Contextual Equivalence

[§5.5, p62]

When are two program phrases semantically equal?

When are two program phrases semantically equal?

Program Logic:

when they satisfy the same logical assertions.

E.g. $C \cong C'$ iff for all pre-, post-conditions P, Q

$$\{P\}\,C\,\{Q\} \Leftrightarrow \{P\}\,C'\,\{Q\}$$

When are two program phrases semantically equal?

Program Logic:

when they satisfy the same logical assertions.

Denotational semantics:

when they have equal denotations.

When are two program phrases semantically equal?

Program Logic:

when they satisfy the same logical assertions.

Denotational semantics:

when they have equal denotations.

Operational semantics:

when they are contextually equivalent.

Contextual equivalence

Two phrases of a programming language are ("Morris style") contextually equivalent ($\cong_{\mathbf{ctx}}$) if occurrences of the first phrase in any program can be replaced by the second phrase without affecting the observable results of executing the program.

We assume the programming language comes with an operational semantics as part of its definition

E.g. PCF term for addition

$$\begin{aligned}&\mathrm{fix}\,(\mathrm{fn}\ p : nat \to nat \to nat.\ \mathrm{fn}\ x : nat.\ \mathrm{fn}\ y : nat \\ &\qquad \mathrm{if}\ \mathrm{zero}(y)\ \mathrm{then}\ x \\ &\qquad \mathrm{else}\ \mathrm{succ}(p\,x\,(\mathrm{pred}(y)))\,)\end{aligned}$$

E.g. PCF term for addition

$$
\begin{aligned}
&\mathrm{fix}\,(\mathrm{fn}\ p : nat \to nat \to nat .\ \mathrm{fn}\ x : nat .\ \mathrm{fn}\ y : nat \\
&\quad \mathrm{if}\ \mathrm{zero}(y)\ \mathrm{then}\ \mathrm{pred}(\mathrm{succ}(x)) \\
&\quad \mathrm{else}\ \mathrm{succ}(p\, x\, (\mathrm{pred}(y))))
\end{aligned}
$$

expect that x and $\mathrm{pred}(\mathrm{succ}\, x)$ are contextually equivalent for PCF

Contextual equivalences

Two phrases of a programming language are ("Morris style") contextually equivalent ($\cong_{\mathbf{ctx}}$) if occurrences of the first phrase in any program can be replaced by the second phrase without affecting the observable results of executing the program.

Different choices lead to possibly different notions of contextual equivalence.

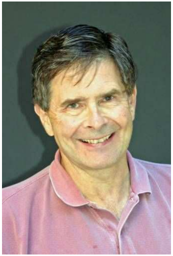
Contextual equivalence

Two phrases of a programming language are ("Morris style") contextually equivalent ($\cong_{\mathbf{ctx}}$) if occurrences of the first phrase in any program can be replaced by the second phrase without affecting the observable results of executing the program.

Gottfried Wilhelm Leibniz (1646–1716):
two mathematical objects are equal
if there is no test to distinguish them.

Contextual equivalence

Two phrases of a programming language are ("Morris style") contextually equivalent ($\cong_{\mathbf{ctx}}$) if occurrences of the first phrase in any program can be replaced by the second phrase without affecting the observable results of executing the program.



first known CS occurrence of this notion in Jim Morris' PhD thesis, *Lambda Calculus Models of Programming Languages* (MIT, 1969)

PCF syntax

Types

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

Expressions

$$\begin{array}{rcl} M & ::= & \mathbf{0} \mid \mathbf{succ}(M) \mid \mathbf{pred}(M) \\ & \mid & \mathbf{true} \mid \mathbf{false} \mid \mathbf{zero}(M) \\ & \mid & x \mid \mathbf{if}\ M\ \mathbf{then}\ M\ \mathbf{else}\ M \\ & \mid & \mathbf{fn}\, x : \tau \,.\, M \mid M\ M \mid \mathbf{fix}(M) \end{array}$$

where $x \in \mathbb{V}$, an infinite set of variables.

PCF contexts $\mathcal{C}$ [p63]

$$\mathcal{C} ::= - \mid 0 \mid \mathrm{succ}(\mathcal{C}) \mid \mathrm{pred}(\mathcal{C})$$
$$\mid \mathrm{zero}(\mathcal{C}) \mid \mathrm{true} \mid \mathrm{false} \mid \mathrm{if}\ \mathcal{C}\ \mathrm{then}\ \mathcal{C}\ \mathrm{else}\ \mathcal{C}$$
$$\mid x \mid \mathbf{fn}\, x : \tau .\, \mathcal{C} \mid \mathcal{C}\,\mathcal{C} \mid \mathrm{fix}(\mathcal{C})$$

