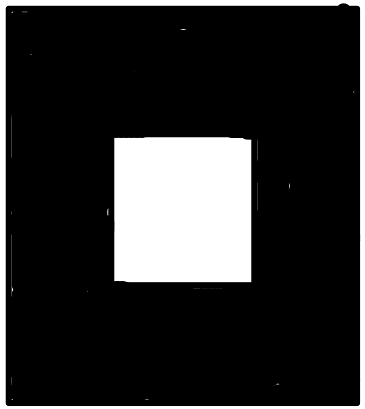
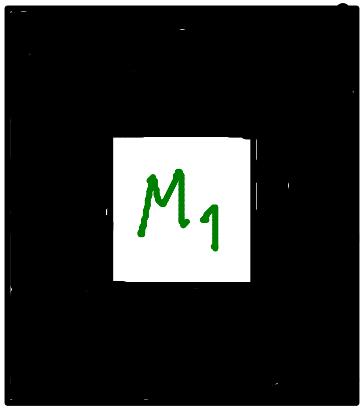
Intuitively, two program phrases are contextually equivalent whenever there is no observable computational difference between running either of them within any given complete program.

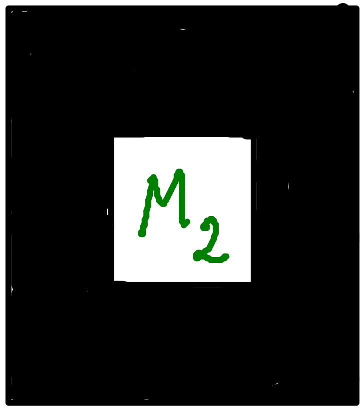
THE IDEA OF CONTEXTUAL EQUIVALENCE

$$M_1 \cong_{ctx} M_2$$

iff

for all program contexts 

running 

and running 

is computationally indistinguishable

Contextual equivalence 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, $M \Downarrow_\tau V \;\Rightarrow\; [\![M]\!] = [\![V]\!]$. in $[\![\tau]\!]$

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

$\mathcal{C}[M_1] \Downarrow_\gamma V \Rightarrow [\![\mathcal{C}[M_1]]\!] = [\![V]\!]$ soundness

$\Rightarrow [\![\mathcal{C}[M_2]]\!] = [\![V]\!]$ compositionality

$\Rightarrow \mathcal{C}[M_2] \Downarrow V$ adequacy

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

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

$\boxed{?}$ 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

For $M \in \underline{PCF}_\tau$, $[\![M]\!] \in [\![\tau]\!]$

Denotational semantics of PCF

To every typing judgement

$[x_1 \mapsto \tau_1, x_2 \mapsto \tau_2, \ldots, x_n \mapsto \tau_n]$

or

$(x_1 : \tau_1, \ldots, x_n : \tau_n)$

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

we associate a continuous function

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

$\underline{dom}(\Gamma) = \{x_1, \ldots, x_n\}$

between domains.

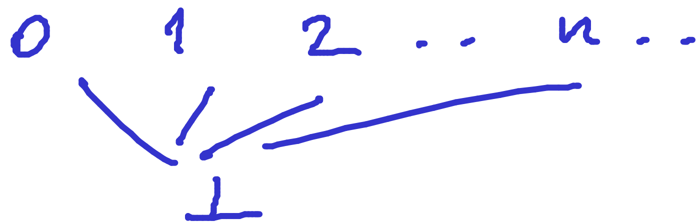
by induction.

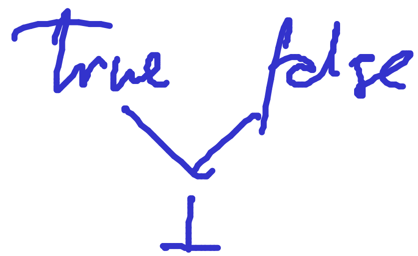
$\tau ::= nat \mid bool \mid \tau_1 \to \tau_2$

Denotational semantics of PCF types

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

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

$N_\perp =$ 

$B_\perp =$ 

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). domain of continuous functions.

