Capabilities: Effects for Free (Supplementary Material with Proofs)

ANONYMOUS AUTHOR(S)

ACM Reference format:
Anonymous Author(s). 2017. Capabilities: Effects for Free (Supplementary Material with Proofs). *PACM Progr. Lang.* 1, 1, Article 1 (January 2017), 7 pages.
DOI: 10.1145/nnnnnnn.nnnnnnn

1 OC PROOFS

Lemma 1.1 (OC Canonical Forms). *Unless the rule used is ε-Subsume, the following are true:*

1. *If* $\Gamma \vdash x : \tau$ with ε *then* $\varepsilon = \varnothing$.
2. *If* $\Gamma \vdash v : \tau$ with ε *then* $\varepsilon = \varnothing$.
3. *If* $\Gamma \vdash v : \{\bar{r}\}$ with ε *then* $v = r$ *and* $\{\bar{r}\} = \{r\}$.
4. *If* $\Gamma \vdash v : \tau_1 \rightarrow_{\varepsilon'} \tau_2$ with ε *then* $v = \lambda x : \tau.e$.

Proof.

1. The only rule that applies to variables is ε-Var which ascribes the type $\varnothing$.
2. By definition a value is either a resource literal or a lambda. The only rules which can type values are ε-Resource and ε-Abs. In the conclusions of both, $\varepsilon = \varnothing$.
3. The only rule ascribing the type $\{\bar{r}\}$ is ε-Resource. Its premises imply the result.
4. The only rule ascribing the type $\tau_1 \rightarrow_{\varepsilon'} \tau_2$ is ε-Abs. Its premises imply the result.

□

Theorem 1.2 (OC Progress). *If $\Gamma \vdash e : \tau$ with ε and e is not a value or variable, then $e \longrightarrow e' \mid \varepsilon$, for some e', ε.*

Proof. By induction on $\Gamma \vdash e : \tau$ with ε.

Case: ε-Var, ε-Resource, or ε-Abs. Then e is a value or variable and the theorem statement holds vacuously.

Case: ε-App. Then $e = e_1\ e_2$. If e_1 is not a value or variable it can be reduced $e_1 \longrightarrow e_1' \mid \varepsilon$ by inductive assumption, so $e_1\ e_2 \longrightarrow e_1'\ e_2 \mid \varepsilon$ by E-App1. If $e_1 = v_1$ is a value and e_2 a non-value, then e_2 can be reduced $e_2 \longrightarrow e_2' \mid \varepsilon$ by inductive assumption, so $e_1\ e_2 \longrightarrow v_1\ e_2' \mid \varepsilon$ by E-App2. Otherwise $e_1 = v_1$ and $e_2 = v_2$ are both values. By inversion on ε-App and canonical forms, $\Gamma \vdash v_1 : \tau_2 \rightarrow_{\varepsilon'} \tau_3$ with $\varnothing$, and $v_1 = \lambda x : \tau_2.e_{body}$. Then $(\lambda x : \tau.e_{body})v_2 \longrightarrow [v_2/x]e_{body} \mid \varnothing$ by E-App3.

Case: ε-OperCall. Then $e = e_1.\pi$. If e_1 is a non-value it can be reduced $e_1 \longrightarrow e_1' \mid \varepsilon$ by inductive assumption, so $e_1.\pi \longrightarrow e_1'.\pi \mid \varepsilon$ by E-OperCall1. Otherwise $e_1 = v_1$ is a value. By inversion on ε-OperCall and canonical forms, $\Gamma \vdash v_1 : \{r\}$ with $\{r.\pi\}$, and $v_1 = r$. Then $r.\pi \longrightarrow$ unit $\mid \{r.\pi\}$ by

2017. 2475-1421/2017/1-ART1 $15.00
DOI: 10.1145/nnnnnnn.nnnnnnn

E-OperCall2.

Case: ε-Subsume. If e is a value or variable, the theorem holds vacuously. Otherwise by inversion on ε-Subsume, $\Gamma \vdash e : \tau' \texttt{ with } \varepsilon'$, and $e \longrightarrow e' \mid \varepsilon$ by inductive assumption.

□

Lemma 1.3 (OC Substitution). *If* $\Gamma, x : \tau' \vdash e : \tau \texttt{ with } \varepsilon$ *and* $\Gamma \vdash v : \tau' \texttt{ with } \varnothing$ *then* $\Gamma \vdash [v/x]e : \tau \texttt{ with } \varepsilon$.

Proof. By induction on the derivation of $\Gamma, x : \tau' \vdash e : \tau \texttt{ with } \varepsilon$.

Case: ε-Var. Then $e = y$ is a variable. Either $y = x$ or $y \neq x$. Suppose $y = x$. By applying canonical Forms to the theorem assumption $\Gamma, x : \tau' \vdash e : \tau' \texttt{ with } \varnothing$, hence $\tau' = \tau$. $[v/x]y = [v/x]x = v$, and by assumption, $\Gamma \vdash v : \tau' \texttt{ with } \varnothing$, so $\Gamma \vdash [v/x]y : \tau \texttt{ with } \varnothing$.

