Queens' College Cambridge

# Denotational Semantics

Alistair O'Brien

Department of Computer Science

May 20, 2022

# 1 Domain Theory

## Posets

**Definition 1.0.1.** (**Partially Ordered Sets**) A *poset* is a pair $(D, \sqsubseteq)$ where $\sqsubseteq : D \longleftrightarrow D$ is a *partial order* on the set $D$:

$$\frac{}{d \sqsubseteq d}\ \textsc{Refl} \qquad \frac{d_1 \sqsubseteq d_2 \quad d_3 \sqsubseteq d_3}{d_1 \sqsubseteq d_3}\ \textsc{Trans} \qquad \frac{d_1 \sqsubseteq d_2 \quad d_2 \sqsubseteq d_1}{d_1 = d_2}\ \textsc{AntiSym}$$

**Definition 1.0.2.** (**Poset** $X \rightharpoonup Y$) The poset $X \rightharpoonup Y$ is defined as:

$$\begin{aligned} X \rightharpoonup Y &= \text{ set of partial functions from } X \text{ to } Y \\ f \sqsubseteq g &\iff \operatorname{dom} f \subseteq \operatorname{dom} g \wedge (\forall x \in \operatorname{dom} f . f(x) = g(x)) \end{aligned}$$

**Definition 1.0.3.** (**Montonicity**) A function $f : D \to E$ between posets $D, E$ is *monotone* if:

$$\frac{d_1 \sqsubseteq d_2}{f(d_1) \sqsubseteq f(d_2)}\ \textsc{Mono}$$

**Definition 1.0.4.** (**Least Element**) An element $d \in S \subseteq D$ of the set $S$ is said to be the *least* if:

$$\forall x \in S . d \sqsubseteq x$$

- By *anti-symmetry* of $\sqsubseteq$, least elements are always unique.

**Definition 1.0.5.** (**Fixed Points**) Let $f : D \to D$ be a function in the poset $D$:

**Fixed Point** A *fixed point* of $f$ is an element $d \in D$ satisfying $f(d) = d$.

**Pre-fixed Point** A *pre-fixed point* of $f$ is an element $d \in D$ satisfying $f(d) \sqsubseteq d$. We write $fix(f)$ for the *least* pre-fixed point of $f$.

**Lemma 1.0.1.** If $f$ is monotone, then $fix(f)$ (if it exists) is a fixed point for $f$.

## Domains

**Definition 1.0.6.** (**Chain**) A chain is an enumerable increasing set of elements $\langle d_i \rangle_{i \geq 0}$:

$$d_0 \sqsubseteq d_1 \sqsubseteq d_2 \sqsubseteq \cdots,$$

The set of chains for a poset $D$ is denoted $\mathsf{Ch}(D)$.

**Definition 1.0.7.** (**Least Upper Bound (Lub)**) A least upper bound for a chain $\langle d_i \rangle_{i \geq 0} \in \mathsf{Ch}(D)$ is an element, written $\bigsqcup_{i \geq 0} d_i$, satisfying:

$$\frac{}{d_m \sqsubseteq \bigsqcup_{i \geq 0} d_i} \textsc{Lub1} \qquad \frac{\forall i \in \mathbb{N} \qquad d_i \sqsubseteq d}{\bigsqcup_{i \geq 0} d_i \sqsubseteq d} \textsc{Lub2}$$

**Definition 1.0.8.** (**Chain-complete Posets (CPO)**) A poset $(D, \sqsubseteq)$ is *chain complete* (a CPO) if for all chains $\langle d_i \rangle_{i \geq 0} \in \mathsf{Ch}(D)$, the lub $\bigsqcup_{i \geq 0} d_i$ exists.

**Lemma 1.0.2.** (**Properties of Lubs**) Let $D$ be cpo:

(i) $\forall d \in D. \bigsqcup d = d$

(ii) For the chain $\langle d_i \rangle_{i \geq 0} \in \mathsf{Ch}(D)$ and $n \in \mathbb{N}$:

$$\bigsqcup_{i \geq 0} d_n = \bigsqcup_{i \geq 0} d_{i+n}$$

(iii) For the chains $\langle d_i \rangle_{i \geq 0}, \langle e_i \rangle_{i \geq 0} \in \mathsf{Ch}(D)$:

$$\frac{\forall i \geq 0 \qquad d_i \sqsubseteq e_i}{\bigsqcup_{i \geq 0} d_i \sqsubseteq \bigsqcup_{i \geq 0} e_i}$$

