FunTAL: Reasonably Mixing a Functional Language with Assembly (Technical Appendix)

Daniel B. Patterson James T. Perconti Christos Dimoulas Amal Ahmed

November 23, 2016

Contents

1 Typed assembly language: T

NOTE: Throughout this technical appendix, we write $\texttt{ret}\,\mathbf{end}\{\tau;\sigma\}\,\{\mathbf{r}_\mathbf{r}\}$ instead of the $\texttt{halt}\,\tau,\sigma\,\{\mathbf{r}_\mathbf{r}\}$ that appears in the accompanying paper. We apologize for any confusion caused by the slight difference in presentation.

1.1 Syntax and Semantics

$$
\begin{array}{rcl}
\tau & ::= & \alpha \mid \mathbf{unit} \mid \mathbf{int} \mid \exists\alpha.\tau \mid \mu\alpha.\tau \mid \mathbf{ref}\,\langle\tau,\ldots,\tau\rangle \mid \mathbf{box}\,\psi \\
\psi & ::= & \forall[\Delta].\{\chi;\sigma\}^{\mathbf{q}} \mid \langle\tau,\ldots,\tau\rangle \\
\mathbf{q} & ::= & \mathbf{r} \mid \mathbf{i} \mid \epsilon \mid \mathbf{end}\{\tau;\sigma\} \\
\omega & ::= & \tau \mid \sigma \mid \mathbf{q} \\
\mathbf{e} & ::= & (\mathbf{I},\mathbf{H}) \\
\mathbf{v} & ::= & (\texttt{ret}\,\mathbf{end}\{\tau;\sigma\}\,\{\mathbf{r}\},\cdot) \\
\mathbf{E} & ::= & (\mathbf{E_I},\cdot) \\
\mathbf{E_I} & ::= & [\cdot] \\
\mathbf{r} & ::= & \texttt{r1} \mid \texttt{r2} \mid \cdots \mid \texttt{r7} \mid \texttt{ra} \\
\mathbf{h} & ::= & \mathbf{code}[\Delta]\{\chi;\sigma\}^{\mathbf{q}}.\mathbf{I} \mid \langle\mathbf{w},\ldots,\mathbf{w}\rangle \\
\mathbf{w} & ::= & () \mid \mathbf{n} \mid \ell \mid \mathbf{pack}\langle\tau,\mathbf{w}\rangle\,\mathbf{as}\,\exists\alpha.\tau \mid \mathbf{fold}_{\mu\alpha.\tau}\,\mathbf{w} \mid \mathbf{w}[\omega] \\
\mathbf{u} & ::= & \mathbf{w} \mid \mathbf{r} \mid \mathbf{pack}\langle\tau,\mathbf{u}\rangle\,\mathbf{as}\,\exists\alpha.\tau \mid \mathbf{fold}_{\mu\alpha.\tau}\,\mathbf{u} \mid \mathbf{u}[\omega] \\
\mathbf{I} & ::= & \iota;\mathbf{I} \mid \texttt{jmp}\,\mathbf{u} \mid \texttt{call}\,\mathbf{u}\,\{\sigma,\mathbf{q}\} \mid \texttt{ret}\,\mathbf{r}\,\{\mathbf{r}\} \mid \texttt{ret}\,\mathbf{i}\,\{\mathbf{r}\} \mid \texttt{ret}\,\mathbf{end}\{\tau;\sigma\}\,\{\mathbf{r}\} \\
\iota & ::= & \mathbf{aop}\,\mathbf{r_d},\mathbf{r_s},\mathbf{u} \mid \texttt{bnz}\,\mathbf{r},\mathbf{u} \mid \texttt{ld}\,\mathbf{r_d},\mathbf{r_s}[\mathbf{i}] \mid \texttt{st}\,\mathbf{r_d}[\mathbf{i}],\mathbf{r_s} \mid \texttt{ralloc}\,\mathbf{r_d},\mathbf{n} \mid \texttt{balloc}\,\mathbf{r_d},\mathbf{n} \mid \texttt{mv}\,\mathbf{r_d},\mathbf{u} \\
 & & \mid \texttt{unpack}\,\langle\alpha,\mathbf{r_d}\rangle\,\mathbf{u} \mid \texttt{unfold}\,\mathbf{r_d},\mathbf{u} \mid \texttt{salloc}\,\mathbf{n} \mid \texttt{sfree}\,\mathbf{n} \mid \texttt{sld}\,\mathbf{r_d},\mathbf{i} \mid \texttt{sst}\,\mathbf{i},\mathbf{r_s} \\
\mathbf{aop} & ::= & \texttt{add} \mid \texttt{sub} \mid \texttt{mult} \\
\mathbf{H} & ::= & \cdot \mid \mathbf{H},\ell \mapsto \mathbf{h} \\
\mathbf{R} & ::= & \cdot \mid \mathbf{R},\mathbf{r} \mapsto \mathbf{w} \\
\mathbf{S} & ::= & \mathbf{nil} \mid \mathbf{w} :: \mathbf{S} \\
\mathbf{M} & ::= & (\mathbf{H},\mathbf{R},\mathbf{S}:\sigma) \\
\Psi & ::= & \cdot \mid \Psi,\ell:{}^{\nu}\psi \\
\nu & ::= & \mathbf{ref} \mid \mathbf{box} \\
\Delta & ::= & \cdot \mid \Delta,\alpha \mid \Delta,\zeta \mid \Delta,\epsilon \\
\chi & ::= & \cdot \mid \chi,\mathbf{r}:\tau \\
\sigma & ::= & \zeta \mid \bullet \mid \tau :: \sigma
\end{array}
$$

Note that we define $\mathbf{E}[\mathbf{e}]$—plugging an evaluation context $\mathbf{E}$ with a component $\mathbf{e}$—as follows:

$$(\mathbf{E_I},\cdot)[(\mathbf{I},\mathbf{H})] \stackrel{\text{def}}{=} (\mathbf{E_I}[\mathbf{I}],\mathbf{H})$$

1.1.1 Return Marker Metafunctions

The metafunctions ret-type and ret-addr-type follow the return marker in order to look up the type returned by a component, or the type of the return address, respectively.

In the case where the return marker is $\mathbf{r}$ or $\mathbf{i}$, ret-type is somewhat redundant since the result of ret-type is contained in the result of ret-addr-type. But when the return marker is $\mathbf{end}\{\tau;\sigma\}$, there is no actual return address, so only ret-type is defined. Both metafunctions are used throughout the type system.

$$\begin{aligned}
\text{ret-type}(\mathbf{r},\chi,\sigma) &= \tau;\sigma' && \text{if } \chi(\mathbf{r}) = \mathbf{box}\,\forall[].\{\mathbf{r}':\tau;\sigma'\}^{\mathbf{q}}\\
\text{ret-type}(\mathbf{i},\chi,\sigma) &= \tau;\sigma' && \text{if } \sigma(\mathbf{i}) = \mathbf{box}\,\forall[].\{\mathbf{r}':\tau;\sigma'\}^{\mathbf{q}}\\
\text{ret-type}(\mathbf{end}\{\tau;\sigma'\},\chi,\sigma) &= \tau;\sigma'
\end{aligned}$$

$$\begin{aligned}
\text{ret-addr-type}(\mathbf{r},\chi,\sigma) &= \forall[].\{\mathbf{r}':\tau;\sigma'\}^{\mathbf{q}'} && \text{if } \chi(\mathbf{r}) = \mathbf{box}\,\forall[].\{\mathbf{r}':\tau;\sigma'\}^{\mathbf{q}'}\\
\text{ret-addr-type}(\mathbf{i},\chi,\sigma) &= \forall[].\{\mathbf{r}':\tau;\sigma'\}^{\mathbf{q}'} && \text{if } \sigma(\mathbf{i}) = \mathbf{box}\,\forall[].\{\mathbf{r}':\tau;\sigma'\}^{\mathbf{q}'}
\end{aligned}$$

1.1.2 Well-Formed Type $\boxed{\Delta \vdash \tau}$

$$\frac{\alpha \in \Delta}{\Delta \vdash \alpha} \qquad \frac{}{\Delta \vdash \mathbf{unit}} \qquad \frac{}{\Delta \vdash \mathbf{int}} \qquad \frac{\Delta,\alpha \vdash \tau}{\Delta \vdash \exists\alpha.\tau} \qquad \frac{\Delta,\alpha \vdash \tau}{\Delta \vdash \mu\alpha.\tau} \qquad \frac{\Delta \vdash \langle\tau_0,\ldots,\tau_n\rangle}{\Delta \vdash \mathbf{ref}\,\langle\tau_0,\ldots,\tau_n\rangle} \qquad \frac{\Delta \vdash \psi}{\Delta \vdash \mathbf{box}\,\psi}$$

1.1.3 Well-Formed Heap Value Type $\boxed{\Delta \vdash \psi}$

The rule for the code block type uses a judgment for well-formed return markers (presented next). Note that the external type environment Δ and the formal type arguments Δ' are kept separate in that premise.

$$\frac{\Delta,\Delta' \vdash \chi \qquad \Delta,\Delta' \vdash \sigma \qquad \Delta[\Delta'];\chi;\sigma \vdash \mathbf{q}}{\Delta \vdash \forall[\Delta'].\{\chi;\sigma\}^{\mathbf{q}}} \qquad \frac{\Delta \vdash \tau_1 \qquad \cdots \qquad \Delta \vdash \tau_n}{\Delta \vdash \langle\tau_0,\ldots,\tau_n\rangle}$$

1.1.4 Well-Formed Return Marker $\boxed{\Delta[\Delta'];\chi;\sigma \vdash \mathbf{q}}$

A code block is not allowed to abstract over its own return marker. Accordingly, this judgment accepts a type variable environment in two pieces, Δ and Δ'. A return marker variable ϵ is only well-formed if ϵ appears in the outer Δ. Other return markers are well-formed if ret-type produces a type and stack type that are well formed under the combined type variable environment Δ,Δ'.

When this judgment is called by the well-formed heap type judgment (see Section 1.1.3 above), the outer Δ is the set of type variables in scope outside the code type, while the inner Δ' contains the formal type parameters. The latter may not bind an ϵ in this position.

$$\frac{\text{ret-type}(\mathbf{q},\chi,\sigma) = \tau;\sigma' \qquad \Delta,\Delta' \vdash \tau \qquad \Delta,\Delta' \vdash \sigma'}{\Delta[\Delta'];\chi;\sigma \vdash \mathbf{q}} \qquad \frac{\epsilon \in \Delta}{\Delta[\Delta'];\chi;\sigma \vdash \epsilon}$$

1.1.5 Well-Formed Register File Type $\boxed{\Delta \vdash \chi}$

$$\frac{}{\Delta \vdash \cdot} \qquad \frac{\Delta \vdash \chi \qquad \Delta \vdash \tau}{\Delta \vdash \chi,\mathbf{r}:\tau}$$

1.1.6 Well-Formed Stack Type $\boxed{\Delta \vdash \sigma}$

$$\frac{\zeta \in \Delta}{\Delta \vdash \zeta} \qquad \frac{}{\Delta \vdash \mathbf{nil}} \qquad \frac{\Delta \vdash \tau \qquad \Delta \vdash \sigma}{\Delta \vdash \tau :: \sigma}$$

1.1.7 Register File Subtyping $\boxed{\Delta \vdash \chi_1 \leq \chi_2}$

$$\frac{\Delta \vdash \chi, \chi'}{\Delta \vdash (\chi, \chi') \leq \chi}$$

1.1.8 Well-Typed Heap Fragment $\boxed{\Psi \vdash \mathbf{H} : \Psi'}$

$$\frac{\begin{array}{c}\mathrm{dom}(\Psi) \cap \mathrm{dom}(\Psi') = \emptyset \qquad \Psi' = \ell_1 :^{\nu_1} \psi_1, \ldots, \ell_n :^{\nu_n} \psi_n \\ \cdot \vdash \psi_1 \;\cdots\; \cdot \vdash \psi_n \qquad \Psi, \Psi' \vdash \mathbf{h}_1 :^{\nu_1} \psi_1 \;\cdots\; \Psi, \Psi' \vdash \mathbf{h}_n :^{\nu_n} \psi_n\end{array}}{\Psi \vdash \{\ell_1 \mapsto \mathbf{h}_1, \ldots, \ell_n \mapsto \mathbf{h}_n\} : \Psi'}$$

1.1.9 Well-Typed Register File $\boxed{\Psi \vdash \mathbf{R} : \chi}$

$$\frac{}{\Psi \vdash \cdot : \cdot} \qquad \frac{\Psi \vdash \mathbf{R} : \chi \qquad \Psi; \cdot \vdash \mathbf{w} : \tau}{\Psi \vdash \mathbf{R}, \mathbf{r} \mapsto \mathbf{w} : \chi, \mathbf{r} : \tau}$$

1.1.10 Well-Typed Stack $\boxed{\Psi \vdash \mathbf{S} : \sigma}$

$$\frac{}{\Psi \vdash \mathbf{nil} : \bullet} \qquad \frac{\Psi; \cdot \vdash \mathbf{w} : \tau \qquad \Psi \vdash \mathbf{S} : \sigma}{\Psi \vdash \mathbf{w} :: \mathbf{S} : \tau :: \sigma}$$

1.1.11 Well-Typed Memory $\boxed{\vdash \mathbf{M} : (\Psi, \chi, \sigma)}$

$$\frac{\cdot \vdash \mathbf{H} : \Psi \qquad \Psi \vdash \mathbf{R} : \chi \qquad \Psi \vdash \mathbf{S} : \sigma}{\vdash (\mathbf{H}, \mathbf{R}, \mathbf{S}) : (\Psi, \chi, \sigma)}$$

1.1.12 Well-Typed Component $\boxed{\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathbf{e} : \tau; \sigma'}$

$$\frac{\Psi \vdash \mathbf{H} : \Psi' \qquad \mathrm{boxheap}(\Psi') \qquad \text{ret-type}(\mathbf{q}, \chi, \sigma) = \tau; \sigma' \qquad (\Psi, \Psi'); \Delta; \chi; \sigma; \mathbf{q} \vdash \mathbf{I}}{\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash (\mathbf{I}, \mathbf{H}) : \tau; \sigma'}$$

$\mathrm{boxheap}(\Psi) \stackrel{\text{def}}{=} \forall (\ell :^{\nu} \psi) \in \Psi.\ \nu = \mathbf{box}$

1.1.13 Well-Typed Heap Value $\boxed{\Psi \vdash \mathrm{h} : {}^{\nu}\psi}$

$$\frac{\cdot \vdash \forall[\Delta].\{\chi;\sigma\}^{\mathrm{q}} \qquad \Psi;\Delta;\chi;\sigma;\mathrm{q} \vdash \mathrm{I}}{\Psi \vdash \mathrm{code}[\Delta]\{\chi;\sigma\}^{\mathrm{q}}.\mathrm{I} : {}^{\mathrm{box}}\forall[\Delta].\{\chi;\sigma\}^{\mathrm{q}}} \qquad \frac{\Psi;\cdot \vdash \mathrm{w}_0 : \tau_0 \qquad \cdots \qquad \Psi;\cdot \vdash \mathrm{w}_{\mathrm{n}} : \tau_{\mathrm{n}}}{\Psi \vdash \langle \mathrm{w}_0, \ldots, \mathrm{w}_{\mathrm{n}} \rangle : {}^{\nu}\langle \tau_0, \ldots, \tau_{\mathrm{n}} \rangle}$$

1.1.14 Well-Typed Word Value $\boxed{\Psi;\Delta \vdash \mathrm{w} : \tau}$

$$\frac{}{\Psi;\Delta \vdash () : \mathrm{unit}} \qquad \frac{}{\Psi;\Delta \vdash \mathrm{n} : \mathrm{int}} \qquad \frac{\ell : {}^{\mathrm{ref}}\psi \in \Psi}{\Psi;\Delta \vdash \ell : \mathrm{ref}\ \psi} \qquad \frac{\ell : {}^{\mathrm{box}}\psi \in \Psi}{\Psi;\Delta \vdash \ell : \mathrm{box}\ \psi}$$

$$\frac{\Psi;\Delta \vdash \mathrm{w} : \tau[\tau'/\alpha]}{\Psi;\Delta \vdash \mathrm{pack}\langle \tau', \mathrm{w} \rangle\ \mathrm{as}\ \exists\alpha.\tau : \exists\alpha.\tau} \qquad \frac{\Psi;\Delta \vdash \mathrm{w} : \tau[\mu\alpha.\tau/\alpha]}{\Psi;\Delta \vdash \mathrm{fold}_{\mu\alpha.\tau}\ \mathrm{w} : \mu\alpha.\tau}$$

$$\frac{\Psi;\Delta \vdash \mathrm{w} : \mathrm{box}\,\forall[\alpha,\Delta'].\{\chi;\sigma\}^{\mathrm{q}} \qquad \Delta \vdash \tau}{\Psi;\Delta \vdash \mathrm{w}[\tau] : \mathrm{box}\,\forall[\Delta'].\{\chi[\tau/\alpha];\sigma[\tau/\alpha]\}^{\mathrm{q}[\tau/\alpha]}}$$

$$\frac{\Psi;\Delta \vdash \mathrm{w} : \mathrm{box}\,\forall[\zeta,\Delta'].\{\chi;\sigma\}^{\mathrm{q}} \qquad \Delta \vdash \sigma'}{\Psi;\Delta \vdash \mathrm{w}[\sigma'] : \mathrm{box}\,\forall[\Delta'].\{\chi[\sigma'/\zeta];\sigma[\sigma'/\zeta]\}^{\mathrm{q}[\sigma'/\zeta]}}$$

$$\frac{\Psi;\Delta \vdash \mathrm{w} : \mathrm{box}\,\forall[\epsilon,\Delta'].\{\chi;\sigma\}^{\mathrm{q}} \qquad \mathrm{ftv}(\mathrm{q}') \subseteq \Delta \qquad \Delta \vdash \forall[\Delta'].\{\chi[\mathrm{q}'/\epsilon];\sigma[\mathrm{q}'/\epsilon]\}^{\mathrm{q}[\mathrm{q}'/\epsilon]}}{\Psi;\Delta \vdash \mathrm{w}[\mathrm{q}'] : \mathrm{box}\,\forall[\Delta'].\{\chi[\mathrm{q}'/\epsilon];\sigma[\mathrm{q}'/\epsilon]\}^{\mathrm{q}[\mathrm{q}'/\epsilon]}}$$

1.1.15 Well-Typed Small Value $\boxed{\Psi;\Delta;\chi \vdash \mathrm{u} : \tau}$

$$\frac{\Psi;\Delta \vdash \mathrm{w} : \tau}{\Psi;\Delta;\chi \vdash \mathrm{w} : \tau} \qquad \frac{\mathrm{r} : \tau \in \chi}{\Psi;\Delta;\chi \vdash \mathrm{r} : \tau} \qquad \frac{\Psi;\Delta;\chi \vdash \mathrm{u} : \tau[\tau'/\alpha]}{\Psi;\Delta;\chi \vdash \mathrm{pack}\langle \tau', \mathrm{u} \rangle\ \mathrm{as}\ \exists\alpha.\tau : \exists\alpha.\tau}$$

$$\frac{\Psi;\Delta;\chi \vdash \mathrm{u} : \tau[\mu\alpha.\tau/\alpha]}{\Psi;\Delta;\chi \vdash \mathrm{fold}_{\mu\alpha.\tau}\ \mathrm{u} : \mu\alpha.\tau} \qquad \frac{\Psi;\Delta;\chi \vdash \mathrm{u} : \mathrm{box}\,\forall[\alpha,\Delta'].\{\chi;\sigma\}^{\mathrm{q}} \qquad \Delta \vdash \tau}{\Psi;\Delta;\chi \vdash \mathrm{u}[\tau] : \mathrm{box}\,\forall[\Delta'].\{\chi[\tau/\alpha];\sigma[\tau/\alpha]\}^{\mathrm{q}[\tau/\alpha]}}$$

$$\frac{\Psi;\Delta;\chi \vdash \mathrm{u} : \mathrm{box}\,\forall[\zeta,\Delta'].\{\chi';\sigma\}^{\mathrm{q}} \qquad \Delta \vdash \sigma'}{\Psi;\Delta;\chi \vdash \mathrm{u}[\sigma'] : \mathrm{box}\,\forall[\Delta'].\{\chi'[\sigma'/\zeta];\sigma[\sigma'/\zeta]\}^{\mathrm{q}[\sigma'/\zeta]}}$$

$$\frac{\Psi;\Delta;\chi \vdash \mathrm{u} : \mathrm{box}\,\forall[\epsilon,\Delta'].\{\chi';\sigma\}^{\mathrm{q}} \qquad \mathrm{ftv}(\mathrm{q}') \subseteq \Delta \qquad \Delta \vdash \forall[\Delta'].\{\chi'[\mathrm{q}'/\epsilon];\sigma[\mathrm{q}'/\epsilon]\}^{\mathrm{q}[\mathrm{q}'/\epsilon]}}{\Psi;\Delta;\chi \vdash \mathrm{u}[\mathrm{q}'] : \mathrm{box}\,\forall[\Delta'].\{\chi'[\mathrm{q}'/\epsilon];\sigma[\mathrm{q}'/\epsilon]\}^{\mathrm{q}[\mathrm{q}'/\epsilon]}}$$

1.1.16 Well-Typed Instruction Sequence $\boxed{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash \mathrm{I}}$

As a side-condition on this judgment, the environment q must not be ϵ (This can be written $\cdot[\Delta];\chi;\sigma\vdash \mathrm{q}$). This argument gives the position of the return address, and a component never abstracts over its own return address.

The rule for sequencing instructions is straightforward: we use the postconditions of the initial instruction ι as preconditions to type check the remaining instructions.

$$\frac{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash \iota \Rightarrow \Delta';\chi';\sigma';\mathrm{q}' \qquad \Psi;\Delta';\chi';\sigma';\mathrm{q}'\vdash \mathrm{I}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash \iota;\mathrm{I}}$$

The return instruction typechecks if the indicated point to return to matches the return marker in the environment, and if the register containing the result has the right type. Note that our type system does not permit returns to an address stored on the stack.

$$\frac{\chi(\mathrm{r}) = \mathrm{box}\,\forall[].\{\mathrm{r}':\tau;\sigma\}^{\mathrm{q}'} \qquad \chi(\mathrm{r}') = \tau}{\Psi;\Delta;\chi;\sigma;\mathrm{r}\vdash \mathtt{ret}\ \mathrm{r}\ \{\mathrm{r}'\}} \qquad \frac{\chi(\mathrm{r}) = \tau}{\Psi;\Delta;\chi;\sigma;\mathrm{end}\{\tau;\sigma\}\vdash \mathtt{ret}\ \mathrm{end}\{\tau;\sigma\}\ \{\mathrm{r}\}}$$

The jump instruction is used to continue to the next code block within a component, or equivalently, to make a tail call. This requires that the code block we jump to share the current return marker, and that its preconditions are consistent with the current types of the register file and stack.

$$\frac{\Psi;\Delta;\chi\vdash \mathrm{u}:\mathrm{box}\,\forall[].\{\chi';\sigma\}^{\mathrm{q}} \qquad \Delta\vdash \chi\leq\chi' \qquad \cdot[\Delta];\chi;\sigma\vdash \mathrm{q}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash \mathtt{jmp}\ \mathrm{u}}$$

To call a subroutine, we are required to protect the current return address by storing it in the tail of the stack that is parametrically hidden from the subroutine. The type rule compares the caller's view of the stack at the time the call is made, σ, to the subroutine's view at the time of the call, $\hat{\sigma}$. It also looks at the subroutine's view at return time, $\hat{\sigma}'$. At both points, the subroutine's view contains an abstract stack tail ζ that must be instantiated by the caller's stack tail type σ_0. The return marker of the caller must be some i that points far enough into σ that the return address is in σ_0. At return time, the part of the stack that was not hidden from the subroutine could have changed length, so the return marker after the subroutine, which instantiates the subroutine's type variable ϵ, must accordingly change.

We also have a type rule for the case of calling a subroutine from the top level, when there is no return address and the return marker is $\mathrm{end}\{\tau;\sigma^*\}$. This case works the same way, except that there is no need to worry about lengths of stacks.

We use the shorthand $\Delta\vdash\chi\setminus\mathrm{q}$ in the following typing rules to ensure that, in the case that q is some register r in the domain of χ, then χ without the mapping for r should be well formed under Δ.

$$\begin{array}{lcll}\Delta\vdash\chi\setminus\mathrm{i} & \stackrel{\mathrm{def}}{=} & \Delta\vdash\chi & \\ \Delta\vdash\chi\setminus\mathrm{r} & \stackrel{\mathrm{def}}{=} & \Delta\vdash\chi & \text{if } \mathrm{r}\notin\mathrm{dom}(\chi)\\ \Delta\vdash\chi_1,\mathrm{r}:\tau,\chi_2\setminus\mathrm{r} & \stackrel{\mathrm{def}}{=} & \Delta\vdash\chi_1,\chi_2 & \end{array}$$

$$\frac{\begin{array}{c}\Psi;\Delta;\chi\vdash \mathrm{u}:\mathrm{box}\,\forall[\zeta,\epsilon].\{\hat{\chi};\hat{\sigma}\}^{\hat{\mathrm{q}}} \qquad \Delta\vdash\hat{\chi}\setminus\hat{\mathrm{q}} \qquad \text{ret-addr-type}(\hat{\mathrm{q}},\hat{\chi},\hat{\sigma}) = \forall[].\{\mathrm{r}:\tau;\hat{\sigma}'\}^{\epsilon} \qquad \Delta\vdash\tau\\ \Delta\vdash\hat{\sigma}'[\sigma_0/\zeta] \qquad \Delta\vdash\forall[].\{\hat{\chi}[\sigma_0/\zeta][\mathrm{i}+\mathrm{k}-\mathrm{j}/\epsilon];\hat{\sigma}[\sigma_0/\zeta][\mathrm{i}+\mathrm{k}-\mathrm{j}/\epsilon]\}^{\hat{\mathrm{q}}} \qquad \Delta\vdash\chi\leq\hat{\chi}[\sigma_0/\zeta][\mathrm{i}+\mathrm{k}-\mathrm{j}/\epsilon]\\ \sigma=\tau_0::\cdots::\tau_{\mathrm{j}}::\sigma_0 \qquad \hat{\sigma}=\tau_0::\cdots::\tau_{\mathrm{j}}::\zeta \qquad \mathrm{j}<\mathrm{i} \qquad \hat{\sigma}'=\tau'_0::\cdots::\tau'_{\mathrm{k}}::\zeta\end{array}}{\Psi;\Delta;\chi;\sigma;\mathrm{i}\vdash \mathtt{call}\ \mathrm{u}\ \{\sigma_0,\mathrm{i}+\mathrm{k}-\mathrm{j}\}}$$

$$\frac{\begin{array}{c}\Psi;\Delta;\chi\vdash \mathrm{u}:\mathrm{box}\,\forall[\zeta,\epsilon].\{\hat{\chi};\hat{\sigma}\}^{\hat{\mathrm{q}}}\\ \Delta\vdash\hat{\chi}\setminus\hat{\mathrm{q}} \qquad \text{ret-addr-type}(\hat{\mathrm{q}},\hat{\chi},\hat{\sigma}) = \mathrm{box}\,\forall[].\{\mathrm{r}:\tau;\hat{\sigma}'\}^{\epsilon} \qquad \Delta\vdash\tau \qquad \Delta\vdash\hat{\sigma}'[\sigma_0/\zeta]\\ \Delta\vdash\forall[].\{\hat{\chi}[\sigma_0/\zeta][\mathrm{end}\{\tau^*;\sigma^*\}/\epsilon];\hat{\sigma}[\sigma_0/\zeta][\mathrm{end}\{\tau^*;\sigma^*\}/\epsilon]\}^{\hat{\mathrm{q}}} \qquad \Delta\vdash\chi\leq\hat{\chi}[\sigma_0/\zeta][\mathrm{end}\{\tau^*;\sigma^*\}/\epsilon]\\ \sigma=\overline{\tau}::\sigma_0 \qquad \hat{\sigma}=\overline{\tau}::\zeta \qquad \hat{\sigma}'=\overline{\tau'}::\zeta\end{array}}{\Psi;\Delta;\chi;\sigma;\mathrm{end}\{\tau^*;\sigma^*\}\vdash \mathtt{call}\ \mathrm{u}\ \{\sigma_0,\mathrm{end}\{\tau^*;\sigma^*\}\}}$$

1.1.17 Well-Typed Instruction $\boxed{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\iota\Rightarrow\Delta';\chi';\sigma';\mathrm{q}'}$

As a side-condition on this judgment, the environment q must not be ϵ.

This judgment uses the following two metafunctions:

$$\mathrm{inc}(\mathrm{q},\mathrm{n})=\begin{cases}\mathrm{i}+\mathrm{n} & \mathrm{q}=\mathrm{i}\\ \mathrm{q} & \text{otherwise}\end{cases}\qquad \mathrm{dec}(\mathrm{q},\mathrm{n})=\begin{cases}\mathrm{i}-\mathrm{n} & \mathrm{q}=\mathrm{i}\geq\mathrm{n}\\ \text{undefined} & \mathrm{q}=\mathrm{i}<\mathrm{n}\\ \mathrm{q} & \text{otherwise}\end{cases}$$

$$\frac{\Psi;\Delta;\chi\vdash\mathrm{r_s}:\mathrm{int}\qquad\Psi;\Delta;\chi\vdash\mathrm{u}:\mathrm{int}\qquad\mathrm{q}\neq\mathrm{r_d}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{aop}\ \mathrm{r_d},\mathrm{r_s},\mathrm{u}\Rightarrow\Delta;\chi[\mathrm{r_d}:\mathrm{int}];\sigma;\mathrm{q}}$$

$$\frac{\Psi;\Delta;\chi\vdash\mathrm{r_{test}}:\mathrm{int}\qquad\Psi;\Delta;\chi\vdash\mathrm{u}:\mathrm{box}\,\forall[].\{\chi';\sigma\}^{\mathrm{q}}\qquad\Delta\vdash\chi\leq\chi'}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{bnz}\ \mathrm{r_{test}},\mathrm{u}\Rightarrow\Delta;\chi;\sigma;\mathrm{q}}$$

$$\frac{\Psi;\Delta;\chi\vdash\mathrm{r_s}:\mathrm{ref}\,\langle\tau_0,\ldots,\tau_\mathrm{n}\rangle\qquad0\leq\mathrm{i}\leq\mathrm{n}\qquad\mathrm{q}\neq\mathrm{r_d}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{ld}\ \mathrm{r_d},\mathrm{r_s}[\mathrm{i}]\Rightarrow\Delta;\chi[\mathrm{r_d}:\tau_\mathrm{i}];\sigma;\mathrm{q}}$$

$$\frac{\Psi;\Delta;\chi\vdash\mathrm{r_s}:\mathrm{box}\,\langle\tau_0,\ldots,\tau_\mathrm{n}\rangle\qquad0\leq\mathrm{i}\leq\mathrm{n}\qquad\mathrm{q}\neq\mathrm{r_d}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{ld}\ \mathrm{r_d},\mathrm{r_s}[\mathrm{i}]\Rightarrow\Delta;\chi[\mathrm{r_d}:\tau_\mathrm{i}];\sigma;\mathrm{q}}$$

$$\frac{\Psi;\Delta;\chi\vdash\mathrm{r_d}:\mathrm{ref}\,\langle\tau_0,\ldots,\tau_\mathrm{n}\rangle\qquad0\leq\mathrm{i}\leq\mathrm{n}\qquad\Psi;\Delta;\chi\vdash\mathrm{r_s}:\tau_\mathrm{i}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{st}\ \mathrm{r_d}[\mathrm{i}],\mathrm{r_s}\Rightarrow\Delta;\chi[\mathrm{r_d}:\mathrm{ref}\,\langle\tau_0,\ldots,\tau_\mathrm{n}\rangle];\sigma;\mathrm{q}}$$

$$\frac{\mathrm{len}(\overline{\tau})=\mathrm{n}\qquad\mathrm{q}\neq\mathrm{r_d}\qquad\chi'=\chi[\mathrm{r_d}:\mathrm{ref}\,\langle\overline{\tau}\rangle]\qquad\mathrm{q}'=\mathrm{dec}(\mathrm{q},\mathrm{n})}{\Psi;\Delta;\chi;\overline{\tau}::\sigma;\mathrm{q}\vdash\mathtt{ralloc}\ \mathrm{r_d},\mathrm{n}\Rightarrow\Delta;\chi';\sigma;\mathrm{q}'}$$

$$\frac{\mathrm{len}(\overline{\tau})=\mathrm{n}\qquad\mathrm{q}\neq\mathrm{r_d}\qquad\chi'=\chi[\mathrm{r_d}:\mathrm{box}\,\langle\overline{\tau}\rangle]\qquad\mathrm{q}'=\mathrm{dec}(\mathrm{q},\mathrm{n})}{\Psi;\Delta;\chi;\overline{\tau}::\sigma;\mathrm{q}\vdash\mathtt{balloc}\ \mathrm{r_d},\mathrm{n}\Rightarrow\Delta;\chi';\sigma;\mathrm{q}'}$$

$$\frac{\Psi;\Delta;\chi\vdash\mathrm{u}:\tau\qquad\mathrm{q}\neq\mathrm{r_d}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{mv}\ \mathrm{r_d},\mathrm{u}\Rightarrow\Delta;\chi[\mathrm{r_d}:\tau];\sigma;\mathrm{q}}$$

$$\frac{\chi(\mathrm{r_s})=\tau}{\Psi;\Delta;\chi;\sigma;\mathrm{r_s}\vdash\mathtt{mv}\ \mathrm{r_d},\mathrm{r_s}\Rightarrow\Delta;\chi[\mathrm{r_d}:\tau];\sigma;\mathrm{r_d}}$$

$$\frac{\Psi;\Delta;\chi\vdash\mathrm{u}:\exists\alpha.\tau\qquad\mathrm{q}\neq\mathrm{r_d}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{unpack}\ \langle\alpha,\mathrm{r_d}\rangle\ \mathrm{u}\Rightarrow\Delta,\alpha;\chi[\mathrm{r_d}:\tau];\sigma;\mathrm{q}}$$

$$\frac{\Psi;\Delta;\chi\vdash\mathrm{u}:\mu\alpha.\tau\qquad\mathrm{q}\neq\mathrm{r_d}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{unfold}\ \mathrm{r_d},\mathrm{u}\Rightarrow\Delta;\chi[\mathrm{r_d}:\tau[\mu\alpha.\tau/\alpha]];\sigma;\mathrm{q}}$$

$$\frac{\sigma'=\mathrm{unit}::\cdots^{\mathrm{n}}::\mathrm{unit}::\sigma\qquad\mathrm{q}'=\mathrm{inc}(\mathrm{q},\mathrm{n})}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{salloc}\ \mathrm{n}\Rightarrow\Delta;\chi;\sigma';\mathrm{q}'}$$

$$\frac{\sigma=\tau_0::\cdots::\tau_{\mathrm{n}-1}::\sigma'\qquad\mathrm{q}'=\mathrm{dec}(\mathrm{q},\mathrm{n})}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{sfree}\ \mathrm{n}\Rightarrow\Delta;\chi;\sigma';\mathrm{q}'}$$

$$\frac{\sigma=\tau_0::\cdots::\tau_\mathrm{i}::\sigma'\qquad\mathrm{q}\neq\mathrm{r_d}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{sld}\ \mathrm{r_d},\mathrm{i}\Rightarrow\Delta;\chi[\mathrm{r_d}:\tau_\mathrm{i}];\sigma;\mathrm{q}}$$

$$\frac{\sigma=\tau_0::\cdots::\tau_\mathrm{i}::\sigma'}{\Psi;\Delta;\chi;\sigma;\mathrm{i}\vdash\mathtt{sld}\ \mathrm{r_d},\mathrm{i}\Rightarrow\Delta;\chi[\mathrm{r_d}:\tau_\mathrm{i}];\sigma;\mathrm{r_d}}$$

$$\frac{\Psi;\chi;\Delta\vdash\mathrm{r_s}:\tau'\qquad\sigma=\tau_0::\cdots::\tau_\mathrm{i}::\sigma_0\qquad\sigma'=\tau_0::\cdots::\tau_{\mathrm{i}-1}::\tau'::\sigma_0\qquad\mathrm{q}\neq\mathrm{i}}{\Psi;\Delta;\chi;\sigma;\mathrm{q}\vdash\mathtt{sst}\ \mathrm{i},\mathrm{r_s}\Rightarrow\Delta;\chi;\sigma';\mathrm{q}}$$

$$\frac{\Psi;\chi;\Delta\vdash\mathrm{r_s}:\tau'\qquad\sigma=\tau_0::\cdots::\tau_\mathrm{i}::\sigma_0\qquad\sigma'=\tau_0::\cdots::\tau_{\mathrm{i}-1}::\tau'::\sigma_0}{\Psi;\Delta;\chi;\sigma;\mathrm{r_s}\vdash\mathtt{sst}\ \mathrm{i},\mathrm{r_s}\Rightarrow\Delta;\chi;\sigma';\mathrm{i}}$$

1.1.18 Reduction Relation

1.1.19 Instruction Sequence Reduction Relation $\boxed{\langle \mathbf{M} \mid \mathbf{I}\rangle \longrightarrow \langle \mathbf{M'} \mid \mathbf{I'}\rangle}$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{aop}\ \mathbf{r_d},\mathbf{r_s},\mathbf{u};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R}[\mathbf{r_d} \mapsto \delta(\mathbf{aop},\mathbf{R}(\mathbf{r_s}),\hat{\mathbf{R}}(\mathbf{u}))],\mathbf{S}) \mid \mathbf{I}\rangle$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{bnz}\ \mathbf{r},\mathbf{u};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathbf{I}\rangle \quad \text{if } \mathbf{R}(\mathbf{r}) = \mathbf{0}$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{bnz}\ \mathbf{r},\mathbf{u};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathbf{I'}[\overline{\omega}/\boldsymbol{\Delta}]\rangle \quad \text{if } \mathbf{R}(\mathbf{r}) = \mathbf{n}, \mathbf{n} \neq \mathbf{0}$$
$$\text{where } \hat{\mathbf{R}}(\mathbf{u}) = \boldsymbol{\ell}[\overline{\omega}] \text{ and } \mathbf{H}(\boldsymbol{\ell}) = \mathbf{code}[\boldsymbol{\Delta}]\{\chi;\sigma\}^{\mathbf{q}}.\mathbf{I'}$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{ld}\ \mathbf{r_d},\mathbf{r_s}[\mathbf{i}];\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R}[\mathbf{r_d} \mapsto \mathbf{w_i}],\mathbf{S}) \mid \mathbf{I}\rangle$$
$$\text{where } \mathbf{R}(\mathbf{r_s}) = \boldsymbol{\ell} \text{ and } \mathbf{H}(\boldsymbol{\ell}) = \langle \mathbf{w_0},\ldots,\mathbf{w_i},\ldots,\mathbf{w_n}\rangle$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{st}\ \mathbf{r_d}[\mathbf{i}],\mathbf{r_s};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H}[\boldsymbol{\ell} \mapsto \langle \mathbf{w_0},\ldots,\mathbf{w'},\ldots,\mathbf{w_n}\rangle],\mathbf{R},\mathbf{S}) \mid \mathbf{I}\rangle$$
$$\text{where } \mathbf{R}(\mathbf{r_s}) = \mathbf{w'}, \mathbf{R}(\mathbf{r_d}) = \boldsymbol{\ell}, \text{and } \mathbf{H}(\boldsymbol{\ell}) = \langle \mathbf{w_0},\ldots,\mathbf{w_i},\ldots,\mathbf{w_n}\rangle$$

$$\langle (\mathbf{H},\mathbf{R},\overline{\mathbf{w}} :: \mathbf{S}) \mid \mathtt{ralloc}\ \mathbf{r_d},\mathbf{n};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H}[\boldsymbol{\ell} \mapsto \langle \overline{\mathbf{w}}\rangle],\mathbf{R}[\mathbf{r_d} \mapsto \boldsymbol{\ell}],\mathbf{S}) \mid \mathbf{I}\rangle \quad \text{if } \boldsymbol{\ell} \notin \mathrm{dom}(\mathbf{H}), \mathrm{len}(\overline{\mathbf{w}}) = \mathbf{n}$$

$$\langle (\mathbf{H},\mathbf{R},\overline{\mathbf{w}} :: \mathbf{S}) \mid \mathtt{balloc}\ \mathbf{r_d},\mathbf{n};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H}[\boldsymbol{\ell} \mapsto \langle \overline{\mathbf{w}}\rangle],\mathbf{R}[\mathbf{r_d} \mapsto \boldsymbol{\ell}],\mathbf{S}) \mid \mathbf{I}\rangle \quad \text{if } \boldsymbol{\ell} \notin \mathrm{dom}(\mathbf{H}), \mathrm{len}(\overline{\mathbf{w}}) = \mathbf{n}$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{mv}\ \mathbf{r_d},\mathbf{u};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R}[\mathbf{r_d} \mapsto \hat{\mathbf{R}}(\mathbf{u})],\mathbf{S}) \mid \mathbf{I}\rangle$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{unpack}\ \langle \alpha,\mathbf{r_d}\rangle\ \mathbf{u};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R}[\mathbf{r_d} \mapsto \mathbf{w}],\mathbf{S}) \mid \mathbf{I}[\tau'/\alpha]\rangle$$
$$\text{where } \hat{\mathbf{R}}(\mathbf{u}) = \mathbf{pack}\langle \tau',\mathbf{w}\rangle \text{ as } \exists\alpha.\tau$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{unfold}\ \mathbf{r_d},\mathbf{u};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R}[\mathbf{r_d} \mapsto \mathbf{w}],\mathbf{S}) \mid \mathbf{I}\rangle \quad \text{where } \hat{\mathbf{R}}(\mathbf{u}) = \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{w}$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{salloc}\ \mathbf{n};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R},\overline{()} :: \mathbf{S}) \mid \mathbf{I}\rangle \quad \mathrm{len}(\overline{()}) = \mathbf{n}$$

$$\langle (\mathbf{H},\mathbf{R},\overline{\mathbf{w}} :: \mathbf{S}) \mid \mathtt{sfree}\ \mathbf{n};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathbf{I}\rangle \quad \mathrm{len}(\overline{\mathbf{w}}) = \mathbf{n}$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{sld}\ \mathbf{r_d},\mathbf{i};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R}[\mathbf{r_d} \mapsto \mathbf{w_i}],\mathbf{S}) \mid \mathbf{I}\rangle \quad \text{where } \mathbf{S} = \mathbf{w_0} :: \cdots :: \mathbf{w_i} :: \mathbf{S_0}$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{sst}\ \mathbf{i},\mathbf{r_s};\mathbf{I}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R},\mathbf{S'}) \mid \mathbf{I}\rangle$$
$$\text{where } \mathbf{R}(\mathbf{r_s}) = \mathbf{w'},$$
$$\mathbf{S} = \mathbf{w_0} :: \cdots :: \mathbf{w_i} :: \mathbf{S_0}, \text{ and } \mathbf{S'} = \mathbf{w_0} :: \cdots :: \mathbf{w'} :: \mathbf{S_0},$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{jmp}\ \mathbf{u}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathbf{I}[\overline{\omega}/\boldsymbol{\Delta}]\rangle$$
$$\text{where } \hat{\mathbf{R}}(\mathbf{u}) = \boldsymbol{\ell}[\overline{\omega}] \text{ and } \mathbf{H}(\boldsymbol{\ell}) = \mathbf{code}[\boldsymbol{\Delta}]\{\chi;\sigma\}^{\mathbf{q}}.\mathbf{I}$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{call}\ \mathbf{u}\ \{\sigma,\mathbf{q}\}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathbf{I}[\overline{\omega}/\boldsymbol{\Delta}][\sigma/\zeta][\mathbf{q}/\epsilon]\rangle$$
$$\text{where } \hat{\mathbf{R}}(\mathbf{u}) = \boldsymbol{\ell}[\overline{\omega}] \text{ and } \mathbf{H}(\boldsymbol{\ell}) = \mathbf{code}[\boldsymbol{\Delta},\zeta,\epsilon]\{\chi;\sigma\}^{\mathbf{q}}.\mathbf{I}$$

$$\langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathtt{ret}\ \mathbf{r}\ \{\mathbf{r'}\}\rangle \longrightarrow \langle (\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathbf{I}[\overline{\omega}/\boldsymbol{\Delta}]\rangle$$
$$\text{where } \mathbf{R}(\mathbf{r}) = \boldsymbol{\ell}[\overline{\omega}] \text{ and } \mathbf{H}(\boldsymbol{\ell}) = \mathbf{code}[\boldsymbol{\Delta}]\{\chi;\sigma\}^{\mathbf{q}}.\mathbf{I}$$

where

$$\begin{aligned}
\hat{\mathbf{R}}(\mathbf{w}) &= \mathbf{w}\\
\hat{\mathbf{R}}(\mathbf{r}) &= \mathbf{R}(\mathbf{r})\\
\hat{\mathbf{R}}(\mathbf{u}[\omega]) &= (\hat{\mathbf{R}}(\mathbf{u}))[\omega]\\
\hat{\mathbf{R}}(\mathbf{pack}\langle \tau',\mathbf{u}\rangle \text{ as } \exists\alpha.\tau) &= \mathbf{pack}\langle \tau',\hat{\mathbf{R}}(\mathbf{u})\rangle \text{ as } \exists\alpha.\tau\\
\hat{\mathbf{R}}(\mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{u}) &= \mathbf{fold}_{\mu\alpha.\tau}\ (\hat{\mathbf{R}}(\mathbf{u}))
\end{aligned}$$

$$\begin{aligned}
\delta(\mathbf{add},\mathbf{n_1},\mathbf{n_2}) &= \mathbf{n_1} + \mathbf{n_2}\\
\delta(\mathbf{sub},\mathbf{n_1},\mathbf{n_2}) &= \mathbf{n_1} - \mathbf{n_2}\\
\delta(\mathbf{mul},\mathbf{n_1},\mathbf{n_2}) &= \mathbf{n_1} * \mathbf{n_2}
\end{aligned}$$

1.1.20 Component Reduction Relation $\boxed{\langle \mathbf{M} \mid \mathbf{e} \rangle \longmapsto \langle \mathbf{M'} \mid \mathbf{e'} \rangle}$

For purposes of our step-indexed logical relation, we consider the reduction rule that loads heap values from a component's heap fragment into the main program heap to take 0 reduction steps.

$$\langle (\mathbf{H}, \mathbf{R}, \mathbf{S}) \mid (\mathbf{I}, (\ell \mapsto \mathbf{h}, \mathbf{H'})) \rangle \longmapsto^0 \langle ((\mathbf{H}, \ell' \mapsto \mathbf{h}[\ell'/\ell]), \mathbf{R}, \mathbf{S}) \mid (\mathbf{I}[\ell'/\ell], \mathbf{H'}[\ell'/\ell]) \rangle \qquad \ell' \notin \mathrm{dom}(\mathbf{H})$$

$$\frac{\langle \mathbf{M} \mid \mathbf{I} \rangle \longrightarrow \langle \mathbf{M'} \mid \mathbf{I'} \rangle}{\langle \mathbf{M} \mid (\mathbf{I}, \cdot) \rangle \longmapsto \langle \mathbf{M'} \mid (\mathbf{I'}, \cdot) \rangle}$$

1.2 Contexts and Contextual Equivalence

$$\begin{aligned} \mathbf{C} &::= (\mathbf{C_I}, \mathbf{H}) \mid (\mathbf{I}, \mathbf{C_H}) \\ \mathbf{C_I} &::= [\cdot] \mid \iota; \mathbf{C_I} \\ \mathbf{C_H} &::= \mathbf{C_H}, \ell \mapsto \mathbf{h} \mid \mathbf{H}, \ell \mapsto \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{C_I} \end{aligned}$$

1.2.1 Plug Function $\boxed{C[e]}$

$$\begin{aligned} (\mathbf{C_I}, \mathbf{H})[(\mathbf{I}, \mathbf{H'})] &= (\mathbf{C_I}[\mathbf{I}], (\mathbf{H}, \mathbf{H'})) \\ (\mathbf{I}, \mathbf{C_H})[(\mathbf{I'}, \mathbf{H'})] &= (\mathbf{I}, (\mathbf{C_H}[\mathbf{I'}], \mathbf{H'})) \end{aligned}$$

$$\begin{aligned} [\cdot][\mathbf{I}] &= \mathbf{I} \\ (\iota; \mathbf{C_I})[\mathbf{I}] &= \iota; \mathbf{C_I}[\mathbf{I}] \end{aligned}$$

$$\begin{aligned} (\mathbf{C_H}, \ell \mapsto \mathbf{h})[\mathbf{I}] &= (\mathbf{C_H}[\mathbf{I}]), \ell \mapsto \mathbf{h} \\ (\mathbf{H}, \ell \mapsto \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{C_I})[\mathbf{I}] &= \mathbf{H}, \ell \mapsto \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.(\mathbf{C_I}[\mathbf{I}]) \end{aligned}$$

1.2.2 Well-Typed Context $\boxed{\vdash \mathbf{C} : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \chi'; \sigma_0; \mathbf{q'} \vdash \tau'; \sigma_1)}$

$$\frac{\Psi' \vdash \mathbf{H} : \Psi \qquad \text{ret-type}(\mathbf{q'}, \chi', \sigma_0) = \tau; \sigma_1 \qquad \vdash \mathbf{C_I} : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow ((\Psi', \Psi); \Delta'; \chi'; \sigma_0; \mathbf{q'})}{\vdash (\mathbf{C_I}, \mathbf{H}) : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \chi'; \sigma_0; \mathbf{q'} \vdash \tau; \sigma_1)}$$

$$\frac{\vdash \mathbf{C_H} : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi' \vdash \Psi) \qquad \text{ret-type}(\mathbf{q'}, \chi', \sigma_0) = \tau; \sigma_1 \qquad (\Psi', \Psi); \Delta'; \chi'; \sigma_0; \mathbf{q'} \vdash \mathbf{I}}{\vdash (\mathbf{I}, \mathbf{C_H}) : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \chi'; \sigma_0; \mathbf{q'} \vdash \tau; \sigma_1)}$$

$$\frac{\Psi \subseteq \Psi' \qquad \Delta \subseteq \Delta' \qquad \Delta \vdash \chi' \leq \chi \qquad \text{ret-type}(\mathbf{q}, \chi, \sigma) = \tau; \sigma'}{\vdash [\cdot] : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \chi'; \sigma; \mathbf{q})}$$

$$\frac{\Psi'; \Delta'; \chi'; \sigma_0; \mathbf{q'} \vdash \iota \Rightarrow \Delta''; \chi''; \sigma_1; \mathbf{q''} \qquad \vdash \mathbf{C_I} : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta''; \chi''; \sigma_1; \mathbf{q''})}{\vdash \iota; \mathbf{C_I} : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \chi'; \sigma_0; \mathbf{q'})}$$

$$\frac{\begin{array}{c} \mathbf{H} = \ell_1 \mapsto \mathbf{h}_1, \ldots, \ell_n \mapsto \mathbf{h}_n \qquad \mathbf{H'} = \ell'_1 \mapsto \mathbf{h}'_1, \ldots, \ell'_m \mapsto \mathbf{h}'_n \\ \Psi = \{\ell_1 : {}^{\nu_1}\psi_1, \ldots, \ell_n : {}^{\nu_n}\psi_n, \ell : {}^{\mathrm{box}}\forall[\Delta'].\{\chi'; \sigma_0\}^{\mathbf{q'}}, \ell'_1 : {}^{\nu'_1}\psi'_1, \ldots, \ell'_m : {}^{\nu'_m}\psi'_m\} \qquad \cdot \vdash \psi_1 \ \cdots \ \cdot \vdash \psi_n \\ \Psi', \Psi \vdash \mathbf{h}_1 : {}^{\nu_1}\psi_1 \ \cdots \ \Psi', \Psi \vdash \mathbf{h}_n : {}^{\nu_n}\psi_n \qquad \vdash \mathbf{C_I} : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow ((\Psi', \Psi); \Delta'; \chi'; \sigma_0; \mathbf{q'}) \\ \cdot \vdash \psi'_1 \ \cdots \ \cdot \vdash \psi'_m \qquad \Psi, \Psi \vdash \mathbf{h}'_1 : {}^{\nu'_1}\psi'_1 \ \cdots \ \Psi, \Psi \vdash \mathbf{h}'_m : {}^{\nu'_m}\psi'_m \end{array}}{\vdash \mathbf{H}, \ell \mapsto \mathbf{code}[\Delta']\{\chi'; \sigma_0\}^{\mathbf{q'}}.\mathbf{C_I}, \mathbf{H'} : (\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi' \vdash \Psi)}$$

1.2.3 Contextual Equivalence

$$
\begin{array}{l}
\Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_1 \approx^{ctx} e_2 : \tau; \hat{\boldsymbol{\sigma}} \stackrel{\text{def}}{=} \\
\quad \Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_1 : \tau; \hat{\boldsymbol{\sigma}} \ \wedge \ \Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_2 : \tau; \hat{\boldsymbol{\sigma}} \ \wedge \\
\quad \forall C, M, \Psi', \boldsymbol{\chi}', \boldsymbol{\sigma}', \mathbf{q}', \tau', \hat{\boldsymbol{\sigma}}'. \\
\qquad \vdash C : (\Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \tau; \hat{\boldsymbol{\sigma}}) \rightsquigarrow (\Psi'; \cdot; \boldsymbol{\chi}'; \boldsymbol{\sigma}'; \mathbf{q}' \vdash \tau'; \hat{\boldsymbol{\sigma}}') \ \wedge \ \vdash M : (\Psi', \boldsymbol{\chi}', \boldsymbol{\sigma}') \\
\qquad \Longrightarrow \ (\langle M \mid C[e_1] \rangle \downarrow \iff \langle M \mid C[e_2] \rangle \downarrow)
\end{array}
$$

1.2.4 CIU Equivalence

$$
\begin{array}{l}
\Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_1 \approx^{ciu} e_2 : \tau; \hat{\boldsymbol{\sigma}} \stackrel{\text{def}}{=} \\
\quad \Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_1 : \tau; \hat{\boldsymbol{\sigma}} \ \wedge \ \Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_2 : \tau; \hat{\boldsymbol{\sigma}} \ \wedge \\
\quad \forall \delta, E, M, \Psi', \mathbf{q}', \tau', \hat{\boldsymbol{\sigma}}'. \\
\qquad \cdot \vdash \delta : \Delta \ \wedge \ \vdash E : (\Psi; \cdot; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \tau; \hat{\boldsymbol{\sigma}}) \rightsquigarrow (\Psi'; \cdot; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q}' \vdash \tau'; \hat{\boldsymbol{\sigma}}') \ \wedge \ \vdash M : (\Psi', \boldsymbol{\chi}, \boldsymbol{\sigma}) \\
\qquad \Longrightarrow \ (\langle M \mid E[\delta(e_1)] \rangle \downarrow \iff \langle M \mid E[\delta(e_2)] \rangle \downarrow)
\end{array}
$$

1.3 Logical Relation

Worlds and Auxiliary Definitions Worlds consist of a sequence of islands that describe the current state of the memories (and how they are related) of the two computations we wish to relate. The essential idea here is that the islands θ in the sequence Θ will specify constraints on *disjoint* parts of memory. We obtain constraints on the entire memory via a disjoint union of the memories specified by the islands.

