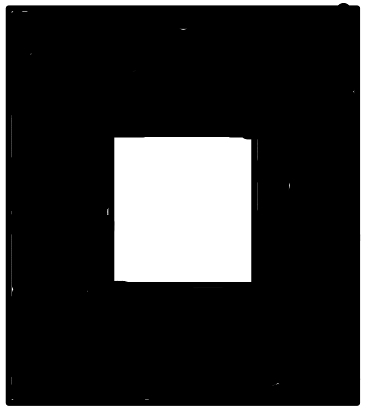
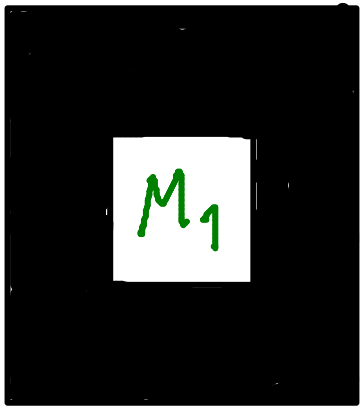
Intuitively, two program phrases are contextually equivalent whenever there is no observable computational difference between running either of them within any given complete program.

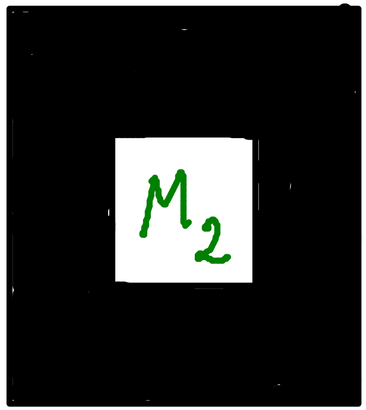
THE IDEA OF CONTEXTUAL EQUIVALENCE

$$M_1 \cong_{ctx} M_2$$

iff

for all program contexts 

running 

and running 

is computationally indistinguishable

Contextual equivalence

Two phrases of a programming language are contextually equivalent if any occurrences of the first phrase in a complete program can be replaced by the second phrase without affecting the observable results of executing the program.

Contextual equivalence of PCF terms

Given PCF terms M_1, M_2, PCF type τ, and a type environment Γ, the relation $\boxed{\Gamma \vdash M_1 \cong_{\mathrm{ctx}} M_2 : \tau}$ 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 $V : \gamma$,

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

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, $[\![M]\!] = [\![V]\!] \in [\![\tau]\!] \;\Longrightarrow\; M \Downarrow_\tau V$.

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. □

Proof principle

To prove

$$M_1 \cong_{\mathrm{ctx}} M_2 : \tau$$

it suffices to establish

$$[\![M_1]\!] = [\![M_2]\!] \text{ in } [\![\tau]\!]$$

Example $[\![\underline{\text{pred}}(0)]\!] = \bot = [\![\Omega_{nat}]\!]$

$$\Rightarrow \quad \underline{\text{pred}}(0) \cong_{ctx} \Omega_{\underline{nat}}$$

Proof principle

To prove

$$M_1 \cong_{\mathrm{ctx}} M_2 : \tau$$

it suffices to establish

$$[\![M_1]\!] = [\![M_2]\!] \text{ in } [\![\tau]\!]$$

$\boxed{?}$ The proof principle is sound, but is it complete? That is, is equality in the denotational model also a necessary condition for contextual equivalence?

Topic 6

Denotational Semantics of PCF

Denotational semantics of PCF

To every typing judgement

$$\Gamma \vdash M : \tau$$

interpret types as domains

we associate a continuous function

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

between domains.

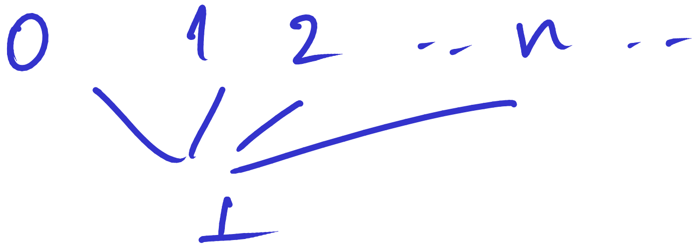
interpret type environments as domains.