**Lemma 1.0.3.** (**Diagonalisation**) Let $D$ be a cpo. For elements $d_{ij} \in D$ (for $i, j \geq 0$) satisfying:

$$i_1 \leq i_2 \wedge j_1 \leq j_2 \implies d_{i_1 j_1} \sqsubseteq d_{i_2 j_2},$$

then

$$\bigsqcup_{i \geq 0} \bigsqcup_{j \geq 0} d_{ij} = \bigsqcup_{j \geq 0} \bigsqcup_{i \geq 0} d_{ij} = \bigsqcup_{k \geq 0} d_{kk}$$

**Definition 1.0.9.** (**Domain**) A *domain* is a cpo $(D, \sqsubseteq)$ with a least element $\perp$

**Definition 1.0.10.** (**Domain $X \rightharpoonup Y$**)

**Lub** $\bigsqcup f_0 \sqsubseteq f_1 \sqsubseteq f_2 \sqsubseteq \cdots$ is partial function $f$ s.t:

$$\operatorname{dom} f = \bigcup_{n \geq 0} \operatorname{dom} f_n$$

$$f(x) = \begin{cases} f_n(x) & \text{if } x \in \operatorname{dom} f_n \\ \text{undefined} & \text{otherwise} \end{cases}$$

**Least element** Least element $\perp$ is undefined partial function $\emptyset$

**Definition 1.0.11.** (**Continuity and Strictness**) If $D, E$ are cpos. A function $f : D \to E$ is *continuous* iff:

(i) $f$ is monotone

(ii) $f$ preserves lubs:

$$\forall \langle d_i \rangle_{i \geq 0} \in \mathsf{Ch}(D). f\left(\bigsqcup_{i \geq 0} d_i\right) = \bigsqcup_{i \geq 0} f(d_i)$$

$f$ is *strict* iff $f(\bot_D) = \bot_E$.

**Theorem 1.0.1.** (**Tarski's Fixed Point Theorem**) Let $f : D \to D$ be a continuous function on the domain $D$:

(i) $f$'s *least pre-fixed point* is $fix(f) = \bigsqcup_{i \geq 0} f^i(\bot)$

(ii) $fix(f)$ is the least fixed point

*Proof.* By induction, we have $f^n(\bot) \sqsubseteq f^{n+1}(\bot)$ for all $n \in \mathbb{N}$. We note that:

$$\begin{aligned} f(fix(f)) &= f\left(\bigsqcup_{i \geq 0} f^i(\bot)\right) \\ &= \bigsqcup_{i \geq 0} f(f^i(\bot)) && (f \text{ is cont.}) \\ &= \bigsqcup_{i \geq 0} f^{i+1}(\bot) && (\text{defn. of } f^n) \\ &= \bigsqcup_{i \geq 0} f^i(\bot) && (\text{lemma 1.0.2}) \\ &= fix(f) \end{aligned}$$

We now show that $fix(f)$ is *least*, that is:

$$\forall d \in D. f(d) = d \implies fix(f) \sqsubseteq d$$

Let $d \in D$ be arbitrary. Assume $f(d) = d$. Sufficient to show that $\forall i \in \mathbb{N}. f^i(\bot) \sqsubseteq d$. Proved by *induction* on $i \in \mathbb{N}$.

**Definition 1.0.12.** (**Flat Domains**) Let $D_\bot = D \cup \{\bot\}$. $(D_\bot, \sqsubseteq)$ is a *flat domain* where $\sqsubseteq : D \longleftrightarrow D$ s.t

$$\frac{}{\bot \sqsubseteq d}\ \textsc{Bot} \qquad\qquad \frac{}{d \sqsubseteq d}\ \textsc{Refl}$$

**Definition 1.0.13.** (**Product Domains**) Let $(D_1, \sqsubseteq_1)$ and $(D_2, \sqsubseteq_2)$ be two domains. $(D_1 \times D_2, \sqsubseteq)$ is a domain:

$$D_1 \times D_2 = \{(d_1, d_2) : d_1 \in D_1, d_2 \in D_2\}$$

$$\frac{d_1 \sqsubseteq d_1' \qquad d_2 \sqsubseteq d_2'}{(d_1, d_2) \sqsubseteq (d_1', d_2')}$$

$$\bigsqcup_{i \geq 0} (d_i^1, d_i^2) = \left(\bigsqcup_{i \geq 0} d_i^1, \bigsqcup_{j \geq 0} d_j^2\right)$$

$$\bot_{1 \times 2} = (\bot_1, \bot_2)$$

**Definition 1.0.14.** (**Function Domains**) Let $(D_1, \sqsubseteq_1)$ and $(D_2, \sqsubseteq_2)$ be two domains. $(D_1 \to D_2, \sqsubseteq)$ is a domain:

$$D_1 \to D_2 = \{f \in D_1 \to D_2 : f \text{ is continuous}\}$$
$$\frac{\forall d \in D_1 \qquad f(d) \sqsubseteq_2 g(d)}{f \sqsubseteq g}$$
$$\bigsqcup_{i \geq 0} f_i = \lambda d \in D. \bigsqcup_{i \geq 0} f_i(d)$$

