Denotational Semantics

Ioannis Markakis

Lectures for Part II CST 2026/2027

Extensionality

Contextual preorder

Contextual preorder $\Gamma \vdash t \leq_{\text{ctx}} t' : \tau$ is the one-sided version of contextual equivalence: for all $\mathcal{C}$ such that $\cdot \vdash_{\Gamma,\tau} \mathcal{C} : \gamma$ where $\gamma \in \{\texttt{nat}, \texttt{bool}\}$ and for all values v,

$$\mathcal{C}[t] \Downarrow_\gamma v \Rightarrow \mathcal{C}[t'] \Downarrow_\gamma v.$$

Contextual preorder

Contextual preorder $\Gamma \vdash t \leq_{\text{ctx}} t' : \tau$ is the one-sided version of contextual equivalence: for all $\mathcal{C}$ such that $\cdot \vdash_{\Gamma,\tau} \mathcal{C} : \gamma$ where $\gamma \in \{\texttt{nat}, \texttt{bool}\}$ and for all values v,

$$\mathcal{C}[t] \Downarrow_\gamma v \Rightarrow \mathcal{C}[t'] \Downarrow_\gamma v.$$

This is a reflexive and transitive relation (a preorder).

Contextual preorder

Contextual preorder $\Gamma \vdash t \leq_{\text{ctx}} t' : \tau$ is the one-sided version of contextual equivalence: for all $\mathcal{C}$ such that $\cdot \vdash_{\Gamma,\tau} \mathcal{C} : \gamma$ where $\gamma \in \{\texttt{nat}, \texttt{bool}\}$ and for all values v,

$$\mathcal{C}[t] \Downarrow_\gamma v \Rightarrow \mathcal{C}[t'] \Downarrow_\gamma v.$$

This is a reflexive and transitive relation (a preorder).

Contextual equivalence is recovered by the contextual preorder via:

$$\Gamma \vdash t \cong_{\text{ctx}} t' : \tau \quad \iff \quad (\Gamma \vdash t \leq_{\text{ctx}} t' : \tau \ \wedge \ \Gamma \vdash t' \leq_{\text{ctx}} t : \tau)$$

Monotonicity of formal approximation

The formal approximation relation is monotonic in each of its arguments.

Lemma

For every type τ, terms $t, t' \in \mathrm{PCF}_\tau$ and $d, d' \in [\![\tau]\!]$:

1. $d \sqsubseteq d' \lhd_\tau t \implies d \lhd_\tau t$
2. $d \lhd_\tau t \leq_{\mathrm{ctx}} t' : \tau \implies d \lhd_\tau t'$

Monotonicity of formal approximation

The formal approximation relation is monotonic in each of its arguments.

Lemma

For every type τ, terms $t, t' \in \mathrm{PCF}_\tau$ and $d, d' \in [\![\tau]\!]$:

1. $d \sqsubseteq d' \lhd_\tau t \implies d \lhd_\tau t$
2. $d \lhd_\tau t \leq_{\mathrm{ctx}} t' : \tau \implies d \lhd_\tau t'$

- We have already proven (1)
- To prove (2) we proceed by induction on τ:
  - For a ground type τ, use $\mathcal{C} = -$
  - For a function type, convert $\mathcal{C}[-]$ to $\mathcal{C}[-\,u]$

Application contexts

To characterise contextual preorder between closed terms, applicative contexts suffice.

Application contexts

To characterise contextual preorder between closed terms, applicative contexts suffice.

Lemma

Let $\cdot \vdash t_1, t_2 : \tau$ be closed terms. Then $t_1 \leq_{\mathrm{ctx}} t_2 : \tau$ if and only if

$$\forall f \in \mathrm{PCF}_{\tau \to \mathtt{bool}} \cdot (f\ t_1 \Downarrow_{\mathtt{bool}} \mathtt{true} \implies f\ t_2 \Downarrow_{\mathtt{bool}} \mathtt{true})$$

To characterise contextual preorder between closed terms, applicative contexts suffice.

