Superficially Substructural Types (Technical Appendix)

Neelakantan R. Krishnaswami
MPI-SWS
neelk@mpi-sws.org

Aaron Turon
Northeastern University
turon@ccs.neu.edu

Derek Dreyer
MPI-SWS
dreyer@mpi-sws.org

Deepak Garg
MPI-SWS
dg@mpi-sws.org

March 2012

Contents

1 The Language

1.1 Syntax

Sorts	σ	::=	$\mathbb{N} \mid 1 \mid \sigma \times \sigma \mid 2 \mid \mathsf{Loc} \mid \sigma \to \sigma \mid \sigma_\perp \mid \mathsf{seq}\ \sigma \mid \mathcal{P}(\sigma)$
Index Terms	t	::=	$n \mid t + t \mid t \times t$
		$\mid$	$\langle\rangle \mid \langle t, t\rangle \mid \pi_1 t \mid \pi_2 t$
		$\mid$	$\mathsf{tt} \mid \mathsf{ff} \mid \mathsf{if}(t, t, t)$
		$\mid$	$\lambda X : \sigma.\ t \mid t\ u$
		$\mid$	$\lfloor t \rfloor \mid \perp \mid \mathsf{case}(t, \perp \to t, \lfloor X \rfloor \to t)$
		$\mid$	$\epsilon \mid t :: t \mid \mathsf{fold}(t, \epsilon \to t, X :: Y \to t)$
		$\mid$	$\{X : \sigma \mid P\}$
		$\mid$	$t \in t \mid t > t \mid t = t$
Propositions	P, Q	::=	$\top \mid P \wedge Q \mid P \supset Q \mid \perp \mid P \vee Q \mid \forall X : \sigma.\ P \mid \exists X : \sigma.\ P$
		$\mid$	$t = u \mid t > u \mid t \in t$
Kinds	κ	::=	$\circ \mid \sigma \to \kappa$
Types	A	::=	$1 \mid A \otimes B \mid A \multimap B \mid\ !A \mid \mathsf{ptr}\ t \mid \mathsf{cap}\ t\ A$
		$\mid$	$\forall X : \sigma :: P.\ A \mid \exists X : \sigma :: P.\ A \mid \forall \alpha : \kappa.\ A \mid \exists \alpha : \kappa.\ A$
		$\mid$	$\mathsf{bool}\ t \mid \mathsf{nat}\ t \mid [A]$
		$\mid$	$\mathsf{if}(t, A, B) \mid \alpha \mid \lambda X : \sigma.\ A \mid A\ t$
Terms	e	::=	$x \mid \langle\rangle \mid \langle e, e'\rangle \mid \mathsf{let}\ \langle x, y\rangle = e\ \mathsf{in}\ e'$
		$\mid$	$\lambda x.\ e \mid e\ e' \mid\ !e \mid \mathsf{let}\ !x = e\ \mathsf{in}\ e'$
		$\mid$	$\mathsf{new}(e) \mid \mathsf{get}_{e'}\ e \mid e :=_{e''} e' \mid \mathsf{fix}\ f(x).\ e \mid \mathsf{share}(e, \overline{v_i})$
		$\mid$	$\mathsf{tt} \mid \mathsf{ff} \mid \mathsf{if}(e, e_1, e_2) \mid$
		$\mid$	$n \mid \mathsf{case}(e, 0 \to e_1, \mathsf{s}\ x \to e_2)$
		$\mid$	$[e] \mid \bullet$
Eval Contexts	E	::=	$[\,] \mid \langle E, e\rangle \mid \langle v, E\rangle \mid \mathsf{let}\ \langle x, y\rangle = E\ \mathsf{in}\ e$
		$\mid$	$E\ e \mid v\ E \mid\ !E \mid \mathsf{let}\ !x = E\ \mathsf{in}\ e \mid \mathsf{if}(E, e_1, e_2)$
		$\mid$	$\mathsf{new}(E) \mid \mathsf{get}_e\ E \mid \mathsf{get}_E\ v \mid E :=_{e'} e \mid v :=_{e'} E \mid v :=_E v'$
		$\mid$	$\mathsf{case}(E, 0 \to e_1, \mathsf{s}\ x \to e_2) \mid \mathsf{share}(E, v)$
Values	v	::=	$\langle\rangle \mid \langle v, v'\rangle \mid \lambda x.\ e \mid \lambda X : \sigma.\ e \mid\ !v \mid \ell \mid \mathsf{fix}\ f(x).\ e \mid x \mid \bullet \mid \mathsf{tt} \mid \mathsf{ff} \mid n$
Heaps	h	::=	$\cdot \mid h, \ell : v$

Contexts

Index/Type	Σ	::=	$\cdot \mid \Sigma, \alpha : \kappa \mid \Sigma, X : \sigma$
Proposition	Π	::=	$\cdot \mid \Pi, P$
Unrestricted	Γ	::=	$\cdot \mid \Gamma, x : A$
Linear	Δ	::=	$\cdot \mid \Delta, x : A$

1.2 Typing

$$\boxed{\Sigma \vdash A : \kappa}$$

$$\frac{\alpha : \kappa \in \Sigma}{\Sigma \vdash \alpha : \kappa} \qquad \frac{\Sigma \vdash A : \sigma \to \kappa \qquad \Sigma \rhd t : \sigma}{\Sigma \vdash A\ t : \kappa} \qquad \frac{\Sigma, X : \sigma \vdash A : \kappa}{\Sigma \vdash \lambda X : \sigma.\ A : \sigma \to \kappa} \qquad \frac{\Sigma, \alpha : \kappa \vdash A : \circ}{\Sigma \vdash \forall \alpha : \kappa.\ A : \circ}$$

$$\frac{\Sigma, X : \sigma \vdash A : \circ \qquad \Sigma, X : \sigma \rhd P : \mathsf{prop} \qquad Q \in \{\forall, \exists\}}{\Sigma \vdash Q\ X : \sigma :: P.\ A : \circ} \qquad \frac{\Sigma \vdash A : \circ \qquad \Sigma \vdash B : \circ}{\Sigma \vdash A \otimes B : \circ} \qquad \frac{\Sigma \vdash A : \circ \qquad \Sigma \vdash B : \circ}{\Sigma \vdash A \multimap B : \circ}$$

$$\frac{}{\Sigma \vdash 1 : \circ} \qquad \frac{\Sigma \rhd t : \mathsf{Loc}}{\Sigma \vdash \mathsf{ptr}\ t : \circ} \qquad \frac{\Sigma \rhd t : \mathsf{Loc} \qquad \Sigma \vdash A : \circ}{\Sigma \vdash \mathsf{cap}\ t\ A : \circ} \qquad \frac{\Sigma \vdash A : \circ}{\Sigma \vdash !A : \circ} \qquad \frac{\Sigma \rhd t : 2}{\Sigma \vdash \mathsf{bool}\ t : \circ} \qquad \frac{\Sigma \rhd t : \mathbb{N}}{\Sigma \vdash \mathsf{nat}\ t : \circ}$$

$$\frac{\Sigma \rhd t : 2 \qquad \Sigma \vdash A : \kappa \qquad \Sigma \vdash B : \kappa}{\Sigma \vdash \mathsf{if}(t, A, B) : \kappa}$$

$$\boxed{\Sigma \rhd P : \mathsf{prop}}$$

$$\frac{\Sigma \rhd P : \mathsf{prop} \qquad \Sigma \rhd Q : \mathsf{prop} \qquad \oplus \in \{\vee, \wedge, \supset\}}{\Sigma \rhd P \oplus Q : \mathsf{prop}} \qquad \frac{c \in \{\top, \bot\}}{\Sigma \rhd c : \mathsf{prop}} \qquad \frac{\Sigma, X : \sigma \rhd P : \mathsf{prop} \qquad Q \in \{\forall, \exists\}}{\Sigma \rhd Q\ X : \sigma.\ P : \mathsf{prop}}$$

$$\frac{\Sigma \rhd t : \sigma \qquad \Sigma \rhd u : \sigma}{\Sigma \rhd t = u : \mathsf{prop}} \qquad \frac{\Sigma \rhd t : \mathbb{N} \qquad \Sigma \rhd u : \mathbb{N}}{\Sigma \rhd t > u : \mathsf{prop}} \qquad \frac{\Sigma \rhd t : \sigma \qquad \Sigma \rhd u : \mathcal{P}(\sigma)}{\Sigma \rhd t \in u : \mathsf{prop}}$$

$$\boxed{\Sigma; \Pi \vdash P}$$

(rules of first-order logic)

$$\boxed{\Sigma \vdash \Pi\ \mathsf{ok}}$$

$$\frac{}{\Sigma \vdash \cdot\ \mathsf{ok}} \qquad \frac{\Sigma \vdash \Pi\ \mathsf{ok} \qquad \Sigma \rhd P : \mathsf{prop}}{\Sigma \vdash \Pi, P\ \mathsf{ok}}$$

$$\boxed{\Sigma \vdash \Gamma\ \mathsf{ok}}$$

$$\frac{}{\Sigma \vdash \cdot\ \mathsf{ok}} \qquad \frac{\Sigma \vdash \Gamma\ \mathsf{ok} \qquad \Sigma \vdash A : \circ}{\Sigma \vdash \Gamma, x : A\ \mathsf{ok}}$$

$$\boxed{\Sigma \vdash \Delta\ \mathsf{ok}}$$

$$\frac{}{\Sigma \vdash \cdot\ \mathsf{ok}} \qquad \frac{\Sigma \vdash \Delta\ \mathsf{ok} \qquad \Sigma \vdash A : \circ}{\Sigma \vdash \Delta, x : A\ \mathsf{ok}}$$

$$\boxed{\Sigma; \Pi \vdash A \equiv B : \kappa}$$

(Standard congruence rules omitted)

$$\frac{\Sigma \vdash A : \kappa}{\Sigma; \Pi \vdash A \equiv A : \kappa} \qquad \frac{\Sigma; \Pi \vdash A \equiv B : \kappa}{\Sigma; \Pi \vdash B \equiv A : \kappa} \qquad \frac{\Sigma; \Pi \vdash A \equiv B : \kappa \qquad \Sigma; \Pi \vdash B \equiv C : \kappa}{\Sigma; \Pi \vdash A \equiv C : \kappa}$$

$$\frac{\Sigma; \Pi \vdash A \equiv B : \kappa \qquad \Sigma, \alpha : \kappa \vdash C : \kappa'}{\Sigma; \Pi \vdash [A/\alpha]C \equiv [B/\alpha]C : \kappa'} \qquad \frac{\Sigma; \Pi \vdash t =_\sigma u \qquad \Sigma, X : \sigma \vdash A : \kappa'}{\Sigma; \Pi \vdash [t/X]A \equiv [u/X]A : \kappa'}$$

$$\frac{\Sigma \vdash (\lambda X : \sigma.\ A)\ t : \kappa}{\Sigma; \Pi \vdash (\lambda X : \sigma.\ A)\ t \equiv [t/X]A : \kappa} \qquad \frac{\Sigma, X : \sigma; \Pi \vdash A\ X \equiv B\ X : \kappa}{\Sigma; \Pi \vdash A \equiv B : \sigma \to \kappa}$$

$$\frac{\Sigma \vdash \mathsf{if}(\mathsf{tt}, A, B) : \kappa}{\Sigma; \Pi \vdash \mathsf{if}(\mathsf{tt}, A, B) \equiv A : \kappa} \qquad \frac{\Sigma \vdash \mathsf{if}(\mathsf{ff}, A, B) : \kappa}{\Sigma; \Pi \vdash \mathsf{if}(\mathsf{ff}, A, B) \equiv B : \kappa} \qquad \frac{\Sigma \rhd t : 2 \qquad \Sigma, X : 2 \vdash A : \kappa}{\Sigma; \Pi \vdash \mathsf{if}(t, [\mathsf{tt}/X]A, [\mathsf{ff}/X]A) \equiv [t/X]A : \kappa}$$

$$\frac{\Sigma, X : \sigma; \Pi \vdash P \iff Q \qquad \Sigma \vdash \forall X : \sigma :: P.\ A : \circ}{\Sigma; \Pi \vdash \forall X : \sigma :: P.\ A \equiv \forall X : \sigma :: Q.\ A : \circ} \qquad \frac{\Sigma, X : \sigma; \Pi \vdash P \iff Q \qquad \Sigma \vdash \exists X : \sigma :: P.\ A : \circ}{\Sigma; \Pi \vdash \exists X : \sigma :: P.\ A \equiv \exists X : \sigma :: Q.\ A : \circ}$$

$$\frac{\Sigma \vdash \forall X : \sigma :: P.\ (A \otimes B) : \circ \qquad X \notin \mathrm{FV}(B)}{\Sigma; \Pi \vdash (\forall X : \sigma :: P.\ A) \otimes B \equiv \forall X : \sigma :: P.\ (A \otimes B) : \circ} \qquad \frac{\Sigma \vdash \exists X : \sigma :: P.\ (A \otimes B) : \circ \qquad X \notin \mathrm{FV}(B)}{\Sigma; \Pi \vdash (\exists X : \sigma :: P.\ A) \otimes B \equiv \exists X : \sigma :: P.\ (A \otimes B) : \circ}$$

$$\frac{\Sigma \vdash A : \circ \qquad \Sigma \rhd t : \mathsf{Loc}}{\Sigma; \Pi \vdash \mathsf{cap}\ t\ A \equiv [\mathsf{cap}\ t\ A] : \circ} \qquad \frac{\Sigma \vdash A : \circ}{\Sigma; \Pi \vdash [[A]] \equiv [A] : \circ} \qquad \frac{\Sigma, X : \sigma \vdash A : \circ \qquad \Sigma, X : \sigma \rhd P : \mathsf{prop}}{\Sigma; \Pi \vdash \exists X : \sigma :: P.\ [A] \equiv [\exists X : \sigma :: P.\ A] : \circ}$$

$$\frac{\Sigma \vdash A : \circ \qquad \Sigma \vdash B : \circ}{\Sigma; \Pi \vdash [A \otimes B] \equiv [B \otimes A] : \circ} \qquad \frac{\Sigma; \Pi \vdash [A] \equiv [A'] : \circ \qquad \Sigma; \Pi \vdash [B] \equiv [B'] : \circ}{\Sigma; \Pi \vdash [A \otimes B] \equiv [A' \otimes B'] : \circ}$$

$$\boxed{\Sigma; \Pi; \Gamma; \Delta \vdash e : A}$$

$$\frac{\Sigma \vdash \Pi\ \mathsf{ok} \qquad \Sigma \vdash \Gamma\ \mathsf{ok} \qquad \Sigma \vdash \Delta\ \mathsf{ok} \qquad x : A \in \Delta}{\Sigma; \Pi; \Gamma; \Delta \vdash x : A} \qquad \frac{\Sigma \vdash \Pi\ \mathsf{ok} \qquad \Sigma \vdash \Gamma\ \mathsf{ok} \qquad \Sigma \vdash \Delta\ \mathsf{ok} \qquad x : A \in \Gamma}{\Sigma; \Pi; \Gamma; \Delta \vdash x : A}$$

$$\frac{\Sigma \vdash \Pi\ \mathsf{ok} \qquad \Sigma \vdash \Gamma\ \mathsf{ok} \qquad \Sigma \vdash \Delta\ \mathsf{ok} \qquad \Sigma \vdash \cdot\ \mathsf{ok}}{\Sigma; \Pi; \Gamma; \Delta \vdash \langle\rangle : 1}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta_1 \vdash e_1 : A \qquad \Sigma; \Pi; \Gamma; \Delta_2 \vdash e_2 : B}{\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \vdash \langle e_1, e_2 \rangle : A \otimes B} \qquad \frac{\Sigma; \Pi; \Gamma; \Delta_1 \vdash e : A \otimes B \qquad \Sigma; \Pi; \Gamma; \Delta_2, x : A, y : B \vdash e' : C}{\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \vdash \mathsf{let}\ \langle x, y \rangle = e\ \mathsf{in}\ e' : C}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta, x : A \vdash e : B}{\Sigma; \Pi; \Gamma; \Delta \vdash \lambda x.\ e : A \multimap B} \qquad \frac{\Sigma; \Pi; \Gamma; \Delta_1 \vdash e : A \multimap B \qquad \Sigma; \Pi; \Gamma; \Delta_2 \vdash e' : A}{\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \vdash e\ e' : B}$$

$$\frac{\Sigma; \Pi; \Gamma; \cdot \vdash v : A}{\Sigma; \Pi; \Gamma; \cdot \vdash !v : !A} \qquad \frac{\Sigma; \Pi; \Gamma; \Delta_1 \vdash e : !A \qquad \Sigma; \Pi; \Gamma, x : A; \Delta_2 \vdash e' : C}{\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \vdash \mathsf{let}\ !x = e\ \mathsf{in}\ e' : C}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta \vdash e : A}{\Sigma; \Pi; \Gamma; \Delta \vdash \mathsf{new}(e) : \exists \ell : \mathsf{Loc} :: \top.\ !\mathsf{ptr}\ l \otimes \mathsf{cap}\ \ell\ A} \qquad \frac{\Sigma; \Pi; \Gamma; \Delta \vdash e : \mathsf{ptr}\ t \qquad \Sigma; \Pi; \Gamma; \Delta' \vdash e' : \mathsf{cap}\ t\ A}{\Sigma; \Pi; \Gamma; \Delta, \Delta' \vdash \mathsf{get}_{e'}\ e : A \otimes \mathsf{cap}\ t\ 1}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta_1 \vdash e : \mathsf{ptr}\ t \qquad \Sigma; \Pi; \Gamma; \Delta_2 \vdash e' : A \qquad \Sigma; \Pi; \Gamma; \Delta_3 \vdash e'' : \mathsf{cap}\ t\ 1}{\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2, \Delta_3 \vdash e :=_{e''} e' : \mathsf{cap}\ t\ A} \qquad \frac{\Sigma; \Pi; \Gamma, f : A \multimap B; x : A \vdash e : B}{\Sigma; \Pi; \Gamma; \cdot \vdash \mathsf{fix}\ f(x).\ e : A \multimap B}$$

$$\frac{}{\Sigma; \Pi; \Gamma; \Delta \vdash \mathsf{tt} : \mathsf{bool}\ \mathsf{tt}} \qquad \frac{}{\Sigma; \Pi; \Gamma; \Delta \vdash \mathsf{ff} : \mathsf{bool}\ \mathsf{ff}}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta \vdash e : \mathsf{bool}\ t \qquad \Sigma; \Pi, t = \mathsf{tt}; \Gamma; \Delta' \vdash e_1 : C \qquad \Sigma; \Pi, t = \mathsf{ff}; \Gamma; \Delta' \vdash e_2 : C}{\Sigma; \Pi; \Gamma; \Delta, \Delta' \vdash \mathsf{if}(e, e_1, e_2) : C} \qquad \frac{}{\Sigma; \Pi; \Gamma; \Delta \vdash n : \mathsf{nat}\ n}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta_1 \vdash e : \mathsf{nat}\ t \qquad \Sigma; \Pi, t = 0; \Gamma; \Delta_2 \vdash e_1 : C \qquad \Sigma, X : \mathbb{N}; \Pi, t = \mathsf{s}\ X; \Gamma; \Delta_2, x : \mathsf{nat}\ X \vdash e_2 : C}{\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \vdash \mathsf{case}(e, 0 \to e_1, \mathsf{s}\ x \to e_2) : C}$$