Denotational semantics of PCF types

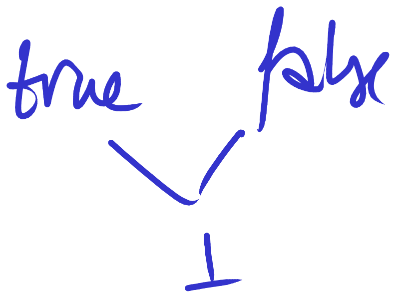
$$[\![nat]\!] \stackrel{\text{def}}{=} \mathbb{N}_\perp \qquad \text{(flat domain)}$$

$$[\![bool]\!] \stackrel{\text{def}}{=} \mathbb{B}_\perp \qquad \text{(flat domain)}$$

$\mathbb{N}_\perp =$



$\mathbb{B}_\perp =$



where $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{B} = \{true, false\}$.

Denotational semantics of PCF types

$$[\![nat]\!] \stackrel{\text{def}}{=} \mathbb{N}_\perp$$ (flat domain)

$$[\![bool]\!] \stackrel{\text{def}}{=} \mathbb{B}_\perp$$ (flat domain)

$$[\![\tau \to \tau']\!] \stackrel{\text{def}}{=} [\![\tau]\!] \to [\![\tau']\!]$$ (function domain).

where $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{B} = \{true, false\}$.

Denotational semantics of PCF type environments

$$[\![\Gamma]\!] \stackrel{\text{def}}{=} \prod_{x \in dom(\Gamma)} [\![\Gamma(x)]\!]$$ (Γ-environments)

$\Gamma = [x_1 \mapsto \tau_1, \ldots, x_n \mapsto \tau_n]$

We have $[\![\tau_i]\!]$ $i = 1, \ldots, n$ domains, and

define $[\![\Gamma]\!]$ again a domain.

$$\stackrel{\text{def}}{\parallel}$$

$$\prod_{i=1\ldots n} [\![\tau_i]\!] \ni (d_1, d_2, \ldots, d_n) \text{ with } d_i \in [\![\tau_i]\!]$$

Denotational semantics of PCF type environments

$$[\![\Gamma]\!] \stackrel{\text{def}}{=} \prod_{x \in dom(\Gamma)} [\![\Gamma(x)]\!] \qquad \text{(Γ-environments)}$$

$=$ the domain of partial functions ρ from variables to domains such that $dom(\rho) = dom(\Gamma)$ and $\rho(x) \in [\![\Gamma(x)]\!]$ for all $x \in dom(\Gamma)$

$\rho \in [\![\Gamma]\!]$

$x \in \underline{dom}(\Gamma) \longmapsto \rho(x) \in [\![\Gamma(x)]\!]$

<u>Example</u> $\Gamma = [x_1 \mapsto \tau_1, \ldots, x_n \mapsto \tau_n]$

$\rho \in [\![\Gamma]\!] \sim x_i \mapsto \rho(x_i) \in [\![\tau_i]\!]$

Denotational semantics of PCF type environments

$$[\![\Gamma]\!] \stackrel{\text{def}}{=} \prod_{x \in dom(\Gamma)} [\![\Gamma(x)]\!] \qquad (\Gamma\text{-environments})$$

$=$ the domain of partial functions ρ from variables to domains such that $dom(\rho) = dom(\Gamma)$ and $\rho(x) \in [\![\Gamma(x)]\!]$ for all $x \in dom(\Gamma)$

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

Example:

1. For the empty type environment $\emptyset$,

$$[\![\emptyset]\!] = \{ \perp \}$$

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

where $\perp$ denotes the unique partial function with $dom(\perp) = \emptyset$.