# Scott Induction

**Definition 1.0.15.** (**Chain-Closed and Admissible Subsets**) Let $D$ be a cpo.

**Chain-closed** A subset $S \subseteq D$ is *chain-closed* iff $\forall \langle d_i \rangle_{i \geq 0} \in \mathsf{Ch}(D)$:

$$\frac{\forall i \geq 0 \qquad d_i \in S}{\bigsqcup_{i \geq 0} d_i \in S}$$

**Admissible** $S \subseteq D$ is *admissible* iff $S$ is *chain-closed* and $\perp \in S$.

**Theorem 1.0.2.** (**Scott's Fixed Point Induction**) Let $D$ be a domain and $f : D \to D$ be a continuous function. Let $S \subseteq D$ be an *admissible subset*:

$$\frac{\forall d \in D \qquad d \in S \implies f(d) \in S}{fix(f) \in S} \textsc{Scott}$$

*Proof.* Let us assume $\forall d \in D. d \in S \implies f(d) \in S$. Since $S$ is *chain-closed*, sufficient to show that $\forall i \geq 0. f^i(\perp) \in S$. Proof by *induction* on $i \geq 0$.

## Chain-Closed Combinators

**Definition 1.0.16.** (**Chain-Closed Primitives**) The chain-closed primitives for the domain $(D, \sqsubseteq)$ are:

$$\begin{aligned} \sqsubseteq_D &= \{(d_1, d_2) \in D \times D : d_1 \sqsubseteq d_2\} \\ =_D &= \{(d_1, d_2) \in D \times D : d_1 = d_2\} \\ \downarrow d &= \{e \in D : e \sqsubseteq d\} \end{aligned}$$

### Syntax for Chain-Closed Sets

Chain-Closed Sets

$$\begin{aligned} X ::= {} & \sqsubseteq_D \mid =_D \mid \downarrow d \\ \mid {} & \overleftarrow{f}(X) && f \text{ is continuous} \\ \mid {} & X \cap X \mid X \cup X \mid \bigcap_{i \in I} X_i \end{aligned}$$

# 2 PCF

## Syntax

| | |
|---|---|
| Types | $\tau ::= \mathbb{N} \mid \mathbb{B} \mid \tau \to \tau$ |
| Terms | $e ::= 0 \mid \mathsf{succ}\ e \mid \mathsf{pred}\ e \mid \mathsf{zero?}\ e$ <br> $\mid \mathsf{true} \mid \mathsf{false} \mid \mathsf{if}\ e\ \mathsf{then}\ e\ \mathsf{else}\ e$ <br> $\mid x \mid \lambda x : \tau.e \mid e\ e \mid \mathsf{fix}\ e$ |
| Values | $v ::= 0 \mid \mathsf{succ}\ v \mid \mathsf{true} \mid \mathsf{false} \mid \lambda x : \tau.e$ |
| Contexts | $\Gamma ::= \cdot \mid \Gamma, x : \tau$ |
| Evaluation Contexts | $\mathbb{E} ::= [\cdot] \mid \mathsf{succ}\ \mathbb{E} \mid \mathsf{pred}\ \mathbb{E} \mid \mathsf{zero?}\ \mathbb{E} \mid \mathsf{if}\ \mathbb{E}\ \mathsf{then}\ e\ \mathsf{else}\ e$ <br> $\mid \mathbb{E}\ e \mid v\ \mathbb{E}$ |

## Typing Rules

$$\frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau}\ \textsc{Hyp} \qquad \frac{}{\Gamma \vdash \mathsf{zero} : \mathbb{N}}\ \textsc{Zero} \qquad \frac{\Gamma \vdash e : \mathbb{N}}{\Gamma \vdash \mathsf{succ}\ e : \mathbb{N}}\ \textsc{Succ}$$

$$\frac{\Gamma \vdash e : \mathbb{N}}{\Gamma \vdash \mathsf{zero?}\ e : \mathbb{B}}\ \textsc{Zero?} \qquad \frac{\Gamma \vdash e : \mathbb{N}}{\Gamma \vdash \mathsf{pred}\ e : \mathbb{N}}\ \textsc{Pred} \qquad \frac{}{\Gamma \vdash \mathsf{true} : \mathbb{B}}\ \textsc{True}$$

$$\frac{}{\Gamma \vdash \mathsf{false} : \mathbb{B}}\ \textsc{False} \qquad \frac{\Gamma \vdash e_1 : \mathbb{B}}{\Gamma \vdash \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 : \tau}\ \textsc{If} \qquad \frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x : \tau_1.e : \tau_1 \to \tau_2}\ \textsc{Fn}$$

$$\frac{\Gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1\ e_2 : \tau_2}\ \textsc{App} \qquad \frac{\Gamma \vdash e : \tau \to \tau}{\Gamma \vdash \mathsf{fix}\ e : \tau}\ \textsc{Fix}$$