Otherwise $y \neq x$. By applying canonical forms to the theorem assumption $\Gamma, x : \tau' \vdash y : \tau \texttt{ with } \varnothing$, so $y : \tau \in \Gamma$. Since $[v/x]y = y$, then $\Gamma \vdash y : \tau \texttt{ with } \varnothing$ by ε-Var.

Case: ε-Resource. Because $e = r$ is a resource literal then $\Gamma \vdash r : \{r\} \texttt{ with } \varnothing$ by canonical forms. By definition $[v/x]r = r$, so $\Gamma \vdash [v/x]r : \{\bar{r}\} \texttt{ with } \varnothing$.

Case: ε-App. By inversion $\Gamma, x : \tau' \vdash e_1 : \tau_2 \rightarrow_{\varepsilon_3} \tau_3 \texttt{ with } \varepsilon_A$ and $\Gamma, x : \tau' \vdash e_2 : \tau_2 \texttt{ with } \varepsilon_B$, where $\varepsilon = \varepsilon_A \cup \varepsilon_B \cup \varepsilon_3$ and $\tau = \tau_3$. From inversion on ε-App and inductive assumption, $\Gamma \vdash [v/x]e_1 : \tau_2 \rightarrow_{\varepsilon_3} \tau_3 \texttt{ with } \varepsilon_A$ and $\Gamma \vdash [v/x]e_2 : \tau_2 \texttt{ with } \varepsilon_B$. By ε-App $\Gamma \vdash ([v/x]e_1)([v/x]e_2) : \tau_3 \texttt{ with } \varepsilon_A \cup \varepsilon_B \cup \varepsilon_3$. By simplifying and applying the definition of `substitution`, this is the same as $\Gamma \vdash [v/x](e_1\ e_2) : \tau \texttt{ with } \varepsilon$.

Case: ε-OperCall. By inversion $\Gamma, x : \tau' \vdash e_1 : \{\bar{r}\} \texttt{ with } \varepsilon_1$ and $\tau = \texttt{Unit}$ and $\varepsilon = \varepsilon_1 \cup \{r.\pi \mid r \in \bar{r}, \pi \in \Pi\}$. By inductive assumption, $\Gamma \vdash [v/x]e_1 : \{\bar{r}\} \texttt{ with } \varepsilon_1$. Then by ε-OperCall, $\Gamma \vdash ([v/x]e_1).\pi : \texttt{Unit with } \varepsilon_1 \cup \{r.\pi \mid r.\pi \in \bar{r} \times \Pi\}$. By simplifying and applying the definition of `substitution`, this is the same as $\Gamma \vdash [v/x](e_1.\pi) : \tau \texttt{ with } \varepsilon$.

Case: ε-Subsume. By inversion, $\Gamma, x : \tau' \vdash e : \tau_2 \texttt{ with } \varepsilon_2$, where $\tau_2 <: \tau$ and $\varepsilon_2 \subseteq \varepsilon$. By inductive hypothesis, $\Gamma \vdash [v/x]e : \tau_2 \texttt{ with } \varepsilon_2$. Then $\Gamma \vdash [v/x]e : \tau \texttt{ with } \varepsilon$ by ε-Subsume.

□

Theorem 1.4 (OC Preservation). *If* $\Gamma \vdash e_A : \tau_A \texttt{ with } \varepsilon_A$ *and* $e_A \longrightarrow e_B \mid \varepsilon$, *then* $\tau_B <: \tau_A$ *and* $\varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$, *for some* $e_B, \varepsilon, \tau_B, \varepsilon_B$.

Proof. By induction on the derivation of $\Gamma \vdash e_A : \tau_A \texttt{ with } \varepsilon_A$ and then the derivation of $e_A \longrightarrow e_B \mid \varepsilon$.

Case: ε-Var, ε-Resource, ε-Unit, ε-Abs. Then e_A is a value and cannot be reduced, so the theorem holds vacuously.

Case: ε-App. Then $e_A = e_1\ e_2$ and $\Gamma \vdash e_1 : \tau_2 \longrightarrow_{\varepsilon_3} \tau_3 \texttt{ with } \varepsilon_1$ and $\Gamma \vdash e_2 : \tau_2 \texttt{ with } \varepsilon_2$ and $\tau_B = \tau_3$ and $\varepsilon_A = \varepsilon_1 \cup \varepsilon_2 \cup \varepsilon_3$. In each case we choose $\tau_B = \tau_A$ and $\varepsilon_B \cup \varepsilon = \varepsilon_A$.

Subcase: E-App1. Then $e_1\ e_2 \longrightarrow e_1'\ e_2 \mid \varepsilon$. By inversion on E-App1, $e_1 \longrightarrow e_1' \mid \varepsilon$. By inductive hypothesis and ε-Subsume $\Gamma \vdash v_1 : \tau_2 \longrightarrow_{\varepsilon_3} \tau_3$ with ε_1. Then $\Gamma \vdash e_1'\ e_2 : \tau_3$ with $\varepsilon_1 \cup \varepsilon_2 \cup \varepsilon_3$ by ε-App.

