![M_1]\!] = [\![M_2]\!]\text{)}$$

$$\Rightarrow \mathcal{C}[M_2] \Downarrow_{nat} V \quad \text{(adequacy)}$$

and symmetrically (& similarly for $\Downarrow_{bool}$). $\square$

Soundness

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

$$\text{if } M \Downarrow_\tau V \text{ then } [\![M]\!] = [\![V]\!] \in [\![\tau]\!] \ .$$

Proof: by rule induction for $M \Downarrow_\tau V$

Induction step for $(\Downarrow_{\text{cbn}})$ $$\frac{M_1 \Downarrow_{\tau \to \tau'} \mathbf{fn}\, x : \tau\, M \qquad M[M_2/x] \Downarrow_{\tau'} V}{M_1\, M_2 \Downarrow_{\tau'} V}$$

Suppose $\begin{cases} [\![M_1]\!] = [\![\mathbf{fn}\, x : \tau .\, M]\!] \\ [\![M[M_2/x]]\!] = [\![V]\!] \end{cases}$

Have to prove $[\![M_1 M_2]\!] = [\![V]\!]$.

Induction step for $(\Downarrow_{\mathrm{cbn}})$
$$\frac{M_1 \Downarrow_{\tau \to \tau'} \mathbf{fn}\, x : \tau\, M \qquad M[M_2/x] \Downarrow_{\tau'} V}{M_1 M_2 \Downarrow_{\tau'} V}$$

Suppose $\begin{cases} [\![M_1]\!] = [\![\mathbf{fn}\, x : \tau .\, M]\!] \\ [\![M[M_2/x]]\!] = [\![V]\!] \end{cases}$

Have to prove $[\![M_1 M_2]\!] = [\![V]\!]$.

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

by definition of $[\![-]\!]$

Induction step for $(\Downarrow_{\mathrm{cbn}})$ $\dfrac{M_1 \Downarrow_{\tau\to\tau'} \mathbf{fn}\, x:\tau\, M \qquad M[M_2/x] \Downarrow_{\tau'} V}{M_1\, M_2 \Downarrow_{\tau'} V}$

Suppose $\begin{cases} [\![M_1]\!] = [\![\mathbf{fn}\, x:\tau .\, M]\!] \\ [\![M[M_2/x]]\!] = [\![V]\!] \end{cases}$

Have to prove $[\![M_1 M_2]\!] = [\![V]\!]$.

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

$$= \underbrace{[\![\mathbf{fn}\, x:\tau .\, M]\!]}_{\lambda d \in [\![\tau]\!] .\, [\![x \mapsto \tau \vdash M]\!](d)} ([\![M_2]\!])$$

Induction step for $(\Downarrow_{cbn})$ $\dfrac{M_1 \Downarrow_{\tau\to\tau'} \mathbf{fn}\, x:\tau\, M \qquad M[M_2/x] \Downarrow_{\tau'} V}{M_1 M_2 \Downarrow_{\tau'} V}$

Suppose $\begin{cases} [\![M_1]\!] = [\![\mathbf{fn}\, x:\tau.\, M]\!] \\ [\![M[M_2/x]]\!] = [\![V]\!] \end{cases}$

Have to prove $[\![M_1 M_2]\!] = [\![V]\!]$.

But
$$\begin{aligned}
[\![M_1 M_2]\!] &= [\![M_1]\!]([\![M_2]\!]) \\
&= [\![\mathbf{fn}\, x:\tau.\, M]\!]([\![M_2]\!]) \\
&= [\![\, x \mapsto \tau \vdash M]\!]([\![M_2]\!])
\end{aligned}$$

by definition of $[\![-]\!]$

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,

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

for all $\rho \in [\![\Gamma]\!]$. (Proved by induction on structure of M')

In particular when $\Gamma = \emptyset$, $[\![x \mapsto \tau \vdash M']\!] : [\![\tau]\!] \to [\![\tau']\!]$ and

$$\boxed{[\![M'[M/x]]\!] = [\![x \mapsto \tau \vdash M']\!]([\![M]\!])}$$

Induction step for $(\Downarrow_{cbn})$ $\dfrac{M_1 \Downarrow_{\tau\to\tau'} \mathbf{fn}\, x:\tau\, M \qquad M[M_2/x] \Downarrow_{\tau'} V}{M_1 M_2 \Downarrow_{\tau'} V}$

Suppose $\begin{cases} [\![M_1]\!] = [\![\mathbf{fn}\, x:\tau.\, M]\!] \\ [\![M[M_2/x]]\!] = [\![V]\!] \end{cases}$

Have to prove $[\![M_1 M_2]\!] = [\![V]\!]$.

