APPENDIX A: PROOF DETAILS

This appendix contains proof details for the paper "Garbage-Collection Safety for Region-Based Type-Polymorphic Programs" (PLDI '23) by Martin Elsman.

Proposition 5 (Type Substitution Closedness). *Assume o is one of μ or π. If $\Omega + \Delta \vdash o : \varphi$ and $\Omega \vdash S : \Delta$ then $\Omega \vdash S(o) : \varphi$.*

Proof. By induction over the structure of o. The interesting case is the case for $\mu = \alpha$ for some type variable α. There are now two cases. We first consider the case where $\alpha \in \mathrm{dom}(S)$. From the definition of coverage, we have $\langle 1 \rangle$ $\Omega \vdash S(\alpha) : \mathrm{frev}(\Delta(\alpha))$ and $\mathrm{dom}(S) = \mathrm{dom}(\Delta)$. Moreover, from assumptions we have $\Omega + \Delta \vdash \alpha : \varphi$, thus, from the definition of containment, we have $\mathrm{frev}((\Omega + \Delta)(\alpha)) \subseteq \varphi$ and thus $\langle 2 \rangle$ $\mathrm{frev}(\Delta(\alpha)) \subseteq \varphi$. From the extensibility property of type containment and from $\langle 1 \rangle$ and $\langle 2 \rangle$, we have $\Omega \vdash S(\alpha) : \varphi$, as required. For the second case where $\alpha \notin \mathrm{dom}(S)$, we have $S(\alpha) = \alpha$. It follows from the definition of coverage that $\alpha \notin \mathrm{dom}(\Delta)$, which leads us to conclude, based on the assumptions and the definition of type containment, that $\Omega \vdash S(\alpha) : \varphi$, as required. □

Proposition 6 (Instantiation Closed Under Region-Effect Substitution). *If S is a region-effect substitution and $\Omega \vdash \sigma \geq \tau$ via S' then $S(\Omega) \vdash S(\sigma) \geq S(\tau)$ via S'', where $S'' = (S \circ S') \downarrow \mathrm{dom}(S')$.*

Proof. We first consider the case where $\sigma = \forall\Delta.\tau'$. From the definition of instantiation, we have $\langle 1 \rangle$ $S'(\tau') = \tau$ and $\langle 2 \rangle$ $\Omega \vdash S' : \Delta$, and, thus, $\langle 3 \rangle$ $\mathrm{dom}(S') = \mathrm{dom}(\Delta)$. Because S is a region-effect substitution, we have $\langle 4 \rangle$ $S(\sigma) = \forall S(\Delta).S(\tau')$ and $\langle 5 \rangle$ $\mathrm{dom}(\Delta) = \mathrm{dom}(S(\Delta))$ and $\langle 6 \rangle$ $\mathrm{dom}(\Delta) \cap \mathrm{fv}(\mathrm{rng}(S)) = \emptyset$. Now, let $S'' = ((S \circ S') \downarrow \mathrm{dom}(S'))$. It follows that we have $\langle 7 \rangle$ $\mathrm{dom}(S'') = \mathrm{dom}(S(\Delta))$. We also have $S(S'(\tau')) = S(\tau)$ from $\langle 1 \rangle$ and $\langle 8 \rangle$ $S \circ S' = S'' \circ S$ because of $\langle 6 \rangle$ and $\langle 3 \rangle$. It follows that we have $\langle 9 \rangle$ $S''(S(\tau')) = S(\tau)$. We now need to show $S(\Omega) \vdash S'' : S(\Delta)$. From $\langle 2 \rangle$ and the definition of substitution coverage, we have $\langle 10 \rangle$ $\Omega \vdash S'(\alpha) : \mathrm{frev}(\Delta(\alpha))$, for all $\alpha \in \mathrm{dom}(S')$. From Proposition 4 and $\langle 10 \rangle$, we have $S(\Omega) \vdash S(S'(\alpha)) : S(\mathrm{frev}(\Delta(\alpha)))$ and thus, from $\langle 8 \rangle$ and because $\mathrm{dom}(S') = \mathrm{dom}(S'')$ follows from the definition of S'', we have $\langle 11 \rangle$ $S(\Omega) \vdash S''(\alpha) : \mathrm{frev}(S(\Delta)(\alpha))$, for all $\alpha \in \mathrm{dom}(S'')$. It follows from $\langle 11 \rangle$ that we have $\langle 12 \rangle$ $S(\Omega) \vdash S'' : S(\Delta)$. Now, from the definition of instantiation and from $\langle 9 \rangle$ and $\langle 12 \rangle$, we have $S(\Omega) \vdash S(\sigma) \geq S(\tau')$ via S'', as required. □