Subcase: E-App2. Then $e_1 = v_1$ is a value and $e_2 \longrightarrow e_2' \mid \varepsilon$. By inversion on E-App2, $e_2 \longrightarrow e_2' \mid \varepsilon$. By inductive hypothesis and ε-Subsume $\Gamma \vdash e_2' : \tau_2$ with ε_2. Then $\Gamma \vdash v_1\ e_2' : \tau_3$ with $\varepsilon_1 \cup \varepsilon_2 \cup \varepsilon_3$ by ε-App.

Subcase: E-App3. Then $e_1 = \lambda x : \tau_2.e_{body}$ and $e_2 = v_2$ are values and $(\lambda x : \tau_2.e_{body})\ v_2 \longrightarrow [v_2/x]e_{body} \mid \varnothing$. By inversion on the rule ε-App used to type $\lambda x : \tau_2.e_{body}$, we know $\Gamma, x : \tau_2 \vdash e_{body} : \tau_3$ with ε_3. $e_1 = v_1$ and $e_2 = v_2$ are values, so $\varepsilon_1 = \varepsilon_2 = \varnothing$ by canonical forms . Then by the substitution lemma, $\Gamma \vdash [v_2/x]e_{body} : \tau_3$ with ε_3 and $\varepsilon_A = \varepsilon_B = \varepsilon$.

Case: ε-OperCall. Then $e_A = e_1.\pi$ and $\Gamma \vdash e_1 : \{\bar{r}\}$ with ε_1 and $\tau_A =$ Unit and $\varepsilon_A = \varepsilon_1 \cup \{r.\pi \mid r \in \bar{r}, \pi \in \Pi\}$.

Subcase: E-OperCall1. Then $e_1.\pi \longrightarrow e_1'.\pi \mid \varepsilon$. By inversion on E-OperCall1, $e_1 \longrightarrow e_1' \mid \varepsilon$. By inductive hypothesis and application of ε-Subsume, $\Gamma \vdash e_1' : \{\bar{r}\}$ with ε_1. Then $\Gamma \vdash e_1'.\pi : \{\bar{r}\}$ with $\varepsilon_1 \cup \{r.\pi \mid r \in \bar{r}, \pi \in \Pi\}$ by ε-OperCall.

Subcase: E-OperCall2. Then $e_1 = r$ is a resource literal and $r.\pi \longrightarrow$ unit $\mid \{r.\pi\}$. By canonical forms, $\varepsilon_1 = \varnothing$. By ε-Unit, $\Gamma \vdash$ unit : Unit with $\varnothing$. Therefore $\tau_B = \tau_A$ and $\varepsilon \cup \varepsilon_B = \{r.\pi\} = \varepsilon_A$. □

Theorem 1.5 (OC Single-step Soundness). *If $\Gamma \vdash e_A : \tau_A$ with ε_A and e_A is not a value, then $e_A \longrightarrow e_B \mid \varepsilon$, where $\Gamma \vdash e_B : \tau_B$ with ε_B and $\tau_B <: \tau_A$ and $\varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$, for some $e_B, \varepsilon, \tau_B, \varepsilon_B$.*

Proof. If e_A is not a value then the reduction exists by the progress theorem. The rest follows by the preservation theorem. □

Theorem 1.6 (OC Multi-step Soundness). *If $\Gamma \vdash e_A : \tau_A$ with ε_A and $e_A \longrightarrow^* e_B \mid \varepsilon$, where $\Gamma \vdash e_B : \tau_B$ with ε_B and $\tau_B <: \tau_A$ and $\varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$.*

Proof. By induction on the length of the multi-step reduction.

Case: Length 0. Then $e_A = e_B$ and $\tau_A = \tau_B$ and $\varepsilon = \varnothing$ and $\varepsilon_A = \varepsilon_B$.

Case: Length $n + 1$. By inversion the multi-step can be split into a multi-step of length n, which is $e_A \longrightarrow^* e_C \mid \varepsilon'$, and a single-step of length 1, which is $e_C \longrightarrow e_B \mid \varepsilon''$, where $\varepsilon = \varepsilon' \cup \varepsilon''$. By inductive assumption and preservation theorem, $\Gamma \vdash e_C : \tau_C$ with ε_C and $\Gamma \vdash e_B : \tau_B$ with ε_B, where $\tau_C <: \tau_A$ and $\varepsilon_C \cup \varepsilon' \subseteq \varepsilon_A$. By single-step soundness, $\tau_B <: \tau_C$ and $\varepsilon_B \cup \varepsilon'' \subseteq \varepsilon_C$. Then by transitivity, $\tau_B <: \tau$ and $\varepsilon_B \cup \varepsilon' \cup \varepsilon'' = \varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$. □

2 CC PROOFS

Lemma 2.1 (CC Canonical Forms). *Unless the rule used is ε-Subsume, the following are true:*

(1) *If $\hat{\Gamma} \vdash x : \hat{\tau}$ with ε then $\varepsilon = \varnothing$.*
(2) *If $\hat{\Gamma} \vdash \hat{v} : \hat{\tau}$ with ε then $\varepsilon = \varnothing$.*
(3) *If $\hat{\Gamma} \vdash \hat{v} : \{\bar{r}\}$ with ε then $\hat{v} = r$ and $\{\bar{r}\} = \{r\}$.*
(4) *If $\hat{\Gamma} \vdash \hat{v} : \hat{\tau}_1 \rightarrow_{\varepsilon'} \hat{\tau}_2$ with ε then $\hat{v} = \lambda x : \tau.\hat{e}$.*

Proof. Same as for OC. □

THEOREM 2.2 (CC PROGRESS). *If* $\hat{\Gamma} \vdash \hat{e} : \hat{\tau}$ $\texttt{with}$ ε *and* $\hat{e}$ *is not a value, then* $\hat{e} \longrightarrow \hat{e}' \mid \varepsilon$*, for some* $\hat{e}', \varepsilon$.

