

# Capabilities: Effects for Free (Supplementary Material with Proofs)

## 1 OC Proofs

► **Lemma 1** (OC Canonical Forms). *Unless the rule used is  $\varepsilon$ -SUBSUME, the following are true:*

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

**Proof.**

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

◀

---

► **Theorem 2** (OC Progress). *If  $\Gamma \vdash e : \tau$  with  $\varepsilon$  and  $e$  is not a value or variable, then  $e \rightarrow e' \mid \varepsilon$ , for some  $e', \varepsilon$ .*

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

Case:  $\varepsilon$ -VAR,  $\varepsilon$ -RESOURCE, or  $\varepsilon$ -ABS. Then  $e$  is a value or variable and the theorem statement holds vacuously.

Case:  $\varepsilon$ -APP. Then  $e = e_1 e_2$ . If  $e_1$  is not a value or variable it can be reduced  $e_1 \rightarrow e'_1 \mid \varepsilon$  by inductive assumption, so  $e_1 e_2 \rightarrow e'_1 e_2 \mid \varepsilon$  by E-APP1. If  $e_1 = v_1$  is a value and  $e_2$  a non-value, then  $e_2$  can be reduced  $e_2 \rightarrow e'_2 \mid \varepsilon$  by inductive assumption, so  $e_1 e_2 \rightarrow v_1 e'_2 \mid \varepsilon$  by E-APP2. Otherwise  $e_1 = v_1$  and  $e_2 = v_2$  are both values. By inversion on  $\varepsilon$ -APP and canonical forms,  $\Gamma \vdash v_1 : \tau_2 \rightarrow_{\varepsilon'} \tau_3$  with  $\emptyset$ , and  $v_1 = \lambda x : \tau_2.e_{body}$ . Then  $(\lambda x : \tau_2.e_{body})v_2 \rightarrow [v_2/x]e_{body} \mid \emptyset$  by E-APP3.

Case:  $\varepsilon$ -OPERCALL. Then  $e = e_1.\pi$ . If  $e_1$  is a non-value it can be reduced  $e_1 \rightarrow e'_1 \mid \varepsilon$  by inductive assumption, so  $e_1.\pi \rightarrow e'_1.\pi \mid \varepsilon$  by E-OPERCALL1. Otherwise  $e_1 = v_1$  is a value. By inversion on  $\varepsilon$ -OPERCALL and canonical forms,  $\Gamma \vdash v_1 : \{r\}$  with  $\{r.\pi\}$ , and  $v_1 = r$ . Then  $r.\pi \rightarrow \text{unit} \mid \{r.\pi\}$  by E-OPERCALL2.

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

◀

---

► **Lemma 3** (OC Substitution). *If  $\Gamma, x : \tau' \vdash e : \tau$  with  $\varepsilon$  and  $\Gamma \vdash v : \tau'$  with  $\emptyset$  then  $\Gamma \vdash [v/x]e : \tau$  with  $\varepsilon$ .*



licensed under Creative Commons License CC-BY



Leibniz International Proceedings in Informatics  
LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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

*Case:  $\varepsilon$ -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  $\Gamma, x : \tau' \vdash e : \tau'$  with  $\emptyset$ , hence  $\tau' = \tau$ .  $[v/x]y = [v/x]x = v$ , and by assumption,  $\Gamma \vdash v : \tau'$  with  $\emptyset$ , so  $\Gamma \vdash [v/x]y : \tau$  with  $\emptyset$ .

Otherwise  $y \neq x$ . By applying canonical forms to the theorem assumption  $\Gamma, x : \tau' \vdash y : \tau$  with  $\emptyset$ , so  $y : \tau \in \Gamma$ . Since  $[v/x]y = y$ , then  $\Gamma \vdash y : \tau$  with  $\emptyset$  by  $\varepsilon$ -VAR.