So $[\![M]\!] = [\![\emptyset \vdash M : \tau]\!](\perp) \in [\![\tau]\!]$

2. $[\![\langle x \mapsto \tau \rangle]\!] = (\{ x \} \to [\![\tau]\!]) \cong [\![\tau]\!]$

3.

$$
\begin{aligned}
&[\![\langle x_1 \mapsto \tau_1, \ldots, x_n \mapsto \tau_n \rangle]\!] \\
&\quad \cong (\{ x_1 \} \to [\![\tau_1]\!]) \times \ldots \times (\{ x_n \} \to [\![\tau_n]\!]) \\
&\quad \cong [\![\tau_1]\!] \times \ldots \times [\![\tau_n]\!]
\end{aligned}
$$

Denotational Semantics of terms

Recall that for $\Gamma \vdash M : \tau$ we aim to compositionally define a continuous function $[\![\Gamma \vdash M]\!] : [\![\Gamma]\!] \longrightarrow [\![\tau]\!]$.

We proceed by induction on the structure of terms, giving

$$[\![\Gamma \vdash M]\!](\rho) \in [\![\tau]\!] \qquad \text{for } \rho \in [\![\Gamma]\!]$$

Denotational semantics of PCF terms, I

$[\![\Gamma \vdash 0]\!] = \lambda \rho \in [\![\Gamma]\!] .\ 0$

$: [\![\Gamma]\!] \to \mathbb{N}_\perp$

$$[\![\Gamma \vdash \mathbf{0}]\!](\rho) \stackrel{\text{def}}{=} 0 \in [\![nat]\!]$$

$$[\![\Gamma \vdash \mathbf{true}]\!](\rho) \stackrel{\text{def}}{=} true \in [\![bool]\!]$$

$$[\![\Gamma \vdash \mathbf{false}]\!](\rho) \stackrel{\text{def}}{=} false \in [\![bool]\!]$$

Denotational semantics of PCF terms, I

$$D_1 \times \cdots \times D_n \xrightarrow{\pi_i} D_i$$
$$(d_1, \ldots, d_n) \longmapsto d_i$$

$$[\![\Gamma \vdash \mathbf{0}]\!](\rho) \stackrel{\text{def}}{=} 0 \in [\![nat]\!]$$

$$[\![\Gamma \vdash \mathbf{true}]\!](\rho) \stackrel{\text{def}}{=} true \in [\![bool]\!]$$

$$[\![\Gamma \vdash \mathbf{false}]\!](\rho) \stackrel{\text{def}}{=} false \in [\![bool]\!]$$

$$[\![\Gamma]\!]$$

$$[\![\Gamma \vdash x]\!](\rho) \stackrel{\text{def}}{=} \rho(x) \in [\![\Gamma(x)]\!] \qquad (x \in dom(\Gamma))$$

$$[\![x_1 : \tau_1, \ldots, x_n : \tau_n \vdash x_i : \tau_i]\!] : \prod_{j=1}^{n} [\![\tau_j]\!] \longrightarrow [\![\tau_i]\!]$$
$$(d_1, \ldots d_n) \longmapsto d_i$$
$$= \pi_i$$

Denotational semantics of PCF terms, II

$$[\![\Gamma \vdash \mathbf{succ}(M)]\!](\rho)$$

$$\stackrel{\text{def}}{=} \begin{cases} [\![\Gamma \vdash M]\!](\rho) + 1 & \text{if } [\![\Gamma \vdash M]\!](\rho) \neq \bot \\ \bot & \text{if } [\![\Gamma \vdash M]\!](\rho) = \bot \end{cases}$$

$$\frac{\Gamma \vdash M : nat}{\Gamma \vdash \underline{succ}(M) : nat}.$$

$$[\![\Gamma \vdash M : nat]\!] : [\![\Gamma]\!] \longrightarrow \mathbb{N}_\bot$$

$$[\![\Gamma \vdash \underline{succ}(M) : nat]\!] : [\![\Gamma]\!] \longrightarrow \mathbb{N}_\bot$$

$$\| \text{ def}$$

$$s \circ [\![\Gamma \vdash M : nat]\!]$$

$$s : \mathbb{N}_\bot \longrightarrow \mathbb{N}_\bot$$

$$n \in \mathbb{N} \longmapsto n+1$$

$$\bot \longmapsto \bot$$

Denotational semantics of PCF terms, II

$$[\![\Gamma \vdash \mathbf{succ}(M)]\!](\rho)$$

$$\stackrel{\text{def}}{=} \begin{cases} [\![\Gamma \vdash M]\!](\rho) + 1 & \text{if } [\![\Gamma \vdash M]\!](\rho) \neq \bot \\ \bot & \text{if } [\![\Gamma \vdash M]\!](\rho) = \bot \end{cases}$$