Proposition 7 (Instantiation Closed Under Type Substitution). *If $\Omega + \Delta \vdash \sigma \geq \tau$ via S' and $\Omega \vdash S : \Delta$ then $\Omega \vdash S(\sigma) \geq S(\tau)$ via S'', where $S'' = (S \circ S') \downarrow \mathrm{dom}(S')$.*

Proof. Follows from the definition of instantiation. □

Proposition 9 (GC-Safety Relation Closed Under Type Substitution). *Assume $\Omega \vdash S : \Delta$. If $G(\Omega + \Delta, \Gamma, e, X, \pi)$ then $G(\Omega, S(\Gamma), e, X, S(\pi))$.*

Proof. From assumptions and because $\mathrm{frv}(S(\pi)) \supseteq S(\mathrm{frv}(\pi))$, for any substitution S, we have, because value containment is closed under substitution and due to value containment extensibility, that $\mathrm{frv}(S(\pi)) \models_{\mathrm{v}} S(e)$. Because $\mathrm{fpv}(S(e)) = \mathrm{fpv}(e)$, it remains to be shown that

$$\forall y \in \mathrm{fpv}(e) \setminus X.\ \Omega \vdash S(\Gamma(y)) : \mathrm{frev}(S(\pi))$$

From assumptions, we have that for all $y \in \mathrm{fpv}(e) \setminus X$,

$$\Omega + \Delta \vdash \Gamma(y) : \mathrm{frev}(\pi)$$

From Proposition 5 and assumptions, we have

$$\Omega \vdash S(\Gamma(y)) : S(\mathrm{frev}(\pi))$$

Now, because $\text{frev}(S(\pi)) \supseteq S(\text{frev}(\pi))$ and because of type-containment effect-extensibility, we have $\Omega \vdash S(\Gamma(y)) : \text{frev}(S(\pi))$, as required. □

Proposition 10 (GC-Safety Relation Closed Under Value Substitution). *If* $x \notin X$ *and* $G(\Omega, \Gamma + \{x : \pi\}, e, X, \pi')$ *and* $\text{frv}(\pi) \models v$ *and* $\text{fpv}(v) = \emptyset$ *then* $G(\Omega, \Gamma, e[v/x], X, \pi')$.

Proof. From assumptions and (4), we have

$$\text{frv}(\pi') \models_{\text{v}} e \tag{5}$$

$$\forall y \in \text{fpv}(e) \setminus X.\Omega \vdash (\Gamma + \{x : \pi\})(y) : \text{frev}(\pi') \tag{6}$$

First, assume $x \in \text{fpv}(e)$. Because $x \notin X$, by choosing x for y, we have from (6) that $\Omega \vdash \pi : \text{frev}(\pi')$. It follows from Proposition 2 that $\text{frev}(\pi) \subseteq \text{frev}(\pi')$ and, thus

$$\text{frv}(\pi) \subseteq \text{frv}(\pi') \tag{7}$$

It follows from assumption, (7), and the value containment extensibility property that we have

$$\text{frv}(\pi') \models v \tag{8}$$

Now, from (5), (8), and the value containment substitution property, we have

$$\text{frv}(\pi') \models_{\text{v}} e[v/x] \tag{9}$$

We also have from (6) and because fpv(v) = ∅ that

$$\forall y \in \text{fpv}(e[v/x]) \setminus X.\Omega \vdash \Gamma(y) : \text{frev}(\pi') \tag{10}$$

From (4), (9), and (10), we have $G(\Omega, \Gamma, e[v/x], X, \pi')$, as required. □

The below detailed proofs follow closely the structure of the proofs provided in [Elsman 2003], but adjusted to treat type variable contexts properly.

Proposition 12 (Typing Closed Under Type Substitution). *If* $\Omega + \Delta, \Gamma \vdash e : \pi, \varphi$ *and* $\Omega \vdash S : \Delta$ *then* $\Omega, S(\Gamma) \vdash S(e) : S(\pi), S(\varphi)$.

Proof. By induction on the derivation of $\Omega + \Delta, \Gamma \vdash e : \pi, \varphi$. The cases for integers (values), pairs (values and expressions), projections (expressions), and identifiers are trivial.