## Operational Semantics

- $\Lambda_\tau = \{e \in \Lambda : \cdot \vdash e : \tau\}$
- 2 semantics:

  **Small-step** $\cdot \rightsquigarrow_\tau \cdot \subseteq \Lambda_\tau \times \Lambda_\tau$

  **Big-step** $\cdot \Downarrow_\tau \cdot \subseteq \Lambda_\tau \times \mathsf{Val}_\tau$

$$\frac{}{v \Downarrow_\tau v}\ \textsc{Val} \qquad \frac{e \Downarrow_\mathbb{N} v}{\mathsf{succ}\ e \Downarrow_\mathbb{N} \mathsf{succ}\ v}\ \textsc{Succ} \qquad \frac{e \Downarrow_\mathbb{N} \mathsf{succ}\ v}{\mathsf{pred}\ e \Downarrow_\mathbb{N} v}\ \textsc{Pred}$$

$$\frac{e \Downarrow_\mathbb{N} \mathsf{zero}}{\mathsf{zero?}\ e \Downarrow_\mathbb{B} \mathsf{true}}\ \textsc{Zero?}_1 \qquad \frac{e \Downarrow_\mathbb{N} \mathsf{succ}\ v}{\mathsf{zero?}\ e \Downarrow_\mathbb{B} \mathsf{false}}\ \textsc{Zero?}_2$$

$$\frac{e_1 \Downarrow_\mathbb{B} \mathsf{true} \qquad e_2 \Downarrow_\tau v}{\mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 \Downarrow_\tau v}\ \textsc{If}_1 \qquad \frac{e_1 \Downarrow_\mathbb{B} \mathsf{false} \qquad e_3 \Downarrow_\tau v}{\mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 \Downarrow_\tau v}\ \textsc{If}_1$$

$$\frac{e_1 \Downarrow_{\tau_1 \to \tau_2} \lambda x : \tau_1.e \qquad \{e_2/x\}e \Downarrow_{\tau_2} v}{e_1\ e_2 \Downarrow_{\tau_2} v}\ \textsc{Fn} \qquad \frac{e\ (\mathsf{fix}\ e) \Downarrow_\tau v}{\mathsf{fix}\ e \Downarrow_\tau v}\ \textsc{Fix}$$

$$\frac{e \rightsquigarrow_\tau e'}{\mathbb{E}[e] \rightsquigarrow_{\tau_\mathbb{E}} \mathbb{E}[e']}\ \textsc{EvalCtx} \qquad \frac{}{\mathsf{pred}(\mathsf{succ}\ v) \rightsquigarrow_\mathbb{N} v}\ \textsc{RedPred}$$

$$\frac{}{\mathsf{zero?}\ \mathsf{zero} \rightsquigarrow_\mathbb{B} \mathsf{true}}\ \textsc{RedZero}_1 \qquad \frac{}{\mathsf{zero?}\ (\mathsf{succ}\ v) \rightsquigarrow_\mathbb{B} \mathsf{false}}\ \textsc{RedZero}_2$$

$$\frac{}{\mathsf{if\ true\ then}\ e_1\ \mathsf{else}\ e_2 \rightsquigarrow_\tau e_1}\ \textsc{RedIf}_1 \qquad \frac{}{\mathsf{if\ false\ then}\ e_1\ \mathsf{else}\ e_2 \rightsquigarrow_\tau e_2}\ \textsc{RedIf}_2$$

$$\frac{}{(\lambda x : \tau_1.e)\ e_2 \rightsquigarrow_{\tau_2} \{e_2/x\}e}\ \textsc{RedFn} \qquad \frac{}{\mathsf{fix}\ e \rightsquigarrow_\tau e\ (\mathsf{fix}\ e)}\ \textsc{RedFix}$$

# Denotational Semantics

$\boxed{[\![\tau]\!] \in \mathsf{Domain}}$

$$\begin{aligned}
[\![\mathbb{N}]\!] &= \mathbb{N}_\perp \\
[\![\mathbb{B}]\!] &= \mathbb{B}_\perp \\
[\![\tau_1 \to \tau_2]\!] &= [\![\tau_1]\!] \to [\![\tau_2]\!]
\end{aligned}$$