Lemma

Let $\cdot \vdash t_1, t_2 : \tau$ be closed terms. Then $t_1 \leq_{\text{ctx}} t_2 : \tau$ if and only if

$$\forall f \in \text{PCF}_{\tau \to \texttt{bool}} \cdot (f\ t_1 \Downarrow_{\texttt{bool}} \texttt{true} \implies f\ t_2 \Downarrow_{\texttt{bool}} \texttt{true})$$

$\implies$ Take $\mathcal{C} = (f\ -)$

$\impliedby$ Define for $\cdot \vdash_{\cdot,\tau} \mathcal{C} : \gamma$ the term $f = \texttt{fun}\, x{:}\tau.\ .\mathcal{C}[x] : \gamma$
Compose it with $g_v : \gamma \to \texttt{bool}$ such that $g_v u \Downarrow \texttt{true}$ if and only if $u \Downarrow v$.
We can define such g_v by case split on γ and v.

Contextual preorder and formal approximation

Formal approximation captures contextual preorder.

Contextual preorder and formal approximation

Formal approximation captures contextual preorder.

Proposition

For all PCF types τ and all closed terms $t_1, t_2 \in \mathrm{PCF}_\tau$

$$t_1 \leq_{\mathrm{ctx}} t_2 : \tau \quad \iff \quad [\![t_1]\!] \lhd_\tau t_2.$$

Formal approximation captures contextual preorder.

Proposition

For all PCF types τ and all closed terms $t_1, t_2 \in \text{PCF}_\tau$

$$t_1 \leq_{\text{ctx}} t_2 : \tau \quad \iff \quad [\![t_1]\!] \lhd_\tau t_2.$$

$\Longrightarrow$ By fundamental property and monotonicity

$\Longleftarrow$ Take arbitrary $f : \tau \to \texttt{bool}$
By fundamental lemma on f and assumption, $[\![f\ t_1]\!] \lhd_{\texttt{bool}} f\ t_2$
Assume that $f\ t_1 \Downarrow \texttt{true}$ to get that $f\ t_2 \Downarrow \texttt{true}$.

Extensionality of contextual preorder

For $\gamma = \texttt{bool}$ or $\texttt{nat}$, the relation $t_1 \leq_{\text{ctx}} t_2 : \gamma$ holds if and only if

$$\forall v.\, (t_1 \Downarrow_\gamma v \Rightarrow t_2 \Downarrow_\gamma v).$$

Extensionality of contextual preorder

For $\gamma = \texttt{bool}$ or $\texttt{nat}$, the relation $t_1 \leq_{\text{ctx}} t_2 : \gamma$ holds if and only if

$$\forall v.\, (t_1 \Downarrow_\gamma v \Rightarrow t_2 \Downarrow_\gamma v).$$

At a function type $\tau \to \tau'$, the relation $t_1 \leq_{\text{ctx}} t_2 : \tau \to \tau'$ holds if and only if

$$\forall t \in \text{PCF}_\tau\, .\, (t_1\ t \leq_{\text{ctx}} t_2\ t : \tau').$$

Full abstraction

Full abstraction

Failure of full abstraction

Recap

We have related operational semantics and denotational semantics:

Recap

We have related operational semantics and denotational semantics:

- Soundness: $t \Downarrow_\tau v \implies [\![t]\!] = [\![v]\!]$ for every type τ
- Adequacy: $[\![t]\!] = [\![v]\!] \implies t \Downarrow_\tau v$ for $\tau \in \{\mathtt{nat}, \mathtt{bool}\}$

Recap

We have related operational semantics and denotational semantics:

- Soundness: $t \Downarrow_\tau v \implies [\![t]\!] = [\![v]\!]$ for every type τ
- Adequacy: $[\![t]\!] = [\![v]\!] \implies t \Downarrow_\tau v$ for $\tau \in \{\texttt{nat}, \texttt{bool}\}$

We have also related contextual with denotational equivalence:

Recap

We have related operational semantics and denotational semantics:

- Soundness: $t \Downarrow_\tau v \implies [\![t]\!] = [\![v]\!]$ for every type τ
- Adequacy: $[\![t]\!] = [\![v]\!] \implies t \Downarrow_\tau v$ for $\tau \in \{\mathtt{nat}, \mathtt{bool}\}$

We have also related contextual with denotational equivalence:

- **Compositionality:** $[\![t]\!] = [\![t']\!] \implies [\![\mathcal{C}[t]]\!] = [\![\mathcal{C}[t']]\!]$ for all terms and contexts
- Using the above gives $[\![t]\!] = [\![t']\!] \implies t \cong_{\mathrm{ctx}} t' : \tau$

Recap

We have related operational semantics and denotational semantics:

- Soundness: $t \Downarrow_\tau v \implies [\![t]\!] = [\![v]\!]$ for every type τ
- Adequacy: $[\![t]\!] = [\![v]\!] \implies t \Downarrow_\tau v$ for $\tau \in \{\mathtt{nat}, \mathtt{bool}\}$

We have also related contextual with denotational equivalence:

- Compositionality: $[\![t]\!] = [\![t']\!] \implies [\![\mathcal{C}[t]]\!] = [\![\mathcal{C}[t']]\!]$ for all terms and contexts
- Using the above gives $[\![t]\!] = [\![t']\!] \implies t \cong_{\mathrm{ctx}} t' : \tau$

- What about the converse?

$$t \cong_{\mathrm{ctx}} t' : \tau \overset{?}{\implies} [\![t]\!] = [\![t']\!]$$

Recap

We have related operational semantics and denotational semantics:

- Soundness: $t \Downarrow_\tau v \implies [\![t]\!] = [\![v]\!]$ for every type τ
- Adequacy: $[\![t]\!] = [\![v]\!] \implies t \Downarrow_\tau v$ for $\tau \in \{\mathtt{nat}, \mathtt{bool}\}$

We have also related contextual with denotational equivalence:

- Compositionality: $[\![t]\!] = [\![t']\!] \implies [\![\mathcal{C}[t]]\!] = [\![\mathcal{C}[t']]\!]$ for all terms and contexts
- Using the above gives $[\![t]\!] = [\![t']\!] \implies t \cong_{\mathrm{ctx}} t' : \tau$

- What about the converse?

$$t \cong_{\mathrm{ctx}} t' : \tau \overset{?}{\implies} [\![t]\!] = [\![t']\!]$$

Full abstraction

A denotational model is called fully abstract when

$$t_1 \cong_{\text{ctx}} t_2 : \tau \Rightarrow [\![t_1]\!] = [\![t_2]\!] \in [\![\tau]\!]$$

Full abstraction

A denotational model is called fully abstract when

$$t_1 \cong_{\text{ctx}} t_2 : \tau \Rightarrow [\![t_1]\!] = [\![t_2]\!] \in [\![\tau]\!]$$

It is a form of completeness of semantic equivalence wrt. contextual equivalence.

Full abstraction

A denotational model is called **fully abstract** when

$$t_1 \cong_{\text{ctx}} t_2 : \tau \Rightarrow [\![t_1]\!] = [\![t_2]\!] \in [\![\tau]\!]$$

It is a form of **completeness** of semantic equivalence wrt. contextual equivalence.

The domain model of PCF is **not** fully abstract.

Parallel or

The *parallel or* function $\mathbf{por} : \mathbb{B}_\bot \times \mathbb{B}_\bot \to \mathbb{B}_\bot$ is defined as given by the following table:

por	true	false	$\bot$
true	true	true	true
false	true	false	$\bot$
$\bot$	true	$\bot$	$\bot$

Left sequential or

The (left) sequential or function $\mathrm{or} : \mathbb{B}_\bot \times \mathbb{B}_\bot \to \mathbb{B}_\bot$ is defined as

$$\mathrm{or} \stackrel{\mathrm{def}}{=} [\![\texttt{fun}\, x\texttt{:bool.}\ \texttt{fun}\, y\texttt{:bool.}\ \texttt{if}\ x\ \texttt{then true else}\ y]\!]$$