Case $e = \langle \lambda x.e' \rangle^{\rho}$. From [TvLam], we have $\Omega + \Delta, \Gamma \vdash e : (\mu_1 \xrightarrow{\epsilon.\varphi} \mu_2, \rho), \emptyset$ and $\{\}, \{x : \mu_1\} \vdash e' : \mu_2, \varphi$ and $\vdash \pi$. Because $\text{ftv}(\pi, e', \varphi) \cap \text{dom}(S) = \emptyset$, we have $\{\}, \{x : S(\mu_1)\} \vdash S(e') : S(\mu_2), S(\varphi)$ and $\vdash S(\pi)$. Moreover, because $\text{frv}(\pi) = \text{frv}(S(\pi))$, we have $\text{frv}(S(\pi)) \models_{\text{v}} S(e')$. We can now apply [TvLam] to get $\Omega, S(\Gamma) \vdash S(e) : S(\pi), \emptyset$, as required.

Case $e = e_1\ e_2$. From [TeApp], we have $\Omega + \Delta, \Gamma \vdash e : \mu, \varphi_0 \cup \varphi_1 \cup \varphi_2 \cup \{\epsilon, \rho\}$ and $\Omega + \Delta, \Gamma \vdash e_1 : (\mu' \xrightarrow{\epsilon.\varphi_0} \mu, \rho), \varphi_1$ and $\Omega + \Delta, \Gamma \vdash e_2 : \mu', \varphi_2$. By induction we have $\Omega, S(\Gamma) \vdash S(e_1) : (S(\mu') \xrightarrow{S(\epsilon.\varphi_0)} S(\mu), S(\rho)), S(\varphi_1)$ and $\Omega, S(\Gamma) \vdash S(e_2) : S(\mu'), S(\varphi_2)$. It follows from the definition of type substitution that $S(\epsilon.\varphi_0) = \epsilon.\varphi_0$. We can now apply [TeApp] to get $\Omega, S(\Gamma) \vdash S(e) : S(\mu), S(\varphi)$, as required.

Case $e = \texttt{letregion}\ \rho\ \texttt{in}\ e'$. From [TeReg], we have $\Omega + \Delta, \Gamma \vdash e : \mu, \varphi \setminus \{\rho, \vec{\epsilon}\}$ and $\Omega + \Delta, \Gamma \vdash e' : \mu, \varphi$ and $\{\rho, \vec{\epsilon}\} \cap \text{frev}(\Gamma, \mu) = \emptyset$. By renaming of bound names and because ρ and $\vec{\epsilon}$ do not appear free in the concluding type judgment, we can assume $\{\rho, \vec{\epsilon}\} \cap \text{frev}(S(\Gamma), S(\mu)) = \emptyset$. By induction, we have $\Omega, S(\Gamma) \vdash S(e') : S(\mu), S(\varphi)$. We can now apply [TeReg], to get $\Omega, S(\Gamma) \vdash \texttt{letregion}\ \rho\ \texttt{in}\ S(e') : S(\mu), S(\varphi) \setminus \{\rho, \vec{\epsilon}\}$. It follows trivially that we have $\Omega, S(\Gamma) \vdash S(e) : S(\mu), S(\varphi \setminus \{\rho, \vec{\epsilon}\})$, as required.

Case $e = e'\ [\vec{\rho}]\ \texttt{at}\ \rho$. From [TeRApp], we have $\Omega + \Delta, \Gamma \vdash e' : (\sigma, \rho'), \varphi$ and $\Omega + \Delta \vdash \sigma \geq \tau$ via $\vec{\rho}$ and $\Omega \vdash \tau$. By induction, we have $\Omega, S(\Gamma) \vdash S(e') : (S(\sigma), S(\rho')), S(\varphi)$. From Proposition 7, we have $\Omega \vdash S(\sigma) \geq S(\tau)$ via $\vec{\rho}$, thus, from [TeRApp], we can conclude $\Omega, S(\Gamma) \vdash S(e) : S(\tau, \rho), S(\varphi \cup \{\rho, \rho'\})$, as required.

Case Rule [TeSub]. We have $\Omega + \Delta, \Gamma \vdash e : \pi, \varphi$ and $\Omega + \Delta, \Gamma \vdash e : \pi, \varphi'$ and $\varphi' \supseteq \varphi$. By induction. we have $\Omega, S(\Gamma) \vdash S(e) : S(\mu), S(\varphi)$. From the definition of type substitution, it follows that $\varphi' \supseteq \varphi$ implies $S(\varphi') \supseteq S(\varphi)$, thus, we can apply [TeSub] to get $\Omega, S(\Gamma) \vdash S(e) : S(\mu), S(\varphi')$, as required. □

Proposition 16 (Value Substitution). *If* $\Omega, \Gamma + \{x : \pi\} \vdash e : \pi', \varphi$ *and* $\vdash v : \pi$ *then* $\Omega, \Gamma \vdash e[v/x] : \pi', \varphi$.