$\boxed{[\![\Gamma]\!] \in \mathsf{Set}}$

$$[\![\Gamma]\!] = (x \in \mathrm{dom}\,\Gamma) \to [\![\Gamma(x)]\!]\,.$$

$\boxed{[\![\Gamma \vdash e : \tau]\!] \in [\![\Gamma]\!] \to [\![\tau]\!]}$

$$\begin{aligned}
[\![\Gamma \vdash \mathsf{zero}]\!]\,\rho &= 0 \\
[\![\Gamma \vdash \mathsf{false}]\!]\,\rho &= \mathit{false} \\
[\![\Gamma \vdash \mathsf{true}]\!]\,\rho &= \mathit{true} \\
[\![\Gamma \vdash x]\!]\,\rho &= \rho(x) \\
[\![\Gamma \vdash \mathsf{succ}\ e]\!]\,\rho &= \begin{cases} [\![\Gamma \vdash e]\!]\,\rho + 1 & \text{if } [\![\Gamma \vdash e]\!]\,\rho \neq \perp \\ \perp & \text{otherwise} \end{cases} \\
[\![\Gamma \vdash \mathsf{pred}\ e]\!]\,\rho &= \begin{cases} [\![\Gamma \vdash e]\!]\,\rho - 1 & \text{if } [\![\Gamma \vdash e]\!]\,\rho > 0 \\ \perp & \text{if } [\![\Gamma \vdash e]\!]\,\rho \in \{0, \perp\} \end{cases}
\end{aligned}$$

$$\llbracket \Gamma \vdash \mathsf{zero?}\ e \rrbracket \rho = \begin{cases} true & \text{if } \llbracket \Gamma \vdash e \rrbracket \rho = 0 \\ false & \text{if } \llbracket \Gamma \vdash e \rrbracket \rho > 0 \\ \bot & \text{if } \llbracket \Gamma \vdash e \rrbracket \rho = \bot \end{cases}$$

$$\llbracket \Gamma \vdash \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 \rrbracket \rho = \begin{cases} \llbracket \Gamma \vdash e_2 \rrbracket \rho & \text{if } \llbracket \Gamma \vdash e_1 \rrbracket \rho = true \\ \llbracket \Gamma \vdash e_3 \rrbracket \rho & \text{if } \llbracket \Gamma \vdash e_1 \rrbracket \rho = false \\ \bot & \text{if } \llbracket \Gamma \vdash e_1 \rrbracket \rho = \bot \end{cases}$$

$$\llbracket \Gamma \vdash e_1\ e_2 \rrbracket \rho = (\llbracket \Gamma \vdash e_1 \rrbracket \rho)(\llbracket \Gamma \vdash e_2 \rrbracket \rho)$$

$$\llbracket \Gamma \vdash \lambda x : \tau_1 . e \rrbracket \rho = \lambda d \in \llbracket \tau_1 \rrbracket . \llbracket \Gamma, x : \tau_1 \vdash e \rrbracket (\rho, x \mapsto d)$$

$$\llbracket \Gamma \vdash \mathsf{fix}\ e \rrbracket \rho = fix(\llbracket \Gamma \vdash e \rrbracket \rho)$$

# Theorems

**Lemma 2.0.1.** (**Typing Properties**) The following holds for $\cdot \vdash \cdot : \cdot$:

**Uniqueness of typing** If $\Gamma \vdash e : \tau_1$ and $\Gamma \vdash e : \tau_2$, then $\tau_1 = \tau_2$.

**Substitution** If $\Gamma \vdash e_1 : \tau_1$ and $\Gamma, x : \tau_1 \vdash e_2 : \tau_2$, then $\Gamma \vdash \{e_1/x\}e_2 : \tau_2$.

*Proof.* Proof by *structural induction* on $e$ and *rule induction* on $\Gamma, x : \tau_1 \vdash e : \tau_2$.

**Lemma 2.0.2.** (**Semantic Properties**) The following holds:

**Soundness and Completeness** $e \Downarrow_\tau v \iff e \rightsquigarrow_\tau^* v$.

**Determinacy** If $e \Downarrow_\tau v_1$ and $e \Downarrow_\tau v_2$, then $v_1 = v_2$.

*Proof.* Proof by *rule induction* on $e \Downarrow_\tau v_1$.

- **Notation**: $\llbracket e \rrbracket = \llbracket \cdot \vdash e \rrbracket \bot$

**Definition 2.0.1.** (**Denotational Semantic Properties**) The following holds:

**Continuity** $\llbracket \Gamma \vdash e \rrbracket \in \llbracket \Gamma \rrbracket \to \llbracket \tau \rrbracket$ is a continuous function in $\llbracket \Gamma \rrbracket \to \llbracket \tau \rrbracket$.