Therefore, we begin with some simple definitions for memory objects that we will make use of in islands. We need to be able to lift various pieces of memory to a full program memory $M = (\mathbf{H}, \mathbf{R}, \mathbf{S})$. In many cases, we may not want to impose a constraint on the register file and stack, so we allow $\bot$ to appear in those positions. Since disjoint heap fragments can be merged, the heap can be left unconstrained just by using an empty heap.

$$\begin{aligned} \mathrm{Regs}_\bot &= \{\mathbf{R}\} \cup \{\bot\} \\ \mathrm{Stack}_\bot &= \{\mathbf{S}\} \cup \{\bot\} \end{aligned} \qquad \begin{aligned} \{\cdot\} &\stackrel{\text{def}}{=} (\{\cdot\}, \bot, \bot) \\ \mathbf{H}\restriction &\stackrel{\text{def}}{=} (\mathbf{H}, \bot, \bot) \\ \mathbf{R}\restriction &\stackrel{\text{def}}{=} (\{\cdot\}, \mathbf{R}, \bot) \\ \mathbf{S}\restriction &\stackrel{\text{def}}{=} (\{\cdot\}, \bot, \mathbf{S}) \end{aligned}$$

A world W consists of a step index k, a pair of heap types Ψ_1 and Ψ_2, and a sequence Θ of islands θ. Each island expresses invariants on certain parts of memory by encoding a state transition system and a memory relation MR that establishes which pairs of memories are acceptable in each state. (See Dreyer *et al.* [1] for details.)

The first three islands in Θ are distinguished: they track the register file, the stack, and the immutable contents of the heap, respectively. We assign these islands the indices i_{reg}, i_{stk}, and i_{box}, respectively. Further islands can be added to a world to encode invariants about mutable data.

$$\begin{aligned} \mathrm{World}_n \stackrel{\text{def}}{=} \{\, & W = (k, \Psi_1, \Psi_2, \Theta) \mid k < n \ \wedge\ \exists m \geq 3.\ \Theta \in \mathrm{Island}_k^m \ \wedge \\ & (\exists s_{\mathrm{reg}}.\ \Theta(i_{\mathrm{reg}}) = \mathrm{island}_{\mathrm{reg}}(s_{\mathrm{reg}}, k) \ \wedge\ \Psi_1 \vdash s_{\mathrm{reg}}.\mathbf{R_1} : s_{\mathrm{reg}}.\boldsymbol{\chi_1} \ \wedge\ \Psi_2 \vdash s_{\mathrm{reg}}.\mathbf{R_2} : s_{\mathrm{reg}}.\boldsymbol{\chi_2}) \ \wedge \\ & (\exists s_{\mathrm{stk}}.\ \Theta(i_{\mathrm{stk}}) = \mathrm{island}_{\mathrm{stk}}(s_{\mathrm{stk}}, k) \ \wedge\ \Psi_1 \vdash s_{\mathrm{stk}}.\mathbf{S_1} : s_{\mathrm{stk}}.\boldsymbol{\sigma_1} \ \wedge\ \Psi_2 \vdash s_{\mathrm{stk}}.\mathbf{S_2} : s_{\mathrm{stk}}.\boldsymbol{\sigma_2}) \ \wedge \\ & (\exists s_{\mathrm{box}}.\ \Theta(i_{\mathrm{box}}) = \mathrm{island}_{\mathrm{box}}(s_{\mathrm{box}}, k) \ \wedge \Psi_1^{\mathrm{ref}} \vdash s_{\mathrm{box}}.\mathbf{H_1} : \Psi_1^{\mathrm{box}} \ \wedge\ \Psi_2^{\mathrm{ref}} \vdash s_{\mathrm{box}}.\mathbf{H_2} : \Psi_2^{\mathrm{box}})\} \\ \mathrm{Island}_n \stackrel{\text{def}}{=} \{\, & \theta = (s, S, \delta, \pi, \mathrm{MR}, \mathrm{bij}) \mid\ s \in S \ \wedge\ S \in \mathrm{Set} \ \wedge\ \delta \subseteq S \times S \ \wedge\ \pi \subseteq \delta \ \wedge \\ & \delta, \pi \text{ reflexive} \wedge \delta, \pi \text{ transitive} \wedge \mathrm{MR} \in S \to \mathrm{MemRel}_n \ \wedge\ \mathrm{bij} \in S \to \mathbb{P}(\mathrm{Val} \times \mathrm{Val}) \,\} \end{aligned}$$

$$\mathrm{MemAtom}_n \stackrel{\text{def}}{=} \{\, (W, M_1, M_2) \mid\ W \in \mathrm{World}_n \wedge\ M_1, M_2 \in \mathrm{Heap} \times \mathrm{Regs}_\bot \times \mathrm{Stack}_\bot \,\}$$

$$\mathrm{MemRel}_n \stackrel{\text{def}}{=} \{\, \varphi_M \subseteq \mathrm{MemAtom}_n \mid\ \forall (W, M_1, M_2) \in \varphi_M.\ \forall W' \sqsupseteq W.\ (W', M_1, M_2) \in \varphi_M \,\}$$

The transition systems for θ_{reg} and θ_{stk} encode the current contents of each side's register file and stack, respectively. They may transition freely between states, since the register file and stack are fairly free in how they can change during program execution. The states of θ_{box} encode the contents of the immutable part of the heap on each side. This island is allowed to transition only by adding more immutable data to the heap.

$$\begin{aligned} i_{\mathrm{reg}} &= 1 \\ S_{\mathrm{reg}} &= \{\, (\mathbf{R_1}, \boldsymbol{\chi_1}, \mathbf{R_2}, \boldsymbol{\chi_2}) \,\} \\ \mathrm{island}_{\mathrm{reg}}(s, k) &= (s, S_{\mathrm{reg}}, S_{\mathrm{reg}} \times S_{\mathrm{reg}}, S_{\mathrm{reg}} \times S_{\mathrm{reg}}, \lambda s.\{(W, s.\mathbf{R_1}\restriction, s.\mathbf{R_2}\restriction) \mid W \in \mathrm{World}_k\}, \lambda s.\emptyset) \end{aligned}$$

$$\begin{aligned} i_{\mathrm{stk}} &= 2 \\ S_{\mathrm{stk}} &= \{\, (\mathbf{S_1}, \boldsymbol{\sigma_1}, \mathbf{S_2}, \boldsymbol{\sigma_2}) \,\} \\ \mathrm{island}_{\mathrm{stk}}(s, k) &= (s, S_{\mathrm{stk}}, S_{\mathrm{stk}} \times S_{\mathrm{stk}}, S_{\mathrm{stk}} \times S_{\mathrm{stk}}, \lambda s.\{(W, s.\mathbf{S_1}\restriction, s.\mathbf{S_2}\restriction) \mid W \in \mathrm{World}_k\}, \lambda s.\emptyset) \end{aligned}$$

$$
\begin{aligned}
i_{\text{box}} &= 3 \\
S_{\text{box}} &= \{\, (H_1, H_2) \,\} \\
\delta_{\text{box}} &= \{((H_1, H_2), (H_1', H_2')) \mid H_1 \subseteq H_1' \wedge H_2 \subseteq H_2'\} \\
\text{island}_{\text{box}}(s, k) &= (s, S_{\text{box}}, \delta_{\text{box}}, \delta_{\text{box}}, \lambda s.\{(W, (s.H_1)\restriction, (s.H_2)\restriction) \mid W \in \text{World}_k\}, \lambda s.\emptyset)
\end{aligned}
$$

Two memory objects that describe disjoint parts of memory can be merged into one compound memory object via the $\otimes$ operator.

$\boxed{M_1 \otimes M_2}$ where $M_1, M_2 \in (\{H\} \times \text{Regs}_\perp \times \text{Stack}_\perp)$

$$
(H_1, \mathbf{R_1}, \mathbf{S_1}) \otimes (H_2, \mathbf{R_2}, \mathbf{S_2}) = \begin{cases} (H_1 \uplus H_2, \mathbf{R}, \mathbf{S}) & \text{where } \mathbf{R} = \mathbf{R_1} \text{ if } \mathbf{R_2} = \perp; \mathbf{R} = \mathbf{R_2} \text{ if } \mathbf{R_1} = \perp \\ & \quad \mathbf{S} = \mathbf{S_1} \text{ if } \mathbf{S_2} = \perp; \mathbf{S} = \mathbf{S_2} \text{ if } \mathbf{S_1} = \perp \\ \text{undefined} & \text{otherwise} \end{cases}
$$

$$
\varphi_M \otimes \varphi_M' \;=\; \{\, (W, M_1 \otimes M_1', M_2 \otimes M_2') \mid (W, M_1, M_2) \in \varphi_M \;\wedge\; (W, M_1', M_2') \in \varphi_M' \,\}
$$

These are standard operations for dealing with step indexing: we can approximate a world or relation to a given number of steps with $\lfloor \cdot \rfloor_k$, and we can expend a step using the $\triangleright$ operator (read "later").

$$
\begin{aligned}
\lfloor (\theta_1, \ldots, \theta_m) \rfloor_k &\stackrel{\text{def}}{=} (\lfloor \theta_1 \rfloor_k, \ldots, \lfloor \theta_m \rfloor_k) \\
\lfloor (s, S, \delta, \pi, \text{MR}, \text{bij}) \rfloor_k &\stackrel{\text{def}}{=} (s, S, \delta, \pi, \lfloor \text{MR} \rfloor_k, \text{bij}) \\
\lfloor \text{MR} \rfloor_k &\stackrel{\text{def}}{=} \lambda s.\; \lfloor \text{MR}(s) \rfloor_k \\
\lfloor \varphi_M \rfloor_k &\stackrel{\text{def}}{=} \{\, (W, M_1, M_2) \in \varphi_M \mid\; W.k < k \,\}
\end{aligned}
$$

$$
\begin{aligned}
\triangleright(k+1, \Psi_1, \Psi_2, \Theta) &\stackrel{\text{def}}{=} (k, \Psi_1, \Psi_2, \lfloor \Theta \rfloor_k) \\
\triangleright\varphi_e &\stackrel{\text{def}}{=} \{\, (W, e_1, e_2) \mid W.k > 0 \implies (\triangleright W, e_1, e_2) \in \varphi_e \,\} \\
\triangleright\varphi_v &\stackrel{\text{def}}{=} \{\, (W, v_1, v_2) \mid W.k > 0 \implies (\triangleright W, v_1, v_2) \in \varphi_v \,\} \\
\triangleright\varphi_w &\stackrel{\text{def}}{=} \{\, (W, w_1, w_2) \mid W.k > 0 \implies (\triangleright W, w_1, w_2) \in \varphi_w \,\}
\end{aligned}
$$

Future worlds W' of a given world W, written $W' \sqsupseteq W$, may differ from W in any or all of the following ways: they may have expended steps, allocated additional memory, added new islands, or taken transitions in existing islands. Public future worlds $W' \sqsupseteq_{\text{pub}} W$ are similar, but must have taken public transitions from the island states in W.

$$
\begin{aligned}
(k', \Psi_1', \Psi_2', \Theta') \sqsupseteq (k, \Psi_1, \Psi_2, \Theta) &\stackrel{\text{def}}{=} k' \le k \;\wedge\; \Psi_1' \supseteq \Psi_1 \;\wedge\; \Psi_2' \supseteq \Psi_2 \;\wedge\; \Theta' \sqsupseteq \lfloor \Theta \rfloor_{k'} \\
&\qquad \wedge\; (k, \Psi_1, \Psi_2, \Theta) \in \text{World} \;\wedge\; (k', \Psi_1', \Psi_2', \Theta') \in \text{World} \\
(\theta_1', \ldots, \theta_{m'}') \sqsupseteq (\theta_1, \ldots, \theta_m) &\stackrel{\text{def}}{=} m' \ge m \;\wedge\; \forall j \in \{1, \ldots, m\}.\; \theta_j' \sqsupseteq \theta_j \\
(s', S', \delta', \pi', \text{MR}', \text{bij}') \sqsupseteq (s, S, \delta, \pi, \text{MR}, \text{bij}) &\stackrel{\text{def}}{=} (S', \delta', \pi', \text{MR}', \text{bij}') = (S, \delta, \pi, \text{MR}, \text{bij}) \;\wedge\; (s, s') \in \delta \\
W' \sqsupset W &\stackrel{\text{def}}{=} W'.k < W.k \;\wedge\; W' \sqsupseteq W
\end{aligned}
$$

$$
\begin{aligned}
(k', \Psi_1', \Psi_2', \Theta') \sqsupseteq_{\text{pub}} (k, \Psi_1, \Psi_2, \Theta) &\stackrel{\text{def}}{=} k' \le k \;\wedge\; \Psi_1' \supseteq \Psi_1 \;\wedge\; \Psi_2' \supseteq \Psi_2 \;\wedge\; \Theta' \sqsupseteq_{\text{pub}} \lfloor \Theta \rfloor_{k'} \\
&\qquad \wedge\; (k, \Psi_1, \Psi_2, \Theta) \in \text{World} \;\wedge\; (k', \Psi_1', \Psi_2', \Theta') \in \text{World} \\
(\theta_1', \ldots, \theta_{m'}') \sqsupseteq_{\text{pub}} (\theta_1, \ldots, \theta_m) &\stackrel{\text{def}}{=} m' \ge m \;\wedge\; \forall j \in \{1, \ldots, m\}.\; \theta_j' \sqsupseteq_{\text{pub}} \theta_j \\
(s', S', \delta', \pi', \text{MR}', \text{bij}') \sqsupseteq_{\text{pub}} (s, S, \delta, \pi, \text{MR}, \text{bij}) &\stackrel{\text{def}}{=} (S', \delta', \pi', \text{MR}', \text{bij}') = (S, \delta, \pi, \text{MR}, \text{bij}) \;\wedge\; (s, s') \in \pi
\end{aligned}
$$

Given a world W, we often need to talk about future worlds of W where the only change is that new immutable memory has been allocated. We use this notation to capture this:

$$
\begin{aligned}
W \boxplus (H_1, H_2) \stackrel{\text{def}}{=} (W.k, W.\Psi_1 \uplus \Psi_1, W.\Psi_2 \uplus \Psi_2, W.\Theta[i_{\text{box}} \mapsto \text{island}_{\text{box}}(W(i_{\text{box}}).s \uplus (H_1, H_2),\; W.k)]) \\
\text{if } W.\Psi_1 \vdash H_1 : \Psi_1 \;\wedge\; W.\Psi_2 \vdash H_2 : \Psi_2 \;\wedge\; \text{boxheap}(\Psi_1) \;\wedge\; \text{boxheap}(\Psi_2).
\end{aligned}
$$

The following are convenient shorthands for frequently-used pieces of a world:

$$\text{currentMR}(\theta) \stackrel{\text{def}}{=} \theta.\text{MR}(\theta.s) \qquad W(i) \stackrel{\text{def}}{=} W.\Theta(i)$$

$$W.\mathbf{R_1} \stackrel{\text{def}}{=} W.\Theta(i_{\text{reg}}).s.\mathbf{R_1} \qquad W.\mathbf{S_1} \stackrel{\text{def}}{=} W.\Theta(i_{\text{stk}}).s.\mathbf{S_1} \qquad W.\boldsymbol{\chi_1} \stackrel{\text{def}}{=} W.\Theta(i_{\text{reg}}).s.\boldsymbol{\chi_1} \qquad W.\boldsymbol{\sigma_1} \stackrel{\text{def}}{=} W.\Theta(i_{\text{stk}}).s.\boldsymbol{\sigma_1}$$
$$W.\mathbf{R_2} \stackrel{\text{def}}{=} W.\Theta(i_{\text{reg}}).s.\mathbf{R_2} \qquad W.\mathbf{S_2} \stackrel{\text{def}}{=} W.\Theta(i_{\text{stk}}).s.\mathbf{S_2} \qquad W.\boldsymbol{\chi_2} \stackrel{\text{def}}{=} W.\Theta(i_{\text{reg}}).s.\boldsymbol{\chi_2} \qquad W.\boldsymbol{\sigma_2} \stackrel{\text{def}}{=} W.\Theta(i_{\text{stk}}).s.\boldsymbol{\sigma_2}$$

$$W.\Phi_1 \stackrel{\text{def}}{=} (W.\Psi_1, W.\boldsymbol{\chi_1}, W.\boldsymbol{\sigma_1}) \qquad W.\Phi_2 \stackrel{\text{def}}{=} (W.\Psi_2, W.\boldsymbol{\chi_2}, W.\boldsymbol{\sigma_2})$$

Atoms are well-formed worlds together with a pair of components or values that are well-typed at the indicated type under the appropriate memory type of the world.

$$\begin{aligned}
&\text{TermAtom}_n[(\mathbf{q_1} \vdash \tau_1; \boldsymbol{\sigma_1}), (\mathbf{q_2} \vdash \tau_2; \boldsymbol{\sigma_2})] \stackrel{\text{def}}{=} \\
&\quad \{\, (W, e_1, e_2) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1; \cdot; W.\boldsymbol{\chi_1}; W.\boldsymbol{\sigma_1}; \mathbf{q_1} \vdash e_1 : \tau_1; \boldsymbol{\sigma_1} \ \wedge \\
&\qquad\qquad W.\Psi_2; \cdot; W.\boldsymbol{\chi_2}; W.\boldsymbol{\sigma_2}; \mathbf{q_2} \vdash e_2 : \tau_2; \boldsymbol{\sigma_2} \,\} \\
&\text{WvalAtom}_n[\boldsymbol{\tau_1}, \boldsymbol{\tau_2}] \stackrel{\text{def}}{=} \{\, (W, \mathbf{w_1}, \mathbf{w_2}) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1; \cdot \vdash \mathbf{w_1} : \boldsymbol{\tau_1} \ \wedge\ W.\Psi_2; \cdot \vdash \mathbf{w_2} : \boldsymbol{\tau_2} \,\} \\
&\text{StackAtom}_n[\boldsymbol{\sigma_1}, \boldsymbol{\sigma_2}] \stackrel{\text{def}}{=} \{\, (W, \mathbf{S_1}\uparrow, \mathbf{S_2}\uparrow) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1 \vdash \mathbf{S_1} : \boldsymbol{\sigma_1} \ \wedge\ W.\Psi_2 \vdash \mathbf{S_2} : \boldsymbol{\sigma_2} \,\} \\
&\text{HvalAtom}_n[\boldsymbol{\psi_1}, \boldsymbol{\psi_2}] \stackrel{\text{def}}{=} \{\, (W, \mathbf{h_1}, \mathbf{h_2}) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1 \vdash \mathbf{h_1} : {}^{\nu}\boldsymbol{\psi_1} \ \wedge\ W.\Psi_2 \vdash \mathbf{h_2} : {}^{\nu}\boldsymbol{\psi_2} \,\} \\
&\text{ContAtom}[(\mathbf{q_1} \vdash \tau_1; \boldsymbol{\sigma_1}), (\mathbf{q_2} \vdash \tau_2; \boldsymbol{\sigma_2})] \rightsquigarrow [(\mathbf{q_1'} \vdash \tau_1'; \boldsymbol{\sigma_1'}), (\mathbf{q_2'} \vdash \tau_2'; \boldsymbol{\sigma_2'})] \stackrel{\text{def}}{=} \\
&\quad \{(W, E_1, E_2) \mid W \in \text{World} \ \wedge \\
&\qquad \vdash E_1 : (W.\Psi_1; \cdot; W.\boldsymbol{\chi_1}; W.\boldsymbol{\sigma_1}; \mathbf{q_1} \vdash \tau_1; \boldsymbol{\sigma_1}) \rightsquigarrow (W.\Psi_1; \cdot; W.\boldsymbol{\chi_1}; W.\boldsymbol{\sigma_1}; \mathbf{q_1'} \vdash \tau_1'; \boldsymbol{\sigma_1'}) \wedge \\
&\qquad \vdash E_2 : (W.\Psi_2; \cdot; W.\boldsymbol{\chi_2}; W.\boldsymbol{\sigma_2}; \mathbf{q_2} \vdash \tau_2; \boldsymbol{\sigma_2}) \rightsquigarrow (W.\Psi_2; \cdot; W.\boldsymbol{\chi_2}; W.\boldsymbol{\sigma_2}; \mathbf{q_2'} \vdash \tau_2'; \boldsymbol{\sigma_2'})\} \\
&\text{ContAtom}[(\mathbf{q_1} \vdash \tau_1; \boldsymbol{\sigma_1}), (\mathbf{q_2} \vdash \tau_2; \boldsymbol{\sigma_2})] \stackrel{\text{def}}{=} \\
&\quad \{(W, E_1, E_2) \mid \exists \mathbf{q_1'}, \mathbf{q_2'}, \tau_1', \tau_2', \boldsymbol{\sigma_1'}, \boldsymbol{\sigma_2'}. \\
&\qquad (W, E_1, E_2) \in \text{ContAtom}[(\mathbf{q_1} \vdash \tau_1; \boldsymbol{\sigma_1}), (\mathbf{q_2} \vdash \tau_2; \boldsymbol{\sigma_2})] \rightsquigarrow [(\mathbf{q_1'} \vdash \tau_1'; \boldsymbol{\sigma_1'}), (\mathbf{q_2'} \vdash \tau_2'; \boldsymbol{\sigma_2'})]\}
\end{aligned}$$

$$\begin{aligned}
&\text{WvalRel}[\boldsymbol{\tau_1}, \boldsymbol{\tau_2}] \stackrel{\text{def}}{=} \{\, \varphi_w \subseteq \text{WvalAtom}[\boldsymbol{\tau_1}, \boldsymbol{\tau_2}] \mid \forall (W, \mathbf{w_1}, \mathbf{w_2}) \in \varphi_w.\ \forall W' \sqsupseteq W.\ (W', \mathbf{w_1}, \mathbf{w_2}) \in \varphi_w \} \\
&\text{TValRel} \stackrel{\text{def}}{=} \{\, \text{VR} = (\boldsymbol{\tau_1}, \boldsymbol{\tau_2}, \varphi_w) \mid \varphi_w \in \text{WvalRel}[\boldsymbol{\tau_1}, \boldsymbol{\tau_2}] \,\} \\
&\text{StackRel}[\boldsymbol{\sigma_1}, \boldsymbol{\sigma_2}] \stackrel{\text{def}}{=} \{\, \varphi_S \subseteq \text{StackAtom}[\boldsymbol{\sigma_1}, \boldsymbol{\sigma_2}] \,\} \\
&\text{TStackRel} \stackrel{\text{def}}{=} \{\, \text{SR} = (\boldsymbol{\sigma_1}, \boldsymbol{\sigma_2}, \varphi_S) \mid \varphi_S \in \text{StackRel}[\boldsymbol{\sigma_1}, \boldsymbol{\sigma_2}] \,\}
\end{aligned}$$

The set $\mathcal{D}[\![\Delta]\!]$ ensures that an environment ρ mapping type variables to value relations is well-formed.

$$\begin{aligned}
&\mathcal{D}[\![\cdot]\!] \stackrel{\text{def}}{=} \{\, \emptyset \,\} \\
&\mathcal{D}[\![\Delta, \boldsymbol{\alpha}]\!] \stackrel{\text{def}}{=} \{\, \rho[\boldsymbol{\alpha} \mapsto \text{VR}] \mid \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \text{VR} \in \text{TValRel} \,\} \\
&\mathcal{D}[\![\Delta, \boldsymbol{\zeta}]\!] \stackrel{\text{def}}{=} \{\, \rho[\boldsymbol{\zeta} \mapsto \text{SR}] \mid \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \text{SR} \in \text{TStackRel} \,\} \\
&\mathcal{D}[\![\Delta, \boldsymbol{\epsilon}]\!] \stackrel{\text{def}}{=} \{\, \rho[\boldsymbol{\epsilon} \mapsto (\mathbf{q_1}, \mathbf{q_2})] \mid \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \text{ftv}(\mathbf{q_1}) = \emptyset \ \wedge\ \text{ftv}(\mathbf{q_2}) = \emptyset \,\}
\end{aligned}$$

We use ρ_1 and ρ_2 to denote the substitutions formed by mapping variables in $\text{dom}\,\rho$ to the first and second components, respectively, of the tuples they map to.

We also use some shorthands for referring to atoms of a particular type in terms of an environment ρ:

$$\begin{aligned}
&\text{TermAtom}[\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\rho \stackrel{\text{def}}{=} \text{TermAtom}[(\rho_1(\mathbf{q}) \vdash \rho_1(\tau); \rho_1(\boldsymbol{\sigma})), (\rho_2(\mathbf{q}) \vdash \rho_2(\tau); \rho_2(\boldsymbol{\sigma}))] \\
&\text{WvalAtom}[\boldsymbol{\tau}]\rho \stackrel{\text{def}}{=} \text{WvalAtom}[\rho_1(\boldsymbol{\tau}), \rho_2(\boldsymbol{\tau})] \\
&\text{HvalAtom}[\boldsymbol{\psi}]\rho \stackrel{\text{def}}{=} \text{HvalAtom}[\rho_1(\boldsymbol{\psi}), \rho_2(\boldsymbol{\psi})] \\
&\text{ContAtom}[\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\rho \rightsquigarrow [\mathbf{q'} \vdash \tau'; \boldsymbol{\sigma'}]\rho' \stackrel{\text{def}}{=} \text{ContAtom}[(\rho_1(\mathbf{q}) \vdash \rho_1(\tau); \rho_1(\boldsymbol{\sigma})), (\rho_2(\mathbf{q}) \vdash \rho_2(\tau); \rho_2(\boldsymbol{\sigma}))] \\
&\qquad\qquad \rightsquigarrow [(\rho_1'(\mathbf{q'}) \vdash \rho_1'(\tau'); \rho_1'(\boldsymbol{\sigma'})), (\rho_2'(\mathbf{q'}) \vdash \rho_2'(\tau'); \rho_2'(\boldsymbol{\sigma'}))]
\end{aligned}$$

The following relation says that a memory relation φ_M satisfies the constraints imposed by a memory relation φ'_M in all worlds accessible from W.

$$\varphi_M \Subset_W \varphi'_M \quad \stackrel{\text{def}}{=} \quad \forall(\widetilde{W}, M_1, M_2) \in \varphi_M.\ \widetilde{W} \sqsupseteq W \implies (\widetilde{W}, M_1, M_2) \in \varphi'_M$$

$$\begin{aligned}
\mathcal{W}[\![\boldsymbol{\alpha}]\!]\rho &= \rho(\boldsymbol{\alpha}).\varphi_w \\
\mathcal{W}[\![\mathbf{unit}]\!]\rho &= \{\, (W, (), ()) \in \mathrm{WvalAtom}[\mathbf{unit}]\rho \,\} \\
\mathcal{W}[\![\mathbf{int}]\!]\rho &= \{\, (W, \mathbf{n}, \mathbf{n}) \in \mathrm{WvalAtom}[\mathbf{int}]\rho \,\} \\
\mathcal{W}[\![\exists\boldsymbol{\alpha}.\boldsymbol{\tau}]\!]\rho &= \{\, (W, \mathbf{pack}\langle\boldsymbol{\tau}_1,\mathbf{w}_1\rangle \mathbf{\ as\ } \rho_1(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}), \mathbf{pack}\langle\boldsymbol{\tau}_2,\mathbf{w}_2\rangle \mathbf{\ as\ } \rho_2(\exists\boldsymbol{\alpha}.\boldsymbol{\tau})) \in \mathrm{WvalAtom}[\exists\boldsymbol{\alpha}.\boldsymbol{\tau}]\rho \mid \\
&\qquad \exists\varphi_w \in \mathrm{WvalRel}[\boldsymbol{\tau}_1, \boldsymbol{\tau}_2].\ (W, \mathbf{w}_1, \mathbf{w}_2) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto (\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varphi_w)] \,\} \\
\mathcal{W}[\![\boldsymbol{\mu\alpha}.\boldsymbol{\tau}]\!]\rho &= \{\, (W, \mathbf{fold}_{\rho_1(\boldsymbol{\mu\alpha}.\boldsymbol{\tau})}\ \mathbf{w}_1, \mathbf{fold}_{\rho_2(\boldsymbol{\mu\alpha}.\boldsymbol{\tau})}\ \mathbf{w}_2) \in \mathrm{WvalAtom}[\boldsymbol{\mu\alpha}.\boldsymbol{\tau}]\rho \mid \\
&\qquad (W, \mathbf{w}_1, \mathbf{w}_2) \in \triangleright\mathcal{W}[\![\boldsymbol{\tau}[\boldsymbol{\mu\alpha}.\boldsymbol{\tau}/\boldsymbol{\alpha}]]\!]\rho \,\} \\
\mathcal{W}[\![\mathbf{ref}\ \boldsymbol{\psi}]\!]\rho &= \{\, (W, \boldsymbol{\ell}_1, \boldsymbol{\ell}_2) \in \mathrm{WvalAtom}[\mathbf{ref}\ \boldsymbol{\psi}]\rho \mid \exists i.\ \forall W' \sqsupseteq W. \\
&\qquad (\boldsymbol{\ell}_1, \boldsymbol{\ell}_2) \in W'(i).\mathrm{bij}(W'(i).s) \wedge \\
&\qquad \exists\varphi_M.\ \mathrm{currentMR}(W'(i)) = \varphi_M \otimes \\
&\qquad\quad \{\, (\widetilde{W}, \{\boldsymbol{\ell}_1 \mapsto \mathbf{h}_1\}\restriction, \{\boldsymbol{\ell}_2 \mapsto \mathbf{h}_2\}\restriction) \in \mathrm{MemAtom} \mid\ (\widetilde{W}, \mathbf{h}_1, \mathbf{h}_2) \in \mathcal{HV}[\![\boldsymbol{\psi}]\!])\rho \,\} \,\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{W}[\![\mathbf{box}\,\langle\boldsymbol{\tau}_1, \ldots, \boldsymbol{\tau}_\mathbf{n}\rangle]\!]\rho = \{\, &(W, \boldsymbol{\ell}_1, \boldsymbol{\ell}_2) \in \mathrm{WvalAtom}[\mathbf{box}\,\langle\boldsymbol{\tau}_1, \ldots, \boldsymbol{\tau}_\mathbf{n}\rangle]\rho \mid \\
&\forall(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}})).\ \widetilde{W} \sqsupseteq W \\
&\implies (\widetilde{W}, M_1(\boldsymbol{\ell}_1), M_2(\boldsymbol{\ell}_2)) \in \mathcal{HV}[\![\langle\boldsymbol{\tau}_1, \ldots, \boldsymbol{\tau}_\mathbf{n}\rangle]\!]\rho \,\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{W}[\![\mathbf{box}\,\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^\mathbf{q}]\!]\rho = \{&(W, \boldsymbol{\ell}_1[\overline{\boldsymbol{\omega_1}}], \boldsymbol{\ell}_2[\overline{\boldsymbol{\omega_2}}]) \in \mathrm{WvalAtom}[\mathbf{box}\,\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^\mathbf{q}]\rho \mid \\
&\forall(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}})).\ \widetilde{W} \sqsupseteq W \\
&\implies (\ M_1(\boldsymbol{\ell}_1) = \mathbf{code}[\overline{\boldsymbol{\beta_1}}, \boldsymbol{\Delta}]\{\boldsymbol{\chi}_1;\boldsymbol{\sigma}_1\}^{\mathbf{q}_1}.\mathbf{I}_1 \wedge \\
&\qquad \rho_1(\boldsymbol{\chi}) = \boldsymbol{\chi}_1[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}] \ \wedge\ \rho_1(\boldsymbol{\sigma}) = \boldsymbol{\sigma}_1[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}] \ \wedge\ \rho_1(\mathbf{q}) = \mathbf{q}_1[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}] \wedge \\
&\qquad M_2(\boldsymbol{\ell}_2) = \mathbf{code}[\overline{\boldsymbol{\beta_2}}, \boldsymbol{\Delta}]\{\boldsymbol{\chi}_2;\boldsymbol{\sigma}_2\}^{\mathbf{q}_2}.\mathbf{I}_2 \wedge \\
&\qquad \rho_2(\boldsymbol{\chi}) = \boldsymbol{\chi}_2[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}] \ \wedge\ \rho_2(\boldsymbol{\sigma}) = \boldsymbol{\sigma}_2[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}] \ \wedge\ \rho_2(\mathbf{q}) = \mathbf{q}_2[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}] \wedge \\
&\qquad (\widetilde{W}, (\mathbf{code}[\boldsymbol{\Delta}]\{\boldsymbol{\chi}_1;\boldsymbol{\sigma}_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}], \\
&\qquad\quad (\mathbf{code}[\boldsymbol{\Delta}]\{\boldsymbol{\chi}_2;\boldsymbol{\sigma}_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}]) \in \mathcal{HV}[\![\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^\mathbf{q}]\!]\rho\ ) \,\}
\end{aligned}$$

$$\begin{aligned}
&\mathcal{HV}[\![\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^\mathbf{q}]\!]\rho = \\
&\quad \{(W, \mathbf{code}[\boldsymbol{\Delta}]\{\rho_1(\boldsymbol{\chi});\rho_1(\boldsymbol{\sigma})\}^{\rho_1(\mathbf{q})}.\mathbf{I}_1, \mathbf{code}[\boldsymbol{\Delta}]\{\rho_2(\boldsymbol{\chi});\rho_2(\boldsymbol{\sigma})\}^{\rho_2(\mathbf{q})}.\mathbf{I}_2) \in \mathrm{HvalAtom}[\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^\mathbf{q}]\rho \mid \\
&\quad\ \forall W' \sqsupseteq W.\ \forall\rho^* \in \mathcal{D}[\![\boldsymbol{\Delta}]\!].\ \forall\boldsymbol{\tau}, \boldsymbol{\sigma'}.\ \ \mathrm{let}\ \rho' = \rho \cup \rho^*\ \mathrm{in}\ \boldsymbol{\tau};\boldsymbol{\sigma'} =_{\rho'} \mathrm{ret\text{-}type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma}) \ \wedge \\
&\qquad \mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho' \ \wedge\ \mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho' \\
&\quad\ \implies (W', (\rho_1^*(\mathbf{I}_1), \cdot), (\rho_2^*(\mathbf{I}_2), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau};\boldsymbol{\sigma'}]\!]\rho' \,\}
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{\tau};\boldsymbol{\sigma'} =_\rho \mathrm{ret\text{-}type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma}) \ \stackrel{\text{def}}{=}\ &\rho_1(\boldsymbol{\tau});\rho_1(\boldsymbol{\sigma'}) = \mathrm{ret\text{-}type}(\rho_1(\mathbf{q}), \rho_1(\boldsymbol{\chi}), \rho_1(\boldsymbol{\sigma})) \ \wedge \\
&\rho_2(\boldsymbol{\tau});\rho_2(\boldsymbol{\sigma'}) = \mathrm{ret\text{-}type}(\rho_2(\mathbf{q}), \rho_2(\boldsymbol{\chi}), \rho_2(\boldsymbol{\sigma}))
\end{aligned}$$

$$\begin{aligned}
\mathcal{HV}[\![\langle\boldsymbol{\tau}_1, \ldots, \boldsymbol{\tau}_\mathbf{n}\rangle]\!]\rho = \{\, &(W, \langle\mathbf{w}_{11}, \ldots, \mathbf{w}_{1\mathbf{n}}\rangle, \langle\mathbf{w}_{21}, \ldots, \mathbf{w}_{2\mathbf{n}}\rangle) \in \mathrm{HvalAtom}[\langle\boldsymbol{\tau}_1, \ldots, \boldsymbol{\tau}_\mathbf{n}\rangle]\rho \mid \\
&\forall\mathbf{j} \in \{\mathbf{1}, \ldots, \mathbf{n}\}.\ (W, \mathbf{w}_{1\mathbf{j}}, \mathbf{w}_{2\mathbf{j}}) \in \mathcal{W}[\![\boldsymbol{\tau}_\mathbf{j}]\!]\rho \,\}
\end{aligned}$$

$$(M_1, M_2) : W \quad \stackrel{\text{def}}{=} \vdash M_1 : W.\Phi_1 \ \wedge \ \vdash M_2 : W.\Phi_2 \ \wedge \\ (W.k > 0 \implies (\triangleright W, M_1, M_2) \in \bigotimes \{ \, \text{currentMR}(\theta) \mid \ \theta \in W.\Theta \, \})$$

$$\text{running}(k, \langle M \mid e \rangle) \quad \stackrel{\text{def}}{=} \exists M', e'. \ \langle M \mid e \rangle \longmapsto^k \langle M' \mid e' \rangle$$

$$\mathcal{O} = \{ \, (W, e_1, e_2) \mid \ \forall (M_1, M_2) : W. \ (\langle M_1 \mid e_1 \rangle \downarrow \ \wedge \ \langle M_2 \mid e_2 \rangle \downarrow) \vee \\ (\text{running}(W.k, \langle M_1 \mid e_1 \rangle) \ \wedge \ \text{running}(W.k, \langle M_2 \mid e_2 \rangle)) \, \}$$

$$\begin{aligned}
\mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho \quad = \{ \, & (W, \mathbf{E_1}, \mathbf{E_2}) \mid \forall W', \mathbf{q'}, \mathbf{r_1}, \mathbf{r_2}. \\
& W' \sqsupseteq_{\text{pub}} W \ \wedge \ (\mathbf{q} =_\rho \mathbf{q'} =_\rho \mathbf{end}\{\tau; \sigma\} \vee \\
& (\exists \mathbf{r}. \mathbf{q'} = \mathbf{r} \ \wedge \ \text{ret-addr}_1(W, \rho_1(\mathbf{q})) = W'.\mathbf{R_1}(\mathbf{r}) \ \wedge \ \text{ret-addr}_2(W, \rho_2(\mathbf{q})) = W'.\mathbf{R_2}(\mathbf{r}) \ \wedge \\
& \qquad \text{ret-reg}_1(W', \mathbf{r}) = \mathbf{r_1} \ \wedge \ \text{ret-reg}_2(W', \mathbf{r}) = \mathbf{r_2}) \wedge \\
& (\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\tau]\!]\rho \ \wedge \ \text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho \\
& \implies (W', \mathbf{E_1}[(\mathtt{ret} \ \rho_1(\mathbf{q'}) \ \{\mathbf{r_1}\}, \cdot)], \mathbf{E_2}[(\mathtt{ret} \ \rho_2(\mathbf{q'}) \ \{\mathbf{r_2}\}, \cdot)]) \in \mathcal{O} \, \}
\end{aligned}$$

$$\mathbf{q} =_\rho \mathbf{q'} \quad \stackrel{\text{def}}{=} \quad \rho_1(\mathbf{q}) = \rho_1(\mathbf{q'}) \ \wedge \ \rho_2(\mathbf{q}) = \rho_2(\mathbf{q'})$$

$$\begin{aligned}
&\text{ret-addr}_1(W, \mathbf{r}) = W.\mathbf{R_1}(\mathbf{r}) \qquad \text{ret-addr}_1(W, \mathbf{i}) = W.\mathbf{S_1}(\mathbf{i}) \\
&\text{ret-addr}_2(W, \mathbf{r}) = W.\mathbf{R_2}(\mathbf{r}) \qquad \text{ret-addr}_2(W, \mathbf{i}) = W.\mathbf{S_2}(\mathbf{i})
\end{aligned}$$

$$\begin{aligned}
&\text{ret-reg}_1(W, \mathbf{r}) = \mathbf{r'} \qquad \text{if } W.\boldsymbol{\chi_1}(\mathbf{r}) = \mathbf{box} \, \forall[].\{\mathbf{r'} : \tau; \sigma'\}^{\mathbf{q}} \\
&\text{ret-reg}_2(W, \mathbf{r}) = \mathbf{r'} \qquad \text{if } W.\boldsymbol{\chi_2}(\mathbf{r}) = \mathbf{box} \, \forall[].\{\mathbf{r'} : \tau; \sigma'\}^{\mathbf{q}}
\end{aligned}$$

$$\begin{aligned}
\mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho \quad = \{ \, & (W, e_1, e_2) \in \text{TermAtom}[\mathbf{q} \vdash \tau; \sigma]\rho \mid \\
& \forall E_1, E_2. \ (W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho \implies (W, E_1[e_1], E_2[e_2]) \in \mathcal{O} \, \}
\end{aligned}$$

$$\begin{aligned}
\mathcal{H}[\![\{\cdot\}]\!] \quad &= \text{World} \\
\mathcal{H}[\![\Psi, \ell : {}^{\text{ref}}\psi]\!] \quad &= \mathcal{H}[\![\Psi]\!] \cap \{ \, W \in \text{World} \mid \ (W, \ell, \ell) \in \mathcal{W}[\![\mathbf{ref} \ \psi]\!]\emptyset \, \} \\
\mathcal{H}[\![\Psi, \ell : {}^{\text{box}}\psi]\!] \quad &= \mathcal{H}[\![\Psi]\!] \cap \{ \, W \in \text{World} \mid \ (W, \ell, \ell) \in \mathcal{W}[\![\mathbf{box} \ \psi]\!]\emptyset \, \}
\end{aligned}$$

$$\mathcal{R}[\![\boldsymbol{\chi}]\!]\rho \quad = \{ \, (W, \mathbf{R_1}\!\restriction, \mathbf{R_2}\!\restriction) \mid \ \forall (\mathbf{r} : \tau) \in \boldsymbol{\chi}. \ (W, \mathbf{R_1}(\mathbf{r}), \mathbf{R_2}(\mathbf{r})) \in \mathcal{W}[\![\tau]\!]\rho \, \}$$

$$\begin{aligned}
\mathcal{S}[\![\zeta]\!]\rho \quad &= \rho(\zeta).\varphi_S \\
\mathcal{S}[\![\bullet]\!]\rho \quad &= \{ \, (W, \mathbf{nil}\!\restriction, \mathbf{nil}\!\restriction) \mid \ W \in \text{World} \, \} \\
\mathcal{S}[\![\tau :: \sigma]\!]\rho \quad &= \{ \, (W, (\mathbf{w_1} :: \mathbf{S_1})\!\restriction, (\mathbf{w_2} :: \mathbf{S_2})\!\restriction) \mid (W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho \ \wedge \ (W, \mathbf{S_1}\!\restriction, \mathbf{S_2}\!\restriction) \in \mathcal{S}[\![\sigma]\!]\rho \, \}
\end{aligned}$$

$$\begin{aligned}
\Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_1 \approx e_2 : \tau; \boldsymbol{\sigma'} \quad \stackrel{\text{def}}{=} \quad & \Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_1 : \tau; \boldsymbol{\sigma'} \ \wedge \ \Psi; \Delta; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash e_2 : \tau; \boldsymbol{\sigma'} \ \wedge \\
& \forall W, \rho. \ W \in \mathcal{H}[\![\Psi]\!] \ \wedge \ \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge \\
& \qquad \text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho \ \wedge \\
& \qquad \text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho \\
& \qquad \implies (W, \rho_1(e_1), \rho_2(e_2)) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma'}]\!]\rho
\end{aligned}$$

1.3.1 Other Logical Equivalences

To simplify the structure of the Lemmas in subsequent chapters, we define the following notions of logical equivalence for heaps, values, and instruction sequences:

Definition 1.1 (Logical Equivalence for Heaps)

$$\mathbf{\Psi} \vdash \mathbf{H_1} \approx_{\mathrm{H}} \mathbf{H_2} : \mathbf{\Psi'} \stackrel{\text{def}}{=} \mathbf{\Psi} \vdash \mathbf{H_1} : \mathbf{\Psi'} \ \wedge \ \mathbf{\Psi} \vdash \mathbf{H_2} : \mathbf{\Psi'} \ \wedge \ \forall (\ell :^{\nu} \psi) \in \mathbf{\Psi'}.\ \mathbf{\Psi}, \mathbf{\Psi'} \vdash \mathbf{H_1}(\ell) \approx_{\mathrm{hv}} \mathbf{H_2}(\ell) :^{\nu} \psi$$

$$\mathbf{\Psi} \vdash \mathbf{h_1} \approx_{\mathrm{hv}} \mathbf{h_2} :^{\nu} \psi \stackrel{\text{def}}{=} \mathbf{\Psi} \vdash \mathbf{h_1} :^{\nu} \psi \ \wedge \ \mathbf{\Psi} \vdash \mathbf{h_2} :^{\nu} \psi \ \wedge \ \forall W \in \mathcal{H}[\![\mathbf{\Psi}]\!].\ (W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\psi]\!]\emptyset$$

Definition 1.2 (Logical Equivalence for Values)

$$\begin{aligned}\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \tau \stackrel{\text{def}}{=}\ & \mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w_1} : \tau \ \wedge \ \mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w_2} : \tau \ \wedge \\ & \forall W \in \mathcal{H}[\![\mathbf{\Psi}]\!].\ \forall \rho \in \mathcal{D}[\![\mathbf{\Delta}]\!].\ (W, \rho_1(\mathbf{w_1}), \rho_2(\mathbf{w_2})) \in \mathcal{W}[\![\tau]\!]\rho\end{aligned}$$

$$\begin{aligned}\mathbf{\Psi}; \mathbf{\Delta}; \chi \vdash \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{u_2} : \tau \stackrel{\text{def}}{=}\ & \mathbf{\Psi}; \mathbf{\Delta}; \chi \vdash \mathbf{u_1} : \tau \ \wedge \ \mathbf{\Psi}; \mathbf{\Delta}; \chi \vdash \mathbf{u_1} : \tau \ \wedge \\ & \forall W \in \mathcal{H}[\![\mathbf{\Psi}]\!].\ \forall \rho \in \mathcal{D}[\![\mathbf{\Delta}]\!].\ \mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho \\ & \quad \Longrightarrow\ (W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\tau]\!]\rho\end{aligned}$$

Definition 1.3 (Logical Equivalence for Instruction Sequences)

$$\begin{aligned}\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathrm{I}} \mathbf{I_2} \stackrel{\text{def}}{=}\ & \mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1} \ \wedge \ \mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_2} \ \wedge \\ & \forall W \in \mathcal{H}[\![\mathbf{\Psi}]\!].\ \forall \rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]. \\ & \quad \mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho \ \wedge \ \mathrm{currentMR}(W(i_{\mathrm{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho \\ & \quad \Longrightarrow\ (W, \rho_1((\mathbf{I_1}, \cdot)), \rho_2((\mathbf{I_2}, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho\end{aligned}$$

1.4 Basic Properties

1.4.1 Operations on Worlds

Lemma 1.4 (World Extension is Reflexive and Transitive)
For any $W, W', W'' \in \text{World}$, we have

1. $W \sqsupseteq W$
2. $W \sqsupseteq_{\mathrm{pub}} W$
3. if $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$, then $W'' \sqsupseteq W$
4. if $W'' \sqsupseteq_{\mathrm{pub}} W'$ and $W' \sqsupseteq_{\mathrm{pub}} W$, then $W'' \sqsupseteq_{\mathrm{pub}} W$.

Proof

1. By definition of $\sqsupseteq$ for worlds and islands, and by the reflexivity of transition relations δ in the definition of World.
2. By definition of $\sqsupseteq_{\mathrm{pub}}$ for worlds and islands, and by the reflexivity of public transition relations π in the definition of World.
3. By definition of $\sqsupseteq$ for worlds and islands, and by the transitivity of transition relations δ in the definition of World.
4. By definition of $\sqsupseteq_{\mathrm{pub}}$ for worlds and islands, and by the transitivity of public transition relations π in the definition of World.

□

Lemma 1.5 (Properties of $\boxplus$)

1. If $(M_1, M_2) : W$ and $M_1' = (\mathbf{H_1}, \bot, \bot)$, $M_2' = (\mathbf{H_2}, \bot, \bot)$, then

$$(M_1 \uplus M_1', M_2 \uplus M_2') : W \boxplus (\mathbf{H_1}, \mathbf{H_2}).$$

2. $(W \boxplus (H_1, H_2)) \boxplus (H_1', H_2') = W \boxplus (H_1 \uplus H_1', H_2 \uplus H_2')$.
3. If $W \in \text{World}$ and $(W \boxplus (H_1, H_2))$ is defined, then $(W \boxplus (H_1, H_2)) \sqsupseteq W$ and $(W \boxplus (H_1, H_2)) \sqsupseteq_{\text{pub}} W$.

Proof

1. By definition of $W(i_{\text{box}})$.
2. By definition of $W(i_{\text{box}})$.
3. By definition of $\sqsupseteq$, $\sqsupseteq_{\text{pub}}$, and $\text{island}_{\text{box}}$.

□

Lemma 1.6 (Properties of $\triangleright$ and $\sqsupset$)
For any $W \in \text{World}$, we have

1. $\triangleright W \sqsupseteq W$
2. $\triangleright W \sqsupseteq_{\text{pub}} W$
3. If $(M_1, M_2) : W$, then $(M_1, M_2) : \triangleright W$.
4. If $W' \sqsupset W$, then $W' \sqsupseteq W$.
5. If $W' \sqsupset W$, then $W' \sqsupseteq \triangleright W$.