PCF contexts $\mathcal{C}$ [p63]

$$
\begin{aligned}
\mathcal{C} ::= {} & - \mid 0 \mid \mathtt{succ}(\mathcal{C}) \mid \mathtt{pred}(\mathcal{C}) \\
& \mid \mathtt{zero}(\mathcal{C}) \mid \mathtt{true} \mid \mathtt{false} \mid \mathtt{if}\ \mathcal{C}\ \mathtt{then}\ \mathcal{C}\ \mathtt{else}\ \mathcal{C} \\
& \mid x \mid \mathtt{fn}\, x : \tau .\, \mathcal{C} \mid \mathcal{C}\,\mathcal{C} \mid \mathtt{fix}(\mathcal{C})
\end{aligned}
$$

a "hole", or place holder, to be filled with a PCF term

PCF contexts $\mathcal{C}$ [p63]

$$\mathcal{C} ::= - \mid 0 \mid succ(\mathcal{C}) \mid pred(\mathcal{C})$$
$$\mid zero(\mathcal{C}) \mid true \mid false \mid if\ \mathcal{C}\ then\ \mathcal{C}\ else\ \mathcal{C}$$
$$\mid x \mid fn\, x : \tau .\, \mathcal{C} \mid \mathcal{C}\,\mathcal{C} \mid fix(\mathcal{C})$$

Notation: $\mathcal{C}[M]$ = PCF term obtained from $\mathcal{C}$ by replacing all occurrences of $-$ by M

$$\mathrm{fix}\,(\mathrm{fn}\ p : nat \to nat \to nat.\ \mathrm{fn}\ x : nat.\ \mathrm{fn}\ y : nat$$
$$\quad \mathrm{if}\ zero(y)\ \mathrm{then}\ pred(succ(x))$$
$$\quad \mathrm{else}\ succ(p\,x\,(pred(y))))$$

is $\mathcal{C}[pred(succ(x))]$ for

$$\mathcal{C} = \mathrm{fix}\,(\mathrm{fn}\ p : nat \to nat \to nat.\ \mathrm{fn}\ x : nat.\ \mathrm{fn}\ y : nat$$
$$\quad \mathrm{if}\ zero(y)\ \mathrm{then}\ -$$
$$\quad \mathrm{else}\ succ(p\,x\,(pred(y))))$$

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 $V : \gamma$,

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

When $\Gamma = \emptyset$, just write $\emptyset \vdash M_1 \cong_{ctx} M_2 : \tau$ as

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

Examples of PCF contextual equivalence

$$(\lambda x : \tau .\, M)\, M' \cong_{ctx} M[M'/x] : \tau'$$

(where $\begin{cases} \lambda x : \tau .\, M : \tau \to \tau' \\ M' : \tau \end{cases}$)

$$M \cong_{ctx} \lambda x : \tau .\, M x : \tau \to \tau'$$

(where $M : \tau \to \tau'$
& $x \notin fv(M)$)

$$\mathbf{fix}(M) \cong_{ctx} M\, \mathbf{fix}(M) : \tau$$

(where $M : \tau \to \tau$)

HOW DOES ONE PROVE SUCH FACTS?

Examples of PCF contextual equivalence

$\{x : nat\} \vdash pred(succ(x)) \cong_{ctx} x : nat$

$\{x : nat\} \vdash zero(0) \cong_{ctx} true : bool$

? $\{x : nat\} \vdash zero(succ(x)) \cong_{ctx} false : bool$

Non-Examples of PCF contextual equivalence

$$\{x : nat\} \vdash pred(succ(x)) \cong_{ctx} x : nat$$

$$\{x : nat\} \vdash zero(0) \cong_{ctx} true : bool$$

$$\{x : nat\} \vdash zero(succ(x)) \not\cong_{ctx} false : bool$$

because for $\mathcal{C} = (\lambda x : nat . -)\,\Omega_{nat}$ we have

$$\begin{cases} \mathcal{C}[zero(succ\, x)] = (\lambda x : nat . zero(succ\, x))\,\Omega_{nat} \not\Downarrow_{nat} \\ \mathcal{C}[false] = (\lambda x : nat . false)\,\Omega_{nat} \Downarrow_{nat} false \end{cases}$$

Non-Examples of PCF contextual equivalence

$\{x : nat\} \vdash pred(succ(x)) \cong_{ctx} x : nat$

$\{x : nat\} \vdash zero(0) \cong_{ctx} true : bool$

$\{x : nat\} \vdash zero(succ(x)) \not\cong_{ctx} false : bool$

because for $\mathcal{C} = (\lambda x : nat . -)\,\Omega_{nat}$ we have

$$\begin{cases} \mathcal{C}[zero(succ\, x)] = (\lambda x : nat . zero(succ\, x))\,\Omega_{nat} \not\Downarrow_{nat} \\ \mathcal{C}[false] = (\lambda x : nat . false)\,\Omega_{nat} \Downarrow_{nat} false \end{cases}$$

<u>MORAL</u>: easy to show $\not\cong_{ctx}$ (usually).