Proof. By induction on the derivation $\Omega, \Gamma + \{x : \pi\} \vdash e : \pi', \varphi$.

Case $e = y$. From assumptions and [TeVar], we have $\Omega, \Gamma + \{x : \pi\} \vdash y : \pi', \varphi$ and $(\Gamma + \{x : \pi\})(y) = \pi'$ and $\varphi = \emptyset$. If $y \neq x$, we have $e[v/x] = y$, thus, because $\Gamma(y) = \pi'$, we can conclude from [TeVar] that $\Omega, \Gamma \vdash e[v/x] : \pi', \varphi$, as required. Otherwise, $y = x$, thus $e[v/x] = v$ and $\pi = \pi'$. From assumptions, [TeVal], and [TeSub], we have $\Omega, \Gamma \vdash e[v/x] : \pi', \varphi$, as required.

Case $e = \lambda y.e'$ at ρ. From assumptions and [TeLam], we have $\Omega, \Gamma + \{x : \pi, y : \mu\} \vdash e' : \mu', \varphi'$ and $\varphi = \{\rho\}$ and $\pi' = (\mu \xrightarrow{\epsilon.\varphi'} \mu', \rho)$. By renaming of bound variables, we can assume $x \neq y$, thus, we can apply the induction hypothesis to get $\Omega, \Gamma + \{y : \mu\} \vdash e'[v/x] : \mu', \varphi'$. By applying [TeLam], we have $\Omega, \Gamma \vdash \lambda y.e'[v/x] : \pi', \varphi$, as required.

The remaining cases follow similarly. □

Proposition 17 (Unique Decomposition). *If* $\vdash e : \pi, \varphi$, *then either (1) e is a value, or (2) there exist a unique* $E_{\varphi'}$, e', *and* π' *such that* $e = E_{\varphi'}[e']$ *and* $\vdash e' : \pi', \varphi \cup \varphi'$ *and* e' *is an instruction.*

Proof. By induction on the structure of e. Suppose e is not a value. There are 8 cases to consider. We proceed by case analysis.

Case $e =$ `letregion` ρ `in` e_1. A derivation $\vdash e : \pi, \varphi$ must end in a use of [TeReg] followed by a number of uses of [TeSub]. It follows that there exist φ_1 and φ_2 such that $\varphi = \varphi_1 \setminus \{\rho\} \cup \varphi_2$ and $\rho \notin \mathrm{frv}(\pi)$ and $\vdash e_1 : \pi, \varphi_1$. By renaming of bound variables, we can assume $\rho \notin \mathrm{frv}(\varphi_2)$. By induction, either e_1 is a value or there exist a unique $E'_{\varphi''}$, ι_1, and π'_1 such that $e_1 = E'_{\varphi''}[\iota_1]$ and $\vdash \iota_1 : \pi'_1, \varphi_1 \cup \varphi''$. If e_1 is not a value then we take $E_{\varphi'} =$ `letregion` ρ `in` $E'_{\varphi''}$, $\varphi' = \varphi'' \cup \{\rho\}$, $\iota = \iota_1$, $\pi' = \pi'_1$, and from [TeSub], we have $\vdash \iota_1 : \pi'_1, \varphi \cup \varphi'$, because $\varphi_1 \cup \varphi'' \subseteq \varphi \cup \varphi'$. Otherwise, $e_1 = v_1$ for some value v_1. Thus, $E_{\varphi'} = [\cdot]$, $\iota =$ `letregion` ρ `in` v_1, $\pi' = \pi$, and $\varphi' = \emptyset$.