Proof

1. By definition of $\triangleright$ and $\sqsupseteq$, it suffices to show that $\lfloor \theta \rfloor_{W.k-1} \sqsupseteq \lfloor \theta \rfloor_{W.k-1}$ for each island $\theta \in W.\Theta$. But this relation is reflexive, so we are done.
2. Similar.
3. Note that if $W.k = 0$, there is nothing to show. Otherwise, the claim follows from the definitions of MemRel and $\lfloor \varphi_M \rfloor_k$.
4. Immediate from the definition of $\sqsupset$.
5. From the definition of $\sqsupset$ we have $W'.k < W.k$ and $W' \sqsupseteq W$. The latter implies that $W' \in \text{World}$, which gives us $0 \leq W'.k$. Hence, $0 < W.k$.
   Let $W = (k+1, \Psi_1, \Psi_2, \Theta)$. We have that:

$$(W'.k, W'.\Psi_1, W'.\Psi_2, W'.\Theta) \sqsupset (k+1, \Psi_1, \Psi_2, \Theta)$$

   We must show that:

$$(W'.k, W'.\Psi_1, W'.\Psi_2, W'.\Theta) \sqsupseteq (k, \Psi_1, \Psi_2, \lfloor \Theta \rfloor_k)$$

   It suffices to show the following:

   - $W'.k \leq (\triangleright W).k$: this follows from $W'.k < W.k$ and $(\triangleright W).k = W.k - 1$.
   - $W'.\Psi_i \supseteq \Psi_i$: by (4) we have $W' \sqsupseteq W$, from which this fact is immediate.
   - $W'.\Theta \sqsupseteq \lfloor \lfloor \Theta \rfloor_k \rfloor_{W'.k}$: From above we have that $W'.\Theta' \sqsupseteq \lfloor \Theta \rfloor_{k'}$. Furthermore, since $W'.k \leq (\triangleright W).k = W.k - 1 = k$, we have that $\lfloor \lfloor \Theta \rfloor_k \rfloor_{W'.k} = \lfloor \Theta \rfloor_{W'.k}$ so we are done.

□

1.4.2 Properties of the Observation Relation

Lemma 1.7 ($\mathcal{O}$ Closed under Anti-Reduction)
Given $W' \sqsupseteq W$, if $W.k \leq W'.k + k_1$, $W.k \leq W'.k + k_2$, and

$$\forall (M_1, M_2) : W.\ \exists (M_1', M_2') : W'.\ \langle M_1 \mid e_1 \rangle \longmapsto^{k_1} \langle M_1' \mid e_1' \rangle \ \wedge\ \langle M_2 \mid e_2 \rangle \longmapsto^{k_2} \langle M_2' \mid e_2' \rangle,$$

then

$$(W', e_1', e_2') \in \mathcal{O} \implies (W, e_1, e_2) \in \mathcal{O}.$$

Proof

Let $(M_1, M_2) : W$. Then, by our assumption, $\langle M_1 \mid e_1 \rangle \longmapsto^{k_1} \langle M_1' \mid e_1' \rangle$ and $\langle M_2 \mid e_2 \rangle \longmapsto^{k_2} \langle M_2' \mid e_2' \rangle$ for some $(M_1', M_2') : W'$. Since $(W', e_1', e_2') \in \mathcal{O}$, we have either that $\langle M_1' \mid e_1' \rangle \downarrow$ and $\langle M_2' \mid e_2' \rangle \downarrow$ or that running$(W'.k, \langle M_1' \mid e_1' \rangle)$ and running$(W'.k, \langle M_2' \mid e_2' \rangle)$.

In the former case, we have $\langle M_1 \mid e_1 \rangle \downarrow$ and $\langle M_2 \mid e_2 \rangle \downarrow$ by assumption. In the latter case, we have running$(W'.k + k_1, \langle M_1 \mid e_1 \rangle)$ and running$(W'.k + k_2, \langle M_2 \mid e_2 \rangle)$. Since we have assumptions that both of these are more steps than needed, we have the result. □

1.4.3 Monotonicity and Reduction

Lemma 1.8 (Monotonicity)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, where $\Delta \vdash \tau$ and $\Delta \vdash \psi$. If $W' \sqsupseteq W$, then

1. $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho \implies (W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho$
2. $(W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\psi]\!]\rho \implies (W', \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\tau]\!]\rho$.

Proof

1. Proved by induction on $W'.k$ and on the structure of τ, simultaneously with Claim 2.

   In each case, we will need to show $(W', \mathbf{w_1}, \mathbf{w_2}) \in \text{WvalAtom}[\tau]\rho$. This amounts to showing that $W'.\Psi_i; \cdot \vdash \mathbf{w_i} : \tau$ for $i \in \{1, 2\}$. We have by assumption that $W.\Psi_i; \cdot \vdash \mathbf{w_i} : \tau$. By definition of world extension, $W'.\Psi_i \supseteq W.\Psi_i$, so this property holds.

   To complete the proof, consider the possible cases of τ:

   Case α Follows from $\rho(\alpha).\varphi_v^T \in \text{WvalRel}[\rho(\alpha).\tau_1, \rho(\alpha).\tau_2]$, which holds by $\rho(\alpha) \in \text{TValRel}$.

   Case $\mathbf{unit}$ Immediate.

   Case $\mathbf{int}$ Immediate.

   Case $\exists \alpha.\tau'$ Follows from the induction hypothesis for the type.

   Case $\mu \alpha.\tau'$ Follows from the induction hypothesis for the step index.

   Case $\mathbf{ref}\ \psi$ We need to show that $(W', \ell_1, \ell_2) \in \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\rho$. Let $W'' \sqsupseteq W'$. By transitivity of world extension, $W'' \sqsupseteq W$. Thus everything we need holds by our assumption that $(W, \ell_1, \ell_2) \in \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\rho$.

   Case $\mathbf{box}\ \langle \tau_1, \ldots, \tau_n \rangle$ We need to show that $(W', \ell_1, \ell_2) \in \mathcal{W}[\![\mathbf{box}\ \langle \tau_1, \ldots, \tau_n \rangle]\!]\rho$.

   Let $(\widetilde{W}, M_1', M_2') \in \text{currentMR}(W'(i_{\text{box}}))$ such that $\widetilde{W} \sqsupset W'$. By definition of $\text{island}_{\text{box}}$, $M_1' = (W'(i_{\text{box}}).s.H_1)\restriction$ and $M_2' = (W'(i_{\text{box}}).s.H_2)\restriction$. By our assumption, to show

   $$(\widetilde{W}, M_1'(\ell_1), M_2'(\ell_2)) \in \mathcal{HV}[\![\langle \tau_1, \ldots, \tau_n \rangle]\!]\rho$$

   it suffices to find some M_1 and M_2 such that $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$, $M_1(\ell_1) = M_1'(\ell_1)$, and $M_2(\ell_2) = M_2'(\ell_2)$, noting that $\widetilde{W} \sqsupset W$ follows from $\widetilde{W} \sqsupset W' \sqsupseteq W$.
   We claim that $M_1 = (W(i_{\text{box}}).s.H_1)\restriction$ and $M_2 = (W(i_{\text{box}}).s.H_2)\restriction$ are suitable. The first condition holds immediately by definition of $\text{island}_{\text{box}}$. Since $W' \sqsupseteq W$, we know that $W'(i_{\text{box}}) \sqsupseteq \lfloor W(i_{\text{box}}) \rfloor_{W'.k}$. Thus $((H_1, H_2), (H_1', H_2')) \in \delta_{\text{box}}$, that is, $H_1 \subseteq H_1'$ and $H_2 \subseteq H_2'$. Since ℓ_1 and ℓ_2 must be in the domain of H_1 and H_2, we have the desired property that $M_1(\ell_1) = M_1'(\ell_1)$ and $M_2(\ell_2) = M_2'(\ell_2)$.

Case $\mathbf{box}\,\forall[\Delta].\{\chi;\sigma\}^{\mathbf{q}}$ Let $(\widetilde{W}, M_1', M_2') \in \text{currentMR}(W'(i_{\text{box}}))$ such that $\widetilde{W} \sqsupset W'$. It suffices to find some M_1 and M_2 such that $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$, $M_1(\ell_1) = M_1'(\ell_1)$, and $M_2(\ell_2) = M_2'(\ell_2)$, noting that $\widetilde{W} \sqsupset W$. This can be done exactly as in the previous case.

2. Proved simultaneously with Claim 1.

   In both cases, we need to show that $(W', \mathbf{h_1}, \mathbf{h_2}) \in \text{HvalAtom}[\psi]\rho$. This amounts to showing that $W'.\Psi_i \vdash \mathbf{h_i} :^{\nu} \psi$ for $i \in \{1, 2\}$. We have by assumption that $W.\Psi_i \vdash \mathbf{h_i} :^{\nu} \psi$. By definition of world extension, $W'.\Psi_i \supseteq W.\Psi_i$, so this property holds.

   Consider the possible cases of ψ:

   Case $\forall[\Delta].\{\chi;\sigma\}^{\mathbf{q}}$ We need to show that $(W', \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\forall[\Delta].\{\chi;\sigma\}^{\mathbf{q}}]\!]\rho$. Let $W'' \sqsupseteq W'$. By transitivity of world extension, $W'' \sqsupseteq W$. Thus everything we need holds by our assumption that $(W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\forall[\Delta].\{\chi;\sigma\}^{\mathbf{q}}]\!]\rho$.

   Case $\langle \tau_1, \ldots, \tau_n \rangle$ Follows from Claim 1 using the induction hypothesis for the type.

□

Lemma 1.9 (Monotonicity for Heaps)
If $W' \sqsupseteq W$ and $W \in \mathcal{H}[\![\Psi]\!]$, then $W' \in \mathcal{H}[\![\Psi]\!]$.

Proof

We use induction on the structure of Ψ. If $\Psi = \{\cdot\}$ then there is nothing to show.

If $\Psi = \Psi', \ell :^{\text{ref}} \psi$, then by the induction hypothesis, $W' \in \mathcal{H}[\![\Psi']\!]$, and it remains to show that $(W', \ell, \ell) \in \mathcal{W}[\![\mathbf{ref}\,\psi]\!]\emptyset$. But this follows from $W \in \mathcal{H}[\![\Psi', \ell :^{\text{ref}} \psi]\!]$ and Lemma 1.8.

If $\Psi = \Psi', \ell :^{\text{box}} \psi$, then by the induction hypothesis, $W' \in \mathcal{H}[\![\Psi']\!]$, and it remains to show that $(W', \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\,\psi]\!]\emptyset$. But this follows from $W \in \mathcal{H}[\![\Psi', \ell :^{\text{box}} \psi]\!]$ and Lemma 1.8. □

Lemma 1.10 (Monotonicity for Evaluation Contexts)
If $W' \sqsupseteq_{\text{pub}} W$ and if either $\mathbf{q} =_\rho \mathbf{q}' =_\rho \mathbf{end}\{\tau;\sigma\}$ or $\text{ret-addr}_1(W, \rho_1(\mathbf{q})) = \text{ret-addr}_1(W', \rho_1(\mathbf{q}'))$ and $\text{ret-addr}_2(W, \rho_2(\mathbf{q})) = \text{ret-addr}_2(W', \rho_2(\mathbf{q}'))$, then

$$(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau;\sigma]\!]\rho \implies (W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q}' \vdash \tau;\sigma]\!]\rho.$$

Proof

Follows from the transitivity of $\sqsupseteq_{\text{pub}}$ and our hypotheses about the relationship between $\mathbf{q}$ and $\mathbf{q}'$. □

Lemma 1.11 ($\mathcal{E}[\![\mathbf{q} \vdash \tau;\sigma]\!]\rho$ Closed under Type-Preserving Anti-Reduction)
Let $(W, e_1, e_2) \in \text{TermAtom}[\mathbf{q} \vdash \tau;\sigma]\rho$. Given $W' \sqsupseteq_{\text{pub}} W$, $W.k \leq W'.k + k_1$, $W.k \leq W'.k + k_2$, and if $\mathbf{q} =_\rho \mathbf{q}' =_\rho \mathbf{end}\{\tau;\sigma\}$ or if $\text{ret-addr}_1(W, \rho_1(\mathbf{q})) = \text{ret-addr}_1(W', \rho_1(\mathbf{q}'))$ and $\text{ret-addr}_2(W, \rho_2(\mathbf{q})) = \text{ret-addr}_2(W', \rho_2(\mathbf{q}'))$, and if

$$\forall (M_1, M_2) : W.\ \exists (M_1', M_2') : W'.\ \langle M_1 \mid e_1 \rangle \longmapsto^{k_1} \langle M_1' \mid e_1' \rangle \ \wedge\ \langle M_2 \mid e_2 \rangle \longmapsto^{k_2} \langle M_2' \mid e_2' \rangle,$$

then

$$(W', e_1', e_2') \in \mathcal{E}[\![\mathbf{q}' \vdash \tau;\sigma]\!]\rho \implies (W, e_1, e_1) \in \mathcal{E}[\![\mathbf{q} \vdash \tau;\sigma]\!]\rho.$$

Proof

Let $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau;\sigma]\!]\rho$. We need to show that $(W, E_1[e_1], E_2[e_2]) \in \mathcal{O}$. Since $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q}' \vdash \tau;\sigma]\!]\rho$ by Lemma 1.10, we have $(W', E_1[e_1'], E_2[e_2']) \in \mathcal{O}$. By inspection of the operational semantics and by assumption, for any $(M_1, M_2) : W$, there is an $(M_1', M_2') : W'$ such that

$$\langle M_1 \mid E_1[e_1] \rangle \longmapsto^{k_1} \langle M_1' \mid E_1[e_1'] \rangle \quad \text{and} \quad \langle M_2 \mid E_2[e_2] \rangle \longmapsto^{k_2} \langle M_2' \mid E_2[e_2'] \rangle.$$

The result follows by Lemma 1.7. □

1.4.4 Substitution

The next lemma is a simple property, but its proof shows the induction structure by which properties of the mutually-dependent parts of the logical relation can be proved.

Definition 1.12

$\xi \ ::= \boldsymbol{\alpha} \mid \boldsymbol{\zeta} \mid \boldsymbol{\epsilon}$

$\mathrm{AR} ::= \mathrm{VR} \mid \mathrm{SR} \mid \mathrm{QR}$

Lemma 1.13
[Weakening] If $\rho[\xi \mapsto \mathrm{AR}] \in \mathcal{D}[\![\Delta, \xi]\!]$ and $\xi \notin \mathrm{ftv}(\boldsymbol{\tau})$, $\xi \notin \mathrm{ftv}(\boldsymbol{\sigma})$, $\xi \notin \mathrm{ftv}(\boldsymbol{\chi})$, $\xi \notin \mathrm{ftv}(\boldsymbol{\psi})$, then

1. $\mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho = \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
2. $\mathcal{R}[\![\boldsymbol{\chi}]\!]\rho = \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho[\xi \mapsto \mathrm{AR}]$
3. $\mathcal{W}[\![\boldsymbol{\tau}]\!]\rho = \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho[\xi \mapsto \mathrm{AR}]$
4. $\mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho = \mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho[\xi \mapsto \mathrm{AR}]$
5. $\mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho = \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
6. $\mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho = \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$.

Proof

Assume $\xi \notin \mathrm{ftv}(\boldsymbol{\tau})$ and $\xi \notin \mathrm{ftv}(\boldsymbol{\sigma})$. We will need to prove the following:

1. (a) $(W, \mathbf{S_1}, \mathbf{S_2}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho \implies (W, \mathbf{S_1}, \mathbf{S_2}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{S_1}, \mathbf{S_2}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{S_1}, \mathbf{S_2}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$
2. (a) $(W, \mathbf{R_1}, \mathbf{R_2}) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho \implies (W, \mathbf{R_1}, \mathbf{R_2}) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{R_1}, \mathbf{R_2}) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{R_1}, \mathbf{R_2}) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$
3. (a) $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho \implies (W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$
4. (a) $(W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho \implies (W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho$
5. (a) $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho \implies (W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho$
6. (a) $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho \implies (W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho$.

We will prove all these claims simultaneously, by induction on $W.k$ and $\boldsymbol{\tau}$.

1. We use an additional induction and case analysis on the structure of $\boldsymbol{\sigma}$.

   Case $\boldsymbol{\zeta}$ Immediate, since $\xi \neq \boldsymbol{\zeta}$.

   Case $\bullet$ Immediate.

   Case $\boldsymbol{\tau} :: \boldsymbol{\sigma}$ For part (a), we have $\mathbf{S_1} = \mathbf{w_1} :: \mathbf{S_1'}$, $\mathbf{S_2} = \mathbf{w_2} :: \mathbf{S_2'}$, $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$, and $(W, \mathbf{S_1'}, \mathbf{S_2'}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$. We need to show that $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho[\xi \mapsto \mathrm{AR}]$ and $(W, \mathbf{S_1'}, \mathbf{S_2'}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$. The latter holds by the induction hypothesis for $\boldsymbol{\sigma}$ and the former holds by claim 3.
   Part (b) is similar.

2. Follows from claim 3.

3. Consider the possible cases of $\boldsymbol{\tau}$:

   Case $\boldsymbol{\alpha}$ Immediate, since $\boldsymbol{\alpha} \neq \xi$.

Case $\mathbf{unit}$ Immediate.

Case $\mathbf{int}$ Immediate.

Case $\exists\alpha.\tau$ By the induction hypothesis for τ.

Case $\mu\alpha.\tau$ By the induction hypothesis for $W.k$.

Case $\mathbf{ref}\,\langle\tau_1,\ldots,\tau_n\rangle$ Follows from claim 4.

Case $\mathbf{box}\,\langle\tau_1,\ldots,\tau_n\rangle$ Follows from claim 4.

Case $\mathbf{box}\,\forall[\Delta].\{\chi;\sigma'\}^{q'}$ Follows from claim 4.

4. Consider the two possible cases of ψ:

   Case $\forall[\Delta].\{\chi;\sigma'\}^{q'}$ Follows from claims 1 and 2 (using the induction hypothesis for τ) and from claim 5 (using the induction hypothesis for $W.k$).

   Case $\langle\tau_1,\ldots,\tau_n\rangle$ Follows from claim 3 (using the induction hypothesis for τ).

5. Follows from claim 6.

6. Follows from claims 1 and 3.

□

Lemma 1.14 (Substitution)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, $\alpha \notin \Delta$, $\Delta \vdash \tau'$, and $\Delta,\alpha \vdash \tau$, $\Delta,\alpha \vdash \sigma$, $\Delta,\alpha \vdash \chi$, $\Delta,\alpha \vdash \psi$. Then

1. $\mathcal{S}[\![\sigma]\!]\rho[\alpha \mapsto (\rho_1(\tau'),\rho_2(\tau'),\mathcal{W}[\![\tau']\!]\rho)] = \mathcal{S}[\![\sigma[\tau'/\alpha]]\!]\rho$
2. $\mathcal{R}[\![\chi]\!]\rho[\alpha \mapsto (\rho_1(\tau'),\rho_2(\tau'),\mathcal{W}[\![\tau']\!]\rho)] = \mathcal{R}[\![\chi[\tau'/\alpha]]\!]\rho$
3. $\mathcal{W}[\![\tau]\!]\rho[\alpha \mapsto (\rho_1(\tau'),\rho_2(\tau'),\mathcal{W}[\![\tau']\!]\rho)] = \mathcal{W}[\![\tau[\tau'/\alpha]]\!]\rho$
4. $\mathcal{HV}[\![\psi]\!]\rho[\alpha \mapsto (\rho_1(\tau'),\rho_2(\tau'),\mathcal{W}[\![\tau']\!]\rho)] = \mathcal{HV}[\![\psi[\tau'/\alpha]]\!]\rho$
5. $\mathcal{E}[\![q \vdash \tau;\sigma]\!]\rho[\alpha \mapsto (\rho_1(\tau'),\rho_2(\tau'),\mathcal{W}[\![\tau']\!]\rho)] = \mathcal{E}[\![q[\tau'/\alpha] \vdash \tau[\tau'/\alpha];\sigma[\tau'/\alpha]]\!]\rho$
6. $\mathcal{K}[\![q \vdash \tau;\sigma]\!]\rho[\alpha \mapsto (\rho_1(\tau'),\rho_2(\tau'),\mathcal{W}[\![\tau']\!]\rho)] = \mathcal{K}[\![q[\tau'/\alpha] \vdash \tau[\tau'/\alpha];\sigma[\tau'/\alpha]]\!]\rho$.

Proof

Follows the structure of the proof of Lemma 1.13. The only case that depends on ρ is in claim 3, in the case where $\tau = \beta$. But the needed equality is immediate in this case, whether $\alpha = \beta$ or not. □

Lemma 1.15 (Substitution for Stack Types)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, $\zeta \notin \Delta$, $\Delta \vdash \sigma'$, and $\Delta,\zeta \vdash \tau$, $\Delta,\zeta \vdash \sigma$, $\Delta,\zeta \vdash \chi$, $\Delta,\zeta \vdash \psi$. Then

1. $\mathcal{S}[\![\sigma]\!]\rho[\zeta \mapsto (\rho_1(\sigma'),\rho_2(\sigma'),\mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{S}[\![\sigma[\sigma'/\zeta]]\!]\rho$
2. $\mathcal{R}[\![\chi]\!]\rho[\zeta \mapsto (\rho_1(\sigma'),\rho_2(\sigma'),\mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{R}[\![\chi[\sigma'/\zeta]]\!]\rho$
3. $\mathcal{W}[\![\tau]\!]\rho[\zeta \mapsto (\rho_1(\sigma'),\rho_2(\sigma'),\mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{W}[\![\tau[\sigma'/\zeta]]\!]\rho$
4. $\mathcal{HV}[\![\psi]\!]\rho[\zeta \mapsto (\rho_1(\sigma'),\rho_2(\sigma'),\mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{HV}[\![\psi[\sigma'/\zeta]]\!]\rho$
5. $\mathcal{E}[\![q \vdash \tau;\sigma]\!]\rho[\zeta \mapsto (\rho_1(\sigma'),\rho_2(\sigma'),\mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{E}[\![q[\sigma'/\zeta] \vdash \tau[\sigma'/\zeta];\sigma[\sigma'/\zeta]]\!]\rho$
6. $\mathcal{K}[\![q \vdash \tau;\sigma]\!]\rho[\zeta \mapsto (\rho_1(\sigma'),\rho_2(\sigma'),\mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{K}[\![q[\sigma'/\zeta] \vdash \tau[\sigma'/\zeta];\sigma[\sigma'/\zeta]]\!]\rho$.

Proof

Follows the structure of the proof of Lemma 1.13. The only case that depends on $\rho(\zeta)$ is in claim 1, in the case where $\sigma = \zeta'$. But the needed equality is immediate, whether $\zeta = \zeta'$ or not. □

Lemma 1.16 (Substitution for Return Markers)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, $\Delta \vdash q'$, and $\Delta,\epsilon \vdash \tau$, $\Delta,\epsilon \vdash \sigma$, $\Delta,\epsilon \vdash \chi$, $\Delta,\epsilon \vdash \psi$. Then

1. $\mathcal{S}[\![\sigma]\!]\rho[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))] = \mathcal{S}[\![\sigma[\mathbf{q}'/\epsilon]]\!]\rho$
2. $\mathcal{R}[\![\chi]\!]\rho[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))] = \mathcal{R}[\![\chi[\mathbf{q}'/\epsilon]]\!]\rho$
3. $\mathcal{W}[\![\tau]\!]\rho[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))] = \mathcal{W}[\![\tau[\mathbf{q}'/\epsilon]]\!]\rho$
4. $\mathcal{HV}[\![\psi]\!]\rho[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))] = \mathcal{HV}[\![\psi[\mathbf{q}'/\epsilon]]\!]\rho$
5. $\mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))] = \mathcal{E}[\![\mathbf{q}[\mathbf{q}'/\epsilon] \vdash \tau[\mathbf{q}'/\epsilon]; \sigma[\mathbf{q}'/\epsilon]]\!]\rho$
6. $\mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))] = \mathcal{K}[\![\mathbf{q}[\mathbf{q}'/\epsilon] \vdash \tau[\mathbf{q}'/\epsilon]; \sigma[\mathbf{q}'/\epsilon]]\!]\rho$.

Proof

Followed the structure of the proof of Lemma 1.13. There are no interesting cases. □

1.4.5 Properties of Semantic Interpretations

Lemma 1.17
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \tau$, then $\mathcal{W}[\![\tau]\!]\rho \in \mathrm{WvalRel}[\rho_1(\tau), \rho_2(\tau)]$.

Proof

Follows from monotonicity. □

Lemma 1.18
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \sigma$, then $\mathcal{S}[\![\sigma]\!]\rho \in \mathrm{StackRel}[\rho_1(\sigma), \rho_2(\sigma)]$.

Proof

Proceed by induction on the structure of σ.

Case ζ From $\Delta \vdash \sigma$ we have that $\zeta \in \Delta$. Since $\rho \in \mathcal{D}[\![\Delta]\!]$, it follows that $\mathcal{S}[\![\zeta]\!]\rho = \rho(\zeta).\varphi_S \in \mathrm{StackRel}[\rho_1(\zeta), \rho_2(\zeta)]$.

Case $\bullet$ In this case, $\mathcal{S}[\![\bullet]\!]\rho = \{ (W, \mathbf{nil}\uparrow, \mathbf{nil}\uparrow) \mid W \in \mathrm{World} \} \in \mathrm{StackRel}[\bullet, \bullet]$ is immediate from the definition of StackRel.

Case $\tau :: \sigma$ For any $(W, \mathbf{w_1} :: \mathbf{S_1}\uparrow, \mathbf{w_2} :: \mathbf{S_2}\uparrow) \in \mathcal{S}[\![\tau :: \sigma]\!]\rho$, we need that $W.\Psi_i \vdash \mathbf{w_i} :: \mathbf{S_i} : \rho_i(\tau :: \sigma)$. From the definition of $\mathcal{S}[\![\tau :: \sigma]\!]\rho$ we have $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho$ and $(W, \mathbf{S_1}\uparrow, \mathbf{S_2}\uparrow) \in \mathcal{S}[\![\sigma]\!]\rho$, from which we have that $W.\Psi_i; \cdot \vdash \mathbf{w_i} : \rho_i(\tau)$ and $W.\Psi_i \vdash \mathbf{S_i} : \rho_i(\sigma)$, which gives us what we need.

□

Lemma 1.19 (Register File Subtyping Implies Inclusion)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \chi \leq \chi'$. Then $\mathcal{R}[\![\chi]\!]\rho \subseteq \mathcal{R}[\![\chi']\!]\rho$.

Proof

Consider arbitrary $(W, M_1, M_2) \in \mathcal{R}[\![\chi]\!]\rho$. Note that $M_1 = \mathbf{R_1}\uparrow$ and $M_2 = \mathbf{R_2}\uparrow$. We must show that $(W, M_1, M_2) = (W, \mathbf{R_1}\uparrow, \mathbf{R_2}\uparrow) \in \mathcal{R}[\![\chi']\!]\rho$.

Consider $(\mathbf{r} : \tau) \in \chi'$. We must show $(W, \mathbf{R_1(r)}, \mathbf{R_2(r)}) \in \mathcal{W}[\![\tau]\!]\rho$. From the hypothesis $\Delta \vdash \chi \leq \chi'$, it follows that $\mathbf{r} : \tau \in \chi$. We use the latter to instantiate $(W, \mathbf{R_1}\uparrow, \mathbf{R_2}\uparrow) \in \mathcal{R}[\![\chi]\!]\rho$, which gives us what we needed to show. □

Lemma 1.20 (World Updates that Respect Register-File Relation)
Let $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ and $W' \sqsupseteq W$.

1. If $W'(i_{\mathrm{reg}}) = W(i_{\mathrm{reg}})$, then $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho$.
2. Let $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\mathrm{reg}} \mapsto \mathrm{island}_{\mathrm{reg}}(s, W.k)])$, where $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \mathbf{w_1}], W.\chi_1[\mathbf{r_d} : \rho_1(\tau)], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \mathbf{w_2}], W.\chi_2[\mathbf{r_d} : \rho_2(\tau)])$. If $(W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho$, then $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\mathbf{r_d} : \tau]]\!]\rho$.

Proof

1. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W'(i_{\text{reg}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$.

   Instantiate the first premise with $(\widetilde{W}, M_1, M_2)$, noting that the latter is in $\text{currentMR}(W(i_{\text{reg}}))$ since $W'(i_{\text{reg}}) = W(i_{\text{reg}})$, and noting that $\widetilde{W} \sqsupseteq W$ by transitivity of $\sqsupseteq$. Hence, $(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$ as we needed to show.

2. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W'(i_{\text{reg}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$. Note that M_i must be of the form $\mathbf{R_i}\uparrow$ and $\mathbf{R_i} = W'.\mathbf{R_i}$.

   Consider arbitrary $(\mathbf{r} : \boldsymbol{\tau'}) \in \boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau}]$. We must show that $(\widetilde{W}, \mathbf{R_1(r)}, \mathbf{R_2(r)}) \in \mathcal{W}[\![\boldsymbol{\tau'}]\!]\rho$.

   Case $\mathbf{r} = \mathbf{r_d}$: Then $\boldsymbol{\tau'} = \boldsymbol{\tau}$ and $\mathbf{R_i(r)} = \mathbf{w_i}$, which means that it suffices to show $(\widetilde{W}, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$. This latter is immediate from the premise $(W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$ using monotonicity (Lemma 1.8).

   Case $\mathbf{r} \neq \mathbf{r_d}$: Then $\mathbf{R_i(r)} = W'.\mathbf{R_i(r)} = W.\mathbf{R_i(r)}$, which means that it suffices to show $(\widetilde{W}, W.\mathbf{R_1(r)}, W.\mathbf{R_2(r)}) \in \mathcal{W}[\![\boldsymbol{\tau'}]\!]\rho$. Instantiate the first premise with $(\widetilde{W}, W.\mathbf{R_1}\uparrow, W.\mathbf{R_2}\uparrow)$ noting that the latter is in $\text{currentMR}(W(i_{\text{reg}}))$ by the definition of $\text{island}_{\text{reg}}$. Also note that $\widetilde{W} \sqsupseteq W$ by transitivity of $\sqsupseteq$. Hence, we have that $(\widetilde{W}, W.\mathbf{R_1}\uparrow, W.\mathbf{R_2}\uparrow) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$. Instantiating the latter with $(\mathbf{r} : \boldsymbol{\tau'}) \in \boldsymbol{\chi}$ gives us $(\widetilde{W}, W.\mathbf{R_1(r)}, W.\mathbf{R_2(r)}) \in \mathcal{W}[\![\boldsymbol{\tau'}]\!]\rho$ as we needed to show.

□

Lemma 1.21 (World Updates that Respect Stack Relation)
Let $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ and $W' \sqsupseteq W$.

1. If $W'(i_{\text{stk}}) = W(i_{\text{stk}})$, then $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$.

2. Let $W.S_1 = w_{11} :: \cdots :: w_{1n} :: S_1'$, $W.S_2 = w_{21} :: \cdots :: w_{2n} :: S_2'$, $\sigma = \tau_1 :: \cdots :: \tau_n :: \sigma'$ and $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\text{stk}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$, where $s = (S_1', \sigma', S_2', \sigma')$. $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma'}]\!]\rho$.

3. Let $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\text{stk}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$, where $s = (w_{11} :: \cdots :: w_{1n} :: S_1, \tau_1 :: \cdots :: \tau_n :: \sigma, w_{21} :: \cdots :: w_{2n} :: S_2, \tau_1 :: \cdots :: \tau_n :: \sigma)$. If $(W', \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\boldsymbol{\tau}_i]\!]\rho$, then $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\tau_1} :: \cdots :: \boldsymbol{\tau_n} :: \boldsymbol{\sigma}]\!]\rho$.

4. Let $W.S_1 = w_{11} :: \cdots :: w_{1n} :: S_1'$, $W.S_2 = w_{21} :: \cdots :: w_{2n} :: S_2'$, $\sigma = \tau_1 :: \cdots :: \tau_n :: \sigma'$ and $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\text{stk}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$, where $s = (w_{11} :: \cdots :: w_{1n-1} :: w_1' :: S_1', \tau_1 :: \cdots :: \tau_{n-1} :: \tau' :: \sigma', w_{21} :: \cdots :: w_{2n-1} :: w_2' :: S_2', \tau_1 :: \cdots :: \tau_{n-1} :: \tau' :: \sigma')$. If $(W', \mathbf{w_1'}, \mathbf{w_2'}) \in \mathcal{W}[\![\boldsymbol{\tau'}]\!]\rho$, then $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\tau_1} :: \cdots :: \boldsymbol{\tau_{n-1}} :: \boldsymbol{\tau'} :: \boldsymbol{\sigma}]\!]\rho$.

Proof

1. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W'(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$.

   Instantiate the first premise with $(\widetilde{W}, M_1, M_2)$, noting that the latter is in $\text{currentMR}(W(i_{\text{stk}}))$ since $W'(i_{\text{stk}}) = W(i_{\text{stk}})$, and noting that $\widetilde{W} \sqsupseteq W$ by transitivity of $\sqsupseteq$. Hence, $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ as we needed to show.

2. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W'(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\sigma']\!]\rho$. Note that M_i must be of the form $\mathbf{S_i'}\uparrow$ and $\mathbf{S_i'} = W'.\mathbf{S_i}$. The desired result follows directly from monotonicity (Lemma 1.8) after unfolding $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$.

3. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W'(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\tau_1 :: \cdots :: \tau_n :: \sigma]\!]\rho$. Note that M_i must be of the form $\mathbf{w_{j1}} :: \cdots :: \mathbf{w_{jn}} :: \mathbf{S_j}\uparrow$ and $\mathbf{w_{j1}} :: \cdots :: \mathbf{w_{jn}} :: \mathbf{S_j} = W'.\mathbf{S_j}$. The desired result follows directly from monotonicity (Lemma 1.8) after unfolding $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\tau_1} :: \cdots :: \boldsymbol{\tau_n} :: \boldsymbol{\sigma}]\!]\rho$ and premise $(W', \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\boldsymbol{\tau}_i]\!]\rho$.

4. Let $\sigma' = \tau_1 :: \cdots :: \tau_n :: \sigma$. Consider arbitrary $1 \leq k \leq |\sigma'|$ such that such that $(\sigma'(k) = \tau_k$. We must show that $(\widetilde{W}, \mathbf{W'.S_1(k)}, \mathbf{W'.S_2(k)}) \in \mathcal{W}[\![\tau]\!]\rho$.

   Case $\mathbf{k = n}$: Then $\tau' = \tau_k$ and $\mathbf{W'.S_j(k)} = \mathbf{w'_j}$, which means that it suffices to show $(\widetilde{W}, \mathbf{w'_1}, \mathbf{w'_2}) \in \mathcal{W}[\![\tau']\!]\rho$. This latter is immediate from the premise $(W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho$ using monotonicity (Lemma 1.8).

   Case $\mathbf{k \neq n}$: Then $\mathbf{W'.S_j(k)} = W.\mathbf{S_j(k)}$, which means that it suffices to show $(\widetilde{W}, W.\mathbf{S_1(k)}, W.\mathbf{S_2(k)}) \in \mathcal{W}[\![\tau_k]\!]\rho$. Instantiate the first premise with $(\widetilde{W}, W.\mathbf{S_1}\restriction, W.\mathbf{S_2}\restriction)$ noting that the latter is in currentMR$(W(i_{\text{reg}}))$ by the definition of island$_{\text{reg}}$. Also note that $\widetilde{W} \sqsupseteq W$ by transitivity of $\sqsupseteq$. Hence, we have that $(\widetilde{W}, W.\mathbf{S_1}\restriction, W.\mathbf{S_2}\restriction) \in \mathcal{R}[\![\sigma]\!]\rho$. Instantiating the latter with $(\tau_k) = \sigma(k)$ gives us $(\widetilde{W}, W.\mathbf{S_1(k)}, W.\mathbf{S_2(k)}) \in \mathcal{W}[\![\tau_k]\!]\rho$ as we needed to show.

□

Lemma 1.22 (Heap Interpretation Extension with Boxheap)
If $W \in \mathcal{H}[\![\Psi]\!]$, $\Psi \vdash \mathbf{H_1} \approx_{\text{H}} \mathbf{H_2} : \Psi'$, and boxheap$(\Psi')$, then $W \boxplus (\mathbf{H_1}, \mathbf{H_2}) \in \mathcal{H}[\![\Psi, \Psi']\!]$.

Proof

By induction on $W.k$.

To show $W \boxplus (\mathbf{H_1}, \mathbf{H_2}) \in \mathcal{H}[\![\Psi, \Psi']\!]$, it suffices to show

$$\forall (\ell :^{\nu} \psi) \in (\Psi, \Psi'). (W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \ell, \ell) \in \mathcal{W}[\![\nu\ \psi]\!]\emptyset$$

where ν is **box** or **ref**.

Consider arbitrary $(\ell :^{\nu} \psi) \in (\Psi, \Psi')$. If $\ell \in \text{dom}(\Psi)$, for any value of $W.k$, it follows from the first premise that $(W, \ell, \ell) \in \mathcal{W}[\![\nu\ \psi]\!]\emptyset$. By Lemma 1.5 we have that $W \boxplus (\mathbf{H_1}, \mathbf{H_2}) \sqsupseteq W$, so by monotonicity we have $(W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \ell, \ell) \in \mathcal{W}[\![\nu\ \psi]\!]\emptyset$.

Therefore, it remains for us to show that if $\ell \in \text{dom}(\Psi')$ then $(W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\ \psi]\!]\emptyset$.

Case $W.k = 0$: Consider arbitrary $(\widetilde{W}, M_1, M_2) \in$ currentMR$((W \boxplus (\mathbf{H_1}, \mathbf{H_2}))(i_{\text{box}}))$ such that $\widetilde{W} \sqsupset (W \boxplus (\mathbf{H_1}, \mathbf{H_2}))$. But the latter implies $\widetilde{W}.k < W.k = 0$ which leads to a contradiction since $\widetilde{W} \in$ World which requires that $\widetilde{W}.k \geq 0$. So we are done.

Case $W.k = n + 1$ for $n \geq 0$: By the induction hypothesis we know that the lemma we wish to prove holds for any W such that $W.k = n$. We must prove it for any W such that $W.k = n + 1$.
We have that $\ell \in \text{dom}(\Psi')$ and must show that $(W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\ \psi]\!]\emptyset$.
Consider arbitrary $(\widetilde{W}, M_1, M_2) \in$ currentMR$((W \boxplus (\mathbf{H_1}, \mathbf{H_2}))(i_{\text{box}}))$ such that $\widetilde{W} \sqsupset (W \boxplus (\mathbf{H_1}, \mathbf{H_2}))$. Note that it must be the case that $M_1 = (W(i_{\text{box}}).s.H_1 \uplus \mathbf{H_1})\restriction$ and $M_2 = (W(i_{\text{box}}).s.H_2 \uplus \mathbf{H_2})\restriction$. Also, since $\ell \in \text{dom}(\Psi')$, from the second premise it follows that $\ell \in \text{dom}(\mathbf{H_1})$ and $\ell \in \text{dom}(\mathbf{H_2})$. Regardless of whether ψ is a code type or tuple type, it suffices to show:

$$\begin{aligned} &(\widetilde{W}, M_1(\ell), M_2(\ell)) \in \mathcal{HV}[\![\psi]\!]\emptyset \\ \equiv\ &(\widetilde{W}, \mathbf{H_1}(\ell), \mathbf{H_2}(\ell)) \in \mathcal{HV}[\![\psi]\!]\emptyset \end{aligned}$$

From the second premise, since $(\ell :^{\text{box}} \psi) \in \Psi'$, it follows that:

$$\Psi, \Psi' \vdash \mathbf{H_1}(\ell) \approx_{\text{hv}} \mathbf{H_2}(\ell) : {}^{\mathbf{box}}\psi. \tag{1}$$

Since $\triangleright W \in \mathcal{H}[\![\Psi]\!]$ by heap monototonicity (Lemma 1.9) and since $(\triangleright W).k = n$, by the induction hypothesis we have that $(\triangleright W \boxplus (\mathbf{H_1}, \mathbf{H_2})) \in \mathcal{H}[\![\Psi, \Psi']\!]$. Thus, we can instantiate (1) with $\triangleright W \boxplus (\mathbf{H_1}, \mathbf{H_2})$, which allows us to conclude that

$$(\triangleright W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \mathbf{H_1}(\ell), \mathbf{H_2}(\ell)) \in \mathcal{HV}[\![\psi]\!]\emptyset$$

Now, since $\widetilde{W} \sqsupset (W \boxplus (\mathbf{H_1}, \mathbf{H_2}))$, we can use by Lemma 1.6 to conclude $\widetilde{W} \sqsupseteq \triangleright(W \boxplus (\mathbf{H_1}, \mathbf{H_2}))$. Hence, by monotonicity, we have $(\widetilde{W}, \mathbf{H_1}(\ell), \mathbf{H_2}(\ell)) \in \mathcal{HV}[\![\psi]\!]\emptyset$ as we needed to show.

□

1.5 Compatibility Lemmas

Lemma 1.23 (Component)
If $\mathbf{\Psi} \vdash \mathbf{H_1} \approx_{\mathrm{H}} \mathbf{H_2} : \mathbf{\Psi'}$, boxheap($\mathbf{\Psi'}$), ret-type($\mathbf{q}, \chi, \sigma$) = $\tau; \sigma'$, and $(\mathbf{\Psi}, \mathbf{\Psi'}); \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathrm{I}} \mathbf{I_2}$, then $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash (\mathbf{I_1}, \mathbf{H_1}) \approx (\mathbf{I_2}, \mathbf{H_2}) : \tau; \sigma'$.

Proof

From the premises, we have that $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash (\mathbf{I_i}, \mathbf{H_i}) : \tau; \sigma'$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, currentMR($W(i_{\mathrm{reg}})$) $\Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR($W(i_{\mathrm{stk}})$) $\Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$(W, \rho_1((\mathbf{I_1}, \mathbf{H_1})), \rho_2((\mathbf{I_2}, \mathbf{H_2}))) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma']\!]\rho$$

or equivalently, noting that the typing rules for heap fragments ensure they have no free type variables,

$$(W, (\rho_1(\mathbf{I_1}), \mathbf{H_1}), (\rho_1(\mathbf{I_2}), \mathbf{H_2})) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma']\!]\rho$$

In the following, let $\tau_{\mathrm{r}}; \sigma_{\mathrm{r}} =$ ret-type($\mathbf{q}, \chi, \sigma$).

We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

- We claim that $(W, (\rho_1(\mathbf{I_1}), \mathbf{H_1}), (\rho_1(\mathbf{I_2}), \mathbf{H_2})) \in$ TermAtom$[\mathbf{q} \vdash \tau_{\mathrm{r}}; \sigma_{\mathrm{r}}]\rho$. To establish this, we must show:
$$W.\Psi_i; \cdot; W.\chi_{\mathrm{i}}; W.\sigma_{\mathrm{i}}; \rho_i(\mathbf{q}) \vdash (\rho_i(\mathbf{I_i}), \mathbf{H_i}) : \rho_i(\tau_{\mathrm{r}}); \rho_i(\sigma_{\mathrm{r}})$$
Applying the typing rule, we see we need to show that
$$W.\mathbf{\Psi_i} \vdash \mathbf{H_i} : \mathbf{\Psi'} \qquad \text{and} \qquad (W.\mathbf{\Psi_i}, \mathbf{\Psi'}); \cdot; W.\chi_{\mathrm{i}}; W.\sigma_{\mathrm{i}}; \rho_i(\mathbf{q}) \vdash \rho_{\mathrm{i}}(\mathbf{I_i})$$
We know that $\mathbf{\Psi} \subseteq W.\mathbf{\Psi_i}$ (from $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$), $\chi \subseteq W.\chi_{\mathrm{i}}$ (from currentMR($W(i_{\mathrm{reg}})$) $\Subset_W \mathcal{R}[\![\chi]\!]\rho$), and $\sigma \subseteq W.\sigma_{\mathrm{i}}$ (from currentMR($W(i_{\mathrm{stk}})$) $\Subset_W \mathcal{S}[\![\sigma]\!]\rho$). Combining these with the premise $(\mathbf{\Psi}, \mathbf{\Psi'}); \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_i}$ yields what we need.
- Let $\mathbf{H'_1} = \mathbf{H_1}[\overline{\ell'/\ell}]$ and $\mathbf{H'_2} = \mathbf{H_2}[\overline{\ell'/\ell}]$, where $\overline{\ell'} \notin (\mathrm{dom}(W.\Psi_1) \cup \mathrm{dom}(W.\Psi_2))$ and $\overline{\ell'}$ are mutually disjoint. Let $\mathbf{\Psi''} = \mathbf{\Psi'}[\overline{\ell'/\ell}]$. Note that $\mathbf{\Psi} \vdash \mathbf{H'_i} : \mathbf{\Psi''}$ and boxheap($\mathbf{\Psi''}$).
Let $W' = W \boxplus (\mathbf{H'_1}, \mathbf{H'_2})$.
- Let $\mathbf{H_{b1}} = W(i_{\mathrm{box}}).s.\mathbf{H_1}$ and $\mathbf{H_{b2}} = W(i_{\mathrm{box}}).s.\mathbf{H_2}$. Note that $W'(i_{\mathrm{box}}).s = (\mathbf{H_{b1}} \uplus \mathbf{H'_1}, \mathbf{H_{b2}} \uplus \mathbf{H'_2})$.
- Note that $W' \in$ World.
- By Lemma 1.5, we have that $W' \sqsupseteq_{\mathrm{pub}} W$
- Consider arbitrary $(M_1, M_2) : W$. Let $M_i = (\mathbf{H_{Mi}}, \mathbf{R_i}, \mathbf{S_i})$. Note that $\mathrm{dom}(\mathbf{H_{Mi}}) = \mathrm{dom}(W.\Psi_i)$, which implies $\overline{\ell'} \notin \mathrm{dom}(\mathbf{H_{Mi}})$. Also note that
$$\langle (\mathbf{H_{Mi}}, \mathbf{R_i}, \mathbf{S_i}) \mid (\rho_i(\mathbf{I_i}), \mathbf{H_i}) \rangle \longmapsto^0 \ldots \longmapsto^0 \langle ((\mathbf{H_{Mi}}, \mathbf{H'_i}), \mathbf{R_i}, \mathbf{S_i}) \mid (\rho_i(\mathbf{I_i})[\overline{\ell'/\ell}], \cdot) \rangle$$
Let $M'_i = ((\mathbf{H_{Mi}}, \mathbf{H'_i}), \mathbf{R_i}, \mathbf{S_i})$. From our choice of W', it follows that
$$(\triangleright W', \mathbf{H_{b1}} \uplus \mathbf{H'_1}, \mathbf{H_{b2}} \uplus \mathbf{H'_2}) \in \mathrm{currentMR}(W'(i_{\mathrm{box}}))$$
which together with $(M_1, M_2) : W$ is sufficient to show $(M'_1, M'_2) : W'$.
- Note that $W.k \leq W'.k$.
- Note that $\mathbf{q} \neq \epsilon$, which follows from the first hypothesis since it is a side condition of the component typing rules.

- Next, from our last hypothesis, by alpha-renaming locations in $\mathrm{dom}(\Psi')$ to $\mathrm{dom}(\Psi'')$—which we can do since $\overline{\ell'} \notin \Psi$, a fact that follows from $\overline{\ell'} \notin W.\Psi_1 \cup W.\Psi_2$ and $W \in \mathcal{H}[\![\Psi]\!]$—we have the following:

$$(\Psi, \Psi''); \Delta; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1}\overline{[\ell'/\ell]} \approx_{\mathrm{I}} \mathbf{I_2}\overline{[\ell'/\ell]}$$

We instantiate the above with W' and ρ. Note that $W' \in \mathcal{H}[\![\Psi, \Psi'']\!]$ by Lemma 1.22; $\rho \in \mathcal{D}[\![\Delta]\!]$ from above; $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho$ by Lemma 1.20 since $W'(i_{\mathrm{reg}}) = W(i_{\mathrm{reg}})$; and $\mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$ by Lemma 1.21 since $W'(i_{\mathrm{stk}}) = W(i_{\mathrm{stk}})$.

Thus, we can conclude that:

$$(W', (\rho_1(\mathbf{I_1})\overline{[\ell'/\ell]}, \cdot), (\rho_2(\mathbf{I_2})\overline{[\ell'/\ell]}, \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

Now, the result follows by Lemma 1.11.

□

Lemma 1.24 (Heap Fragment)
Let $\cdot \vdash \psi_1, \ldots, \cdot \cdot \cdot \vdash \psi_n$ and $\Psi' = \ell_1 : {}^{\nu_1}\psi_1, \ldots, \ell_n : {}^{\nu_n}\psi_n$ such that $\mathrm{dom}(\Psi) \cap \mathrm{dom}(\Psi') = \emptyset$. If for each i, we have $\Psi, \Psi' \vdash \mathbf{h_{1i}} \approx_{\mathrm{hv}} \mathbf{h_{2i}} : {}^{\nu_i}\psi_i$, then $\Psi \vdash \ell_1 \mapsto \mathbf{h_{11}}, \ldots \ell_n \mapsto \mathbf{h_{1n}} \approx_{\mathrm{H}} \ell_1 \mapsto \mathbf{h_{21}}, \ldots \ell_n \mapsto \mathbf{h_{2n}} : \Psi'$.

Proof

From $\Psi, \Psi' \vdash \mathbf{h_{1i}} \approx_{\mathrm{hv}} \mathbf{h_{2i}} : {}^{\nu_i}\psi_i$ we have $\Psi, \Psi' \vdash \mathbf{h_{1i}} : {}^{\nu_i}\psi_i$ and $\Psi, \Psi' \vdash \mathbf{h_{2i}} : {}^{\nu_i}\psi_i$. This means that $\Psi \vdash \ell_1 \mapsto \mathbf{h_{i1}}, \ldots \ell_n \mapsto \mathbf{h_{in}} : \Psi'$ for $i \in \{1, 2\}$. Now choose arbitrary $\ell_i \mapsto \psi_i \in \Psi'$. We must show $\Psi, \Psi' \vdash \mathbf{H_1}(\ell_i) \approx_{\mathrm{hv}} \mathbf{H_2}(\ell_i) : {}^{\nu_i}\psi_i$, where $\mathbf{H_i} = \ell_1 \mapsto \mathbf{h_{i1}}, \ell_2 \ldots$. But note that $\mathbf{H_1}(\ell_i)$ is $\mathbf{h_{1i}}$, and from the hypothesis we know that $\Psi, \Psi' \vdash \mathbf{h_{1i}} \approx_{\mathrm{hv}} \mathbf{h_{2i}} : {}^{\nu_i}\psi_i$, so the result is immediate. □

Lemma 1.25 (Code Block)
If $\cdot \vdash \forall[\Delta].\{\chi; \sigma\}^{\mathbf{q}}$ and $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathrm{I}} \mathbf{I_2}$, then
$\Psi \vdash \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{I_1} \approx_{\mathrm{hv}} \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{I_2} : {}^{\mathbf{box}}\forall[\Delta].\{\chi; \sigma\}^{\mathbf{q}}$.

Proof

By our hypothesis, $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1}$ and $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_2}$, so we have

$$\Psi \vdash \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{I_1} : {}^{\mathbf{box}}\forall[\Delta].\{\chi; \sigma\}^{\mathbf{q}} \quad \text{and} \quad \Psi \vdash \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{I_2} : {}^{\mathbf{box}}\forall[\Delta].\{\chi; \sigma\}^{\mathbf{q}}.$$

Let $W \in \mathcal{H}[\![\Psi]\!]$. We need to show that

$$(W, \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{I_1}, \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{I_2}) \in \mathcal{HV}[\![\forall[\Delta].\{\chi; \sigma\}^{\mathbf{q}}]\!]\emptyset.$$

Let $W' \sqsupseteq W$, $\rho \in \mathcal{D}[\![\Delta]\!]$ such that $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho$ and $\mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$. We need to show that $(W', (\rho_1(\mathbf{I_1}), \cdot), (\rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho$.