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

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

*Case:  $\varepsilon$ -OPERCALL.* By inversion  $\Gamma, x : \tau' \vdash e_1 : \{\bar{r}\}$  with  $\varepsilon_1$  and  $\tau = \text{Unit}$  and  $\varepsilon = \varepsilon_1 \cup \{r.\pi \mid r \in \bar{r}, \pi \in \Pi\}$ . By inductive assumption,  $\Gamma \vdash [v/x]e_1 : \{\bar{r}\}$  with  $\varepsilon_1$ . Then by  $\varepsilon$ -OPERCALL,  $\Gamma \vdash ([v/x]e_1).\pi : \text{Unit}$  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  $\Gamma \vdash [v/x](e_1.\pi) : \tau$  with  $\varepsilon$ .

*Case:  $\varepsilon$ -SUBSUME.* By inversion,  $\Gamma, x : \tau' \vdash e : \tau_2$  with  $\varepsilon_2$ , where  $\tau_2 < \tau$  and  $\varepsilon_2 \subseteq \varepsilon$ . By inductive hypothesis,  $\Gamma \vdash [v/x]e : \tau_2$  with  $\varepsilon_2$ . Then  $\Gamma \vdash [v/x]e : \tau$  with  $\varepsilon$  by  $\varepsilon$ -SUBSUME. ◀

► **Theorem 4 (OC Preservation).** *If  $\Gamma \vdash e_A : \tau_A$  with  $\varepsilon_A$  and  $e_A \rightarrow e_B \mid \varepsilon$ , 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  $\Gamma \vdash e_A : \tau_A$  with  $\varepsilon_A$  and then the derivation of  $e_A \rightarrow e_B \mid \varepsilon$ .

*Case:  $\varepsilon$ -VAR,  $\varepsilon$ -RESOURCE,  $\varepsilon$ -UNIT,  $\varepsilon$ -ABS.* Then  $e_A$  is a value and cannot be reduced, so the theorem holds vacuously.

*Case:  $\varepsilon$ -APP.* Then  $e_A = e_1 e_2$  and  $\Gamma \vdash e_1 : \tau_2 \rightarrow_{\varepsilon_3} \tau_3$  with  $\varepsilon_1$  and  $\Gamma \vdash e_2 : \tau_2$  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  $e_1 e_2 \rightarrow e'_1 e_2 \mid \varepsilon$ . By inversion on E-APP1,  $e_1 \rightarrow e'_1 \mid \varepsilon$ . By inductive hypothesis and  $\varepsilon$ -SUBSUME  $\Gamma \vdash v_1 : \tau_2 \rightarrow_{\varepsilon_3} \tau_3$  with  $\varepsilon_1$ . Then  $\Gamma \vdash e'_1 e_2 : \tau_3$  with  $\varepsilon_1 \cup \varepsilon_2 \cup \varepsilon_3$  by  $\varepsilon$ -APP.

**Subcase: E-APP2.** Then  $e_1 = v_1$  is a value and  $e_2 \rightarrow e'_2 \mid \varepsilon$ . By inversion on E-APP2,  $e_2 \rightarrow e'_2 \mid \varepsilon$ . By inductive hypothesis and  $\varepsilon$ -SUBSUME  $\Gamma \vdash e'_2 : \tau_2$  with  $\varepsilon_2$ . Then  $\Gamma \vdash v_1 e'_2 : \tau_3$  with  $\varepsilon_1 \cup \varepsilon_2 \cup \varepsilon_3$  by  $\varepsilon$ -APP.

