# Retrofitting Purity with Comonads & Capabilities

Vikraman Choudhury

Indiana University Bloomington

May 24, 2019

# Outline

# Capabilities

*Systems view*

A capability is a communicable, unforgeable token of authority, cf. Object Capabilities, Memory Capabilities.

# Capabilities

*PL view*

A capability is a static token over a set of memory regions, that indicates that the region is presently valid to access, cf. typed memory management.

# Outline

# Capabilities

**$\mathbb{C}$ : Set**

$\mathbb{C}$ is a set of capabilities, with decidable equality.
$(\wp(\mathbb{C}), \subseteq)$ is the complete lattice ordered by set inclusion.

# Weighted spaces

$\mathcal{W}$ : Cat

$$
\begin{aligned}
\mathrm{Obj}_{\mathcal{W}} &:= X = (|X| : \mathrm{Set},\ w_X : |X| \to \wp(\mathcal{C})) \\
\mathrm{Hom}_{\mathcal{W}}(X, Y) &:= \left\{ f \in |X| \to |Y| \;\middle|\; \begin{array}{l} \forall x \in |X|, \\ w_Y(f(x)) \subseteq w_X(x) \end{array} \right\}
\end{aligned}
$$

# Finite products

*Terminal object*

$$\begin{aligned} |1| &:= \{ * \} \\ w_1(*) &:= \emptyset \end{aligned}$$

*Products*

$$\begin{aligned} |A \times B| &:= |A| \times |B| \\ w_{A\times B}(a, b) &:= w_A(a) \cup w_B(b) \end{aligned}$$

# Cartesian closed

*Exponentials*

$$
\begin{aligned}
|A \to B| &:= |A| \to |B| \\
w_{A \to B}(f) &:= \left\{ c \in \mathcal{C} \;\middle|\; \begin{array}{l} \exists a \in |A|, \\ c \in w_B(f(a)), \\ c \notin w_A(a) \end{array} \right\}
\end{aligned}
$$

*Currying isomorphism*

$$\mathrm{Hom}_{\mathcal{W}}(C \times A, B) \cong \mathrm{Hom}_{\mathcal{W}}(C, A \to B)$$

# Monoidal closed

*Tensor*

$$
\begin{aligned}
|A \otimes B| \quad &:= \quad \left\{ (a,b) \in |A| \times |B| \;\middle|\; w_A(a) \cap w_B(b) = \emptyset \right\} \\
w_{A \otimes B}(a,b) \quad &:= \quad w_A(a) \cup w_A(b)
\end{aligned}
$$

# Monoidal closed

*Linear exponentials*

$$|A \multimap B| \quad := \quad \left\{ f \in |A| \to |B| \;\middle|\; \begin{array}{l} \exists C \in \wp(\mathcal{C}), \forall a \in |A|, \\ C \cap w_A(a) = \emptyset \Rightarrow \\ w_B(f(a)) \subseteq C \cup w_A(a) \end{array} \right\}$$

$$w_{A \to B}(f) \quad := \quad \left\{ c \in \mathcal{C} \;\middle|\; \begin{array}{l} \exists a \in |A|, \\ c \in w_B(f(a)), \\ c \notin w_A(a) \end{array} \right\}$$

*Tensor-hom adjunction*

$$\mathrm{Hom}_{\mathcal{W}}(C \otimes A, B) \cong \mathrm{Hom}_{\mathcal{W}}(C, A \multimap B)$$

# Comonad

$\square : \mathcal{W} \to \mathcal{W}$

$$
\begin{aligned}
|\square A| &:= \{\, a \in |A| \mid w_A(a) = \emptyset \,\} \\
w_{\square A}(a) &:= w_A(a) = \emptyset
\end{aligned}
$$

$$
\begin{aligned}
\varepsilon_A : \square A &\to A \\
a &\mapsto a \\
\delta_A : \square A &\xrightarrow{\sim} \square\square A \\
a &\mapsto a
\end{aligned}
$$

*$\square$ is idempotent*

$\delta_A$ is an isomorphism.