By Lemma 1.9, $W' \in \mathcal{H}[\![\Psi]\!]$. We can instantiate our hypothesis with W' and ρ to get the result. □

Lemma 1.26 (Tuple)
If for each i, we have $\Psi; \cdot \vdash \mathbf{w_{1i}} \approx_{\mathrm{w}} \mathbf{w_{2i}} : \tau_i$, then $\Psi \vdash \langle \mathbf{w_{10}}, \ldots, \mathbf{w_{in}} \rangle \approx_{\mathrm{hv}} \langle \mathbf{w_{20}}, \ldots, \mathbf{w_{2n}} \rangle : {}^{\nu}\langle \tau_0, \ldots, \tau_n \rangle$.

Proof

Clearly, $\Psi \vdash \langle \mathbf{w_{10}}, \ldots, \mathbf{w_{in}} \rangle : {}^{\nu}\langle \tau_0, \ldots, \tau_n \rangle$ and $\Psi \vdash \langle \mathbf{w_{10}}, \ldots, \mathbf{w_{in}} \rangle : {}^{\nu}\langle \tau_0, \ldots, \tau_n \rangle$.

Let $W \in \mathcal{H}[\![\Psi]\!]$. We need to show that $(W, \langle \mathbf{w_{10}}, \ldots, \mathbf{w_{in}} \rangle, \langle \mathbf{w_{20}}, \ldots, \mathbf{w_{2n}} \rangle) \in \mathcal{HV}[\![\langle \tau_0, \ldots, \tau_n \rangle]\!]\emptyset$. But this only requires that for each i, $(W, \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\tau_i]\!]\emptyset$, and this holds by our hypothesis. □

Lemma 1.27 (Unit)
$\Psi; \Delta \vdash () \approx_{\mathrm{w}} () : \mathbf{unit}$.

Proof

Immediate, by definition of $\mathcal{W}[\![\mathbf{unit}]\!]\rho$. □

Lemma 1.28 (Integer)
$\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{n} \approx_{\mathrm{w}} \mathbf{n} : \mathbf{int}$.

Proof

Immediate, by definition of $\mathcal{W}[\![\mathbf{int}]\!]\rho$. □

Lemma 1.29 (Mutable Location)
If $\ell : {}^{\mathrm{ref}}\psi \in \mathbf{\Psi}$, then $\mathbf{\Psi}; \mathbf{\Delta} \vdash \ell \approx_{\mathrm{w}} \ell : \mathbf{ref}\ \psi$.

Proof

By our hypothesis, $\mathbf{\Psi}; \cdot \vdash \ell : \mathbf{ref}\ \psi$. Let $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$. We need to show that $(W, \ell, \ell) \in \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\rho$. We know that $\mathrm{ftv}(\psi) = \emptyset$, so by Lemma 1.13, $\mathcal{W}[\![\mathbf{ref}\ \psi]\!]\rho = \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\emptyset$. By definition of $\mathcal{H}[\![\mathbf{\Psi}]\!]$, $(W, \ell, \ell) \in \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\emptyset$, so we are done. □

Lemma 1.30 (Immutable Location)
If $\ell : {}^{\mathrm{box}}\psi \in \mathbf{\Psi}$, then $\mathbf{\Psi}; \mathbf{\Delta} \vdash \ell \approx_{\mathrm{w}} \ell : \mathbf{box}\ \psi$.

Proof

By our hypothesis, $\mathbf{\Psi}; \cdot \vdash \ell : \mathbf{box}\ \psi$. Let $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$. We need to show that $(W, \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\ \psi]\!]\rho$. We know that $\mathrm{ftv}(\psi) = \emptyset$, so by Lemma 1.13, $\mathcal{W}[\![\mathbf{box}\ \psi]\!]\rho = \mathcal{W}[\![\mathbf{box}\ \psi]\!]\emptyset$. By definition of $\mathcal{H}[\![\mathbf{\Psi}]\!]$, $(W, \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\ \psi]\!]\emptyset$, so we are done. □

Lemma 1.31 (Pack)
If $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \tau[\tau'/\alpha]$, then $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{pack}\langle \tau', \mathbf{w_1} \rangle\ \mathbf{as}\ \exists \alpha.\tau \approx_{\mathrm{w}} \mathbf{pack}\langle \tau', \mathbf{w_2} \rangle\ \mathbf{as}\ \exists \alpha.\tau : \exists \alpha.\tau$.

Proof

We have $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{pack}\langle \tau', \mathbf{w_1} \rangle\ \mathbf{as}\ \exists \alpha.\tau : \exists \alpha.\tau$ and $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{pack}\langle \tau', \mathbf{w_2} \rangle\ \mathbf{as}\ \exists \alpha.\tau : \exists \alpha.\tau$ by our hypothesis and the typing rules.

Let $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$. We need to show that

$$(W, \rho_1(\mathbf{pack}\langle \tau', \mathbf{w_1} \rangle\ \mathbf{as}\ \exists \alpha.\tau), \rho_2(\mathbf{pack}\langle \tau', \mathbf{w_2} \rangle\ \mathbf{as}\ \exists \alpha.\tau)) \in \mathcal{W}[\![\exists \alpha.\tau]\!]\rho.$$

By our hypothesis, $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau[\tau'/\alpha]]\!]\rho$. By Lemma 1.14,

$$\mathcal{W}[\![\tau[\tau'/\alpha]]\!]\rho = \mathcal{W}[\![\tau]\!]\rho[\alpha \mapsto (\rho_1(\tau'), \rho_2(\tau'), \mathcal{W}[\![\tau']\!]\rho)].$$

Thus we can complete the proof by supplying $\mathcal{W}[\![\tau']\!]\rho$ as the relation required by $\mathcal{W}[\![\exists \alpha.\tau]\!]\rho$. □

Lemma 1.32 (Fold)
If $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \tau[\mu\alpha.\tau/\alpha]$, then $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{w_2} : \mu\alpha.\tau$.

Proof

We have $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{w_1} : \mu\alpha.\tau$ and $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{w_2} : \mu\alpha.\tau$ by our hypothesis and the typing rules.

Let $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$. We need to show that

$$(W, \rho_1(\mathbf{w_1}), \rho_2(\mathbf{w_2})) \in \triangleright \mathcal{W}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

By our hypothesis, $(W, \rho_1(\mathbf{w_1}), \rho_2(\mathbf{w_2})) \in \mathcal{W}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$. The result follows by monotonicity. □

Lemma 1.33 (Word Type Application)
If $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \mathbf{box}\ \forall[\alpha, \mathbf{\Delta}'].\{\chi; \sigma\}^{\mathrm{q}}$ and $\mathbf{\Delta} \vdash \tau$, then

$$\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w_1}[\tau] \approx_{\mathrm{w}} \mathbf{w_2}[\tau] : \mathbf{box}\ \forall[\mathbf{\Delta}'].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathrm{q}[\tau/\alpha]}.$$

Proof

From the hypotheses, we have $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w}_i[\tau] : \mathbf{box}\,\forall[\mathbf{\Delta'}].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathbf{q}[\tau/\alpha]}$ for $i = 1$, $i = 2$.
Let $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$. We need to show that

$$(W, \rho_1(\mathbf{w}_1[\tau]), \rho_2(\mathbf{w}_2[\tau])) \in \mathcal{W}[\![\mathbf{box}\,\forall[\mathbf{\Delta'}].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathbf{q}[\tau/\alpha]}]\!]\rho.$$

Let $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$ such that $\widetilde{W} \sqsupset W$. Instantiating the first hypothesis with W and ρ, noting that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, we have that

$$(W, \rho_1(\mathbf{w}_1), \rho_2(\mathbf{w}_2)) \in \mathcal{W}[\![\mathbf{box}\,\forall[\alpha, \mathbf{\Delta'}].\{\chi; \sigma\}^{\mathbf{q}}]\!]\rho.$$

Hence, there must be some ℓ_i and $\overline{\omega_i}$ such that $\rho_i(\mathbf{w}_i) = \ell_i[\overline{\omega_i}]$. Instantiating the above with $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$, noting that $\widetilde{W} \sqsupset W$, we have that $M_i(\ell_i) = \mathbf{code}[\overline{\beta_i}, \alpha, \mathbf{\Delta'}]\{\chi_i; \sigma_i\}^{\mathbf{q}_i}.\mathbf{I}_i$, $\rho_i(\chi) = \chi_i[\overline{\omega_i/\beta_i}]$, $\rho_i(\sigma) = \sigma_i[\overline{\omega_i/\beta_i}]$, $\rho_i(\mathbf{q}) = \mathbf{q}_i[\overline{\omega_i/\beta_i}]$, and

$$(\widetilde{W}, (\mathbf{code}[\alpha, \mathbf{\Delta'}]\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\omega_1/\beta_1}], (\mathbf{code}[\alpha, \mathbf{\Delta'}]\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\alpha, \mathbf{\Delta'}].\{\chi; \sigma\}^{\mathbf{q}}]\!]\rho. \quad (2)$$

From the above equalities, we can conclude $\rho_i(\chi[\tau/\alpha]) = \chi_i[\overline{\omega_i/\beta_i}][\rho_i(\tau)/\alpha]$, $\rho_i(\sigma[\tau/\alpha]) = \sigma_i[\overline{\omega_i/\beta_i}][\rho_i(\tau)/\alpha]$, and $\rho_i(\mathbf{q}[\tau/\alpha]) = \mathbf{q}_i[\overline{\omega_i/\beta_i}][\rho_i(\tau)/\alpha]$.
It remains to show that

$$(\widetilde{W}, (\mathbf{code}[\mathbf{\Delta'}]\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\omega_1/\beta_1}][\rho_1(\tau)/\alpha], (\mathbf{code}[\mathbf{\Delta'}]\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\omega_2/\beta_2}][\rho_2(\tau)/\alpha]) \in \mathcal{HV}[\![\forall[\mathbf{\Delta'}].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathbf{q}[\tau/\alpha]}]\!]\rho.$$

Let $W' \sqsupseteq \widetilde{W}$, $\rho^* \in \mathcal{D}[\![\mathbf{\Delta'}]\!]$, $\rho' = \rho \cup \rho^*$ such that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\tau/\alpha]]\!]\rho'$ and $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma[\tau/\alpha]]\!]\rho'$. We need to show that

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\omega_1/\beta_1}][\rho_1(\tau)/\alpha]), \rho_2^*(\mathbf{I}_2[\overline{\omega_2/\beta_2}][\rho_2(\tau)/\alpha])) \in \mathcal{E}[\![\mathbf{q}[\tau/\alpha] \vdash \text{ret-type}(\mathbf{q}[\tau/\alpha], \chi[\tau/\alpha], \sigma[\tau/\alpha])]\!]\rho'.$$

Next, we instantiate (5) with W', $\rho^\dagger = \rho^*[\alpha \mapsto (\rho_1(\tau), \rho_2(\tau), \mathcal{W}[\![\tau]\!]\rho)]$, and $\tau'; \mathbf{sigma'} = \text{ret-type}(\mathbf{q}, \chi, \sigma)$, noting that $W' \sqsupseteq \widetilde{W}$ and $\rho^\dagger \in \mathcal{D}[\![\alpha, \mathbf{\Delta'}]\!]$, the latter since $\mathcal{W}[\![\tau]\!]\rho \in \text{WvalRel}[\rho_1(\tau), \rho_2(\tau)]$ by Lemma 1.17. Let $\rho'' = \rho \cup \rho^\dagger$. Note that $\rho'' = \rho'[\alpha \mapsto (\rho_1(\tau), \rho_2(\tau), \mathcal{W}[\![\tau]\!]\rho)] = \rho'[\alpha \mapsto (\rho_1'(\tau), \rho_2'(\tau), \mathcal{W}[\![\tau]\!]\rho')]$. Using Lemma 1.14 we have that $\mathcal{R}[\![\chi[\tau/\alpha]]\!]\rho' = \mathcal{R}[\![\chi]\!]\rho''$ and $\mathcal{S}[\![\sigma[\tau/\alpha]]\!]\rho' = \mathcal{R}[\![\sigma]\!]\rho''$. Therefore, note that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho''$ and $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho''$. Hence, it follows that

$$(W', \rho_1^\dagger(\mathbf{I}_1[\overline{\omega_1/\beta_1}]), \rho_2^\dagger(\mathbf{I}_2[\overline{\omega_2/\beta_2}])) \in \mathcal{E}[\![\mathbf{q} \vdash \tau'; \sigma']\!]\rho''.$$

Note that the above is equivalent to

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\omega_1/\beta_1}][\rho_1(\tau)/\alpha]), \rho_2^*(\mathbf{I}_2[\overline{\omega_2/\beta_2}][\rho_2(\tau)/\alpha])) \in \mathcal{E}[\![\mathbf{q} \vdash \tau'; \sigma']\!]\rho''.$$

By Lemma 1.14, we have that

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\omega_1/\beta_1}][\rho_1(\tau)/\alpha]), \rho_2^*(\mathbf{I}_2[\overline{\omega_2/\beta_2}][\rho_2(\tau)/\alpha])) \in \mathcal{E}[\![\mathbf{q}[\tau/\alpha] \vdash \tau'[\tau/\alpha]; \sigma'[\tau/\alpha]]\!]\rho'.$$

Finally, note that by the definition of ret-type, since $\text{ret-type}(\mathbf{q}, \chi, \sigma) = \tau'; \sigma'$, it follows that $\text{ret-type}(\mathbf{q}[\tau/\alpha], \chi[\tau/\alpha], \sigma[\tau/\alpha]) = \tau'[\tau/\alpha]; \sigma'[\tau/\alpha]$, which allows us to conclude:

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\omega_1/\beta_1}][\rho_1(\tau)/\alpha]), \rho_2^*(\mathbf{I}_2[\overline{\omega_2/\beta_2}][\rho_2(\tau)/\alpha])) \in \mathcal{E}[\![\mathbf{q}[\tau/\alpha] \vdash \text{ret-type}(\mathbf{q}[\tau/\alpha], \chi[\tau/\alpha], \sigma[\tau/\alpha])]\!]\rho'.$$

□

Lemma 1.34 (Stack Type Application)
If $\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w}_1 \approx_{\text{w}} \mathbf{w}_2 : \mathbf{box}\,\forall[\zeta, \mathbf{\Delta'}].\{\chi; \sigma\}^{\mathbf{q}}$ and $\mathbf{\Delta} \vdash \sigma'$, then

$$\mathbf{\Psi}; \mathbf{\Delta} \vdash \mathbf{w}_1[\sigma'] \approx_{\text{w}} \mathbf{w}_2[\sigma'] : \mathbf{box}\,\forall[\mathbf{\Delta'}].\{\chi[\sigma'/\zeta]; \sigma[\sigma'/\zeta]\}^{\mathbf{q}[\sigma'/\zeta]}.$$

Proof

From the hypotheses, we have $\Psi; \Delta \vdash \mathbf{w_i}[\sigma'] : \mathbf{box}\,\forall[\Delta'].\{\chi[\sigma'/\zeta]; \sigma[\sigma'/\zeta]\}^{\mathbf{q}[\sigma'/\zeta]}$ for $i = 1$, $i = 2$.

Let $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$. We need to show that

$$(W, \rho_1(\mathbf{w_1}[\sigma']), \rho_2(\mathbf{w_2}[\sigma'])) \in \mathcal{W}[\![\mathbf{box}\,\forall[\Delta'].\{\chi[\sigma'/\zeta]; \sigma[\sigma'/\zeta]\}^{\mathbf{q}[\sigma'/\zeta]}]\!]\rho.$$

Let $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$ such that $\widetilde{W} \sqsupset W$. Instantiating the first hypothesis with W and ρ, noting that $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, we have that

$$(W, \rho_1(\mathbf{w_1}), \rho_2(\mathbf{w_2})) \in \mathcal{W}[\![\mathbf{box}\,\forall[\zeta, \Delta'].\{\chi; \sigma\}^{\mathbf{q}}]\!]\rho.$$

Hence, there must be some $\ell_\mathbf{i}$ and $\overline{\omega_\mathbf{i}}$ such that $\rho_\mathbf{i}(\mathbf{w_i}) = \ell_\mathbf{i}[\overline{\omega_\mathbf{i}}]$. Instantiating the above with $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$, noting that $\widetilde{W} \sqsupset W$, we have that $M_i(\ell_\mathbf{i}) = \mathbf{code}[\overline{\beta_\mathbf{i}}, \zeta, \Delta']\{\chi_\mathbf{i}; \sigma_\mathbf{i}\}^{\mathbf{q}_\mathbf{i}}.\mathbf{I_i}$, $\rho_i(\chi) = \chi_\mathbf{i}[\overline{\omega_\mathbf{i}/\beta_\mathbf{i}}]$, $\rho_i(\sigma) = \sigma_\mathbf{i}[\overline{\omega_\mathbf{i}/\beta_\mathbf{i}}]$, $\rho_i(\mathbf{q}) = \mathbf{q_i}[\overline{\omega_\mathbf{i}/\beta_\mathbf{i}}]$, and

$$(\widetilde{W}, (\mathbf{code}[\zeta, \Delta']\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I_1})[\overline{\omega_1/\beta_1}], (\mathbf{code}[\zeta, \Delta']\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I_2})[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \Delta'].\{\chi; \sigma\}^{\mathbf{q}}]\!]\rho. \quad (3)$$

From the above equalities, we can conclude $\rho_i(\chi[\sigma'/\zeta]) = \chi_\mathbf{i}[\overline{\omega_\mathbf{i}/\beta_\mathbf{i}}][\rho_\mathbf{i}(\sigma')/\zeta]$, $\rho_i(\sigma[\sigma'/\zeta]) = \sigma_\mathbf{i}[\overline{\omega_\mathbf{i}/\beta_\mathbf{i}}][\rho_\mathbf{i}(\sigma')/\zeta]$, and $\rho_i(\mathbf{q}[\sigma'/\zeta]) = \mathbf{q_i}[\overline{\omega_\mathbf{i}/\beta_\mathbf{i}}][\rho_\mathbf{i}(\sigma')/\zeta]$.

It remains to show that

$$(\widetilde{W}, (\mathbf{code}[\Delta']\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I_1})[\overline{\omega_1/\beta_1}][\rho_1(\sigma')/\zeta], (\mathbf{code}[\Delta']\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I_2})[\overline{\omega_2/\beta_2}][\rho_2(\sigma')/\zeta]) \in \mathcal{HV}[\![\forall[\Delta'].\{\chi[\sigma'/\zeta]; \sigma[\sigma'/\zeta]\}^{\mathbf{q}[\sigma'/\zeta]}]\!]\rho.$$

Let $W' \sqsupseteq \widetilde{W}$, $\rho^* \in \mathcal{D}[\![\Delta']\!]$, $\rho' = \rho \cup \rho^*$ such that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\sigma'/\zeta]]\!]\rho'$ and $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma[\sigma'/\zeta]]\!]\rho'$. We need to show that

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\sigma')/\zeta]), \rho_2^*(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\sigma')/\zeta])) \in \mathcal{E}[\![\mathbf{q}[\sigma'/\zeta] \vdash \text{ret-type}(\mathbf{q}[\sigma'/\zeta], \chi[\sigma'/\zeta], \sigma[\sigma'/\zeta])]\!]\rho'.$$

Next, we instantiate (6) with W', $\tau'; \sigma'' = \text{ret-type}(\mathbf{q}, \chi, \sigma)$, and $\rho^\dagger = \rho^*[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)]$, noting that $W' \sqsupseteq \widetilde{W}$ and $\rho^\dagger \in \mathcal{D}[\![\zeta, \Delta']\!]$, the latter since $\mathcal{S}[\![\sigma']\!]\rho \in \text{StackRel}[\rho_1(\sigma'), \rho_2(\sigma')]$ by Lemma 1.18. Let $\rho'' = \rho \cup \rho^\dagger$. Note that $\rho'' = \rho'[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)] = \rho'[\zeta \mapsto (\rho_1'(\sigma'), \rho_2'(\sigma'), \mathcal{S}[\![\sigma']\!]\rho')]$. Using Lemma 1.15 we have that $\mathcal{R}[\![\chi[\sigma'/\zeta]]\!]\rho' = \mathcal{R}[\![\chi]\!]\rho''$ and $\mathcal{S}[\![\sigma[\sigma'/\zeta]]\!]\rho' = \mathcal{R}[\![\sigma]\!]\rho''$. Therefore, note that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho''$ and $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho''$. Hence, it follows that

$$(W', \rho_1^\dagger(\mathbf{I_1}[\overline{\omega_1/\beta_1}]), \rho_2^\dagger(\mathbf{I_2}[\overline{\omega_2/\beta_2}])) \in \mathcal{E}[\![\mathbf{q} \vdash \tau'; \sigma'']\!]\rho''.$$

Note that the above is equivalent to

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\sigma')/\zeta]), \rho_2^*(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\sigma')/\zeta])) \in \mathcal{E}[\![\mathbf{q} \vdash \tau'; \sigma'']\!]\rho''.$$

By Lemma 1.15, we have that

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\sigma')/\zeta]), \rho_2^*(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\sigma')/\zeta])) \in \mathcal{E}[\![\mathbf{q}[\sigma'/\zeta] \vdash \tau'[\sigma'/\zeta]; \sigma''[\sigma'/\zeta]]\!]\rho'.$$

Finally, note that by the definition of ret-type, since $\text{ret-type}(\mathbf{q}, \chi, \sigma) = \tau'; \sigma''$, it follows that $\text{ret-type}(\mathbf{q}[\sigma'/\zeta], \chi[\sigma'/\zeta], \sigma[\sigma'/\zeta]) = \tau'[\sigma'/\zeta]; \sigma''[\sigma'/\zeta]$, which allows us to conclude:

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\sigma')/\zeta]), \rho_2^*(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\sigma')/\zeta])) \in \mathcal{E}[\![\mathbf{q}[\sigma'/\zeta] \vdash \text{ret-type}(\mathbf{q}[\sigma'/\zeta], \chi[\sigma'/\zeta], \sigma[\sigma'/\zeta])]\!]\rho'.$$

□

Lemma 1.35 (Return Marker Type Application)
If $\Psi; \Delta \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \mathbf{box}\,\forall[\epsilon, \Delta'].\{\chi; \sigma\}^{\mathbf{q}}$, $\mathrm{ftv}(\mathbf{q}') \subseteq \Delta$, and $\Delta \vdash \forall[\Delta'].\{\chi[\mathbf{q}'/\epsilon]; \sigma[\mathbf{q}'/\epsilon]\}^{\mathbf{q}[\mathbf{q}'/\epsilon]}$, then

$$\Psi; \Delta \vdash \mathbf{w_1}[\mathbf{q}'] \approx_{\mathrm{w}} \mathbf{w_2}[\mathbf{q}'] : \mathbf{box}\,\forall[\Delta'].\{\chi[\mathbf{q}'/\epsilon]; \sigma[\mathbf{q}'/\epsilon]\}^{\mathbf{q}[\mathbf{q}'/\epsilon]}.$$

Proof

From the hypotheses, we have $\Psi; \Delta \vdash \mathbf{w_i}[\mathbf{q}'] : \mathbf{box}\,\forall[\Delta'].\{\chi[\mathbf{q}'/\epsilon]; \sigma[\mathbf{q}'/\epsilon]\}^{\mathbf{q}[\mathbf{q}'/\epsilon]}$ for $i = 1$, $i = 2$.

Let $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$. We need to show that

$$(W, \rho_1(\mathbf{w_1}[\mathbf{q}'])), \rho_2(\mathbf{w_2}[\mathbf{q}'])) \in \mathcal{W}[\![\mathbf{box}\,\forall[\Delta'].\{\chi[\mathbf{q}'/\epsilon]; \sigma[\mathbf{q}'/\epsilon]\}^{\mathbf{q}[\mathbf{q}'/\epsilon]}]\!]\rho.$$

Let $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$ such that $\widetilde{W} \sqsupset W$. Instantiating the first hypothesis with W and ρ, noting that $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, we have that

$$(W, \rho_1(\mathbf{w_1}), \rho_2(\mathbf{w_2})) \in \mathcal{W}[\![\mathbf{box}\,\forall[\epsilon, \Delta'].\{\chi; \sigma\}^{\mathbf{q}}]\!]\rho.$$

Hence, there must be some ℓ_{i} and $\overline{\omega_{\mathrm{i}}}$ such that $\rho_{\mathrm{i}}(\mathbf{w_i}) = \ell_{\mathrm{i}}[\overline{\omega_{\mathrm{i}}}]$. Instantiating the above with $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$, noting that $\widetilde{W} \sqsupset W$, we have that $M_i(\ell_{\mathrm{i}}) = \mathbf{code}[\overline{\beta_{\mathrm{i}}}, \epsilon, \Delta']\{\chi_{\mathrm{i}}; \sigma_{\mathrm{i}}\}^{\mathbf{q_i}}.\mathbf{I_i}$, $\rho_i(\chi) = \chi_{\mathrm{i}}[\overline{\omega_{\mathrm{i}}/\beta_{\mathrm{i}}}]$, $\rho_i(\sigma) = \sigma_{\mathrm{i}}[\overline{\omega_{\mathrm{i}}/\beta_{\mathrm{i}}}]$, $\rho_i(\mathbf{q}) = \mathbf{q_i}[\overline{\omega_{\mathrm{i}}/\beta_{\mathrm{i}}}]$, and

$$(\widetilde{W}, (\mathbf{code}[\epsilon, \Delta']\{\chi_1; \sigma_1\}^{\mathbf{q_1}}.\mathbf{I_1})[\overline{\omega_1/\beta_1}], (\mathbf{code}[\epsilon, \Delta']\{\chi_2; \sigma_2\}^{\mathbf{q_2}}.\mathbf{I_2})[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\epsilon, \Delta'].\{\chi; \sigma\}^{\mathbf{q}}]\!]\rho. \quad (4)$$

From the above equalities, we can conclude $\rho_i(\chi[\mathbf{q}'/\epsilon]) = \chi_{\mathrm{i}}[\overline{\omega_{\mathrm{i}}/\beta_{\mathrm{i}}}][\rho_{\mathrm{i}}(\mathbf{q}')/\epsilon]$, $\rho_i(\sigma[\mathbf{q}'/\epsilon]) = \sigma_{\mathrm{i}}[\overline{\omega_{\mathrm{i}}/\beta_{\mathrm{i}}}][\rho_{\mathrm{i}}(\mathbf{q}')/\epsilon]$, and $\rho_i(\mathbf{q}[\mathbf{q}'/\epsilon]) = \mathbf{q_i}[\overline{\omega_{\mathrm{i}}/\beta_{\mathrm{i}}}][\rho_{\mathrm{i}}(\mathbf{q}')/\epsilon]$.

It remains to show that

$$(\widetilde{W}, (\mathbf{code}[\Delta']\{\chi_1; \sigma_1\}^{\mathbf{q_1}}.\mathbf{I_1})[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon], (\mathbf{code}[\Delta']\{\chi_2; \sigma_2\}^{\mathbf{q_2}}.\mathbf{I_2})[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon]) \in \mathcal{HV}[\![\forall[\Delta'].\{\chi[\mathbf{q}'/\epsilon]; \sigma[\mathbf{q}'/\epsilon]\}^{\mathbf{q}[\mathbf{q}'/\epsilon]}]\!]\rho.$$

Let $W' \sqsupseteq \widetilde{W}$, $\rho^* \in \mathcal{D}[\![\Delta']\!]$, $\rho' = \rho \cup \rho^*$ such that $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\mathbf{q}'/\epsilon]]\!]\rho'$ and $\mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma[\mathbf{q}'/\epsilon]]\!]\rho'$. We need to show that

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon]), \rho_2^*(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon])) \in \mathcal{E}[\![\mathbf{q}[\mathbf{q}'/\epsilon] \vdash \mathrm{ret\text{-}type}(\mathbf{q}[\mathbf{q}'/\epsilon], \chi[\mathbf{q}'/\epsilon], \sigma[\mathbf{q}'/\epsilon])]\!]\rho'.$$

Next, we instantiate (7) with W', $\tau'; \sigma'' = \mathrm{ret\text{-}type}(\mathbf{q}, \chi, \sigma)$, and $\rho^\dagger = \rho^*[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))]$, noting that $W' \sqsupseteq \widetilde{W}$ and $\rho^\dagger \in \mathcal{D}[\![\epsilon, \Delta']\!]$, the latter since the hypothesis specifies $ftv(\mathbf{q}') \subseteq \Delta$ and thus $ftv(\rho_i(\mathbf{q}')) = \emptyset$. Let $\rho'' = \rho \cup \rho^\dagger$. Note that $\rho'' = \rho'[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))] = \rho'[\epsilon \mapsto (\rho_1'(\mathbf{q}'), \rho_2'(\mathbf{q}'))]$. Using Lemma 1.16 we have that $\mathcal{R}[\![\chi[\mathbf{q}'/\epsilon]]\!]\rho' = \mathcal{R}[\![\chi]\!]\rho''$ and $\mathcal{S}[\![\sigma[\mathbf{q}'/\epsilon]]\!]\rho' = \mathcal{R}[\![\sigma]\!]\rho''$. Therefore, note that $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho''$ and $\mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho''$. Hence, it follows that

$$(W', \rho_1^\dagger(\mathbf{I_1}[\overline{\omega_1/\beta_1}]), \rho_2^\dagger(\mathbf{I_2}[\overline{\omega_2/\beta_2}])) \in \mathcal{E}[\![\mathbf{q} \vdash \tau'; \sigma']\!]\rho'', \quad \text{where } \tau'; \sigma' = \mathrm{ret\text{-}type}(\mathbf{q}, \chi, \sigma).$$

Note that the above is equivalent to

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon]), \rho_2^*(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon])) \in \mathcal{E}[\![\mathbf{q} \vdash \tau'; \sigma']\!]\rho''.$$

By Lemma 1.16, we have that

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon]), \rho_2^*(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon])) \in \mathcal{E}[\![\mathbf{q}[\mathbf{q}'/\epsilon] \vdash \tau'[\mathbf{q}'/\epsilon]; \sigma'[\mathbf{q}'/\epsilon]]\!]\rho'.$$

Finally, note that by the definition of ret-type, since $\mathrm{ret\text{-}type}(\mathbf{q}, \chi, \sigma) = \tau'; \sigma'$, it follows that $\mathrm{ret\text{-}type}(\mathbf{q}[\mathbf{q}'/\epsilon], \chi[\mathbf{q}'/\epsilon], \sigma[\mathbf{q}'/\epsilon]) = \tau'[\mathbf{q}'/\epsilon]; \sigma'[\mathbf{q}'/\epsilon]$, which allows us to conclude:

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon]), \rho_2^*(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon])) \in \mathcal{E}[\![\mathbf{q}[\mathbf{q}'/\epsilon] \vdash \mathrm{ret\text{-}type}(\mathbf{q}[\mathbf{q}'/\epsilon], \chi[\mathbf{q}'/\epsilon], \sigma[\mathbf{q}'/\epsilon])]\!]\rho'.$$

□

Lemma 1.36 (Word Value)
If $\Psi; \Delta \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \tau$, then $\Psi; \Delta; \chi \vdash \mathbf{w_1} \approx_{\mathrm{u}} \mathbf{w_2} : \tau$.

Proof

We need to first show that $\Psi; \Delta; \chi \vdash \mathbf{w_1} : \tau$ and $\Psi; \Delta; \chi \vdash \mathbf{w_2} : \tau$.

From the hypothesis, we know that $\Psi; \Delta \vdash \mathbf{w_1} : \tau$ and $\Psi; \Delta \vdash \mathbf{w_1} : \tau$, and the typing rule for small values yields the above.

Next, consider arbitrary $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$ such that $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$. We need to show that $(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{w_1})), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{w_2}))) \in \mathcal{W}[\![\tau]\!]\rho$.

Instantiating the hypothesis with W and ρ, noting that $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, we have that $(W, \rho_1(\mathbf{w_1}), \rho_2(\mathbf{w_2})) \in \mathcal{W}[\![\tau]\!]\rho$. Note that $\mathbf{w_1}$ and $\mathbf{w_2}$ are not registers, which means that $\rho_i(\mathbf{w_i})$ are not registers. Hence, $W.\hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{w_i})) = \rho_i(\mathbf{w_i})$, which means our proof obligation is immediate from $(W, \rho_1(\mathbf{w_1}), \rho_2(\mathbf{w_2})) \in \mathcal{W}[\![\tau]\!]\rho$. □

Lemma 1.37 (Register)
If $\mathbf{r} : \tau \in \chi$, then $\Psi; \Delta; \chi \vdash \mathbf{r} \approx_{\mathrm{u}} \mathbf{r} : \tau$.

Proof

Consider arbitrary $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$ such that $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$.

We know $\rho_i(\mathbf{r}) = \mathbf{r}$, which means we must show

$$(W, W.\hat{\mathbf{R}}_1(\mathbf{r}), \hat{\mathbf{R}}_2(\mathbf{r})) = (W, W.\mathbf{R}_1(\mathbf{r}), \mathbf{R}_2(\mathbf{r})) \in \mathcal{W}[\![\tau]\!]\rho$$

Since $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ and $\mathbf{r} : \tau \in \chi$, the definition of $\mathcal{R}[\![\chi]\!]\rho$ yields the result. □

Lemma 1.38 (Pack)
If $\Psi; \Delta; \chi \vdash \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{u_2} : \tau[\tau'/\alpha]$, then $\Psi; \Delta; \chi \vdash \mathbf{pack}\langle\tau', \mathbf{u_1}\rangle \mathbf{as} \exists\alpha.\tau \approx_{\mathrm{u}} \mathbf{pack}\langle\tau', \mathbf{u_2}\rangle \mathbf{as} \exists\alpha.\tau : \exists\alpha.\tau$.

Proof

We have $\Psi; \Delta; \chi \vdash \mathbf{pack}\langle\tau', \mathbf{u_1}\rangle \mathbf{as} \exists\alpha.\tau : \exists\alpha.\tau$ and $\Psi; \Delta; \chi \vdash \mathbf{pack}\langle\tau', \mathbf{u_2}\rangle \mathbf{as} \exists\alpha.\tau : \exists\alpha.\tau$ by our hypothesis and the typing rules.

Let $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, where $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$. We need to show that

$$(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{pack}\langle\tau', \mathbf{u_1}\rangle \mathbf{as} \exists\alpha.\tau)), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{pack}\langle\tau', \mathbf{u_2}\rangle \mathbf{as} \exists\alpha.\tau))) \in \mathcal{W}[\![\exists\alpha.\tau]\!]\rho$$

which is equivalent to

$$(W, \rho_1(\mathbf{pack}\langle\tau', W.\hat{\mathbf{R}}_1(\mathbf{u_1})\rangle \mathbf{as} \exists\alpha.\tau)), \rho_2(\mathbf{pack}\langle\tau', W.\hat{\mathbf{R}}_2(\mathbf{u_2})\rangle \mathbf{as} \exists\alpha.\tau))) \in \mathcal{W}[\![\exists\alpha.\tau]\!]\rho.$$

By instantiating our hypothesis with W and ρ, we have that $(W, W.\hat{\mathbf{R}}_1(\mathbf{u_1}), W.\hat{\mathbf{R}}_2(\mathbf{u_2})) \in \mathcal{W}[\![\tau[\tau'/\alpha]]\!]\rho$. By Lemma 1.14,

$$\mathcal{W}[\![\tau[\tau'/\alpha]]\!]\rho = \mathcal{W}[\![\tau]\!]\rho[\alpha \mapsto (\rho_1(\tau'), \rho_2(\tau'), \mathcal{W}[\![\tau']\!]\rho)].$$

By Lemma 1.17, $\mathcal{W}[\![\tau']\!]\rho \in \mathrm{WvalRel}[\rho_1(\tau'), \rho_2(\tau')]$. Thus we can complete the proof by supplying $\mathcal{W}[\![\tau']\!]\rho$ as the relation required by $\mathcal{W}[\![\exists\alpha.\tau]\!]\rho$.

□

Lemma 1.39 (Fold)
If $\Psi; \Delta; \chi \vdash \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{u_2} : \tau[\mu\alpha.\tau/\alpha]$, then $\Psi; \Delta; \chi \vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{u_2} : \mu\alpha.\tau$.

Proof

We have $\Psi; \Delta; \chi \vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{u}_1 : \mu\alpha.\tau$ and $\Psi; \Delta; \chi \vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{u}_2 : \mu\alpha.\tau$ by our hypothesis and the typing rules.

Let $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$ where $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$.

We need to show that

$$(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{u}_1)), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{u}_2))) \in \mathcal{W}[\![\mu\alpha.\tau]\!]\rho.$$

This proof goal is equivalent to

$$(W, \mathbf{fold}_{\rho_1(\mu\alpha.\tau)}\ \mathbf{W}.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u}_1)), \mathbf{fold}_{\rho_2(\mu\alpha.\tau)}\ \mathbf{W}.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u}_2))) \in \mathcal{W}[\![\mu\alpha.\tau]\!]\rho.$$

To establish this goal, it is sufficient to establish the following subgoal,

$$(W, W.\hat{\mathbf{R}}_1(\rho_1(u_1)), W.\hat{\mathbf{R}}_2(\rho_2(u_2))) \in \triangleright\mathcal{W}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

Using W and ρ from unrolling our hypothesis, $\Psi; \Delta; \chi \vdash \mathbf{u}_1 \approx_{\mathrm{u}} \mathbf{u}_2 : \tau[\mu\alpha.\tau/\alpha]$ we obtain

$$(W, W.\hat{\mathbf{R}}_1(\rho_1(u_1)), W.\hat{\mathbf{R}}_2(\rho_2(u_2))) \in \mathcal{W}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

We derive the desired subgoal from the above conclusion and lemmas 1.6 and 1.8.

□

Lemma 1.40 (Word Type Application)
If $\Psi; \Delta; \chi \vdash \mathbf{u}_1 \approx_{\mathrm{u}} \mathbf{u}_2 : \mathbf{box}\,\forall[\alpha, \Delta'].\{\chi; \sigma\}^{\mathbf{q}}$ and $\Delta \vdash \tau$, then

$$\Psi; \Delta; \chi \vdash \mathbf{u}_1[\tau] \approx_{\mathrm{u}} \mathbf{u}_2[\tau] : \mathbf{box}\,\forall[\Delta'].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathbf{q}[\tau/\alpha]}.$$

Proof

From the hypotheses, we have $\Psi; \Delta; \chi \vdash \mathbf{u}_i[\tau] : \mathbf{box}\,\forall[\Delta'].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathbf{q}[\tau/\alpha]}$ for $i = 1$, $i = 2$.

Let $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, where $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$.

We need to show that

$$(W, \hat{\mathbf{R}}_1(\rho_1(\mathbf{u}_1[\tau])), \hat{\mathbf{R}}_1(\rho_2(\mathbf{u}_2[\tau]))) \in \mathcal{W}[\![\mathbf{box}\,\forall[\Delta'].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathbf{q}[\tau/\alpha]}]\!]\rho.$$

Let $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$ such that $\widetilde{W} \sqsupset W$. Instantiating the first hypothesis with W and ρ, noting that $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, we have that

$$(W, \hat{\mathbf{R}}_1(\rho_1(\mathbf{u}_1)), \hat{\mathbf{R}}_1(\rho_2(\mathbf{u}_2))) \in \mathcal{W}[\![\mathbf{box}\,\forall[\alpha, \Delta'].\{\chi; \sigma\}^{\mathbf{q}}]\!]\rho.$$

Hence, there must be some ℓ_i and $\overline{\omega_i}$ such that $\hat{\mathbf{R}}_i(\rho_i(\mathbf{u}_i)) = \ell_i[\overline{\omega_i}]$. Instantiating the above with $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$, noting that $\widetilde{W} \sqsupset W$, we have that $M_i(\ell_i) = \mathbf{code}[\overline{\beta_i}, \alpha, \Delta']\{\chi_i; \sigma_i\}^{\mathbf{q}_i}.\mathbf{I}_i$, $\rho_i(\chi) = \chi_i[\overline{\omega_i/\beta_i}]$, $\rho_i(\sigma) = \sigma_i[\overline{\omega_i/\beta_i}]$, $\rho_i(\mathbf{q}) = \mathbf{q}_i[\overline{\omega_i/\beta_i}]$, and

$$(\widetilde{W}, (\mathbf{code}[\alpha, \Delta']\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\omega_1/\beta_1}], (\mathbf{code}[\alpha, \Delta']\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\alpha, \Delta'].\{\chi; \sigma\}^{\mathbf{q}}]\!]\rho. \quad (5)$$

From the above equalities, we can conclude $\rho_i(\chi[\tau/\alpha]) = \chi_i[\overline{\omega_i/\beta_i}][\rho_i(\tau)/\alpha]$, $\rho_i(\sigma[\tau/\alpha]) = \sigma_i[\overline{\omega_i/\beta_i}][\rho_i(\tau)/\alpha]$, and $\rho_i(\mathbf{q}[\tau/\alpha]) = \mathbf{q}_i[\overline{\omega_i/\beta_i}][\rho_i(\tau)/\alpha]$.

It remains to show that

$$(\widetilde{W}, (\mathbf{code}[\Delta']\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\omega_1/\beta_1}][\rho_1(\tau)/\alpha], (\mathbf{code}[\Delta']\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\omega_2/\beta_2}][\rho_2(\tau)/\alpha]) \in \mathcal{HV}[\![\forall[\Delta'].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathbf{q}[\tau/\alpha]}]\!]\rho.$$

Let $W' \sqsupseteq \widetilde{W}$, $\rho^* \in \mathcal{D}[\![\mathbf{\Delta'}]\!]$, $\rho' = \rho \cup \rho^*$ such that currentMR$(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}[\boldsymbol{\tau}/\boldsymbol{\alpha}]]\!]\rho'$ and currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}[\boldsymbol{\tau}/\boldsymbol{\alpha}]]\!]\rho'$. We need to show that

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}][\boldsymbol{\rho_1}(\boldsymbol{\tau})/\boldsymbol{\alpha}]), \rho_2^*(\mathbf{I_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}][\boldsymbol{\rho_2}(\boldsymbol{\tau})/\boldsymbol{\alpha}])) \in \mathcal{E}[\![\mathbf{q}[\boldsymbol{\tau}/\boldsymbol{\alpha}] \vdash \text{ret-type}(\mathbf{q}[\boldsymbol{\tau}/\boldsymbol{\alpha}], \boldsymbol{\chi}[\boldsymbol{\tau}/\boldsymbol{\alpha}], \boldsymbol{\sigma}[\boldsymbol{\tau}/\boldsymbol{\alpha}])]\!]\rho'.$$

Next, we instantiate (5) with W', $\boldsymbol{\tau'}; \boldsymbol{\sigma'} = \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})$ and $\rho^\dagger = \rho^*[\boldsymbol{\alpha} \mapsto (\rho_1(\boldsymbol{\tau}), \rho_2(\boldsymbol{\tau}), \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho)]$, noting that $W' \sqsupseteq \widetilde{W}$ and that $\rho^\dagger \in \mathcal{D}[\![\boldsymbol{\alpha}, \mathbf{\Delta'}]\!]$, the latter since $\mathcal{W}[\![\boldsymbol{\tau}]\!]\rho \in \text{WvalRel}[\rho_1(\boldsymbol{\tau}), \rho_2(\boldsymbol{\tau})]$ by Lemma 1.17. Let $\rho'' = \rho \cup \rho^\dagger$. Note that $\rho'' = \rho'[\boldsymbol{\alpha} \mapsto (\rho_1(\boldsymbol{\tau}), \rho_2(\boldsymbol{\tau}), \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho)] = \rho'[\boldsymbol{\alpha} \mapsto (\rho_1'(\boldsymbol{\tau}), \rho_2'(\boldsymbol{\tau}), \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho')]$. Using Lemma 1.14 we have that $\mathcal{R}[\![\boldsymbol{\chi}[\boldsymbol{\tau}/\boldsymbol{\alpha}]]\!]\rho' = \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho''$ and $\mathcal{S}[\![\boldsymbol{\sigma}[\boldsymbol{\tau}/\boldsymbol{\alpha}]]\!]\rho' = \mathcal{R}[\![\boldsymbol{\sigma}]\!]\rho''$. Therefore, note that currentMR$(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho''$ and currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho''$. Hence, it follows that

$$(W', \rho_1^\dagger(\mathbf{I_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}]), \rho_2^\dagger(\mathbf{I_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}])) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau'}; \boldsymbol{\sigma'}]\!]\rho''.$$

Note that the above is equivalent to

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}][\boldsymbol{\rho_1}(\boldsymbol{\tau})/\boldsymbol{\alpha}]), \rho_2^*(\mathbf{I_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}][\boldsymbol{\rho_2}(\boldsymbol{\tau})/\boldsymbol{\alpha}])) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau'}; \boldsymbol{\sigma'}]\!]\rho''.$$

By Lemma 1.14, we have that

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}][\boldsymbol{\rho_1}(\boldsymbol{\tau})/\boldsymbol{\alpha}]), \rho_2^*(\mathbf{I_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}][\boldsymbol{\rho_2}(\boldsymbol{\tau})/\boldsymbol{\alpha}])) \in \mathcal{E}[\![\mathbf{q}[\boldsymbol{\tau}/\boldsymbol{\alpha}] \vdash \boldsymbol{\tau'}[\boldsymbol{\tau}/\boldsymbol{\alpha}]; \boldsymbol{\sigma'}[\boldsymbol{\tau}/\boldsymbol{\alpha}]]\!]\rho'.$$

Finally, note that by the definition of ret-type, since $\text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma}) = \boldsymbol{\tau'}; \boldsymbol{\sigma'}$, it follows that $\text{ret-type}(\mathbf{q}[\boldsymbol{\tau}/\boldsymbol{\alpha}], \boldsymbol{\chi}[\boldsymbol{\tau}/\boldsymbol{\alpha}], \boldsymbol{\sigma}[\boldsymbol{\tau}/\boldsymbol{\alpha}]) = \boldsymbol{\tau'}[\boldsymbol{\tau}/\boldsymbol{\alpha}]; \boldsymbol{\sigma'}[\boldsymbol{\tau}/\boldsymbol{\alpha}]$, which allows us to conclude:

$$(W', \rho_1^*(\mathbf{I_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}][\boldsymbol{\rho_1}(\boldsymbol{\tau})/\boldsymbol{\alpha}]), \rho_2^*(\mathbf{I_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}][\boldsymbol{\rho_2}(\boldsymbol{\tau})/\boldsymbol{\alpha}])) \in \mathcal{E}[\![\mathbf{q}[\boldsymbol{\tau}/\boldsymbol{\alpha}] \vdash \text{ret-type}(\mathbf{q}[\boldsymbol{\tau}/\boldsymbol{\alpha}], \boldsymbol{\chi}[\boldsymbol{\tau}/\boldsymbol{\alpha}], \boldsymbol{\sigma}[\boldsymbol{\tau}/\boldsymbol{\alpha}])]\!]\rho'.$$

□

Lemma 1.41 (Stack Type Application)
If $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi} \vdash \mathbf{u_1} \approx_{\text{u}} \mathbf{u_2} : \mathbf{box}\,\forall[\boldsymbol{\zeta}, \mathbf{\Delta'}].\{\boldsymbol{\chi}; \boldsymbol{\sigma}\}^{\mathbf{q}}$ and $\mathbf{\Delta} \vdash \boldsymbol{\sigma'}$, then

$$\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi} \vdash \mathbf{u_1}[\boldsymbol{\sigma'}] \approx_{\text{u}} \mathbf{u_2}[\boldsymbol{\sigma'}] : \mathbf{box}\,\forall[\mathbf{\Delta'}].\{\boldsymbol{\chi}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]; \boldsymbol{\sigma}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]\}^{\mathbf{q}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]}.$$

Proof

From the hypotheses, we have $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi} \vdash \mathbf{u_i}[\boldsymbol{\sigma'}] : \mathbf{box}\,\forall[\mathbf{\Delta'}].\{\boldsymbol{\chi}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]; \boldsymbol{\sigma}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]\}^{\mathbf{q}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]}$ for $i = 1$, $i = 2$.
Let $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, where currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$.
We need to show that

$$(W, \hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1}[\boldsymbol{\sigma'}])), \hat{\mathbf{R}}_2(\rho_2(\mathbf{u_2}[\boldsymbol{\sigma'}]))) \in \mathcal{W}[\![\mathbf{box}\,\forall[\mathbf{\Delta'}].\{\boldsymbol{\chi}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]; \boldsymbol{\sigma}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]\}^{\mathbf{q}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]}]\!]\rho.$$

Let $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$ such that $\widetilde{W} \sqsupset W$. Instantiating the first hypothesis with W and ρ, noting that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, we have that

$$(W, \hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1})), \hat{\mathbf{R}}_1(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\mathbf{box}\,\forall[\boldsymbol{\zeta}, \mathbf{\Delta'}].\{\boldsymbol{\chi}; \boldsymbol{\sigma}\}^{\mathbf{q}}]\!]\rho.$$

Hence, there must be some $\boldsymbol{\ell_i}$ and $\overline{\boldsymbol{\omega_i}}$ such that $\hat{\mathbf{R}}_1(\rho_i(\mathbf{u_i})) = \boldsymbol{\ell_i}[\overline{\boldsymbol{\omega_i}}]$. Instantiating the above with $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$, noting that $\widetilde{W} \sqsupset W$, we have that $M_i(\boldsymbol{\ell_i}) = \mathbf{code}[\overline{\boldsymbol{\beta_i}}, \boldsymbol{\zeta}, \mathbf{\Delta'}]\{\boldsymbol{\chi_i}; \boldsymbol{\sigma_i}\}^{\mathbf{q_i}}.\mathbf{I_i}$, $\rho_i(\boldsymbol{\chi}) = \boldsymbol{\chi_i}[\overline{\boldsymbol{\omega_i}/\boldsymbol{\beta_i}}]$, $\rho_i(\boldsymbol{\sigma}) = \boldsymbol{\sigma_i}[\overline{\boldsymbol{\omega_i}/\boldsymbol{\beta_i}}]$, $\rho_i(\mathbf{q}) = \mathbf{q_i}[\overline{\boldsymbol{\omega_i}/\boldsymbol{\beta_i}}]$, and

$$(\widetilde{W}, (\mathbf{code}[\boldsymbol{\zeta}, \mathbf{\Delta'}]\{\boldsymbol{\chi_1}; \boldsymbol{\sigma_1}\}^{\mathbf{q_1}}.\mathbf{I_1})[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}], (\mathbf{code}[\boldsymbol{\zeta}, \mathbf{\Delta'}]\{\boldsymbol{\chi_2}; \boldsymbol{\sigma_2}\}^{\mathbf{q_2}}.\mathbf{I_2})[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}]) \in \mathcal{HV}[\![\forall[\boldsymbol{\zeta}, \mathbf{\Delta'}].\{\boldsymbol{\chi}; \boldsymbol{\sigma}\}^{\mathbf{q}}]\!]\rho. \quad (6)$$

From the above equalities, we can conclude $\rho_i(\boldsymbol{\chi}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]) = \boldsymbol{\chi_i}[\overline{\boldsymbol{\omega_i}/\boldsymbol{\beta_i}}][\boldsymbol{\rho_i}(\boldsymbol{\sigma'})/\boldsymbol{\zeta}]$, $\rho_i(\boldsymbol{\sigma}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]) = \boldsymbol{\sigma_i}[\overline{\boldsymbol{\omega_i}/\boldsymbol{\beta_i}}][\boldsymbol{\rho_i}(\boldsymbol{\sigma'})/\boldsymbol{\zeta}]$, and $\rho_i(\mathbf{q}[\boldsymbol{\sigma'}/\boldsymbol{\zeta}]) = \mathbf{q_i}[\overline{\boldsymbol{\omega_i}/\boldsymbol{\beta_i}}][\boldsymbol{\rho_i}(\boldsymbol{\sigma'})/\boldsymbol{\zeta}]$.