**Subcase: E-APP3.** Then  $e_1 = \lambda x : \tau_2.e_{body}$  and  $e_2 = v_2$  are values and  $(\lambda x : \tau_2.e_{body}) v_2 \rightarrow [v_2/x]e_{body} \mid \emptyset$ . By inversion on the rule  $\varepsilon$ -APP used to type  $\lambda x : \tau_2.e_{body}$ , we know  $\Gamma, x : \tau_2 \vdash e_{body} : \tau_3$  with  $\varepsilon_3$ .  $e_1 = v_1$  and  $e_2 = v_2$  are values, so  $\varepsilon_1 = \varepsilon_2 = \emptyset$  by canonical forms. Then by the substitution lemma,  $\Gamma \vdash [v_2/x]e_{body} : \tau_3$  with  $\varepsilon_3$  and

$$\varepsilon_A = \varepsilon_B = \varepsilon.$$

*Case:*  $\varepsilon$ -OPERCALL. Then  $e_A = e_1.\pi$  and  $\Gamma \vdash e_1 : \{\bar{r}\}$  with  $\varepsilon_1$  and  $\tau_A = \text{Unit}$  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  $\varepsilon$ -SUBSUME,  $\Gamma \vdash e'_1 : \{\bar{r}\}$  with  $\varepsilon_1$ . Then  $\Gamma \vdash e'_1.\pi : \{\bar{r}\}$  with  $\varepsilon_1 \cup \{r.\pi \mid r \in \bar{r}, \pi \in \Pi\}$  by  $\varepsilon$ -OPERCALL.

**Subcase:** E-OPERCALL2. Then  $e_1 = r$  is a resource literal and  $r.\pi \longrightarrow \text{unit} \mid \{r.\pi\}$ . By canonical forms,  $\varepsilon_1 = \emptyset$ . By  $\varepsilon$ -UNIT,  $\Gamma \vdash \text{unit} : \text{Unit}$  with  $\emptyset$ . Therefore  $\tau_B = \tau_A$  and  $\varepsilon \cup \varepsilon_B = \{r.\pi\} = \varepsilon_A$ .  $\blacktriangleleft$

► **Theorem 5** (OC Single-step Soundness). *If  $\Gamma \vdash e_A : \tau_A$  with  $\varepsilon_A$  and  $e_A$  is not a value, then  $e_A \longrightarrow e_B \mid \varepsilon$ , where  $\Gamma \vdash e_B : \tau_B$  with  $\varepsilon_B$  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.  $\blacktriangleleft$

► **Theorem 6** (OC Multi-step Soundness). *If  $\Gamma \vdash e_A : \tau_A$  with  $\varepsilon_A$  and  $e_A \longrightarrow^* e_B \mid \varepsilon$ , where  $\Gamma \vdash e_B : \tau_B$  with  $\varepsilon_B$  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  $\varepsilon = \emptyset$  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  $\varepsilon_C$  and  $\Gamma \vdash e_B : \tau_B$  with  $\varepsilon_B$ , 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  $\varepsilon_B \cup \varepsilon' \cup \varepsilon'' = \varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$ .  $\blacktriangleleft$

## 2 CC Proofs

► **Lemma 7** (CC Canonical Forms). *Unless the rule used is  $\varepsilon$ -SUBSUME, the following are true:*

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

**Proof.** Same as for OC.  $\blacktriangleleft$

► **Theorem 8** (CC Progress). *If  $\hat{\Gamma} \vdash \hat{e} : \hat{\tau}$  with  $\varepsilon$  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  $\hat{\Gamma} \vdash \hat{e} : \hat{\tau}$  with  $\varepsilon$ .

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

► **Lemma 9** (CC Substitution). *If  $\hat{\Gamma}, x : \hat{\tau}' \vdash \hat{e} : \hat{\tau}$  with  $\varepsilon$  and  $\hat{\Gamma} \vdash \hat{v} : \hat{\tau}'$  with  $\emptyset$  then  $\hat{\Gamma} \vdash [\hat{v}/x]\hat{e}_A : \hat{\tau}$  with  $\varepsilon$ .*

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

*Case:*  $\varepsilon$ -MODULE. Then the following are true.