PROOF. By induction on the derivation of $\hat{\Gamma} \vdash \hat{e} : \hat{\tau}$ $\texttt{with}$ ε.

Case: ε-MODULE. Then $\hat{e} = \texttt{import}(\varepsilon_s)\ x = \hat{e}_i$ $\texttt{in}$ e. If $\hat{e}_i$ is a non-value then $\hat{e}_i \longrightarrow \hat{e}_i' \mid \varepsilon$ by inductive assumption and $\texttt{import}(\varepsilon_s)\ x = \hat{e}_i$ $\texttt{in}$ $e \longrightarrow \texttt{import}(\varepsilon_s)\ x = \hat{e}_i'$ $\texttt{in}$ $e \mid \varepsilon$ by E-MODULE1. Otherwise $\hat{e}_i = \hat{v}_i$ is a value and $\texttt{import}(\varepsilon_s)\ x = \hat{v}_i$ $\texttt{in}$ $e \longrightarrow [\hat{v}_i/x]\texttt{annot}(e, \varepsilon_s) \mid \varnothing$ by E-MODULE2. □

LEMMA 2.3 (CC SUBSTITUTION). *If* $\hat{\Gamma}, x : \hat{\tau}' \vdash \hat{e} : \hat{\tau}$ $\texttt{with}$ ε *and* $\hat{\Gamma} \vdash \hat{v} : \hat{\tau}'$ $\texttt{with}$ $\varnothing$ *then* $\hat{\Gamma} \vdash [\hat{v}/x]\hat{e}_A : \hat{\tau}$ $\texttt{with}$ ε.

PROOF. By induction on the derivation of $\hat{\Gamma}, x : \hat{\tau}' \vdash \hat{e} : \hat{\tau}$ $\texttt{with}$ ε.

Case: ε-MODULE. Then the following are true.

(1) $\hat{e} = \texttt{import}(\varepsilon_s)\ x = \hat{e}_i$ $\texttt{in}$ e
(2) $\hat{\Gamma}, y : \hat{\tau}' \vdash \hat{e}_i : \hat{\tau}_i$ $\texttt{with}$ ε_i
(3) $y : \texttt{erase}(\hat{\tau}_i) \vdash e : \tau$
(4) $\hat{\Gamma}, y : \hat{\tau}' \vdash \texttt{import}(\varepsilon_s)\ x = \hat{e}_i$ $\texttt{in}$ $e : \texttt{annot}(\tau, \varepsilon_s)$ $\texttt{with}$ $\varepsilon_s \cup \varepsilon_i$
(5) $\varepsilon_s = \texttt{effects}(\hat{\tau}_i) \cup \texttt{ho-effects}(\texttt{annot}(\tau, \varnothing))$
(6) $\hat{\tau}_A = \texttt{annot}(\tau, \varepsilon)$
(7) $\hat{\varepsilon}_A = \varepsilon_s \cup \varepsilon_i$

By applying inductive assumption to (2) $\hat{\Gamma} \vdash [\hat{v}/x]\hat{e}_i : \hat{\tau}_i$ $\texttt{with}$ ε_i. Then by ε-MODULE $\hat{\Gamma} \vdash \texttt{import}(\varepsilon_s)\ y = [\hat{v}/x]\hat{e}_i$ $\texttt{in}$ $e : \texttt{annot}(\tau_i, \varepsilon_s)$ $\texttt{with}$ $\varepsilon_s \cup \varepsilon_i$. By definition of $\texttt{substitution}$, the form in this judgement is the same as $[\hat{v}/x]\hat{e}$. □

LEMMA 2.4 (CC APPROXIMATION 1). *If* $\texttt{effects}(\hat{\tau}) \subseteq \varepsilon$ *and* $\texttt{ho-safe}(\hat{\tau}, \varepsilon)$ *then* $\hat{\tau} <: \texttt{annot}(\texttt{erase}(\hat{\tau}), \varepsilon)$.

LEMMA 2.5 (CC APPROXIMATION 2). *If* $\texttt{ho-effects}(\hat{\tau}) \subseteq \varepsilon$ *and* $\texttt{safe}(\hat{\tau}, \varepsilon)$ *then* $\texttt{annot}(\texttt{erase}(\hat{\tau}), \varepsilon) <: \hat{\tau}$.

PROOF. By simultaneous induction on derivations of $\texttt{safe}$ and $\texttt{ho-safe}$.