Case $e = e_1\ e_2$. A derivation $\vdash e : \pi, \varphi$ must end in a use of [TeApp], followed by a number of uses of [TeSub]. It follows that there exist $\mu, \varphi_1, \varphi_2, \mu', \epsilon, \varphi_0$, and φ_3 such that $\varphi = \varphi_0 \cup \varphi_1 \cup \varphi_2 \cup \{\epsilon, \rho\} \cup \varphi_3$ and $\vdash e_1 : (\mu \xrightarrow{\epsilon.\varphi_0} \mu', \rho), \varphi_1$ and $\vdash e_2 : \mu, \varphi_2$ and $\pi = \mu'$. By induction, either e_1 is a value or else there exist $E'_{\varphi'_1}$, ι_1, and π'_1 such that $e_1 = E'_{\varphi'_1}[\iota_1]$ and $\vdash \iota_1 : \pi'_1, \varphi_1 \cup \varphi'_1$. If e_1 is not a value, then we take $E_{\varphi'} = E'_{\varphi'_1}\ e_2$, $\iota = \iota_1$, $\pi' = \pi'_1$, and because $\varphi' = \varphi'_1$ and $\varphi_1 \subseteq \varphi$, we can apply [TeSub] to get $\vdash \iota_1 : \pi'_1, \varphi \cup \varphi'$. Otherwise, $e_1 = v_1$ for some value v_1. We can now apply the induction hypothesis to get that either e_2 is a value or else there exist $E'_{\varphi'_2}$, ι_2, and π'_2 such that $e_2 = E'_{\varphi'_2}[\iota_2]$ and $\vdash \iota_2 : \pi'_2, \varphi_2 \cup \varphi'_2$. If e_2 is not a value, then we take $E_{\varphi'} = v_1\ E'_{\varphi'_2}$, $\iota = \iota_2$, $\pi' = \pi'_2$, and because $\varphi' = \varphi'_2$ and $\varphi_2 \subseteq \varphi$, we can apply [TeSub] to get $\vdash \iota_2 : \pi'_2, \varphi \cup \varphi'$. Otherwise $e_2 = v_2$ for some value v_2. Because $\vdash v_1 : (\mu \xrightarrow{\epsilon.\varphi_0} \mu', \rho), \varphi_1$, we can conclude from inspecting the typing rules for values (canonical forms) that $v_1 = \langle \lambda x.e' \rangle^{\rho}$. Thus, $E_{\varphi'} = [\cdot]$, $\varphi' = \emptyset$, $\iota = \langle \lambda x.e' \rangle^{\rho}\ v_2$, and $\pi' = \pi$.

The remaining 6 cases follow similarly. □

Proposition 18 (Type Preservation). *If* $\vdash e : \pi, \varphi$ *and* $e \xhookrightarrow{\varphi} e'$ *then* $\vdash e' : \pi, \varphi$.

Proof. By induction on the structure of e. We proceed by case analysis.

Case $e = \lambda x.e_0$ at ρ. From assumptions and [TeLam], we have $\pi = (\mu_1 \xrightarrow{\epsilon.\varphi_0} \mu_2, \rho)$ and $\{x : \mu_1\} \vdash e_0 : \mu_2, \varphi_0$ and $\vdash \pi$ and $G(\{\}, \{\}, e_0, \{x\}, \pi)$ and $\varphi = \{\rho\}$. From [Lam], we have $\rho \in \varphi$ and

$e' = \langle \lambda x.e_0 \rangle^\rho$. From definition (4), we have $\mathrm{frv}(\pi) \models_{\mathrm{v}} e_0$. Now, by use of [TvLam] and [TeSub], we have $\vdash e' : \pi, \varphi$, as required.

Case $e = \texttt{letregion}\ \rho\ \texttt{in}\ v$. From assumptions and from [TeReg], there exist φ' and μ such that $\varphi = \varphi' \setminus \{\rho\}$ and $\vdash v : \mu, \varphi'$ and $\pi = \mu$. It follows from [TeVal] that $\vdash v : \mu, \emptyset$, thus, from [Reg] and [TeSub], we have $\vdash e' : \pi, \varphi$, as required.

Case $e = \langle \lambda x.e_1 \rangle^\rho\ v$. From assumptions, [TeApp], and [TvLam], there exist μ, μ_1, ϵ, and φ_0 such that $\pi = \mu$ and $\{x : \mu_1\} \vdash e_1 : \mu, \varphi_0$ and $\vdash v : \mu_1, \varphi_1$, and $\varphi = \varphi_0 \cup \{\epsilon, \rho\}$. From [TeVal], we have $\vdash v : \mu_1, \emptyset$. Thus, from Proposition 16, we have $\vdash e_1[v/x] : \mu, \varphi_0$. Now, because $\varphi \supseteq \varphi_0$, we can apply [TeSub] to get $\vdash e' : \pi, \varphi$, as required.