# Comonad

*$\square$ is strong monoidal*

$$
\begin{aligned}
m^I : 1 &\xrightarrow{\sim} \square 1 \\
* &\mapsto * \\
m^{\times}_{A,B} : (\square A \times \square B) &\xrightarrow{\sim} \square(A \times B) \\
(a\ ,\ b) &\mapsto (a\ ,\ b) \\
m^{\otimes}_{A,B} : (\square A \otimes \square B) &\xrightarrow{\sim} \square(A \otimes B) \\
(a\ ,\ b) &\mapsto (a\ ,\ b)
\end{aligned}
$$

# Monad

$T : \mathcal{W} \to \mathcal{W}$

$$
\begin{aligned}
|T(A)| &= |A| \times (\mathcal{C} \to \Sigma^*) \\
w_{T(A)}(a, o) &= w_A(a) \cup \{ c \in \mathcal{C} \mid o(c) \neq \varepsilon \}
\end{aligned}
$$

$$
\begin{aligned}
\eta_A : A &\to TA \\
a &\mapsto (a, \lambda c.\varepsilon) \\
\mu_A : TTA &\to TA \\
((a, o_1), o_2) &\mapsto (a, \lambda c.o_2(c) \bullet o_1(c))
\end{aligned}
$$

# Monad

*T is strong wrt products*

$$\begin{aligned} \tau_{A,B} : A \times TB &\quad\to\quad T(A \times B) \\ (a,(b,o)) &\quad\mapsto\quad ((a,b),o) \\ \sigma_{A,B} : TA \times B &\quad\to\quad T(A \times B) \\ ((a,o),b) &\quad\mapsto\quad ((a,b),o) \end{aligned}$$

$$\begin{aligned} \beta_{A,B} \quad &: \quad TA \times TB \to T(A \times B) \\ &:= \quad \tau_{TA,B} \,;\, T\sigma_{A,B} \,;\, \mu_{A\times B} \end{aligned}$$

# Comonad & Monad

**$\square$ *cancels* $T$**

$$\phi_A : \square T A \xrightarrow{\sim} \square A$$

# Outline

# Syntax

*Types*

$$A, B \quad ::= \quad \top \mid A \times B \mid A \Rightarrow B \mid \mathsf{str} \mid \mathsf{cap} \mid \Box A$$

*Terms*

$$\begin{aligned} e \quad ::= & \quad () \mid (e_1 \, , e_2) \mid \mathsf{fst}\, e \mid \mathsf{snd}\, e \mid x \mid \lambda x : A.\, e \mid e_1\, e_2 \\ \mid & \quad s \mid c \mid \boxed{e} \mid \mathsf{let}\ \boxed{x} = e_1 \ \mathsf{in}\ e_2 \mid \mathsf{print}(e_1, e_2) \end{aligned}$$

*Values*

$$v \quad ::= \quad x \mid () \mid (v_1 \, , v_2) \mid \lambda x : A.\, e \mid s \mid c \mid \boxed{e}$$

# Syntax

*Qualifiers*

$$q, r \quad ::= \quad \circ \mid \bullet$$

*Contexts*

$$\Gamma, \Delta, \Psi \quad ::= \quad \cdot \mid \Gamma, x : A^q$$

*Substitutions*

$$\theta, \phi \quad ::= \quad \langle\rangle \mid \langle \theta, e^q / x \rangle$$