$\boxed{\Sigma; \Pi; \Gamma; \Delta \vdash e : A}$ ... continued

$$\frac{\Sigma; \Pi; \Gamma; \Delta \vdash v : A}{\Sigma; \Pi; \Gamma; \Delta \vdash \bullet : [A]}$$

$$\frac{\Sigma, X : \sigma; \Pi, P; \Gamma; \Delta \vdash v : A \qquad i \notin \mathrm{FV}(\Pi), \mathrm{FV}(\Gamma), \mathrm{FV}(\Delta)}{\Sigma; \Pi; \Gamma; \Delta \vdash v : \forall X : \sigma :: P.\ A}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta \vdash e : \forall X : \sigma :: P.\ A \qquad \Sigma \rhd t : \sigma \qquad \Sigma; \Pi \vdash [t/X]P}{\Sigma; \Pi; \Gamma; \Delta \vdash e : [t/X]A}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta \vdash e : [t/X]A \qquad \Sigma \rhd t : \sigma \qquad \Sigma; \Pi \vdash [t/X]P}{\Sigma; \Pi; \Gamma; \Delta \vdash e : \exists X : \sigma :: P.\ A}$$

$$\frac{\begin{array}{c}\Sigma, X : \sigma; \Pi, P; \Gamma; \Delta, x : A \vdash e : C \\ \Sigma; \Pi; \Gamma; \Delta' \vdash v : \exists X : \sigma :: P.\ A \qquad X \notin \mathrm{FV}(\Pi), \mathrm{FV}(\Gamma), \mathrm{FV}(\Delta), \mathrm{FV}(\Delta'), \mathrm{FV}(C)\end{array}}{\Sigma; \Pi; \Gamma; \Delta, \Delta' \vdash [v/x]e : C}$$

$$\frac{\Sigma, \alpha : \kappa; \Pi; \Gamma; \Delta \vdash v : B \qquad \alpha \notin \mathrm{FV}(\Gamma), \mathrm{FV}(\Delta)}{\Sigma; \Pi; \Gamma; \Delta \vdash v : \forall \alpha : \kappa.\ B} \qquad \frac{\Sigma; \Pi; \Gamma; \Delta \vdash e : \forall \alpha : \kappa.\ B \qquad \Sigma \vdash A : \kappa}{\Sigma; \Pi; \Gamma; \Delta \vdash e : [A/\alpha]B}$$

$$\frac{\Sigma \vdash A : \kappa \qquad \Sigma, \alpha : \kappa \vdash B : \circ \qquad \Sigma; \Pi; \Gamma; \Delta \vdash e : [A/\alpha]B}{\Sigma; \Pi; \Gamma; \Delta \vdash e : \exists \alpha : \kappa.\ B}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta \vdash v : \exists \alpha : \kappa.\ B \qquad \Sigma, \alpha : \kappa; \Pi; \Gamma; \Delta', x : B \vdash e : C \qquad \alpha \notin \mathrm{FV}(\Delta'), \mathrm{FV}(\Delta), \mathrm{FV}(\Gamma), \mathrm{FV}(C)}{\Sigma; \Pi; \Gamma; \Delta, \Delta' \vdash [v/x]e : C}$$

$$\frac{\Sigma; \Pi; \Gamma; \Delta \vdash e : A \qquad \Sigma; \Pi \vdash A \equiv B : \circ}{\Sigma; \Pi; \Gamma; \Delta \vdash e : B}$$

$$\frac{\Sigma; \Pi \vdash P \vee Q \qquad \Sigma; \Pi, P; \Gamma; \Delta \vdash e : A \qquad \Sigma; \Pi, Q; \Gamma; \Delta \vdash e : A \qquad \Sigma \vdash A : \circ}{\Sigma; \Pi; \Gamma; \Delta \vdash e : A}$$

$$\frac{\Sigma; \Pi \vdash \exists X : \sigma.\ P \qquad \Sigma, X : \sigma; \Pi, P; \Gamma; \Delta \vdash e : A \qquad \Sigma \vdash A : \circ}{\Sigma; \Pi; \Gamma; \Delta \vdash e : A} \qquad \frac{\Sigma; \Pi \vdash \bot \qquad \Sigma \vdash A : \circ}{\Sigma; \Pi; \Gamma; \Delta \vdash e : A}$$

1.3 Sharing Construct

$$\frac{\Sigma \vdash A : \sigma \to \circ \qquad \Sigma; \Pi; \Gamma; \Delta \vdash e : [A\ t] \qquad \Sigma; \Pi \vdash \mathrm{monoid}_\sigma(\epsilon, (\cdot)) \qquad \Sigma; \Pi; \Gamma; \cdot \vdash v_i : [A/\alpha]\mathrm{specT}_i}{\Sigma; \Pi; \Gamma; \Delta \vdash \mathsf{share}(e, \overline{v_i}) : \exists \alpha : \sigma \to \circ.\ [\alpha\ t] \otimes \overline{!\mathrm{specT}_i} \otimes !\mathrm{splitT} \otimes !\mathrm{joinT} \otimes !\mathrm{promoteT}}$$

where

$$\begin{array}{rcl}
\mathrm{specT}_i & = & \forall X : \sigma.\ \forall Y : \sigma_i' :: P_i.\ B_i \otimes [\alpha\ (t_i \cdot X)] \multimap \\
& & \quad \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [\alpha\ (t_i' \cdot X)] \\
& & \quad \text{where } X, \alpha \notin \mathrm{FV}(P_i), \mathrm{FV}(Q_i), \mathrm{FV}(B_i), \mathrm{FV}(C_i), \mathrm{FV}(t_i), \mathrm{FV}(t_i') \\
\mathrm{splitT} & = & \forall X, Y : \sigma.\ [\alpha\ (X \cdot Y)] \multimap [\alpha\ X] \otimes [\alpha\ Y] \\
\mathrm{joinT} & = & \forall X, Y : \sigma.\ [\alpha\ X] \otimes [\alpha\ Y] \multimap [\alpha\ (X \cdot Y)] \\
\mathrm{promoteT} & = & \forall X : \sigma :: X = X \cdot X.\ [\alpha\ X] \multimap ![\alpha\ X] \\
\mathrm{monoid}_\sigma(\epsilon, (\cdot)) & = & \forall X : \sigma.\ \epsilon \cdot X = X \wedge \\
& & \forall X, Y : \sigma.\ X \cdot Y = Y \cdot X \wedge \\
& & \forall X, Y, Z : \sigma.\ (X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)
\end{array}$$

1.4 Operational Semantics

$$
\begin{array}{ll}
\langle h; \mathsf{let}\ \langle\rangle = \langle\rangle\ \mathsf{in}\ e\rangle & \hookrightarrow \langle h; e\rangle \\
\langle h; \mathsf{let}\ \langle x_1, x_2\rangle = \langle v_1, v_2\rangle\ \mathsf{in}\ e\rangle & \hookrightarrow \langle h; [v_1/x_1, v_2/x_2]e\rangle \\
\langle h; (\lambda x.\ e)\ v\rangle & \hookrightarrow \langle h; [v/x]e\rangle \\
\langle h; \mathsf{let}\ !x = !v\ \mathsf{in}\ e\rangle & \hookrightarrow \langle h; [v/x]e\rangle \\
\langle h; \mathsf{new}(v)\rangle & \hookrightarrow \langle h \uplus [\ell : v]; \langle !\ell, \bullet\rangle\rangle \\
\langle h \uplus [\ell : v]; \mathsf{get}_\bullet\ \ell\rangle & \hookrightarrow \langle h \uplus [\ell : \langle\rangle]; \langle v, \bullet\rangle\rangle \\
\langle h \uplus [\ell : \langle\rangle]; \ell :=_\bullet v\rangle & \hookrightarrow \langle h \uplus [\ell : v]; \bullet\rangle \\
\langle h; (\mathsf{fix}\ f(x).\ e)\ v\rangle & \hookrightarrow \langle h; [\mathsf{fix}\ f(x).\ e/f, v/x]e\rangle \\
\langle h; [e]\rangle & \hookrightarrow \langle h; \bullet\rangle \\
\langle h; \mathsf{if}(\mathsf{tt}, e, e')\rangle & \hookrightarrow \langle h; e\rangle \\
\langle h; \mathsf{if}(\mathsf{ff}, e, e')\rangle & \hookrightarrow \langle h; e'\rangle \\
\langle h; \mathsf{case}(0, 0 \to e, \mathsf{s}\ x \to e')\rangle & \hookrightarrow \langle h; e\rangle \\
\langle h; \mathsf{case}(\mathsf{s}\ v, 0 \to e, \mathsf{s}\ x \to e')\rangle & \hookrightarrow \langle h; [v/x]e'\rangle
\end{array}
$$

$$
\begin{array}{lll}
\langle h; \mathsf{share}(v, \overline{v_i})\rangle & & \hookrightarrow \left\langle h \uplus [\ell : \mathsf{ff}]; \left\langle \langle\rangle, \overline{!\mathrm{op}_i}, !\mathrm{split}, !\mathrm{join}, !\mathrm{promote}\right\rangle\right\rangle \\
\quad \text{where} \quad \mathrm{op}_i & = & \lambda x.\ \mathsf{let}\ \langle \mathit{flag}, \_\rangle = \mathsf{get}_\bullet\ \ell\ \mathsf{in} \\
 & & \quad \mathsf{let}\ \_ = \ell :=_\bullet \mathsf{tt}\ \mathsf{in} \\
 & & \quad \mathsf{if}\ \mathit{flag} \\
 & & \quad \mathsf{then}\ (\mathsf{fix}\ f(x).\ f\ x)\ \langle\rangle \\
 & & \quad \mathsf{else}\ \mathsf{let}\ y = v_i\ x\ \mathsf{in} \\
 & & \qquad \mathsf{let}\ \_ = \ell :=_\bullet \mathsf{ff}\ \mathsf{in} \\
 & & \qquad y \\
\mathrm{split} & = & \lambda x.\ \langle \bullet, \bullet\rangle \\
\mathrm{join} & = & \lambda x.\ \bullet \\
\mathrm{promote} & = & \lambda x.\ !\bullet
\end{array}
$$

$$\frac{\langle h; e\rangle \hookrightarrow \langle h'; e'\rangle}{\langle h; E[e]\rangle \hookrightarrow \langle h'; E[e']\rangle}$$

2 Semantics

2.1 Semantics of Sorts and Kinds

$$
\begin{array}{lcl}
\mathcal{S}[\![-]\!] & : & \mathrm{Sort} \to \mathrm{Set} \\
\mathcal{S}[\![\mathbb{N}]\!] & = & \mathbb{N} \\
\mathcal{S}[\![1]\!] & = & \{*\} \\
\mathcal{S}[\![\sigma \times \sigma']\!] & = & \mathcal{S}[\![\sigma]\!] \times \mathcal{S}[\![\sigma']\!] \\
\mathcal{S}[\![\sigma \to \sigma']\!] & = & \mathcal{S}[\![\sigma]\!] \to \mathcal{S}[\![\sigma']\!] \\
\mathcal{S}[\![2]\!] & = & \{\mathsf{tt}, \mathsf{ff}\} \\
\mathcal{S}[\![\sigma_\perp]\!] & = & \{\perp\} + \mathcal{S}[\![\sigma]\!] \\
\mathcal{S}[\![\mathsf{seq}\ \sigma]\!] & = & \{x_1 \cdot \ldots \cdot x_k \mid x_i \in \mathcal{S}[\![\sigma]\!]\} \\
\mathcal{S}[\![\mathcal{P}(\sigma)]\!] & = & \mathcal{P}(\mathcal{S}[\![\sigma]\!])
\end{array}
$$

$$
\begin{array}{lcl}
\mathcal{K}[\![-]\!] & : & \mathrm{Kind} \to \mathrm{Set} \\
\mathcal{K}[\![\circ]\!] & = & \mathrm{ValPred} \\
\mathcal{K}[\![\sigma \to \kappa]\!] & = & \mathcal{S}[\![\sigma]\!] \to \mathcal{K}[\![\kappa]\!]
\end{array}
$$

2.2 Logical Semantics

2.2.1 Entailment Relation

The models relation $\models_\Sigma$ is a subset of $\{(\rho, P) \mid \rho \in \mathrm{Env}(\Sigma) \wedge \Sigma \rhd P : \mathsf{prop}\}$

$$
\begin{array}{lcl}
\rho \models_\Sigma \top & \iff & \text{always} \\
\rho \models_\Sigma P \wedge Q & \iff & \rho \models_\Sigma P \text{ and } \rho \models_\Sigma Q \\
\rho \models_\Sigma P \supset Q & \iff & \text{if } \rho \models_\Sigma P \text{ then } \rho \models_\Sigma Q \\
\rho \models_\Sigma \bot & \iff & \text{never} \\
\rho \models_\Sigma P \vee Q & \iff & \rho \models_\Sigma P \text{ or } \rho \models_\Sigma Q \\
\rho \models_\Sigma \forall X : \sigma.\ P & \iff & \forall d \in \mathcal{S}[\![\sigma]\!].\ \rho[X \mapsto d] \models_{\Sigma, X:\sigma} P \\
\rho \models_\Sigma \exists X : \sigma.\ P & \iff & \exists d \in \mathcal{S}[\![\sigma]\!].\ \rho[X \mapsto d] \models_{\Sigma, X:\sigma} P \\
\rho \models_\Sigma t = u : \sigma & \iff & \mathcal{I}[\![\Sigma \rhd t : \sigma]\!]\rho = \mathcal{I}[\![\Sigma \rhd u : \sigma]\!]\rho \\
\rho \models_\Sigma t > u : \sigma & \iff & \mathcal{I}[\![\Sigma \rhd t : \sigma]\!]\rho > \mathcal{I}[\![\Sigma \rhd u : \sigma]\!]\rho \\
\rho \models_\Sigma t \in u : \sigma & \iff & \mathcal{I}[\![\Sigma \rhd t : \sigma]\!]\rho \in \mathcal{I}[\![\Sigma \rhd u : \sigma]\!]\rho
\end{array}
$$

2.3 Worlds

$$
\begin{array}{rcl}
\text{World}_n & \stackrel{\text{def}}{=} & \left\{ W = (k, \omega) \;\middle|\; \begin{array}{l} k < n, \exists j.\ \omega \in \text{Island}_k^{j+1} \\ \omega[0] = \text{HIsland}_k \end{array} \right\} \\
\text{Island}_n & \stackrel{\text{def}}{=} & \left\{ \iota = (M, \cdot, \epsilon, I, E) \;\middle|\; \begin{array}{l} (M, \cdot, \epsilon) \text{ commutative monoid}, \\ I \in M \to \text{ResPred}_n \\ E \in \text{EnvPred}(M) \end{array} \right\} \\
\text{HIsland}_n & \stackrel{\text{def}}{=} & \left(\begin{array}{l} \text{Heap}_\bot, \uplus, \emptyset, \\ \lambda h.\{(W, \epsilon) \mid W \in \text{World}_n, h \neq \bot\}, \\ \text{Heap}_\bot \end{array} \right) \\
\text{ResPred}_n & \stackrel{\text{def}}{=} & \left\{ \varphi \subseteq \text{ResAtom}_n \;\middle|\; \begin{array}{rl} \forall W' \sqsupseteq W.\ (W, r) \in \varphi \\ \implies & (W', r) \in \varphi \end{array} \right\} \\
\text{ResAtom}_n & \stackrel{\text{def}}{=} & \left\{ (W, r) \;\middle|\; \begin{array}{l} W \in \text{World}_n,\ \forall i.\ a_i \in W.\omega[i].M, \\ r = (a_0, \ldots, a_{m-1}), m = |W.\omega| \end{array} \right\} \\
\text{EnvPred}(M) & \stackrel{\text{def}}{=} & \{E \subseteq M \mid \forall a \in E, a \in M.\ a \cdot a' \in E\} \\
\text{ValPred} & \stackrel{\text{def}}{=} & \left\{ V \subseteq \text{ValAtom} \;\middle|\; \begin{array}{l} \forall W' \sqsupseteq W.\ (W, r, v) \in V \\ \Rightarrow \forall r'.(W', r \cdot r', v) \in V \end{array} \right\} \\
\text{ValAtom} & \stackrel{\text{def}}{=} & \{(W, r, v) \mid \exists n.\ (W, r) \in \text{ResAtom}_n\}
\end{array}
$$

$$
\begin{array}{rcl}
\triangleright(k+1, \omega) & \stackrel{\text{def}}{=} & (k, \lfloor \omega \rfloor_k) \\
\lfloor (\iota_1, \ldots, \iota_n) \rfloor_k & \stackrel{\text{def}}{=} & (\lfloor \iota_1 \rfloor_k, \ldots, \lfloor \iota_n \rfloor_k) \\
\lfloor (M, \cdot, \epsilon, I, E) \rfloor_k & \stackrel{\text{def}}{=} & (M, \cdot, \epsilon, \lambda a. \lfloor I(a) \rfloor_k, E) \\
\lfloor \varphi \rfloor_k & \stackrel{\text{def}}{=} & \{(W, r) \in \varphi \mid W.k < k\}
\end{array}
$$

$$
\begin{array}{rcl}
(\iota'_1, \ldots, \iota'_{n'}) \sqsupseteq (\iota_1, \ldots, \iota_n) & \stackrel{\text{def}}{=} & n' \geq n,\ \ \forall i \leq n.\ \iota'_i = \iota_i \\
(k', \omega') \sqsupseteq_j (k, \omega) & \stackrel{\text{def}}{=} & k' = k - j,\ \ \omega' \sqsupseteq \lfloor \omega \rfloor_{k'} \\
(k', \omega') \sqsupseteq (k, \omega) & \stackrel{\text{def}}{=} & \exists j.\ ((k', \omega') \sqsupseteq_j (k, \omega))
\end{array}
$$

$$
\begin{array}{rcl}
(s, r, r_{\text{F}}) : W & \stackrel{\text{def}}{=} & s = s_0 \cdot \ldots \cdot s_{m-1},\ m = |W.\omega|, \\
& & \forall i \in 0 \ldots (m-1). \\
& & \quad (\triangleright W, s_i) \in W.\omega[i].I((s \cdot r \cdot r_{\text{F}})[i]) \wedge \\
& & \quad r_{\text{F}}[i] \in W.\omega[i].E
\end{array}
$$

$$
\begin{array}{rcl}
r'' \sqsupseteq r & \stackrel{\text{def}}{=} & \exists r'.\ r'' = r \cdot r' \\
|r| & \stackrel{\text{def}}{=} & r[0] \\
\langle h; e \rangle \hookrightarrow_j \langle h'; e' \rangle & \stackrel{\text{def}}{=} & \exists D :: (\langle h; e \rangle \hookrightarrow^* \langle h'; e' \rangle) \wedge |D| \leq j
\end{array}
$$