Case $e = \langle \texttt{fun}\ f\ \texttt{[}\vec{\rho}\texttt{]}\ x = e_1 \rangle^\rho\ \texttt{[}\vec{\rho}\,'\texttt{]}\ \texttt{at}\ \rho'$. There are two possibilities. Either [TvFun] applies or [TvRec] applies.

case Rule [TvFun]. From assumptions, [TeRApp], and [TvFun], we have $\pi = (\tau, \rho')$, $\varphi = \{\rho, \rho'\}$, $v = \langle \texttt{fun}\ f\ \texttt{[}\vec{\rho}\texttt{]}\ x = e_1 \rangle^\rho$ and $\sigma = \forall \vec{\rho}\vec{\epsilon}\Delta.\mu_1 \xrightarrow{\epsilon.\varphi_0} \mu_2$, and

$$\vdash v : (\sigma, \rho) \tag{11}$$
$$\vdash \sigma \geq \tau \text{ via } \vec{\rho}\,' \tag{12}$$
$$\{\}, \{x : \mu_1\} \vdash e_1 : \mu_2, \varphi_0 \tag{13}$$

From (13), we have $f \notin \mathrm{fpv}(e_1)$, thus, we have

$$\{\}, \{x : \mu_1\} \vdash e_1[v/f] : \mu_2, \varphi_0 \tag{14}$$

From the definition of instantiation and from (12), there exists a substitution $S = (S^{\mathrm{t}}, [\vec{\rho}\,'/\vec{\rho}], S^{\mathrm{e}})$ such that

$$S(\mu_1 \xrightarrow{\epsilon.\varphi_0} \mu_2) = \tau \tag{15}$$
$$\{\} \vdash S^{\mathrm{t}} : \Delta \tag{16}$$

From (14) and [TeLam], we have

$$\vdash \lambda x.e_1[v/f]\ \texttt{at}\ \rho' : (\mu_1 \xrightarrow{\epsilon.\varphi_0} \mu_2, \rho'), \{\rho'\} \tag{17}$$

By renaming of bound names, we can assume $S(v) = v$ and $S(\rho') = \rho'$, thus, from (15), (16), (17), Proposition 11, and Proposition 12, we have $\vdash \lambda x.e_1[\vec{\rho}\,'/\vec{\rho}][v/f]\ \texttt{at}\ \rho' : (\tau, \rho'), \{\rho'\}$. We can now apply [TeSub] to get $\vdash e' : \pi, \varphi$, as required.

case Rule [TvRec]. From assumptions, [TeRApp], and [TvRec], we have $\pi = (\tau, \rho')$, $\varphi = \{\rho, \rho'\}$, $v = \langle \texttt{fun}\ f\ \texttt{[}\vec{\rho}\texttt{]}\ x = e_1 \rangle^\rho$ and $\sigma = \forall \vec{\rho}\vec{\epsilon}\Delta.\mu_1 \xrightarrow{\epsilon.\varphi_0} \mu_2$, and

$$\vdash v : (\sigma, \rho) \tag{18}$$
$$\sigma' = \forall \vec{\rho}\vec{\epsilon}.\mu_1 \xrightarrow{\epsilon.\varphi_0} \mu_2 \tag{19}$$
$$\vdash \sigma \geq \tau \text{ via } \vec{\rho}\,' \tag{20}$$
$$\{f : (\sigma', \rho)\}, x : \mu_1\} \vdash e_1 : \mu_2, \varphi_0 \tag{21}$$

From (18), (19), and [TvRec], we have

$$\vdash v : (\sigma', \rho) \tag{22}$$

From Proposition 16 and (22) and (21), we have

$$\{x : \mu_1\} \vdash e_1[v/f] : \mu_2, \varphi_0 \tag{23}$$

From the definition of instantiation and from (20), there exists a substitution $S = (S^{\text{t}}, [\vec{\rho}\,'/\vec{\rho}], S^{\text{e}})$ such that

$$S(\mu_1 \xrightarrow{\epsilon.\varphi_0} \mu_2) = \tau \tag{24}$$

$$\{\} \vdash S^{\text{t}} : \Delta \tag{25}$$

From (23) and [TeLam], we have

$$\vdash \lambda x.e_1[v/f] \texttt{ at } \rho' : (\mu_1 \xrightarrow{\epsilon.\varphi_0} \mu_2, \rho'), \{\rho'\} \tag{26}$$

By renaming of bound names, we can assume $S(v) = v$ and $S(\rho') = \rho'$, thus, from (24), (25), (26), Proposition 11, and Proposition 12, we have $\vdash \lambda x.e_1[\vec{\rho}\,'/\vec{\rho}][v/f] \texttt{ at } \rho' : (\tau, \rho'), \{\rho'\}$. We can now apply [TeSub] to get $\vdash e' : \pi, \varphi$, as required.