# Syntax

*Judgments*

$$\mathcal{J} \quad ::= \quad x : A^q \in \Gamma \mid \Gamma \supseteq \Delta \mid \Gamma \vdash \theta : \Delta$$
$$\mid \quad \Gamma \vdash e : A \mid \Gamma \vdash^{\circ} e : A$$

$$(\cdot)^{\bigcirc} \quad := \quad \cdot$$
$$(\Gamma, x : A^{\bigcirc})^{\bigcirc} \quad := \quad \Gamma^{\bigcirc}, x : A^{\bigcirc}$$
$$(\Gamma, x : A^{\bullet})^{\bigcirc} \quad := \quad \Gamma^{\bigcirc}$$

$$\langle\rangle^{\bigcirc} \quad := \quad \langle\rangle$$
$$\langle\theta, e^{\bigcirc}/x\rangle^{\bigcirc} \quad := \quad \langle\theta^{\bigcirc}, e^{\bigcirc}/x\rangle$$
$$\langle\theta, e^{\bullet}/x\rangle^{\bigcirc} \quad := \quad \theta^{\bigcirc}$$

# Typing rules

$$\frac{x : A^q \in \Gamma}{\Gamma \vdash x : A}\ \textsc{Var} \qquad \frac{\Gamma, x : A^{\bullet} \vdash e : B}{\Gamma \vdash \lambda x : A.\, e : A \Rightarrow B}\ \Rightarrow \mathrm{I}$$

$$\frac{\Gamma \vdash e_1 : A \Rightarrow B \qquad \Gamma \vdash e_2 : A}{\Gamma \vdash e_1\, e_2 : B}\ \Rightarrow \mathrm{E}$$

# Typing rules

$$\frac{\Gamma^{\circ} \vdash e : A}{\Gamma \vdash^{\circ} e : A}\ \textsc{ctx-}\circ \qquad \frac{\Gamma \vdash^{\circ} e : A}{\Gamma \vdash \boxed{e} : \Box A}\ \Box\,\mathrm{I}$$

$$\frac{\Gamma \vdash e_1 : \Box A \qquad \Gamma, x : A^{\circ} \vdash e_2 : B}{\Gamma \vdash \mathsf{let}\ \boxed{x} = e_1\ \mathsf{in}\ e_2 : B}\ \Box\,\mathrm{E}$$

# Typing rules

$$\frac{\Gamma \vdash e_1 : \mathsf{cap} \qquad \Gamma \vdash e_2 : \mathsf{str}}{\Gamma \vdash \mathsf{print}(e_1, e_2) : \top}\ \textsc{Print}$$

# Substitution rules

$$\frac{}{\Gamma \vdash \langle\rangle : \cdot}\ \textsc{sub-id}$$

$$\frac{\Gamma \vdash \theta : \Delta \qquad \Gamma \vdash^{\circ} e : A}{\Gamma \vdash \langle \theta, e^{\bigcirc}/x \rangle : \Delta, x : A^{\bigcirc}}\ \textsc{sub-}\bigcirc$$

$$\frac{\Gamma \vdash \theta : \Delta \qquad \Gamma \vdash v : A}{\Gamma \vdash \langle \theta, v^{\bullet}/x \rangle : \Delta, x : A^{\bullet}}\ \textsc{sub-}\bullet$$

# Outline

# Types

$[\![A]\!] : \mathcal{U}$

$$
\begin{aligned}
[\![\top]\!] &:= 1 \\
[\![A \times B]\!] &:= [\![A]\!] \times [\![B]\!] \\
[\![A \Rightarrow B]\!] &:= [\![A]\!] \to T[\![B]\!] \\
[\![\mathsf{str}]\!] &:= \Sigma^* \\
[\![\mathsf{cap}]\!] &:= \mathcal{C} \\
[\![\Box A]\!] &:= \Box[\![A]\!]
\end{aligned}
$$

# Contexts

$[\![\Gamma]\!] : \mathcal{W}$

$$
\begin{aligned}
[\![\cdot]\!] &:= 1 \\
[\![\Gamma, x : A^{\circ}]\!] &:= [\![\Gamma]\!] \times \square [\![A]\!] \\
[\![\Gamma, x : A^{\bullet}]\!] &:= [\![\Gamma]\!] \times [\![A]\!]
\end{aligned}
$$