2.4 Semantics of Types

$$
\begin{array}{rcl}
\mathcal{V}[\![\Sigma \vdash A : \kappa]\!] & : & \mathrm{Env}(\Sigma) \to \mathcal{K}[\![\kappa]\!] \\
\mathcal{V}[\![\Sigma \vdash 1 : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, \langle\rangle)\} \\
\mathcal{V}[\![\Sigma \vdash A_1 \otimes A_2 : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r_1 \cdot r_2, \langle v_1, v_2\rangle) \mid (W, r_1, v_1) \in \mathcal{V}[\![A_1]\!]\rho \wedge (W, r_2, v_2) \in \mathcal{V}[\![A_2]\!]\rho\} \\
\mathcal{V}[\![\Sigma \vdash A \multimap B : \circ]\!]\rho & \stackrel{\text{def}}{=} & \left\{(W, r, v) \;\middle|\; \begin{array}{c} \forall W' \sqsupseteq W.\, \forall (W', r', v') \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho. \\ (W', r \cdot r', v\ v') \in \mathcal{E}[\![\Sigma \vdash B : \circ]\!]\rho \end{array}\right\} \\
\mathcal{V}[\![\Sigma \vdash\ !A : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r \cdot r', !v) \mid (W, r, v) \in \mathcal{V}[\![A]\!]\rho \wedge r = r \cdot r\} \\
\mathcal{V}[\![\Sigma \vdash \mathsf{ptr}\ t : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, \ell) \mid \ell = \mathcal{I}[\![t]\!]\rho\} \\
\mathcal{V}[\![\Sigma \vdash \mathsf{cap}\ t\ A : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r \cdot [\ell : v], \bullet) \mid \ell = \mathcal{I}[\![t]\!]\rho \wedge (W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho\} \\
\mathcal{V}[\![\Sigma \vdash \forall X : \sigma :: P.\ A : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, v) \mid \forall d \in \mathcal{S}[\![\sigma]\!].\ \rho[X \mapsto d] \models P \Longrightarrow (W, r, v) \in \mathcal{V}[\![\Sigma, X : \sigma \vdash A : \circ]\!]\rho[X \mapsto d]\} \\
\mathcal{V}[\![\Sigma \vdash \exists X : \sigma :: P.\ A : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, v) \mid \exists d \in \mathcal{S}[\![\sigma]\!].\ \rho[X \mapsto d] \models P \wedge (W, r, v) \in \mathcal{V}[\![\Sigma, X : \sigma \vdash A : \circ]\!]\rho[X \mapsto d]\} \\
\mathcal{V}[\![\Sigma \vdash \forall \alpha : \kappa.\ A : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, v) \mid \forall V \in \mathcal{K}[\![\kappa]\!].\ (W, r, v) \in \mathcal{V}[\![\Sigma, \alpha : \kappa \vdash A : \circ]\!]\rho[\alpha \mapsto V]\} \\
\mathcal{V}[\![\Sigma \vdash \exists \alpha : \kappa.\ A : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, v) \mid \exists V \in \mathcal{K}[\![\kappa]\!].\ (W, r, v) \in \mathcal{V}[\![\Sigma, \alpha : \kappa \vdash A : \circ]\!]\rho[\alpha \mapsto V]\} \\
\mathcal{V}[\![\Sigma \vdash \alpha : \circ]\!]\rho & \stackrel{\text{def}}{=} & \rho(\alpha) \\
\mathcal{V}[\![\Sigma \vdash \mathsf{bool}\ t : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, d) \mid d = \mathcal{I}[\![t]\!]\rho\} \\
\mathcal{V}[\![\Sigma \vdash \mathsf{nat}\ t : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, d) \mid d = \mathcal{I}[\![t]\!]\rho\} \\
\mathcal{V}[\![\Sigma \vdash [A] : \circ]\!]\rho & \stackrel{\text{def}}{=} & \{(W, r, \bullet) \mid \exists v.\ (W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho\} \\
\mathcal{V}[\![\Sigma \vdash \mathsf{if}(t, A, B) : \kappa]\!]\rho & \stackrel{\text{def}}{=} & \begin{cases} \mathcal{V}[\![\Sigma \vdash A : \kappa]\!]\rho & \mathcal{I}[\![t]\!]\rho = \mathsf{tt} \\ \mathcal{V}[\![\Sigma \vdash B : \kappa]\!]\rho & \mathcal{I}[\![t]\!]\rho = \mathsf{ff} \end{cases} \\
\mathcal{V}[\![\lambda X : \sigma.\ A]\!]\rho & \stackrel{\text{def}}{=} & \lambda d \in \mathcal{S}[\![\sigma]\!].\ \mathcal{V}[\![\Sigma, X : \sigma \vdash A : \circ]\!]\rho[X \mapsto d] \\
\mathcal{V}[\![\Sigma \vdash A\ t : \kappa]\!]\rho & \stackrel{\text{def}}{=} & (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \kappa]\!]\rho)(\mathcal{I}[\![t]\!]\rho)
\end{array}
$$

$$
\mathcal{E}[\![A]\!]\rho \stackrel{\text{def}}{=} \left\{(W, r, e) \;\middle|\; \begin{array}{ll} \text{if} & j < W.k, \quad (s, r, r_{\mathrm{F}}) : W, \quad \langle |s \cdot r \cdot r_{\mathrm{F}}|; e\rangle \hookrightarrow_j \langle h; e'\rangle \not\hookrightarrow \\ \text{then} & W' \sqsupseteq_j W,\ (s', r', r'_{\mathrm{F}}) : W',\ h = |s' \cdot r' \cdot r'_{\mathrm{F}}|,\ r'_{\mathrm{F}} \sqsupseteq r_{\mathrm{F}},\ (W', r', e') \in \mathcal{V}[\![A]\!]\rho \end{array}\right\}
$$

2.5 Semantics of Contexts

$$
\begin{array}{rcl}
\mathrm{Env}(\cdot) & \stackrel{\text{def}}{=} & \emptyset \\
\mathrm{Env}(\Sigma, \alpha : \kappa) & \stackrel{\text{def}}{=} & \{\rho, \alpha \mapsto V \mid \rho \in \mathrm{Env}(\Sigma),\ V \in \mathcal{K}[\![\kappa]\!]\} \\
\mathrm{Env}(\Sigma, X : \sigma) & \stackrel{\text{def}}{=} & \{\rho, X \mapsto d \mid \rho \in \mathrm{Env}(\Sigma),\ d \in \mathcal{S}[\![\sigma]\!]\}
\end{array}
$$

Substitutions for unrestricted context Defined by induction over a derivation of $\Sigma \vdash \Gamma\ \mathsf{ok}$.

$$
\begin{array}{rcl}
\mathcal{U}[\![\Sigma \vdash \cdot\ \mathsf{ok}]\!]\ \rho\ W & \stackrel{\text{def}}{=} & \{\cdot\} \\
\mathcal{U}[\![\Sigma \vdash \Gamma, x : A\ \mathsf{ok}]\!]\ \rho\ W & \stackrel{\text{def}}{=} & \{\gamma, x \mapsto (r, v) \mid \gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W \wedge (W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho \wedge r = r \cdot r\}
\end{array}
$$

Substitutions for linear context Defined by induction over a derivation of $\Sigma \vdash \Delta\ \mathsf{ok}$.

$$
\begin{array}{rcl}
\mathcal{L}[\![\Sigma \vdash \cdot\ \mathsf{ok}]\!]\ \rho\ W & \stackrel{\text{def}}{=} & \{\cdot\} \\
\mathcal{L}[\![\Sigma \vdash \Delta, x : A\ \mathsf{ok}]\!]\ \rho\ W & \stackrel{\text{def}}{=} & \{\delta, x \mapsto (r, v) \mid \delta \in \mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W \wedge (W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho\}
\end{array}
$$

Functions $\pi(\gamma)$ and $\pi(\delta)$ For $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$, define $\pi(\gamma)$ to be the monoidal product of the first components of all elements in the range of γ. Similarly, define $\pi(\delta)$ for $\delta \in \mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W$.

2.6 Semantics of Typing Judgments

Suppose $\Sigma \vdash \Gamma\ \mathsf{ok}$ and $\Sigma \vdash \Delta\ \mathsf{ok}$. We say that $\Sigma; \Pi; \Gamma; \Delta \Vdash e : A$, if for every W, $\rho \in \mathrm{Env}(\Sigma)$, $\rho \models_\Sigma \Pi$, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$ and $\delta \in \mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W$, it is the case that $(W, \pi(\gamma) \cdot \pi(\delta), \delta(\gamma(e))) \in \mathcal{E}[\![A]\!]\rho$.

Similarly, we say that $\Sigma; \Pi; \Gamma; \Delta \Vdash^{\mathrm{V}} v : A$, if for every W, $\rho \in \mathrm{Env}(\Sigma)$, $\rho \models_\Sigma \Pi$, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$ and $\delta \in \mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W$, it is the case that $(W, \pi(\gamma) \cdot \pi(\delta), \delta(\gamma(v))) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$.

3 Differences from the Paper

The definition of the model presented in the previous section differs slightly from, but is *more general* than, the definition of the model presented in the paper that this Appendix accompanies. First, in this Appendix, each island contains a set E (the environment invariant), which constrains the possible frame resources that are allowed on the island in the definition of $\mathcal{E}[\![A]\!]\rho$, but no such set exists in the definition of island in the paper. This additional set is included here because we expect it to be useful in encoding more advanced forms of state transition systems in our model, which we want to explore in future work. Because the paper omits this environment invariant E, it also conflates r and r_{F} in the satisfaction relation at worlds: Instead of defining a quaternary relation $(s, r, r_{\mathrm{F}}) : W$ as in this Appendix, the paper defines a ternary relation $(s, r') : W$ and instantiates r' with $r \cdot r_{\mathrm{F}}$ in the definition of $\mathcal{E}[\![A]\!]\rho$. A second point of difference is that the definition of $\mathcal{E}[\![A]\!]\rho$ provided in this Appendix existentially quantifies over a new environment resource r'_{F}, which extends the initial environment resource r_{F}, but in the definition in the paper, $r'_{\mathrm{F}} = r_{\mathrm{F}}$. A third difference between the two is notational: This Appendix uses the notation $(W, r, v) \in \mathcal{V}[\![A]\!]\rho$, whereas the paper writes the same definition as $(r, v) \in \mathcal{V}[\![A]\!]^W_\rho$.

Modulo the notational difference, it is easy to show that the definitions of $\mathcal{V}[\![A]\!]\rho$ and $\mathcal{E}[\![A]\!]\rho$ in the paper equate to the respective definitions in this Appendix if we force the environment's invariant in each island to be the entire monoid of the island. This justifies why the model in this Appendix is more general than the model in the paper. Furthermore, the only construction of E in the soundness proof of the next section sets E equal to the entire monoid, so the soundness proof here also implies soundness w.r.t. the slightly different model in the paper.

4 Fundamental Theorem and Soundness

Lemma 1. *Well-formedness If* $\Sigma; \Pi; \Gamma; \Delta \vdash e : A$, *then* $\Sigma \vdash \Gamma\ \mathsf{ok}$ *and* $\Sigma \vdash \Delta\ \mathsf{ok}$.

Proof. By simultaneous induction on typing and kinding derivations. □

Futures Let $a \in \mathcal{K}[\![\kappa]\!]$. We define $\mathrm{futures}(a) \in \mathcal{K}[\![\kappa]\!]$ by induction on κ as follows:

$$\begin{aligned} \mathrm{futures}(a \in \mathcal{K}[\![\circ]\!]) &\stackrel{\mathrm{def}}{=} \{(W', r, v) \mid (W', r, v) \in a \wedge W' \sqsupseteq W\} \\ \mathrm{futures}(f \in \mathcal{K}[\![\sigma \to \kappa]\!]) &\stackrel{\mathrm{def}}{=} \lambda x \in \mathcal{S}[\![\sigma]\!].\ \mathrm{futures}(f\ x) \end{aligned}$$

Lemma 2 (World monotonicity)**.** *The following hold:*

1. $a \in \mathcal{V}[\![\Sigma \vdash A : \kappa]\!]\rho$ *implies* $\mathrm{futures}(a) = a$
2. $W' \sqsupseteq W$ *implies* $\mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W \subseteq \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W'$
3. $W' \sqsupseteq W$ *implies* $\mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W \subseteq \mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W'$

Proof. (1) follows by induction on the given derivation of $\Sigma \vdash A : \kappa$. The interesting case of type variables α follows from the restriction that every element in $\mathcal{K}[\![\circ]\!]$ is future-closed. (2) and (3) are trivial consequences of (1) at $\kappa = \circ$, using the definitions of $\mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$ and $\mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W$. □

Lemma 3 (Resource shifting)**.** *If* $(s, r \cdot r', r_{\mathrm{F}}) : W$, *then* $(s, r, r' \cdot r_{\mathrm{F}}) : W$.

Proof. Let $m = |W.\omega|$. To show $(s, r, r' \cdot r_{\mathrm{F}}) : W$, we need to show two things: (G1) $s = s_0 \cdot \ldots \cdot s_{m-1}$ and for every $i \in \{0, \ldots, m-1\}$, $(\triangleright W, s_i) \in W.\omega[i].I(s[i] \cdot r[i] \cdot r'[i] \cdot r_{\mathrm{F}}[i])$, and (G2) For every $i \in \{0, \ldots, m-1\}$, $r_{\mathrm{F}}[i] \cdot res'[i] \in W.\omega[i].E$. (G1) is exactly the corresponding statement of invariance satisfaction for the given relation $(s, r \cdot r', r_{\mathrm{F}}) : W$. (G2) follows because the given relation $(s, r \cdot r', r_{\mathrm{F}}) : W$ implies that $r_{\mathrm{F}}[i] \in W.\omega[i].E$ and E is closed under extensions. □

Resource Futures Let $a \in \mathcal{K}[\![\kappa]\!]$. We define $\mathrm{rfutures}(a) \in \mathcal{K}[\![\kappa]\!]$ by induction on κ as follows:

$$\begin{array}{rcl} \mathrm{rfutures}(a \in \mathcal{K}[\![\circ]\!]) & \stackrel{\text{def}}{=} & \{(W, r', v) \mid (W, r, v) \in a \wedge r' \sqsupseteq r\} \\ \mathrm{rfutures}(f \in \mathcal{K}[\![\sigma \to \kappa]\!]) & \stackrel{\text{def}}{=} & \lambda x \in \mathcal{S}[\![\sigma]\!].\ \mathrm{rfutures}(f\ x) \end{array}$$

Lemma 4 (Resource monotonicity)**.** *The following hold:*

1. *If* $(W, r, e) \in \mathcal{E}[\![A]\!]\rho$ *and* $r_1 \sqsupseteq r$*, then* $(W, r_1, e) \in \mathcal{E}[\![A]\!]\rho$*.*
2. *If* $a \in \mathcal{V}[\![\Sigma \vdash A : \kappa]\!]\rho$*, then* $\mathrm{rfutures}(a) = a$

Proof. (1) is proved as follows. Because $r_1 \sqsupseteq r$, there is some r_2 such that $r_1 = r \cdot r_2$. Following the definition of $(W, r_1, e) \in \mathcal{E}[\![A]\!]\rho$, assume that $j < W.k$, $(s, r \cdot r_2, r_{\mathrm{F}}) : W$ and $\langle |s \cdot r \cdot r_2 \cdot r_{\mathrm{F}}|; e\rangle \hookrightarrow_j \langle h; e'\rangle \not\hookrightarrow$. Now observe that $(s, r \cdot r_2, r_{\mathrm{F}}) : W$ implies $(s, r, r_{\mathrm{F}} \cdot r_2) : W$ by Lemma 3, so instantiating the definition of $(W, r, e) \in \mathcal{E}[\![A]\!]\rho$ with $r = r$, $r_{\mathrm{F}} = r_{\mathrm{F}} \cdot r_2$, $s = s$, we get $W' \sqsupseteq_j W$, $(s', r', r'_{\mathrm{F}}) : W'$, $\sigma = |s' \cdot r' \cdot r'_{\mathrm{F}}|$, $r'_{\mathrm{F}} \sqsupseteq r_{\mathrm{F}} \cdot r_2$ and $(W', r'_{\mathrm{F}}, e') \in \mathcal{V}[\![A]\!]\rho$. It remains only to show that $r'_{\mathrm{F}} \sqsupseteq r_{\mathrm{F}}$, but this follows trivially from $r'_{\mathrm{F}} \sqsupseteq r_{\mathrm{F}} \cdot r_2$.

(2) follows by induction on kinding judgments. For the case of $A \multimap B$, we use (1). □

Lemma 5 (Value inclusion)**.** *If* $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$*, then* $(W, r, v) \in \mathcal{E}[\![A]\!]\rho$*.*

Proof. Since $\langle |s \cdot r \cdot r_{\mathrm{F}}|; v\rangle \hookrightarrow_0 \langle |s \cdot r \cdot r_{\mathrm{F}}|; v\rangle \not\hookrightarrow$, we can choose $W' = W$, $s' = s$, $r' = r$ and $r'_{\mathrm{F}} = r_{\mathrm{F}}$ in the definition $\mathcal{E}[\![A]\!]\rho$ to obtain the result. □

Lemma 6 (Evaluation cut)**.** *If* $\Sigma; \Pi; \Gamma; \Delta_1 \Vdash e : A$ *and* $\Sigma; \Pi; \Gamma; \Delta_2, x : A \Vdash E[x] : B$*, then* $\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \Vdash E[e] : B$*.*

Proof. We want to show that $\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \Vdash E[e] : B$. Following the definition of $\Vdash$, assume a W, $\rho \in \mathrm{Env}(\Sigma)$, $\rho \models_\Sigma \Pi$, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$ and $\delta \in \mathcal{L}[\![\Sigma \vdash \Delta_1, \Delta_2\ \mathsf{ok}]\!]\ \rho\ W$. From the last fact, we know that there are δ_1, δ_2 such that $\delta_1 \in \mathcal{L}[\![\Sigma \vdash \Delta_1\ \mathsf{ok}]\!]\ \rho\ W$ and $\delta_2 \in \mathcal{L}[\![\Sigma \vdash \Delta_2\ \mathsf{ok}]\!]\ \rho\ W$. We want to show that $(W, \pi(\gamma) \cdot \pi(\delta_1) \cdot \pi(\delta_2), \delta_2(\delta_1(\gamma(E[e])))) \in \mathcal{E}[\![B]\!]\rho$, or, equivalently, $(W, \pi(\gamma) \cdot \pi(\delta_1) \cdot \pi(\delta_2), \delta_2(\gamma(E))[\delta_1(\gamma(e))]) \in \mathcal{E}[\![B]\!]\rho$. For ease of notation, define

1. $r_0 = \pi(\gamma)$, $r_1 = \pi(\delta_1)$ and $r_2 = \pi(\delta_2)$

Then, we want to show that $(W, r_0 \cdot r_1 \cdot r_2, \delta_2(\gamma(E))[\delta_1(\gamma(e))]) \in \mathcal{E}[\![B]\!]\rho$. Note that because $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$,

2. $r_0 \cdot r_0 = r_0$

Expanding the definition of $\mathcal{E}[\![B]\!]\rho$, pick $j < W.k$, s and r_{F} such that

3. $(s, r_0 \cdot r_1 \cdot r_2, r_{\mathrm{F}}) : W$
4. $\langle |r_0 \cdot r_1 \cdot r_2|; \delta_2(\gamma(E))[\delta_1(\gamma(e))]\rangle \hookrightarrow_j \langle h'; e'\rangle \not\hookrightarrow$

It follows immediately that there are $\hat{e}$, $\hat{h}$, j_1, j_2 such that

5. $j_1 + j_2 = j$
6. $\langle |r_0 \cdot r_1 \cdot r_2|; \delta_1(\gamma(e))\rangle \hookrightarrow_{j_1} \left\langle \hat{h}; \hat{e} \right\rangle \not\hookrightarrow$
7. $\left\langle \hat{h}; \delta_2(\gamma(E))[\hat{e}] \right\rangle \hookrightarrow_{j_2} \langle h'; e'\rangle \not\hookrightarrow$

From the assumption $\Sigma; \Pi; \Gamma; \Delta_1 \Vdash e : A$, we know that $(W, r_0 \cdot r_1, \gamma(\delta_1(e))) \in \mathcal{E}[\![A]\!]\rho$. Instantiating the definition of $\mathcal{E}[\![A]\!]\rho$ with $W = W$, $r = r_0 \cdot r_1$, $j = j_1$, $s = s$, $r_{\mathrm{F}} = r_{\mathrm{F}} \cdot r_2 \cdot r_0$ and fact 6, we obtain $\hat{W}$, $\hat{s}$, $\hat{r}$, $\hat{r_{\mathrm{F}}}$ such that:

8. $\hat{W} \sqsupseteq_{j_1} W$
9. $(\hat{s}, \hat{r}, \hat{r_{\mathrm{F}}}) : \hat{W}$
10. $\hat{h} = |\hat{s} \cdot \hat{r} \cdot \hat{r_{\mathrm{F}}}|$
11. $\hat{r_{\mathrm{F}}} \sqsupseteq r_{\mathrm{F}} \cdot r_2 \cdot r_0$
12. $(\hat{W}, \hat{r}, \hat{e}) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$ (This forces $\hat{e}$ to be a value, say $\hat{v}$)

From fact 11, there must be a $\hat{r_{\mathrm{F}}}'$ such that

13. $\hat{r_{\mathrm{F}}} = r_{\mathrm{F}} \cdot r_2 \cdot r_0 \cdot \hat{r_{\mathrm{F}}}'$

From the assumption $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$, fact 8 and Lemma 2(2), we get that

14. $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ \hat{W}$

Similarly, from the assumption $\delta_2 \in \mathcal{L}[\![\Sigma \vdash \Delta_2\ \mathsf{ok}]\!]\ \rho\ W$, fact 8 and Lemma 2(3), we get that

15. $\delta_2 \in \mathcal{L}[\![\Sigma \vdash \Delta_2\ \mathsf{ok}]\!]\ \rho\ \hat{W}$

This, together with fact 12 implies that:

16. $(\delta_2, x \mapsto (\hat{r}, \hat{v})) \in \mathcal{L}[\![\Sigma \vdash \Delta_2, x : A\ \mathsf{ok}]\!]\ \rho\ \hat{W}$

Using facts 14 and 16 with the definition of $\Sigma; \Pi; \Gamma; \Delta_2, x : A \Vdash E[x] : B$, we derive that $(\hat{W}, \pi(\gamma) \cdot \pi(\delta_2) \cdot \hat{r}, \delta_2(\gamma(E))[\hat{v}]) \in \mathcal{E}[\![B]\!]\rho$. Equivalently, $(\hat{W}, r_0 \cdot r_2 \cdot \hat{r}, \delta_2(\gamma(E))[\hat{v}]) \in \mathcal{E}[\![B]\!]\rho$. We now wish to instantiate the definition of $\mathcal{E}[\![B]\!]\rho$ with $W = \hat{W}$, $j = j_2$, $r = r_0 \cdot r_2 \cdot \hat{r}$, $r_{\mathrm{F}} = r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}' \cdot r_0$, $s = \hat{s}$ and fact 7. To do that, we must check the following:

(G1) $j_2 < \hat{W}.k$

(G2) $\hat{h} = |\hat{s} \cdot r_0 \cdot r_2 \cdot \hat{r} \cdot r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}' \cdot r_0|$

(G3) $(\hat{s}, r_0 \cdot r_2 \cdot \hat{r}, r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}' \cdot r_0) : \hat{W}$

We prove all three facts below:

Proof of (G1): From fact 8, we know that $W.k = \hat{W}.k + j_1$. Since $j_1 + j_2 = j$, we get $\hat{W}.k - j_2 = W.k - j$. Since $j < W.k$ by assumption, $\hat{W}.k - j_2 > 0$, as required.