Case: $\hat{\tau} = \{\bar{r}\}$ Then $\hat{\tau} = \texttt{annot}(\texttt{erase}(\hat{\tau}), \varepsilon)$ and the results for both lemmas hold immediately.

Case: $\hat{\tau} = \hat{\tau}_1 \rightarrow_{\varepsilon'} \hat{\tau}_2, \texttt{effects}(\hat{\tau}) \subseteq \varepsilon, \texttt{ho-safe}(\hat{\tau}, \varepsilon)$ It is sufficient to show $\hat{\tau}_2 <: \texttt{annot}(\texttt{erase}(\hat{\tau}_2), \varepsilon)$ and $\texttt{annot}(\texttt{erase}(\hat{\tau}_1), \varepsilon) <: \hat{\tau}_1$, because the result will hold by S-EFFECTS. To achieve this we shall inductively apply lemma 1 to $\hat{\tau}_2$ and lemma 2 to $\hat{\tau}_1$.

From $\texttt{effects}(\hat{\tau}) \subseteq \varepsilon$ we have $\texttt{ho-effects}(\hat{\tau}_1) \cup \varepsilon' \cup \texttt{effects}(\hat{\tau}_2) \subseteq \varepsilon$ and therefore $\texttt{effects}(\hat{\tau}_2) \subseteq \varepsilon$. From $\texttt{ho-safe}(\hat{\tau}, \varepsilon)$ we have $\texttt{ho-safe}(\hat{\tau}_2, \varepsilon)$. Therefore we can apply lemma 1 to $\hat{\tau}_2$.

From $\texttt{effects}(\hat{\tau}) \subseteq \varepsilon$ we have $\texttt{ho-effects}(\hat{\tau}_1) \cup \varepsilon' \cup \texttt{effects}(\hat{\tau}_2) \subseteq \varepsilon$ and therefore $\texttt{ho-effects}(\hat{\tau}_1) \subseteq \varepsilon$. From $\texttt{ho-safe}(\hat{\tau}, \varepsilon)$ we have $\texttt{ho-safe}(\hat{\tau}_1, \varepsilon)$. Therefore we can apply lemma 2 to $\hat{\tau}_1$.

Case: $\hat{\tau} = \hat{\tau}_1 \rightarrow_{\varepsilon'} \hat{\tau}_2, \texttt{ho-effects}(\hat{\tau}) \subseteq \varepsilon, \texttt{safe}(\hat{\tau}, \varepsilon)$ It is sufficient to show $\texttt{annot}(\texttt{erase}(\hat{\tau}_2), \varepsilon) <: \hat{\tau}_2$ and $\hat{\tau}_1 <: \texttt{annot}(\texttt{erase}(\hat{\tau}_1), \varepsilon)$, because the result will hold by S-Effects. To achieve this we shall inductively apply lemma 2 to $\hat{\tau}_2$ and lemma 1 to $\hat{\tau}_1$.

From $\texttt{ho-effects}(\hat{\tau}) \subseteq \varepsilon$ we have $\texttt{effects}(\hat{\tau}_1) \cup \texttt{ho-effects}(\hat{\tau}_2) \subseteq \varepsilon$ and therefore $\texttt{ho-effects}(\hat{\tau}_2) \subseteq \varepsilon$. From $\texttt{safe}(\hat{\tau}, \varepsilon)$ we have $\texttt{safe}(\hat{\tau}_2, \varepsilon)$. Therefore we can apply lemma 2 to $\hat{\tau}_2$.

From $\texttt{ho-effects}(\hat{\tau}) \subseteq \varepsilon$ we have $\texttt{effects}(\hat{\tau}_1) \cup \texttt{ho-effects}(\hat{\tau}_2) \subseteq \varepsilon$ and therefore $\texttt{effects}(\hat{\tau}_1) \subseteq \varepsilon$. From $\texttt{safe}(\hat{\tau}, \varepsilon)$ we have $\texttt{ho-safe}(\hat{\tau}_1, \varepsilon)$. Therefore we can apply lemma 1 to $\hat{\tau}_1$.

□

Lemma 2.6 (CC Annotation). *If the following are true:*

(1) $\hat{\Gamma} \vdash \hat{v}_i : \hat{\tau}_i \texttt{ with } \varnothing$
(2) $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash e : \tau$
(3) $\texttt{effects}(\hat{\tau}_i) \cup \texttt{ho-effects}(\texttt{annot}(\tau, \varnothing)) \cup \texttt{effects}(\texttt{annot}(\Gamma, \varnothing)) \subseteq \varepsilon_s$
(4) $\texttt{ho-safe}(\hat{\tau}_i, \varepsilon_s)$

Then $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau}_i \vdash \texttt{annot}(e, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varepsilon_s$.

Proof. By induction on the derivation of $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash e : \tau$. When applying the inductive assumption, e, τ, and Γ may vary, but the other variables are fixed.

Case: T-Var. Then $e = x$ and $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash x : \tau$. Either $x = y$ or $x \neq y$.