$[\![x : A^q \in \Gamma]\!] : [\![\Gamma]\!] \to [\![A]\!]$

$$
\left[\!\!\left[ \frac{}{x : A^{\bullet} \in (\Gamma, x : A^{\bullet})} \right]\!\!\right] := \pi_2
$$

$$
\left[\!\!\left[ \frac{}{x : A^{\circ} \in (\Gamma, x : A^{\circ})} \right]\!\!\right] := \pi_2 \mathbin{;} \varepsilon_A
$$

$$
\left[\!\!\left[ \frac{x : A^q \in \Gamma \qquad (x \neq y)}{x : A^q \in (\Gamma, y : B^r)} \right]\!\!\right] := \pi_1 \mathbin{;} [\![x : A^q \in \Gamma]\!]
$$

# Combinators

$\mathsf{Wk}(\Gamma \supseteq \Delta) : [\![\Gamma]\!] \to [\![\Delta]\!]$

$$
\begin{array}{rcl}
\mathsf{Wk}(\cdot \supseteq \cdot) & := & id_1 \\
\mathsf{Wk}(\Gamma, x : A^q \supseteq \Delta) & := & \pi_1 \mathbin{;} \mathsf{Wk}(\Gamma \supseteq \Delta) \\
\mathsf{Wk}(\Gamma, x : A^{\circ} \supseteq \Delta, x : A^{\circ}) & := & [\mathsf{Wk}(\Gamma \supseteq \Delta) \times id_{\Box A}] \\
\mathsf{Wk}(\Gamma, x : A^{\bullet} \supseteq \Delta, x : A^{\bullet}) & := & [\mathsf{Wk}(\Gamma \supseteq \Delta) \times id_{A}]
\end{array}
$$

# Combinators

$$\rho(\Gamma) : [\![\Gamma]\!] \to [\![\Gamma^{\circ}]\!]$$

$$\begin{aligned} \rho(\cdot) &:= id_1 \\ \rho(\Gamma, x : A^{\circ}) &:= [\rho(\Gamma) \times id_{\Box A}] \\ \rho(\Gamma, x : A^{\bullet}) &:= \pi_1 \mathbin{;} \rho(\Gamma) \end{aligned}$$

$$\mathcal{M}(\Gamma) : [\![\Gamma^{\circ}]\!] \xrightarrow{\sim} \Box[\![\Gamma^{\circ}]\!]$$

$$\begin{aligned} \mathcal{M}(\cdot) &:= id_1 \\ \mathcal{M}(\Gamma, x : A^{\circ}) &:= [\mathcal{M}(\Gamma) \times \delta_A] \mathbin{;} m^{\times}_{\Gamma^{\circ}, \Box A} \\ \mathcal{M}(\Gamma, x : A^{\bullet}) &:= \mathcal{M}(\Gamma) \end{aligned}$$

# Expressions

$$[\![\Gamma \vdash e : A]\!] : [\![\Gamma]\!] \to T[\![A]\!]$$

$$\left[\!\!\left[ \frac{x : A^q \in \Gamma}{\Gamma \vdash x : A} \right]\!\!\right] := [\![x : A^q \in \Gamma]\!] \,;\, \eta_A$$

$$\left[\!\!\left[ \frac{\Gamma, x : A^{\bullet} \vdash e : B}{\Gamma \vdash \lambda x : A.\, e : A \Rightarrow B} \right]\!\!\right] := \mathsf{curry}\left([\![\Gamma, x : A^{\bullet} \vdash e : B]\!]\right) ; \eta_{A \to TB}$$

---

$$\left[\!\!\left[ \frac{\Gamma \vdash e_1 : A \Rightarrow B \qquad \Gamma \vdash e_2 : A}{\Gamma \vdash e_1\, e_2 : B} \right]\!\!\right]$$

$$:= \quad let \begin{cases} f & := [\![\Gamma \vdash e_1 : A \Rightarrow B]\!] \\ g & := [\![\Gamma \vdash e_2 : A]\!] \end{cases}$$

$$in \quad \langle f, g \rangle \,;\, \beta_{A \to TB, A} \,;\, T\,\mathsf{ev}_{A, TB} \,;\, \mu_B$$