Proof of (G2): From facts 10 and 21, we get $\hat{h} = |\hat{s} \cdot \hat{r} \cdot r_{\mathrm{F}} \cdot r_2 \cdot r_0 \cdot \hat{r_{\mathrm{F}}}'|$. The result follow immediately from fact 2 ($r_0 \cdot r_0 = r_0$).

Proof of (G3): Following the definition of $(\hat{s}, r_0 \cdot r_2 \cdot \hat{r}, r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}' \cdot r_0) : \hat{W}$, we need to prove two propositions: (a) $(\triangleright\hat{W}, \hat{s}) \in \mathrm{inv}(\hat{W}, r_0 \cdot r_2 \cdot \hat{r} \cdot r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}' \cdot r_0)$, and (b) $r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}' \cdot r_0 \in \mathrm{env}(\hat{W})$. We can rewrite (a) as $(\triangleright\hat{W}, \hat{s}) \in \mathrm{inv}(\hat{W}, \hat{r} \cdot \hat{r_{\mathrm{F}}})$, which follows immediately from fact 18.

To prove (b), we must show that for every $j < |\hat{W}.\omega|$, $(r_0 \cdot r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}')[j] \in \hat{W}.\omega[j].E$. We now consider two cases: $j < |W.\omega|$ and $j \geq |W.\omega|$. For $j < |W.\omega|$, we know from fact 3 that $r_{\mathrm{F}}[j] \in W.\omega[j].E$. Because $W.\omega[j].E$ is closed under extensions, $(r_0 \cdot r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}')[j] \in W.\omega[j].E$. Finally, because $\hat{W} \sqsupseteq W$, $W.\omega[j] = \hat{W}.\omega[j]$, so we derive the required $(r_0 \cdot r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}')[j] \in \hat{W}.\omega[j].E$. For $j \geq |W.\omega|$, $r_0 \cdot r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}'[j] = \hat{r_{\mathrm{F}}}'[j] = \hat{r_{\mathrm{F}}}[j]$ (because r_0, r_{F}, r_2 only contribute units at indexes beyond $|W.\omega|$), so we only need to show that $\hat{r_{\mathrm{F}}}[j] \in \hat{W}.\omega[j].E$. This follows from fact 18.

Having proved (G1)–(G3), we instantiate the definition of $\mathcal{E}[\![B]\!]\rho$ with $W = \hat{W}$, $j = j_2$, $r = r_0 \cdot r_2 \cdot \hat{r}$, $r_{\mathrm{F}} = r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}' \cdot r_0$, $s = \hat{s}$ and fact 7. This yields W', s', r', r'_{F} such that:

17. $W' \sqsupseteq_{j_2} \hat{W}$

18. $(s', r', r'_{\mathrm{F}}) : W'$

19. $h' = |s' \cdot r' \cdot r'_{\mathrm{F}}|$

20. $r'_{\mathrm{F}} \sqsupseteq r_{\mathrm{F}} \cdot \hat{r_{\mathrm{F}}}' \cdot r_0$

21. $(W', r', e') \in \mathcal{V}[\![\Sigma \vdash B : \circ]\!]\rho$ (This forces e' to be a value, say v')

It remains only to check that (a) $W' \sqsupseteq_j W$ and (b) $r'_{\mathrm{F}} \sqsupseteq r_{\mathrm{F}}$. (a) follows from facts 8, 17 and $j = j_1 + j_2$. (b) follows from fact 20. □

Lemma 7 (World stepping)**.** *For every world W, $\triangleright^n W \sqsupseteq_n W$.*

Proof. We only need to show that $\triangleright W \sqsupseteq_1 W$. The rest follows by induction on n. To prove $\triangleright W \sqsupseteq_1 W$, suppose that $W = (k+1, \omega)$. Then, $\triangleright W = (k, \lfloor\omega\rfloor_k)$. It suffices to show that $(k, \lfloor\omega\rfloor_k) \sqsupseteq (k+1, \omega)$, which, by definition of $\sqsupseteq$ at worlds, reduces to proving that $\lfloor\omega\rfloor_k \sqsupseteq \lfloor\omega\rfloor_k$, which holds trivially. □

Lemma 8. *If* $(W, s) \in \omega[i].I(r)$ *and* $W.k < j$*, then* $(W, s) \in \lfloor\omega\rfloor_j[i].I(r)$.

Proof. Immediate from definition of $\lfloor\omega\rfloor_j$. □

Lemma 9 (World step satisfaction)**.** *If* $(s, r, r_{\mathrm{F}}) : W$*, then* $(s, r, r_{\mathrm{F}}) : \triangleright W$.

Proof. Let $W = (k + 1, \omega)$. Then, $\triangleright W = (k, \lfloor\omega\rfloor_k)$. To prove $(s, r, r_{\mathrm{F}}) : \triangleright W$, we need to show two facts for every $i \in \{0, \ldots, |W.\omega| - 1\}$:

1. $r_{\mathrm{F}}[i] \in \lfloor\omega\rfloor_k[i].E$
2. $(\triangleright\triangleright W, s[i]) \in \lfloor\omega\rfloor_k[i].I(s[i] \cdot r[i] \cdot r_{\mathrm{F}}[i])$

(1) follows immediately from the following two facts:

- $r_{\mathrm{F}}[i] \in \omega[i].E$ (because $(s, r, r_{\mathrm{F}}) : W$)
- $\lfloor\omega\rfloor_k[i].E = \omega[i].E$ (by definition of $\lfloor\cdot\rfloor_k$)

To prove (2), we note that because $(s, r, r_{\mathrm{F}}) : W$, we have $(\triangleright W, s[i]) \in \omega[i].I(s[i]\cdot r[i]\cdot r_{\mathrm{F}}[i])$. By Lemma 7, $\triangleright\triangleright W \sqsupseteq \triangleright W$ and because $I(s[i] \cdot r[i] \cdot r_{\mathrm{F}}[i])$ is closed under world extension, we obtain $(\triangleright\triangleright W, s[i]) \in \omega[i].I(s[i] \cdot r[i] \cdot r_{\mathrm{F}}[i])$. Finally, $(\triangleright\triangleright W).k = k - 1 < k$, so by Lemma 8, we have $(\triangleright\triangleright W, s[i]) \in \lfloor\omega\rfloor_k[i].I(s[i] \cdot r[i] \cdot r_{\mathrm{F}}[i])$, as needed. □

Lemma 10 (Administrative closure)**.** *If for every* h, $\langle h; e\rangle \hookrightarrow_n \langle h; \hat{e}\rangle$ *and* $(W, r, \hat{e}) \in \mathcal{E}[\![A]\!]\rho$*, then* $(W, r, e) \in \mathcal{E}[\![A]\!]\rho$.

Proof. We want to show that $(W, r, e) \in \mathcal{E}[\![A]\!]\rho$. Following the definition of $\mathcal{E}[\![A]\!]\rho$, pick $j, s, r_{\mathrm{F}}, h, e'$ such that

1. $j < W.k$
2. $(s, r, r_{\mathrm{F}}) : W$
3. $\langle |s \cdot r \cdot r_{\mathrm{F}}|; e\rangle \hookrightarrow_j \langle h; e'\rangle \not\hookrightarrow$

Because evaluation is deterministic, we must have:

4. $\langle |s \cdot r \cdot r_{\mathrm{F}}|; e\rangle \hookrightarrow_n \langle |s \cdot r \cdot r_{\mathrm{F}}|; \hat{e}\rangle \hookrightarrow_m \langle h; e'\rangle \not\hookrightarrow$
5. $j = m + n$

Let $\hat{W} = \triangleright^n W$. By Lemma 7, $\hat{W} \sqsupseteq_n W$, so by facts 1 and 5 we get:

6. $m < \hat{W}.k$

By Lemma 9 on fact 2,

7. $(s, r, r_{\mathrm{F}}) : \hat{W}$

Instantiating the definition of the given fact $(W, r, \hat{e}) \in \mathcal{E}[\![A]\!]\rho$ with $j = m, s = s, r = r, r_{\mathrm{F}} = r_{\mathrm{F}}, h = h, e' = e'$ using facts 6, 7, and 4, we get $W', s', r', r'_{\mathrm{F}}$ such that:

8. $W' \sqsupseteq_m \hat{W}$
9. $(s', r', r'_{\mathrm{F}}) : W'$
10. $\sigma = |s' \cdot r' \cdot r'_{\mathrm{F}}|$
11. $r'_{\mathrm{F}} \sqsupseteq r_{\mathrm{F}}$
12. $(W, r', e') \in \mathcal{V}[\![A]\!]\rho$

It remains only to check that $W' \sqsupseteq_j W$. This follows trivially from three previously derived facts: $j = m + n$, $W' \sqsupseteq_m \hat{W}$ and $\hat{W} \sqsupseteq_n W$. □

Lemma 11 (Index context weakening)**.** *Let* $\rho \in \mathrm{Env}(\Sigma)$, $\rho' \in \mathrm{Env}(\Sigma')$ *and* $\mathrm{dom}(\Sigma) \cap \mathrm{dom}(\Sigma') = \emptyset$*. Then, the following hold whenever the left hand sides are defined:*

1. $\rho \models_\Sigma P$ *implies* $\rho, \rho' \models_{\Sigma,\Sigma'} P$.

2. $\mathcal{V}[\![\Sigma \vdash A : \kappa]\!]\rho = \mathcal{V}[\![\Sigma, \Sigma' \vdash A : \kappa]\!](\rho, \rho')$.

3. $\mathcal{E}[\![A]\!]\rho = \mathcal{E}[\![A]\!](\rho, \rho')$.

4. $\mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W = \mathcal{U}[\![\Sigma, \Sigma' \vdash \Gamma\ \mathsf{ok}]\!]\ (\rho, \rho')\ W$

5. $\mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W = \mathcal{L}[\![\Sigma, \Sigma' \vdash \Delta\ \mathsf{ok}]\!]\ (\rho, \rho')\ W$

Proof. (1)–(5) follow by induction on the definitions of the various relations. The proof requires the assumption that $\mathcal{I}[\![\Sigma \rhd t : \sigma]\!]\rho = \mathcal{I}[\![\Sigma, \Sigma' \rhd t : \sigma]\!](\rho, \rho')$ when the left hand side is defined. □

Lemma 12 (Index term substitution)**.** *Let* $\mathrm{dom}(\Sigma) \cap \mathrm{dom}(\Sigma') = \emptyset$, $\rho \in \mathrm{Env}(\Sigma)$, $\Sigma \rhd t : \sigma$ *and* $d = \mathcal{I}[\![\Sigma \rhd t : \sigma]\!]\rho$. *Then, the following hold whenever the left hand sides are defined:*

1. $\rho, X \mapsto d \models_{\Sigma, X:\sigma} P$ *iff* $\rho \models_\Sigma [t/X]P$.

2. $\mathcal{V}[\![\Sigma, X : \sigma \vdash A : \kappa]\!](\rho, X \mapsto d) = \mathcal{V}[\![\Sigma \vdash [t/X]A : \kappa]\!]\rho$.

3. $\mathcal{E}[\![A]\!](\rho, X \mapsto d) = \mathcal{E}[\![[t/X]A]\!]\rho$.

4. $\mathcal{U}[\![\Sigma, X : \sigma \vdash \Gamma\ \mathsf{ok}]\!]\ (\rho, X \mapsto d)\ W = \mathcal{U}[\![\Sigma \vdash [t/X]\Gamma\ \mathsf{ok}]\!]\ \rho\ W$

5. $\mathcal{L}[\![\Sigma, X : \sigma \vdash \Delta\ \mathsf{ok}]\!]\ (\rho, X \mapsto d)\ W = \mathcal{L}[\![\Sigma \vdash [t/X]\Delta\ \mathsf{ok}]\!]\ \rho\ W$

Proof. By induction on the definitions of the various relations. The proof requires the assumption that $\mathcal{I}[\![\Sigma, X : \sigma \rhd t' : \sigma']\!](\rho, X \mapsto d) = \mathcal{I}[\![\Sigma \rhd [t/X]t' : \sigma']\!]\rho$. □

Lemma 13 (Type substitution)**.** *Let* $\mathrm{dom}(\Sigma) \cap \mathrm{dom}(\Sigma') = \emptyset$, $\rho \in \mathrm{Env}(\Sigma)$, $\Sigma \vdash A : \kappa$ *and* $a = \mathcal{V}[\![\Sigma \vdash A : \kappa]\!]\rho$. *Then, the following hold whenever the left hand sides are defined:*

1. $\rho, \alpha \mapsto a \models_{\Sigma, \alpha:\kappa} P$ *iff* $\rho \models_\Sigma P$.

2. $\mathcal{V}[\![\Sigma, \alpha : \kappa \vdash B : \kappa']\!](\rho, \alpha \mapsto a) = \mathcal{V}[\![\Sigma \vdash [A/\alpha]B : \kappa']\!]\rho$.

3. $\mathcal{E}[\![B]\!](\rho, \alpha \mapsto a) = \mathcal{E}[\![[A/\alpha]B]\!]\rho$.

4. $\mathcal{U}[\![\Sigma, \alpha : \kappa \vdash \Gamma\ \mathsf{ok}]\!]\ (\rho, \alpha \mapsto a)\ W = \mathcal{U}[\![\Sigma \vdash [A/\alpha]\Gamma\ \mathsf{ok}]\!]\ \rho\ W$

5. $\mathcal{L}[\![\Sigma, \alpha : \kappa \vdash \Delta\ \mathsf{ok}]\!]\ (\rho, \alpha \mapsto a)\ W = \mathcal{L}[\![\Sigma \vdash [A/\alpha]\Delta\ \mathsf{ok}]\!]\ \rho\ W$

Proof. By induction on the definitions of the various relations. □

Lemma 14 (Propositional soundness)**.** *If* $\Sigma; \Pi \vdash P$, *then for every* $\rho \in \mathrm{Env}(\Sigma)$, $\rho \models_\Sigma \Pi$ *implies* $\rho \models_\Sigma P$.

Proof. By soundness of the proof system for first-order logic (i.e., by induction on the proof of $\Sigma; \Pi \vdash P$). □

Lemma 15. *If* $W' \sqsupseteq_j W$, *then* $\triangleright W' \sqsupseteq_j \triangleright W$.

Proof. Suppose $W' = (k' + 1, \omega')$ and $W = (k + 1, \omega)$ where $\omega' = \iota'_0, \ldots, \iota'_{n'}$ and $\omega = \iota_0, \ldots, \iota_n$. Then, $\triangleright W' = (k', \lfloor \omega' \rfloor_{k'})$ and $\triangleright W = (k, \lfloor \omega \rfloor_k)$. To show that $\triangleright W' \sqsupseteq_j \triangleright W'$, we must prove the following three statements:

(G1) $k' + j = k$: Because $W' \sqsupseteq_j W$, $k' + 1 + j = k + 1$, so $k' + j = k$.

(G2) $n' \geq n$: This follows immediately from $W' \sqsupseteq_j W$.

(G3) For $i \leq n$, $\lfloor \iota'_i \rfloor_{k'} = \lfloor \lfloor \iota_i \rfloor_k \rfloor_{k'}$: Note that because $k' \leq k$, $\lfloor \lfloor \iota_i \rfloor_k \rfloor_{k'} = \lfloor \iota_i \rfloor_{k'}$. So, it suffices to prove that $\lfloor \iota'_i \rfloor_{k'} = \lfloor \iota_i \rfloor_{k'}$. From $W' \sqsupseteq_j W$ we know that $\iota'_i = \lfloor \iota_i \rfloor_{k'+1}$. Therefore, $\lfloor \iota'_i \rfloor_{k'} = \lfloor \lfloor \iota_i \rfloor_{k'+1} \rfloor_{k'} = \lfloor \iota_i \rfloor_{k'}$, as required.

□

Lemma 16 (Soundness of sharing)**.** *If* $\Sigma \vdash A : \sigma \to \circ$ *and* $\Sigma; \Pi \vdash \mathrm{monoid}_\sigma(\epsilon, (\cdot))$*, then the following semantic inference rule is sound:*

$$\frac{\Sigma; \Pi; \Gamma; \Delta \Vdash e : [A\ t] \qquad \Sigma; \Pi; \Gamma; \cdot \Vdash v_i^s : [A/\alpha]\mathrm{specT}_i}{\Sigma; \Pi; \Gamma; \Delta \Vdash \mathsf{share}(e, \overline{v_i^s}) : \exists \alpha : \sigma \to \circ.\ [\alpha\ t] \otimes \overline{!\mathrm{specT}_i} \otimes !\mathrm{splitT} \otimes !\mathrm{joinT} \otimes !\mathrm{promoteT}}$$

where

$$\begin{array}{rcl}
\mathrm{specT}_i & = & \forall X : \sigma.\ \forall Y : \sigma_i' :: P_i.\ B_i \otimes [\alpha\ (t_i \cdot X)] \multimap \\
& & \quad \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [\alpha\ (t_i' \cdot X)] \\
& & \quad \textit{where } X, \alpha \notin \mathrm{FV}(P_i), \mathrm{FV}(Q_i), \mathrm{FV}(B_i), \mathrm{FV}(C_i), \mathrm{FV}(t_i), \mathrm{FV}(t_i') \\
\mathrm{splitT} & = & \forall X, Y : \sigma.\ [\alpha\ (X \cdot Y)] \multimap [\alpha\ X] \otimes [\alpha\ Y] \\
\mathrm{joinT} & = & \forall X, Y : \sigma.\ [\alpha\ X] \otimes [\alpha\ Y] \multimap [\alpha\ (X \cdot Y)] \\
\mathrm{promoteT} & = & \forall X : \sigma :: X = X \cdot X.\ [\alpha\ X] \multimap\ !\,[\alpha\ X] \\
\mathrm{monoid}_\sigma(\epsilon, (\cdot)) & = & \begin{array}{l} \forall X : \sigma.\ \epsilon \cdot X = X \wedge \\ \forall X, Y : \sigma.\ X \cdot Y = Y \cdot X \wedge \\ \forall X, Y, Z : \sigma.\ (X \cdot Y) \cdot Z = X \cdot (Y \cdot Z) \end{array}
\end{array}$$

Proof. Let $B = \exists \alpha : \sigma \to \circ.\ [\alpha\ t] \otimes \overline{!\mathrm{specT}_i} \otimes !\mathrm{splitT} \otimes !\mathrm{joinT} \otimes !\mathrm{promoteT}$. We want to prove that $\Sigma; \Pi; \Gamma; \Delta \Vdash \mathsf{share}(e, \overline{v_i^s}) : B$. By applying Lemma 6 using the premise and the evaluation context $E = \mathsf{share}([\,], \overline{v_i})$, we reduce this obligation to that of proving $\Sigma; \Pi; \Gamma; x : [A\ t] \Vdash \mathsf{share}(x, \overline{v_i^s}) : B$.