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

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

► **Lemma 10** (CC Approximation 1). *If  $\text{effects}(\hat{\tau}) \subseteq \varepsilon$  and  $\text{ho-safe}(\hat{\tau}, \varepsilon)$  then  $\hat{\tau} <: \text{annot}(\text{erase}(\hat{\tau}), \varepsilon)$ .*

► **Lemma 11** (CC Approximation 2). *If  $\text{ho-effects}(\hat{\tau}) \subseteq \varepsilon$  and  $\text{safe}(\hat{\tau}, \varepsilon)$  then  $\text{annot}(\text{erase}(\hat{\tau}), \varepsilon) <: \hat{\tau}$ .*

**Proof.** By simultaneous induction on derivations of **safe** and **ho-safe**.

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

*Case:*  $\hat{\tau} = \hat{\tau}_1 \rightarrow_{\varepsilon'} \hat{\tau}_2$ ,  $\text{effects}(\hat{\tau}) \subseteq \varepsilon$ ,  $\text{ho-safe}(\hat{\tau}, \varepsilon)$  It is sufficient to show  $\hat{\tau}_2 <: \text{annot}(\text{erase}(\hat{\tau}_2), \varepsilon)$  and  $\text{annot}(\text{erase}(\hat{\tau}_1), \varepsilon) <: \hat{\tau}_1$ , 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  $\text{effects}(\hat{\tau}) \subseteq \varepsilon$  we have  $\text{ho-effects}(\hat{\tau}_1) \cup \varepsilon' \cup \text{effects}(\hat{\tau}_2) \subseteq \varepsilon$  and therefore  $\text{effects}(\hat{\tau}_2) \subseteq \varepsilon$ . From  $\text{ho-safe}(\hat{\tau}, \varepsilon)$  we have  $\text{ho-safe}(\hat{\tau}_2, \varepsilon)$ . Therefore we can apply lemma 1 to  $\hat{\tau}_2$ .

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

*Case:*  $\hat{\tau} = \hat{\tau}_1 \rightarrow_{\varepsilon'} \hat{\tau}_2$ ,  $\text{ho-effects}(\hat{\tau}) \subseteq \varepsilon$ ,  $\text{safe}(\hat{\tau}, \varepsilon)$  It is sufficient to show  $\text{annot}(\text{erase}(\hat{\tau}_2), \varepsilon) <: \hat{\tau}_2$  and  $\hat{\tau}_1 <: \text{annot}(\text{erase}(\hat{\tau}_1), \varepsilon)$ , 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  $\text{ho-effects}(\hat{\tau}) \subseteq \varepsilon$  we have  $\text{effects}(\hat{\tau}_1) \cup \text{ho-effects}(\hat{\tau}_2) \subseteq \varepsilon$  and therefore  $\text{ho-effects}(\hat{\tau}_2) \subseteq \varepsilon$ . From  $\text{safe}(\hat{\tau}, \varepsilon)$  we have  $\text{safe}(\hat{\tau}_2, \varepsilon)$ . Therefore we can apply lemma 2 to  $\hat{\tau}_2$ .

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

◀

---

► **Lemma 12** (CC Annotation). *If the following are true:*

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

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

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

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

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

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

*Case:* T-RESOURCE. Then  $\Gamma, y : \text{erase}(\hat{\tau}_i) \vdash r : \{r\}$ . By  $\varepsilon$ -RESOURCE,  $\hat{\Gamma}, \text{annot}(\Gamma, \varepsilon), y : \hat{\tau}_i \vdash r : \{r\}$  with  $\emptyset$ . Applying definitions,  $\text{annot}(r, \varepsilon) = r$  and  $\text{annot}(\{r\}, \varepsilon_s) = \{r\}$ , so this judgement can be rewritten as  $\hat{\Gamma}, \text{annot}(\Gamma, \varepsilon), y : \hat{\tau}_i \vdash \text{annot}(e, \varepsilon_s) : \text{annot}(\tau, \varepsilon_s)$  with  $\emptyset$ . By  $\varepsilon$ -SUBSUME,  $\hat{\Gamma}, \text{annot}(\Gamma, \varepsilon_s), y : \hat{\tau}_i \vdash \text{annot}(e, \varepsilon_s) : \text{annot}(\tau, \varepsilon_s)$  with  $\varepsilon_s$ .