**Substitution** If $\Gamma \vdash e_1 : \tau_1$ and $\Gamma, x : \tau \vdash e_2 : \tau_2$, then

$$\llbracket \Gamma \vdash \{e_1/x\}e_2 \rrbracket \rho = \llbracket \Gamma, x : \tau_1 \vdash e_2 \rrbracket (\rho, x \mapsto \llbracket \Gamma \vdash e_1 \rrbracket \rho)$$

**Soundness** If $e \Downarrow_\tau v$ then $\llbracket e \rrbracket = \llbracket v \rrbracket$

*Proof.* Proof by *rule induction* on $\Gamma \vdash e : \tau$, $\Gamma, x : \tau \vdash e_2 : \tau_2$ and $e \Downarrow_\tau v$.

## Adequacy

**Definition 2.0.2.** (**Denotational Approximation**) The binary relation $\cdot \lhd_\tau \cdot \subseteq \llbracket \tau \rrbracket \times \Lambda_\tau$ is defined as:

$$d \lhd_{\mathbb{N}} e \iff d \in \mathbb{N} \implies e \Downarrow_{\mathbb{N}} \mathsf{succ}^d\ \mathsf{zero}$$

$$d \lhd_{\mathbb{B}} e \iff \begin{cases} d = true & \implies e \Downarrow_{\mathbb{B}} \mathsf{true} \\ d = false & \implies e \Downarrow_{\mathbb{B}} \mathsf{false} \end{cases}$$

$$d_1 \lhd_{\tau_1 \to \tau_2} e_1 \iff \forall d_2 \in [\![\tau_1]\!], e_2 \in \Lambda_{\tau_1}. d_2 \lhd_{\tau_1} e_2 \implies d_1(d_2) \lhd_{\tau_2} e_1\ e_2$$

The contextual extensions for $\Gamma$, where $\rho \in [\![\Gamma]\!]$ and $\theta$ is a $\Gamma$-substitution:

$$\rho \lhd_{\Gamma} \theta \iff \forall x \in \operatorname{dom} \Gamma. \rho(x) \lhd_{\Gamma(x)} \theta(x)$$

**Lemma 2.0.3.**

(i) $\bot \lhd_\tau e$ for all $e \in \Lambda_\tau$

(ii) $\{d \in [\![\tau]\!] : d \lhd_\tau e\}$ is a chain-closed subset.

(iii) If $d_2 \sqsubseteq d_1$ and $d_2 \lhd_\tau e_1$ and $\forall v \in \mathsf{Val}_\tau. e_1 \Downarrow_\tau v \implies e_2 \Downarrow_\tau v$, then $d_2 \lhd_\tau e_2$.

*Proof.* Proof by *structural induction* on $\tau$.

**Theorem 2.0.1.** (**Fundamental Property**) If $\Gamma \vdash e : \tau$, then for all $\rho \in [\![\Gamma]\!]$ and $\theta \in \mathsf{Subst}(\Gamma)$:

$$\rho \lhd_\Gamma \theta \implies [\![\Gamma \vdash e]\!] \rho \lhd_\tau \theta(e)$$

*Proof.* Proof by *rule induction* on $\Gamma \vdash e : \tau$.

**Theorem 2.0.2.** (**Adequacy**) For types $\tau \in \{\mathbb{N}, \mathbb{B}\}$,

$$[\![e]\!] = [\![v]\!] \in [\![\tau]\!] \implies e \Downarrow_\tau v$$

*Proof.* By fundamental property, we have $[\![e]\!] \lhd_\tau e$ (for $\Gamma = \cdot, \rho = \bot, \theta = \emptyset$). Cases on $\tau$:

- $\tau = \mathbb{N}$. We have $v = \mathsf{succ}^n\ \mathsf{zero}$ for some $n \in \mathbb{N}$, thus:

$$\begin{aligned} [\![e]\!] &= [\![\mathsf{succ}^n\ \mathsf{zero}]\!] = n \\ &\implies n = [\![e]\!] \rhd_\tau e && \text{(fund. prop)} \\ &\implies e \Downarrow_{\mathbb{N}} \mathsf{succ}^n\ \mathsf{zero} && \text{(defn. of } \lhd_{\mathbb{N}}) \end{aligned}$$