# Expressions

$$[\![\Gamma \vdash e : A]\!] : [\![\Gamma]\!] \to T[\![A]\!]$$

$$\left[\!\!\left[ \frac{\Gamma \vdash^\circ e : A}{\Gamma \vdash \boxed{e} : \Box A} \right]\!\!\right] \quad := \quad [\![\Gamma \vdash^\circ e : A]\!]_p \,;\, \eta_{\Box A}$$

$$[\![\Gamma \vdash^\circ e : A]\!]_p : [\![\Gamma]\!] \to \Box[\![A]\!]$$

$$\left[\!\!\left[ \frac{\Gamma^{\bigcirc} \vdash e : A}{\Gamma \vdash^\circ e : A} \right]\!\!\right]_p \quad := \quad \rho(\Gamma) \,;\, \mathcal{M}(\Gamma) \,;\, \Box[\![\Gamma^{\bigcirc} \vdash e : A]\!] \,;\, \phi_A$$

$$\Gamma \xrightarrow{\rho(\Gamma)} \Gamma^{\bigcirc} \xrightarrow{\mathcal{M}(\Gamma)} \Box\Gamma^{\bigcirc} \xrightarrow{\Box[\![\Gamma^{\bigcirc} \vdash e:A]\!]} \Box TA \xrightarrow{\phi_A} \Box A$$

# Expressions

$$[\![\Gamma \vdash e : A]\!] : [\![\Gamma]\!] \to T[\![A]\!]$$

$$\left[\!\!\left[ \frac{\Gamma \vdash e_1 : \Box A \qquad \Gamma, x : A^{\circ} \vdash e_2 : B}{\Gamma \vdash \mathsf{let}\ \boxed{x} = e_1\ \mathsf{in}\ e_2 : B} \right]\!\!\right]$$

$$:= \quad \begin{array}{ll} let & \begin{cases} f := [\![\Gamma \vdash e_1 : \Box A]\!] \\ g := [\![\Gamma, x : A^{\circ} \vdash e_2 : B]\!] \end{cases} \\ in & \langle id_\Gamma , f \rangle \mathbin{;} \tau_{\Gamma,\Box A} \mathbin{;} Tg \mathbin{;} \mu_B \end{array}$$

$$\Gamma \xrightarrow{\langle id_\Gamma, f\rangle} \Gamma \times T\Box A \xrightarrow{\tau_{\Gamma,\Box A}} T(\Gamma \times \Box A) \xrightarrow{Tg} T^2 B \xrightarrow{\mu_B} TB$$

# Expressions

$$[\![\Gamma \vdash e : A]\!] : [\![\Gamma]\!] \to T[\![A]\!]$$

$$\left[\!\!\left[ \frac{\Gamma \vdash e_1 : \mathsf{cap} \qquad \Gamma \vdash e_2 : \mathsf{str}}{\Gamma \vdash \mathsf{print}(e_1, e_2) : \top} \right]\!\!\right]$$

$$:= \quad \mathit{let} \left\{ \begin{array}{rcl} f & := & [\![\Gamma \vdash e_1 : \mathsf{cap}]\!] \\ g & := & [\![\Gamma \vdash e_2 : \mathsf{str}]\!] \\ p & : & \mathbb{C} \times \Sigma^* \to T1 \\ (c, s) & \mapsto & \left( 1 \,,\, \lambda c'. \begin{cases} s & \text{if } c = c' \\ \varepsilon & \text{otherwise} \end{cases} \right) \end{array} \right.$$

$$\mathit{in} \quad \langle f \,, g \rangle \,;\, \beta_{\mathbb{C}, \Sigma^*} \,;\, Tp \,;\, \mu_1$$