Case $e = \#1\ (v_1, v_2)$. From assumptions, [TeSel], and [TvPair], we have $\vdash v_1 : \mu, \emptyset$. We can now apply [TeSub] to get $\vdash v_1 : \mu, \varphi$, as required.

Case $e = E_{\varphi'}[e'']$. We have $e'' \xhookrightarrow{\varphi\cup\varphi'} e'''$ and $\varphi \cap \varphi' = \emptyset$ and $e' = E_{\varphi'}[e''']$. We now proceed by case analysis on the structure of $E_{\varphi'}$.

case $E_{\varphi'}[e''] = (e'', e_2) \texttt{ at } \rho$. We have $\varphi' = \emptyset$. From assumptions and [TePair] we have $\vdash e'' : \mu_1, \varphi_1$, $\vdash e_2 : \mu_2, \varphi_2$, $\mu = (\mu_1 \times \mu_2, \rho)$, and $\varphi = \varphi_1 \cup \varphi_2 \cup \{\rho\}$. By applying [TeSub], we have $\vdash e'' : \mu_1, \varphi$. We can now apply the induction hypothesis to get $\vdash e''' : \mu_1, \varphi$. By applying [TePair], we have $\vdash E_{\varphi'}[e'''] : \mu, \varphi$, as required.

case $E_{\varphi'}[e''] = (v_1, e'') \texttt{ at } \rho$. We have $\varphi' = \emptyset$. From assumptions and [TePair] we have $\vdash v_1 : \mu_1, \varphi_1$, $\vdash e'' : \mu_2, \varphi_2$, $\mu = (\mu_1 \times \mu_2, \rho)$, and $\varphi = \varphi_1 \cup \varphi_2 \cup \{\rho\}$. By applying [TeSub], we have $\vdash e'' : \mu_2, \varphi$. We can now apply the induction hypothesis to get $\vdash e''' : \mu_2, \varphi$. By applying [TePair], we have $\vdash E_{\varphi'}[e'''] : \mu, \varphi$, as required.

case $E_{\varphi'}[e''] = \#i\ e''$, $i \in \{1, 2\}$. We have $\varphi' = \emptyset$. From assumptions and [TeSel], we have $\vdash e'' : (\mu_1 \times \mu_2, \rho), \varphi'$, $\mu = \mu_i$ and $\varphi = \varphi' \cup \{\rho\}$. By applying [TeSub], we have $\vdash e'' : (\mu_1 \times \mu_2, \rho), \varphi$, thus, we can apply the induction hypothesis to get $\vdash e''' : (\mu_1 \times \mu_2, \rho), \varphi$. We can now apply [TeSel] to get $\vdash E_{\varphi'}[e'''] : \mu, \varphi$, as required.

case $E_{\varphi'}[e''] = \texttt{let } x = e'' \texttt{ in } e_2$. We have $\varphi' = \emptyset$. From assumptions and [TeLet], there exists π such that $\vdash e'' : \pi, \varphi_1$, $\{x : \pi\} \vdash e_2 : \mu, \varphi_2$, and $\varphi = \varphi_1 \cup \varphi_2$. Applying [TeSub], we have $\vdash e'' : \pi, \varphi$. By induction, we have $\vdash e''' : \pi, \varphi$. We can now apply [TeLet] to get $\vdash E_{\varphi'}[e'''] : \mu, \varphi$, as required.

case $E_{\varphi'}[e''] = e''\ e_2$. From assumptions and [TeApp], it follows that there exist ϵ, φ_0, φ_1, φ_2, and ρ such that $\vdash e'' : (\mu_2 \xrightarrow{\epsilon.\varphi_0} \mu, \rho), \varphi_1$, $\vdash e_2 : \mu_2, \varphi_2$, and $\varphi = \varphi_0 \cup \varphi_1 \cup \varphi_2 \cup \{\epsilon, \rho\}$. From [TeSub], we have $\vdash e'' : (\mu_2 \xrightarrow{\epsilon.\varphi_0} \mu, \rho), \varphi$, thus, by induction, we have $\vdash e''' : (\mu_2 \xrightarrow{\epsilon.\varphi_0} \mu, \rho), \varphi$. We can now apply [TeApp] to get $\vdash E_{\varphi'}[e'''] : \mu, \varphi$, as required.

case $E_{\varphi'}[e''] = v\ e''$. As above.