Assume a world W, $\rho \in \mathrm{Env}(\Sigma)$ such that $\rho \models_\Sigma \Pi$, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$, and a $(W, r, \bullet) \in \mathcal{V}[\![\Sigma \vdash [A\ t] : \circ]\!]\rho$. It suffices to prove that $(W, \pi(\gamma) \cdot r, \mathsf{share}(\bullet, \overline{\gamma(v_i^s)})) \in \mathcal{E}[\![B]\!]\rho$. Let $r^s = \pi(\gamma)$. We need to prove that:

$$(W, r^s \cdot r, \mathsf{share}(\bullet, \overline{\gamma(v_i^s)})) \in \mathcal{E}[\![B]\!]\rho$$

Following the definition $\mathcal{E}[\![\cdot]\!]\cdot$, pick r_F, s, $j < W.k$, h, e' such that:

1. $j < W.k$
2. $(s, r^s \cdot r, r_\mathrm{F}) : W$
3. $\left\langle |s \cdot r^s \cdot r \cdot r_\mathrm{F}|; \mathsf{share}(\bullet, \overline{\gamma(v_i^s)}) \right\rangle \hookrightarrow_j \langle h; e' \rangle \not\hookrightarrow$.

Call this point (A) in the proof — we will return to it later to complete the proof.

From the operational semantics of the construct $\mathsf{share}(\cdot, \cdot)$, we immediately derive that $j = 1$ and

4. $e' = v_0 = \langle \bullet, !\overline{\mathrm{op_i}}, !\mathrm{split}, !\mathrm{join}, !\mathrm{promote} \rangle$
5. $h = |s \cdot r^s \cdot r \cdot r_\mathrm{F}| \uplus [\ell : \mathsf{ff}]$

Assume that $|W.\omega| = |(\triangleright W).\omega| = n$. Because $\Sigma; \Pi \vdash \mathrm{monoid}_\sigma(\epsilon, (\cdot))$, there is a monoid on $\mathcal{S}[\![\sigma]\!]$ with operation $+ = \mathcal{I}[\![\cdot]\!]\rho$ and unit element $\mathcal{I}[\![\epsilon]\!]\rho$, which also we denote with ϵ. We now define a new world W_s that extends $\triangleright W$ with one new, $(n+1)$th island as follows. The new island is $(M, \cdot, \epsilon, I, E)$, where $M = \{U(x), L(x, y)\ \mid\ x, y \in \mathcal{S}[\![\sigma]\!]\} \uplus \{\bot\}$ and the operation $\cdot$ is defined as follows:

$$\begin{array}{rcl}
U(x) \cdot U(y) & = & U(x + y) \\
L(x, y) \cdot U(z) & = & L(x, y + z) \\
L(_) \cdot L(_) & = & \bot \\
\bot \cdot _ & = & \bot
\end{array}$$

It is easily checked that the element $\epsilon = U(\epsilon)$ is a unit for the monoid. We further define:

$$\begin{array}{rcl}
I(U(x)) & = & \{(W, r \cdot [\ell : \mathsf{ff}])\ \mid\ \exists v.\ (W, r, v) \in (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \circ]\!]\rho)\ x\} \\
I(L(x, y)) & = & \{(W, r \cdot [\ell : \mathsf{tt}])\ \mid\ x = y\} \\
I(\bot) & = & \emptyset \\
E & = & M
\end{array}$$

We denote by $\langle a \rangle$ the element of W_s: $(\epsilon, \ldots, \epsilon, a)$.

Let $d = \mathcal{I}[\![t]\!]\rho$. Returning to point (A) of our proof, we choose $W' = W_s$, $s' = s \cdot [\ell : \mathsf{ff}] \cdot r$, $r'_\mathrm{F} = r_\mathrm{F}$, $r' = r^s \cdot \langle U(d) \rangle$ and show the following to complete the proof.

(G1) $W' \sqsupseteq_j W$. This is immediate because $j = 1$ and $W' = W_s \sqsupseteq_0 (\triangleright W) \sqsupseteq_1 W$.

(G2) $((s \cdot [\ell : \mathsf{ff}] \cdot r, r^s \cdot \langle U(d) \rangle, r_{\mathrm{F}}) : W_s$. This is proved below.

(G3) $h = |s \cdot [\ell : \mathsf{ff}] \cdot r \cdot r_{\mathrm{F}} \cdot r^s \cdot \langle U(d) \rangle|$. This is immediate from fact (5).

(G4) $r'_{\mathrm{F}} = r_{\mathrm{F}}$. This is trivial because $r'_{\mathrm{F}} = r_{\mathrm{F}}$.

(G5) $(W_s, r^s \cdot \langle U(d) \rangle, v_0) \in \mathcal{V}[\![\Sigma \vdash B : \circ]\!]\rho$. This is proved below.

Proof of (G2). By Lemma 9 applied to fact (2), we obtain that:

6. $(s, r^s \cdot r, r_{\mathrm{F}}) : \triangleright W$

To prove (G2), we must prove the following two facts:

(G2.1) $\forall i < n + 1.\ r_{\mathrm{F}}[i] \in W_s.\omega[i].E$

Proof: For $i < n$, $W_s.\omega[i] = (\triangleright W).\omega[i]$, so we only need to show that $\forall i < n + 1.\ r_{\mathrm{F}}[i] \in (\triangleright W).\omega[i].E$, which follows from fact (6). For $i = n$, the statement is trivial because, by construction of W_s, $W_s.\omega[n].E = M$.

(G2.2) $s \cdot [\ell : \mathsf{ff}] \cdot r = s_0 \cdot \ldots \cdot s_n$, where $(\triangleright W_s, s_i) \in W_s.\omega[i].I(s[i] \cdot [\ell : \mathsf{ff}][i] \cdot (r \cdot r^s)[i] \cdot \langle U(d) \rangle[i] \cdot r_{\mathrm{F}}[i])$

Proof: From fact (6), we know that:

7. $s = s'_0 \cdot \ldots \cdot s'_n$ where $(\triangleright\triangleright W, s'_i) \in (\triangleright W).\omega[i].I(s[i] \cdot (r \cdot r^s)[i] \cdot r_{\mathrm{F}}[i])$

We choose: $s_0 = s'_0$, …, $s_{n-1} = s'_{n-1}$, $s_n = [\ell : \mathsf{ff}] \cdot r$ and split 3 cases:

Case $i = 0$: We have to show that $(\triangleright W_s, s_0) \in W_s.\omega[0].I(s[0] \cdot [\ell : \mathsf{ff}] \cdot (r \cdot r^s)[0] \cdot r_{\mathrm{F}}[0])$. Because $W_s.\omega[0] = (\triangleright W).\omega[0]$ by construction, it suffices to prove that $(\triangleright W_s, s_0) \in (\triangleright W).\omega[0].I(s[0] \cdot [\ell : \mathsf{ff}] \cdot (r \cdot r^s)[0] \cdot r_{\mathrm{F}}[0])$. Since invariant of island 0 is independent of the argument, it also suffices to prove that $(\triangleright W_s, s_0) \in (\triangleright W).\omega[0].I(s[0] \cdot (r \cdot r^s)[0] \cdot r_{\mathrm{F}}[0])$. By construction, $W_s \sqsupseteq \triangleright W$. Therefore, by Lemma 15, $\triangleright W_s \sqsupseteq \triangleright\triangleright W$. Hence, because I at each island is closed under world extensions, it suffices to prove that $(\triangleright\triangleright W, s_0) \in (\triangleright W).\omega[0].I(s[0] \cdot (r \cdot r^s)[0] \cdot r_{\mathrm{F}}[0])$. This follows from fact (7).

Case $0 < i < n$: We have to show that $(\triangleright W_s, s_i) \in W_s.\omega[i].I(s[i] \cdot (r \cdot r^s)[i] \cdot r_{\mathrm{F}}[i])$. As in the previous case, it suffices to prove that $(\triangleright\triangleright W, s_i) \in (\triangleright W).\omega[i].I(s[i] \cdot (r \cdot r^s)[i] \cdot r_{\mathrm{F}}[i])$, which follows from fact (7).

Case $i = n$: We must show that $(\triangleright W_s, [\ell : \mathsf{ff}] \cdot r) \in W_s.\omega[n].I(U(d))$. By construction, $W_s.\omega[n].I(U(d)) = \{(W, r \cdot [\ell : \mathsf{ff}]) \mid \exists v.\ (W, r, v) \in (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \circ]\!]\rho)\ d\}$. Therefore, it suffices to prove that $\exists v.\ (W, r, v) \in (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \circ]\!]\rho)\ d$. Since $d = \mathcal{I}[\![t]\!]\rho$, this is equivalent to $\exists v.\ (W, r, v) \in (\mathcal{V}[\![\Sigma \vdash A\ t : \circ]\!]\rho)$, which follows from our initial assumption that $(W, r, \bullet) \in (\mathcal{V}[\![\Sigma \vdash [A\ t] : \circ]\!]\rho)$.

Proof of (G5). We have to show that $(W_s, r^s \cdot \langle U(d) \rangle, v_0) \in \mathcal{V}[\![\Sigma \vdash B : \circ]\!]\rho$. Since $B = \exists \alpha : \sigma \to \circ. \ldots$, we need a witness for α. We pick the following witness:

$$T = \lambda x \in \mathcal{S}[\![\sigma]\!].\ \{(W, r, \bullet) \mid r[n] \sqsupseteq U(x)\}$$

It now suffices to prove that $(W_s, r^s \cdot \langle U(d) \rangle, v_0) \in \mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash [\alpha\ t] \otimes \overline{!\mathrm{specT}_i} \otimes !\mathrm{splitT} \otimes !\mathrm{joinT} \otimes !\mathrm{promoteT} : \circ]\!](\rho, \alpha \mapsto T)$. Following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$ at $\otimes$ and ! and observing that because $r^s = \pi(\gamma)$, $r^s = r^s \cdot r^s$, it suffices to prove each of the following:

(G5.1) $(W_s, \langle U(d) \rangle, \bullet) \in \mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash [\alpha\ t] : \circ]\!](\rho, \alpha \mapsto T)$

(G5.2) $(W_s, \epsilon, \mathrm{split}) \in \mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash \mathrm{splitT} : \circ]\!](\rho, \alpha \mapsto T)$

(G5.3) $(W_s, \epsilon, \mathrm{join}) \in \mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash \mathrm{joinT} : \circ]\!](\rho, \alpha \mapsto T)$

(G5.4) $(W_s, \epsilon, \mathrm{promote}) \in \mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash \mathrm{promoteT} : \circ]\!](\rho, \alpha \mapsto T)$

(G5.5) $(W_s, r^s, \mathrm{op}_i) \in \mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash \mathrm{specT}_i : \circ]\!](\rho, \alpha \mapsto T)$

We prove each of these.

Proof of (G5.1). It suffices to prove that there is v such that:

$$\begin{array}{rcl}(W_s, \langle U(t)\rangle, v) & \in & \mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash \alpha\ t : \circ]\!](\rho, \alpha \mapsto T) \\ & = & (\mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash \alpha : \sigma \to \circ]\!](\rho, \alpha \mapsto T))\ (\mathcal{I}[\![t]\!](\rho, \alpha \mapsto T)) \\ & = & T\ d \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d)\}\end{array}$$

Since $\langle U(d)\rangle[n] = U(d) \sqsupseteq U(d)$, we choose $v = \bullet$ to complete the proof.

Proof of (G5.2). By definition, split $= \lambda x.\ \langle \bullet, \bullet\rangle$ and splitT $= \forall X, Y : \sigma.\ [\alpha\ (X \cdot Y)] \multimap [\alpha\ X] \otimes [\alpha\ Y]$. Following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$ at type $\forall\cdot.\ \cdot$, pick arbitrary $d_1, d_2 \in \mathcal{S}[\![\sigma]\!]$ and define $\rho' = \rho, \alpha \mapsto T, X \mapsto d_1, Y \mapsto d_2$ and $\Sigma' = \Sigma, \alpha : \sigma \to \circ, X : \sigma, Y : \sigma$. It suffices to prove that: $(W_s, \epsilon, \lambda x.\ \langle \bullet, \bullet\rangle) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ (X \cdot Y)] \multimap [\alpha\ X] \otimes [\alpha\ Y] : \circ]\!]\rho'$.

Following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$, pick $W' \sqsupseteq W_s$ and r', v' such that

8. $(W', r', v') \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ (X \cdot Y)] : \circ]\!]\rho'$

It suffices to prove that:

(G5.2.1) $(W', r', \langle \bullet, \bullet\rangle) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ X] \otimes [\alpha\ Y] : \circ]\!]\rho'$

From fact (8), there is v'' such that:

$$\begin{array}{rcl}(W', r', v'') & \in & \mathcal{V}[\![\Sigma' \vdash \alpha\ (X \cdot Y) : \circ]\!]\rho' \\ & = & (\mathcal{V}[\![\Sigma' \vdash \alpha : \sigma \to \circ]\!]\rho')\ (\mathcal{I}[\![X \cdot Y]\!]\rho') \\ & = & T\ (d_1 + d_2) \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d_1 + d_2)\} \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d_1) \cdot U(d_2)\}\end{array}$$

Therefore,

9. $r'[n] \sqsupseteq U(d_1) \cdot U(d_2)$
10. $\exists \hat{a}$: $r'[n] = U(d_1) \cdot U(d_2) \cdot \hat{a}$.

Define $r_1 = \langle U(d_1)\rangle$ and $r_2 = (r_2[0], \ldots, r_2[n])$, where:

$$r_2[n] \quad = \quad \begin{cases} r'[i] & i < n \\ U(d_2) \cdot \hat{a} & i = n \end{cases}$$

Because of fact (10), $r_1 \cdot r_2 = r'$. So, our goal (G5.2.1) can be reduced to proving:

(G5.2.2) $(W', r_1, \bullet) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ X] : \circ]\!]\rho'$

Proof: It suffices to prove that:

$$\begin{array}{rcl}(W', r_1, \bullet) & \in & \mathcal{V}[\![\Sigma' \vdash \alpha\ X : \circ]\!]\rho' \\ & = & (\mathcal{V}[\![\Sigma' \vdash \alpha : \sigma \to \circ]\!]\rho')\ (\mathcal{I}[\![X]\!]\rho') \\ & = & T\ d_1 \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d_1)\}\end{array}$$

Since $r_1[n] = U(d_1) \sqsupseteq U(d_1)$, we are done.

(G5.2.3) $(W', r_2, \bullet) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ Y] : \circ]\!]\rho'$

Proof: It suffices to prove that:

$$\begin{array}{rcl}(W', r_2, \bullet) & \in & \mathcal{V}[\![\Sigma' \vdash \alpha\ Y : \circ]\!]\rho' \\ & = & (\mathcal{V}[\![\Sigma' \vdash \alpha : \sigma \to \circ]\!]\rho')\ (\mathcal{I}[\![Y]\!]\rho') \\ & = & T\ d_2 \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d_2)\}\end{array}$$

Since $r_2[n] = (U(d_2) \cdot \hat{a}) \sqsupseteq U(d_2)$, we are done.

Proof of (G5.3). By definition, join $= \lambda x.\ \bullet$ and joinT $= \forall X, Y : \sigma.\ [\alpha\ X] \otimes [\alpha\ Y] \multimap [\alpha\ (X \cdot Y)]$. Following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$, pick $d_1, d_2 \in \mathcal{S}[\![\sigma]\!]$ and define $\rho' = \rho, \alpha \mapsto T, X \mapsto d_1, Y \mapsto d_2$ and $\Sigma' = \Sigma, \alpha : \sigma \to \circ, X : \sigma, Y : \sigma$. It suffices to prove that: $(W_s, \epsilon, \lambda x.\ \bullet) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ X] \otimes [\alpha\ Y] \multimap [\alpha\ (X \cdot Y)] : \circ]\!]\rho'$. Again following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$, pick a $W' \sqsupseteq W_s$ and r', v' such that

11. $(W', r', v') \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ X] \otimes [\alpha\ Y] : \circ]\!]\rho'$

It suffices to prove that $(W', r', \bullet) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ (X \cdot Y)] : \circ]\!]\rho'$. It further suffices to prove that

$$\begin{array}{rcl} (W', r', \bullet) & \in & \mathcal{V}[\![\Sigma' \vdash \alpha\ (X \cdot Y) : \circ]\!]\rho' \\ & = & T\ (d_1 + d_2) \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d_1 + d_2)\} \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d_1) \cdot U(d_2)\} \end{array}$$

Therefore, it suffices to prove that:

(G5.3.1) $r'[n] \sqsupseteq U(d_1) \cdot U(d_2)$

From fact (11), we know that $r' = r_1 \cdot r_2$ and $v' = \langle v_1, v_2 \rangle$ such that: $(W', r_1, v_1) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ X] : \circ]\!]\rho'$ and $(W', r_2, v_2) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ Y] : \circ]\!]\rho'$. Hence, there are v_1', v_2' such that:

12. $(W', r_1, v_1') \in \mathcal{V}[\![\Sigma' \vdash \alpha\ X : \circ]\!]\rho'$
13. $(W', r_2, v_2') \in \mathcal{V}[\![\Sigma' \vdash \alpha\ Y : \circ]\!]\rho'$

Simplifying the right hand side of fact (12), we get $(W', r_1, v_1') \in T\ d_1 = \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d_1)\}$. Therefore, $r_1[n] \sqsupseteq U(d_1)$. Similarly, using fact (13), $r_2[n] \sqsupseteq U(d_2)$. Combining, we get $r'[n] = r_1[n] \cdot r_2[n] \sqsupseteq U(d_1) \cdot U(d_2)$, which is exactly our required subgoal (G5.3.1).

Proof of (G5.4). By definition, promote $= \lambda x.\ !\bullet$ and promoteT $= \forall X : \sigma :: X = X \cdot X.\ [\alpha\ X] \multimap ![\alpha\ X]$. Following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$, pick $d' \in \mathcal{S}[\![\sigma]\!]$ and define $\Sigma' = \Sigma, \alpha : \sigma \to \circ, X : \sigma$ and $\rho' = \rho, \alpha \mapsto T, X \mapsto d'$. Assume that $\rho' \models_{\Sigma'} X = X \cdot X$. Note that this implies:

14. $d' = d' + d'$

It suffices to prove that $(W_s, \epsilon, \lambda x.\ !\bullet) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ X] \multimap ![\alpha\ X] : \circ]\!]\rho'$. Again following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$, pick a $W' \sqsupseteq W_s$ and r', v' such that

15. $(W', r', v') \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ X] : \circ]\!]\rho'$

It suffices to prove that:

(G5.4.1) $(W', r', !\bullet) \in \mathcal{V}[\![\Sigma' \vdash ![\alpha\ X] : \circ]\!]\rho'$

From fact (15), there is a v'' such that

$$\begin{array}{rcl} (W', r', v'') & \in & \mathcal{V}[\![\Sigma' \vdash \alpha\ X : \circ]\!]\rho' \\ & = & T\ d' \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d')\} \end{array}$$

Therefore, $r'[n] \sqsupseteq U(d')$. Define $\hat{r} = (\epsilon, \ldots, \epsilon, U(d'))$. Clearly, $r' \sqsupseteq \hat{r}$, so by Lemma 4, we can reduce our subgoal (G5.4.1) to $(W', \hat{r}, !\bullet) \in \mathcal{V}[\![\Sigma' \vdash ![\alpha\ X] : \circ]\!]\rho'$. Because of fact (14), $\hat{r} = \hat{r} \cdot \hat{r}$, so it suffices to prove that $(W', \hat{r}, \bullet) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ X] : \circ]\!]\rho'$, which is further reduced to $(W', \hat{r}, \bullet) \in \mathcal{V}[\![\Sigma' \vdash \alpha\ X : \circ]\!]\rho'$. Note that $\mathcal{V}[\![\Sigma' \vdash \alpha\ X : \circ]\!]\rho' = T\ d' = \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(d')\}$. So we only need to prove that $\hat{r}[n] \sqsupseteq U(d')$, which is trivial because $\hat{r}[n] = U(d')$.