# Values

$$[\![\Gamma \vdash v : A]\!]_v : [\![\Gamma]\!] \to [\![A]\!]$$

$$[\![\frac{}{\Gamma \vdash () : \top}]\!]_v := !_\Gamma$$

$$[\![\frac{\Gamma \vdash v_1 : A \qquad \Gamma \vdash v_2 : B}{\Gamma \vdash (v_1, v_2) : A \times B}]\!]_v := \langle [\![\Gamma \vdash v_1 : A]\!]_v , [\![\Gamma \vdash v_2 : B]\!]_v \rangle$$

$$[\![\frac{x : A^q \in \Gamma}{\Gamma \vdash x : A}]\!]_v := [\![x : A^q \in \Gamma]\!]$$

$$[\![\frac{\Gamma, x : A^\bullet \vdash e : B}{\Gamma \vdash \lambda x : A.e : A \Rightarrow B}]\!]_v := \mathsf{curry}\left([\![\Gamma, x : A^\bullet \vdash e : B]\!]\right)$$

$$[\![\frac{\Gamma \vdash^\circ e : A}{\Gamma \vdash \boxed{e} : \Box A}]\!]_v := [\![\Gamma \vdash^\circ e : A]\!]_p$$

# Substitutions

$$[\![\Gamma \vdash \theta : \Delta]\!] : [\![\Gamma]\!] \to [\![\Delta]\!]$$

$$[\![ \frac{}{\Gamma \vdash \langle\rangle : \cdot} ]\!] \quad := \quad !_\Gamma$$

$$[\![ \frac{\Gamma \vdash \theta : \Delta \qquad \Gamma \vdash^\circ e : A}{\Gamma \vdash \langle \theta, e^{\bigcirc}/x \rangle : \Delta, x : A^{\bigcirc}} ]\!] \quad := \quad \langle [\![\Gamma \vdash \theta : \Delta]\!], [\![\Gamma \vdash^\circ e : A]\!]_p \rangle$$

$$[\![ \frac{\Gamma \vdash \theta : \Delta \qquad \Gamma \vdash v : A}{\Gamma \vdash \langle \theta, v^{\bullet}/x \rangle : \Delta, x : A^{\bullet}} ]\!] \quad := \quad \langle [\![\Gamma \vdash \theta : \Delta]\!], [\![\Gamma \vdash v : A]\!]_v \rangle$$

# Outline

# Syntactic substitution

**$\theta(e)$**

$$
\begin{array}{rcl}
\theta(x) & := & \theta[x] \\
\theta(\lambda x.\, e) & := & \lambda y.\, \langle \theta, y^{\bullet}/x \rangle(e) \\
\theta(e_1\, e_2) & := & \theta(e_1)\, \theta(e_2) \\
\theta(\boxed{e}) & := & \boxed{\theta^{\circ}(e)} \\
\theta(\mathsf{let}\ \boxed{x} = e_1\ \mathsf{in}\ e_2) & := & \mathsf{let}\ \boxed{y} = \theta(e_1)\ \mathsf{in}\ \langle \theta, y^{\circ}/x \rangle(e_2) \\
\theta(\mathsf{print}(e_1, e_2)) & := & \mathsf{print}(\theta(e_1), \theta(e_2))
\end{array}
$$

**$\theta[x]$**

$$
\theta[x] \quad := \quad \begin{cases} \lightning & \theta = \langle\rangle \\ e & \theta = \langle \phi, e^{q}/x \rangle \\ \phi[x] & \theta = \langle \phi, e^{q}/y \rangle, x \neq y \end{cases}
$$

# Soundness of syntactic substitution

*Weakening lemma*

1. If $\Gamma \supseteq \Delta$ and $\Delta \vdash e : A$, then $\Gamma \vdash e : A$.
2. If $\Gamma \supseteq \Delta$ and $\Delta \vdash \theta : \Psi$, then $\Gamma \vdash \theta : \Psi$.

*Substitution theorem*

If $\Gamma \vdash \theta : \Delta$ and $\Delta \vdash e : A$, then $\Gamma \vdash \theta(e) : A$.