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

Denotational semantics of PCF type environments

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

$[\![x_1 \mapsto \tau_1, \ldots, x_n \mapsto \tau_n]\!] = [\![\tau_1]\!] \times \cdots \times [\![\tau_n]\!]$

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

$\shortparallel$

$(\rho_1, \ldots, \rho_n)$ where $\rho_i \in [\![\tau_i]\!]$ $i = 1 \ldots n$

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 $x \in dom(\Gamma)$

Example:

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

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

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

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

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

3.

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

<u>Recall:</u> We want to define

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

a continuous function; that is, for all $\rho \in [\![\Gamma]\!]$, define

$$[\![\Gamma \vdash M : \tau]\!](\rho) \in [\![\tau]\!] .$$

Denotational semantics of PCF terms, I

$$[\![\Gamma \vdash 0]\!] : [\![\Gamma]\!] \to \mathbb{N}_\perp$$

$$\rho \mapsto 0$$

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

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

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

$D_1 \times D_2 \times \cdots \times D_n \xrightarrow[\pi_i]{} D_i$ continuous.

Denotational semantics of PCF terms, I

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

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

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

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

$[\![x_1 \mapsto \tau_1, x_2 \mapsto \tau_2, \ldots, x_n \mapsto \tau_n \vdash x_i : \tau_i]\!](\rho_1, \rho_2, \ldots, \rho_n) = \rho_i$

Denotational semantics of PCF terms, II

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

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

$$\frac{M \Downarrow V}{\underline{succ}(M) \Downarrow \underline{succ}(V)}$$

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

By induction: cont.

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

$$[\![\Gamma \vdash \underline{succ}(M)]\!] = \underbrace{s}_{\text{cont } \mathbb{N}_\bot \to \mathbb{N}_\bot : \begin{cases} \bot \mapsto \bot \\ n \mapsto n+1 \end{cases}} \circ [\![\Gamma \vdash M]\!]$$

Denotational semantics of PCF terms, II

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

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

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

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

$$\frac{M \Downarrow \underline{succ}(V)}{\underline{pred}(M) \Downarrow V}$$

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

$$\begin{cases} 0, \bot \longmapsto \bot \\ n+1 \longmapsto n \end{cases}$$

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

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

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

$$[\![\Gamma \vdash \underset{\sigma \to \tau}{M_1}\ \underset{\sigma}{M_2}]\!](\rho) \stackrel{\text{def}}{=} \underbrace{\big([\![\Gamma \vdash M_1]\!](\rho)\big)}_{\text{in } [\![\sigma]\!] \to [\![\tau]\!]}\ \underbrace{\big([\![\Gamma \vdash M_2]\!](\rho)\big)}_{\text{in } [\![\sigma]\!]} \quad \text{in } [\![\tau]\!]$$

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

$$[\![\Gamma \vdash M_1]\!] : \underset{\text{cont.}}{[\![\Gamma]\!] \longrightarrow} ([\![\sigma]\!] \to [\![\tau]\!]) \qquad [\![\Gamma \vdash M_2]\!] : \underset{\text{cont.}}{[\![\Gamma]\!] \to [\![\sigma]\!]}$$

$$\frac{D \xrightarrow{f} (E \to F) \qquad D \xrightarrow{g} E}{D \xrightarrow[\langle f, g\rangle]{} (E \to F) \times E \xrightarrow{\text{eval}} F}$$

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

$$h, e \longmapsto \begin{array}{c} \text{eval}(h, e) \\ \shortparallel \\ h(e) \end{array}$$

$$[\![\Gamma[x\mapsto\tau] \vdash M : \sigma]\!] : [\![\Gamma[x\mapsto\tau]]\!] \longrightarrow [\![\sigma]\!]$$

Denotational semantics of PCF terms, IV

$\sim$ in $[\![\tau]\!] \to [\![\sigma]\!]$

$$[\![\Gamma \vdash \mathbf{fn}\, x : \tau \,.\, M]\!](\rho)$$

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

$$[\![\Gamma \vdash \mathrm{fn}\, x:\tau.\, M]\!] = curry([\![\Gamma, x:\tau \vdash M]\!]).$$

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

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

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

$$f : D \times E \longrightarrow F \quad \rightsquigarrow \quad \mathrm{curry}(f) : D \longrightarrow (E \to F)$$
$$d \longmapsto (e \mapsto f(d,e))$$

curry is cont.

Denotational semantics of PCF terms, V

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

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.