Proof of (G5.5). We want to prove that $(W_s, r^s, \mathrm{op}_i) \in \mathcal{V}[\![\Sigma, \alpha : \sigma \to \circ \vdash \mathrm{specT}_i : \circ]\!](\rho, \alpha \mapsto T)$. By definition, $\mathrm{specT}_i = \forall X : \sigma.\ \forall Y : \sigma_i' :: P_i.\ B_i \otimes [\alpha\ (t_i \cdot X)] \multimap \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [\alpha\ (t_i' \cdot X)]$. Following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$, pick $a \in \mathcal{S}[\![\sigma]\!]$ and $d_1 \in \mathcal{S}[\![\sigma_i']\!]$ and define $\rho' = \rho, \alpha \mapsto T, X \mapsto a, Y \mapsto d_1$ and $\Sigma' = \Sigma, \alpha : \sigma \to \circ, X : \sigma, Y : \sigma_i'$. Assume that:

16. $\rho' \models_{\Sigma'} P_i$

It suffices to prove that $(W_s, r^s, \mathrm{op}_i) \in \mathcal{V}[\![\Sigma' \vdash B_i \otimes [\alpha\ (t_i \cdot X)] \multimap \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [\alpha\ (t_i' \cdot X)] : \circ]\!]\rho'$. Again following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$, pick a $W_0 \sqsupseteq W'$, r_a, v_a such that:

17. $(W_0, r_a, v_a) \in \mathcal{V}[\![\Sigma' \vdash B_i \otimes [\alpha\ (t_i \cdot X)] : \circ]\!]\rho'$

It suffices to prove that $(W_0, r^s \cdot r_a, \mathrm{op}_i\ v_a) \in \mathcal{E}[\![\exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [\alpha\ (t_i' \cdot X)]]\!]\rho'$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]\cdot$, pick $j_0, s_0, r_{\mathrm{F0}}, h_f, e_f$ such that:

18. $j_0 < W_0.k$

19. $(s_0, r^s \cdot r_a, r_{\mathrm{F0}}) : W_0$

20. $\langle |s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}}|; \mathrm{op}_i\ v_a\rangle \hookrightarrow_{j_0} \langle h_f; e_f\rangle \not\hookrightarrow$

Call this point (B) in the proof. We will return to it later to complete the proof. Let $n_0 = |W_0.\omega|$. Since $W_0 \sqsupseteq W_s$, $n_0 \geq n+1$. Further for $i \in \{0, \ldots, n\}$. $W_0.\omega[i] = W_s.\omega[i]$. From fact (19), we know that

21. $s_0 = s_{0,0} \cdot \ldots \cdot s_{0,n_0}$ such that (in particular),
$(\triangleright W_0, s_{0,n}) \in W_0.\omega[n].I((s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}})[n]) = W_s.\omega[n].I((s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}})[n])$.

The definition of I on the $(n+1)$th island now forces either $[\ell : \mathsf{ff}] \in s_{0,n}$ or $[\ell : \mathsf{tt}] \in s_{0,n}$. Hence, either $[\ell : \mathsf{ff}] \in s_0$ or $[\ell : \mathsf{tt}] \in s_0$. Further, because $(\triangleright W_0, s_{0,0}) \in W_0.\omega[0].I((s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}})[0]) = W_s.\omega[0].I((s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}})[0])$, $(s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}})[0]$ cannot equal $\bot$, so either $[\ell : \mathsf{tt}] \in |s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}}|$ or $[\ell : \mathsf{ff}] \in |s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}}|$. If the former, then using the definition of op_i, we know that $\langle |s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}}|; \mathrm{op}_i\ v_a\rangle$ diverges (by taking the 'then' branch in the definition of op_i). But from fact (20) we know that this configuration does not diverge, so it follows that $[\ell : \mathsf{ff}] \in |s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}}|$ and accordingly, $[\ell : \mathsf{ff}] \in s_{0,n}$. Let:

22. $s_{0,n} = s_{0,n}' \cdot [\ell : \mathsf{ff}]$ and $s_0' = s_{0,0} \cdot \ldots \cdot s_{0,n-1} \cdot s_{0,n}' \cdot s_{0,n+1} \cdot \ldots \cdot s_{0,n_0}$.

Using the definition of I on the $(n+1)$th island, we also get

23. $(s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}})[n] = U(g)$ for some $g \in \mathcal{S}[\![\sigma]\!]$.

Using fact (20) and our analysis above we also deduce that there are j_1 and j_0' such that:

24. $\langle |s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}}|; \mathrm{op}_i\ v_a\rangle \hookrightarrow_{j_1} \langle |s_0' \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}}| \cdot [\ell : \mathsf{tt}]; E[(\gamma(v_i^s))\ v_a]\rangle \hookrightarrow_{j_0'} \langle h_f; e_f\rangle \not\hookrightarrow$ where

$$\mathrm{E}[\,] \;=\; \begin{array}{l}\mathsf{let}\ y = [\,]\ \mathsf{in}\\ \quad \mathsf{let}\ \_ = \ell :=_\bullet \mathsf{ff}\ \mathsf{in}\\ \quad y\end{array}$$

25. $j_0 = j_1 + j_0'$

Analyzing fact (24) further, we deduce that there are j_2 and j_3 such that:

26. $j_0' = j_2 + j_3$

27. $\langle |s_0' \cdot r^s \cdot r_a \cdot r_{\mathrm{F0}}| \cdot [\ell : \mathsf{tt}]; (\gamma(v_i^s))\ v_a\rangle \hookrightarrow_{j_2} \langle h_1; e_1\rangle \not\hookrightarrow$

28. $\langle h_1; E[e_1]\rangle \hookrightarrow_{j_3} \langle h_f; e_f\rangle \not\hookrightarrow$

Our next objective is to show that $(\gamma(v_i^s))\ v_a$ is semantically well-typed and then apply the definition of $\mathcal{E}[\![\cdot]\!]\cdot$ to fact (27). From fact (17), we know that there are $r_a^B, r_a^\alpha, v_a^B, v_a^\alpha$ such that:

29. $r_a = r_a^B \cdot r_a^\alpha$

30. $v_a = \langle v_a^B, v_a^\alpha\rangle$

31. $(W_0, r_a^B, v_a^B) \in \mathcal{V}[\![\Sigma' \vdash B_i : \circ]\!]\rho'$

32. $(W_0, r_a^\alpha, v_a^\alpha) \in \mathcal{V}[\![\Sigma' \vdash [\alpha\ (t_i \cdot X)] : \circ]\!]\rho'$

Let $m = \mathcal{I}[\![t_i]\!]\rho$. Fact (32) forces that $v_a^\alpha = \bullet$ and implies that there is a $v_a^{\alpha\prime}$ such that:

$$\begin{array}{rcl}(W_0, r_a^\alpha, v_a^{\alpha\prime}) & \in & \mathcal{V}[\![\Sigma' \vdash \alpha\ (t_i \cdot X) : \circ]\!]\rho' \\ & = & T\ (m+a) \\ & = & \{(W, r, \bullet)\ \mid\ r[n] \sqsupseteq U(m) \cdot U(a)\}\end{array}$$

Therefore, $r_a^\alpha[n] \sqsupseteq U(m) \cdot U(a)$. Further from fact (23), $U(g) = (r_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F}0})[n] \sqsupseteq r_a^\alpha[n+1]$, so by the definition of the monoid at the $(n+1)$th island, there is some a' such that:

33. $r_a^\alpha[n] = U(m + a + a')$.

34. Choose f such that $U(f) = (s_0' \cdot r^s \cdot r_a^B \cdot r_{\mathrm{F}0})[n]$. Then, $g = m + a + a' + f$. Define $g' = a + a' + f$.

From facts (21), (22) and (23), we know that $(\triangleright W_0, s_{0,n}' \cdot [\ell : \mathsf{ff}]) \in W_s.\omega[n].I(U(g))$. Hence, using the definition of I on the $(n+1)$th island, we deduce that there is v such that

$$\begin{array}{rcl}(\triangleright W_0, s_{0,n}', v) & \in & (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \circ]\!]\rho)\ g \\ & = & (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \circ]\!]\rho)\ (g' + m)\end{array}$$

Pick a fresh variable X'. Then, by Lemmas 12 and 11, we get $(\triangleright W_0, s_{0,n}', v) \in \mathcal{V}[\![\Sigma', X' : \sigma \vdash A\ (t_i \cdot X') : \circ]\!](\rho', X' \mapsto g')$. This immediately implies:

35. $(\triangleright W_0, s_{0,n}', \bullet) \in \mathcal{V}[\![\Sigma', X' : \sigma \vdash [A\ (t_i \cdot X')] : \circ]\!](\rho', X' \mapsto g')$

Choose:

36. $W_1 = \triangleright^{j_1} W_0$. Note that because of fact (24), $j_1 > 1$.

By Lemma 2 applied to facts (35) and (36), we derive that:

37. $(W_1, s_{0,n}', \bullet) \in \mathcal{V}[\![\Sigma', X' : \sigma \vdash [A\ (t_i \cdot X')] : \circ]\!](\rho', X' \mapsto g')$

By Lemmas 2 and 11 applied to fact (31), we deduce:

38. $(W_1, r_a^B, v_a^B) \in \mathcal{V}[\![\Sigma', X' : \sigma \vdash B_i : \circ]\!](\rho', X' \mapsto g')$

Noting that $v_a = \langle v_a^B, v_a^\alpha \rangle = \langle v_a^B, \bullet \rangle$, we deduce from facts (37) and (38) that:

39. $(W_1, s_{0,n}' \cdot r_a^B, v_a) \in \mathcal{V}[\![\Sigma', X' : \sigma \vdash B_i \otimes [A\ (t_i \cdot X')] : \circ]\!](\rho', X' \mapsto g')$

Using the second premise of the given inference rule, we derive that $(W, r^s, \gamma(v_i^s)) \in \mathcal{V}[\![\Sigma \vdash [A/\alpha]\mathrm{specT}_i : \circ]\!]\rho$. Expanding the definition of specT_i, noting that $\alpha \notin B_i, C_i$, we get

$$(W, r^s, \gamma(v_i^s)) \in \mathcal{V}[\![\Sigma \vdash \forall X : \sigma.\ \forall Y : \sigma_i' :: P_i.\ B_i \otimes [A\ (t_i \cdot X)] \multimap \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [A\ (t_i' \cdot X)] : \circ]\!]\rho$$

α-renaming X to X' noting that by the side condition on specT_i, $X \notin P_i, Q_i, B_i, C_i, t_i, t_i'$, we get:

$$(W, r^s, \gamma(v_i^s)) \in \mathcal{V}[\![\Sigma \vdash \forall X' : \sigma.\ \forall Y : \sigma_i' :: P_i.\ B_i \otimes [A\ (t_i \cdot X')] \multimap \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [A\ (t_i' \cdot X')] : \circ]\!]\rho$$

Using Lemma 2, observing that $W_1 = \triangleright^{j_1} W_0 \sqsupseteq W_0 \sqsupseteq W_s \sqsupseteq \triangleright W \sqsupseteq W$, we obtain:

$$(W_s, r^s, \gamma(v_i^s)) \in \mathcal{V}[\![\Sigma \vdash \forall X' : \sigma.\ \forall Y : \sigma_i' :: P_i.\ B_i \otimes [A\ (t_i \cdot X')] \multimap \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [A\ (t_i' \cdot X')] : \circ]\!]\rho$$

We now instantiate the definition of $\mathcal{V}[\![\cdot]\!]\cdot$ at the type $\forall \cdot :: \cdot.\ \cdot$ choosing the substitution $\rho', X' \mapsto g'$ (recall that ρ' contains $Y \mapsto d_1$). From fact (16) and Lemma 11, we obtain that $\rho', X' \mapsto g' \models_{\Sigma', X' : \sigma} P_i$. Hence, we get:

40. $(W_s, r^s, \gamma(v_i^s)) \in \mathcal{V}[\![\Sigma', X' : \sigma \vdash B_i \otimes [A\ (t_i \cdot X')] \multimap \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [A\ (t_i' \cdot X')] : \circ]\!](\rho', X' \mapsto g')$

From facts (39) and (40), following the definition of $\mathcal{V}[\![\cdot]\!]\cdot$ at $\multimap$, we get:

41. $(W_s, r^s \cdot r_a^B \cdot s_{0,n}', (\gamma(v_i^s))\ v_a) \in \mathcal{E}[\![\exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [A\ (t_i' \cdot X')]]\!](\rho', X' \mapsto g')$

Now we wish to instantiate the definition of $\mathcal{E}[\![\cdot]\!]\cdot$ in fact (41) using the reduction in fact (27). We choose:

42. $W = W_1$,
$j = j_2$
$r = r^s \cdot r_a^B \cdot s'_{0,n}$
$s = s_{0,0} \cdot \ldots \cdot s_{0,n-1} \cdot [\ell : \mathtt{tt}] \cdot s_{0,n+1} \cdot s_{0,n_0}$
$r_{\mathrm{F}} = \langle L(g', a + a') \rangle \cdot r_{\mathrm{F}0} \cdot (r_a^\alpha \backslash \{n\})$.

where $(r_a^\alpha \backslash \{n\})$ is the same as r_a^α except in the $(n+1)$th island, where the value is ϵ (or $U(\epsilon)$). Call this point (C) in the proof, as we will return to it later. To apply the definition of $\mathcal{E}[\![\cdot]\!]\cdot$, we must show that:

(G5.5.1) $j_2 < W_1.k$.

Proof: $W_1.k = (\triangleright^{j_1} W_0).k = W_0.k - j_1$. Therefore, $W_1.k - j_2 = W_0.k - (j_1 + j_2)$. From facts (25) and (26), $j_0 \geq j_1 + j_2$. Therefore, $W_1.k - j_2 \geq W_0.k - j_0 > 0$ (by fact (18)).

(G5.5.2) Following fact (27): $|s'_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F}0}| \cdot [\ell : \mathtt{tt}] = |r \cdot s \cdot r_{\mathrm{F}}|$.

Proof: Immediate because on all islands except the $(n+1)$th, r, s, r_{F} is a repartitioning of $s'_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F}0}$.

(G5.5.3) $(s, r, r_{\mathrm{F}}) : W_1$.

Proof: Applying Lemma 9 to facts (19) and (36), we get:

43. $(s_0, r^s \cdot r_a, r_{\mathrm{F}0}) : W_1$

It suffices to prove three facts:

(G5.5.3.1) For every $j < n_0$. $r_{\mathrm{F}}[j] \in W_1.\omega[j].E$.
Proof: For $j \neq n$, $r_{\mathrm{F}}[j] = r_a^\alpha[j] \cdot r_{\mathrm{F}0}[j] \sqsupseteq r_{\mathrm{F}0}[j]$. Since $W_1.\omega[j].E$ is extension closed, the subgoal is immediate from fact (43). For $j = n$, the subgoal is trivial because $W_1.\omega[n].E = G$.

(G5.5.3.2) For $j \neq n$, $(\triangleright W_1, s_{0,j}) \in W_1.\omega[j].I((s \cdot r \cdot r_{\mathrm{F}})[j])$.
Proof: By definition of r, s, r_{F}, for $j \neq n$, $(s \cdot r \cdot r_{\mathrm{F}})[j] = (s_0 \cdot r^s \cdot r_a \cdot r_{\mathrm{F}0})[j]$. Therefore, the result is immediate from fact (43).

(G5.5.3.3) $(\triangleright W_1, [\ell : \mathtt{tt}]) \in W_1.\omega[n].I((s \cdot r \cdot r_{\mathrm{F}})[n])$
Proof: From facts (42) and (34), we get $(s \cdot r \cdot r_{\mathrm{F}})[n] = L(g', a + a') \cdot U(f) = L(g', a + a' + f) = L(g', g')$. Therefore by definition of the $(n+1)$th island, $W_1.\omega[n].I((s \cdot r \cdot r_{\mathrm{F}})[n]) = W_1.\omega[n].I(L(g', g')) = \{(W, r \cdot [\ell : \mathtt{tt}])\}$. The subgoal is then obviously true.

We now return to point (C) of our proof. Because of (G5.5.1)–(G5.5.3), we can instantiate the definition of $\mathcal{E}[\![\cdot]\!]\cdot$ at point (C) of the proof to obtain $W_2, s_2, r_2, r_{\mathrm{F}2}$ such that:

44. $W_2 \sqsupseteq_{j_2} W_1$

45. $(s_2, r_2, r_{\mathrm{F}2}) : W_2$

46. $h_1 = |s_2 \cdot r_2 \cdot r_{\mathrm{F}2}|$

47. $r_{\mathrm{F}2} \sqsupseteq \langle L(g', a + a') \rangle \cdot r_{\mathrm{F}0} \cdot (r_a^\alpha \backslash \{n\})$

48. $(W_2, r_2, e_1) \in \mathcal{V}[\![\Sigma', X' : \sigma \vdash \exists Z : \sigma''_i :: Q_i.\ C_i \otimes [A\ (t'_i \cdot X')] : \circ]\!](\rho', X' \mapsto g')$.

From fact (48) we know that there is a $d_2 \in \mathcal{S}[\![\sigma'']\!]$ such that

49. $\rho', X' \mapsto g', Z \mapsto d_2 \models_{\Sigma', X' : \sigma, Z : \sigma''} Q_i$

Let $\Sigma'' = \Sigma', X' : \sigma, Z : \sigma''$ and $\rho'' = \rho', X' \mapsto g', Z \mapsto d_2$. Then fact (49) also implies:

50. $\rho'' \models_{\Sigma''} Q_i$

Continuing with fact (48), we further derive v_2^C, r_2^C, r_2^A such that:

51. $e_1 = \langle v_2^C, \bullet \rangle$

52. $r_2 = r_2^C \cdot r_2^A$

53. $(W_2, r_2^C, v_2^C) \in \mathcal{V}[\![\Sigma'' \vdash C : \circ]\!]\rho''$

54. $(W_2, r_2^A, \bullet) \in \mathcal{V}[\![\Sigma'' \vdash [A\ (t_i' \cdot X')] : \circ]\!]\rho''$

Let $m' = \mathcal{I}[\![t_i']\!]\rho$. From fact (54), we obtain a v_2' such that $(W_2, r_2^A, v_2') \in \mathcal{V}[\![\Sigma'' \vdash A\ (t_i' \cdot X') : \circ]\!]\rho''$. Therefore,

55. $(W_2, r_2^A, v_2') \in (\mathcal{V}[\![\Sigma'' \vdash [A] : \circ]\!]\rho'')\ (m' + g')$

From fact (47), either $(s_2 \cdot r_2 \cdot r_{\mathrm{F}2})[n]$ is $L(g', \_)$ or it is $\bot$. By fact (45), $(\triangleright W_2, s_{2,n}) \in W_2.\omega[n].I((s_2 \cdot r_2 \cdot r_{\mathrm{F}2})[n])$, so following the definition of the $(n+1)$th island's I, we get:

56. $(s_2 \cdot r_2 \cdot r_{\mathrm{F}2})[n] = L(g', g')$

57. $s_{2,n} = [\ell : \mathsf{tt}] \cdot s_{2,n}'$ for some $s_{2,n}'$

From facts (57) and (46), we also get:

58. $h_1 = h_1' \cdot [\ell : \mathsf{tt}]$ for some h_1'

From facts (28), (51) and (58) we get using the operational semantics that:

59. $\langle h_1; E[e_1]\rangle \hookrightarrow_{j_3} \langle h_1' \cdot [\ell : \mathsf{ff}]; \langle v_2^c, \bullet\rangle\rangle \not\hookrightarrow$. (Therefore, h_f in fact (28) equals $h_1' \cdot [\ell : \mathsf{ff}]$.)