But
$$\begin{aligned} [\![M_1 M_2]\!] &= [\![M_1]\!]([\![M_2]\!]) \\ &= [\![\mathbf{fn}\, x:\tau.\, M]\!]([\![M_2]\!]) \\ &= [\![x \mapsto \tau \vdash M]\!]([\![M_2]\!]) \\ &= [\![M[M_2/x]]\!] \end{aligned}$$

Induction step for $(\Downarrow_{\mathrm{cbn}})$ $$\frac{M_1 \Downarrow_{\tau\to\tau'} \mathbf{fn}\, x : \tau\, M \qquad M[M_2/x] \Downarrow_{\tau'} V}{M_1 M_2 \Downarrow_{\tau'} V}$$

Suppose $\begin{cases} [\![M_1]\!] = [\![\mathbf{fn}\, x : \tau .\, M]\!] \\ [\![M[M_2/x]]\!] = [\![V]\!] \end{cases}$

Have to prove $[\![M_1 M_2]\!] = [\![V]\!]$.

But
$$\begin{aligned} [\![M_1 M_2]\!] &= [\![M_1]\!]([\![M_2]\!]) \\ &= [\![\mathbf{fn}\, x : \tau .\, M]\!]([\![M_2]\!]) \\ &= [\![x \mapsto \tau \vdash M]\!]([\![M_2]\!]) \\ &= [\![M[M_2/x]]\!] = [\![V]\!] \end{aligned}$$

Q.E.D.

Adequacy

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

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

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:

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

$$\parallel$$

$$\lambda d \in [\![\tau]\!] . d$$

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

of type nat or bool

M_1 & M' are of function type

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.

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*

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

   closed PCF terms of type τ

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

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

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

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

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

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

equivalently:

$$d = \bot \;\vee\; (d \in \mathbb{N} \wedge M \Downarrow_{nat} \mathrm{succ}^d(0))$$

Definition of

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

Definition of

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

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

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

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

The full

Definition of $d \lhd_\tau M$ ($d \in [\![\tau]\!], M \in \mathrm{PCF}_\tau$)

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

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

$$d \lhd_{\tau \to \tau'} M \overset{\text{def}}{\Leftrightarrow} \forall e, N \ (e \lhd_\tau N \Rightarrow d(e) \lhd_{\tau'} M\, N)$$

Fundamental property

Theorem. *For all* $\Gamma = \{x_1 \mapsto \tau_1, \ldots, x_n \mapsto \tau_n\}$ *and all* $\Gamma \vdash M : \tau$, *if* $d_1 \lhd_{\tau_1} M_1, \ldots, d_n \lhd_{\tau_n} M_n$ *then*

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

Fundamental property

Theorem. *For all* $\Gamma = [x_1 \mapsto \tau_1, \dots, x_n \mapsto \tau_n]$ *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 $M \in \mathrm{PCF}_\tau$.

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

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 $[\![\tau]\!]$.

(Easy proof by induction on structure of types τ.)

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

(Easy proofs by induction on structure of types τ.)

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*

$$\rho \lhd_\Gamma \sigma \;\Rightarrow\; [\![\Gamma \vdash M]\!](\rho) \lhd_\tau M[\sigma]$$

(Proof by rule induction for $\Gamma \vdash M : \tau$ — see sect. 7.2)

- $\rho \lhd_\Gamma \sigma$ 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 $x \in dom(\Gamma)$.

Proof of Adequacy property

Case $\gamma = nat$.

$$
\begin{aligned}
\llbracket M \rrbracket = \llbracket V \rrbracket & \\
\implies\ & \llbracket M \rrbracket = \llbracket \mathbf{succ}^n(\mathbf{0}) \rrbracket && \text{for some } n \in \mathbb{N} \\
\implies\ & n = \llbracket M \rrbracket \lhd_\gamma M && \text{by Fundamental Property} \\
\implies\ & M \Downarrow \mathbf{succ}^n(\mathbf{0}) && \text{by definition of } \lhd_{nat}
\end{aligned}
$$

Case $\gamma = bool$ is similar.