- $\tau = \mathbb{B}$. Similar

# Contextual Equivalence

Contexts $\mathscr{C} ::= [\cdot] \mid \mathsf{zero} \mid \mathsf{succ}\ \mathscr{C} \mid \mathsf{zero?}\ \mathscr{C} \mid \mathsf{true} \mid \mathsf{false} \mid \mathsf{if}\ \mathscr{C}\ \mathsf{then}\ \mathscr{C}\ \mathsf{else}\ \mathscr{C}$
$\mid x \mid \lambda x : \tau_1.\mathscr{C} \mid \mathscr{C}\ \mathscr{C} \mid \mathsf{fix}\ \mathscr{C}$

**Definition 2.0.3.** (**Contextual Equivalence**) For $e_1, e_2 \in \Lambda, \tau \in \mathsf{Type}, \Gamma \in \mathsf{Ctx}$, $e_1, e_2$ are contextually equivalent $\Gamma \vdash e_1 \cong e_2 : \tau$ iff

$$\begin{aligned} &\Gamma \vdash e_1 : \tau \land \Gamma \vdash e_2 : \tau \\ &\quad \land (\forall \mathscr{C}, \gamma \in \{\mathbb{N}, \mathbb{B}\}, v \in \mathsf{Val}_\tau. \mathscr{C}[e_1] \Downarrow_\gamma v \iff \mathscr{C}[e_2] \Downarrow_\gamma v) \end{aligned}$$

**Theorem 2.0.3.** (**Compositionality**) If $\Gamma \vdash e_1 : \tau, \Gamma \vdash e_2 : \tau$ and $\Gamma' \vdash \mathscr{C}[e_1] : \tau', \Gamma' \vdash \mathscr{C}[e_2] : \tau'$ and $[\![\Gamma \vdash e_1]\!] = [\![\Gamma \vdash e_2]\!]$, then

$$[\![\Gamma' \vdash \mathscr{C}[e_1]]\!] = [\![\Gamma' \vdash \mathscr{C}[e']]\!]$$

*Proof.* Proof by *structural induction* on $\mathscr{C}$.

- **Useful Lemma**: $[\![e_1]\!] = [\![e_2]\!] \implies [\![\mathscr{C}[e_1]]\!] = [\![\mathscr{C}[e_2]]\!]$

**Theorem 2.0.4.** (**Coincidence Theorem**) For all $\Gamma \in \mathsf{Ctx}, e_1, e_2 \in \Lambda, \tau \in \mathsf{Type}$,

$$[\![\Gamma \vdash e_1]\!] = [\![\Gamma \vdash e_2]\!] \in [\![\tau]\!] \implies \Gamma \vdash e_1 \cong e_2 : \tau$$

*Proof.* Cases on $\gamma$ (in $\Gamma \vdash e_1 \cong e_2 : \tau$) using soundness, compositionality and adequacy.

**Definition 2.0.4.** (**Contextual Preorder**) For $e_1, e_2 \in \Lambda, \tau \in \mathsf{Type}, \Gamma \in \mathsf{Ctx}$, $e_2$ contextually extends $e_1$ $\Gamma \vdash e_1 \leq e_2 : \tau$ iff

$$\begin{aligned}&\Gamma \vdash e_1 : \tau \wedge \Gamma \vdash e_2 : \tau \\ &\quad \wedge (\forall \mathscr{C}, \gamma \in \{\mathbb{N}, \mathbb{B}\}, v \in \mathsf{Val}_\tau . \mathscr{C}[e_1] \Downarrow_\gamma v \implies \mathscr{C}[e_2] \Downarrow_\gamma v)\end{aligned}$$

**Theorem 2.0.5.** For all $e_1, e_2 \in \Lambda_\tau$,

$$e_1 \leq e_2 : \tau \iff [\![e_1]\!] \lhd_\tau e_2$$

*Proof.*
($\implies$) Proof by fundamental property and $e_1 \leq e_2 : \tau \iff \forall e \in \Lambda_{\tau \to \mathbb{B}} . e\ e_1 \Downarrow_{\mathbb{B}} \mathsf{true} \implies e\ e_2 \Downarrow_{\mathbb{B}} \mathsf{true}$.
($\impliedby$) Proof by fundamental property and $e_1 \leq e_2 : \tau \wedge d \lhd_\tau e_1 \implies d \lhd_\tau e_2$ (proved by *structural induction* on $\tau$).

# Full Abstraction

- **Problem**: Coincidence theorem is not bi-directional, this does not hold:

$$e_1 \cong e_2 : \tau \not\Longrightarrow [\![e_1]\!] = [\![e_2]\!]$$

**Definition 2.0.5.** (**Fully Abstract**) A denotational model is *fully abstract* when

$$\Gamma \vdash e_1 \cong e_2 : \tau \iff [\![\Gamma \vdash e_1]\!] = [\![\Gamma \vdash e_2]\!] \in [\![\tau]\!]$$

**Theorem 2.0.6.** PCF is **not fully abstract**.

*Proof.* Construct terms $e_1, e_2 \in \Lambda$ s.t $[\![e_1]\!] \neq [\![e_2]\!]$ and $e_1 \cong e_2 : \tau$.