From fact (47), there is a $r_{\mathrm{F}2}'$ such that:

60. $r_{\mathrm{F}2} = \langle L(g', a + a')\rangle \cdot r_{\mathrm{F}0} \cdot (r_a^\alpha \backslash \{n\}) \cdot r_{\mathrm{F}2}'$

We now return to point (B) in our proof and construct $W', s', r', r_{\mathrm{F}}'$ to satisfy the definition of $\mathcal{E}[\![\cdot]\!]\cdot$ and close the proof. Let $n_2 = |W_2.\omega|$. We select:

61. $r_{\mathrm{F}}' = r_{\mathrm{F}0} \cdot (r_a^\alpha \backslash \{n\}) \cdot r_{\mathrm{F}2}'$
$r' = r_2^C \cdot \langle U(m' + a + a')\rangle$
$s' = s_0' \cdot \ldots \cdot s_{n_2}'$ where
$s_i' = \begin{cases} s_{2,i} & \text{if } i \neq n \\ s_{2,n}' \cdot [\ell : \mathsf{ff}] \cdot r_2^A & \text{if } i = n \end{cases}$
$W' = \triangleright^{j_3} W_2$

To complete the proof, it suffices to prove each of the following:

(G5.5.4) $W' \sqsupseteq_{j_0} W_0$

(G5.5.5) $(s', r', r_{\mathrm{F}}') : W'$

(G5.5.6) $h_1' \cdot [\ell : \mathsf{ff}] = |s' \cdot r' \cdot r_{\mathrm{F}}'|$

(G5.5.7) $r_{\mathrm{F}}' \sqsupseteq r_{\mathrm{F}0}$

(G5.5.8) $(W', r', \langle v_2^C, \bullet\rangle) \in \mathcal{V}[\![\Sigma' \vdash \exists Z : \sigma_i'' :: Q_i.\ C_i \otimes [A\ (t_i' \cdot X)] : \circ]\!]\rho'$

We prove each of these below.

Proof of (G5.5.4). Using facts (36), (44) and (61), we derive that $W' \sqsupseteq_{j_1+j_2+j_3} W_0$. From facts (25) and (26), we know that $j_0 = j_1 + j_2 + j_3$, which closes the subgoal.

Proof of (G5.5.5). Using Lemma 9 on fact (45) and noting that $W' = \triangleright^{j_3} W_1$, we obtain:

62. $(s_2, r_2, r_{\mathrm{F}2}) : W'$

It suffices to prove the following:

(G5.5.5.1) For each $j < n_2$, $r_{\mathrm{F}}'[j] \in W'.\omega[j].E$

Proof: Using facts (60) and (61), for $j \neq n$, $r_{\mathrm{F}}'[j] = r_{\mathrm{F}2}[j]$. Therefore for $j \neq n$, it is enough to prove that $r_{\mathrm{F}2}[j] \in W'.\omega[j].E$, which follows from fact (62). For $j = n$, the subgoal holds trivially because $W'.\omega[n].E = W_s.\omega[n].E = G$.

(G5.5.5.2) For each $j < n_2$, $(\triangleright W', s'_j) \in W'.\omega[j].I((s' \cdot r' \cdot r'_{\mathrm{F}})[j])$.

Proof: We consider three cases.

Case. $j = 0$. Then from fact (61), $s'_0 = s_{2,0}$. So, we must show that $(\triangleright W', s_{2,0}) \in W'.\omega[0].I((s' \cdot r' \cdot r'_{\mathrm{F}})[0])$. From fact (62), we know that $(\triangleright W', s_{2,0}) \in W'.\omega[0].I((s_2 \cdot r_2 \cdot r_{\mathrm{F2}})[0])$. But on island 0, $I(x)$ is independent of x, so we are done.

Case. $j = n$. From facts (56), (52) and (60), we derive that $(s_2 \cdot r_2^C \cdot r_2^A \cdot r_{\mathrm{F0}} \cdot r'_{\mathrm{F2}})[n] \cdot L(g', a + a') = L(g', g')$. Therefore, there is a g'' such that:

63. $(s_2 \cdot r_2^C \cdot r_2^A \cdot r_{\mathrm{F0}} \cdot r'_{\mathrm{F2}})[n] = U(g'')$ and $g' = a + a' + g''$

Now observe that

$$\begin{array}{rcll} (s' \cdot r' \cdot r'_{\mathrm{F}})[n] & = & (s_2 \cdot r_2^C \cdot r_2^A \cdot r_{\mathrm{F0}} \cdot r'_{\mathrm{F2}})[n] \cdot U(m' + a + a') & \text{(Fact (61))} \\ & = & U(g'') \cdot U(m' + a + a') & \text{(Fact (63))} \\ & = & U(g'' + m' + a + a') & \\ & = & U(m' + g') & \text{(Fact (63))} \end{array}$$

We need to prove that $(\triangleright W', s'_n) \in W'.\omega[n].I((s' \cdot r' \cdot r'_{\mathrm{F}})[n]) = W'.\omega[n].I(U(m' + g'))$. Because $W' \sqsupseteq W_s$, this happens iff $(\triangleright W', s'_n) \in W_s.\omega[n].I(U(m'+g')) = \{(W, r \cdot [\ell : \mathsf{ff}]) \mid \exists v.\ (W, r, v) \in (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \circ]\!]\rho)\ (m' + g')\}$. From fact (61), $s'_n = s'_{2,n} \cdot [\ell : \mathsf{ff}] \cdot r_2^A$. Therefore, it is enough to prove that there is a v such that $(\triangleright W', s'_{2,n} \cdot r_2^A, v) \in (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \circ]\!]\rho)\ (m' + g')$. By Lemma 4 and 2, it suffices to prove that $(\triangleright W', s'_{2,n} \cdot r_2^A, v) \in (\mathcal{V}[\![\Sigma \vdash A : \sigma \to \circ]\!]\rho)\ (m' + g')$. This follows from fact (55) and Lemma 11 (choosing $v = v'_2$).

Case. $j \notin \{0, n\}$. In this case $(s' \cdot r' \cdot r'_{\mathrm{F}})[j] = (s_2 \cdot r_2 \cdot r_{\mathrm{F2}})[j]$. So the result follows from fact (62).

Proof of (G5.5.6). Follows immediately from facts (46), (52), (58) and (61).

Proof of (G5.5.7). Immediate from fact (61).

Proof of (G5.5.8). Let $\Sigma''' = \Sigma', Z : \sigma''$ and $\rho''' = \rho', Z \mapsto d_2$. Observing that from fact (61), $r' = r_2^C \cdot \langle U(m' + a + a') \rangle$, it suffices to prove the following:

(G5.5.8.1) $\rho''' \models_{\Sigma'''} Q_i$.

Proof: This follows from fact (50) and Lemma 11.

(G5.5.8.2) $(W', r_2^C, v_2^C) \in \mathcal{V}[\![\Sigma''' \vdash C_i : \circ]\!]\rho'''$

Proof: Follows from fact (53) using Lemmas 2 and 11.

(G5.5.8.3) $(W', \langle U(m' + a + a') \rangle, \bullet) \in \mathcal{V}[\![\Sigma''' \vdash [A\ (t'_i \cdot X)] : \circ]\!]\rho'''$

Proof: It suffices to prove that

$$\begin{array}{rcl} (W', \langle U(m' + a + a') \rangle, \bullet) & \in & \mathcal{V}[\![\Sigma''' \vdash A\ (t'_i \cdot X) : \circ]\!]\rho''' \\ & = & (\mathcal{V}[\![\Sigma''' \vdash A : \sigma \to \circ]\!]\rho''')\ (m' + a) \\ & = & T\ (m' + a) \\ & = & \{(W, r, \bullet) \mid r[n] \sqsupseteq U(m' + a)\} \end{array}$$

Therefore, it suffices to show that $U(m' + a + a') \sqsupseteq U(m' + a)$, i.e., $U(m' + a) \cdot U(a') \sqsupseteq U(m' + a)$, which is trivial.

□

Theorem 1 (Fundamental Theorem)**.** *The following hold:*

1. *If* $\Sigma; \Pi; \Gamma; \Delta \vdash e : A$, *then* $\Sigma; \Pi; \Gamma; \Delta \Vdash e : A$.
2. *If* $\Sigma; \Pi; \Gamma; \Delta \vdash v : A$, *then* $\Sigma; \Pi; \Gamma; \Delta \Vdash^{\mathrm{V}} v : A$.

Proof. By simultaneous induction on the given typing derivations. Due to Lemma 5, (2) is stronger than (1) for values, so in cases where the term in the conclusion must be a value, we prove only (2). We introduce some notation. For an arbitrarily chosen world W, let $\rho \in \mathrm{Env}(\Sigma)$ such that $\rho \models_\Sigma \Pi$, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$ and $\delta \in \mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W$.

Case. $\dfrac{\Sigma \vdash \Pi\ \mathsf{ok} \qquad \Sigma \vdash \Gamma\ \mathsf{ok} \qquad \Sigma \vdash \Delta\ \mathsf{ok} \qquad x : A \in \Delta}{\Sigma; \Pi; \Gamma; \Delta \vdash x : A}$

Here x is a value, so we prove only (2). We need to show that $(W, \pi(\gamma) \cdot \pi(\delta), \delta(\gamma(x))) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$. Let $(x \mapsto (r, v)) \in \delta$. Since $\delta \in \mathcal{L}[\![\Sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho\ W$, we know that $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$. By Lemma 4, $(W, \pi(\gamma) \cdot \pi(\delta), v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$. The proof closes when we observe that $\delta(\gamma(x)) = v$.

Case. $\dfrac{\Sigma \vdash \Pi\ \mathsf{ok} \qquad \Sigma \vdash \Gamma\ \mathsf{ok} \qquad \Sigma \vdash \Delta\ \mathsf{ok} \qquad x : A \in \Gamma}{\Sigma; \Pi; \Gamma; \Delta \vdash x : A}$

Here x is a value, so we prove only (2). We need to show that $(W, \pi(\gamma) \cdot \pi(\delta), \delta(\gamma(x))) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$. Let $(x \mapsto (r, v)) \in \gamma$. Since $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$, we know that $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$. By Lemma 4, $(W, \pi(\gamma) \cdot \pi(\delta), v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$. The proof closes when we observe that $\delta(\gamma(x)) = v$.

Case. $\dfrac{\Sigma \vdash \Pi\ \mathsf{ok} \qquad \Sigma \vdash \Gamma\ \mathsf{ok} \qquad \Sigma \vdash \Delta\ \mathsf{ok} \qquad \Sigma \vdash \cdot\ \mathsf{ok}}{\Sigma; \Pi; \Gamma; \Delta \vdash \langle\rangle : 1}$

Here $\langle\rangle$ is a value, so we prove only (2). Since $\gamma(\delta(\langle\rangle)) = \langle\rangle$, if suffices to show that $(W, \pi(\gamma) \cdot \pi(\delta), \langle\rangle) \in \mathcal{V}[\![\Sigma \vdash 1 : \circ]\!]\rho$. This follows from the definition of $\mathcal{V}[\![\cdot]\!]\cdot$.

Case. $\dfrac{\Sigma; \Pi; \Gamma; \Delta_1 \vdash e_1 : A \qquad \Sigma; \Pi; \Gamma; \Delta_2 \vdash e_2 : B}{\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \vdash \langle e_1, e_2\rangle : A \otimes B}$

Proof of (1): Define $E_1 = \langle [\,], e_2\rangle$. From i.h.(1) on the first premise, we know that $\Sigma; \Pi; \Gamma; \Delta_1 \Vdash e_1 : A$, so by Lemma 6, it suffices to prove that $\Sigma; \Pi; \Gamma; \Delta_1, x : A \Vdash \langle x, e_2\rangle : A \otimes B$. Define $E_2 = \langle x, [\,]\rangle$. Then, our subgoal can be written as $\Sigma; \Pi; \Gamma; \Delta_1, x : A \Vdash E_2[e_2] : A \otimes B$. From i.h.(1) on the second premise, we know that $\Sigma; \Pi; \Gamma; \Delta_2 \Vdash e_2 : B$. So, by Lemma 6, it suffices to show that $\Sigma; \Pi; \Gamma; x : A, y : B \Vdash E_2[y] : A \otimes B$, i.e., $\Sigma; \Pi; \Gamma; x : A, y : B \Vdash \langle x, y\rangle : A \otimes B$. To prove this, assume that $\delta \in \mathcal{L}[\![\Sigma \vdash x : A, y : B\ \mathsf{ok}]\!]\ \rho\ W$. It suffices to prove that $(W, \pi(\delta), \langle\delta(x), \delta(y)\rangle) \in \mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$. By definition, $\delta \in \mathcal{L}[\![\Sigma \vdash x : A, y : B\ \mathsf{ok}]\!]\ \rho\ W$, implies that $\delta = (x \mapsto (r_1, v_1), y \mapsto (r_2, x_2))$, where $(W, r_1, x_1) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$ and $(W, r_2, x_2) \in \mathcal{V}[\![\Sigma \vdash B : \circ]\!]\rho$. The last two facts immediately imply $(W, r_1 \cdot r_2, \langle x_1, x_2\rangle) \in \mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$, i.e., $(W, \pi(\delta), \langle\delta(x), \delta(y)\rangle) \in \mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$, as required.

Proof of (2): If $\langle e_1, e_2\rangle$ is a value, then both e_1 and e_2 are values. Pick a W, $\rho \in \mathrm{Env}(\Sigma)$, such that $\rho \models_\Sigma \Pi$, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$ and for $i = 1, 2$, $\delta_i \in \mathcal{L}[\![\Sigma \vdash \Delta_i\ \mathsf{ok}]\!]\ \rho\ W$. We want to show that $(W, \pi(\gamma) \cdot \pi(\delta_1) \cdot \pi(\delta_2), \delta_1(\delta_2(\gamma(\langle e_1, e_2\rangle)))) \in \mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$.

By i.h.(2) on the first premise, we derive that $(W, \pi(\gamma) \cdot \pi(\delta_1), \delta_1(\gamma(e_1))) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$ and similarly from the second premise we obtain $(W, \pi(\gamma) \cdot \pi(\delta_2), \delta_2(\gamma(e_2))) \in \mathcal{V}[\![\Sigma \vdash B : \circ]\!]\rho$. By definition of $\mathcal{V}[\![\cdot]\!]\cdot$, we now get $(W, \pi(\gamma) \cdot \pi(\delta_1) \cdot \pi(\gamma) \cdot \pi(\delta_2), \langle\delta_1(\gamma(e_1)), \delta_2(\gamma(e_2))\rangle) \in \mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$. Observing that $\pi(\gamma) \cdot \pi(\gamma) = \pi(\gamma)$, we immediately derive $(W, \pi(\gamma) \cdot \pi(\delta_1) \cdot \pi(\delta_2), \delta_1(\delta_2(\gamma(\langle e_1, e_2\rangle)))) \in \mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$, as needed.

Case. $\dfrac{\Sigma; \Pi; \Gamma; \Delta_1 \vdash e : A \otimes B \qquad \Sigma; \Pi; \Gamma; \Delta_2, x : A, y : B \vdash e' : C}{\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \vdash \mathsf{let}\ \langle x, y\rangle = e\ \mathsf{in}\ e' : C}$

Here, statement (2) is vacuous because the term in the conclusion is not a value. To prove (1), we want to show that $\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \Vdash \mathsf{let}\ \langle x, y\rangle = e\ \mathsf{in}\ e' : C$. Define the evaluation context $E = (\mathsf{let}\ \langle x, y\rangle = [\,]\ \mathsf{in}\ e')$. Then, we want to show that $\Sigma; \Pi; \Gamma; \Delta_1, \Delta_2 \Vdash E[e] : C$. By i.h.(1) on the first premise we know that $\Sigma; \Pi; \Gamma; \Delta_1 \Vdash e : A \otimes B$. So, by Lemma 6, it is enough to show that $\Sigma; \Pi; \Gamma; \Delta_2, z : A \otimes B \Vdash E[z] : C$ or, equivalently, $\Sigma; \Pi; \Gamma; \Delta_2, z : A \otimes B \Vdash \mathsf{let}\ \langle x, y\rangle = z\ \mathsf{in}\ e' : C$. To prove this, pick W, $\rho \in \mathrm{Env}(\Sigma)$, $\rho \models_\Sigma \Pi$, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$ and $(\delta, z \mapsto (r, v)) \in \mathcal{L}[\![\Sigma \vdash \Delta_2, z : A \otimes B\ \mathsf{ok}]\!]\ \rho\ W$. We need to show that $(W, \pi(\gamma) \cdot \pi(\delta_2) \cdot r, \mathsf{let}\ \langle x, y\rangle = v\ \mathsf{in}\ \delta_2(\gamma(e'))) \in \mathcal{E}[\![C]\!]\rho$.

From $(\delta, z \mapsto (r, v)) \in \mathcal{L}[\![\Sigma \vdash \Delta_2, z : A \otimes B\ \mathsf{ok}]\!]\ \rho\ W$, we get $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$. Expanding the definition of the latter, we know that there are r_1, r_2, v_1, v_2 such that $v = \langle v_1, v_2\rangle$, $r = r_1 \cdot r_2$, $(W, r_1, v_1) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$ and $(W, r_2, v_2) \in \mathcal{V}[\![\Sigma \vdash B : \circ]\!]\rho$. By i.h.(1) on the second premise, it follows that $(W, \pi(\gamma) \cdot \pi(\delta_2) \cdot r_1 \cdot r_2, [v_2/y][v_1/x](\delta_2(\gamma(t')))) \in \mathcal{E}[\![C]\!]\rho$. Since for every h, $\langle h; \mathsf{let}\ \langle x, y\rangle = v\ \mathsf{in}\ \delta_2(\gamma(e'))\rangle \hookrightarrow \langle h; [v_2/y][v_1/x](\delta_2(\gamma(t')))\rangle$, Lemma 10 implies that $(W, \pi(\gamma) \cdot \pi(\delta_2) \cdot r, \mathsf{let}\ \langle x, y\rangle = v\ \mathsf{in}\ \delta_2(\gamma(e'))) \in \mathcal{E}[\![C]\!]\rho$, as required.

Case. $\dfrac{\Sigma, X : \sigma; \Pi, P; \Gamma; \Delta \vdash v : A \qquad i \notin \mathrm{FV}(\Pi), \mathrm{FV}(\Gamma), \mathrm{FV}(\Delta)}{\Sigma; \Pi; \Gamma; \Delta \vdash v : \forall X : \sigma :: P.\ A}$

Since the term in the conclusion is a value, we prove only (2). We want to show that $(W, \pi(\gamma)\cdot\pi(\delta), \delta(\gamma(v))) \in \mathcal{V}[\![\Sigma \vdash (\forall X : \sigma :: P.\ A) : \circ]\!]\rho$. Following the definition of $\mathcal{V}[\![\Sigma \vdash (\forall X : \sigma :: P.\ A) : \circ]\!]\rho$, assume that there is term $t \in \mathcal{S}[\![\sigma]\!]$ such that $\rho[X \mapsto t] \models_\Sigma P$. We need to show that $(W, \pi(\gamma)\cdot\pi(\delta), \delta(\gamma(v))) \in \mathcal{V}[\![\Sigma, X : \sigma \vdash A : \circ]\!]\rho[X \mapsto t]$. Define $\rho' = \rho[X \mapsto t]$. It suffices to show that $(W, \pi(\gamma)\cdot\pi(\delta), \delta(\gamma(v))) \in \mathcal{V}[\![\Sigma, X : \sigma \vdash A : \circ]\!]\rho'$.

From Lemma 11, we obtain that $\gamma \in \mathcal{U}[\![\Sigma, X : \sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho'\ W$, $\delta \in \mathcal{L}[\![\Sigma, X : \sigma \vdash \Delta\ \mathsf{ok}]\!]\ \rho'\ W$ and $\rho' \models_{\Sigma, X:\sigma} \Pi, P$. Hence, we can instantiate the i.h.(2) on the premise with ρ', γ and δ to obtain $(W, \pi(\gamma)\cdot\pi(\delta), \delta(\gamma(v))) \in \mathcal{V}[\![\Sigma, X : \sigma \vdash A : \circ]\!]\rho'$, as required.

