Contextual equivalence

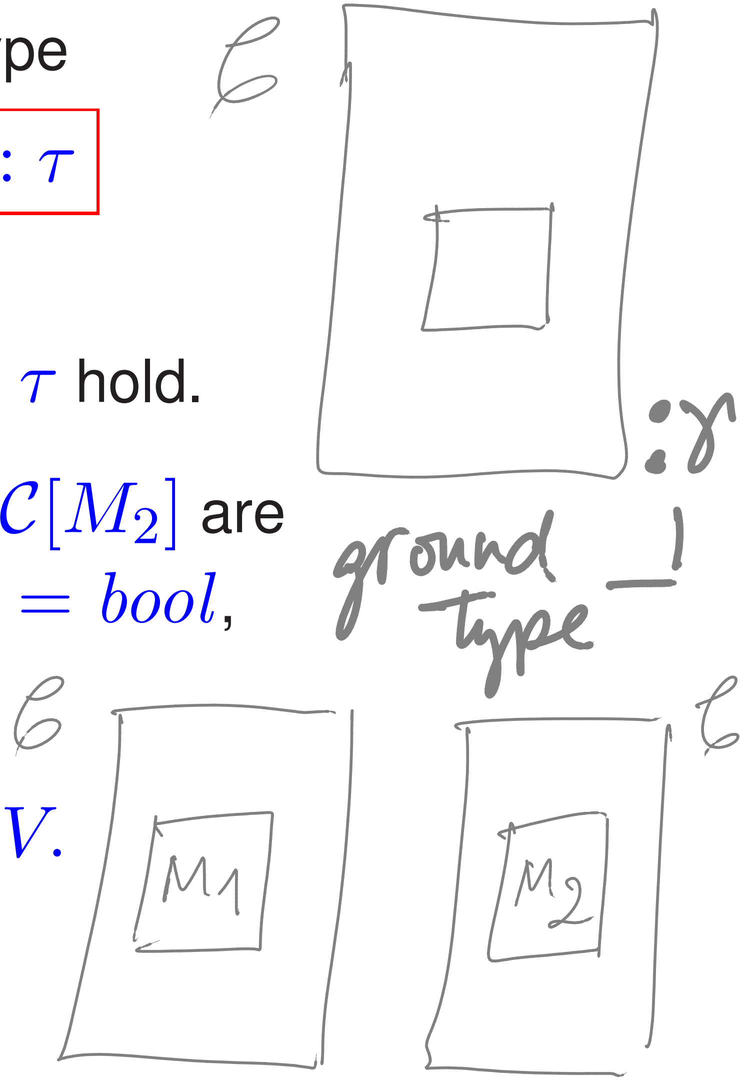
Two phrases of a programming language are contextually equivalent if any occurrences of the first phrase in a complete program can be replaced by the second phrase without affecting the observable results of executing the program.

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

$$\frac{[\![M]\!] = [\![M']\!]}{[\![\mathcal{C}[M]]\!] = [\![\mathcal{C}[M']]\!]}$$

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

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

$$\mathcal{C}[M_1] \Downarrow V \Rightarrow [\![\mathcal{C}[M_1]]\!] = [\![V]\!]$$

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

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

$$[\![M_1]\!] = [\![M_2]\!] \Rightarrow [\![\mathcal{C}[M_1]]\!] = [\![\mathcal{C}[M_2]]\!]$$

$M_1 \lesssim_{ctx} M_2$

so that $M_1 \cong_{ctx} M_2$

$\Uparrow$

$M_1 \lesssim_{ctx} M_2 \wedge M_2 \lesssim_{ctx} M_1$

Proof principle

To prove

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

it suffices to establish

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

$$\frac{[\![M_1]\!] = [\![M_2]\!]}{M_1 \cong_{ctx} M_2}$$

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

In particular, for closed M of type τ, $[\![M]\!] \in [\![\tau]\!]$

So for $P : \sigma \to \tau$, $[\![P]\!] \in ([\![\sigma]\!] \to [\![\tau]\!])$ Hence if

Denotational semantics of PCF

To every typing judgement

CONTINUOUS

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

we associate a continuous function

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

between domains.

a function mapping inputs $[\![\sigma]\!]$ to outputs $[\![\tau]\!]$ is not continuous then it cannot be implemented by a program.