Note $e_1 \cong e_2 : \tau$ is vacously true if $\forall e \in \Lambda . e_1\ e \not\Downarrow \wedge e_2\ e \not\Downarrow$. Thus it suffices to construct terms s.t $[\![e_1]\!]\, f \neq [\![e_2]\!]\, f$ for some $f \in [\![\tau_1]\!]$ and $e_1, e_2 \in \Lambda_{\tau_1 \to \tau_2}$.

**Definition 2.0.6.** (**Parallel-or**) $por : \mathbb{B}_\perp \to \mathbb{B}_\perp \to \mathbb{B}_\perp$ is the function defined by:

| $por$ | $true$ | $false$ | $\perp$ |
|---|---|---|---|
| $true$ | $true$ | $true$ | $true$ |
| $false$ | $true$ | $false$ | $\perp$ |
| $\perp$ | $true$ | $\perp$ | $\perp$ |

**Lemma 2.0.4.** (**Undefinability of por**) There is no term $e \in \Lambda$ s.t $[\![e]\!] = por$.

*Proof.* Assume exists $e$ s.t $[\![e]\!] = por$. Note that by semantics of $por$, $[\![e \ \mathsf{true}\ \Omega]\!] = true$, however, $[\![e\ \Omega]\!] = \perp$ for all function terms $e$. A contradiction!

- $por$ can be used to prove Theorem 2.0.6. Construct 2 terms $e_1, e_2$ :

$$\begin{aligned} e_i = \lambda f : \mathbb{B} \to \mathbb{B} \to \mathbb{B}.& \\ &\mathsf{if}\ (f\ \mathsf{true}\ \Omega)\ \mathsf{then} \\ &\quad \mathsf{if}\ (f\ \Omega\ \mathsf{true})\ \mathsf{then} \\ &\quad\quad \mathsf{if}\ (f\ \mathsf{false}\ \mathsf{false})\ \mathsf{then}\ \Omega\ \mathsf{else}\ b_i \\ &\quad \mathsf{else}\ \Omega \\ &\mathsf{else}\ \Omega \end{aligned}$$

  where $b_1 = \mathsf{true}, b_2 = \mathsf{false}$ and $\Omega = \mathsf{fix}\ (\lambda x : \mathbb{B}.x)$.

  **Meaning**: $e_i$ evaluates to $b_i$ if $f$ is $por$, otherwise returns $\Omega$.

  We have $[\![e_1]\!]\ (por) \neq [\![e_2]\!]\ (por)$ and $e_1, e_2$ are vacously contextually equivalent since $e_1, e_2$ terminates iff $[\![f]\!] = por$ (which cannot hold since $por$ is not definable in PCF).

## PCF + por

Terms $\quad e ::= \ldots \mid \mathsf{por}(e, e)$

$\boxed{\Gamma \vdash e : \tau}$

$$\frac{\Gamma \vdash e_1 : \mathbb{B} \qquad \Gamma \vdash e_2 : \mathbb{B}}{\Gamma \vdash \mathsf{por}(e_1, e_2) : \mathbb{B}}\ \textsc{Por}$$

$\boxed{e \Downarrow_\tau v}$

$$\frac{e_1 \Downarrow_\mathbb{B} \mathsf{true}}{\mathsf{por}(e_1, e_2) \Downarrow_\mathbb{B} \mathsf{true}}\ \textsc{Por}_1 \qquad \frac{e_2 \Downarrow_\mathbb{B} \mathsf{true}}{\mathsf{por}(e_1, e_2) \Downarrow_\mathbb{B} \mathsf{true}}\ \textsc{Por}_2$$

$$\frac{e_1 \Downarrow_\mathbb{B} \mathsf{false} \qquad e_2 \Downarrow_\mathbb{B} \mathsf{false}}{\mathsf{por}(e_1, e_2) \Downarrow_\mathbb{B} \mathsf{false}}\ \textsc{Por}_3$$

$[\![\Gamma \vdash e : \tau]\!] \in [\![\Gamma]\!] \to [\![\tau]\!]$

$$[\![\Gamma \vdash \mathsf{por}(e_1, e_2)]\!]\ \rho = por([\![\Gamma \vdash e_1]\!]\ \rho, [\![\Gamma \vdash e_2]\!]\ \rho)$$

**Theorem 2.0.7.** PCF + por is fully abstract