# Soundness of semantic substitution

*Weakening lemma*

1. If $\Gamma \supseteq \Delta$ and $\Delta \vdash e : A$, then

$$[\![\Gamma \vdash e : A]\!] = \mathsf{Wk}(\Gamma \supseteq \Delta) \,;\, [\![\Delta \vdash e : A]\!].$$

2. If $\Gamma \supseteq \Delta$ and $\Delta \vdash e : A$, then

$$[\![\Gamma \vdash \theta : \Psi]\!] = \mathsf{Wk}(\Gamma \supseteq \Delta) \,;\, [\![\Delta \vdash \theta : \Psi]\!].$$

# Soundness of semantic substitution

*Pure lemma*

If $\Gamma \vdash^\circ e : A$, then

$$[\![\Gamma \vdash e : A]\!] = [\![\Gamma \vdash^\circ e : A]\!]_p \,;\, \varepsilon_A \,;\, \eta_A.$$

*Value lemma*

If $\Gamma \vdash v : A$, then

$$[\![\Gamma \vdash v : A]\!] = [\![\Gamma \vdash v : A]\!]_v \,;\, \eta_A.$$

*Substitution theorem*

If $\Gamma \vdash \theta : \Delta$ and $\Delta \vdash e : A$, then

$$[\![\Gamma \vdash \theta(e) : A]\!] = [\![\Gamma \vdash \theta : \Delta]\!] \,;\, [\![\Delta \vdash e : A]\!].$$

# Outline

# Equational Theory

$$\frac{\Gamma, x : A^{\bullet} \vdash e_1 \approx e_2 : B}{\Gamma \vdash \lambda x.\, e_1 \approx \lambda x.\, e_2 : A \Rightarrow B} \; \lambda\text{-CONG}$$

$$\frac{\Gamma \vdash e_1 \approx e_2 : A \Rightarrow B \qquad \Gamma \vdash e_3 \approx e_4 : A}{\Gamma \vdash e_1\, e_3 \approx e_2\, e_4 : B} \; \text{APP-CONG}$$

$$\frac{\Gamma^{\circ} \vdash e_1 \approx e_2 : A}{\Gamma \vdash \boxed{e_1} \approx \boxed{e_2} : \Box A} \; \Box\text{-CONG}$$

$$\frac{\Gamma \vdash e_1 \approx e_2 : \Box A \qquad \Gamma, x : A^{\circ} \vdash e_3 \approx e_4 : B}{\Gamma \vdash (\mathsf{let}\ \boxed{x} = e_1\ \mathsf{in}\ e_3) \approx (\mathsf{let}\ \boxed{x} = e_2\ \mathsf{in}\ e_4) : B} \; \mathsf{let}\ \Box\text{-CONG}$$

# Equational Theory

$$\frac{\Gamma, x : A^{\bullet} \vdash e : B \qquad \Gamma \vdash v : A}{\Gamma \vdash (\lambda x.\, e)\, v \approx [v/x]e : B} \Rightarrow \beta$$

$$\frac{\Gamma \vdash^{\circ} e : A \Rightarrow B}{\Gamma \vdash e \approx \lambda x.\, e\, x : A \Rightarrow B} \Rightarrow \eta\text{-}\circ \qquad \frac{\Gamma \vdash v : A \Rightarrow B}{\Gamma \vdash v \approx \lambda x.\, v\, x : A \Rightarrow B} \Rightarrow \eta\text{-}\bullet$$

$$\frac{\Gamma^{\circ} \vdash e_1 : A \qquad \Gamma, x : A^{\circ} \vdash e_2 : B}{\Gamma \vdash \text{let } \boxed{x} = \boxed{e_1} \text{ in } e_2 \approx [e_1/x]e_2 : B} \;\square\; \beta$$