It is given by the following table:

or	true	false	$\bot$
true	true	true	true
false	true	false	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

Parallel vs sequential or

por	true	false	⊥
true	true	true	true
false	true	false	⊥
⊥	true	⊥	⊥

or	true	false	⊥
true	true	true	true
false	true	false	⊥
⊥	⊥	⊥	⊥

Parallel vs sequential or

por	true	false	⊥
true	true	true	true
false	true	false	⊥
⊥	true	⊥	⊥

or	true	false	⊥
true	true	true	true
false	true	false	⊥
⊥	⊥	⊥	⊥

or is sequential, but **por** is not.

Undefinability or parallel or

Theorem

There is no closed PCF term

$$t : \mathtt{bool} \to \mathtt{bool} \to \mathtt{bool}$$

satisfying

$$[\![t]\!] = \mathrm{por} : \mathbb{B}_\bot \to \mathbb{B}_\bot \to \mathbb{B}_\bot \ .$$

Undefinability or parallel or

Theorem

There is no closed PCF term

$$t : \mathtt{bool} \to \mathtt{bool} \to \mathtt{bool}$$

satisfying

$$[\![t]\!] = \mathrm{por} : \mathbb{B}_\perp \to \mathbb{B}_\perp \to \mathbb{B}_\perp \ .$$

The proof – originally by Plotkin – is beyond the scope of this course.

Failure of full abstraction

The denotational model of Pcf in domains and continuous functions is not fully abstract.

Failure of full abstraction

The denotational model of PCF in domains and continuous functions is not fully abstract.

For well-chosen $T_{\mathtt{true}}$ and $T_{\mathtt{false}}$,

$$T_{\mathtt{true}} \cong_{\mathrm{ctx}} T_{\mathtt{false}} : (\mathtt{bool} \to \mathtt{bool} \to \mathtt{bool}) \to \mathtt{bool}$$

$$[\![T_{\mathtt{true}}]\!] \neq [\![T_{\mathtt{false}}]\!] \in (\mathbb{B} \to \mathbb{B} \to \mathbb{B}) \to \mathbb{B}$$

Failure of full abstraction

The denotational model of Pcf in domains and continuous functions is not fully abstract.

For well-chosen $T_{\mathtt{true}}$ and $T_{\mathtt{false}}$,

$$T_{\mathtt{true}} \cong_{\mathrm{ctx}} T_{\mathtt{false}} : (\mathtt{bool} \to \mathtt{bool} \to \mathtt{bool}) \to \mathtt{bool}$$

$$[\![T_{\mathtt{true}}]\!] \neq [\![T_{\mathtt{false}}]\!] \in (\mathbb{B} \to \mathbb{B} \to \mathbb{B}) \to \mathbb{B}$$

Idea:

- for all $f \in PCF_{\mathtt{bool}\to\mathtt{bool}\to\mathtt{bool}}$, ensure $T_b\ f \Uparrow_{\mathtt{bool}}$…
- but $[\![T_b]\!](\mathrm{por}) = [\![b]\!]$.

Example of full abstraction failure

$$
\begin{aligned}
T_b \overset{\text{def}}{=}\ & \texttt{fun}\ f\colon \texttt{bool} \to (\texttt{bool} \to \texttt{bool}).\\
& \quad \texttt{if}(f\ \texttt{true}\ \Omega_{\texttt{bool}})\ \texttt{then}\\
& \quad\quad \texttt{if}\ (f\ \Omega_{\texttt{bool}}\ \texttt{true})\ \texttt{then}\\
& \quad\quad\quad \texttt{if}\ (f\ \texttt{false}\ \texttt{false})\ \texttt{then}\ \Omega_{\texttt{bool}}\ \texttt{else}\ b\\
& \quad\quad \texttt{else}\ \Omega_{\texttt{bool}}\\
& \quad \texttt{else}\ \Omega_{\texttt{bool}}
\end{aligned}
$$