It remains to show that

$$(\widetilde{W}, (\mathbf{code}[\boldsymbol{\Delta}']\{\boldsymbol{\chi}_1;\boldsymbol{\sigma}_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\boldsymbol{\omega}_1/\boldsymbol{\beta}_1}][\rho_1(\boldsymbol{\sigma}')/\boldsymbol{\zeta}], (\mathbf{code}[\boldsymbol{\Delta}']\{\boldsymbol{\chi}_2;\boldsymbol{\sigma}_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\boldsymbol{\omega}_2/\boldsymbol{\beta}_2}][\rho_2(\boldsymbol{\sigma}')/\boldsymbol{\zeta}]) \in \mathcal{HV}[\![\forall[\boldsymbol{\Delta}'].\{\boldsymbol{\chi}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}];\boldsymbol{\sigma}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]\}^{\mathbf{q}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]}]\!]\rho.$$

Let $W' \sqsupseteq \widetilde{W}$, $\rho^* \in \mathcal{D}[\![\boldsymbol{\Delta}']\!]$, $\rho' = \rho \cup \rho^*$ such that $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]]\!]\rho'$ and $\mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]]\!]\rho'$. We need to show that

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\boldsymbol{\omega}_1/\boldsymbol{\beta}_1}][\rho_1(\boldsymbol{\sigma}')/\boldsymbol{\zeta}]), \rho_2^*(\mathbf{I}_2[\overline{\boldsymbol{\omega}_2/\boldsymbol{\beta}_2}][\rho_2(\boldsymbol{\sigma}')/\boldsymbol{\zeta}])) \in \mathcal{E}[\![\mathbf{q}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}] \vdash \text{ret-type}(\mathbf{q}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}], \boldsymbol{\chi}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}], \boldsymbol{\sigma}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}])]\!]\rho'.$$

Next, we instantiate (6) with W', $\boldsymbol{\tau}';\boldsymbol{\sigma}'' = \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})$, and $\rho^\dagger = \rho^*[\boldsymbol{\zeta} \mapsto (\rho_1(\boldsymbol{\sigma}'), \rho_2(\boldsymbol{\sigma}'), \mathcal{S}[\![\boldsymbol{\sigma}']\!]\rho)]$, noting that $W' \sqsupseteq \widetilde{W}$ and $\rho^\dagger \in \mathcal{D}[\![\boldsymbol{\zeta}, \boldsymbol{\Delta}']\!]$, the latter since $\mathcal{S}[\![\boldsymbol{\sigma}']\!]\rho \in \mathrm{StackRel}[\rho_1(\boldsymbol{\sigma}'), \rho_2(\boldsymbol{\sigma}')]$ by Lemma 1.18. Let $\rho'' = \rho \cup \rho^\dagger$. Note that $\rho'' = \rho'[\boldsymbol{\zeta} \mapsto (\rho_1(\boldsymbol{\sigma}'), \rho_2(\boldsymbol{\sigma}'), \mathcal{S}[\![\boldsymbol{\sigma}']\!]\rho)] = \rho'[\boldsymbol{\zeta} \mapsto (\rho'_1(\boldsymbol{\sigma}'), \rho'_2(\boldsymbol{\sigma}'), \mathcal{S}[\![\boldsymbol{\sigma}']\!]\rho')]$. Using Lemma 1.15 we have that $\mathcal{R}[\![\boldsymbol{\chi}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]]\!]\rho' = \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho''$ and $\mathcal{S}[\![\boldsymbol{\sigma}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]]\!]\rho' = \mathcal{R}[\![\boldsymbol{\sigma}]\!]\rho''$. Therefore, note that $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho''$ and $\mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho''$. Hence, it follows that

$$(W', \rho_1^\dagger(\mathbf{I}_1[\overline{\boldsymbol{\omega}_1/\boldsymbol{\beta}_1}]), \rho_2^\dagger(\mathbf{I}_2[\overline{\boldsymbol{\omega}_2/\boldsymbol{\beta}_2}])) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}';\boldsymbol{\sigma}'']\!]\rho'', \quad \text{where } \boldsymbol{\tau}';\boldsymbol{\sigma}'' = \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma}).$$

Note that the above is equivalent to

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\boldsymbol{\omega}_1/\boldsymbol{\beta}_1}][\rho_1(\boldsymbol{\sigma}')/\boldsymbol{\zeta}]), \rho_2^*(\mathbf{I}_2[\overline{\boldsymbol{\omega}_2/\boldsymbol{\beta}_2}][\rho_2(\boldsymbol{\sigma}')/\boldsymbol{\zeta}])) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}';\boldsymbol{\sigma}'']\!]\rho''.$$

By Lemma 1.15, we have that

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\boldsymbol{\omega}_1/\boldsymbol{\beta}_1}][\rho_1(\boldsymbol{\sigma}')/\boldsymbol{\zeta}]), \rho_2^*(\mathbf{I}_2[\overline{\boldsymbol{\omega}_2/\boldsymbol{\beta}_2}][\rho_2(\boldsymbol{\sigma}')/\boldsymbol{\zeta}])) \in \mathcal{E}[\![\mathbf{q}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}] \vdash \boldsymbol{\tau}'[\boldsymbol{\sigma}'/\boldsymbol{\zeta}];\boldsymbol{\sigma}''[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]]\!]\rho'.$$

Finally, note that by the definition of ret-type, since $\text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma}) = \boldsymbol{\tau}';\boldsymbol{\sigma}''$, it follows that $\text{ret-type}(\mathbf{q}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}], \boldsymbol{\chi}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}], \boldsymbol{\sigma}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]) = \boldsymbol{\tau}'[\boldsymbol{\sigma}'/\boldsymbol{\zeta}];\boldsymbol{\sigma}''[\boldsymbol{\sigma}'/\boldsymbol{\zeta}]$, which allows us to conclude:

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\boldsymbol{\omega}_1/\boldsymbol{\beta}_1}][\rho_1(\boldsymbol{\sigma}')/\boldsymbol{\zeta}]), \rho_2^*(\mathbf{I}_2[\overline{\boldsymbol{\omega}_2/\boldsymbol{\beta}_2}][\rho_2(\boldsymbol{\sigma}')/\boldsymbol{\zeta}])) \in \mathcal{E}[\![\mathbf{q}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}] \vdash \text{ret-type}(\mathbf{q}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}], \boldsymbol{\chi}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}], \boldsymbol{\sigma}[\boldsymbol{\sigma}'/\boldsymbol{\zeta}])]\!]\rho'.$$

□

Lemma 1.42 (Return Marker Type Application)
If $\boldsymbol{\Psi};\boldsymbol{\Delta};\boldsymbol{\chi} \vdash \mathbf{u}_1 \approx_{\mathrm{u}} \mathbf{u}_2 : \mathbf{box}\,\forall[\boldsymbol{\epsilon}, \boldsymbol{\Delta}'].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^{\mathbf{q}}$, $\mathrm{ftv}(\mathbf{q}') \subseteq \boldsymbol{\Delta}$, and $\boldsymbol{\Delta} \vdash \forall[\boldsymbol{\Delta}'].\{\boldsymbol{\chi}[\mathbf{q}'/\boldsymbol{\epsilon}];\boldsymbol{\sigma}[\mathbf{q}'/\boldsymbol{\epsilon}]\}^{\mathbf{q}[\mathbf{q}'/\boldsymbol{\epsilon}]}$, then

$$\boldsymbol{\Psi};\boldsymbol{\Delta};\boldsymbol{\chi} \vdash \mathbf{u}_1[\mathbf{q}'] \approx_{\mathrm{u}} \mathbf{u}_2[\mathbf{q}'] : \mathbf{box}\,\forall[\boldsymbol{\Delta}'].\{\boldsymbol{\chi}[\mathbf{q}'/\boldsymbol{\epsilon}];\boldsymbol{\sigma}[\mathbf{q}'/\boldsymbol{\epsilon}]\}^{\mathbf{q}[\mathbf{q}'/\boldsymbol{\epsilon}]}.$$

Proof

From the hypotheses, we have $\boldsymbol{\Psi};\boldsymbol{\Delta};\boldsymbol{\chi} \vdash \mathbf{u}_i[\mathbf{q}'] : \mathbf{box}\,\forall[\boldsymbol{\Delta}'].\{\boldsymbol{\chi}[\mathbf{q}'/\boldsymbol{\epsilon}];\boldsymbol{\sigma}[\mathbf{q}'/\boldsymbol{\epsilon}]\}^{\mathbf{q}[\mathbf{q}'/\boldsymbol{\epsilon}]}$ for $i = 1$, $i = 2$.
Let $W \in \mathcal{H}[\![\boldsymbol{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\boldsymbol{\Delta}]\!]$, where $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$.
We need to show that

$$(W, \hat{\mathbf{R}}_1(\rho_1(\mathbf{u}_1[\mathbf{q}'])), \hat{\mathbf{R}}_1(\rho_2(\mathbf{u}_2[\mathbf{q}']))) \in \mathcal{W}[\![\mathbf{box}\,\forall[\boldsymbol{\Delta}'].\{\boldsymbol{\chi}[\mathbf{q}'/\boldsymbol{\epsilon}];\boldsymbol{\sigma}[\mathbf{q}'/\boldsymbol{\epsilon}]\}^{\mathbf{q}[\mathbf{q}'/\boldsymbol{\epsilon}]}]\!]\rho.$$

Let $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$ such that $\widetilde{W} \sqsupset W$. Instantiating the first hypothesis with W and ρ, noting that $W \in \mathcal{H}[\![\boldsymbol{\Psi}]\!]$ and $\rho \in \mathcal{D}[\![\boldsymbol{\Delta}]\!]$, we have that

$$(W, \hat{\mathbf{R}}_1(\rho_1(\mathbf{u}_1)), \hat{\mathbf{R}}_1(\rho_2(\mathbf{u}_2))) \in \mathcal{W}[\![\mathbf{box}\,\forall[\boldsymbol{\epsilon}, \boldsymbol{\Delta}'].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^{\mathbf{q}}]\!]\rho.$$

Hence, there must be some $\boldsymbol{\ell}_i$ and $\overline{\boldsymbol{\omega}_i}$ such that $\hat{\mathbf{R}}_1(\rho_i(\mathbf{u}_i)) = \boldsymbol{\ell}_i[\overline{\boldsymbol{\omega}_i}]$. Instantiating the above with $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$, noting that $\widetilde{W} \sqsupset W$, we have that $M_i(\boldsymbol{\ell}_i) = \mathbf{code}[\overline{\boldsymbol{\beta}_i}, \boldsymbol{\epsilon}, \boldsymbol{\Delta}']\{\boldsymbol{\chi}_i;\boldsymbol{\sigma}_i\}^{\mathbf{q}_i}.\mathbf{I}_i$, $\rho_i(\boldsymbol{\chi}) = \boldsymbol{\chi}_i[\overline{\boldsymbol{\omega}_i/\boldsymbol{\beta}_i}]$, $\rho_i(\boldsymbol{\sigma}) = \boldsymbol{\sigma}_i[\overline{\boldsymbol{\omega}_i/\boldsymbol{\beta}_i}]$, $\rho_i(\mathbf{q}) = \mathbf{q}_i[\overline{\boldsymbol{\omega}_i/\boldsymbol{\beta}_i}]$, and

$$(\widetilde{W}, (\mathbf{code}[\boldsymbol{\epsilon}, \boldsymbol{\Delta}']\{\boldsymbol{\chi}_1;\boldsymbol{\sigma}_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\boldsymbol{\omega}_1/\boldsymbol{\beta}_1}], (\mathbf{code}[\boldsymbol{\epsilon}, \boldsymbol{\Delta}']\{\boldsymbol{\chi}_2;\boldsymbol{\sigma}_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\boldsymbol{\omega}_2/\boldsymbol{\beta}_2}]) \in \mathcal{HV}[\![\forall[\boldsymbol{\epsilon}, \boldsymbol{\Delta}'].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^{\mathbf{q}}]\!]\rho. \quad (7)$$

From the above equalities, we can conclude $\rho_i(\chi[\mathbf{q}'/\epsilon]) = \chi_i[\overline{\omega_i/\beta_i}][\rho_i(\mathbf{q}')/\epsilon]$, $\rho_i(\sigma[\mathbf{q}'/\epsilon]) = \sigma_i[\overline{\omega_i/\beta_i}][\rho_i(\mathbf{q}')/\epsilon]$, and $\rho_i(\mathbf{q}[\mathbf{q}'/\epsilon]) = \mathbf{q}_i[\overline{\omega_i/\beta_i}][\rho_i(\mathbf{q}')/\epsilon]$.

It remains to show that

$$(\widetilde{W}, (\mathbf{code}[\Delta']\{\chi_1;\sigma_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon], (\mathbf{code}[\Delta']\{\chi_2;\sigma_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon]) \in \mathcal{HV}[\![\forall[\Delta'].\{\chi[\mathbf{q}'/\epsilon];\sigma[\mathbf{q}'/\epsilon]\}^{\mathbf{q}[\mathbf{q}'/\epsilon]}]\!]\rho.$$

Let $W' \sqsupseteq \widetilde{W}$, $\rho^* \in \mathcal{D}[\![\Delta']\!]$, $\rho' = \rho \cup \rho^*$ such that currentMR$(W'(i_{\text{reg}})) \in_{W'} \mathcal{R}[\![\chi[\mathbf{q}'/\epsilon]]\!]\rho'$ and currentMR$(W'(i_{\text{stk}})) \in_{W'} \mathcal{S}[\![\sigma[\mathbf{q}'/\epsilon]]\!]\rho'$. We need to show that

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon]), \rho_2^*(\mathbf{I}_2[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon])) \in \mathcal{E}[\![\mathbf{q}[\mathbf{q}'/\epsilon] \vdash \text{ret-type}(\mathbf{q}[\mathbf{q}'/\epsilon], \chi[\mathbf{q}'/\epsilon], \sigma[\mathbf{q}'/\epsilon])]\!]\rho'.$$

Next, we instantiate (7) with W', $\tau';\sigma' = \text{ret-type}(\mathbf{q}, \chi, \sigma)$, and $\rho^\dagger = \rho^*[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))]$, noting that $W' \sqsupseteq \widetilde{W}$ and $\rho^\dagger \in \mathcal{D}[\![\epsilon, \Delta']\!]$, the latter since the hypothesis specifies $ftv(\mathbf{q}') \subseteq \Delta$ and thus $ftv(\rho_i(\mathbf{q}')) = \emptyset$. Let $\rho'' = \rho \cup \rho^\dagger$. Note that $\rho'' = \rho'[\epsilon \mapsto (\rho_1(\mathbf{q}'), \rho_2(\mathbf{q}'))] = \rho'[\epsilon \mapsto (\rho_1'(\mathbf{q}'), \rho_2'(\mathbf{q}'))]$. Using Lemma 1.16 we have that $\mathcal{R}[\![\chi[\mathbf{q}'/\epsilon]]\!]\rho' = \mathcal{R}[\![\chi]\!]\rho''$ and $\mathcal{S}[\![\sigma[\mathbf{q}'/\epsilon]]\!]\rho' = \mathcal{R}[\![\sigma]\!]\rho''$. Therefore, note that currentMR$(W'(i_{\text{reg}})) \in_{W'} \mathcal{R}[\![\chi]\!]\rho''$ and currentMR$(W'(i_{\text{stk}})) \in_{W'} \mathcal{S}[\![\sigma]\!]\rho''$. Hence, it follows that

$$(W', \rho_1^\dagger(\mathbf{I}_1[\overline{\omega_1/\beta_1}]), \rho_2^\dagger(\mathbf{I}_2[\overline{\omega_2/\beta_2}])) \in \mathcal{E}[\![\mathbf{q} \vdash \tau';\sigma']\!]\rho'', \quad \text{where } \tau';\sigma' = \text{ret-type}(\mathbf{q}, \chi, \sigma).$$

Note that the above is equivalent to

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon]), \rho_2^*(\mathbf{I}_2[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon])) \in \mathcal{E}[\![\mathbf{q} \vdash \tau';\sigma']\!]\rho''.$$

By Lemma 1.16, we have that

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon]), \rho_2^*(\mathbf{I}_2[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon])) \in \mathcal{E}[\![\mathbf{q}[\mathbf{q}'/\epsilon] \vdash \tau'[\mathbf{q}'/\epsilon];\sigma'[\mathbf{q}'/\epsilon]]\!]\rho'.$$

Finally, note that by the definition of ret-type, since ret-type$(\mathbf{q}, \chi, \sigma) = \tau';\sigma'$, it follows that ret-type$(\mathbf{q}[\mathbf{q}'/\epsilon], \chi[\mathbf{q}'/\epsilon], \sigma[\mathbf{q}'/\epsilon]) = \tau'[\mathbf{q}'/\epsilon];\sigma'[\mathbf{q}'/\epsilon]$, which allows us to conclude:

$$(W', \rho_1^*(\mathbf{I}_1[\overline{\omega_1/\beta_1}][\rho_1(\mathbf{q}')/\epsilon]), \rho_2^*(\mathbf{I}_2[\overline{\omega_2/\beta_2}][\rho_2(\mathbf{q}')/\epsilon])) \in \mathcal{E}[\![\mathbf{q}[\mathbf{q}'/\epsilon] \vdash \text{ret-type}(\mathbf{q}[\mathbf{q}'/\epsilon], \chi[\mathbf{q}'/\epsilon], \sigma[\mathbf{q}'/\epsilon])]\!]\rho'.$$

□

Lemma 1.43 (Arithmetic Operation)
If $\Psi;\Delta;\chi \vdash \mathbf{r}_{s1} \approx_u \mathbf{r}_{s2} : \mathbf{int}$, $\Psi;\Delta;\chi \vdash \mathbf{u}_1 \approx_u \mathbf{u}_2 : \mathbf{int}$, $\mathbf{q} \neq \mathbf{r}_d$, and $\Psi;\Delta;\chi[\mathbf{r}_d : \mathbf{int}];\sigma;\mathbf{q} \vdash \mathbf{I}_1 \approx_I \mathbf{I}_2$, then $\Psi;\Delta;\chi;\sigma;\mathbf{q} \vdash \mathbf{aop}\ \mathbf{r}_d, \mathbf{r}_{s1}, \mathbf{u}_1; \mathbf{I}_1 \approx_I \mathbf{aop}\ \mathbf{r}_d, \mathbf{r}_{s2}, \mathbf{u}_2; \mathbf{I}_2$.

Proof

Inspecting $\approx_I$, we see that $\Psi;\Delta;\chi;\sigma;\mathbf{q} \vdash \mathbf{aop}\ \mathbf{r}_d, \mathbf{r}_{si}, \mathbf{u}_i; \mathbf{I}_i$ for $i \in \{1, 2\}$.

Now choose arbitrary $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$ such that currentMR$(W(i_{\text{reg}})) \in_W \mathcal{R}[\![\chi]\!]\rho$ and currentMR$(W(i_{\text{stk}})) \in_W \mathcal{S}[\![\sigma]\!]\rho$.

We need to show $(W, \rho_1((\mathbf{aop}\ \mathbf{r}_d, \mathbf{r}_{s1}, \mathbf{u}_1; \mathbf{I}_1, \cdot)), \rho_2((\mathbf{aop}\ \mathbf{r}_d, \mathbf{r}_{s2}, \mathbf{u}_2; \mathbf{I}_2, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho$,

Noting that $\mathbf{u}_i$ is either an integer or a register pointing to one, we can push the substitution in to yield the following obligation:

$$(W, (\mathbf{aop}\ \mathbf{r}_d, \mathbf{r}_{s1}, \mathbf{u}_1; \rho_1(\mathbf{I}_1), \cdot)), (\mathbf{aop}\ \mathbf{r}_d, \mathbf{r}_{s2}, \mathbf{u}_2; \rho_2(\mathbf{I}_2), \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E}_i$ and memories M_i, we can immediately show that running$(0, \langle M_i \mid E_i[e_i] \rangle)$.

In the following, assume $W.k > 0$ and let $\tau_r;\sigma_r = \text{ret-type}(\mathbf{q}, \chi, \sigma)$.

We will prove this by appealing to Lemma 1.11 with an empty heap fragment. In order to do this, we show the following:

- First, we must show that the above triple is in $\text{TermAtom}[\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})]\rho$.
  Since W is drawn from $\mathcal{H}[\![\boldsymbol{\Psi}]\!]\rho$, we know it is in World, which means what we have left to show is that:
  $$W.\Psi_1; \cdot; W.\boldsymbol{\chi_1}; W.\boldsymbol{\sigma_1}; \rho_1(\mathbf{q}) \vdash \rho_1(e_1) : \rho_1(\text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})) \text{ and}$$
  $$W.\Psi_2; \cdot; W.\boldsymbol{\chi_2}; W.\boldsymbol{\sigma_2}; \rho_2(\mathbf{q}) \vdash \rho_2(e_1) : \rho_2(\text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma}))$$
  where $\rho_1(e_1)$ and $\rho_2(e_2)$ are the two components under consideration.
  From the typing judgement for components, we see that we need to show that $W.\Psi_1; \cdot; W.\boldsymbol{\chi_1}; W.\boldsymbol{\sigma_1}; \rho_1(\mathbf{q}) \vdash \mathbf{aop\ r_d, r_{s1}, u_1;}\ \rho_1(\mathbf{I_1})$ and similarly for the second case.
  From the hypothesis, we know $\boldsymbol{\Psi}; \cdot; \boldsymbol{\chi}; \boldsymbol{\sigma}; \rho_1(\mathbf{q}) \vdash \mathbf{aop\ r_d, r_{s1}, u_1;}\ \boldsymbol{\rho_1(I_1)}$. From the fact that $W \in \mathcal{H}[\![\boldsymbol{\Psi}]\!]$, we know that $W.\Psi_1$ is a superset of $\boldsymbol{\Psi}$, and similarly from $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$ we know that $W.\mathbf{R_1}$ contains well typed bindings for everything in $\boldsymbol{\chi}$, and since W is a world, this means $W.\boldsymbol{\chi_1}$ is a superset of $\boldsymbol{\chi}$. Similarly, from $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ we know that $W.\boldsymbol{\sigma_1}$ is a superset of $\boldsymbol{\sigma}$, and combining all of these, via weakening, we get what we need.
- Next, we must choose a W', where $W' \sqsupseteq_{\text{pub}} W$ and $W.k \leq W'.k + k_1$, $W.k + k_2$, where k_1 and k_2 will be determined later.
  Let $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \delta(\mathbf{aop}, W.\mathbf{R_1}(\mathbf{r_{s1}}), W.\hat{\mathbf{R}}_\mathbf{1}(\mathbf{u_1}))], W.\boldsymbol{\chi_1}[\mathbf{r_d : int}],$
  $W.\mathbf{R_2}[\mathbf{r_d} \mapsto \delta(aop, W.\mathbf{R_2}(r_{s2}), W.\hat{\mathbf{R}}_\mathbf{2}(\mathbf{u_2}))], W.\boldsymbol{\chi_2}[r_d : int])$ and
  $W' = (W.k, W.\boldsymbol{\Psi_1}, W.\boldsymbol{\Psi_2}, W.\Theta[i_{\text{reg}} \mapsto \text{Island}_{\text{reg}}(s, W.k)])$.
  Since $s.\mathbf{R_i} : s.\boldsymbol{\chi_i}$, $W' \in World$ and the rest is unchanged, $W' \sqsupseteq_{\text{pub}} W$.
- Further, we must show that the return address (if it is not $\mathbf{end}\{\boldsymbol{\tau}; \boldsymbol{\sigma}\}$) is unchanged in W'. Since $\mathbf{q}$ is the same, the only way that it could have changed would be if it were a memory location that changed, but the only change to memory is $\mathbf{r_d}$ and from the hypothesis $\mathbf{q} \neq \mathbf{r_d}$.
- Finally, consider arbitrary $M_1, M_2 : W$, where $(H_i, R_i, S_i) = M_i$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{ \text{currentMR}(\theta) \mid \theta \in W.\Theta \}$. From the latter, we have the following fact for island i_{reg}: $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$.
  The reduction relation tells us that
  $\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid \mathbf{aop\ r_d, r_{si}, u_i;}\ \rho_i(\mathbf{I_i}) \rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \boldsymbol{\delta}(\mathbf{aop}, \mathbf{R_i}(\mathbf{r_{si}}), \hat{\mathbf{R}}_\mathbf{i}(\mathbf{u_i}))], \mathbf{S_i}) \mid \rho_i(\mathbf{I_i}) \rangle$
  Let $M_i' = (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \boldsymbol{\delta}(\mathbf{aop}, \mathbf{R_i}(\mathbf{r_{si}}), \hat{\mathbf{R}}_\mathbf{i}(\mathbf{u_i}))], \mathbf{S_i})$. Based on the definition of W', we can see that $(M_1', M_2') : W'$. Note that $k_1 = k_2 = 1$, and thus $W.k \leq W'.k + k_i$.
  We now instantiate the hypothesis with W' and ρ. By Lemma 1.9, W' is in $\mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$. From Lemma 1.21, since $W(i_{stk}) = W'(i_{stk})$, $\text{currentMR}(W'(i_{stk})) \Subset_W \mathcal{W}[\![\mathbf{sigma}]\!]\rho$.
  Using Lemma 1.20, we claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi[r_d : int]\!]\rho$. In order to show this, we need that $(W', \delta(aop, R_1(r_{s1}), \hat{R}_1(u_1)), \delta(aop, R_2(r_{s2}), \hat{R}_1(u_2))) \in \mathcal{W}[\![int]\!]\rho$.
  Note that from the first two hypothesis, $(W, W.\hat{R}_1(u_1), W.\hat{R}_2(u_2)) \in \mathcal{W}[\![int]\!]\rho$, which means $W.\hat{R}_i(u_i)$ is an integer, and similarly for $W.R_i(r_{si})$. This means that $\delta(aop, W.R_i(r_{si}), W.\hat{R}_i(u_i))$ is also an integer, and thus we can conclude:
  $$(W, \delta(aop, W.R_1(r_{s1}), W.\hat{R}_1(u_1)), \delta(aop, W.R_2(r_{s2}), W.\hat{R}_2(u_2))) \in \mathcal{W}[\![\mathbf{int}]\!]\rho$$
  By monotonicity, it follows that:
  $$(W', \delta(aop, W'.R_1(r_{s1}), W'.\hat{R}_1(u_1)), \delta(aop, W'.R_2(r_{s2}), W'.\hat{R}_2(u_2))) \in \mathcal{W}[\![\mathbf{int}]\!]\rho,$$
  With that, we can conclude that $(W', \rho_1((I_1, \cdot)), \rho_2((I_2, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}[\mathbf{r_d : int}], \boldsymbol{\sigma})]\!]\rho$. Since we know that $r_d \neq q$, $\text{ret-type}(\mathbf{q}, \boldsymbol{\chi}[\mathbf{r_d : int}], \boldsymbol{\sigma}) = \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})$ and thus we can use Lemma 1.11 to get the result.

□

Lemma 1.44 (Branch)
If $\Psi;\Delta;\chi \vdash \mathbf{r_1} \approx_u \mathbf{r_2} : \mathbf{int}$, $\Psi;\Delta;\chi \vdash \mathbf{u_1} \approx_u \mathbf{u_2} : \mathbf{box}\,\forall[].\{\chi';\sigma\}^{\mathbf{q}}$, $\Delta \vdash \chi \leq \chi'$, and $\Psi;\Delta;\chi;\sigma;\mathbf{q} \vdash \mathbf{I_1} \approx_I \mathbf{I_2}$, then $\Psi;\Delta;\chi;\sigma;\mathbf{q} \vdash \mathtt{bnz}\,\mathbf{r_1},\mathbf{u_1};\mathbf{I_1} \approx_I \mathtt{bnz}\,\mathbf{r_2},\mathbf{u_2};\mathbf{I_2}$.

Proof

Clearly, $\Psi;\Delta;\chi;\sigma;\mathbf{q} \vdash \mathtt{bnz}\,\mathbf{r_1},\mathbf{u_1};\mathbf{I_1}$ and $\Psi;\Delta;\chi;\sigma;\mathbf{q} \vdash \mathtt{bnz}\,\mathbf{r_1},\mathbf{u_1};\mathbf{I_2}$ follow from the premises.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$(W, \rho_1((\mathtt{bnz}\,\mathbf{r_1},\mathbf{u_1};\mathbf{I_1},\cdot)), \rho_2((\mathtt{bnz}\,\mathbf{r_2},\mathbf{u_2};\mathbf{I_2},\cdot))) = W, (\mathtt{bnz}\,\mathbf{r_1},\rho_1(\mathbf{u_1});\mathbf{I_1},\cdot), (\mathtt{bnz}\,\mathbf{r_2},\rho_2(\mathbf{u_2});\mathbf{I_2},\cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-typ}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that running$(0, \langle M_i \mid E_i[e_i]\rangle)$.

In the following, assume $W.k > 0$ and let $\tau_r;\sigma_r = \text{ret-type}(\mathbf{q},\chi,\sigma)$. From our first hypothesis, $\Psi;\Delta;\chi \vdash \mathbf{r_1} \approx_u \mathbf{r_2} : \mathbf{int}$. Thus $W.R_1(r_1) = W.R_2(r_2)$. We proceed by cases on $W.R_1(r_1)$

- $W.R_1(r_1) = 0$
  We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.
  - $(W, (\mathtt{bnz}\,\mathbf{r_1},\rho_1(\mathbf{u_1});\rho_1(\mathbf{I_1}),\cdot), (\mathtt{bnz}\,\mathbf{r_2},\rho_2(\mathbf{u_2});\rho_2(\mathbf{I_2}),\cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_r;\sigma_r]\rho$. To establish this, we must show $W.\Psi_i;\cdot;W.\chi_i;W.\sigma_i;\rho_i(\mathbf{q}) \vdash (\mathtt{bnz}\,\mathbf{r_i},\rho_i(\mathbf{u_i});\rho_i(\mathbf{I_i}),\cdot) : \rho_i(\tau_r);\rho_i(\sigma_r)$. The latter follows from $\Psi;\Delta;\chi;\sigma;\mathbf{q} \vdash \mathtt{bnz}\,\mathbf{r_i},\mathbf{u_i};\mathbf{I_i}$ using the component typing rule and the properties of W and ρ that we have by assumption.
  - We define $W' = W$. Note that $W' \in \text{World}$ since $W \in \mathit{world}$.
  - $W \sqsupseteq_{\text{pub}} W$ trivially.
  - Consider arbitrary M_1 and M_2 such that$(M_1, M_2) : W$. Let $M_i = (\mathbf{H_i},\mathbf{R_i},\mathbf{S_i})$.
    From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\,\text{currentMR}(\theta) \mid \theta \in W.\Theta\,\}$.
    From the latter, we obtain a fact for island i_{reg}: $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$.
    From that it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\mathbf{R_i}(r_i) = 0$.
    From the above fact and the reduction semantics we derive that
    $$\langle (\mathbf{H_i},\mathbf{R_i},\mathbf{S_i}) \mid (\mathtt{bnz}\,\mathbf{r_i},\rho_i(\mathbf{u_i});\rho_1(\mathbf{I_i}),\cdot)\rangle \longmapsto^1 \langle (\mathbf{H_i},\mathbf{R_i},\mathbf{S_i}) \mid (\rho_i(\mathbf{I_i}),\cdot)\rangle$$
    Let $M_i' = M_i = (\mathbf{H_i},\mathbf{R_i},\mathbf{S_i})$. Note that $(M_1', M_2') : W'$ is equivalent to $(M_1, M_2) : W$, which holds trivially by assumption.
  - Note that $W.k = W'.k$ since $W'.k = W.k$.
  - Note that $\mathbf{q} \neq \epsilon$, which follows from the third hypothesis. Further, since we haven't changed the world, we can see that the the return address does not change.
  - ret-type$(\mathbf{q},\chi,\sigma) = \text{ret-type}(\mathbf{q},\chi,\sigma)$ holds trivially.
  - currentMR$(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho$ holds trivilaly by assumption currentMR$(W)(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ and $W' = W$.
  - currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$ holds trivilaly by assumption currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$ and $W' = W$.

  Hence, we can conclude that
  $$(W', (\rho_1(\mathbf{I_1}), (\rho_2(\mathbf{I_2}),\cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q},\chi,\sigma)]\!]\rho$$
  Now, the result follows by Lemma 1.11.
- $W.R_1(r_1) = n, n \neq 0$
  We instantiate the second hypothesis, $\Psi;\Delta;\chi \vdash \mathbf{u_1} \approx_u \mathbf{u_2} : \mathbf{box}\,\forall[].\{\chi';\sigma\}^{\mathbf{q}}$. with W and ρ, noting $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$. Thus we have that $(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\chi';\sigma\}^{\mathbf{q}}]\!]\rho$. From the definition of the latter, we have that $W.\hat{\mathbf{R}}_i(\rho_i(\mathbf{u_i})) = \ell_i[\overline{\omega_i}]$.
  We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

– $(W, (\texttt{bnz}\,\mathbf{r_1}, \rho_1(\mathbf{u_1}); \rho_1(\mathbf{I_1}), \cdot), (\texttt{bnz}\,\mathbf{r_2}, \rho_2(\mathbf{u_2}); \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_r; \sigma_r]\rho$. To establish this, we must show $W.\Psi_i; \cdot; W.\chi_i; W.\sigma_i; \rho_i(\mathbf{q}) \vdash (\texttt{bnz}\,\mathbf{r_i}, \rho_i(\mathbf{u_i}); \rho_i(\mathbf{I_i}), \cdot) : \rho_i(\tau_r); \rho_i(\sigma_r)$. The latter follows from $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \texttt{bnz}\,\mathbf{r_i}, \mathbf{u_i}; \mathbf{I_i}$ using the component typing rule and the properties of W and ρ that we have by assumption.
– We define $W' = \triangleright W$. Note that W' ∈ World since $W.k > 0$ and W ∈ World.
– $\triangleright W \sqsupseteq_{\text{pub}} W$ by Lemma 1.6.
– Consider arbitrary $(M_1, M_2) : W$. Let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$.
From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \text{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$. From the latter, we have two facts, one for island i_{reg} and the other for island i_{box}.
First, we have that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\mathbf{R_i}(r_i) = n, n \neq 0$ and $\hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i})) = \ell_i[\overline{\omega_i}]$.
Second, we have that there exist some $\mathbf{H_{b1}} \subseteq \mathbf{H_1}$ and $\mathbf{H_{b2}} \subseteq \mathbf{H_2}$ such that $(\triangleright W, \mathbf{H_{b1}}\restriction, \mathbf{H_{b2}}\restriction) \in \text{currentMR}(W(i_{\text{box}}))$. We use the latter to instantiate $(W, \ell_1[\overline{\omega_1}], \ell_2[\overline{\omega_2}]) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\chi'; \sigma\}^{\mathbf{q}}]\!]\rho$, noting that $\triangleright W \sqsupset W$, which allows us to conclude:
  * $\mathbf{H_{bi}}(\ell_i) = \mathbf{code}[\overline{\beta_i}]\{\chi_i; \sigma_i\}^{\mathbf{q_i}}.\mathbf{I}'_\mathbf{i}$,
  * $\rho_i(\chi') = \chi_i[\overline{\omega_i/\beta_i}]$,
  * $\rho_i(\sigma) = \sigma_i[\overline{\omega_i/\beta_i}]$,
  * $\rho_i(\mathbf{q}) = \mathbf{q_i}[\overline{\omega_i/\beta_i}]$, and
  * $(\triangleright W, (\mathbf{code}[]\{\chi_1; \sigma_1\}^{\mathbf{q_1}}.\mathbf{I}'_1)[\overline{\omega_1/\beta_1}], (\mathbf{code}[]\{\chi_2; \sigma_2\}^{\mathbf{q_2}}.\mathbf{I}'_2)[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[].\{\chi'; \sigma\}^{\mathbf{q}}]\!]\rho$

  Hence, we have that $\hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i})) = \ell_i[\overline{\omega_i}]$ and $\mathbf{H_i}(\ell_i) = \mathbf{code}[\overline{\beta_i}]\{\chi_i; \sigma_i\}^{\mathbf{q_i}}.\mathbf{I}'_\mathbf{i}$, and, from the reduction semantics and $R_i(r_i) = n, n \neq 0$, we derive that

$$\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\texttt{bnz}\,\mathbf{r_i}, \rho_i(\mathbf{u_i}); \rho_1(\mathbf{I_i}), \cdot)\rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\mathbf{I}'_\mathbf{i}[\overline{\omega_i/\beta_i}], \cdot)\rangle$$

  Let $M'_i = M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$. Note that $(M'_1, M'_2) : W'$ is equivalent to $(M_1, M_2) : \triangleright W$, which follows by Lemma 1.6.
– Note that $W.k \leq W'.k + 1$ since $W'.k = (\triangleright W).k = W.k - 1$.
– Note that $\mathbf{q} \neq \epsilon$, which follows from the third hypothesis. Further, since we haven't changed the world, we can see that the the return address does not change.
– Note that

$$\begin{aligned}
&(\triangleright W, (\mathbf{code}[]\{\chi_1; \sigma_1\}^{\mathbf{q_1}}.\mathbf{I}'_1)[\overline{\omega_1/\beta_1}],\\
&\qquad (\mathbf{code}[]\{\chi_2; \sigma_2\}^{\mathbf{q_2}}.\mathbf{I}'_2)[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[].\{\chi'; \sigma\}^{\mathbf{q}}]\!]\rho\\
\equiv\ &(\triangleright W, \mathbf{code}[]\{\chi_1[\overline{\omega_1/\beta_1}]; \sigma_1[\overline{\omega_1/\beta_1}]\}^{\mathbf{q_1}[\overline{\omega_1/\beta_1}]}.\mathbf{I}'_1[\overline{\omega_1/\beta_1}],\\
&\qquad \mathbf{code}[]\{\chi_2[\overline{\omega_2/\beta_2}]; \sigma_2[\overline{\omega_2/\beta_2}]\}^{\mathbf{q_2}[\overline{\omega_2/\beta_2}]}.\mathbf{I}'_2[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[].\{\chi'; \sigma\}^{\mathbf{q}}]\!]\rho\\
\equiv\ &(\triangleright W, (\mathbf{code}[]\{\rho_1(\chi'); \rho_1(\sigma)\}^{\rho_1(\mathbf{q})}.\mathbf{I}'_1[\overline{\omega_1/\beta_1}],\\
&\qquad \mathbf{code}[]\{\rho_2(\chi'); \rho_2(\sigma)\}^{\rho_2(\mathbf{q})}.\mathbf{I}'_2[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[].\{\chi'; \sigma\}^{\mathbf{q}}]\!]\rho
\end{aligned}$$

  Instantiate the latter with $\triangleright W$. We note the following:
  * $\triangleright W \sqsupseteq \triangleright W$ by reflexivity.
  * ret-type$(\mathbf{q}, \chi', \sigma)$ = ret-type$(\mathbf{q}, \chi, \sigma)$. The latter is immediate except in the case when $\mathbf{q}$ is some register $\mathbf{r}'$, in which case we must show that $\mathbf{r}' \in \text{dom}(\chi')$ since otherwise ret-type$(\mathbf{q}, \chi', \sigma)$ would be undefined. But note that from our first premise, it follows that $\Delta \vdash \mathbf{box}\,\forall[].\{\chi'; \sigma\}^{\mathbf{q}}$. By inversion of typing rules, we have that $\Delta \vdash \forall[].\{\chi'; \sigma\}^{\mathbf{q}}$, and hence $\Delta[]; \chi'; \sigma \vdash \mathbf{q}$. From the latter it follows that ret-type$(\mathbf{q}, \chi', \sigma)$ is defined. Hence, if $\mathbf{q}$ is some register $\mathbf{r}'$, it must be that $\mathbf{r}' \in \text{dom}(\chi')$. Moreover, from the second premise, it follows that $\chi'(\mathbf{r}') = \chi(\mathbf{r}')$. This is enough to establish our claim.
  * currentMR$((\triangleright W)(i_{\text{reg}}))$ $\Subset_{\triangleright W}$ $\mathcal{R}[\![\chi']\!]\rho$. To show this, consider arbitrary $(\widetilde{W}, M_1, M_2) \in$ currentMR$((\triangleright W)(i_{\text{reg}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W$. We must show that

$$(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\chi']\!]\rho$$

Note that $(\triangleright W).k = W.k-1$ and that $\text{currentMR}((\triangleright W)(i_{\text{reg}})) = \lfloor \text{currentMR}(W(i_{\text{reg}})) \rfloor_{W.k-1}$. Thus, $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{reg}}))$. Using the latter we can instantiate $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ with $(\widetilde{W}, M_1, M_2)$, noting that $\widetilde{W} \sqsupseteq W$ (by transitivity of $\sqsupseteq$), which gives us $(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\chi]\!]\rho$. Finally, by Lemma 1.19 (register-file subtyping implies inclusion) we have that $\mathcal{R}[\![\chi]\!]\rho \subseteq \mathcal{R}[\![\chi']\!]\rho$, which is sufficient to show what we need.

* $\text{currentMR}(\triangleright W(i_{\text{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\sigma]\!]\rho$. To show this, consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}((\triangleright W)(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W$. We must show that

$$(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\sigma]\!]\rho$$

Note that $(\triangleright W).k = W.k-1$ and that $\text{currentMR}((\triangleright W)(i_{\text{stk}})) = \lfloor \text{currentMR}(W(i_{\text{stk}})) \rfloor_{W.k-1}$. Thus, $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{stk}}))$. Using the latter we can instantiate $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$ with $(\widetilde{W}, M_1, M_2)$, noting that $\widetilde{W} \sqsupseteq W$ (by transitivity of $\sqsupseteq$), which gives us $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\sigma]\!]\rho$ as needed.

Hence, we can conclude that

$$(\triangleright W, (\rho_1(\mathbf{I}_1'[\overline{\omega_1/\beta_1}]), \cdot), (\rho_2(\mathbf{I}_2'[\overline{\omega_2/\beta_2}]), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi', \sigma)]\!]\rho$$

Now, the result follows by Lemma 1.11.

□

Lemma 1.45 (Load from Mutable Tuple)
If $\Psi; \Delta; \chi \vdash \mathbf{r_{s1}} \approx_{\text{u}} \mathbf{r_{s2}} : \mathbf{ref}\ \langle \tau_0, \ldots, \tau_n \rangle$, $\mathbf{0} \le \mathbf{i} \le \mathbf{n}$, $\mathbf{q} \neq \mathbf{r_d}$, and $\Psi; \Delta; \chi[\mathbf{r_d} : \tau_i]; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$, then $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \mathbf{I_2}$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \mathbf{I_1}$ and $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1((\mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \mathbf{I_2}, \cdot)))\\ = (W, (\mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.\end{aligned}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i] \rangle)$.

In the following, assume $W.k > 0$ and let $\tau_{\mathbf{r}}; \sigma_{\mathbf{r}} = \text{ret-type}(\mathbf{q}, \chi, \sigma)$.

Moreover, note the following preliminary facts:

- By instantiating our first hypothesis with W and ρ, we have that $(W, W.\hat{\mathbf{R}}_{\mathbf{1}}(\mathbf{r_{s1}}), W.\hat{\mathbf{R}}_{\mathbf{2}}(\mathbf{r_{s2}})) \in \mathcal{W}[\![\mathbf{ref}\ \langle \tau_0, \ldots, \tau_n \rangle]\!]\rho$. From the definition of the latter, we have that $W.\hat{\mathbf{R}}_{\mathbf{1}}(\mathbf{r_{s1}}) = \ell_1$ and $W.\hat{\mathbf{R}}_{\mathbf{2}}(\mathbf{r_{s2}}) = \ell_2$ and we know there exists an island i such that

$$\begin{aligned}&\forall W' \sqsupseteq W.(\ell_1, \ell_2) \in W'(i).\text{bij}(W'(i).s) \ \wedge \exists \varphi_M.\ \text{currentMR}(W'(i)) = \varphi_M \otimes\\ &\quad \{\, (\widetilde{W}, \{\ell_1 \mapsto \mathbf{h_1}\}\restriction, \{\ell_2 \mapsto \mathbf{h_2}\}\restriction) \in \text{MemAtom} \mid\ (\widetilde{W}, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \tau_0, \ldots, \tau_n \rangle]\!]\rho \,\} \quad (8)\end{aligned}$$

We proceed by analogy to Lemma 1.11, but choose a world W' after choosing memories, so we cannot use the Lemma as stated.

- We claim that $(W, (\mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\rho$. To establish this, we must show $W.\Psi_j; \cdot; W.\chi_{\mathbf{j}}; W.\sigma_{\mathbf{j}}; \rho_j(\mathbf{q}) \vdash (\mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{sj}}[\mathbf{i}]; \rho_j(\mathbf{I_j}), \cdot) : \rho_j(\tau_{\mathbf{r}}); \rho_j(\sigma_{\mathbf{r}})$. The latter follows from $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{sj}}[\mathbf{i}]; \mathbf{I_j}$ using the component typing rule and the properties of W and ρ that we have by assumption.

- Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, choose arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho$.
  We must show that $(W, E_1[(\mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}$.
  In order to do that, choose arbitrary $(M_1, M_2) : W$. We need to show that the expressions either both terminate with these memories or are both still running after $W.k$ steps.
  We do this by taking one step and then using the resulting memories, finding a world that we can then use with the final hypothesis we are given.
  Let $M_j = (\mathbf{H_j}, \mathbf{R_j}, \mathbf{S_j})$ for $j \in \{1, 2\}$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \mathrm{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$. From the latter, we can have the following two facts, one for island i_{reg} and one for the island i (which we know exists from the preliminary facts we collected above and keeps track of the references $\boldsymbol{\ell_i}$ and $\boldsymbol{\ell_2}$ that we wish to update).
  First, we have that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \mathrm{currentMR}(W(i_{\mathrm{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\hat{\mathbf{R}}_1(\mathbf{r_{s1}}) = \boldsymbol{\ell_1}$, $\hat{\mathbf{R}}_2(\mathbf{r_{s2}}) = \boldsymbol{\ell_2}$, (which are the same $\boldsymbol{\ell_1}$ and $\boldsymbol{\ell_2}$ from our preliminary facts above).
  Second, we have that there exist some $\mathbf{H_{r1}} \subseteq \mathbf{H_1}$ and $\mathbf{H_{r2}} \subseteq \mathbf{H_2}$ such that $(\triangleright W, \mathbf{H_{r1}}\restriction, \mathbf{H_{r2}}\restriction) \in \mathrm{currentMR}(W(i))$. Instantiating (8) with W, noting $W \sqsupseteq W$ by reflexivity, we have that

$$\mathrm{currentMR}(W(i)) = \varphi_M \otimes \{\, (\widetilde{W}, \{\boldsymbol{\ell_1} \mapsto \mathbf{h_1}\}\restriction, \{\boldsymbol{\ell_2} \mapsto \mathbf{h_2}\}\restriction) \in \mathrm{MemAtom} \mid (\widetilde{W}, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle]\!]\rho \,\}$$

  Hence, we have that $\mathbf{H_1}(\boldsymbol{\ell_1}) = \mathbf{H_{r1}}(\boldsymbol{\ell_1}) = \mathbf{h_1}$, and $\mathbf{H_1}(\boldsymbol{\ell_2}) = \mathbf{H_{r2}}(\boldsymbol{\ell_2}) = \mathbf{h_2}$, as well as $(\triangleright W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle]\!]\rho$. From the latter, it follows that $\mathbf{h_1} = \langle \mathbf{w_{10}}, \ldots, \mathbf{w_{1n}} \rangle$ and $\mathbf{h_2} = \langle \mathbf{w_{20}}, \ldots, \mathbf{w_{2n}} \rangle$. Moreover, since we have as our second hypothesis $\mathbf{0} \leq \mathbf{i} \leq \mathbf{n}$, it follows that $(\triangleright W, \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\boldsymbol{\tau_i}]\!]\rho$.
  Next, by the reduction semantics of our language, with all of the above facts in hand, we have that:
  $\langle M_j \mid E_j[(\mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{sj}}[\mathbf{i}]; \rho_j(\mathbf{I_j}), \cdot)] \rangle \longrightarrow \langle (\mathbf{H_j}, \mathbf{R_j}[\mathbf{r_d} \mapsto \mathbf{w_{ji}}], \mathbf{S_j}) \mid E_j[(\rho_j(\mathbf{I_j}), \cdot)] \rangle$.
  Let $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}], W.\boldsymbol{\chi_1}[\mathbf{r_d} : \rho_1(\boldsymbol{\tau_i})], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \mathbf{w_{2i}}], W.\boldsymbol{\chi_2}[\mathbf{r_d} : \rho_2(\boldsymbol{\tau_i})])$,
  Now let $W' = (W.k, W.\boldsymbol{\Psi_1}, W.\boldsymbol{\Psi_2}, W.\Theta[i_{\mathrm{reg}} \mapsto \mathrm{island}_{\mathrm{reg}}(s, W.k)])$.
- We claim that $W' \in \mathrm{World}$.
  It suffices to show $W'.\Psi_j; \cdot \vdash \mathbf{w_{ji}} : \rho_j(\boldsymbol{\tau_i})$.
  Since $(\triangleright W, \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\boldsymbol{\tau_i}]\!]\rho$ and $\triangleright W.\boldsymbol{\Psi_j} = W'.\boldsymbol{\Psi_j}$, WvalAtom gets us what we need.
- We claim that $(M_1', M_2') : W'$.
- Instantiating the last hypothesis with W', noting that Lemmas 1.20 and 1.21 yield the required obligations on memory relations, we know that $(W', E_1[(\rho_1(\mathbf{I_1}), \cdot)], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}$.
  This means that either $\langle M_j' \mid E_j[(\rho_j(\mathbf{I_j}), \cdot)] \rangle \downarrow$ or $\mathrm{running}(W'.k, \langle M_j' \mid E_j[(\rho_j(\mathbf{I_j}), \cdot)] \rangle)$.
  In the former case, that clearly means that $\langle M_j \mid E_j[(\mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{sj}}[\mathbf{i}]; \rho_j(\mathbf{I_j}), \cdot)] \rangle \downarrow$.
  In the latter case, note that $W'.k \leq W.k{+}1$, which means that $\mathrm{running}(W.k, \langle M_j \mid E_j[(\mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{sj}}[\mathbf{i}]; \rho_j(\mathbf{I_j}), \cdot)] \rangle)$ holds, and so we are done.

□

Lemma 1.46 (Load from Immutable Tuple)
If $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi} \vdash \mathbf{r_{s1}} \approx_{\mathrm{u}} \mathbf{r_{s2}} : \mathbf{box}\,\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle$, $\mathbf{0} \leq \mathbf{i} \leq \mathbf{n}$, $\mathbf{q} \neq \mathbf{r_d}$, and $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau_i}]; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$, then $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \mathbf{I_2}$.

Proof

Clearly, $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \mathbf{I_1}$ and $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$. We need to show that

$$(W, \rho_1((\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \mathbf{I_1}, \cdot)), \rho_2((\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \mathbf{I_2}, \cdot))) \\ = (W, (\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot), (\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})]\!]\rho. \quad (9)$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that running$(0, \langle M_i \mid E_i[e_i]\rangle)$.

In the following, assume $W.k > 0$ and let $\boldsymbol{\tau_r}; \boldsymbol{\sigma_r} = \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})$.

Moreover, note the following preliminary fact:

- By instantiating our first hypothesis with W and ρ, we have that $(W, W.\hat{\mathbf{R}}_\mathbf{1}(\mathbf{r_{s1}}), W.\hat{\mathbf{R}}_\mathbf{2}(\mathbf{r_{s2}})) \in \mathcal{W}[\![\textbf{box}\,\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n}\rangle]\!]\rho$. From the definition of the latter, we have that $W.\hat{\mathbf{R}}_\mathbf{1}(\mathbf{r_{s1}}) = \boldsymbol{\ell_1}$ and $W.\hat{\mathbf{R}}_\mathbf{2}(\mathbf{r_{s2}}) = \boldsymbol{\ell_2}$ and

$$\forall(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}})).\ \widetilde{W} \sqsupset W \\ \implies (\widetilde{W}, M_1(\boldsymbol{\ell_1}), M_2(\boldsymbol{\ell_2})) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n}\rangle]\!]\rho\,\} \quad (10)$$

With the above fact in hand, we now prove (9).