*Case:* T-ABS. Then  $\Gamma, y : \text{erase}(\hat{\tau}_i) \vdash \lambda x : \tau_2.e_{\text{body}} : \tau_2 \rightarrow \tau_3$ . Applying definitions, (5)  $\text{annot}(e, \varepsilon_s) = \text{annot}(\lambda x : \tau_2.e_{\text{body}}, \varepsilon_s) = \lambda x : \text{annot}(\tau_2, \varepsilon_s).\text{annot}(e_{\text{body}}, \varepsilon_s)$  and  $\text{annot}(\tau, \varepsilon_s) = \text{annot}(\tau_2 \rightarrow \tau_3, \varepsilon_s) = \text{annot}(\tau_2, \varepsilon_s) \rightarrow_{\varepsilon_s} \text{annot}(\tau_3, \varepsilon_s)$ . By inversion on T-ABS, we get the sub-derivation (6)  $\Gamma, y : \text{erase}(\hat{\tau}_i), x : \tau_2 \vdash e_{\text{body}} : \tau_2$ . 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  $\text{effects}(\text{annot}(\Gamma, x : \tau_2, \emptyset)) \subseteq \varepsilon_s$ . We already know  $\text{effects}(\text{annot}(\Gamma, \emptyset)) \subseteq \varepsilon_s$  by assumption (3). Also by

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

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

*Case: T-OPERCALL.* Then  $\Gamma, y : \text{erase}(\hat{\tau}_i) \vdash e_1. \pi : \text{Unit}$ . By inversion we get the subderivation  $\Gamma, y : \text{erase}(\hat{\tau}_i) \vdash e_1 : \{\bar{r}\}$ . Applying the inductive assumption,  $\hat{\Gamma}, \text{annot}(\Gamma, \varepsilon), y : \hat{\tau}_i \vdash \text{annot}(e_1, \varepsilon_s) : \text{annot}(\{\bar{r}\}, \varepsilon_s) \text{ with } \varepsilon_s$ . By definition,  $\text{annot}(\{\bar{r}\}, \varepsilon_s) = \{\bar{r}\}$ , so this judgement can be rewritten as  $\hat{\Gamma}, \text{annot}(\Gamma, \emptyset), y : \hat{\tau}_i \vdash e_1 : \{\bar{r}\} \text{ with } \varepsilon_s$ . By  $\varepsilon$ -OPERCALL,  $\hat{\Gamma}, \text{annot}(\Gamma, \emptyset), y : \hat{\tau}_i \vdash \text{annot}(e_1. \pi, \varepsilon_s) : \{\bar{r}\} \text{ with } \varepsilon_s \cup \{\bar{r}. \pi\}$ . 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  $\varepsilon$ -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),  $\text{effects}(\hat{\tau}) \subseteq \varepsilon_s$ , so  $\bar{r}. \pi \subseteq \{r. \pi \mid r \in \bar{r}, \pi \in \Pi\} = \text{effects}(\{\bar{r}\}) \subseteq \varepsilon_s$ .

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

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

---

► **Theorem 13 (CC Preservation).** *If  $\hat{\Gamma} \vdash \hat{e}_A : \hat{\tau}_A \text{ with } \varepsilon_A$  and  $\hat{e}_A \longrightarrow \hat{e}_B \mid \varepsilon$ , then  $\hat{\Gamma} \vdash \hat{e}_B : \hat{\tau}_B \text{ with } \varepsilon_B$ , 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  $\hat{\Gamma} \vdash \hat{e}_A : \hat{\tau}_A \text{ with } \varepsilon_A$  and then the derivation of  $\hat{e}_A \longrightarrow \hat{e}_B \mid \varepsilon$ .