Case. $\dfrac{\Sigma; \Pi; \Gamma; \Delta \vdash e : \forall X : \sigma :: P.\ A \qquad \Sigma \rhd t : \sigma \qquad \Sigma; \Pi \vdash [t/X]P}{\Sigma; \Pi; \Gamma; \Delta \vdash e : [t/X]A}$

Proof of (1): We want to show that $\Sigma; \Pi; \Gamma; \Delta \Vdash e : [t/X]A$. Define $E = [\ ]$. By i.h.(1) on the first premise, we know that $\Sigma; \Pi; \Gamma; \Delta \Vdash e : \forall X : \sigma :: P.\ A$, so by Lemma 6, it suffices to show that $\Sigma; \Pi; \Gamma; x : (\forall X : \sigma :: P.\ A) \Vdash E[x] : [t/X]A$ or, equivalently, $\Sigma; \Pi; \Gamma; x : (\forall X : \sigma :: P.\ A) \Vdash x : [t/X]A$. Following the definition, choose W, $\rho \in \mathrm{Env}(\Sigma)$, $\rho \models_\Sigma \Pi$, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$ and $(x \mapsto (r, v)) \in \mathcal{L}[\![\Sigma \vdash x : (\forall X : \sigma :: P.\ A)\ \mathsf{ok}]\!]\ \rho\ W$. It suffices to prove that $(W, \pi(\gamma)\cdot r, v) \in \mathcal{E}[\![[t/X]A]\!]\rho$. By Lemma 4, we reduce this to proving $(W, r, v) \in \mathcal{E}[\![[t/X]A]\!]\rho$, and by Lemma 5, to $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash [t/X]A : \circ]\!]\rho$.

Further, from the second premise we know that $\mathcal{I}[\![\Sigma \rhd t : \sigma]\!]\rho$ is defined. Let this value be d. From the third premise and Lemma 14 we know that $\rho \models_\Sigma [t/X]P$, so by Lemma 12, we get $\rho, X \mapsto d \models_{\Sigma, X:\sigma} P$. From $(x \mapsto (r, v)) \in \mathcal{L}[\![\Sigma \vdash x : (\forall X : \sigma :: P.\ A)\ \mathsf{ok}]\!]\ \rho\ W$, we know that $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash (\forall X : \sigma :: P.\ A) : \circ]\!]\rho$. Expanding the definition of $\mathcal{V}[\![\Sigma \vdash (\forall X : \sigma :: P.\ A) : \circ]\!]\rho$ at $X = d$, we get $(W, r, v) \in \mathcal{V}[\![\Sigma, X : \sigma \vdash A : \circ]\!](\rho, X \mapsto d)$. By Lemma 12, $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash [t/X]A : \circ]\!]\rho$, which is what we wanted to prove.

Proof of (2): Assume that e is a value. We want to prove that $(W, \pi(\gamma)\cdot\pi(\delta), \delta(\gamma(e))) \in \mathcal{V}[\![\Sigma \vdash [t/X]A : \circ]\!]\rho$. From i.h.(2) on the first premise, we know that $(W, \pi(\gamma)\cdot\pi(\delta), \delta(\gamma(e))) \in \mathcal{V}[\![\Sigma \vdash (\forall X : \sigma :: P.\ A) : \circ]\!]\rho$. Let $d = \mathcal{I}[\![\Sigma \rhd t : \sigma]\!]\rho$ (which is defined by the second premise). From the third premise and Lemma 14, we know that $\rho, X \mapsto d \models_{\Sigma, X:\sigma} P$. Expanding the definition of$\mathcal{V}[\![\Sigma \vdash (\forall X : \sigma :: P.\ A) : \circ]\!]\rho$ at $X = d$, we get $(W, r, v) \in \mathcal{V}[\![\Sigma, X : \sigma \vdash A : \circ]\!](\rho, X \mapsto d)$. By Lemma 12, $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash [t/X]A : \circ]\!]\rho$, which is what we wanted to prove.

Case. $\dfrac{\Sigma; \Pi; \Gamma; \Delta \vdash e : A}{\Sigma; \Pi; \Gamma; \Delta \vdash \mathsf{new}(e) : \exists \ell : \mathsf{Loc} :: \top.\ !\mathsf{ptr}\ \ell \otimes \mathsf{cap}\ \ell\ A}$

Here, the term in the conclusion is never a value, so it suffices to prove (1). We want to show that $(W, \pi(\gamma)\cdot\pi(\delta), \mathsf{new}(e)) \in \mathcal{E}[\![\exists \ell : \mathsf{Loc} :: \top.\ !\mathsf{ptr}\ \ell \otimes \mathsf{cap}\ \ell\ A]\!]\rho$. Defining $E = \mathsf{new}([\ ])$ and using Lemma 6 with the i.h.(1) on the premise, we reduce this to proving that for any $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$, we have $(W, \pi(\gamma)\cdot r, \mathsf{new}(v)) \in \mathcal{E}[\![\exists \ell : \mathsf{Loc} :: \top.\ !\mathsf{ptr}\ \ell \otimes \mathsf{cap}\ \ell\ A]\!]\rho$. Following the definition of $\mathcal{E}[\![\cdot]\!]\rho$, pick $j, s, r_\mathrm{F}, h, e'$ such that:

1. $j < W.k$
2. $(s, \pi(\gamma)\cdot r, r_\mathrm{F}) : W$
3. $\langle |s \cdot \pi(\gamma) \cdot r \cdot r_\mathrm{F}|; \mathsf{new}(v)\rangle \hookrightarrow_j \langle h; e'\rangle \not\hookrightarrow$

The operational semantics force:

4. $j = 1$
5. $e' = \langle !\ell, \bullet\rangle$ for some ℓ
6. $h = |s \cdot \pi(\gamma) \cdot r \cdot r_\mathrm{F}| \uplus [\ell : v]$

We choose $W' = \triangleright W$, $s' = s$, $r' = r \cdot [\ell : v]$, $r'_\mathrm{F} = \pi(\gamma) \cdot r_\mathrm{F}$. It suffices to prove each of the following:

(G1) $W' \sqsupseteq_j W$, i.e., $\triangleright W \sqsupseteq_1 W$

(G2) $(s', r', r'_\mathrm{F}) : W'$

(G3) $h = |s' \cdot r' \cdot r'_\mathrm{F}|$

(G4) $r'_\mathrm{F} \sqsupseteq r_\mathrm{F}$

(G5) $(W', r', e') \in \mathcal{V}[\![\Sigma \vdash \exists \ell : \mathsf{Loc} :: \top.\ !\mathsf{ptr}\ \ell \otimes \mathsf{cap}\ \ell\ A : \circ]\!]\rho$.

We prove each of these.

Proof of (G1): Immediate from Lemma 7.

Proof of (G2): Expanding the definitions of W', s', r' and r'_{F}, we need to show that $(s, r \cdot [\ell : v], \pi(\gamma) \cdot r_{\mathrm{F}}) : \triangleright W$. By Lemma 9 applied to fact 2, we get $(s, \pi(\gamma) \cdot r, r_{\mathrm{F}}) : \triangleright W$. By Lemma 3, $(s, r, \pi(\gamma) \cdot r_{\mathrm{F}}) : \triangleright W$. We complete the proof by noting that $r \cdot [\ell : v]$ and r differ only in their components on the first island (the heap), whose invariant does not depend on the local resource r at all.

Proof of (G3): Immediate from fact 6 and the definitions of s', r' and r'_{F}.

Proof of (G4): Trivial because $r'_{\mathrm{F}} = r' \cdot r_{\mathrm{F}}$.

Proof of (G5): We instantiate the definition of $\mathcal{V}[\![\Sigma \vdash \exists \ell : \mathsf{Loc} :: \top.\ !\mathsf{ptr}\ \ell \otimes \mathsf{cap}\ \ell\ A : \circ]\!]\rho$ by choosing the witness for the existential (called x in the definition) to be ℓ. It now suffices to show that $(W', r', e') \in \mathcal{V}[\![\Sigma \vdash\ !\mathsf{ptr}\ x \otimes \mathsf{cap}\ x\ A : \circ]\!](\rho, x \mapsto \ell)$ or, equivalently, $(\triangleright W, r \cdot [\ell : v], \langle !\ell, \bullet \rangle) \in \mathcal{V}[\![\Sigma \vdash\ !\mathsf{ptr}\ x \otimes \mathsf{cap}\ x\ A : \circ]\!](\rho, x \mapsto \ell)$. Because $\ell = \mathcal{I}[\![\ell]\!]\rho$, by Lemma 12, this is equivalent to proving $(\triangleright W, r \cdot [\ell : v], \langle !\ell, \bullet \rangle) \in \mathcal{V}[\![\Sigma \vdash\ !\mathsf{ptr}\ \ell \otimes \mathsf{cap}\ \ell\ A : \circ]\!]\rho$. Using the definition of $\mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$, it suffices to prove that: (G6) $(\triangleright W, \epsilon, !\ell) \in \mathcal{V}[\![\Sigma \vdash\ !\mathsf{ptr}\ \ell : \circ]\!]\rho$, and (G7) $(\triangleright W, r \cdot [\ell : v], \bullet) \in \mathcal{V}[\![\Sigma \vdash\ \mathsf{cap}\ \ell\ A : \circ]\!]\rho$. To prove (G6), it suffices to show that $(\triangleright W, \epsilon, \ell) \in \mathcal{V}[\![\Sigma \vdash\ \mathsf{ptr}\ \ell : \circ]\!]\rho$, which reduces to $\ell = \mathcal{I}[\![\ell]\!]\rho$, which is true by definition of $\mathcal{I}[\![\cdot]\!]\cdot$. To prove (G7), we must prove that $\ell = \mathcal{I}[\![\ell]\!]\rho$ and that $(\triangleright W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$. The former has already been proved and the latter follows from Lemma 2 applied to our assumption $(W, r, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$ and (G1).

Case. $\dfrac{\Sigma; \Pi; \Gamma; \Delta \vdash e : \mathsf{ptr}\ t \qquad \Sigma; \Pi; \Gamma; \Delta' \vdash e' : \mathsf{cap}\ t\ A}{\Sigma; \Pi; \Gamma; \Delta, \Delta' \vdash \mathsf{get}_{e'}\ e : A \otimes \mathsf{cap}\ t\ 1}$

Here the term in the conclusion cannot be a value, so we only have to prove (1). We want to show that $\Sigma; \Pi; \Gamma; \Delta, \Delta' \Vdash \mathsf{get}_{e'}\ e : A \otimes \mathsf{cap}\ t\ 1$. Using Lemma 6 twice with i.h.(1) on the two premises, we reduce this to proving $\Sigma; \Pi; \Gamma; x : \mathsf{ptr}\ t, y : \mathsf{cap}\ t\ A \Vdash \mathsf{get}_y\ x : A \otimes \mathsf{cap}\ t\ 1$. Expanding the definition, pick $\rho \in \mathrm{Env}(\Sigma)$ such that $\rho \models_\Sigma \Pi$, a world W, $\gamma \in \mathcal{U}[\![\Sigma \vdash \Gamma\ \mathsf{ok}]\!]\ \rho\ W$, $(W, r_1, v_1) \in \mathcal{V}[\![\Sigma \vdash\ \mathsf{ptr}\ t : \circ]\!]\rho$ and $(W, r_2, v_2) \in \mathcal{V}[\![\Sigma \vdash\ \mathsf{cap}\ t\ A : \circ]\!]\rho$. It suffices to prove that $(W, \pi(\gamma) \cdot r_1 \cdot r_2, \mathsf{get}_{v_2}\ v_1) \in \mathcal{E}[\![A \otimes \mathsf{cap}\ t\ 1]\!]\rho$. By Lemma 5, this goal is reduced to:

(G1) $(W, r_1 \cdot r_2, \mathsf{get}_{v_2}\ v_1) \in \mathcal{E}[\![A \otimes \mathsf{cap}\ t\ 1]\!]\rho$

Let $\ell = \mathcal{I}[\![t]\!]\rho$. Because $(W, r_1, v_1) \in \mathcal{V}[\![\Sigma \vdash\ \mathsf{ptr}\ t : \circ]\!]\rho$, we know that

1. $v_1 = \ell$

From $(W, r_2, v_2) \in \mathcal{V}[\![\Sigma \vdash\ \mathsf{cap}\ t\ A : \circ]\!]\rho$ we know that

2. $v_2 = \bullet$
3. $r_2 = [\ell : v] \cdot \hat{r_2}$
4. $(W, \hat{r_2}, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$

To prove (G1), we expand the definition of $\mathcal{E}[\![A \otimes \mathsf{cap}\ t\ 1]\!]\rho$ and pick j, s, r_{F}, h such that:

5. $j < W.k$
6. $(s, r_1 \cdot r_2, r_{\mathrm{F}}) : W$
7. $\langle |s \cdot r_1 \cdot r_2 \cdot r_{\mathrm{F}}|; \mathsf{get}_{v_2}\ v_1 \rangle \hookrightarrow_j \langle h; e' \rangle \not\hookrightarrow$

Now we note that from fact 3, $|s \cdot r_1 \cdot r_2 \cdot r_{\mathrm{F}}| = |s \cdot r_1 \cdot \hat{r_2} \cdot r_{\mathrm{F}}| \uplus [\ell : v]$. Therefore, the operational semantics and fact 7 force:

8. $j = 1$
9. $h = |s \cdot r_1 \cdot \hat{r_2} \cdot r_{\mathrm{F}}| \uplus [\ell : \langle\rangle]$
10. $t' = \langle v, \bullet \rangle$

We now choose $W' = \triangleright W$, $s' = s$, $r' = r_1 \cdot \hat{r_2} \cdot [\ell : \langle\rangle]$, $r'_{\mathrm{F}} = r_{\mathrm{F}}$. To prove (G1), it suffices to prove that:

(G2) $W' \sqsupseteq_j W$

(G3) $(s', r', r'_{\mathrm{F}}) : W'$

(G4) $h = |s' \cdot r' \cdot r'_{\mathrm{F}}|$

(G5) $r'_{\mathrm{F}} \sqsupseteq r_{\mathrm{F}}$

(G6) $(W', r', e') \in \mathcal{V}[\![\Sigma \vdash A \otimes \mathsf{cap}\ t\ 1 : \circ]\!]\rho$

We prove each of these subgoals below:

Proof of (G2): Because $j = 1$ and $W' = \triangleright W$, we need to prove $\triangleright W \sqsupseteq_1 W$. This follows immediately from Lemma 7.

Proof of (G3): Expanding the definitions of s', r', r'_{F} and W', it suffices to prove that $(s, r_1 \cdot \hat{r_2} \cdot [\ell : v], r_{\mathrm{F}}) : \triangleright W$. By Lemma 9 applied to fact 6, we get $(s, r_1 \cdot r_2, r_{\mathrm{F}}) : \triangleright W$. Observe that $r_1 \cdot r_2 = r_1 \cdot \hat{r_2} \cdot [\ell : v]$ differs from $r_1 \cdot \hat{r_2} \cdot [\ell : \langle\rangle]$ only on the first component, whose invariant is independent of the corresponding monoidal value. Therefore, the previously derived fact $(s, r_1 \cdot r_2, r_{\mathrm{F}}) : \triangleright W$ also implies $(s, r_1 \cdot \hat{r_2} \cdot [\ell : v], r_{\mathrm{F}}) : \triangleright W$, as needed.

Proof of (G4): Immediate from fact 9 and the choice of s', r' and r'_{F}.

Proof of (G5): Trivial because $r'_{\mathrm{F}} = r_{\mathrm{F}}$.

Proof of (G6): From fact 10, we know that $t' = \langle v, \bullet\rangle$. So, we need to prove that $(\triangleright W, r_1 \cdot \hat{r_2} \cdot [\ell : \langle\rangle], \langle v, \bullet\rangle) \in \mathcal{V}[\![\Sigma \vdash A \otimes \mathsf{cap}\ t\ 1 : \circ]\!]\rho$. By Lemma 4, we reduce this to proving $(\triangleright W, \hat{r_2} \cdot [\ell : \langle\rangle], \langle v, \bullet\rangle) \in \mathcal{V}[\![\Sigma \vdash A \otimes \mathsf{cap}\ t\ 1 : \circ]\!]\rho$. Expanding the definition of $\mathcal{V}[\![\Sigma \vdash A \otimes B : \circ]\!]\rho$, it suffices to prove that: (G6a) $(\triangleright W, \hat{r_2}, v) \in \mathcal{V}[\![\Sigma \vdash A : \circ]\!]\rho$ and (G6b) $(\triangleright W, [\ell : \langle\rangle], \bullet) \in \mathcal{V}[\![\Sigma \vdash \mathsf{cap}\ t\ 1 : \circ]\!]\rho$. (G6a) follows from fact 4 and Lemma 2. To prove (G6b), it suffices to show that $\ell = \mathcal{I}[\![t]\!]\rho$ and $(\triangleright W, \epsilon, \langle\rangle) \in \mathcal{V}[\![\Sigma \vdash 1 : \circ]\!]\rho$. The first of these is our definition of ℓ. The second follows from definition of the relation $\mathcal{V}[\![\cdot]\!]\cdot$ at the type 1.

Case.
$$\frac{\Sigma \vdash A : \sigma \to \circ \qquad \Sigma; \Pi; \Gamma; \Delta \vdash e : [A\ t] \qquad \Sigma; \Pi \vdash \mathrm{monoid}_\sigma(\epsilon, (\cdot)) \qquad \Sigma; \Pi; \Gamma; \cdot \vdash v_i : [A/\alpha]\mathrm{specT}_i}{\Sigma; \Pi; \Gamma; \Delta \vdash \mathsf{share}(e, \overline{v_i}) : \exists \alpha : \sigma \to \circ.\ [\alpha\ t] \otimes \overline{!\mathrm{specT}_i} \otimes !\mathrm{splitT} \otimes !\mathrm{joinT} \otimes !\mathrm{promoteT}}$$

where

$$\begin{aligned}
\mathrm{specT}_i &= \forall X : \sigma.\ \forall Y : \sigma'_i :: P_i.\ B_i \otimes [\alpha\ (t_i \cdot X)] \multimap \\
&\qquad \exists Z : \sigma''_i :: Q_i.\ C_i \otimes [\alpha\ (t'_i \cdot X)] \\
&\qquad \text{where } X, \alpha \notin \mathrm{FV}(P_i), \mathrm{FV}(Q_i), \mathrm{FV}(B_i), \mathrm{FV}(C_i), \mathrm{FV}(t_i), \mathrm{FV}(t'_i) \\
\mathrm{splitT} &= \forall X, Y : \sigma.\ [\alpha\ (X \cdot Y)] \multimap [\alpha\ X] \otimes [\alpha\ Y] \\
\mathrm{joinT} &= \forall X, Y : \sigma.\ [\alpha\ X] \otimes [\alpha\ Y] \multimap [\alpha\ (X \cdot Y)] \\
\mathrm{promoteT} &= \forall X : \sigma :: X = X \cdot X.\ [\alpha\ X] \multimap ![\alpha\ X] \\
\mathrm{monoid}_\sigma(\epsilon, (\cdot)) &= \forall X : \sigma.\ \epsilon \cdot X = X \wedge \\
&\quad \forall X, Y : \sigma.\ X \cdot Y = Y \cdot X \wedge \\
&\quad \forall X, Y, Z : \sigma.\ (X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)
\end{aligned}$$

Because $\mathsf{share}(e, \overline{v_i})$ is not a value, we only need to prove (1), which follows immediately from Lemma 16.

Case. All other cases are standard. □

Theorem 2 (Adequacy)**.** *If* $\cdot; \cdot; \cdot; \cdot \Vdash e : A$ *and* $\langle \emptyset; e\rangle \hookrightarrow_* \langle h; e'\rangle \not\hookrightarrow$*, then* e' *is a value.*

Proof. Since $\langle \emptyset; e\rangle \hookrightarrow_* \langle h; e'\rangle \not\hookrightarrow$, there is some j such that $\langle \emptyset; e\rangle \hookrightarrow_j \langle h; e'\rangle \not\hookrightarrow$. Pick any $n > j$ and choose $W = (n, (\mathrm{HIsland}_n))$. From $\cdot; \cdot; \cdot; \cdot \Vdash e : A$, we know that $e \in \mathcal{E}[\![A]\!]\cdot$. Instantiating its definition with the W we chose previously and $s = r = r_{\mathrm{F}} = (\epsilon)$, we immediately derive that for some W', r', $(W', r', e') \in \mathcal{V}[\![\cdot \vdash A : \circ]\!]\cdot$. From the definition $\mathcal{V}[\![\cdot]\!]\cdot$, we immediately get that e' is a value. □

Corollary 3 (Soundness of the Type System)**.** *If* $\cdot; \cdot; \cdot; \cdot \vdash e : A$ *and* $\langle \emptyset; e\rangle \hookrightarrow_* \langle h; e'\rangle \not\hookrightarrow$*, then* e' *is a value.*

Proof. Immediate from Theorems 1 and 2. □