- We claim that $(W, (\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot), (\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \boldsymbol{\tau_r}; \boldsymbol{\sigma_r}]\rho$. To establish this we must show $W.\Psi_1; \cdot; W.\boldsymbol{\chi_1}; W.\boldsymbol{\sigma_1}; \rho_1(\mathbf{q}) \vdash (\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot) : \rho_1(\boldsymbol{\tau_r}); \rho_1(\boldsymbol{\sigma_r})$ and $W.\Psi_2; \cdot; W.\boldsymbol{\chi_2}; W.\boldsymbol{\sigma_2}; \rho_2(\mathbf{q}) \vdash (\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot) : \rho_2(\boldsymbol{\tau_r}); \rho_2(\boldsymbol{\sigma_r})$. Each follows from $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \mathbf{I_2}$ respectively using the component typing rule and the properties of W and ρ that we have by assumption.
- Consider arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}_r; \boldsymbol{\sigma_r}]\!]\rho$. We must show

$$(W, E_1[(\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

  Consider arbitrary $(M_1, M_2) : W$. We must show either that $\langle M_1 \mid E_1[(\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow$ and $\langle M_2 \mid E_2[(\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow$, or running$(W.k, \langle M_1 \mid E_1[(\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot)]\rangle)$ and running$(W.k, \langle M_2 \mid E_2[(\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s2}}[\mathbf{i}]; \rho_2(\mathbf{I_2}), \cdot)]\rangle)$.

  Let $M_1 = (\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1})$ and $M_2 = (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2})$.

  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\,\text{currentMR}(\theta) \mid \theta \in W.\Theta\,\}$. From the latter, we can have the following two facts, one for island i_{reg} and one for the island i_{box}.

  First, we have that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\hat{\mathbf{R}}_\mathbf{1}(\mathbf{r_{s1}}) = \boldsymbol{\ell_1}$, $\hat{\mathbf{R}}_\mathbf{2}(\mathbf{r_{s2}}) = \boldsymbol{\ell_2}$, (which are the same $\boldsymbol{\ell_1}, \boldsymbol{\ell_2}$ from our preliminary fact above).

  Second, we have that there exist some $\mathbf{H_{r1}} \subseteq \mathbf{H_1}$ and $\mathbf{H_{r2}} \subseteq \mathbf{H_2}$ such that $(\triangleright W, \mathbf{H_{r1}}\restriction, \mathbf{H_{r2}}\restriction) \in \text{currentMR}(W(i_{\text{box}}))$. Instantiating (10) with $\triangleright W$, we have that

$$(\triangleright W, \mathbf{H_{r1}}\restriction(\boldsymbol{\ell_1}), \mathbf{H_{r2}}\restriction(\boldsymbol{\ell_2})) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n}\rangle]\!]\rho\,\}$$

  Hence, we have that $\mathbf{H_1}(\boldsymbol{\ell_1}) = \mathbf{H_{r1}}(\boldsymbol{\ell_1}) = \mathbf{h_1}$, and $\mathbf{H_1}(\boldsymbol{\ell_2}) = \mathbf{H_{r2}}(\boldsymbol{\ell_2}) = \mathbf{h_2}$, as well as $(\triangleright W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n}\rangle]\!]\rho$. From the latter, it follows that $\mathbf{h_1} = \langle \mathbf{w_{10}}, \ldots, \mathbf{w_{1n}}\rangle$ and $\mathbf{h_2} = \langle \mathbf{w_{20}}, \ldots, \mathbf{w_{2n}}\rangle$. Moreover, since we have as our second hypothesis $\mathbf{0} \leq \mathbf{i} \leq \mathbf{n}$, it follows that $(W, \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\boldsymbol{\tau_i}]\!]\rho$.

  Next, by the reduction semantics of our language, with all of the above facts in hand, we have that:

$$\langle M_1 \mid E_1[(\texttt{ld}\,\mathbf{r_d}, \mathbf{r_{s1}}[\mathbf{i}]; \rho_1(\mathbf{I_1}), \cdot)]\rangle \longrightarrow \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle$$

and

$$\langle M_2 \mid E_2[(\mathtt{ld}\ \mathbf{r_d}, \mathbf{r_{s2}[i]}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \longrightarrow \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle$$

where $M_1' = (\mathbf{H_1}, \mathbf{R_1}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}], \mathbf{S_1})$ with $\mathbf{R_1}(\mathbf{r_{s1}}) = \boldsymbol{\ell_1}$ and $\mathbf{H_1}(\boldsymbol{\ell_1}) = \langle \mathbf{w_{10}}, ..., \mathbf{w_{1i}}, ..., \mathbf{w_{1n}}\rangle$, and $M_2' = (\mathbf{H_2}, \mathbf{R_2}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}], \mathbf{S_2})$ with $\mathbf{R_2}(\mathbf{r_{s2}}) = \boldsymbol{\ell_2}$ and $\mathbf{H_2}(\boldsymbol{\ell_2}) = \langle \mathbf{w_{20}}, ..., \mathbf{w_{2i}}, ..., \mathbf{w_{2n}}\rangle$.
Note that in order to complete our proof, it suffices to show:

$$\begin{array}{l}(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge\ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee \\ (\text{running}(W.k-1, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge\ \text{running}(W.k-1, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))\end{array}$$

Let $W' = (W.k, W.\boldsymbol{\Psi_1}, W.\boldsymbol{\Psi_2}, W.\Theta[i_{\text{reg}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$ where

$$s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}], W.\boldsymbol{\chi_1}[\mathbf{r_d} : \boldsymbol{\tau_i}], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \mathbf{w_{2i}}], W.\boldsymbol{\chi_2}[\mathbf{r_d} : \boldsymbol{\tau_i}]).$$

We claim that $W' \in \text{World}$. Recall that we have $(W, w_{1i}, w_{2i}) \in \mathcal{W}[\![\boldsymbol{\tau}_i]\!]\rho$. Thus we have that $W.\Psi_i; \cdot \vdash w_{ji} : \rho_i(\boldsymbol{\tau}_i)$. Given our choice of W' and since $W \in \text{World}$, it follows that $W'.\Psi_i; \cdot \vdash w_{ji} : \rho_i(\boldsymbol{\tau}_i)$ which is sufficient to establish our claim.
Moreover, note that $W' \sqsupseteq W$ and $W' \sqsupseteq_{\text{pub}} W$. Both follow immediately given our choice of W' and the definition of $\text{island}_{\text{reg}}$.
We proceed by showing that $(M_1', M_2') : W'$ and then instantiating our final premise $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau_i}]; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$.

- We claim that $(M_1', M_2') : W'$. We prove this claim by establishing the following:
  - $\vdash M_1' : W'.\Phi_1$ and $\vdash M_2' : W'.\Phi_2$, both of which easily follow from $(M_1, M_2) : W$ and the facts that $W'.\boldsymbol{\chi_1} = W.\boldsymbol{\chi_1}[\mathbf{r_d} : \rho_1(\boldsymbol{\tau_i})]$, $W'.\boldsymbol{\chi_2} = W.\boldsymbol{\chi_2}[\mathbf{r_d} : \rho_2(\boldsymbol{\tau_i})]$ and that we have updated registers r_d in with well-typed words, i.e., with words of the types designated by the ith elements of $W.\Psi_1(\boldsymbol{\ell_1})$ and $W.\Psi_2(\boldsymbol{\ell_2})$, namely $\rho_1(\boldsymbol{\tau_i})$ and $\rho_2(\boldsymbol{\tau_i})$.
  - We assume that $W.k > 0$ (and thus $W'.k > 0$). We must show that

    $$(\triangleright W', M_1', M_2') \in \bigotimes \{\, \text{currentMR}(\theta) \mid \theta \in W'.\Theta \,\}$$

    The latter follows from $(M_1, M_2) : W$ and monotonicity of MemRel given that we establish the following claim for island i_{reg}:

    $$(\triangleright W', \mathbf{W.R_1}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}]\restriction, \mathbf{W.R_2}[\mathbf{r_d} \mapsto \mathbf{w_{2i}}]\restriction) \in \text{currentMR}(W'(i_{\text{reg}}))$$

    Recall that $W'.R_i = W.R_i[r_d \mapsto w_{ji}]$. Thus we obtain trivially that $(\triangleright W', W.R_1[r_d \mapsto w_{1i}], W.R_2[r_d \mapsto w_{2i}]) \in \{(\widetilde{W}, W'.R_1, W'.R_2) \mid \widetilde{W} \in \text{World}_{W.k}\}$. From the latter, we establish directly our claim that

    $$(\triangleright W', \mathbf{W.R_1}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}]\restriction, \mathbf{W.R_2}[\mathbf{r_d} \mapsto \mathbf{w_{2i}}]\restriction) \in \text{currentMR}(W'(i_{\text{reg}}))$$

- Next, we instantiate our final hypothesis with W' and ρ. Note that $\rho \in \mathcal{D}[\![\boldsymbol{\Delta}]\!]$ by assumption, $W' \in \mathcal{H}[\![\boldsymbol{\Psi}]\!]$ by heap monotonicity (Lemma 1.9) and that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ by Lemma 1.21 since $W'(i_{\text{stk}}) = W(i_{\text{stk}})$. We also claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau_i}]]\!]\rho$. Above, we have established that $(W', w_{1i}, w_{2i}) \in \mathcal{W}[\![\boldsymbol{\tau}_i]\!]$ which, using Lemma 1.20, is sufficient to establish our claim. Hence, we have that

  $$(W', (\rho_1(\mathbf{I_1}, \cdot)), (\rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}_{\mathbf{r}}; \boldsymbol{\sigma}_{\mathbf{r}}]\!]\rho$$

  Instantiate the above with E_1 and E_2. Note that we have $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}_{\mathbf{r}}; \boldsymbol{\sigma}_{\mathbf{r}}]\!]\rho$ which follows from $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}_{\mathbf{r}}; \boldsymbol{\sigma}_{\mathbf{r}}]\!]\rho$ by monotonicity for evaluation contexts (Lemma 1.10), since our choice of W', $W' \sqsupseteq_{\text{pub}} W$ and our third hypothesis, $\mathbf{q} \neq \mathbf{r_d}$, let us easily establish all the premises of that lemma.
  Hence, we have

  $$(W', E_1[(\rho_1(\mathbf{I_1}, \cdot))], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Instantiate the latter with M_1' and M_2', noting that $(M_1', M_2') : W'$. Hence, we have

$$(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee$$
$$(\text{running}(W.k, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))$$

which implies what we needed to show.

□

Lemma 1.47 (Store to Mutable Tuple)
If $\mathbf{\Psi}; \mathbf{\Delta}; \chi \vdash \mathbf{r_{d1}} \approx_{\mathrm{u}} \mathbf{r_{d2}} : \mathbf{ref}\ \langle \tau_0, \ldots, \tau_n \rangle$, $\mathbf{0 \le i \le n}$, $\mathbf{\Psi}; \mathbf{\Delta}; \chi \vdash \mathbf{r_{s1}} \approx_{\mathrm{u}} \mathbf{r_{s2}} : \tau_i$, and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$, then $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \mathbf{I_2}$.

Proof

Clearly, $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$(W, \rho_1((\mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \mathbf{I_2}, \cdot)))$$
$$= (W, (\mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho. \quad (11)$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i]\rangle)$.

In the following, assume $W.k > 0$ and let $\tau_{\mathbf{r}}; \sigma_{\mathbf{r}} = \text{ret-type}(\mathbf{q}, \chi, \sigma)$.

Moreover, note the following preliminary facts:

- By instantiating our first hypothesis with W and ρ, we have that $(W, W.\hat{\mathbf{R}}_{\mathbf{1}}(\mathbf{r_{d1}}), W.\hat{\mathbf{R}}_{\mathbf{2}}(\mathbf{r_{d2}})) \in \mathcal{W}[\![\mathbf{ref}\ \langle \tau_0, \ldots, \tau_n \rangle]\!]\rho$. From the definition of the latter, we have that $W.\hat{\mathbf{R}}_{\mathbf{1}}(\mathbf{r_{d1}}) = \ell_1$ and $W.\hat{\mathbf{R}}_{\mathbf{2}}(\mathbf{r_{d2}}) = \ell_2$ and we know there exists an island i such that

$$\forall W' \sqsupseteq W.(\ell_1, \ell_2) \in W'(i).\text{bij}(W'(i).s) \ \wedge \exists \varphi_M.\ \text{currentMR}(W'(i)) = \varphi_M \otimes$$
$$\{\, (\widetilde{W}, \{\ell_1 \mapsto \mathbf{h_1}\}\restriction, \{\ell_2 \mapsto \mathbf{h_2}\}\restriction) \in \text{MemAtom} \mid \ (\widetilde{W}, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \tau_0, \ldots, \tau_n \rangle]\!]\rho \,\} \quad (12)$$

- By instantiating the third hypothesis with W and ρ, we have that $(W, W.\hat{\mathbf{R}}_{\mathbf{1}}(\mathbf{r_{s1}}), W.\hat{\mathbf{R}}_{\mathbf{2}}(\mathbf{r_{s2}})) \in \mathcal{W}[\![\tau_i]\!]\rho$. From the latter, we have that there exist some $\mathbf{w'_{1i}}$ and $\mathbf{w'_{2i}}$ such that $W.\hat{\mathbf{R}}_{\mathbf{1}}(\mathbf{r_{s1}}) = \mathbf{w'_{1i}}$ and $W.\hat{\mathbf{R}}_{\mathbf{2}}(\mathbf{r_{s2}}) = \mathbf{w'_{2i}}$.

With the above facts in hand, we now prove (11).

- We claim that $(W, (\mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\rho$. To establish this we must show $W.\Psi_1; \cdot; W.\chi_1; W.\sigma_1; \rho_1(\mathbf{q}) \vdash (\mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \rho_1(\mathbf{I_1}), \cdot) : \rho_1(\tau_{\mathbf{r}}); \rho_1(\sigma_{\mathbf{r}})$ and $W.\Psi_2; \cdot; W.\chi_2; W.\sigma_2; \rho_2(\mathbf{q}) \vdash (\mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \rho_2(\mathbf{I_2}), \cdot) : \rho_2(\tau_{\mathbf{r}}); \rho_2(\sigma_{\mathbf{r}})$. Each follows from $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \mathbf{I_2}$, respectively, using the component typing rule and the properties of W and ρ that we have by assumption.
- Consider arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_r; \sigma_{\mathbf{r}}]\!]\rho$. We must show that

$$(W, E_1[(\mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

  Consider arbitrary $(M_1, M_2) : W$. We must show either that $\langle M_1 \mid E_1[(\mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow$ and $\langle M_2 \mid E_2[(\mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow$, or $\text{running}(W.k, \langle M_1 \mid E_1[(\mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \rho_1(\mathbf{I_1}), \cdot)]\rangle)$ and $\text{running}(W.k, \langle M_2 \mid E_2[(\mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \rho_2(\mathbf{I_2}), \cdot)]\rangle)$.
  Let $M_1 = (\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1})$ and $M_2 = (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2})$.

From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \mathrm{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$. From the latter, we can have the following two facts, one for island i_{reg} and one for the island i (which we know exists from the preliminary facts we collected above and keeps track of the references $\boldsymbol{\ell_i}$ and $\boldsymbol{\ell_2}$ that we wish to update).

First, we have that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \mathrm{currentMR}(W(i_{\mathrm{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\hat{\mathbf{R}}_\mathbf{1}(\mathbf{r_{d1}}) = \boldsymbol{\ell_1}$, $\hat{\mathbf{R}}_\mathbf{2}(\mathbf{r_{d2}}) = \boldsymbol{\ell_2}$, $\hat{\mathbf{R}}_\mathbf{1}(\mathbf{r_{s1}}) = \mathbf{w'_{1i}}$, $\hat{\mathbf{R}}_\mathbf{2}(\mathbf{r_{d2}}) = \mathbf{w'_{2i}}$ (which are the same $\boldsymbol{\ell_1}, \boldsymbol{\ell_2}, \mathbf{w'_{1i}}$, and $\mathbf{w'_{1i}}$ from our preliminary facts above).

Second, we have that there exist some $\mathbf{H_{r1}} \subseteq \mathbf{H_1}$ and $\mathbf{H_{r2}} \subseteq \mathbf{H_2}$ such that $(\triangleright W, \mathbf{H_{r1}}\restriction, \mathbf{H_{r2}}\restriction) \in \mathrm{currentMR}(W(i))$. Instantiating (12) with W, noting $W \sqsupseteq W$ by reflexivity, we have that

$$\mathrm{currentMR}(W(i)) = \varphi_M \otimes \{\, (\widetilde{W}, \{\boldsymbol{\ell_1} \mapsto \mathbf{h_1}\}\restriction, \{\boldsymbol{\ell_2} \mapsto \mathbf{h_2}\}\restriction) \in \mathrm{MemAtom} \mid (\widetilde{W}, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle]\!]\rho \,\}$$

Hence, we have that $\mathbf{H_1}(\boldsymbol{\ell_1}) = \mathbf{H_{r1}}(\boldsymbol{\ell_1}) = \mathbf{h_1}$, and $\mathbf{H_1}(\boldsymbol{\ell_2}) = \mathbf{H_{r2}}(\boldsymbol{\ell_2}) = \mathbf{h_2}$, as well as $(\triangleright W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle]\!]\rho$. From the latter, it follows that $\mathbf{h_1} = \langle \mathbf{w_{10}}, \ldots, \mathbf{w_{1n}} \rangle$ and $\mathbf{h_2} = \langle \mathbf{w_{20}}, \ldots, \mathbf{w_{2n}} \rangle$. Moreover, since we have as our second hypothesis $\mathbf{0} \leq \mathbf{i} \leq \mathbf{n}$, it follows that $(\triangleright W, \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\boldsymbol{\tau_i}]\!]\rho$.

Next, by the reduction semantics of our language, with all of the above facts in hand, we have that:

$$\langle (\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1}) \mid E_1[(\mathtt{st}\ \mathbf{r_{d1}}[\mathbf{i}], \mathbf{r_{s1}}; \rho_1(\mathbf{I_1}), \cdot)] \rangle \longmapsto^1 \langle (\mathbf{H_1}[\boldsymbol{\ell_1} \mapsto \mathbf{h'_1}], \mathbf{R_1}, \mathbf{S_1}) \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)] \rangle$$

and

$$\langle (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2}) \mid E_2[(\mathtt{st}\ \mathbf{r_{d2}}[\mathbf{i}], \mathbf{r_{s2}}; \rho_2(\mathbf{I_2}), \cdot)] \rangle \longmapsto^1 \langle (\mathbf{H_2}[\boldsymbol{\ell_2} \mapsto \mathbf{h'_2}], \mathbf{R_2}, \mathbf{S_2}) \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)] \rangle$$

where $\mathbf{h'_1} = \langle \mathbf{w_{10}}, \ldots, \mathbf{w'_{1i}}, \ldots, \mathbf{w_{1n}} \rangle$ and $\mathbf{h'_2} = \langle \mathbf{w_{20}}, \ldots, \mathbf{w'_{2i}}, \ldots, \mathbf{w_{2n}} \rangle$.

Let $M'_1 = (\mathbf{H_1}[\boldsymbol{\ell_1} \mapsto \mathbf{h'_1}], \mathbf{R_1}, \mathbf{S_1})$, let $M'_2 = (\mathbf{H_2}[\boldsymbol{\ell_2} \mapsto \mathbf{h'_2}], \mathbf{R_2}, \mathbf{S_2})$.

Note that in order to complete our proof, it suffices to show:

$$\begin{array}{l} (\langle M'_1 \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)] \rangle \downarrow \ \wedge\ \langle M'_2 \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)] \rangle \downarrow) \ \vee \\ (\mathrm{running}(W.k - 1, \langle M'_1 \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)] \rangle) \ \wedge\ \mathrm{running}(W.k - 1, \langle M'_2 \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)] \rangle)) \end{array}$$

We proceed by showing that $(M'_1, M'_2) : W$ and then instantiating our final hypothesis $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathbf{I_1} \approx_\mathbf{I} \mathbf{I_2}$.

- We claim that $(M'_1, M'_2) : W$. We prove this claim by establishing the following:
  - $\vdash M'_1 : W.\Phi_1$ and $\vdash M'_2 : W.\Phi_2$, both of which easily follow from $(M_1, M_2) : W$ and the fact that we have updated locations $\boldsymbol{\ell_1}$ and $\boldsymbol{\ell_2}$ in a type-preserving manner, i.e., with tuples of the types designated by $W.\Psi_1(\boldsymbol{\ell_1})$ and $W.\Psi_2(\boldsymbol{\ell_2})$, namely $\rho_1(\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle)$ and $\rho_2(\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle)$.
  - We assume that $W.k > 0$ and we must show that

    $$(\triangleright W, M'_1, M'_2) \in \bigotimes\{\, \mathrm{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$$

    The latter follows from $(M_1, M_2) : W$, if we establish the following claim for island i:

    $$(\triangleright W, \mathbf{H_{r1}}[\boldsymbol{\ell_1} \mapsto \mathbf{h'_1}]\restriction, \mathbf{H_{r1}}[\boldsymbol{\ell_1} \mapsto \mathbf{h'_2}]\restriction) \in \mathrm{currentMR}(W(i))$$

    Recall that

    $$\mathrm{currentMR}(W(i)) = \varphi_M \otimes \{\, (\widetilde{W}, \{\boldsymbol{\ell_1} \mapsto \mathbf{h_1}\}\restriction, \{\boldsymbol{\ell_2} \mapsto \mathbf{h_2}\}\restriction) \in \mathrm{MemAtom} \mid (\widetilde{W}, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle]\!]\rho \,\}$$

Note that by monotonicity, we have $(\triangleright W, \mathbf{w'_{1i}}, \mathbf{w'_{2i}}) \in \mathcal{W}[\![\tau_i]\!]\rho$. From the latter, together with $(\triangleright W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \tau_0, \ldots, \tau_n \rangle]\!]\rho$, it follows that $(\triangleright W, \mathbf{h'_1}, \mathbf{h'_2}) \in \mathcal{HV}[\![\langle \tau_0, \ldots, \tau_n \rangle]\!]\rho$. Also, from $(\triangleright W, \mathbf{H_{r1}}\restriction, \mathbf{H_{r2}}\restriction) \in \text{currentMR}(W(i))$, we have that $(\triangleright W, \mathbf{H_{r1}} \setminus \{\ell_1\}, \mathbf{H_{r2}} \setminus \{\ell_2\}) \in \varphi_M$.
The latter two facts, are sufficient to establish our claim that $(\triangleright W, \mathbf{H_{r1}}[\ell_1 \mapsto \mathbf{h'_1}]\restriction, \mathbf{H_{r1}}[\ell_1 \mapsto \mathbf{h'_2}]\restriction) \in \text{currentMR}(W(i))$.

– Next, we instantiate our final premise with W and ρ. Note that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. Hence, we have that

$$(W, (\rho_1(\mathbf{I_1}, \cdot)), (\rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \tau_r; \sigma_r]\!]\rho$$

Instantiate the above with E_1 and E_2. Note that we have $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_r; \sigma_r]\!]\rho$. Hence, we have

$$(W, E_1[(\rho_1(\mathbf{I_1}, \cdot))], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Instantiate the latter with M'_1 and M'_2, noting that $(M'_1, M'_2) : W$. Hence, we have

$$\begin{array}{l}(\langle M'_1 \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M'_2 \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee \\ (\text{running}(W.k, \langle M'_1 \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k, \langle M'_2 \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))\end{array}$$

which implies what we needed to show.

□

Lemma 1.48 (Allocate Mutable Tuple)
If $\text{len}(\overline{\tau}) = \mathbf{n}$, $\mathbf{q} \neq \mathbf{r_d}$, and $\Psi; \Delta; \chi[\mathbf{r_d} : \text{ref } \langle \overline{\tau} \rangle]; \sigma; \text{dec}(\mathbf{q}, \mathbf{n}) \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$,
then $\Psi; \Delta; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_1} \approx_{\mathbf{I}} \texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}$.

Proof

Clearly, $\Psi; \Delta; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_1}$ and $\Psi; \Delta; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\overline{\tau} :: \sigma]\!]\rho$. We need to show that

$$\begin{array}{l}(W, \rho_1((\texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_1}, \cdot)), \rho_2((\texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}, \cdot))) \\ \quad = (W, (\texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot), (\texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \overline{\tau} :: \sigma)]\!]\rho. \quad (13)\end{array}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i]\rangle)$.

In the following, assume $W.k > 0$ and let $\tau_r; \sigma_r = \text{ret-type}(\mathbf{q}, \chi, \overline{\tau} :: \sigma)$ and $\overline{\tau} = \tau_1 :: \cdots :: \tau_m$.

Moreover, note the following preliminary facts:

- By our first hypothesis, we have that $m = n$.
- By our third hypothesis and the typing rules, we have that , $\text{dec}(\mathbf{q}, \mathbf{n}) \neq \epsilon$ and $\text{dec}(\mathbf{q}, \mathbf{n}) \neq$ undefined. A consequence of the latter fact is that if $\mathbf{q} = \mathbf{i}$ then $\mathbf{i} \geq \mathbf{n}$.
- By our assumption $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\overline{\tau} :: \sigma]\!]\rho$ and the first fact, we have there exist $w_{11}, ..., w_{1n}, w_{21}, ..., w_{2n}$, S'_1 and S'_2 such that $W.S_1 = w_{11} :: \cdots :: w_{1n} :: S'_1$, $W.S_2 = w_{21} :: \cdots :: w_{2n} :: S'_2$ and $(W, w_{1i}, w_{2i}) \in \mathcal{W}[\![\tau_i]\!]\rho$.

With the above facts in hand, we now prove (13).

- We claim $(W, (\texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot), (\texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_r; \sigma_r]\rho$. From the definitions of $\text{TermAtom}[\mathbf{q} \vdash \tau_r; \sigma_r]\rho$ and $\text{TermAtom}[\mathbf{q} \vdash \tau_r; \sigma_r]$, it suffices to show $W.\Psi_1; \cdot; W.\chi_1; W.\sigma_1; \rho_1(\mathbf{q}) \vdash (\texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot) : \rho_1(\tau_r); \rho_1(\sigma_r)$ and $W.\Psi_2; \cdot; W.\chi_2; W.\sigma_2; \rho_2(\mathbf{q}) \vdash (\texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot) : \rho_2(\tau_r); \rho_2(\sigma_r)$. Each follows from $\Psi; \Delta; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_1}$ and $\Psi; \Delta; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \texttt{ralloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}$ respectively using the component typing rule and the properties of W and ρ that we have by assumption.

- Consider arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_r; \sigma_r]\!]\rho$. We must show that

$$(W, E_1[(\texttt{ralloc}\,\mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\texttt{ralloc}\,\mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Let $M_1 = (\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1})$ and $M_2 = (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2})$.
From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\,\text{currentMR}(\theta) \mid \theta \in W.\Theta\,\}$. From the latter, we can have the following facts for island i_{stk}.
We have that $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \text{currentMR}(W(i_{\text{stk}}))$. From the latter it follows that $\mathbf{S_j} = W.\mathbf{S_j} = w_{j1} :: \cdots :: w_{jn} :: S'_j$.
Next, by the reduction semantics of our language, with all of the above facts in hand, we have that:

$$\langle M_1 \mid E_1[(\texttt{ralloc}\,\mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)]\rangle \longrightarrow \langle M'_1 \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle$$

and

$$\langle M_2 \mid E_2[(\texttt{ralloc}\,\mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \longrightarrow \langle M'_2 \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle$$

where $M'_1 = (\mathbf{H'_1}, \mathbf{R'_1}, \mathbf{S'_1})$ where $\mathbf{R'_1} = \mathbf{R_1}[r_d \mapsto \ell_1]$ and $\mathbf{H'_1} = \mathbf{H_1}[\ell_1 \mapsto \langle w_{11}, \cdots, w_{1n}\rangle]$, and where $M'_2 = (\mathbf{H'_2}, \mathbf{R'_2}, \mathbf{S'_2})$ where $\mathbf{R'_2} = \mathbf{R_2}[r_d \mapsto \ell_2]$ and $\mathbf{H'_2} = \mathbf{H_2}[\ell_2 \mapsto \langle w_{21}, \cdots, w_{2n}\rangle]$.
Note that, by the reduction semantics, $\ell_1 \notin dom(\mathbf{H_1})$ and $\ell_2 \notin dom(\mathbf{H_2})$.
Note that in order to complete our proof, it suffices to show:

$$\begin{array}{l}(\langle M'_1 \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge\ \langle M'_2 \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee \\ (\text{running}(W.k-1, \langle M'_1 \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge\ \text{running}(W.k-1, \langle M'_2 \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))\end{array}$$

Let $W' = (W.k, \mathbf{\Psi'_1}, \mathbf{\Psi'_2}, \Theta')$ where

1. $\mathbf{\Psi'_j} = \mathbf{\Psi_j}, \ell_{\mathbf{j}} : {}^{\mathbf{ref}}\langle \tau_{\mathbf{1}}, \cdots, \tau_{\mathbf{n}}\rangle$;
2. $|\Theta'| = |\Theta| + 1 = i_\ell$';
3. $\forall i \notin \{i_{\text{reg}}, i_{\text{stk}}, i_\ell\}.\, \Theta'(i) = W.\Theta(i)$;
4. $\Theta'(i_{\text{reg}}) = \text{island}_{\text{reg}}(s, W.k)$ with $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \ell_1], W.\boldsymbol{\chi_1}[\mathbf{r_d} : \rho_1(\mathbf{ref}\ \langle \tau_{\mathbf{1}}, \cdots, \tau_{\mathbf{n}}\rangle)], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \ell_2], W.\boldsymbol{\chi_2}[\mathbf{r_d} : \rho_2(\mathbf{ref}\ \langle \tau_{\mathbf{1}}, \cdots, \tau_{\mathbf{n}}\rangle)])$.
5. $\Theta'(i_{\text{stk}}) = \text{island}_{\text{stk}}(s, W.k)$ with $s = (\mathbf{S_1}, \boldsymbol{\sigma}, \mathbf{S_2}, \boldsymbol{\sigma})$;
6. $\Theta'(i_\ell)$ is such that $\forall W' \sqsupseteq W$.
$(\boldsymbol{\ell_1}, \boldsymbol{\ell_2}) \in W'(i_\ell).\text{bij}(W'(i_\ell).s)\ \wedge$
$\exists \varphi_M.\ \text{currentMR}(W'(i_\ell)) = \varphi_M\ \otimes$
$\{\,(\widetilde{W}, \{\boldsymbol{\ell_1} \mapsto \mathbf{h_1}\}\restriction, \{\boldsymbol{\ell_2} \mapsto \mathbf{h_2}\}\restriction) \in \text{MemAtom} \mid\ (\widetilde{W}, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \tau_{\mathbf{1}}, \cdots, \tau_{\mathbf{n}}\rangle]\!]\rho\,\}$

We claim that $W' \in \text{World}$. Recall that we have $(W, w_{1i}, w_{2i}) \in \mathcal{W}[\![\tau_i]\!]\rho$. Thus we have that $W.\Psi_j; \cdot \vdash w_{ji} : \rho_j(\tau_i)$. Given our choice of W' and since $W \in \text{World}$, it follows that $W'.\Psi_j; \cdot \vdash w_{ji} : \rho_j(\tau_i)$ which is sufficient to establish our claim.
Moreover, note that $W' \sqsupseteq W$ and $W' \sqsupseteq_{\text{pub}} W$. Both follow immediately given our choice of W' and the definition of $\text{island}_{\text{reg}}$, and $\text{island}_{\text{stk}}$.
We proceed by showing that $(M'_1, M'_2) : W'$ and then instantiating our final hypothesis

$$\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}[\mathbf{r_d} : \mathbf{ref}\ \langle \overline{\tau}\rangle]; \boldsymbol{\sigma}; \text{dec}(\mathbf{q}, \mathbf{n}) \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$$

  - We claim that $(M'_1, M'_2) : W'$. We prove this claim by establishing the following:
    - $\vdash M'_1 : W'.\Phi_1$ and $\vdash M'_2 : W'.\Phi_2$. Note the following facts:
      - $W'.\boldsymbol{\chi_1} = W.\boldsymbol{\chi_1}[\mathbf{r_d} : \rho_1(\tau_{\mathbf{i}})]$ and $W'.\boldsymbol{\chi_2} = W.\boldsymbol{\chi_2}[\mathbf{r_d} : \rho_2(\tau_{\mathbf{i}})]$;
      - $W'.\boldsymbol{\sigma_1} = \sigma$ and $W'.\boldsymbol{\sigma_2} = \sigma$;
      - $W'.\mathbf{\Psi_1} = W.\mathbf{\Psi_1}, \ell_1 : {}^{ref}\langle \tau_1, \cdots, \tau_n\rangle$ and $W'.\mathbf{\Psi_2} = W.\mathbf{\Psi_2}, \ell_2 : {}^{ref}\langle \tau_1, \cdots, \tau_n\rangle$.

Both claims follow easily from $(M_1, M_2) : W$, the above facts, the fact that we have initialized location $\boldsymbol{\ell}$ in both memories with well-typed words, i.e., with tuples of types $\rho_1(\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle)$ and $\rho_2(\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle)$, and the fact that we have updated registers r_d to hold locations that point to well-typed words, i.e., the locations $\boldsymbol{\ell_1}$ and $\boldsymbol{\ell_2}$ that point to words of types $\rho_1(\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle)$ and $\rho_2(\langle \boldsymbol{\tau_0}, \ldots, \boldsymbol{\tau_n} \rangle)$.

∗ We assume that $W.k > 0$ (and thus $W'.k > 0$). We must show that

$$(\triangleright W', M_1', M_2') \in \bigotimes \{ \text{currentMR}(\theta) \mid \theta \in W'.\Theta \}$$

The latter follows from $(M_1, M_2) : W$ and monotonicity of MemRel given that we establish the following claims:

1. For island i_{reg}, $(\triangleright W', \mathbf{W.R_1[r_d \mapsto w_{1i}]}\restriction, \mathbf{W.R_2[r_d \mapsto w_{2i}]}\restriction) \in \text{currentMR}(W'(i_{\text{reg}}))$;
2. For island i_{stk}, $(\triangleright W', S_1', S_2') \in \text{currentMR}(W'(i_{\text{stk}}))$;
3. For island i_ℓ, $(\triangleright W', \{\boldsymbol{\ell_1} \mapsto \langle \mathbf{w_{11}}, \cdots, \mathbf{w_{1n}} \rangle\}\restriction, \{\boldsymbol{\ell_2} \mapsto \langle \mathbf{w_{21}}, \cdots, \mathbf{w_{2n}} \rangle\}\restriction) \in \text{currentMR}(\Theta'(i_\ell))$.

For the first claim recall that $W'.R_j = W.R_j[r_d \mapsto w_{ji}]$. Thus we obtain trivially that $(\triangleright W', W.R_1[r_d \mapsto w_{1i}], W.R_2[r_d \mapsto w_{2i}]) \in \{(\widetilde{W}, W'.R_1, W'.R_2) \mid \widetilde{W} \in \text{World}_{W.k}\}$.
From the latter, we establish directly our claim that

$$(\triangleright W', \mathbf{W.R_1[r_d \mapsto w_{1i}]}\restriction, \mathbf{W.R_2[r_d \mapsto w_{2i}]}\restriction) \in \text{currentMR}(W'(i_{\text{reg}}))$$

For the second claim recall that $W'.S_i = S_i'$. Thus we obtain trivially that $(\triangleright W', S_1', S_2') \in \{(\widetilde{W}, W'.S_1, W'.S_2) \mid \widetilde{W} \in \text{World}_{W.k}\}$. From the latter, we establish directly our claim that

$$(\triangleright W', S_1', S_2') \in \text{currentMR}(W'(i_{\text{stk}}))$$

For the fourth claim recall that we have $(W, w_{1i}, w_{2i}) \in \mathcal{W}[\![\boldsymbol{\tau_i}]\!]\rho$. Thus, from monotonicity (lemma 1.8), we obtain $(\triangleright W', w_{1i}, w_{2i}) \in \mathcal{W}[\![\boldsymbol{\tau_i}]\!]\rho$. Moreover, by construction island $W'(i_\ell)$ is such that $\forall W' \sqsupseteq W$.
$(\boldsymbol{\ell_1}, \boldsymbol{\ell_2}) \in W'(i_\ell).\text{bij}(W'(i_\ell).s) \ \wedge$
$\exists \varphi_M.\ \text{currentMR}(W'(i_\ell)) = \varphi_M \ \otimes$
$\{ (\widetilde{W}, \{\boldsymbol{\ell_1} \mapsto \mathbf{h_1}\}\restriction, \{\boldsymbol{\ell_2} \mapsto \mathbf{h_2}\}\restriction) \in \text{MemAtom} \mid \ (\widetilde{W}, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\langle \boldsymbol{\tau_1}, \cdots, \boldsymbol{\tau_n} \rangle]\!]\rho \}$
From the latter, we establish directly our claim that

$$(\triangleright W', \{\boldsymbol{\ell_1} \mapsto \langle \mathbf{w_{11}}, \cdots, \mathbf{w_{1n}} \rangle\}\restriction, \{\boldsymbol{\ell_2} \mapsto \langle \mathbf{w_{21}}, \cdots, \mathbf{w_{2n}} \rangle\}\restriction) \in \text{currentMR}(\Theta'(i_l))$$

– Next, we instantiate our final hypothesis with W' and ρ. Note that $\rho \in \mathcal{D}[\![\boldsymbol{\Delta}]\!]$ by assumption, $W' \in \mathcal{H}[\![\boldsymbol{\Psi}]\!]$ by heap monotonicity (Lemma 1.9). Let W'' that is the same as W' but $W''(i_{\text{stk}}) = W(i_{\text{stk}})$ $W'(i_{\text{stk}}) = W(i_{\text{stk}})$. We claim that $\text{currentMR}(W''(i_{\text{stk}})) \Subset_{W''} \mathcal{S}[\![\boldsymbol{\tau_1} :: \cdots :: \boldsymbol{\tau_n} :: \boldsymbol{\sigma}]\!]\rho$ by the first case of lemma 1.21 and $\text{currentMR}(W''(i_{\text{reg}})) \Subset_{W''} \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$ by the first case of lemma 1.20. Let W''' that is the same as W'' but $W'''(i_i stk) = W'(i_i stk)$. Clearly $W''' \sqsupseteq W''$ and $W' \sqsupseteq W'''$. We claim that $\text{currentMR}(W'''(i_{\text{stk}})) \Subset_{W'''} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ by the second case of lemma 1.21 since $W'''(i_{\text{stk}}) = \text{island}_{\text{stk}}(s, W.k)$ with $s = (S_1, \sigma, S_2, \sigma)$ where $W''(i_{\text{stk}}) = \text{island}_{\text{stk}}(s, W.k)$ with $s = (w_{11} :: \cdots :: w_{1n} :: S_1, \tau_1 :: \cdots :: \tau_n :: \sigma, w_{21} :: \cdots :: w_{2n} :: S_2, \tau_1 :: \cdots :: \tau_n :: \sigma)$. Moreover we claim that $\text{currentMR}(W'''(i_{\text{reg}})) \Subset_{W'''} \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$ by the first case of Lemma 1.20. Finaly, we claim that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ and $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau_i}]]\!]\rho$. The first follows directly from the first case of lemma 1.21 since we have shown that $\text{currentMR}(W'''(i_{\text{stk}})) \Subset_{W'''} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ and $W' \sqsupseteq W'''$. The second follows directly from the second case of lemma 1.20 since, above, we have established that $(W', w_{1i}, w_{2i}) \in \mathcal{W}[\![\boldsymbol{\tau_i}]\!]$ and $\text{currentMR}(W''(i_{\text{reg}})) \Subset_{W''} \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$, and $W' \sqsupseteq W'''$. Hence, we have that

$$(W', (\rho_1(\mathbf{I_1}, \cdot)), (\rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau_r}; \boldsymbol{\sigma_r}]\!]\rho$$

Instantiate the above with E_1 and E_2. Note that we have $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau_r}; \boldsymbol{\sigma_r}]\!]\rho$ which follows from $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau_r}; \boldsymbol{\sigma_r}]\!]\rho$ by monotonicity for evaluation contexts

(Lemma 1.10), since our choice of W', $W' \sqsupseteq_{\text{pub}} W$ and our third hypothesis, $\mathbf{q} \neq \mathbf{r_d}$, and the preliminary fact that if $\mathbf{q} = \mathbf{i}$ then $\mathbf{i} \geq \mathbf{n}$ let us easily establish all the premises of that lemma.
Hence, we have

$$(W', E_1[(\rho_1(\mathbf{I_1}, \cdot))], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Instantiate the latter with M_1' and M_2', noting that $(M_1', M_2') : W'$. Hence, we have

$$\begin{array}{l}(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee \\ (\text{running}(W.k, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))\end{array}$$

which implies what we needed to show.

□

Lemma 1.49 (Allocate Immutable Tuple)
If $\text{len}(\overline{\tau}) = \mathbf{n}$, $\mathbf{q} \neq \mathbf{r_d}$, and $\mathbf{\Psi}; \mathbf{\Delta}; \chi[\mathbf{r_d} : \mathbf{box}\ \langle\overline{\tau}\rangle]; \sigma; \text{dec}(\mathbf{q}, \mathbf{n}) \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$,
then $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}$.

Proof

Clearly, $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\overline{\tau} :: \sigma]\!]\rho$. We need to show that

$$\begin{array}{l}(W, \rho_1((\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}, \cdot))) \\ \qquad = (W, (\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \overline{\tau} :: \sigma)]\!]\rho.\end{array}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i]\rangle$.

In the following, assume $W.k > 0$ and let $\tau_{\mathbf{r}}; \sigma_{\mathbf{r}} = \text{ret-type}(\mathbf{q}, \chi, \sigma)$.

We proceed by unfolding the definition of $\mathcal{E}[\![\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\!]\rho$ and proving the resulting obligations:

- $(W, (\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\rho$. From the definitions of $\text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\rho$ and $\text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]$, it suffices to show $W.\Psi_1; \cdot; W.\chi_{\mathbf{1}}; W.\sigma_{\mathbf{1}}; \rho_1(\mathbf{q}) \vdash (\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot) : \rho_1(\tau_{\mathbf{r}}); \rho_1(\sigma_{\mathbf{r}})$ and $W.\Psi_2; \cdot; W.\chi_{\mathbf{2}}; W.\sigma_{\mathbf{2}}; \rho_2(\mathbf{q}) \vdash (\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot) : \rho_2(\tau_{\mathbf{r}}); \rho_2(\sigma_{\mathbf{r}})$. Each follows from $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \overline{\tau} :: \sigma; \mathbf{q} \vdash \mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}$ respectively using the component typing rule and the properties of W and ρ that we have by assumption.
- For arbitrary E_1 and E_2, $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_r; \sigma_{\mathbf{r}}]\!]\rho$ implies

  $$(W, E_1[(\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

  From the definition of $\mathcal{O}$, this requires to show that given arbitrary $(M_1, M_2) : W$, $\langle M_1 \mid E_1[(\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow$ iff $\langle M_2 \mid E_2[(\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow$. We proceed by running each expression for one step and then using the resulting memories, to construct a world that we can then use with our second hypothesis, $\mathbf{\Psi}; \mathbf{\Delta}; \chi[\mathbf{r_d} : \mathbf{ref}\ \langle\overline{\tau}\rangle]; \sigma; \text{dec}(\mathbf{q}, \mathbf{n}) \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$:
  - Assume that our two arbitrary memories are of the form $M_1 = (H_1, R_1, S_1)$ and $M_2 = (H_2, R_2, S_2)$.
    From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \text{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$. From the latter, we have the following fact for island i_{stk}: $(\triangleright W, \mathbf{S_1} \restriction, \mathbf{S_2} \restriction) \in \text{currentMR}(W(i_{\text{stk}}))$. From the latter it follows that $\mathbf{S_i} = W.\mathbf{S_i}$.
    From the reduction semantics of our language we obtain that:

    $$\langle M_1 \mid E_1[(\mathtt{balloc}\ \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)]\rangle \longrightarrow \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle$$

and

$$\langle M_2 \mid E_2[(\texttt{balloc}\,\mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \longrightarrow \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle$$

where $M_1' = (\mathbf{H_1'}, \mathbf{R_1'}, \mathbf{S_1'})$ with $\mathbf{R_1'} = \mathbf{R_1}[r_d \mapsto \ell_1]$, $\mathbf{H_1'} = \mathbf{H_1}[\ell_1 \mapsto \overline{w_1}]$ and $\mathbf{S_1} = \overline{w_1} :: \mathbf{S_1'}$, and $M_2' = (\mathbf{H_2'}, \mathbf{R_2'}, \mathbf{S_2'})$ with $\mathbf{R_2'} = \mathbf{R_2}[r_d \mapsto \ell_1]$, $\mathbf{H_2'} = \mathbf{H_2}[\ell_1 \mapsto \overline{w_2}]$ and $\mathbf{S_2} = \overline{w_2} :: \mathbf{S_2'}$.

– Let $s_{reg} = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \ell_1], W.\chi_1[\mathbf{r_d} : \rho_1(\mathbf{box}\,\langle\overline{\tau}\rangle)], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \ell_2], W.\chi_2[\mathbf{r_d} : \rho_2(\mathbf{box}\,\langle\overline{\tau}\rangle)])$, $s_{box} = (W.\mathbf{H_1}[\ell_1 \mapsto \overline{w_1}], W.\mathbf{H_2}[\ell_2 \mapsto \overline{w_2}])$ and $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\text{reg}} \mapsto \text{island}_{\text{reg}}(s_{reg}, W.k), i_{\text{bo}}$ $\text{island}_{\text{box}}(s_{box}, W.k)])$ where $W.\mathbf{S_i} = \overline{w_i} :: \mathbf{S_i'}$.

– We claim that $W' \in \text{World}$. From the restriction $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\overline{\tau} :: \sigma]\!]\rho$, we have that

$$(W, W.\mathbf{S_1}(j), W.\mathbf{S_2}(j)) \in \mathcal{W}[\![\tau_j]\!]\rho$$

for $j \in \{1..n\}$.
And thus $(W, \overline{w_1}, \overline{w_2}) \in \mathcal{HV}[\![\langle\overline{\tau}\rangle]\!]\rho$.
Thus we have that $W.\Psi_i; \cdot \vdash \ell_i : \rho_i(\mathbf{box}\,\langle\overline{\tau}\rangle)$ and $W.\Psi_i \vdash \overline{w_i} :^{box} \rho_i(\langle\overline{\tau}\rangle)$.
Given our choice of W' and since $W \in \text{World}$, it follows that $W'.\Psi_i; \cdot \vdash W.\hat{\mathbf{R}}_i(\rho_i(\mathbf{u_i})) : \rho_i(\tau)$ which is sufficient to establish our claim.

– Next, to use our third hypothesis, we note that $W' \in \mathcal{H}[\![\Psi]\!]$ by heap monotonicity (Lemma 1.9) and that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\overline{\tau} :: \sigma]\!]\rho$ by Lemma 1.21 since $W'(i_{\text{stk}}) = W(i_{\text{stk}})$. We also claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\mathbf{r_d} : \mathbf{box}\,\langle\overline{\tau}\rangle]]\!]\rho$. We have that $(W, \ell_1, \ell_2) \in \mathcal{W}[\![\mathbf{box}\,\langle\overline{\tau}\rangle]\!]\rho$. Hence, by monotonicity and the definition of W' we have

$$(W', \ell_1, \ell_2) = (W', W'.\mathbf{R_1}(\mathbf{r_d}), W'.\mathbf{R_2}(\mathbf{r_d})) \in \mathcal{W}[\![\mathbf{box}\,\langle\overline{\tau}\rangle]\!]\rho,$$

which, using Lemma 1.20, is sufficient to establish our claim.
Therefore we can apply our third hypothesis to W' and ρ, finding that

$$(W', \rho_1((\mathbf{I_1}, \cdot)), \rho_2((\mathbf{I_2}, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

– By unfolding that definition we derive that given $(M_1'', M_2'') : W'$, $(W', E_1[(\rho_1(\mathbf{I_1}), \cdot)], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}$. By construction $(M_1', M_2') : W'$ and thus by unfolding the definition of $\mathcal{O}$, we obtain $\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow$ and $\langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow$, or $\text{running}(W'.k, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle)$ and $\text{running}(W'.k, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle)$. In the first case, it is straightforward to derive from the reduction semantics that $\langle M_1 \mid E_1[(\texttt{balloc}\,\mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow$ and $\langle M_2 \mid E_2[(\texttt{balloc}\,\mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow$. In the second case, since $W'.k = W.k$, we derive that $\text{running}(W.k, \langle M_1 \mid E_1[(\texttt{balloc}\,\mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)]\rangle$ and $\text{running}(W.k, \langle M_2 \mid E_2[(\texttt{balloc}\,\mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]\rangle$. Thus we conclude that:

$$(W, E_1[(\texttt{balloc}\,\mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\texttt{balloc}\,\mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

□

Lemma 1.50 (Move)
If $\Psi; \Delta; \chi \vdash \mathbf{u_1} \approx_{\text{u}} \mathbf{u_2} : \tau$, $\mathbf{q} \neq \mathbf{r_d}$, and $\Psi; \Delta; \chi[\mathbf{r_d} : \tau]; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\text{I}} \mathbf{I_2}$,
then $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \texttt{mv}\,\mathbf{r_d}, \mathbf{u_1}; \mathbf{I_1} \approx_{\text{I}} \texttt{mv}\,\mathbf{r_d}, \mathbf{u_2}; \mathbf{I_2}$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \texttt{mv}\,\mathbf{r_d}, \mathbf{u_1}; \mathbf{I_1}$ and $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \texttt{mv}\,\mathbf{r_d}, \mathbf{u_2}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$(W, \rho_1((\texttt{mv}\,\mathbf{r_d}, \mathbf{u_1}; \mathbf{I_1}, \cdot)), \rho_2((\texttt{mv}\,\mathbf{r_d}, \mathbf{u_2}; \mathbf{I_2}, \cdot))) = (W, (\texttt{mv}\,\mathbf{r_d}, \rho_1(\mathbf{u_1}); \rho_1(\mathbf{I_1}), \cdot), (\texttt{mv}\,\mathbf{r_d}, \rho_2(\mathbf{u_2}); \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i]\rangle$.

In the following, assume $W.k > 0$ and let $\tau_r; \sigma_r = \text{ret-type}(\mathbf{q}, \chi, \sigma)$.