$$[\![\Gamma \vdash \mathbf{pred}(M)]\!](\rho)$$

$$\stackrel{\text{def}}{=} \begin{cases} [\![\Gamma \vdash M]\!](\rho) - 1 & \text{if } [\![\Gamma \vdash M]\!](\rho) > 0 \\ \bot & \text{if } [\![\Gamma \vdash M]\!](\rho) = 0, \bot \end{cases}$$

$$[\![\Gamma \vdash pred(M)]\!] \stackrel{def}{=} p \circ [\![\Gamma \vdash M]\!]$$

$$p : \mathbb{N}_\bot \to \mathbb{N}_\bot$$

$$\bot, 0 \longmapsto \bot$$

$$(n \in \mathbb{N}) \quad n+1 \longmapsto n$$

Denotational semantics of PCF terms, II

$$[\![\Gamma \vdash \mathbf{succ}(M)]\!](\rho)$$

$$\stackrel{\text{def}}{=} \begin{cases} [\![\Gamma \vdash M]\!](\rho) + 1 & \text{if } [\![\Gamma \vdash M]\!](\rho) \neq \bot \\ \bot & \text{if } [\![\Gamma \vdash M]\!](\rho) = \bot \end{cases}$$

$$[\![\Gamma \vdash \mathbf{pred}(M)]\!](\rho)$$

$$\stackrel{\text{def}}{=} \begin{cases} [\![\Gamma \vdash M]\!](\rho) - 1 & \text{if } [\![\Gamma \vdash M]\!](\rho) > 0 \\ \bot & \text{if } [\![\Gamma \vdash M]\!](\rho) = 0, \bot \end{cases}$$

$$[\![\Gamma \vdash \mathbf{zero}(M)]\!](\rho) \stackrel{\text{def}}{=} \begin{cases} \mathit{true} & \text{if } [\![\Gamma \vdash M]\!](\rho) = 0 \\ \mathit{false} & \text{if } [\![\Gamma \vdash M]\!](\rho) > 0 \\ \bot & \text{if } [\![\Gamma \vdash M]\!](\rho) = \bot \end{cases}$$

Denotational semantics of PCF terms, III

$$[\![\Gamma \vdash \mathbf{if}\ M_1\ \mathbf{then}\ M_2\ \mathbf{else}\ M_3]\!](\rho)$$

$$\stackrel{\text{def}}{=} \begin{cases} [\![\Gamma \vdash M_2]\!](\rho) & \text{if } [\![\Gamma \vdash M_1]\!](\rho) = \mathit{true} \\ [\![\Gamma \vdash M_3]\!](\rho) & \text{if } [\![\Gamma \vdash M_1]\!](\rho) = \mathit{false} \\ \perp & \text{if } [\![\Gamma \vdash M_1]\!](\rho) = \perp \end{cases}$$

$$[\![\Gamma \vdash M_1\ M_2]\!](\rho) \stackrel{\text{def}}{=} ([\![\Gamma \vdash M_1]\!](\rho))\ ([\![\Gamma \vdash M_2]\!](\rho))$$

$\rho \in [\![\Gamma]\!]$

$M_1 : \tau \to \sigma \qquad M_2 : \tau$

$[\![M_1]\!] : [\![\Gamma]\!] \to ([\![\tau]\!] \to [\![\sigma]\!]) \qquad [\![M_2]\!] : [\![\Gamma]\!] \to [\![\tau]\!]$

$$[\![\Gamma \vdash M_1 : \tau \to \sigma]\!] : [\![\Gamma]\!] \longrightarrow ([\![\tau]\!] \to [\![\sigma]\!])$$

$$[\![\Gamma \vdash M_2 : \tau]\!] : [\![\Gamma]\!] \longrightarrow [\![\tau]\!]$$

(1) Pair $[\![M_1]\!]$ and $[\![M_2]\!]$:

$$D \xrightarrow{f_1} D_1$$

$$D \xrightarrow[f_2]{} D_2$$

cont.