*Case:  $\varepsilon$ -IMPORT.* Then by inversion on the rules used, the following are true:

1.  $\hat{e}_A = \text{import}(\varepsilon_s) x = \hat{v}_i \text{ in } e$
2.  $x : \text{erase}(\hat{\tau}_i) \vdash e : \tau$
3.  $\hat{\Gamma} \vdash \hat{e}_i : \hat{\tau}_i \text{ with } \varepsilon_1$
4.  $\hat{\Gamma} \vdash \hat{e}_A : \text{annot}(\tau, \varepsilon_s) \text{ with } \varepsilon_s \cup \varepsilon_1$
5.  $\text{effects}(\hat{\tau}_i) \cup \text{ho-effects}(\text{annot}(\tau, \emptyset)) \subseteq \varepsilon_s$
6.  $\text{ho-safe}(\hat{\tau}_i, \varepsilon_s)$

**Subcase 1:** E-IMPORT1. Then  $\text{import}(\varepsilon_s) x = \hat{e}_i \text{ in } e \longrightarrow \text{import}(\varepsilon_s) x = \hat{e}'_i \text{ in } e \mid \varepsilon$  and by inversion,  $\hat{e}_i \longrightarrow \hat{e}'_i \mid \varepsilon$ . By inductive assumption and subsumption,  $\hat{\Gamma} \vdash \hat{e}'_i : \hat{\tau}'_i \text{ with } \varepsilon_1$ . Then by  $\varepsilon$ -IMPORT,  $\hat{\Gamma} \vdash \text{import}(\varepsilon_s) x = \hat{e}'_i \text{ in } e : \text{annot}(\tau, \varepsilon_s) \text{ with } \varepsilon_s$ .

**Subcase 2:** E-IMPORT2. Then  $\hat{e}_i = \hat{v}_i$  is a value and  $\varepsilon_1 = \emptyset$  by canonical forms. Apply the annotation lemma with  $\Gamma = \emptyset$  to get  $\hat{\Gamma}, x : \hat{\tau}_i \vdash \text{annot}(e, \varepsilon_s) : \text{annot}(\tau, \varepsilon_s) \text{ with } \varepsilon_s$ . From assumption (4) and canonical forms we have  $\hat{\Gamma} \vdash \hat{v} : \hat{\tau}_i \text{ with } \emptyset$ . Applying the substitution lemma,  $\hat{\Gamma} \vdash [\hat{v}_i/x] \text{annot}(e, \varepsilon) : \text{annot}(\tau, \varepsilon_s) \text{ with } \varepsilon_s$ . Then  $\varepsilon \cup \varepsilon_B = \varepsilon_A = \varepsilon_s$  and  $\tau_A = \tau_B = \text{annot}(\tau, \varepsilon_s)$ .

◀

---

► **Theorem 14** (CC Single-step Soundness). *If  $\hat{\Gamma} \vdash \hat{e}_A : \hat{\tau}_A \text{ with } \varepsilon_A$  and  $\hat{e}_A$  is not a value, then  $\hat{e}_A \longrightarrow \hat{e}_B \mid \varepsilon$ , where  $\hat{\Gamma} \vdash \hat{e}_B : \hat{\tau}_B \text{ with } \varepsilon_B$  and  $\hat{\tau}_B <: \hat{\tau}_A$  and  $\varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$ , for some  $\hat{e}_B$ ,  $\varepsilon$ ,  $\hat{\tau}_B$ , and  $\varepsilon_B$ .*

► **Theorem 15** (CC Multi-step Soundness). *If  $\hat{\Gamma} \vdash \hat{e}_A : \hat{\tau}_A \text{ with } \varepsilon_A$  and  $\hat{e}_A \longrightarrow^* e_B \mid \varepsilon$ , then  $\hat{\Gamma} \vdash \hat{e}_B : \hat{\tau}_B \text{ with } \varepsilon_B$ , where  $\hat{\tau}_B <: \hat{\tau}_A$  and  $\varepsilon_B \cup \varepsilon \subseteq \varepsilon_A$ , for some  $\hat{\tau}_B$ ,  $\varepsilon_B$ .*

**Proof.** The same as for OC.

◀