But how do we prove valid instances of $\cong_{ctx}$?

Contextual preorder between PCF terms

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

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

Facts about $\leq_{ctx}$

- If $M\,N \leq_{ctx} N : \tau$, then $\mathbf{fix}\, M \leq_{ctx} N : \tau$

  (cf. (lfp2) on Slide 19)

Facts about $\leq_{ctx}$

- If $M\,N \leq_{ctx} N : \tau$, then $\mathrm{fix}\,M \leq_{ctx} N : \tau$
  (cf. (lfp2) on Slide 19)

- $\mathrm{fix}\,M \leq_{ctx} N : \tau$ iff for all $n \geq 0$,
  $\mathrm{fix}^n M \leq_{ctx} N : \tau$

where
$$\begin{cases} \mathrm{fix}^0 M \triangleq \Omega_\tau \\ \mathrm{fix}^{n+1} M \triangleq M(\mathrm{fix}^n M) = \underbrace{M(M(\cdots M}_{n+1\text{ times}}\,\Omega_\tau)\cdots) \end{cases}$$

(cf. Tarski FPT)

Facts about $\leq_{ctx}$

- If $M\,N \leq_{ctx} N : \tau$, then $\mathbf{fix}\,M \leq_{ctx} N : \tau$
  (cf. (lfp2) on Slide 19)

- $\mathbf{fix}\,M \leq_{ctx} N : \tau$ iff for all $n \geq 0$,
  $\mathbf{fix}^n M \leq_{ctx} N : \tau$

where
$$\begin{cases} \mathbf{fix}^0 M \triangleq \Omega_\tau \\ \mathbf{fix}^{n+1} M \triangleq M(\mathbf{fix}^n M) = \underbrace{M(M(\cdots M}_{n+1 \text{ times}}\,\Omega_\tau)\cdots) \end{cases}$$

(cf. Tarski FPT)

HOW TO PROVE SUCH FACTS?

PCF denotational semantics — aims

PCF denotational semantics — aims

- PCF types $\tau \;\mapsto\;$ domains $[\![\tau]\!]$.

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.

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.

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

$$\boxed{\begin{array}{l} [\![\Gamma]\!] = [\![\tau_1]\!] \times \cdots \times [\![\tau_n]\!] \\ \text{if } \Gamma = \{x_1 : \tau_1, \ldots, x_n : \tau_n\} \end{array}}$$

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

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

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

  not at function types, because...

Example 5.6.1

[p65]

$$V \triangleq \mathrm{fn}\ x : nat . (\mathrm{fn}\ y : nat . y)\, 0$$

$$V' \triangleq \mathrm{fn}\ x : nat .\ 0$$

Satisfy:

$$V \not\Downarrow_{nat \to nat} V'$$

because in general can only prove $V \Downarrow V'$ for $V' = V$

Example 5.6.1 [p65]

$$\boxed{\begin{array}{l} V \triangleq \mathbf{fn}\ x : nat.\ (\mathbf{fn}\ y : nat.\ y)\ 0 \\ \hline V' \triangleq \mathbf{fn}\ x : nat.\ 0 \end{array}}$$

satisfy:

$$V \not\Downarrow_{nat \to nat} V'$$

$$[\![V]\!] = [\![V']\!]$$

because $(\mathbf{fn}\ y : nat.\ y)\ 0 \Downarrow_{nat} 0$

so $[\![(\mathbf{fn}\ y : nat\ y)\ 0]\!] = [\![0]\!]$ by Soundness

Example 5.6.1 [p65]

$$V \triangleq \mathrm{fn}\, x : nat. (\mathrm{fn}\, y : nat.\, y)\, 0$$

$$V' \triangleq \mathrm{fn}\, x : nat.\ 0$$

satisfy:

$$V \not\Downarrow_{nat \to nat} V'$$

$$[\![V]\!] = [\![V']\!]$$

because $(\mathrm{fn}\, y : nat. y)\, 0 \Downarrow_{nat} 0$

so $[\![(\mathrm{fn}\, y : nat. y)\, 0]\!] = [\![0]\!]$ by soundness

so $[\![\mathcal{C}[(\mathrm{fn}\, y : nat. y)\, 0]]\!] = [\![\mathcal{C}[0]]\!]$ by compositionality

and we can take $\mathcal{C} = \mathrm{fn}\, x : nat. -$.

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

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 $\Downarrow_{bool}$). $\square$

Proof principle

To prove

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

it suffices to establish

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

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?

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?

In Chapter 8 we find the answer is no!