Exercise $\Downarrow$

$$\overline{}$$

$$D \xrightarrow[\langle f_1, f_2 \rangle]{} D_1 \times D_2$$

cont.

$$d \longmapsto (f_1(d), f_2(d))$$

$$\langle [\![M_1]\!], [\![M_2]\!] \rangle$$

$$: [\![\Gamma]\!] \longrightarrow ([\![\tau]\!] \to [\![\sigma]\!]) \times [\![\tau]\!]$$

$$\begin{tikzcd}
\llbracket M_1 \, M_2 \rrbracket : \llbracket \Gamma \rrbracket \arrow[rr] \arrow[dr, "\langle \llbracket M_1 \rrbracket, \llbracket M_2 \rrbracket \rangle\ \mathrm{def}"'] & & \llbracket \sigma \rrbracket \\
& (\llbracket \tau \rrbracket \to \llbracket \sigma \rrbracket) \times \llbracket \tau \rrbracket \arrow[ur, "\underline{\mathrm{eval}}"'] &
\end{tikzcd}$$

(2)

$$(D \to E) \times D \xrightarrow{\mathrm{eval}} E$$

continuous.

$$f \ , \ d \longmapsto f(d)$$

$$\underline{\mathrm{eval}} \stackrel{\mathrm{def}}{=} \lambda(f, d).\, f(d)$$

$$\llbracket M_1 \, M_2 \rrbracket = \underline{\mathrm{eval}} \circ \langle \llbracket M_1 \rrbracket, \llbracket M_2 \rrbracket \rangle$$

$$\frac{\Gamma[x \mapsto \tau] \vdash M : \sigma}{\Gamma \vdash \underline{\mathrm{fn}}\, x : \tau . M : \tau \to \sigma}$$

$$[\![\Gamma[x \mapsto \tau] \vdash M : \sigma]\!] : \underbrace{[\![\Gamma[x \mapsto \tau]]\!]}_{\substack{\shortparallel \\ [\![\Gamma]\!] \times [\![\tau]\!]}} \longrightarrow [\![\sigma]\!]$$

define

$$[\![\Gamma \vdash \underline{\mathrm{fn}}\, x . M : \tau \to \sigma]\!] : [\![\Gamma]\!] \longrightarrow ([\![\tau]\!] \to [\![\sigma]\!])$$

$$\shortparallel \mathrm{def}$$

$$\underline{\mathrm{curry}}([\![\Gamma[x \mapsto \tau] \vdash M]\!]) .$$

$$C \times D \xrightarrow{f} E \qquad \text{cont}$$

$$\Downarrow \quad \underline{\text{Exercise}}$$

$$C \xrightarrow{\text{curry}(f)} (D \to E) \qquad \text{cont}$$

$$\underline{\text{curry}}(f)(c) = \lambda d \in D.\ f(c,d)$$

Denotational semantics of PCF terms, IV

$$\llbracket \Gamma \vdash \mathbf{fn}\, x : \tau \,.\, M \rrbracket(\rho) \qquad\qquad (x \notin dom(\Gamma))$$
$$\stackrel{\text{def}}{=} \lambda d \in \llbracket \tau \rrbracket \,.\, \llbracket \Gamma[x \mapsto \tau] \vdash M \rrbracket(\rho[x \mapsto d])$$

NB: $\rho[x \mapsto d] \in \llbracket \Gamma[x \mapsto \tau] \rrbracket$ is the function mapping x to $d \in \llbracket \tau \rrbracket$ and otherwise acting like ρ.

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

$fix : (D \to D) \to D$ continuous.

Denotational semantics of PCF terms, V

$$[\![\Gamma \vdash \mathbf{fix}(M)]\!](\rho) \stackrel{\text{def}}{=} \mathit{fix}([\![\Gamma \vdash M]\!](\rho))$$

$$[\![\Gamma \vdash fix(M)]\!] = fix \circ [\![\Gamma \vdash M]\!]$$

Recall that fix is the function assigning least fixed points to continuous functions.

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.