Subcase 1: $x = y$. Then $y : \texttt{erase}(\hat{\tau}_i) \vdash y : \tau$ so $\tau = \texttt{erase}(\hat{\tau}_i)$. By ε-Var, $y : \hat{\tau}_i \vdash x : \hat{\tau}_i \texttt{ with } \varnothing$. By definition $\texttt{annot}(x, \varepsilon_s) = x$, so (5) $y : \hat{\tau}_i \vdash \texttt{annot}(x, \varepsilon_s) : \hat{\tau}_i \texttt{ with } \varnothing$. By (3) and (4) we know $\texttt{effects}(\hat{\tau}_i) \subseteq \varepsilon_s$ and $\texttt{ho-safe}(\hat{\tau}_i, \varepsilon_s)$. By the approximation lemma, $\hat{\tau}_i <: \texttt{annot}(\texttt{erase}(\hat{\tau}_i), \varepsilon_s)$. We know $\texttt{erase}(\hat{\tau}_i) = \tau$, so this judgement can be rewritten as $\hat{\tau}_i <: \texttt{annot}(\tau, \varepsilon_s)$. From this we can use ε-Subsume to narrow the type of (5) and widen the approximate effects of (5) from $\varnothing$ to ε_s, giving $y : \hat{\tau}_i \vdash \texttt{annot}(x, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varepsilon_s$. Finally, by widening the context, $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), \hat{\tau}_i \vdash \texttt{annot}(x, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varepsilon_s$.

Subcase 2: $x \neq y$. Because $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash x : \tau$ and $x \neq y$ then $x : \tau \in \Gamma$. Then $x : \texttt{annot}(\tau, \varepsilon_s) \in \texttt{annot}(\Gamma, \varepsilon_s)$ so $\texttt{annot}(\Gamma, \varepsilon_s) \vdash x : \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varnothing$ by ε-Var. By definition $\texttt{annot}(x, \varepsilon_s) = x$, so $\texttt{annot}(\Gamma, \varepsilon_s) \vdash \texttt{annot}(x, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varnothing$. Applying ε-Subsume gives $\texttt{annot}(\Gamma, \varepsilon_s) \vdash \texttt{annot}(x, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varepsilon_s$. By widening the context $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau}_i \vdash \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varepsilon'$.

Case: T-Resource. Then $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash r : \{r\}$. By ε-Resource, $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon), y : \hat{\tau}_i \vdash r : \{r\} \texttt{ with } \varnothing$. Applying definitions, $\texttt{annot}(r, \varepsilon) = r$ and $\texttt{annot}(\{r\}, \varepsilon_s) = \{r\}$, so this judgement can be rewritten as $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon), y : \hat{\tau}_i \vdash \texttt{annot}(e, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varnothing$. By ε-Subsume, $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau}_i \vdash \texttt{annot}(e, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s) \texttt{ with } \varepsilon_s$.

Case: T-Abs. Then $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash \lambda x : \tau_2.e_{body} : \tau_2 \rightarrow \tau_3$. Applying definitions, (5) $\texttt{annot}(e, \varepsilon_s) = \texttt{annot}(\lambda x : \tau_2.e_{body}, \varepsilon_s) = \lambda x : \texttt{annot}(\tau_2, \varepsilon_s).\texttt{annot}(e_{body}, \varepsilon_s)$ and $\texttt{annot}(\tau, \varepsilon_s) = \texttt{annot}(\tau_2 \rightarrow \tau_3, \varepsilon_s) = \texttt{annot}(\tau_2, \varepsilon_s) \rightarrow_{\varepsilon_s} \texttt{annot}(\tau_3, \varepsilon_s)$. By inversion on T-Abs, we get the sub-derivation (6) $\Gamma, y : \texttt{erase}(\hat{\tau}_i), x : \tau_2 \vdash e_{body} : \tau_2$. We shall apply the inductive assumption to this judgement with an unannotated context consisting of $\Gamma, x : \tau_2$. To be a valid application of the lemma, it is required that $\texttt{effects}(\texttt{annot}(\Gamma, x : \tau_2, \varnothing) \subseteq \varepsilon_s$. We already know

$\texttt{effects}(\texttt{annot}(\Gamma, \varnothing)) \subseteq \varepsilon_s$ by assumption (3). Also by assumption (3), $\texttt{ho-effects}(\texttt{annot}(\tau_2 \to \tau_3, \varnothing)) \subseteq \varepsilon_s$; then by definition of $\texttt{ho-effects}$, $\texttt{effects}(\texttt{annot}(\tau_2, \varnothing)) \subseteq \texttt{ho-effects}(\texttt{annot}(\tau_2 \to \tau_3, \varnothing))$, so $\texttt{effects}(\texttt{annot}(x : \tau_2,)\varepsilon_s) \subseteq \varepsilon_s$ by transitivity. Then by applying the inductive assumption to (6), $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), \texttt{annot}(x : \tau_2, \varepsilon_s), y : \hat{\tau}_i \vdash \texttt{annot}(e_{body}, \varepsilon_s) : \texttt{annot}(\tau_3, \varepsilon_s)\ \texttt{with}\ \varepsilon_s$. By ε-Abs, $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau}_i \vdash \lambda x : \texttt{annot}(\hat{\tau}_2, \varepsilon_s).\texttt{annot}(e_{body}, \varepsilon_s) : \texttt{annot}(\hat{\tau}_2, \varepsilon_s) \to_{\varepsilon_s} \texttt{annot}(\hat{\tau}_3, \varepsilon_s)\ \texttt{with}\ \varnothing$. By applying the identities from (5), this judgement can be rewritten as $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau}_i \vdash \texttt{annot}(e, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s)\ \texttt{with}\ \varnothing$. Finally, by applying ε-Subsume, $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau}_i \vdash \texttt{annot}(e, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon_s)\ \texttt{with}\ \varepsilon_s$.