case $E_{\varphi'}[e''] = e''\ [\vec{\rho}] \texttt{ at } \rho$. As above.

case $E_{\varphi'}[e''] = \texttt{letregion}\ \rho\ \texttt{in}\ e''$. We have $\varphi' = \{\rho\}$. From assumptions and from [TeReg], there exist φ'' and $\vec{\epsilon}$ such that $\varphi = \varphi'' \setminus \{\rho, \vec{\epsilon}\}$, and $\vdash e'' : \mu, \varphi''$. From [TeSub], we have $\vdash e'' : \mu, \varphi \cup \varphi'$. We can now apply the induction hypothesis to get $\vdash e''' : \mu, \varphi \cup \varphi'$. Now, because $\varphi = (\varphi \cup \varphi') \setminus \{\rho, \vec{\epsilon}\}$, we can apply [TeReg] to get $\vdash E_{\varphi'}[e'''] : \mu, \varphi$, as required.

The remaining cases follow similarly. □

Proposition 19. (Progress). *If $\vdash e : \pi, \varphi$ then either e is a value or $e \xhookrightarrow{\varphi} e'$, for some e'.*

Proof. If e is not a value, then by Proposition 17 there exist a unique $E_{\varphi'}$, ι, and π' such that $e = E_{\varphi'}[\iota]$ and $\vdash \iota : \pi', \varphi \cup \varphi'$. We argue that $\iota \xhookrightarrow{\varphi\cup\varphi'} e_2$, for some e_2, so that $E_{\varphi'}[\iota] \xhookrightarrow{\varphi} E_{\varphi'}[e_2]$ follows from [Ctx]. We now consider all cases where ι could possibly be stuck.

Case $\iota = \lambda x.e_1'$ at ρ. We have $\vdash \lambda x.e_1'$ at $\rho : \pi', \varphi \cup \varphi'$. This derivation must be an application of [TeLam] followed by a number of applications of [TeSub]. Thus, we have $\rho \in \varphi \cup \varphi'$. It follows that we can apply [Lam] to get $e_2 = \langle \lambda x.e_1' \rangle^{\rho}$.

Case $\iota = \langle \lambda x.e_{\mathrm{x}} \rangle^{\rho}\ v$. We have $\vdash \langle \lambda x.e_{\mathrm{x}} \rangle^{\rho}\ v : \pi', \varphi \cup \varphi'$. This derivation must end in an application of [TeApp] followed by a number of applications of [TeSub]. Thus, by applying [TeVal], there exist μ, μ', ϵ, and φ_0 such that $\vdash \langle \lambda x.e_{\mathrm{x}} \rangle^{\rho} : (\mu \xrightarrow{\epsilon.\varphi_0} \mu', \rho), \emptyset$ and $\vdash v : \mu, \emptyset$ and $\pi' = \mu'$ and $\varphi_0 \cup \{\epsilon, \rho\} \subseteq \varphi \cup \varphi'$. Now, because $\rho \in \varphi \cup \varphi'$, we can apply [App] to get $e_2 = e_{\mathrm{x}}[v/x]$.

Case $\iota = \langle \texttt{fun}\ f\ \texttt{[}\vec{\rho}\texttt{]}\ x = e_0 \rangle^{\rho'}\ \texttt{[}\vec{\rho}'\texttt{]}$ at ρ. The derivation $\vdash \iota : \pi', \varphi \cup \varphi'$ must end in an application of [TeRapp] followed by a number of applications of [TeSub], thus, from [TeVal], there exist σ and τ' such that $\pi' = (\tau', \rho)$ and

$$\vdash \langle \texttt{fun}\ f\ \texttt{[}\vec{\rho}\texttt{]}\ x = e_0 \rangle^{\rho'} : (\sigma, \rho'), \emptyset \tag{27}$$

$$\{\rho, \rho'\} \subseteq \varphi \cup \varphi' \tag{28}$$

Because $\rho' \in \varphi \cup \varphi'$ follows from (28), we can apply [Rapp] to get $e_2 = \lambda x.e_0[\vec{\rho}\,'/\vec{\rho}][v/f]$ at ρ, where $v = \langle \texttt{fun}\ f\ \texttt{[}\vec{\rho}\texttt{]}\ x = e_0 \rangle^{\rho'}$.

Case $\iota = \texttt{letregion}\ \rho\ \texttt{in}\ v$. It follows immediately from [Reg] that $e_2 = v$.

The remaining cases follow similarly. □

Received 2022-11-10; accepted 2023-03-31