We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

- We claim that $(W, (\texttt{mv}\ \mathbf{r_d}, \rho_1(\mathbf{u_1}); \rho_1(\mathbf{I_1}), \cdot), (\texttt{mv}\ \mathbf{r_d}, \rho_2(\mathbf{u_2}); \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_r; \sigma_r]\rho$. To establish this, we must show $W.\Psi_i; \cdot; W.\chi_i; W.\sigma_i; \rho_i(\mathbf{q}) \vdash (\texttt{mv}\ \mathbf{r_d}, \rho_i(\mathbf{u_i}); \rho_i(\mathbf{I_i}), \cdot) : \rho_i(\tau_r); \rho_i(\sigma_r)$. The latter follows from $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \texttt{mv}\ \mathbf{r_d}, \mathbf{u_i}; \mathbf{I_i}$ using the component typing rule and the properties of W and ρ that we have by assumption.
- Let $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto W.\hat{\mathbf{R}}_\mathbf{1}(\rho_1(\mathbf{u_1}))], W.\chi_1[\mathbf{r_d} : \rho_1(\tau)], W.\mathbf{R_2}[\mathbf{r_d} \mapsto W.\hat{\mathbf{R}}_\mathbf{2}(\rho_1(\mathbf{u_2}))], W.\chi_2[\mathbf{r_d} : \rho_2(\tau)])$ and $W' = (W.k, W.\mathbf{\Psi_1}, W.\mathbf{\Psi_2}, W.\Theta[i_{\text{reg}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$.
- We claim that $W' \in \text{World}$. Instantiating the first hypothesis with W and ρ, we have that

  $$(W, W.\hat{\mathbf{R}}_\mathbf{1}(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_\mathbf{2}(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\tau]\!]\rho$$

  Thus we have that $W.\Psi_i; \cdot \vdash W.\hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i})) : \rho_i(\tau)$. Given our choice of W' and since $W \in \text{World}$, it follows that $W'.\Psi_i; \cdot \vdash W.\hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i})) : \rho_i(\tau)$ which is sufficient to establish our claim.
- Note that $W' \sqsupseteq_{\text{pub}} W$. The latter is immediate given our choice of W' and the definition of $\text{island}_{\text{reg}}$.
- Consider arbitrary $(M_1, M_2) : W$. Let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{ \text{currentMR}(\theta) \mid \theta \in W.\Theta \}$. From the latter, we have the following fact for island i_{reg}: $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i})) = W.\hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i}))$.
  Note that

  $$\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\texttt{mv}\ \mathbf{r_d}, \rho_i(\mathbf{u_i}); \rho_i(\mathbf{I_i}), \cdot) \rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i}))], \mathbf{S_i}) \mid (\rho_i(\mathbf{I_i}), \cdot) \rangle$$

  Let $M_i' = (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i}))], \mathbf{S_i})$. Given our choice of W', since $\mathbf{R_i} = W.\mathbf{R_i}$, we have that $(M_1', M_2') : W'$.
- Note that $W.k \leq W'.k + 1$.
- Note that $\mathbf{q} \neq \epsilon$, which follows from the third hypothesis since it is a side condition of the instruction typing rules. Further, since $\mathbf{q} \neq \mathbf{r_d}$, which was the only memory location changed between W and W', we can see that the the return address does not change.
- Next, to use our third hypothesis, we note that $W' \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ by heap monotonicity (Lemma 1.9) and that $\text{currentMR}(W'(i_{\text{stk}})) \Subset W'\mathcal{S}[\![\sigma]\!]\rho$ by Lemma 1.21 since $W'(i_{\text{stk}}) = W(i_{\text{stk}})$. We also claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\mathbf{r_d} : \tau]]\!]\rho$. From above, we have that $(W, W.\hat{\mathbf{R}}_\mathbf{1}(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_\mathbf{2}(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\tau]\!]\rho$. Hence, by monotonicity and the definition of W' we have

  $$(W', W.\hat{\mathbf{R}}_\mathbf{1}(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_\mathbf{2}(\rho_2(\mathbf{u_2}))) = (W', W'.\mathbf{R_1}(\mathbf{r_d}), W'.\mathbf{R_2}(\mathbf{r_d})) \in \mathcal{W}[\![\tau]\!]\rho,$$

  which, using Lemma 1.20, is sufficient to establish our claim.
  Therefore we can apply our third hypothesis to W' and ρ, finding that

  $$(W', \rho_1((\mathbf{I_1}, \cdot)), \rho_2((\mathbf{I_2}, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

Now, the result follows by Lemma 1.11. □

Lemma 1.51 (Move Return Address)
If $\chi(\mathbf{r_s}) = \tau$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi[\mathbf{r_d} : \tau]; \sigma; \mathbf{r_d} \vdash \mathbf{I_1} \approx_\mathbf{I} \mathbf{I_2}$, then $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{r_s} \vdash \texttt{mv}\ \mathbf{r_d}, \mathbf{r_s}; \mathbf{I_1} \approx_\mathbf{I} \texttt{mv}\ \mathbf{r_d}, \mathbf{r_s}; \mathbf{I_2}$.

Proof

Clearly, $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{r_s} \vdash \texttt{mv}\ \mathbf{r_d}, \mathbf{r_s}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{r_s} \vdash \texttt{mv}\ \mathbf{r_d}, \mathbf{r_s}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$(W, \rho_1((\texttt{mv}\ \mathbf{r_d}, \mathbf{r_s}; \mathbf{I_1}, \cdot)), \rho_2((\texttt{mv}\ \mathbf{r_d}, \mathbf{r_s}; \mathbf{I_2}, \cdot))) = (W, (\texttt{mv}\ \mathbf{r_d}, \mathbf{r_s}; \rho_1(\mathbf{I_1}), \cdot), (\texttt{mv}\ \mathbf{r_d}, \mathbf{r_s}; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{r_s} \vdash \text{ret-type}(\mathbf{r_s}, \chi, \sigma)]\!]\rho.$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that running$(0, \langle M_i \mid E_i[e_i] \rangle)$.

In the following, assume $W.k > 0$ and let $\boldsymbol{\tau_r}; \boldsymbol{\sigma_r} = \text{ret-type}(\mathbf{r_s}, \boldsymbol{\chi}, \boldsymbol{\sigma})$.

We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

- We claim that $(W, (\mathtt{mv}\, \mathbf{r_d}, \mathbf{r_s}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{mv}\, \mathbf{r_d}, \mathbf{r_s}; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{r_s} \vdash \boldsymbol{\tau_r}; \boldsymbol{\sigma_r}]\rho$. To establish this, we must show $W.\Psi_i; \cdot; W.\boldsymbol{\chi_i}; W.\boldsymbol{\sigma_i}; \mathbf{r_s} \vdash (\mathtt{mv}\, \mathbf{r_d}, \mathbf{r_s}; \rho_i(\mathbf{I_i}), \cdot) : \rho_i(\boldsymbol{\tau_r}); \rho_i(\boldsymbol{\sigma_r})$. The latter follows from $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{r_s} \vdash \mathtt{mv}\, \mathbf{r_d}, \mathbf{r_s}; \mathbf{I_i}$ using the component typing rule and the properties of W and ρ that we have by assumption.
- Let $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto W.\mathbf{R_1}(\mathbf{r_s})], W.\boldsymbol{\chi_1}[\mathbf{r_d} : \rho_1(\boldsymbol{\tau})], W.\mathbf{R_2}[\mathbf{r_d} \mapsto W.\mathbf{R_2}(\mathbf{r_s})], W.\boldsymbol{\chi_2}[\mathbf{r_d} : \rho_2(\boldsymbol{\tau})])$ and $W' = (W.k, W.\boldsymbol{\Psi_1}, W.\boldsymbol{\Psi_2}, W.\Theta[i_{\text{reg}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$.
- We claim that $W' \in \text{World}$. By our first hypothesis, we have that $(\mathbf{r_s} : \boldsymbol{\tau}) \in \boldsymbol{\chi}$. It then follows from currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$ and the definition of $\text{island}_{\text{reg}}$ that

  $$(W, W.\mathbf{R_1}(\mathbf{r_s}), W.\mathbf{R_2}(\mathbf{r_s})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$$

  Thus we have that $W.\Psi_i; \cdot \vdash W.\mathbf{R_i}(\mathbf{r_s}) : \rho_i(\boldsymbol{\tau})$. Given our choice of W' and since $W \in \text{World}$, it follows that $W'.\Psi_i; \cdot \vdash W.\mathbf{R_i}(\mathbf{r_s}) : \rho_i(\boldsymbol{\tau})$ which is sufficient to establish our claim.
- Note that $W' \sqsupseteq_{\text{pub}} W$. The latter is immediate given our choice of W' and the definition of $\text{island}_{\text{reg}}$.
- Consider arbitrary $(M_1, M_2) : W$. Let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{ \text{currentMR}(\theta) \mid \theta \in W.\Theta \}$. From the latter, we have the following fact for island i_{reg}: $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$.
  Note that

  $$\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\mathtt{mv}\, \mathbf{r_d}, \mathbf{r_s}; \rho_i(\mathbf{I_i}), \cdot) \rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \mathbf{R_i}(\mathbf{r_s})], \mathbf{S_i}) \mid (\rho_i(\mathbf{I_i}), \cdot) \rangle)$$

  Let $M_i' = (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \mathbf{R_i}(\mathbf{r_s})], \mathbf{S_i})$. Given our choice of W', since $\mathbf{R_i} = W.\mathbf{R_i}$, we have that $(M_1', M_2') : W'$.
- Note that $W.k \leq W'.k + 1$.
- Note that $\text{ret-addr}_1(W, \mathbf{r_s}) = \text{ret-addr}_1(W', \mathbf{r_d})$ and $\text{ret-addr}_2(W, \mathbf{r_s}) = \text{ret-addr}_2(W', \mathbf{r_d})$.
- Next, to use our second hypothesis, we note that $W' \in \mathcal{H}[\![\boldsymbol{\Psi}]\!]$ by heap monotonicity (Lemma 1.9) and that currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ by Lemma 1.21 since $W'(i_{\text{stk}}) = W(i_{\text{stk}})$. We also claim that currentMR$(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau}]]\!]\rho$. From $(W, W.\mathbf{R_1}(\mathbf{r_s}), W.\mathbf{R_2}(\mathbf{r_s})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$ by monotonicity and the definition of W', we have

  $$(W', W.\mathbf{R_1}(\mathbf{r_s}), W.\mathbf{R_2}(\mathbf{r_s})) = (W', W'.\mathbf{R_1}(\mathbf{r_d}), W'.\mathbf{R_2}(\mathbf{r_d})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho,$$

  which, using Lemma 1.20, is sufficient to establish our claim.
  Therefore we can apply our second hypothesis to W' and ρ, finding that

  $$(W', \rho_1((\mathbf{I_1}, \cdot)), \rho_2((\mathbf{I_2}, \cdot))) \in \mathcal{E}[\![\mathbf{r_d} \vdash \text{ret-type}(\mathbf{r_d}, \boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau}], \boldsymbol{\sigma})]\!]\rho = \mathcal{E}[\![\mathbf{r_d} \vdash \text{ret-type}(\mathbf{r_s}, \boldsymbol{\chi}, \boldsymbol{\sigma})]\!]\rho.$$

Now, the result follows by Lemma 1.11. □

Lemma 1.52 (Unpack)
If $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi} \vdash \mathbf{u_1} \approx_{\text{u}} \mathbf{u_2} : \exists \boldsymbol{\alpha}.\boldsymbol{\tau}$, $\mathbf{q} \neq \mathbf{r_d}$, and $\boldsymbol{\Psi}; \boldsymbol{\Delta}, \boldsymbol{\alpha}; \boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau}]; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathbf{I_1} \approx_{\text{I}} \mathbf{I_2}$,
then $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{unpack}\, \langle \boldsymbol{\alpha}, \mathbf{r_d} \rangle\, \mathbf{u_1}; \mathbf{I_1} \approx_{\text{I}} \mathtt{unpack}\, \langle \boldsymbol{\alpha}, \mathbf{r_d} \rangle\, \mathbf{u_2}; \mathbf{I_2}$.

Proof

Clearly, $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \mathbf{u_1}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \mathbf{u_2}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$(W, \rho_1((\texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \mathbf{u_1}; \mathbf{I_1}, \cdot)), \rho_2((\texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \mathbf{u_2}; \mathbf{I_2}, \cdot)))$$
$$= (W, (\texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \rho_1(\mathbf{u_1}); \rho_1(\mathbf{I_1}), \cdot), (\texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \rho_2(\mathbf{u_2}); \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i] \rangle$.

In the following, assume $W.k > 0$ and let $\tau_{\mathbf{r}}; \sigma_{\mathbf{r}} = \text{ret-type}(\mathbf{q}, \chi, \sigma)$.

We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

- We claim that $(W, (\texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \rho_1(\mathbf{u_1}); \rho_1(\mathbf{I_1}), \cdot), (\texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \rho_2(\mathbf{u_2}); \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\rho$. To establish this, we must show $W.\Psi_i; \cdot; W.\chi_{\mathbf{i}}; W.\sigma_{\mathbf{i}}; \rho_i(\mathbf{q}) \vdash (\texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \rho_i(\mathbf{u_i}); \rho_i(\mathbf{I_i}), \cdot) : \rho_i(\tau_{\mathbf{r}}); \rho_i(\sigma_{\mathbf{r}})$. The latter follows from $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \mathbf{q} \vdash \texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \mathbf{u_i}; \mathbf{I_i}$ using the component typing rule and the properties of W and ρ that we have by assumption.
- Let $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \mathbf{w_1}], W.\chi_{\mathbf{1}}[\mathbf{r_d} : \rho_1(\tau)], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \mathbf{w_2}], W.\chi_{\mathbf{2}}[\mathbf{r_d} : \rho_2(\tau)])$ where $W.\hat{\mathbf{R}}_{\mathbf{i}}(\mathbf{u_i}) = \mathbf{pack}\langle \tau', \mathbf{w_i} \rangle\ \mathbf{as}\ \exists \alpha.\tau$ and $W' = (W.k, W.\mathbf{\Psi_1}, W.\mathbf{\Psi_2}, W.\Theta[i_{\text{reg}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$.
- We claim that $W' \in \text{World}$. Instantiating the first hypothesis with W and ρ, we have that
$$(W, W.\hat{\mathbf{R}}_{\mathbf{1}}(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_{\mathbf{2}}(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\exists \alpha.\tau]\!]\rho$$
Thus we have that $W.\Psi_i; \cdot \vdash W.\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) : \rho_i(\exists \alpha.\tau)$. Given our choice of W' and since $W \in \text{World}$, it follows that $W'.\Psi_i; \cdot \vdash W.\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) : \rho_i(\exists \alpha.\tau)$ which is sufficient to establish our claim.
- Note that $W' \sqsupseteq_{\text{pub}} W$. The latter is immediate given our choice of W' and the definition of $\text{island}_{\text{reg}}$.
- Consider arbitrary $(M_1, M_2) : W$. Let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$.
From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{ \text{currentMR}(\theta) \mid \theta \in W.\Theta \}$. From the latter, we have the following fact for island i_{reg}: $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$.
Note that
$$\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\texttt{unpack}\ \langle \alpha, \mathbf{r_d} \rangle\ \rho_i(\mathbf{u_i}); \rho_i(\mathbf{I_i}), \cdot) \rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \mathbf{w_i}], \mathbf{S_i}) \mid (\rho_i[\alpha \mapsto \tau'](\mathbf{I_i}), \cdot) \rangle$$
Where $W.\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) = \mathbf{pack}\langle \tau', \alpha \rangle\ \mathbf{as}\ \exists \alpha.\tau$. Let $M_i' = (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \mathbf{w_i}], \mathbf{S_i})$. Note that $(M_1', M_2') : W'$.
- Note that $W.k \leq W'.k + 1$.
- Note that $\mathbf{q} \neq \epsilon$, which follows from the third hypothesis since it is a side condition of the instruction typing rules. Further, since $\mathbf{q} \neq \mathbf{r_d}$, which was the only memory location changed between W and W', we can see that the the return address does not change.
- Next, to use our third hypothesis, we note that $W' \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ by heap monotonicity (Lemma 1.9).
From above, we have that $(W, W.\hat{\mathbf{R}}_{\mathbf{1}}(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_{\mathbf{2}}(\rho_2(\mathbf{u_2}))) = (W, pack\langle \tau', w_1 \rangle\ as\ \rho_1(\exists \alpha.\tau), pack\langle \tau', w_1 \rangle\ as\ \rho_1(\exists \alpha.\tau$ $\mathcal{W}[\![\exists \alpha.\tau]\!]\rho$.
From the definition of $\mathcal{W}[\![\exists \alpha.\tau]\!]\rho$, we have that $(W, w_1, w_2) \in \mathcal{W}[\![\tau]\!]\rho[\alpha \mapsto (\tau', \tau', \varphi_w)]$ for some φ_w.
We choose $\rho' = \rho[\alpha \mapsto (\tau', \tau', \varphi_w)] \in \mathcal{D}[\![\mathbf{\Delta}, \alpha]\!]$.
We claim that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho'$. From Lemma 1.21 we have $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'}$ $\mathcal{S}[\![\sigma]\!]\rho$ since $W'(i_{\text{stk}}) = W(i_{\text{stk}})$. From substitution, we know that $\mathcal{S}[\![\sigma]\!]\rho' = \mathcal{S}[\![\sigma[\tau'/\alpha]]\!]\rho$. Since σ is well-formed under $\mathbf{\Delta}$, α is not free and thus $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho'$.
We also claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\mathbf{r_d} : \tau]]\!]\rho'$. From substitution, since χ is well-formed under Δ, we know that this is equivalent to $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\mathbf{r_d} : \tau[\tau'/\alpha]]]\!]\rho$.

We can use Lemma 1.20 provided we can show that $(W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau[\tau'/\alpha]]\!]\rho$. But this, via substitution, is equivalent to showing that $(W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho'$, which we have from the first hypothesis.

Therefore we can apply our third hypothesis to W' and ρ', finding that

$$(W', \rho_1'((\mathbf{I_1}, \cdot)), \rho_2'((\mathbf{I_2}, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho'.$$

Now, the result follows by Lemma 1.11.

□

Lemma 1.53 (Unfold)
If $\Psi; \Delta; \chi \vdash \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{u_2} : \mu\alpha.\tau$, $\mathbf{q} \neq \mathbf{r_d}$, and $\Psi; \Delta; \chi[\mathbf{r_d} : \tau[\mu\alpha.\tau/\alpha]]; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$,
then $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{unfold}\,\mathbf{r_d}, \mathbf{u_1}; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{unfold}\,\mathbf{r_d}, \mathbf{u_2}; \mathbf{I_2}$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{unfold}\,\mathbf{r_d}, \mathbf{u_1}; \mathbf{I_1}$ and $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{unfold}\,\mathbf{r_d}, \mathbf{u_2}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1((\mathtt{unfold}\,\mathbf{r_d}, \mathbf{u_1}; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{unfold}\,\mathbf{r_d}, \mathbf{u_2}; \mathbf{I_2}, \cdot)))\\ &\quad = (W, (\mathtt{unfold}\,\mathbf{r_d}, \rho_1(\mathbf{u_1}); \rho_1(\mathbf{I_1}), \cdot), (\mathtt{unfold}\,\mathbf{r_d}, \rho_2(\mathbf{u_2}); \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.\end{aligned}$$

In the following, let $\tau_{\mathrm{r}}; \sigma_{\mathrm{r}} = \text{ret-type}(\mathbf{q}, \chi, \sigma)$.

We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

- We claim that $(W, (\mathtt{unfold}\,\mathbf{r_d}, \rho_1(\mathbf{u_1}); \rho_1(\mathbf{I_1}), \cdot), (\mathtt{unfold}\,\mathbf{r_d}, \rho_2(\mathbf{u_2}); \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_{\mathrm{r}}; \sigma_{\mathrm{r}}]\rho$. To establish this, we must show $W.\Psi_{\mathrm{i}}; \cdot; W.\chi_{\mathrm{i}}; W.\sigma_{\mathrm{i}}; \rho_i(\mathbf{q}) \vdash (\mathtt{unfold}\,\mathbf{r_d}, \rho_i(\mathbf{u_i}); \rho_i(\mathbf{I_i}), \cdot) : \rho_i(\tau_{\mathrm{r}}); \rho_i(\sigma_{\mathrm{r}})$. The latter follows from $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{unfold}\,\mathbf{r_d}, \mathbf{u_i}; \mathbf{I_i}$ using the component typing rule and the properties of W and ρ that we have by assumption.
- Let $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \mathbf{w_1}], W.\chi_1[\mathbf{r_d} : \rho_1(\tau[\mu\alpha.\tau/\alpha])], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \mathbf{w_2}], W.\chi_2[\mathbf{r_d} : \rho_2(\tau[\mu\alpha.\tau/\alpha])])$ where $W.\hat{\mathbf{R}}_{\mathbf{i}}(\mathbf{u_i}) = \mathbf{fold}_{\mu\alpha.\tau}\,\mathbf{w_i}$ and $W' = (W.k - 1, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\text{reg}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$.
- We claim that $W' \in \text{World}$. Instantiating the first hypothesis with W and ρ, we have that

  $$(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\mu\alpha.\tau]\!]\rho$$

  From the definition of $\mathcal{W}[\![\mu\alpha.\tau]\!]\rho$, we have that $(W, \mathbf{w_1}, \mathbf{w_2}) \in \triangleright\mathcal{W}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$.
  This means that $W.\Psi_{\mathrm{i}}; \cdot \vdash \mathbf{w_1} : \rho_i(\tau[\mu\alpha.\tau/\alpha])$.
  Given our choice of W' and since $W \in \text{World}$, it follows that $W'.\Psi_{\mathrm{i}}; \cdot \vdash \mathbf{w_1} : \rho_i(\tau[\mu\alpha.\tau/\alpha])$ which is sufficient to establish our claim.
- Note that $W' \sqsupseteq_{\text{pub}} W$. The latter is immediate given our choice of W' and the definition of $\text{island}_{\text{reg}}$.
- Consider arbitrary $(M_1, M_2) : W$. Let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$. Note that

  $$\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\mathtt{unfold}\,\mathbf{r_d}, \rho_i(\mathbf{u_i}); \rho_i(\mathbf{I_i}), \cdot) \rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \mathbf{w_i}], \mathbf{S_i}) \mid (\rho_i(\mathbf{I_i}), \cdot) \rangle$$

  Where $W.\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) = \mathbf{fold}_{\mu\alpha.\tau}\,\mathbf{w_i}$. Let $M_i' = (\mathbf{H_i}, \mathbf{R_i}[\mathbf{r_d} \mapsto \mathbf{w_i}], \mathbf{S_i})$. Note that $(M_1', M_2') : W'$.
- Note that $W.k \leq W'.k + 1$.
- Note that $\mathbf{q} \neq \epsilon$, which follows from the third hypothesis since it is a side condition of the instruction typing rules. Further, since $\mathbf{q} \neq \mathbf{r_d}$, which was the only memory location changed between W and W', we can see that the the return address does not change.

- Next, to use our third hypothesis, we note that $W' \in \mathcal{H}[\![\Psi]\!]$ by heap monotonicity (Lemma 1.9).
  From above, we have that $(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u}_1)), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u}_2))) = (W, \rho_1(\mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{w}_1), \rho_2(\mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{w}_2)) \in \mathcal{W}[\![\mu\alpha.\tau]\!]\rho$.
  From the definition of $\mathcal{W}[\![\mu\alpha.\tau]\!]\rho$, we have that $(W, \mathbf{w}_1, \mathbf{w}_2) \in \triangleright\mathcal{W}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$.
  We claim that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$. This follows from Lemma 1.21.
  We also claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\mathbf{r_d} : \tau[\mu\alpha.\tau/\alpha]]]\!]\rho$. In order to show this, we need to show that $(W', \mathbf{w}_1, \mathbf{w}_2) \in \mathcal{W}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$. From the definition of $\mathcal{W}[\![\mu\alpha.\tau]\!]\rho$ we have that $(\triangleright W, \mathbf{w}_1, \mathbf{w}_2) \in \mathcal{W}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$. But $W' \sqsupseteq \triangleright W$, since $W' \sqsupseteq W$ and $W'.k \leq W.k - 1$, which means from monotonicity, the required condition holds.
  Therefore we can apply our third hypothesis to W' and ρ, finding that

$$(W', \rho_1((\mathbf{I}_1, \cdot)), \rho_2((\mathbf{I}_2, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

Now, the result follows by Lemma 1.11. □

Lemma 1.54 (Allocate Stack Space)
If $\Psi; \Delta; \chi; \mathbf{unit} :: \cdots^{\mathbf{n}} :: \mathbf{unit} :: \sigma; \text{inc}(\mathbf{q}, \mathbf{n}) \vdash \mathbf{I}_1 \approx_{\mathbf{I}} \mathbf{I}_2$, then $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{salloc}\ \mathbf{n}; \mathbf{I}_1 \approx_{\mathbf{I}} \mathtt{salloc}\ \mathbf{n}; \mathbf{I}_2$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{salloc}\ \mathbf{n}; \mathbf{I}_1$ and $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{salloc}\ \mathbf{n}; \mathbf{I}_2$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1((\mathtt{salloc}\ \mathbf{n}; \mathbf{I}_1, \cdot)), \rho_2((\mathtt{salloc}\ \mathbf{n}; \mathbf{I}_2, \cdot))) \\ = (W, (\mathtt{salloc}\ \mathbf{n}; \rho_1(\mathbf{I}_1), \cdot), (\mathtt{salloc}\ \mathbf{n}; \rho_2(\mathbf{I}_2), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho. \quad (14)\end{aligned}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E}_\mathbf{i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i] \rangle)$.

In the following, assume $W.k > 0$ and let $\tau_\mathbf{r}; \sigma_\mathbf{r} = \text{ret-type}(\mathbf{q}, \chi, \overline{\tau} :: \sigma)$.

We now prove (13).

We proceed by unfolding the definition of $\mathcal{E}[\![\mathbf{q} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]\!]\rho$ and proving the resulting obligations:

- We claim $(W, (\mathtt{salloc}\ \mathbf{n}; \rho_1(\mathbf{I}_1), \cdot), (\mathtt{salloc}\ \mathbf{n}; \rho_2(\mathbf{I}_2), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]\rho$. From the definitions of $\text{TermAtom}[\mathbf{q} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]\rho$ and $\text{TermAtom}[\mathbf{q} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]$, it suffices to show $W.\Psi_1; \cdot; W.\chi_1; W.\sigma_1; \rho_1(\mathbf{q}) \vdash (\mathtt{salloc}\ \mathbf{n}; \rho_1(\mathbf{I}_1), \cdot) : \rho_1(\tau_\mathbf{r}); \rho_1(\sigma_\mathbf{r})$ and $W.\Psi_2; \cdot; W.\chi_2; W.\sigma_2; \rho_2(\mathbf{q}) \vdash (\mathtt{salloc}\ \mathbf{n}; \rho_2(\mathbf{I}_2), \cdot) : \rho_2(\tau_\mathbf{r}); \rho_2(\sigma_\mathbf{r})$. Each follows from $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{salloc}\ \mathbf{n}; \mathbf{I}_1$ and $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{salloc}\ \mathbf{n}; \mathbf{I}_2$ respectively using the component typing rule and the properties of W and ρ that we have by assumption.
- Consider arbitrary E_1 and E_2 such that. $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_r; \sigma_\mathbf{r}]\!]\rho$. We must show that

$$(W, E_1[(\mathtt{salloc}\ \mathbf{n}; \rho_1(\mathbf{I}_1), \cdot)], E_2[(\mathtt{salloc}\ \mathbf{n}; \rho_2(\mathbf{I}_2), \cdot)]) \in \mathcal{O}.$$

  Let $M_1 = (\mathbf{H}_1, \mathbf{R}_1, \mathbf{S}_1)$ and $M_2 = (\mathbf{H}_2, \mathbf{R}_2, \mathbf{S}_2)$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \text{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$. From the latter, we can have the following facts for island i_{stk}.
  We have that $(\triangleright W, \mathbf{S}_1\!\upharpoonright, \mathbf{S}_2\!\upharpoonright) \in \text{currentMR}(W(i_{\text{stk}}))$. From the latter it follows that $\mathbf{S}_\mathbf{j} = W.\mathbf{S}_\mathbf{j}$.
  Next, by the reduction semantics of our language, with all of the above facts in hand, we have that:

$$E_1[(\rho_1(\mathbf{I}_1), \cdot)]$$

  and

$$\langle M_2 \mid E_2[(\mathtt{salloc}\ \mathbf{n}; \rho_2(\mathbf{I}_2), \cdot)] \rangle \longrightarrow \langle M_2' \mid E_2[(\rho_2(\mathbf{I}_2), \cdot)] \rangle$$

where $M_1' = (\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1'})$ with $\mathbf{S_1'} = () :: \cdots^n :: () :: \mathbf{S_1}$, and $M_2' = (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2'})$ with $\mathbf{S_2'} = () :: \cdots^n :: () :: \mathbf{S_2}$.

Note that in order to complete our proof, it suffices to show:

$$(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee$$
$$(\text{running}(W.k-1, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k-1, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))$$

Let $W' = (W.k, W.\mathbf{\Psi_1}, W.\mathbf{\Psi_2}, \Theta')$ where

1. $\forall i \neq i_{\text{stk}}.\, \Theta'(i) = W.\Theta(i)$;
2. $\Theta'(i_{\text{stk}}) = \text{island}_{\text{stk}}(s, W.k)$ with $s = (\mathbf{S_1'}, \mathit{unit} :: \cdots^n :: \mathit{unit} :: W.\boldsymbol{\sigma_1}, \mathbf{S_2'}, \mathit{unit} :: \cdots^n :: \mathit{unit} :: W.\boldsymbol{\sigma_2})$.

We claim that $W' \in \text{World}$. Note that we have $(W, (), ()) \in \mathcal{W}[\![\mathbf{unit}]\!]\rho$. Thus we have that $W.\Psi_j; \cdot \vdash () : \rho_j(\mathbf{unit})$. Given our choice of W' and since $W \in \text{World}$, it follows that $W'.\Psi_j; \cdot \vdash () : \rho_j(\mathbf{unit})$ which is sufficient to establish our claim.

We proceed by showing that $(M_1', M_2') : W'$ and then instantiating our hypothesis

$$\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \mathbf{unit} :: \cdots^{\mathbf{n}} :: \mathbf{unit} :: \boldsymbol{\sigma}; \text{inc}(\mathbf{q}, \mathbf{n}) \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$$

– We claim that $(M_1', M_2') : W'$. We prove this claim by establishing the following:
  * $\vdash M_1' : W'.\Phi_1$ and $\vdash M_2' : W'.\Phi_2$. Note the following facts:
    · $W'.\boldsymbol{\chi_1} = W.\boldsymbol{\chi_1}$ and $W'.\boldsymbol{\chi_2} = W.\boldsymbol{\chi_2}$;
    · $W'.\boldsymbol{\sigma_1} = \mathit{unit} :: \cdots^n :: \mathit{unit} :: W.\boldsymbol{\sigma_1})$ and $W'.\boldsymbol{\sigma_2} = \mathit{unit} :: \cdots^n :: \mathit{unit} :: W.\boldsymbol{\sigma_2})$;
    · $W'.\mathbf{\Psi_1} = W.\mathbf{\Psi_1}$ and $W'.\mathbf{\Psi_2} = W.\mathbf{\Psi_2}$.

    Both claims follow easily from $(M_1, M_2) : W$ the above facts, and the fact that we have extended both stacks with same number of well-typed words, i.e., with n () words.
  * We assume that $W.k > 0$ (and thus $W'.k > 0$). We must show that

$$(\triangleright W', M_1', M_2') \in \bigotimes \{ \text{currentMR}(\theta) \mid \theta \in W'.\Theta \}$$

    The latter follows from $(M_1, M_2) : W$ and monotonicity of MemRel given that we establish the following claim for island i_{stk}

$$(\triangleright W', S_1', S_2') \in \text{currentMR}(W'(i_{\text{stk}}))$$

    .

    Recall that $W'.S_i = S_i'$. Thus we obtain trivially that $(\triangleright W', S_1', S_2') \in \{(\widetilde{W}, W'.S_1, W'.S_2) \mid \widetilde{W} \in \text{World}_{W.k}\}$. From the latter, we establish directly our claim that

$$(\triangleright W', S_1', S_2') \in \text{currentMR}(W'(i_{\text{stk}}))$$

– Next, we instantiate our final hypothesis with W' and ρ. Note that $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$ by assumption, $W' \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ by heap monotonicity (Lemma 1.9). We claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$ by the first case of Lemma 1.20. Moreover we claim that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma'}]\!]\rho$ Our claim follows directly from the third case of lemma 1.21 since, above, we have established that $(W', (), ()) \in \mathcal{W}[\![\mathbf{unit}]\!]$ and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$. Hence, we have that

$$(W', (\rho_1(\mathbf{I_1}, \cdot)), (\rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau}_{\mathbf{r}}; \boldsymbol{\sigma}_{\mathbf{r}}]\!]\rho$$

  Instantiate the above with E_1 and E_2. Note that we have $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}_{\mathbf{r}}; \boldsymbol{\sigma}_{\mathbf{r}}]\!]\rho$ which follows from $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}_{\mathbf{r}}; \boldsymbol{\sigma}_{\mathbf{r}}]\!]\rho$ by monotonicity for evaluation contexts (Lemma 1.10), since our choice of W', $W' \sqsupseteq_{\text{pub}} W$ and the reduction does not affect the return marker.

  Hence, we have

$$(W', E_1[(\rho_1(\mathbf{I_1}, \cdot))], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Instantiate the latter with M_1' and M_2', noting that $(M_1', M_2') : W'$. Hence, we have

$$(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee$$
$$(\text{running}(W.k, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))$$

which implies what we needed to show.

□

Lemma 1.55 (Free Stack Space)
If $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \sigma; \text{dec}(\mathbf{q}, \mathbf{n}) \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$, then $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \tau_0 :: \cdots :: \tau_{\mathbf{n-1}} :: \sigma; \mathbf{q} \vdash \mathtt{sfree}\ \mathbf{n}; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{sfree}\ \mathbf{n}; \mathbf{I_2}$.

Proof

Clearly, $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \tau_0 :: \cdots :: \tau_{\mathbf{n-1}} :: \sigma; \mathbf{q} \vdash \mathtt{sfree}\ \mathbf{n}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \tau_0 :: \cdots :: \tau_{\mathbf{n-1}} :: \sigma; \mathbf{q} \vdash \mathtt{sfree}\ \mathbf{n}; \mathbf{I_2}$.
Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\tau_0 :: \cdots :: \tau_{\mathbf{n-1}} :: \sigma]\!]\rho$. We need to show that

$$(W, \rho_1((\mathtt{sfree}\ \mathbf{n}; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{sfree}\ \mathbf{n}; \mathbf{I_2}, \cdot)))$$
$$= (W, (\mathtt{sfree}\ \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sfree}\ \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \tau_0 :: \cdots :: \tau_{\mathbf{n-1}} :: \sigma)]\!]\rho. \quad (15)$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i]\rangle)$.
In the following, assume $W.k > 0$ and let $\tau_{\mathbf{r}}; \sigma_{\mathbf{r}} = \text{ret-type}(\mathbf{q}, \chi, \overline{\tau} :: \sigma)$ and $\overline{\tau} = \tau_1 :: \cdots :: \tau_m$.
Moreover, note the following preliminary fact:

- By our hypothesis and the typing rules, we have that , $\text{dec}(\mathbf{q}, \mathbf{n}) \neq \epsilon$ and $\text{dec}(\mathbf{q}, \mathbf{n}) \neq$ undefined. A consequence of the latter fact is that if $\mathbf{q} = \mathbf{i}$ then $\mathbf{i} \geq \mathbf{n}$.

With the above facts in hand, we now prove (15).

- We claim $(W, (\mathtt{sfree}\ \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sfree}\ \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\rho$. From the definitions of $\text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\rho$ and $\text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]$, it suffices to show $W.\Psi_1; \cdot; W.\chi_1; W.\sigma_1; \rho_1(\mathbf{q}) \vdash (\mathtt{sfree}\ \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot) : \rho_1(\tau_{\mathbf{r}}); \rho_1(\sigma_{\mathbf{r}})$ and $W.\Psi_2; \cdot; W.\chi_2; W.\sigma_2; \rho_2(\mathbf{q}) \vdash (\mathtt{sfree}\ \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot) : \rho_2(\tau_{\mathbf{r}}); \rho_2(\sigma_{\mathbf{r}})$. Each follows from $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \tau_0 :: \cdots :: \tau_{\mathbf{n-1}} :: \sigma; \mathbf{q} \vdash \mathtt{sfree}\ \mathbf{n}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \chi; \tau_0 :: \cdots :: \tau_{\mathbf{n-1}} :: \sigma; \mathbf{q} \vdash \mathtt{sfree}\ \mathbf{n}; \mathbf{I_2}$ respectively using the component typing rule and the properties of W and ρ that we have by assumption.
- Consider arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_r; \sigma_{\mathbf{r}}]\!]\rho$. We must show that

$$(W, E_1[(\mathtt{sfree}\ \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\mathtt{sfree}\ \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Let $M_1 = (\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1})$ and $M_2 = (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2})$.
From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \text{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$.
From the latter, we can have the following facts for island i_{stk}.
We have that $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \text{currentMR}(W(i_{\text{stk}}))$. From the latter it follows that $\mathbf{S_j} = W.\mathbf{S_j} = w_{j1} :: \cdots :: w_{jn} :: S_j'$.
Next, by the reduction semantics of our language, with all of the above facts in hand, we have that:

$$\langle M_1 \mid E_1[(\mathtt{sfree}\ \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot)]\rangle \longrightarrow \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle$$

and

$$\langle M_2 \mid E_2[(\mathtt{sfree}\ \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \longrightarrow \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle$$

where $M_1' = (\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1'})$ and $M_2' = (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2'})$.

Note that in order to complete our proof, it suffices to show:

$$(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee$$
$$(\text{running}(W.k-1, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k-1, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))$$

Let $W' = (W.k, W.\mathbf{\Psi_1}, W.\mathbf{\Psi_2}, \Theta')$ where

1. $\forall i \neq i_{\text{reg}}, i_{\text{stk}}, \Theta'(i) = W.\Theta(i)$;
2. $\Theta'(i_{\text{stk}}) = \text{island}_{\text{stk}}(s, W.k)$ with $s = (S_1', \sigma, S_2', \sigma)$.

We claim that $W' \in \text{World}$. Given our choice of W' and since $W \in \text{World}$, it is starightforward to establish our claim.
Moreover, note that $W' \sqsupseteq W$ and $W' \sqsupseteq_{\text{pub}} W$. Both follow immediately given our choice of W' and the definition of $\text{island}_{\text{stk}}$.
We proceed by showing that $(M_1', M_2') : W'$ and then instantiating our hypothesis

$$\mathbf{\Psi}; \mathbf{\Delta}; \mathbf{\chi}; \mathbf{\sigma}; \text{dec}(\mathbf{q}, \mathbf{n}) \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$$

.

- We claim that $(M_1', M_2') : W'$. We prove this claim by establishing the following:
  - $\vdash M_1' : W'.\Phi_1$ and $\vdash M_2' : W'.\Phi_2$. Note the following facts:
    - $W'.\mathbf{\chi_1} = W.\mathbf{\chi_1}$ and $W'.\mathbf{\chi_2} = W.\mathbf{\chi_2}$;
    - $W'.\mathbf{\sigma_1} = \sigma$ and $W'.\mathbf{\sigma_2} = \sigma$;
    - $W'.\mathbf{\Psi_1} = W.\mathbf{\Psi_1}$ and $W'.\mathbf{\Psi_2} = W.\mathbf{\Psi_2}$.

    Both claims follow easily from $(M_1, M_2) : W$, the above facts and the fact that we remove n words from the top of each stack.
  - We assume that $W.k > 0$ (and thus $W'.k > 0$). We must show that

    $$(\triangleright W', M_1', M_2') \in \bigotimes \{ \text{currentMR}(\theta) \mid \theta \in W'.\Theta \}$$

    The latter follows from $(M_1, M_2) : W$ and monotonicity of MemRel given that we establish the following claim for island i_{stk}:

    $$(\triangleright W', S_1', S_2') \in \text{currentMR}(W'(i_{\text{stk}}))$$

    Recall that $W'.S_i = S_i'$. Thus we obtain trivially that $(\triangleright W', S_1', S_2') \in \{(\widetilde{W}, W'.S_1, W'.S_2) \mid \widetilde{W} \in \text{World}_{W.k}\}$. From the latter, we establish directly our claim that

    $$(\triangleright W', S_1', S_2') \in \text{currentMR}(W'(i_{\text{stk}}))$$

- Next, we instantiate our final hypothesis with W' and ρ. Note that $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$ by assumption, $W' \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ by heap monotonicity (Lemma 1.9). We claim that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\mathbf{\sigma}]\!]\rho$ by the second case of lemma 1.21 since $W'(i_{\text{stk}}) = \text{island}_{\text{stk}}(s, W.k)$ with $s = (S_1, \sigma, S_2, \sigma)$ where $W(i_{\text{stk}}) = \text{island}_{\text{stk}}(s, W.k)$ with $s = (w_{11} :: \cdots :: w_{1n} :: S_1, \tau_1 :: \cdots :: \tau_n :: \sigma, w_{21} :: \cdots :: w_{2n} :: S_2, \tau_1 :: \cdots :: \tau_n :: \sigma)$. Moreover we claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\mathbf{\chi}]\!]\rho$ by the first case of Lemma 1.20. Hence, we have that

  $$(W', (\rho_1(\mathbf{I_1}, \cdot)), (\rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\!]\rho$$

  Instantiate the above with E_1 and E_2. Note that we have $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\!]\rho$ which follows from $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\!]\rho$ by monotonicity for evaluation contexts (Lemma 1.10), since our choice of W', $W' \sqsupseteq_{\text{pub}} W$ and the preliminary fact that if $\mathbf{q} = \mathbf{i}$ then $\mathbf{i} \geq \mathbf{n}$ let us easily establish all the premises of that lemma.
  Hence, we have

  $$(W', E_1[(\rho_1(\mathbf{I_1}, \cdot))], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Instantiate the latter with M_1' and M_2', noting that $(M_1', M_2') : W'$. Hence, we have

$$(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee$$
$$(\text{running}(W.k, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))$$

which implies what we needed to show.

□

Lemma 1.56 (Load from Stack)
If $\boldsymbol{\sigma}(\mathbf{i}) = \boldsymbol{\tau}$, $\mathbf{q} \neq \mathbf{r_d}$, and $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau}_\mathbf{i}]; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathbf{I_1} \approx_\mathbf{I} \mathbf{I_2}$, then $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \mathbf{I_1} \approx_\mathbf{I} \mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \mathbf{I_2}$.

Proof

Clearly, $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \mathbf{I_1}$ and $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\boldsymbol{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\boldsymbol{\Delta}]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$. We need to show that

$$(W, \rho_1((\mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \mathbf{I_2}, \cdot)))$$
$$= (W, (\mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})]\!]\rho.$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i]\rangle$.

In the following, assume $W.k > 0$ and let $\boldsymbol{\tau}_\mathbf{r}; \boldsymbol{\sigma}_\mathbf{r} = \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})$.

We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

- We claim that $(W, (\mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \boldsymbol{\tau}_\mathbf{r}; \boldsymbol{\sigma}_\mathbf{r}]\rho$. To establish this, we must show $W.\Psi_j; \cdot; W.\boldsymbol{\chi}_\mathbf{j}; W.\boldsymbol{\sigma}_\mathbf{j}; \rho_j(\mathbf{q}) \vdash (\mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \rho_j(\mathbf{I_j}), \cdot) : \rho_j(\boldsymbol{\tau}_\mathbf{r}); \rho_j(\boldsymbol{\sigma}_\mathbf{r})$. The latter follows from $\boldsymbol{\Psi}; \boldsymbol{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{sld}\ \mathbf{r_d}, \mathbf{i}; \mathbf{I_j}$ using the component typing rule and the properties of W and ρ that we have by assumption.
- Let $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto W.\mathbf{S_1(i)}], W.\boldsymbol{\chi}_\mathbf{1}[\mathbf{r_d} : \rho_1(\boldsymbol{\tau})], W.\mathbf{R_2}[\mathbf{r_d} \mapsto W.\mathbf{S_2(i)}], W.\boldsymbol{\chi}_\mathbf{2}[\mathbf{r_d} : \rho_2(\boldsymbol{\tau})])$ and $W' = (W.k, W.\boldsymbol{\Psi}_\mathbf{1}, W.\boldsymbol{\Psi}_\mathbf{2}, W.\Theta[i_{\text{reg}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$.
- We claim that $W' \in \text{World}$.
  From the hypothesis, we know that $(W, W.\mathbf{S_1}\ \restriction, W.\mathbf{S_2}\ \restriction) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$. Since $\boldsymbol{\sigma}(i) = \boldsymbol{\tau}$, this means $(W, W.\mathbf{S_1(i)}, W.\mathbf{S_2(i)}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$.
  Given our choice of W' and since $W \in \text{World}$, this is sufficient to establish our claim.
- Note that $W' \sqsupseteq_{\text{pub}} W$. The latter is immediate given our choice of W' and the definition of $\text{island}_{\text{reg}}$.
- Consider arbitrary $(M_1, M_2) : W$. Let $M_j = (\mathbf{H_j}, \mathbf{R_j}, \mathbf{S_j})$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \text{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$. From the latter, we have the following fact for island i_{stk}: $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \text{currentMR}(W(i_{\text{stk}}))$. From the latter it follows that $\mathbf{S_i} = W.\mathbf{S_i}$.
  Note that

$$\langle (\mathbf{H_j}, \mathbf{R_j}, \mathbf{S_j}) \mid (\mathtt{sld}\ \mathbf{r_d}, i; \rho_j(\mathbf{I_j}), \cdot)\rangle \longmapsto^1 \langle (\mathbf{H_j}, \mathbf{R_j}[\mathbf{r_d} \mapsto \mathbf{S_i}(i)], \mathbf{S_j}) \mid (\rho_j(\mathbf{I_j}), \cdot)\rangle$$

  Let $M_j' = (\mathbf{H_j}, \mathbf{R_j}[\mathbf{r_d} \mapsto \mathbf{S_j}(i)], \mathbf{S_j})$. Note that $(M_1', M_2') : W'$.
- Note that $W.k \leq W'.k + 1$.
- Note that $\mathbf{q} \neq \boldsymbol{\epsilon}$, which follows from the third hypothesis since it is a side condition of the instruction typing rules. Further, since $\mathbf{q} \neq \mathbf{r_d}$, which was the only memory location changed between W and W', we can see that the the return address does not change.

- Next, to use our third hypothesis, we note that $W' \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ by heap monotonicity (Lemma 1.9) and that currentMR($W'(i_{\text{stk}})$) $\Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ by Lemma 1.21 since $W'(i_{\text{stk}}) = W(i_{\text{stk}})$. We also claim that currentMR($W'(i_{\text{reg}})$) $\Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau}]]\!]\rho$. From above, we have that $(W, W.\mathbf{S_1}(i), W.\mathbf{S_2}(i)) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$. Hence, by monotonicity and the definition of W' we have

$$(W', W.\mathbf{S_1}(i), W.\mathbf{S_2}(i)) = (W', W'.\mathbf{R_1}(\mathbf{r_d}), W'.\mathbf{R_2}(\mathbf{r_d})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho,$$

which, using Lemma 1.20, is sufficient to establish our claim.

Therefore we can apply our third hypothesis to W' and ρ, finding that

$$(W', \rho_1((\mathbf{I_1}, \cdot)), \rho_2((\mathbf{I_2}, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})]\!]\rho.$$

Now, the result follows by Lemma 1.11.

□

Lemma 1.57 (Load Return Address from Stack)
If $\boldsymbol{\sigma}(\mathbf{i}) = \tau_i$ and $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}[\mathbf{r_d} : \boldsymbol{\tau}_\mathbf{i}]; \boldsymbol{\sigma}; \mathbf{r_d} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$, then $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{i} \vdash \mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \mathbf{I_2}$.

Proof

Clearly, $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{i} \vdash \mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{i} \vdash \mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, currentMR($W(i_{\text{reg}})$) $\Subset_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$, and currentMR($W(i_{\text{stk}})$) $\Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1((\mathtt{sld}\, \mathbf{r_d}, \mathbf{n}; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{sld}\, \mathbf{r_d}, \mathbf{n}; \mathbf{I_2}, \cdot))) \\ = (W, (\mathtt{sld}\, \mathbf{r_d}, \mathbf{n}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sld}\, \mathbf{r_d}, \mathbf{n}; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{i} \vdash \text{ret-type}(\mathbf{i}, \boldsymbol{\chi}, \boldsymbol{\sigma})]\!]\rho. \quad (16)\end{aligned}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that running$(0, \langle M_i \mid E_i[e_i] \rangle)$.

In the following, assume $W.k > 0$ and let $\boldsymbol{\tau}_\mathbf{r}; \boldsymbol{\sigma}_\mathbf{r} = \text{ret-type}(\mathbf{i}, \boldsymbol{\chi}, \boldsymbol{\sigma})$.

Moreover, note the following preliminary fact:

- By our first and second hypothesis, and the typing rules we obtain that $\sigma = \tau_1 :: \cdots :: \tau_i :: \sigma'$.
- By our assumption currentMR($W(i_{\text{stk}})$) $\Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ and the previous fact, we have that $w_{11}, ..., w_{1i}, w_{21}, ..., w_{2i}$, S_1', S_2' such that $W.S_1 = w_{11} :: \cdots :: w_{1i} :: S_1'$, $W.S_2 = w_{21} :: \cdots :: w_{2i} :: S_2'$ and $(W, w_{1i}, w_{2i}) \in \mathcal{W}[\![\boldsymbol{\tau}_\mathbf{i}]\!]\rho$.

With the above facts in hand, we now prove (16).

- We claim $(W, (\mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{i} \vdash \boldsymbol{\tau}_\mathbf{r}; \boldsymbol{\sigma}_\mathbf{r}]\rho$. From the definitions of TermAtom$[\mathbf{i} \vdash \boldsymbol{\tau}_\mathbf{r}; \boldsymbol{\sigma}_\mathbf{r}]\rho$ and TermAtom$[\mathbf{i} \vdash \boldsymbol{\tau}_\mathbf{r}; \boldsymbol{\sigma}_\mathbf{r}]$, it suffices to show $W.\Psi_1; \cdot; W.\boldsymbol{\chi}_\mathbf{1}; W.\boldsymbol{\sigma}_\mathbf{1}; \rho_1(\mathbf{i}) \vdash (\mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot) : \rho_1(\boldsymbol{\tau}_\mathbf{r}); \rho_1(\boldsymbol{\sigma}_\mathbf{r})$ and $W.\Psi_2; \cdot; W.\boldsymbol{\chi}_\mathbf{2}; W.\boldsymbol{\sigma}_\mathbf{2}; \rho_2(\mathbf{i}) \vdash (\mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot) : \rho_2(\boldsymbol{\tau}_\mathbf{r}); \rho_2(\boldsymbol{\sigma}_\mathbf{r})$. Each follows from $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{i} \vdash \mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{i} \vdash \mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \mathbf{I_2}$ respectively using the component typing rule and the properties of W and ρ that we have by assumption.
- Consider arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{i} \vdash \boldsymbol{\tau}_r; \boldsymbol{\sigma}_\mathbf{r}]\!]\rho$. We must show that

$$(W, E_1[(\mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\mathtt{sld}\, \mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Let $M_1 = (\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1})$ and $M_2 = (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2})$.

From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{ \text{currentMR}(\theta) \mid \theta \in W.\Theta \}$. From the latter, we can have the following facts for island i_{stk}.

We have that $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \text{currentMR}(W(i_{\text{stk}}))$. From the latter it follows that $\mathbf{S_j} = W.\mathbf{S_j} = w_{j1} :: \cdots :: w_{ji} :: S_j'$.

Next, by the reduction semantics of our language, with all of the above facts in hand, we have that:

$$\langle M_1 \mid E_1[(\mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot)]\rangle \longrightarrow \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle$$

and

$$\langle M_2 \mid E_2[(\mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \longrightarrow \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle$$

where $M_1' = (\mathbf{H_1}, \mathbf{R_1'}, \mathbf{S_1})$ with $\mathbf{H_1} = H_1'[r_d \mapsto w_{1i}]$, and $M_2' = (\mathbf{H_2}, \mathbf{R_2'}, \mathbf{S_2})$ with $\mathbf{H_2'} = H_2[r_d \mapsto w_2 i]$.

Note that in order to complete our proof, it suffices to show:

$$\begin{array}{l}(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee \\ (\mathrm{running}(W.k-1, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \mathrm{running}(W.k-1, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))\end{array}$$

Let $W' = (W.k, W.\mathbf{\Psi_1}, W.\mathbf{\Psi_2}, \Theta')$ where

1. $\forall i \notin \{i_{\mathrm{reg}}\}.\, \Theta'(i) = W.\Theta(i)$;
2. $\Theta'(i_{\mathrm{reg}}) = \mathrm{island}_{\mathrm{reg}}(s, W.k)$ with $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}], W.\boldsymbol{\chi_1}[\mathbf{r_d} : \rho_1(\tau_i)], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \mathbf{w_{2i}}], W.\boldsymbol{\chi_2}[\mathbf{r_d} : \rho_2(\rho_1(\tau_i))]$.

We claim that $W' \in \mathrm{World}$. Recall that we have $(W, w_{1i}, w_{2i}) \in \mathcal{W}[\![\tau_i]\!]\rho$. Thus we have that $W.\Psi_j; \cdot \vdash w_{ji} : \rho_j(\tau_i)$. Given our choice of W' and since $W \in \mathrm{World}$, it follows that $W'.\Psi_j; \cdot \vdash w_{ji} : \rho_j(\tau_i)$ which is sufficient to establish our claim.

Moreover, note that $W' \sqsupseteq W$ and $W' \sqsupseteq_{\mathrm{pub}} W$. Both follow immediately given our choice of W' and the definition of $\mathrm{island}_{\mathrm{reg}}$, and $\mathrm{island}_{\mathrm{stk}}$.