Case: T-App. Then $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash e_1\ e_2 : \tau_3$ and by inversion $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash e_1 : \tau_2 \to \tau_3$ and $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash e_2 : \tau_2$. By applying the inductive assumption to these judgements, $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau}_i \vdash \texttt{annot}(e_1, \varepsilon_2) : \texttt{annot}(\tau_2, \varepsilon_s) \to_{\varepsilon_s} \texttt{annot}(\tau_3, \varepsilon_s)\ \texttt{with}\ \varepsilon_s$ and $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau} \vdash \texttt{annot}(e_2, \varepsilon_s) : \texttt{annot}(\tau_2, \varepsilon_s)\ \texttt{with}\ \varepsilon_s$. Then by ε-App, we get $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau} \vdash \texttt{annot}(e_1, \varepsilon_s)\ \texttt{annot}(e_2, \varepsilon_s) : \texttt{annot}(\tau_3, \varepsilon)\ \texttt{with}\ \varepsilon$. Unfolding the definition of $\texttt{annot}$, this judgement can be rewritten as $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau} \vdash \texttt{annot}(e_1\ e_2, \varepsilon_s) : \texttt{annot}(\tau_3, \varepsilon)\ \texttt{with}\ \varepsilon$. Finally, because $e = e_1\ e_2$ and $\tau = \tau_3$, this is the same as $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon_s), y : \hat{\tau} \vdash \texttt{annot}(e, \varepsilon_s) : \texttt{annot}(\tau, \varepsilon)\ \texttt{with}\ \varepsilon$.

Case: T-OperCall. Then $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash e_1.\pi : \texttt{Unit}$. By inversion we get the sub-derivation $\Gamma, y : \texttt{erase}(\hat{\tau}_i) \vdash e_1 : \{\bar{r}\}$. Applying the inductive assumption, $\hat{\Gamma}, \texttt{annot}(\Gamma, \varepsilon), y : \hat{\tau}_i \vdash \texttt{annot}(e_1, \varepsilon_s) : \texttt{annot}(\{\bar{r}\}, \varepsilon_s)\ \texttt{with}\ \varepsilon_s$. By definition, $\texttt{annot}(\{\bar{r}\}, \varepsilon_s) = \{\bar{r}\}$, so this judgement can be rewritten as $\hat{\Gamma}, \texttt{annot}(\Gamma, \varnothing), y : \hat{\tau}_i \vdash e_1 : \{\bar{r}\}\ \texttt{with}\ \varepsilon_s$. By ε-OperCall, $\hat{\Gamma}, \texttt{annot}(\Gamma, \varnothing), y : \hat{\tau} \vdash \texttt{annot}(e_1.\pi, \varepsilon_s) : \{\bar{r}\}\ \texttt{with}\ \varepsilon_s \cup \{\bar{r}.\pi\}$. All that remains is to show $\{\bar{r}.\pi\} \subseteq \varepsilon$. We shall do this by considering which subcontext left of the turnstile is capturing $\{\bar{r}\}$. Technically, $\hat{\Gamma}$ may not have a binding for every $r \in \bar{r}$: the judgement for e_1 might be derived using S-Resources and ε-Subsume. However, at least one binding for some $r \in \bar{r}$ must be present in $\hat{\Gamma}$ to get the original typing judgement being subsumed, so we shall assume without loss of generality that $\hat{\Gamma}$ contains a binding for every $r \in \bar{r}$.

Subcase 1: $\{\bar{r}\} = \hat{\tau}$. By assumption (3), $\texttt{effects}(\hat{\tau}) \subseteq \varepsilon_s$, so $\bar{r}.\pi \subseteq \{r.\pi \mid r \in \bar{r}, \pi \in \Pi\} = \texttt{effects}(\{\bar{r}\}) \subseteq \varepsilon_s$.

Subcase 2: $r : \{\bar{r}\} \in \texttt{annot}(\Gamma, \varepsilon_s)$. Then $\bar{r}.\pi \in \texttt{effects}(\{\bar{r}\}) \subseteq \texttt{effects}(\texttt{annot}(\Gamma, \varnothing))$, and by assumption (3) $\texttt{effects}(\texttt{annot}(\Gamma, \varnothing)) \subseteq \varepsilon_s$, so $\bar{r}.\pi \in \varepsilon_s$.