# Equational Theory

*Evaluation Contexts*

$$
\begin{array}{lcl}
\mathcal{C} & ::= & [\cdot] \mid e\,\mathcal{C} \mid \mathcal{C}\,e \mid \lambda x : A.\,\mathcal{C} \\
 & \mid & \boxed{\mathcal{C}} \mid \mathsf{let}\ \boxed{x} = \mathcal{C}\ \mathsf{in}\ e \mid \mathsf{let}\ \boxed{x} = e\ \mathsf{in}\ \mathcal{C} \\
\mathcal{E} & ::= & [\cdot] \mid e\,\mathcal{E} \mid \mathcal{E}\,v \\
 & \mid & \mathsf{let}\ \boxed{x} = \mathcal{E}\ \mathsf{in}\ e \mid \mathsf{let}\ \boxed{x} = v\ \mathsf{in}\ \mathcal{E}
\end{array}
$$

$$
\frac{\Gamma \vdash^{\circ} e : \Box A \qquad \Gamma \vdash \mathcal{C}\langle\!\langle e \rangle\!\rangle : B \qquad \Gamma \vdash \mathsf{let}\ \boxed{x} = e\ \mathsf{in}\ \mathcal{C}\langle\!\langle \boxed{x} \rangle\!\rangle : B}{\Gamma \vdash \mathcal{C}\langle\!\langle e \rangle\!\rangle \approx \mathsf{let}\ \boxed{x} = e\ \mathsf{in}\ \mathcal{C}\langle\!\langle \boxed{x} \rangle\!\rangle : B}\ \Box\ \eta\text{-}\circ
$$

$$
\frac{\Gamma \vdash e : \Box A \qquad \Gamma \vdash \mathcal{E}\langle\!\langle e \rangle\!\rangle : B \qquad \Gamma \vdash \mathsf{let}\ \boxed{x} = e\ \mathsf{in}\ \mathcal{E}\langle\!\langle \boxed{x} \rangle\!\rangle : B}{\Gamma \vdash \mathcal{E}\langle\!\langle e \rangle\!\rangle \approx \mathsf{let}\ \boxed{x} = e\ \mathsf{in}\ \mathcal{E}\langle\!\langle \boxed{x} \rangle\!\rangle : B}\ \Box\ \eta\text{-}\bullet
$$

# Soundness

*Soundness theorem*

If $\Gamma \vdash e_1 \approx e_2 : A$, then $[\![\Gamma \vdash e_1 : A]\!] = [\![\Gamma \vdash e_2 : A]\!]$.

# Embedding

| | | | |
|---|---|---|---|
| Types | $\underline{b}$ | $:=$ | $b$ |
| | $\underline{A \Rightarrow B}$ | $:=$ | $\square\, \underline{A} \Rightarrow \underline{B}$ |
| Contexts | $\underline{\cdot}$ | $:=$ | $\cdot$ |
| | $\underline{\Gamma, x : A}$ | $:=$ | $\underline{\Gamma}, x : \underline{A}^{\circ}$ |
| Terms | $\underline{x}$ | $:=$ | $x$ |
| | $\underline{\lambda x : A.\, e}$ | $:=$ | $\lambda z : \square\, \underline{A}.\ \mathsf{let}\ \boxed{x} = z\ \mathsf{in}\ \underline{e}$ |
| | $\underline{e_1\, e_2}$ | $:=$ | $\underline{e_1}\ \boxed{\underline{e_2}}$ |

# Soundness

*Type preserving*

If $\Gamma \vdash_\lambda e : A$, then $\Gamma \vdash e : A$.

*Equality preserving*

If $\Gamma \vdash_\lambda e_1 \approx e_2 : A$, then $\Gamma \vdash e_1 \approx e_2 : A$.

*Conservative extension*

If $\Gamma \vdash_\lambda e_1 : A$ and $\Gamma \vdash_\lambda e_1 : A$ and $\Gamma \vdash e_1 \approx e_2 : A$,
then $\Gamma \vdash_\lambda e_1 \approx e_2 : A$.

# Outline

# Epilogue

- We gave the syntax & semantics of an effectful lambda calculus.
- We use a comonadic modality to filter out effects.
- The language is *good*.
- One could extend the comonad to a graded comonad indexed by capabilities.
- The category has more structure, and we could add fancier types.
- Questions?