Denotational semantics of PCF types

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

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

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

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

$\Gamma = \{ x \mapsto \tau_x \}$

Denotational semantics of PCF type environments

$\{$ finite domain of variables.

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

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 $x \in dom(\Gamma)$

For $\Gamma = \{x_i \mapsto \tau_i\}_{i=1,\dots,n}$

$\rho \in [\![\Gamma]\!]$ s.t. $\rho(x_i) \in [\![\tau_i]\!]$

Equivalently viewing Γ as $\langle x_1 : \tau_1, \dots, x_n : \tau_n \rangle$

$[\![\Gamma]\!] = [\![\tau_1]\!] \times [\![\tau_2]\!] \times \dots \times [\![\tau_n]\!]$

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

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 PCF terms, I

For $\Gamma \vdash M : \tau$

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

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

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

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

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

Denotational semantics of PCF terms, I

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

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

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

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

$\Gamma = \langle x_1 : \tau_1, \ldots, x_n : \tau_n \rangle$

$[\![\Gamma \vdash x_i]\!](v_1, \ldots, v_n) = v_i$

Denotational semantics of PCF terms, II

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

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

the strict extension of
$succ : \mathbb{N} \to \mathbb{N}$

$$\begin{tikzcd} [\![\Gamma]\!] \arrow[r, "{[\![\Gamma \vdash M]\!]}"] \arrow[rr, bend right, "{[\![\Gamma \vdash \underline{succ}\, M]\!]}"'] & \mathbb{N}_\bot \arrow[r, "succ_\bot"] & \mathbb{N}_\bot \end{tikzcd}$$

Denotational semantics of PCF terms, II

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

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

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

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

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

$[\![M_1]\!] : [\![\Gamma]\!] \to ([\![\alpha]\!] \to [\![\beta]\!])$ $\qquad$ $[\![M_2]\!] : [\![\Gamma]\!] \to [\![\alpha]\!]$

Denotational semantics of PCF terms, III

$[\![M_1]\!]\rho \in ([\![\alpha]\!] \to [\![\beta]\!])$ $\qquad$ $[\![M_2]\!](\rho) \in [\![\alpha]\!]$

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

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

$$[\![\Gamma \vdash \underbrace{M_1}_{\alpha \to \beta}\ \underbrace{M_2}_{\alpha}]\!](\rho) \stackrel{\text{def}}{=} \left([\![\Gamma \vdash M_1]\!](\rho)\right) \left([\![\Gamma \vdash M_2]\!](\rho)\right)$$

$$\frac{\Gamma, x:\tau \vdash M : \sigma}{\Gamma \vdash \mathbf{fn}\, x:\tau . M : \tau \to \sigma}$$

$$[\![\Gamma]\!] \times [\![\tau]\!] \longrightarrow [\![\sigma]\!]$$

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

Denotational semantics of PCF terms, IV

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

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

$$\frac{\Gamma \vdash M : \tau \to \tau}{\Gamma \vdash fix(M) : \tau}$$

$$[\![\Gamma]\!] \longrightarrow ([\![\tau]\!] \to [\![\tau]\!])$$

$$[\![\Gamma]\!] \longrightarrow [\![\tau]\!]$$

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.

$$\begin{tikzcd}
[\![\Gamma]\!] \arrow[r, "{[\![M]\!]}"] \arrow[rr, bend right, "{[\![fix(M)]\!]}"'] & ([\![\tau]\!] \to [\![\tau]\!]) \arrow[r, "fix"] & [\![\tau]\!]
\end{tikzcd}$$

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

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