Subcase 3: $r : \{\bar{r}\} \in \hat{\Gamma}$. Because $\Gamma, y : \texttt{erase}(\hat{\tau}) \vdash e_1 : \{\bar{r}\}$, then $\bar{r} \in \Gamma$ or $r = \tau$. If $r \in \texttt{annot}(\Gamma, \varnothing)$ then subcase 2 holds. Else $r = \texttt{erase}(\hat{\tau})$. Because $\hat{\tau} = \{\bar{r}\}$, then $\texttt{erase}(\{\bar{r}\}) = \{\bar{r}\}$, so $\hat{\tau} = \tau$; therefore subcase 1 holds. □

Theorem 2.7 (CC Preservation). *If* $\hat{\Gamma} \vdash \hat{e}_A : \hat{\tau}_A\ \texttt{with}\ \varepsilon_A$ *and* $\hat{e}_A \longrightarrow \hat{e}_B \mid \varepsilon$*, then* $\hat{\Gamma} \vdash \hat{e}_B : \hat{\tau}_B\ \texttt{with}\ \varepsilon_B$*, where* $\hat{e}_B <: \hat{e}_A$ *and* $\varepsilon \cup \varepsilon_B \subseteq \varepsilon_A$*, for some* $\hat{e}_B, \varepsilon, \hat{\tau}_B, \varepsilon_B$.

Proof. By induction on the derivation of $\hat{\Gamma} \vdash \hat{e}_A : \hat{\tau}_A\ \texttt{with}\ \varepsilon_A$ and then the derivation of $\hat{e}_A \longrightarrow \hat{e}_B \mid \varepsilon$.

Case: ε-Import. Then by inversion on the rules used, the following are true:

(1) $\hat{e}_A = \texttt{import}(\varepsilon_s)\ x = \hat{v}_i\ \texttt{in}\ e$
(2) $x : \texttt{erase}(\hat{\tau}_i) \vdash e : \tau$

(3) $\hat{\Gamma} \vdash \hat{e}_i : \hat{\tau}_i$ with ε_1
(4) $\hat{\Gamma} \vdash \hat{e}_A : \mathsf{annot}(\tau, \varepsilon_s)$ with $\varepsilon_s \cup \varepsilon_1$
(5) $\mathsf{effects}(\hat{\tau}_i) \cup \mathsf{ho\text{-}effects}(\mathsf{annot}(\tau, \varnothing)) \subseteq \varepsilon_s$
(6) $\mathsf{ho\text{-}safe}(\hat{\tau}_i, \varepsilon_s)$

Subcase 1: E-Import1. Then $\mathsf{import}(\varepsilon_s)\ x = \hat{e}_i\ \mathsf{in}\ e \longrightarrow \mathsf{import}(\varepsilon_s)\ x = \hat{e}'_i\ \mathsf{in}\ e \mid \varepsilon$ and by inversion, $\hat{e}_i \longrightarrow \hat{e}'_i \mid \varepsilon$. By inductive assumption and subsumption, $\hat{\Gamma} \vdash \hat{e}'_i : \hat{\tau}'_i$ with ε_1. Then by ε-Import, $\hat{\Gamma} \vdash \mathsf{import}(\varepsilon_s)\ x = \hat{e}'_i\ \mathsf{in}\ e : \mathsf{annot}(\tau, \varepsilon_s)$ with ε_s.

Subcase 2: E-Import2. Then $\hat{e}_i = \hat{v}_i$ is a value and $\varepsilon_1 = \varnothing$ by canonical forms. Apply the annotation lemma with $\Gamma = \varnothing$ to get $\hat{\Gamma}, x : \hat{\tau}_i \vdash \mathsf{annot}(e, \varepsilon_s) : \mathsf{annot}(\tau, \varepsilon_s)$ with ε_s. From assumption (4) and canonical forms we have $\hat{\Gamma} \vdash \hat{v} : \hat{\tau}_i$ with $\varnothing$. Applying the substitution lemma, $\hat{\Gamma} \vdash [\hat{v}_i/x]\mathsf{annot}(e, \varepsilon) : \mathsf{annot}(\tau, \varepsilon_s)$ with ε_s. Then $\varepsilon \cup \varepsilon_B = \varepsilon_A = \varepsilon_s$ and $\tau_A = \tau_B = \mathsf{annot}(\tau, \varepsilon_s)$.

□

Theorem 2.8 (CC Single-step Soundness). *If $\hat{\Gamma} \vdash \hat{e}_A : \hat{\tau}_A$ with ε_A and $\hat{e}_A$ is not a value, then $\hat{e}_A \longrightarrow \hat{e}_B \mid \varepsilon$, where $\hat{\Gamma} \vdash \hat{e}_B : \hat{\tau}_B$ with ε_B and $\hat{\tau}_B <: \hat{\tau}_A$ and $\varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$, for some $\hat{e}_B$, ε, $\hat{\tau}_B$, and ε_B.*

Theorem 2.9 (CC Multi-step Soundness). *If $\hat{\Gamma} \vdash \hat{e}_A : \hat{\tau}_A$ with ε_A and $\hat{e}_A \longrightarrow^* e_B \mid \varepsilon$, then $\hat{\Gamma} \vdash \hat{e}_B : \hat{\tau}_B$ with ε_B, where $\hat{\tau}_B <: \hat{\tau}_A$ and $\varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$, for some $\hat{\tau}_B$, ε_B.*

Proof. The same as for OC. □