We proceed by showing that $(M_1', M_2') : W'$ and then instantiating our final hypothesis

$$\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{i} \vdash \mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \mathbf{I_2}$$

– We claim that $(M_1', M_2') : W'$. We prove this claim by establishing the following:
  * $\vdash M_1' : W'.\Phi_1$ and $\vdash M_2' : W'.\Phi_2$. Note the following facts:
    · $W'.\boldsymbol{\chi_1} = W.\boldsymbol{\chi_1}[\mathbf{r_d} : \rho_1(\tau_i)]$ and $W'.\boldsymbol{\chi_2} = W.\boldsymbol{\chi_2}[\mathbf{r_d} : \rho_2(\tau_i)]$;
    · $W'.\boldsymbol{\sigma_1} = \sigma$ and $W'.\boldsymbol{\sigma_2} = \sigma$;
    · $W'.\mathbf{\Psi_1} = W.\mathbf{\Psi_1}$ and $W'.\mathbf{\Psi_2} = W.\mathbf{\Psi_2}$.

    Both claims follow easily from $(M_1, M_2) : W$, the above facts, the fact that we have updater register $\mathbf{r_d}$ in both memories words well-typed words, i.e., with words of types $\rho_1(\tau_i)$ and $\rho_2(\tau_i)$.
  * We assume that $W.k > 0$ (and thus $W'.k > 0$). We must show that

$$(\triangleright W', M_1', M_2') \in \bigotimes \{\, \mathrm{currentMR}(\theta) \mid \theta \in W'.\Theta \,\}$$

    The latter follows from $(M_1, M_2) : W$ and monotonicity of MemRel given that we establish the following claim for island i_{reg}, $(\triangleright W', \mathbf{W.R_1}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}]\uparrow, \mathbf{W.R_2}[\mathbf{r_d} \mapsto \mathbf{w_{2i}}]\uparrow) \in \mathrm{currentMR}(W'(i_{\mathrm{reg}}))$.

    For the claim recall that $W'.R_i = W.R_i[r_d \mapsto w_{ji}]$. Thus we obtain trivially that $(\triangleright W', W.R_1[r_d \mapsto w_{1i}], W.R_2[r_d \mapsto w_{2i}]) \in \{(\widetilde{W}, W'.R_1, W'.R_2) \mid \widetilde{W} \in \mathrm{World}_{W.k}\}$. From the latter, we establish directly our claim that

$$(\triangleright W', \mathbf{W.R_1}[\mathbf{r_d} \mapsto \mathbf{w_{1i}}]\uparrow, \mathbf{W.R_2}[\mathbf{r_d} \mapsto \mathbf{w_{2i}}]\uparrow) \in \mathrm{currentMR}(W'(i_{\mathrm{reg}}))$$

– By lemmas 1.20 and 1.21, and by unfloding the definition of our second hypothesis, $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}[\mathbf{r_d} : \tau_i]; \boldsymbol{\sigma}; \mathbf{r_d} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$, we derive that given $(M_1'', M_2'') : W'$, $(W', E_1[(\rho_1(\mathbf{I_1}), \cdot)], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}$. By construction $(M_1', M_2') : W'$ and thus by unfolding the definition of $\mathcal{O}$, we obtain $\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow$ and $\langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow$, or $\mathrm{running}(W'.k, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle)$ and $\mathrm{running}(W'.k, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle)$. In the first case, it is straightforward to derive from the reduction semantics that $\langle M_1 \mid E_1[(\mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow$ and $\langle M_2 \mid E_2[(\mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow$. In the second case, since $W'.k = W.k$, we derive that $\mathrm{running}(W.k, \langle M_1 \mid E_1[(\mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot)]\rangle$ and $\mathrm{running}(W.k, \langle M_2 \mid E_2[(\mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot)]\rangle$. Thus we conclude that:

$$(W, E_1[(\mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \rho_1(\mathbf{I_1}), \cdot)], E_2[(\mathtt{sld}\,\mathbf{r_d}, \mathbf{i}; \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

– Next, we instantiate our final hypothesis with W' and ρ. Note that $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$ by assumption, $W' \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ by heap monotonicity (Lemma 1.9). We claim currentMR$(W'(i_{\text{stk}})) \in_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ which follows directly from the first case of lemma 1.21. We claim currentMR$(W'(i_{\text{reg}})) \in_{W'} \mathcal{R}[\![\boldsymbol{\chi}[\mathbf{r_d} : \tau_i]]\!]\rho$. The claim follows directly from the second case of lemma 1.20 since, above, we have established that $(W', w_{1i}, w_{2i}) \in \mathcal{W}[\![\tau_i]\!]$ and by assumption currentMR$(W(i_{\text{reg}})) \in_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$. Hence, we have that

$$(W', (\rho_1(\mathbf{I_1}, \cdot)), (\rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \tau_r; \boldsymbol{\sigma}_r]\!]\rho$$

Instantiate the above with E_1 and E_2. Note that we have $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_r; \boldsymbol{\sigma}_r]\!]\rho$ which follows from $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_r; \boldsymbol{\sigma}_r]\!]\rho$ by monotonicity for evaluation contexts (Lemma 1.10), since our choice of W', $W' \sqsupseteq_{\text{pub}} W$ and our second hypothesis let us easily establish all the premises of that lemma, including that ret-addr$_1(W, i) =$ ret-addr$_1(W, r_d)$ and ret-addr$_2(W, i) =$ ret-addr$_2(W, r_d)$.
Hence, we have

$$(W', E_1[(\rho_1(\mathbf{I_1}, \cdot))], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Instantiate the latter with M_1' and M_2', noting that $(M_1', M_2') : W'$. Hence, we have

$$\begin{aligned}&(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee \\ &(\text{running}(W.k, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))\end{aligned}$$

which implies what we needed to show.

□

Lemma 1.58 (Store to Stack)
If $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi} \vdash \mathbf{r_{s1}} \approx_{\text{u}} \mathbf{r_{s2}} : \tau'$, $\mathbf{q} \neq \mathbf{i}$, and $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \tau_0 :: \cdots :: \tau_{i-1} :: \tau' :: \boldsymbol{\sigma}; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$,
then $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \tau_0 :: \cdots :: \tau_i :: \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{sst}\ \mathbf{i}, \mathbf{r_{s1}}; \mathbf{I_1} \approx_{\mathbf{I}} \mathtt{sst}\ \mathbf{i}, \mathbf{r_{s2}}; \mathbf{I_2}$.

Proof

Clearly, $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \tau_0 :: \cdots :: \tau_i :: \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{sst}\ \mathbf{i}, \mathbf{r_{s1}}; \mathbf{I_1}$ and $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \tau_0 :: \cdots :: \tau_i :: \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{sst}\ \mathbf{i}, \mathbf{r_{s2}}; \mathbf{I_2}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, currentMR$(W(i_{\text{reg}})) \in_W \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \in_W \mathcal{S}[\![\tau_0 :: \cdots :: \tau_i :: \boldsymbol{\sigma}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1((\mathtt{sst}\ \mathbf{i}, \mathbf{r_{s1}}; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{sst}\ \mathbf{i}, \mathbf{r_{s2}}; \mathbf{I_2}, \cdot))) \\ &\qquad = (W, (\mathtt{sst}\ \mathbf{i}, \rho_1(\mathbf{r_{s1}}); \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sst}\ \mathbf{i}, \rho_2(\mathbf{r_{s2}}); \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})]\!]\rho.\end{aligned}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that running$(0, \langle M_i \mid E_i[e_i]\rangle)$.

In the following, assume $W.k > 0$ and let $\tau_r; \boldsymbol{\sigma}_r =$ ret-type$(\mathbf{q}, \boldsymbol{\chi}, \tau_0 :: \cdots :: \tau_i :: \boldsymbol{\sigma})$.

We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

- We claim that $(W, (\mathtt{sst}\ \mathbf{i}, \rho_1(\mathbf{r_{s1}}); \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sst}\ \mathbf{i}, \rho_2(\mathbf{r_{s2}}); \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\![\mathbf{q} \vdash \tau_r; \boldsymbol{\sigma}_r]\!]\rho$. To establish this, we must show $W.\Psi_i; \cdot; W.\boldsymbol{\chi}_i; W.\boldsymbol{\sigma}_i; \rho_i(\mathbf{q}) \vdash (\mathtt{sst}\ \mathbf{i}, \rho_i(\mathbf{r_{si}}); \rho_i(\mathbf{I_i}), \cdot) : \rho_i(\tau_r); \rho_i(\boldsymbol{\sigma}_r)$. The latter follows from $\mathbf{\Psi}; \mathbf{\Delta}; \boldsymbol{\chi}; \boldsymbol{\sigma}; \mathbf{q} \vdash \mathtt{sst}\ \mathbf{i}, \mathbf{r_{si}}; \mathbf{I_i}$ using the component typing rule and the properties of W and ρ that we have by assumption.
- Let $s = (W.\mathbf{S_1}[\mathbf{i} \mapsto W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{r_{s1}}))], W.\boldsymbol{\sigma}_1[\mathbf{i} : \rho_1(\tau')], W.\mathbf{S_2}[\mathbf{i} \mapsto W.\hat{\mathbf{R}}_2(\rho_1(\mathbf{r_{s2}}))], W.\boldsymbol{\sigma}_2[\mathbf{i} : \rho_2(\tau')])$ and $W' = (W.k, W.\mathbf{\Psi}_1, W.\mathbf{\Psi}_2, W.\Theta[i_{\text{stk}} \mapsto \text{island}_{\text{stk}}(s, W.k)])$.
- We claim that $W' \in$ World. Instantiating the first hypothesis with W and ρ, we have that

  $$(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{r_{s1}})), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{r_{s2}}))) \in \mathcal{W}[\![\tau']\!]\rho$$

  Thus we have that $W.\Psi_i; \cdot \vdash W.\hat{\mathbf{R}}_i(\rho_i(\mathbf{r_{si}})) : \rho_i(\tau')$. Given our choice of W' and since $W \in$ World, it follows that $W'.\Psi_i; \cdot \vdash W.\hat{\mathbf{R}}_i(\rho_i(\mathbf{r_{si}})) : \rho_i(\tau')$ which is sufficient to establish our claim.

- Note that $W' \sqsupseteq_{\text{pub}} W$. The latter is immediate given our choice of W' and the definition of $\text{island}_{\text{stk}}$.
- Consider arbitrary $(M_1, M_2) : W$. Let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{ \text{currentMR}(\theta) \mid \theta \in W.\Theta \}$. From the latter, we have the following fact for island i_{reg}: $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$.
  Note that
  $$\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\mathtt{sst}\ \mathbf{i}, \rho_i(\mathbf{r_{si}}); \rho_i(\mathbf{I_i}), \cdot) \rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}[\mathbf{i} \mapsto \hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{r_{si}}))]) \mid (\rho_i(\mathbf{I_i}), \cdot) \rangle$$
  Let $M_i' = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}[\mathbf{i} \mapsto \hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{r_{si}}))])$. Note that $(M_1', M_2') : W'$.
- Note that $W.k \leq W'.k + 1$.
- Note that $\mathbf{q} \neq \boldsymbol{\epsilon}$, which follows from the third hypothesis since it is a side condition of the instruction typing rules. Further, since $\mathbf{q} \neq \mathbf{i}$, which was the only memory location changed between W and W', we can see that the the return address does not change.
- Next, to use our third hypothesis, we note that $W' \in \mathcal{H}[\![\Psi]\!]$ by heap monotonicity (Lemma 1.9) and that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho$ by Lemma 1.20 since $W'(i_{\text{reg}}) = W(i_{\text{reg}})$. We also claim that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\tau_0 :: \cdots :: \tau' :: \sigma]\!]\rho$. From above, we have that $(W, W.\hat{\mathbf{R}}_\mathbf{1}(\rho_1(\mathbf{r_{s1}})), W.\hat{\mathbf{R}}_\mathbf{2}(\rho_2(\mathbf{r_{s2}}))) \in \mathcal{W}[\![\tau']\!]\rho$. Hence, by monotonicity and the definition of W' we have
  $$(W', W.\hat{\mathbf{R}}_\mathbf{1}(\rho_1(\mathbf{r_{s1}})), W.\hat{\mathbf{R}}_\mathbf{2}(\rho_2(\mathbf{r_{s2}}))) = (W', W'.\mathbf{S_1(i)}, W'.\mathbf{S_2(i)}) \in \mathcal{W}[\![\tau']\!]\rho,$$
  which, using Lemma 1.21, is sufficient to establish our claim.
  Therefore we can apply our third hypothesis to W' and ρ, finding that
  $$(W', \rho_1((\mathbf{I_1}, \cdot)), \rho_2((\mathbf{I_2}, \cdot))) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

Now, the result follows by Lemma 1.11.

□

Lemma 1.59 (Store Return Address to Stack)
If $\chi(\mathbf{r_s}) = \tau'$ and $\Psi; \Delta; \chi; \tau_0 :: \cdots :: \tau_{\mathbf{i}-1} :: \tau' :: \sigma; \mathbf{i} \vdash \mathbf{I_1} \approx_\mathbf{I} \mathbf{I_2}$,
then $\Psi; \Delta; \chi; \tau_0 :: \cdots :: \tau_\mathbf{i} :: \sigma; \mathbf{r_s} \vdash \mathtt{sst}\ \mathbf{i}, \mathbf{r_s}; \mathbf{I_1} \approx_\mathbf{I} \mathtt{sst}\ \mathbf{i}, \mathbf{r_s}; \mathbf{I_2}$.

Proof

Clearly, $\Psi; \Delta; \chi; \tau_0 :: \cdots :: \tau_\mathbf{i} :: \sigma; \mathbf{r_s} \vdash \mathtt{sst}\ \mathbf{i}, \mathbf{r_s}; \mathbf{I_1}$ and $\Psi; \Delta; \chi; \tau_0 :: \cdots :: \tau_\mathbf{i} :: \sigma; \mathbf{r_s} \vdash \mathtt{sst}\ \mathbf{i}, \mathbf{r_s}; \mathbf{I_2}$.
Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\tau_0 :: \cdots :: \tau_\mathbf{i} :: \sigma]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1((\mathtt{sst}\ \mathbf{i}, \mathbf{r_s}; \mathbf{I_1}, \cdot)), \rho_2((\mathtt{sst}\ \mathbf{i}, \mathbf{r_s}; \mathbf{I_2}, \cdot))) \\ = (W, (\mathtt{sst}\ \mathbf{i}, \mathbf{r_s}; \rho_1(\mathbf{I_1}), \cdot), (\mathtt{sst}\ \mathbf{i}, \mathbf{r_s}; \rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{r_s} \vdash \text{ret-type}(\mathbf{r_s}, \chi, \sigma)]\!]\rho. \quad (17)\end{aligned}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i] \rangle)$.

In the following, assume $W.k > 0$ and let $\tau_\mathbf{r}; \sigma_\mathbf{r} = \text{ret-type}(\mathbf{r_s}, \chi, \sigma)$.

Moreover, note the following preliminary fact:

- By our first second hypothesis, and $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ we have that there exist w_1, and w_2 such that $W.R_1(r_s) = w_1$ and $W.R_2(r_s) = w_2$, $(W, w_1, w_2) \in \mathcal{W}[\![\tau']\!]\rho$.

With the above facts in hand, we now prove (17).

- claim that $(\texttt{sst}\, i, r_s; \rho_1(\mathbf{I_1}), \cdot), (\texttt{sst}\ \mathbf{i, r_s;}\ \rho_2(\mathbf{I_2}), \cdot)) \in \text{TermAtom}[\mathbf{r_s} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]\rho$. From the definitions of $\text{TermAtom}[\mathbf{r_s} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]\rho$ and $\text{TermAtom}[\mathbf{r_s} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]$, it suffices to show $W.\Psi_1; \cdot; W.\chi_1; W.\sigma_1; \rho_1(\mathbf{r_s}) \vdash (\texttt{sld}\ \mathbf{r_d, i;}\ \rho_1(\mathbf{I_1}), \cdot) : \rho_1(\tau_\mathbf{r}); \rho_1(\sigma_\mathbf{r})$ and $W.\Psi_2; \cdot; W.\chi_2; W.\sigma_2; \rho_2(\mathbf{r_s}) \vdash (\texttt{sld}\ \mathbf{r_d, i;}\ \rho_2(\mathbf{I_2}), \cdot) : \rho_2(\tau_\mathbf{r}); \rho_2(\sigma_\mathbf{r})$. Each follows from $\Psi; \Delta; \chi; \tau_0 :: \cdots :: \tau_\mathbf{i} :: \sigma; \mathbf{r_s} \vdash \texttt{sst}\ \mathbf{i, r_s; I_1}$ and$\Psi; \Delta; \chi; \tau_0 :: \cdots :: \tau_\mathbf{i} :: \sigma; \mathbf{r_s} \vdash \texttt{sst}\ \mathbf{i, r_s; I_2}$ respectively using the component typing rule and the properties of W and ρ that we have by assumption.
- Consider arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{r_s} \vdash \tau_r; \sigma_\mathbf{r}]\!]\rho$. We must show that

$$(W, E_1[(\texttt{sst}\ \mathbf{i, r_s;}\ \rho_1(\mathbf{I_1}), \cdot)], E_2[(\texttt{sst}\ \mathbf{i, r_s;}\ \rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

  onsider arbitrary $(M_1, M_2) : W$. We must show either that $\langle M_1 \mid E_1[(\texttt{st}\ \mathbf{r_{d1}[i], r_{s1};}\ \rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow$ and $\langle M_2 \mid E_2[(\texttt{st}\ \mathbf{r_{d2}[i], r_{s2};}\ \rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow$, or $\text{running}(W.k, \langle M_1 \mid E_1[(\texttt{st}\ \mathbf{r_{d1}[i], r_{s1};}\ \rho_1(\mathbf{I_1}), \cdot)]\rangle)$ and $\text{running}(W.k, \langle M_2 \mid E_2[(\texttt{st}\ \mathbf{r_{d2}[i], r_{s2};}\ \rho_2(\mathbf{I_2}), \cdot)]\rangle)$.
  Let $M_1 = (\mathbf{H_1, R_1, S_1})$ and $M_2 = (\mathbf{H_2, R_2, S_2})$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \text{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$. From the latter, we can have the following fact for island i_{reg}.
  We have that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\hat{\mathbf{R}}_\mathbf{1}(\mathbf{r_s}) = \mathbf{w_1}$ and $\hat{\mathbf{R}}_\mathbf{2}(\mathbf{r_s}) = \mathbf{w_2}$ (which are the same $\mathbf{w_1}$ and $\mathbf{w_2}$ from our preliminary facts above).
  Next, by the reduction semantics of our language, with all of the above facts in hand, we have that:

$$\langle M_1 \mid E_1[(\texttt{sst}\ \mathbf{i, r_s;}\ \rho_1(\mathbf{I_1}), \cdot)]\rangle \longrightarrow \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle$$

  and

$$\langle M_2 \mid E_2[(\texttt{sst}\ \mathbf{i, r_s;}\ \rho_2(\mathbf{I_2}), \cdot)]\rangle \longrightarrow \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle$$

  where $M_1' = (\mathbf{H_1, R_1, S_1'})$ with $\mathbf{S_1'} = S_1[i \mapsto w_1]$, and $M_2' = (\mathbf{H_2, R_2, S_2'})$ with $\mathbf{S_2'} = S_2[i \mapsto w_2]$.
  Note that in order to complete our proof, it suffices to show:

$$\begin{array}{l}(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge\ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee \\ (\text{running}(W.k-1, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge\ \text{running}(W.k-1, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))\end{array}$$

  We proceed by showing that $(M_1', M_2') : W$ and then instantiating our final hypothesis $\Psi; \Delta; \chi; \tau_0 :: \cdots :: \tau_\mathbf{i} :: \sigma; \mathbf{r_s}$ $\texttt{sst}\ \mathbf{i, r_s; I_1} \approx_\mathbf{I} \texttt{sst}\ \mathbf{i, r_s; I_2}$.
  - We claim that $(M_1', M_2') : W$. We prove this claim by establishing the following:
    * $\vdash M_1' : W.\Phi_1$ and $\vdash M_2' : W.\Phi_2$, both of which easily follow from $(M_1, M_2) : W$ and the fact that we have updated the ith element of each stack with well-typed words of the same type, i.e., with words with types $\rho_1(\tau')$ and $\rho_2(\tau')$ respectively.
    * We assume that $W.k > 0$ and we must show that

$$(\triangleright W, M_1', M_2') \in \bigotimes\{\, \text{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$$

      The latter follows from $(M_1, M_2) : W$ and monotonicity of MemRel given that we establish the following claim for island i_{stk}, $(\triangleright W', \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction) \in \text{currentMR}(W'(i_{\text{stk}}))$.
      Recall that $W'.S_i = S_i'$. Thus we obtain trivially that $(\triangleright W', S_1', S_2') \in \{(\widetilde{W}, W'.S_1, W'.S_2) \mid \widetilde{W} \in \text{World}_{W.k}\}$. From the latter, we establish directly our claim that

$$(\triangleright W', S_1', S_2') \in \text{currentMR}(W'(i_{\text{stk}}))$$

  - Next, we instantiate our final hypothesis with W' and ρ. Note that $\rho \in \mathcal{D}[\![\Delta]\!]$ by assumption, $W' \in \mathcal{H}[\![\Psi]\!]$ by heap monotonicity (Lemma 1.9). We claim that $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho$ by the first case of Lemma 1.20. Moreover we claim that $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma']\!]\rho$ Our claim follows directly from the fourt case of lemma 1.21 since, above, we have

established that $(W', w_1, w_2) \in \mathcal{W}[\![\tau']\!]$ and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. Hence, we have that

$$(W', (\rho_1(\mathbf{I_1}, \cdot)), (\rho_2(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]\!]\rho$$

Instantiate the above with E_1 and E_2. Note that we have $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]\!]\rho$ which follows from $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau_\mathbf{r}; \sigma_\mathbf{r}]\!]\rho$ by monotonicity for evaluation contexts (Lemma 1.10), since our choice of W', $W' \sqsupseteq_{\text{pub}} W$ our second hypothesis let us easily establish all the premises of that lemma, including that $\text{ret-addr}_1(W, r_s) = \text{ret-addr}_1(W, i)$ and $\text{ret-addr}_2(W, r_s) = \text{ret-addr}_2(W, i)$.
Hence, we have

$$(W', E_1[(\rho_1(\mathbf{I_1}, \cdot))], E_2[(\rho_2(\mathbf{I_2}), \cdot)]) \in \mathcal{O}.$$

Instantiate the latter with M_1' and M_2', noting that $(M_1', M_2') : W'$. Hence, we have

$$\begin{aligned}&(\langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle \downarrow \ \wedge \ \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle \downarrow) \ \vee \\ &(\text{running}(W.k, \langle M_1' \mid E_1[(\rho_1(\mathbf{I_1}), \cdot)]\rangle) \ \wedge \ \text{running}(W.k, \langle M_2' \mid E_2[(\rho_2(\mathbf{I_2}), \cdot)]\rangle))\end{aligned}$$

which implies what we needed to show.

□

Lemma 1.60 (Return from Call)
If $\chi(\mathbf{r}) = \mathbf{box}\,\forall[].\{\mathbf{r}' : \tau; \sigma\}^{\mathbf{q}'}$ and $\chi(\mathbf{r}') = \tau$, then $\Psi; \Delta; \chi; \sigma; \mathbf{r} \vdash \mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\} \approx_\mathbf{I} \mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\}$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{r} \vdash \mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. From the first premise, we have that $\text{ret-type}(\mathbf{r}, \chi, \sigma) = \tau; \sigma$. We need to show that

$$(W, \rho_1((\mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\}, \cdot)), \rho_2((\mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\}, \cdot))) = (W, (\mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\}, \cdot), (\mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\}, \cdot)) \in \mathcal{E}[\![\mathbf{r} \vdash \tau; \sigma]\!]\rho.$$

Consider arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{r} \vdash \tau; \sigma]\!]\rho$. We need to show that

$$(W, E_1[(\mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\}, \cdot)], E_2[(\mathtt{ret}\ \mathbf{r}\ \{\mathbf{r}'\}, \cdot)]) \in \mathcal{O}$$

Instantiate $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{r} \vdash \tau; \sigma]\!]\rho$ with W, $\mathbf{r}$, $\mathbf{r}'$, and $\mathbf{r}'$. Note that $W \sqsupseteq_{\text{pub}} W$ (by reflexivity), the return markers are both $\mathbf{r}$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We also claim that $(\triangleright W, W.\mathbf{R_1}(\mathbf{r}'), W.\mathbf{R_2}(\mathbf{r}')) \in \mathcal{W}[\![\tau]\!]\rho$. Instantiate $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ with $(\triangleright W, W.\mathbf{R_1}\restriction, W.\mathbf{R_2}\restriction)$ noting that the latter is in $\text{currentMR}(W(i_{\text{reg}})$ by the definition of $\text{island}_{\text{reg}}$ and that $\triangleright W \sqsupseteq W$. Hence, we have $(\triangleright W, W.\mathbf{R_1}\restriction, W.\mathbf{R_2}\restriction) \in \mathcal{R}[\![\chi]\!]\rho$. By the second premise, we have that $(\mathbf{r}' : \tau) \in \chi$. Therefore our claim follows from the definition of $\mathcal{R}[\![\chi]\!]\rho$. Thus, we have exactly what we needed to show. □

Lemma 1.61 (Return at End)
If $\chi(\mathbf{r}) = \tau$, then $\Psi; \Delta; \chi; \sigma; \mathbf{end}\{\tau; \sigma\} \vdash \mathtt{ret}\ \mathbf{end}\{\tau; \sigma\}\ \{\mathbf{r}\} \approx_\mathbf{I} \mathtt{ret}\ \mathbf{end}\{\tau; \sigma\}\ \{\mathbf{r}\}$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{end}\{\tau; \sigma\} \vdash \mathtt{ret}\ \mathbf{end}\{\tau; \sigma\}\ \{\mathbf{r}\}$.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1((\mathtt{ret}\ \mathbf{end}\{\tau; \sigma\}\ \{\mathbf{r}\}, \cdot)), \rho_2((\mathtt{ret}\ \mathbf{end}\{\tau; \sigma\}\ \{\mathbf{r}\}, \cdot))) \\ &= (W, (\mathtt{ret}\ \mathbf{end}\{\rho_1(\tau); \rho_1(\sigma)\}\ \{\mathbf{r}\}, \cdot), (\mathtt{ret}\ \mathbf{end}\{\rho_1(\tau); \rho_1(\sigma)\}\ \{\mathbf{r}\}, \cdot)) \in \mathcal{E}[\![\mathbf{end}\{\tau; \sigma\} \vdash \tau; \sigma]\!]\rho.\end{aligned}$$

Consider arbitrary E_1 and E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau;\sigma\} \vdash \tau;\sigma]\!]\rho$. We need to show that

$$(W, E_1[(\mathtt{ret}\ \mathbf{end}\{\rho_1(\tau);\rho_1(\sigma)\}\ \{\mathbf{r}\}, \cdot)], E_2[(\mathtt{ret}\ \mathbf{end}\{\rho_1(\tau);\rho_1(\sigma)\}\ \{\mathbf{r}\}, \cdot)]) \in \mathcal{O}$$

Instantiate $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau;\sigma\} \vdash \tau;\sigma]\!]\rho$ with W, $\mathbf{end}\{\tau;\sigma\}$, $\mathbf{r}$, and $\mathbf{r}$. Note that $W \sqsupseteq_{\text{pub}} W$ (by reflexivity), the return markers are both $\mathbf{end}\{\tau;\sigma\}$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We also claim that $(\triangleright W, W.\mathbf{R_1}(\mathbf{r}), W.\mathbf{R_2}(\mathbf{r})) \in \mathcal{W}[\![\tau]\!]\rho$. Instantiate $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ with $(\triangleright W, W.\mathbf{R_1}\restriction, W.\mathbf{R_2}\restriction)$ noting that the latter is in $\text{currentMR}(W(i_{\text{reg}})$ by the definition of $\text{island}_{\text{reg}}$ and that $\triangleright W \sqsupseteq W$. Hence, we have $(\triangleright W, W.\mathbf{R_1}\restriction, W.\mathbf{R_2}\restriction) \in \mathcal{R}[\![\chi]\!]\rho$. By the first premise, we have that $(\mathbf{r} : \tau) \in \chi$. Therefore our claim follows from the definition of $\mathcal{R}[\![\chi]\!]\rho$. Thus, we have exactly what we needed to show. □

Lemma 1.62 (Jump)
If $\Psi; \Delta; \chi \vdash \mathbf{u_1} \approx_{\text{u}} \mathbf{u_2} : \mathbf{box}\,\forall[].\{\chi';\sigma\}^{\mathbf{q}}$, $\Delta \vdash \chi \le \chi'$, and $\cdot[\Delta]; \chi; \sigma \vdash \mathbf{q}$,
then $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{jmp}\ \mathbf{u_1} \approx_{\mathbf{I}} \mathtt{jmp}\ \mathbf{u_2}$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{jmp}\ \mathbf{u_1}$ and $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{jmp}\ \mathbf{u_2}$ follow from the premises.

Consider arbitrary W and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$(W, \rho_1((\mathtt{jmp}\ \mathbf{u_1}, \cdot)), \rho_2((\mathtt{jmp}\ \mathbf{u_2}, \cdot))) = (W, (\mathtt{jmp}\ \rho_1(\mathbf{u_1}), \cdot), (\mathtt{jmp}\ \rho_2(\mathbf{u_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho.$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts $\mathbf{E_i}$ and memories M_i, we can immediately show that $\text{running}(0, \langle M_i \mid E_i[e_i] \rangle)$.

In the following, assume $W.k > 0$ and let $\tau_{\mathbf{r}}; \sigma_{\mathbf{r}} = \text{ret-type}(\mathbf{q}, \chi, \sigma)$.

Instantiate the first premise with W and ρ, noting $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$. Thus we have that $(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\chi';\sigma\}^{\mathbf{q}}]\!]\rho$. From the definition of the latter, we have that $W.\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) = \ell_{\mathbf{i}}[\overline{\omega_{\mathbf{i}}}]$.

We will use Lemma 1.11 to complete the proof, so we start by establishing the premises of that lemma.

- We claim that $(W, (\mathtt{jmp}\ \rho_1(\mathbf{u_1}), \cdot), (\mathtt{jmp}\ \rho_2(\mathbf{u_2}), \cdot)) \in \text{TermAtom}[\mathbf{q} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\rho$. To establish this, we must show $W.\Psi_i; \cdot; W.\chi_{\mathbf{i}}; W.\sigma_{\mathbf{i}}; \rho_i(\mathbf{q}) \vdash (\mathtt{jmp}\ \rho_i(\mathbf{u_i}), \cdot) : \rho_i(\tau_{\mathbf{r}}); \rho_i(\sigma_{\mathbf{r}})$. The latter follows from $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash \mathtt{jmp}\ \mathbf{u_i}$ using the component typing rule and the properties of W and ρ that we have by assumption.
- Let $W' = \triangleright W$. Note that $W' \in \text{World}$ since $W.k > 0$ and $W \in \text{World}$.
- Note that $\triangleright W \sqsupseteq_{\text{pub}} W$ by Lemma 1.6.
- Consider arbitrary $(M_1, M_2) : W$. Let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$.
  From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\, \text{currentMR}(\theta) \mid \theta \in W.\Theta \,\}$. From the latter, we have two facts, one for island i_{reg} and the other for island i_{box}.
  First, we have that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) = \ell_{\mathbf{i}}[\overline{\omega_{\mathbf{i}}}]$.
  Second, we have that there exist some $\mathbf{H_{b1}} \subseteq \mathbf{H_1}$ and $\mathbf{H_{b2}} \subseteq \mathbf{H_2}$ such that $(\triangleright W, \mathbf{H_{b1}}\restriction, \mathbf{H_{b2}}\restriction) \in \text{currentMR}(W(i_{\text{box}}))$. We use the latter to instantiate $(W, \ell_1[\overline{\omega_1}], \ell_2[\overline{\omega_2}]) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\chi';\sigma\}^{\mathbf{q}}]\!]\rho$, noting that $\triangleright W \sqsupset W$, which allows us to conclude:
  - $\mathbf{H_{bi}}(\ell_{\mathbf{i}}) = \mathbf{code}[\overline{\beta_{\mathbf{i}}}]\{\chi_{\mathbf{i}};\sigma_{\mathbf{i}}\}^{\mathbf{q_i}}.\mathbf{I_i}$,
  - $\rho_i(\chi') = \chi_{\mathbf{i}}[\overline{\omega_{\mathbf{i}}/\beta_{\mathbf{i}}}]$,
  - $\rho_i(\sigma) = \sigma_{\mathbf{i}}[\overline{\omega_{\mathbf{i}}/\beta_{\mathbf{i}}}]$,
  - $\rho_i(\mathbf{q}) = \mathbf{q_i}[\overline{\omega_{\mathbf{i}}/\beta_{\mathbf{i}}}]$, and
  - $(\triangleright W, (\mathbf{code}[]\{\chi_1;\sigma_1\}^{\mathbf{q_1}}.\mathbf{I_1})[\overline{\omega_1/\beta_1}], (\mathbf{code}[]\{\chi_2;\sigma_2\}^{\mathbf{q_2}}.\mathbf{I_2})[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[].\{\chi';\sigma\}^{\mathbf{q}}]\!]\rho$

Hence, we have that $\hat{\mathbf{R}}_\mathbf{i}(\rho_i(\mathbf{u_i})) = \ell_\mathbf{i}[\overline{\omega_\mathbf{i}}]$ and $\mathbf{H}_\mathbf{i}(\ell_\mathbf{i}) = \mathbf{code}[\overline{\beta_\mathbf{i}}]\{\chi_\mathbf{i}; \sigma_\mathbf{i}\}^{\mathbf{q_i}}.\mathbf{I_i}$, and

$$\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\mathtt{jmp}\, \rho_i(\mathbf{u_i}), \cdot)\rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid (\mathbf{I_i}[\overline{\omega_i/\beta_i}], \cdot)\rangle$$

Let $M_i' = M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$. Note that $(M_1', M_2') : W'$ is equivalent to $(M_1, M_2) : \triangleright W$, which follows by Lemma 1.6.

- Note that $W.k \leq W'.k + 1$ since $W'.k = (\triangleright W).k = W.k - 1$.
- Note that $\mathbf{q} \neq \epsilon$, which follows from the third hypothesis. Further, since we haven't changed the world, we can see that the the return address does not change.
- Note that

$$\begin{aligned}
&(\triangleright W, (\mathbf{code}[]\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\omega_1/\beta_1}],\\
&\qquad (\mathbf{code}[]\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[].\{\chi'; \sigma\}^{\mathbf{q}}]\!]\rho\\
\equiv\ &(\triangleright W, \mathbf{code}[]\{\chi_1[\overline{\omega_1/\beta_1}]; \sigma_1[\overline{\omega_1/\beta_1}]\}^{\mathbf{q}_1[\overline{\omega_1/\beta_1}]}.\mathbf{I}_1[\overline{\omega_1/\beta_1}],\\
&\qquad \mathbf{code}[]\{\chi_2[\overline{\omega_2/\beta_2}]; \sigma_2[\overline{\omega_2/\beta_2}]\}^{\mathbf{q}_2[\overline{\omega_2/\beta_2}]}.\mathbf{I}_2[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[].\{\chi'; \sigma\}^{\mathbf{q}}]\!]\rho\\
\equiv\ &(\triangleright W, (\mathbf{code}[]\{\rho_1(\chi')]; \rho_1(\sigma)\}^{\rho_1(\mathbf{q})}.\mathbf{I}_1[\overline{\omega_1/\beta_1}],\\
&\qquad \mathbf{code}[]\{\rho_2(\chi'); \rho_2(\sigma)\}^{\rho_2(\mathbf{q})}.\mathbf{I}_2[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[].\{\chi'; \sigma\}^{\mathbf{q}}]\!]\rho
\end{aligned}$$

  Instantiate the latter with $\triangleright W$ and $\tau; \mathbf{sigma'} = \text{ret-type}(\mathbf{q}, \chi, \sigma)$. We note the following:

  - We have $\triangleright W \sqsupseteq \triangleright W$ by reflexivity.
  - We claim that $\text{ret-type}(\mathbf{q}, \chi', \sigma) =_\rho \text{ret-type}(\mathbf{q}, \chi, \sigma)$. Since $\mathbf{q} \neq \epsilon$, the latter is immediate except in the case when $\mathbf{q}$ is some register $\mathbf{r'}$, in which case we must show that $\mathbf{r'} \in \text{dom}(\chi')$ since otherwise $\text{ret-type}(\mathbf{q}, \chi', \sigma)$ would be undefined. But note that from our first premise, it follows that $\mathbf{\Delta} \vdash \mathbf{box}\,\forall[].\{\chi'; \sigma\}^{\mathbf{q}}$. By inversion of typing rules, we have that $\mathbf{\Delta} \vdash \forall[].\{\chi'; \sigma\}^{\mathbf{q}}$, and hence $\mathbf{\Delta}[]; \chi'; \sigma \vdash \mathbf{q}$. From the latter it follows that $\text{ret-type}(\mathbf{q}, \chi', \sigma)$ is defined. Hence, if $\mathbf{q}$ is some register $\mathbf{r'}$, it must be that $\mathbf{r'} \in \text{dom}(\chi')$. Moreover, from the second premise, it follows that $\chi'(\mathbf{r'}) = \chi(\mathbf{r'})$. This is enough to establish our claim.
  - We claim that $\text{currentMR}((\triangleright W)(i_{\text{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\chi']\!]\rho$. To show this, consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}((\triangleright W)(i_{\text{reg}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W$. We must show that

$$(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\chi']\!]\rho$$

    Note that $(\triangleright W).k = W.k - 1$ and that $\text{currentMR}((\triangleright W)(i_{\text{reg}})) = \lfloor \text{currentMR}(W(i_{\text{reg}}))\rfloor_{W.k-1}$. Thus, $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{reg}}))$. Using the latter we can instantiate $\text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ with $(\widetilde{W}, M_1, M_2)$, noting that $\widetilde{W} \sqsupseteq W$ (by transitivity of $\sqsupseteq$), which gives us $(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\chi]\!]\rho$. Finally, by Lemma 1.19 (register-file subtyping implies inclusion) we have that $\mathcal{R}[\![\chi]\!]\rho \subseteq \mathcal{R}[\![\chi']\!]\rho$, which is sufficient to show what we need.
  - We note that $\text{currentMR}(\triangleright W(i_{\text{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\sigma]\!]\rho$. To show this, consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}((\triangleright W)(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W$. We must show that

$$(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\sigma]\!]\rho$$

    Note that $(\triangleright W).k = W.k - 1$ and that $\text{currentMR}((\triangleright W)(i_{\text{stk}})) = \lfloor \text{currentMR}(W(i_{\text{stk}}))\rfloor_{W.k-1}$. Thus, $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{stk}}))$. Using the latter we can instantiate $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$ with $(\widetilde{W}, M_1, M_2)$, noting that $\widetilde{W} \sqsupseteq W$ (by transitivity of $\sqsupseteq$), which gives us $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\sigma]\!]\rho$ as needed.

  Hence, we can conclude that

$$(\triangleright W, (\rho_1(\mathbf{I_1}[\overline{\omega_1/\beta_1}]), \cdot), (\rho_2(\mathbf{I_2}[\overline{\omega_2/\beta_2}]), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi', \sigma)]\!]\rho$$

Now, the result follows by Lemma 1.11. □

Lemma 1.63 (Call)
Given the following:

- $\Psi; \Delta; \chi \vdash \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{u_2} : \mathbf{box}\,\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathrm{q}}}$,
- ret-addr-type$(\hat{\mathrm{q}}, \hat{\chi}, \hat{\sigma}) = \forall[].\{\mathbf{r} : \tau; \hat{\sigma}'\}^{\epsilon}$,
- $\Delta \vdash \sigma_0$,
- $\Delta \vdash \forall[].\{\hat{\chi}[\sigma_0/\zeta][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]; \hat{\sigma}[\sigma_0/\zeta][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]\}^{\hat{\mathrm{q}}}$,
- $\Delta \vdash \chi \leq \hat{\chi}[\sigma_0/\zeta][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]$,
- $\sigma = \tau_0 :: \cdots :: \tau_{\mathbf{j}} :: \sigma_0$,
- $\hat{\sigma} = \tau_0 :: \cdots :: \tau_{\mathbf{j}} :: \zeta$,
- $\mathbf{j} < \mathbf{i}$, and
- $\hat{\sigma}' = \tau'_0 :: \cdots :: \tau'_{\mathbf{k}} :: \zeta$,

we have that $\Psi; \Delta; \chi; \sigma; \mathbf{i} \vdash \mathtt{call}\ \mathbf{u_1}\ \{\sigma_0, \mathbf{i}+\mathbf{k}-\mathbf{j}\} \approx_{\mathbf{I}} \mathtt{call}\ \mathbf{u_2}\ \{\sigma_0, \mathbf{i}+\mathbf{k}-\mathbf{j}\}$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{i} \vdash \mathtt{call}\ \mathbf{u_1}\ \{\sigma_0, \mathbf{i}+\mathbf{k}-\mathbf{j}\}$ and $\Psi; \Delta; \chi; \sigma; \mathbf{i} \vdash \mathtt{call}\ \mathbf{u_2}\ \{\sigma_0, \mathbf{i}+\mathbf{k}-\mathbf{j}\}$ follow from the premises.

Consider arbitrary W, γ, and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$, currentMR$(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\mathrm{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1((\mathtt{call}\ \mathbf{u_1}\ \{\sigma_0, \mathbf{i}+\mathbf{k}-\mathbf{j}\}, \cdot))), \rho_2(\gamma_2((\mathtt{call}\ \mathbf{u_2}\ \{\sigma_0, \mathbf{i}+\mathbf{k}-\mathbf{j}\}, \cdot))))$$
$$= (W, (\mathtt{call}\ \rho_1(\mathbf{u_1})\ \{\rho_1(\sigma_0), \mathbf{i}+\mathbf{k}-\mathbf{j}\}, \cdot), (\mathtt{call}\ \rho_2(\mathbf{u_2})\ \{\rho_2(\sigma_0), \mathbf{i}+\mathbf{k}-\mathbf{j}\}, \cdot)) \in \mathcal{E}[\![\mathbf{i} \vdash \text{ret-type}(\mathbf{i}, \chi, \sigma)]\!]\rho.$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts E_i and memories M_i, we can immediately show that running$(0, \langle M_i \mid E_i[e_i] \rangle)$.

In the following, assume $W.k > 0$ and let $\tau_{\mathbf{r}}; \sigma_{\mathbf{r}} = \text{ret-type}(\mathbf{i}, \chi, \sigma)$.

Consider arbitrary $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{i} \vdash \tau_{\mathbf{r}}; \sigma_{\mathbf{r}}]\!]\rho$. We need to show that

$$(W, E_1[(\mathtt{call}\ \rho_1(\mathbf{u_1})\ \{\rho_1(\sigma_0), \mathbf{i}+\mathbf{k}-\mathbf{j}\}, \cdot)], E_2[(\mathtt{call}\ \rho_2(\mathbf{u_2})\ \{\rho_2(\sigma_0), \mathbf{i}+\mathbf{k}-\mathbf{j}\}, \cdot)]) \in \mathcal{O}$$

Consider arbitrary $(M_1, M_2) : W$. We must show that for $i \in \{1, 2\}$, either both configurations $\langle M_i \mid E_i[(\mathtt{call}\ \rho_i(\mathbf{u_i})\ \{\rho_i(\sigma_0), \mathbf{i}+\mathbf{k}-\mathbf{j}\}, \cdot)] \rangle$ terminate or both are running at $W.k$.

Instantiate the first premise with W and ρ, noting $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and currentMR$(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$. Thus we have that $(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\mathbf{box}\,\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathrm{q}}}]\!]\rho$. From the definition of the latter, we have that $W.\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) = \ell_{\mathbf{i}}[\overline{\omega_{\mathbf{i}}}]$.

Next, let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$.

From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\,\text{currentMR}(\theta) \mid \theta \in W.\Theta\,\}$. From the latter, we have three facts, one each for islands i_{reg}, i_{stk}, and i_{box}.

First, we have that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\mathrm{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) = \ell_{\mathbf{i}}[\overline{\omega_{\mathbf{i}}}]$.

Second, we have $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \text{currentMR}(W(i_{\mathrm{stk}}))$. From the latter and currentMR$(W(i_{\mathrm{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$, it follows that $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathcal{S}[\![\sigma]\!]\rho$. From the premise $\sigma = \tau_0 :: \cdots :: \tau_{\mathbf{j}} :: \sigma_0$, it follows that $\mathbf{S_1} = \mathbf{w_{10}} :: \cdots :: \mathbf{w_{1j}} :: \mathbf{S_{10}}$, $\mathbf{S_2} = \mathbf{w_{20}} :: \cdots :: \mathbf{w_{2j}} :: \mathbf{S_{20}}$, $(\triangleright W, \mathbf{w_{1n}}, \mathbf{w_{2n}}) \in \mathcal{W}[\![\tau_{\mathbf{n}}]\!]\rho$ for $n \in \{0, \ldots, j\}$, and $(\triangleright W, \mathbf{S_{10}}\restriction, \mathbf{S_{20}}\restriction) \in \mathcal{S}[\![\sigma_0]\!]\rho$.

Third, we have that there exist some $\mathbf{H_{b1}} \subseteq \mathbf{H_1}$ and $\mathbf{H_{b2}} \subseteq \mathbf{H_2}$ such that $(\triangleright W, \mathbf{H_{b1}}\restriction, \mathbf{H_{b2}}\restriction) \in \text{currentMR}(W(i_{\mathrm{box}}))$. We use the latter to instantiate $(W, \ell_1[\overline{\omega_1}], \ell_2[\overline{\omega_2}]) \in \mathcal{W}[\![\mathbf{box}\,\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathrm{q}}}]\!]\rho$, noting that $\triangleright W \sqsupset W$, which allows us to conclude:

- $\mathbf{H_{bi}}(\ell_i) = \mathbf{code}[\overline{\beta_i}, \zeta, \epsilon]\{\chi_i; \sigma_i\}^{q_i}.\mathbf{I_i}$,
- $\rho_i(\hat{\chi}) = \chi_i[\overline{\omega_i/\beta_i}]$,
- $\rho_i(\hat{\sigma}) = \sigma_i[\overline{\omega_i/\beta_i}]$,
- $\rho_i(\hat{\mathbf{q}}) = \mathbf{q_i}[\overline{\omega_i/\beta_i}]$, and
- $(\triangleright W, (\mathbf{code}[\zeta, \epsilon]\{\chi_1; \sigma_1\}^{q_1}.\mathbf{I_1})[\overline{\omega_1/\beta_1}], (\mathbf{code}[\zeta, \epsilon]\{\chi_2; \sigma_2\}^{q_2}.\mathbf{I_2})[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{q}}]\!]\rho$

Hence, we know that $\hat{\mathbf{R}}_i(\rho_i(\mathbf{u_i})) = \ell_i[\overline{\omega_i}]$ and $\mathbf{H_i}(\ell_i) = \mathbf{code}[\overline{\beta_i}, \zeta, \epsilon]\{\chi_i; \sigma_i\}^{q_i}.\mathbf{I_i}$, and therefore

$$\langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid E_i[(\mathtt{call}\ \rho_i(\mathbf{u_i})\ \{\rho_i(\sigma_0), \mathbf{i+k-j}\}, \cdot)]\rangle \longmapsto^1 \langle (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i}) \mid E_i[(\mathbf{I_i}[\overline{\omega_i/\beta_i}][\rho_i(\sigma_0)/\zeta][(\mathbf{i+k-j})/\epsilon], \cdot)]\rangle$$

Therefore, it suffices to show that for $i \in \{1, 2\}$, either both configurations $\langle M_i \mid E_i[(\mathbf{I_i}[\overline{\omega_i/\beta_i}][\rho_i(\sigma_0)/\zeta][(\mathbf{i+k-j})/\epsilon], \cdot)]\rangle$ terminate or both are running at $W.k-1$.

We proceed by noting that from the premise ret-addr-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \forall[].\{\mathbf{r} : \tau; \hat{\sigma'}\}^{\epsilon}$, by definition of ret-addr-type, it must be that either $\hat{\mathbf{q}} = \mathbf{r_{ra}}$ or $\hat{\mathbf{q}} = \mathbf{i_{ra}}$.

Further, we note that we have

$$\begin{aligned}
&(\triangleright W, (\mathbf{code}[\zeta, \epsilon]\{\chi_1; \sigma_1\}^{q_1}.\mathbf{I_1})[\overline{\omega_1/\beta_1}], \\
&\qquad (\mathbf{code}[\zeta, \epsilon]\{\chi_2; \sigma_2\}^{q_2}.\mathbf{I_2})[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{q}}]\!]\rho \\
\equiv\ &(\triangleright W, \mathbf{code}[\zeta, \epsilon]\{\chi_1[\overline{\omega_1/\beta_1}]; \sigma_1[\overline{\omega_1/\beta_1}]\}^{q_1[\overline{\omega_1/\beta_1}]}.\mathbf{I_1}[\overline{\omega_1/\beta_1}], \\
&\qquad \mathbf{code}[\zeta, \epsilon]\{\chi_2[\overline{\omega_2/\beta_2}]; \sigma_2[\overline{\omega_2/\beta_2}]\}^{q_2[\overline{\omega_2/\beta_2}]}.\mathbf{I_2}[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{q}}]\!]\rho \\
\equiv\ &(\triangleright W, \mathbf{code}[\zeta, \epsilon]\{\rho_1(\hat{\chi}); \rho_1(\hat{\sigma})\}^{\rho_1(\hat{\mathbf{q}})}.\mathbf{I_1}[\overline{\omega_1/\beta_1}], \\
&\qquad \mathbf{code}[\zeta, \epsilon]\{\rho_2(\hat{\chi}); \rho_2(\hat{\sigma})\}^{\rho_2(\hat{\mathbf{q}})}.\mathbf{I_2}[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{q}}]\!]\rho
\end{aligned}$$

Instantiate the latter with $\triangleright W$, ρ^*, τ, and $\hat{\sigma'}$, where

$$\begin{aligned}
&\rho^* = \{\zeta \mapsto (\rho_1(\sigma_0), \rho_2(\sigma_0), \varphi_S), \epsilon \mapsto (\mathbf{i+k-j}, \mathbf{i+k-j})\} \text{ and} \\
&\varphi_S = \{(\widetilde{W}, \mathbf{S_{10}}\restriction, \mathbf{S_{20}}\restriction) \mid \widetilde{W} \sqsupseteq \triangleright W\}
\end{aligned}$$

We note the following:

- We have $\triangleright W \sqsupseteq \triangleright W$ by reflexivity.
- Note that $\rho^* \in \mathcal{D}[\![\zeta, \epsilon]\!]$, which follows by the definition of $\mathcal{D}[\![\cdot]\!]$ and by applying Lemma 1.18 to $(\triangleright W, \mathbf{S_{10}}\restriction, \mathbf{S_{20}}\restriction) \in \mathcal{S}[\![\sigma_0]\!]\rho$.
- Let $\rho' = \rho \cup \rho^*$.
- Note that $\tau; \hat{\sigma'} =_{\rho'}$ ret-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma})$. This follows by applying the substitutions ρ'_1 and ρ'_2 to ret-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \tau; \hat{\sigma'}$, which in turn follows from the premise ret-addr-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \forall[].\{\mathbf{r} : \tau; \hat{\sigma'}\}^{\epsilon}$.
- We claim that currentMR$(W(i_{\text{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\hat{\chi}]\!]\rho'$. (†)

  To show this, consider arbitrary $(\widetilde{W}, M_1^*, M_2^*) \in$ currentMR$(W(i_{\text{reg}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W$. We must show that
  $$(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{R}[\![\hat{\chi}]\!]\rho'$$
  Instantiate currentMR$(W(i_{\text{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\chi]\!]\rho$ with $(\widetilde{W}, M_1^*, M_2^*) \in$ currentMR$(W(i_{\text{reg}}))$, noting that $\widetilde{W} \sqsupseteq \triangleright W$, which gives us $(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{R}[\![\chi]\!]\rho$. Finally, by Lemma 1.19 (register-file subtyping implies inclusion) applied to the premise $\mathbf{\Delta} \vdash \chi \leq \hat{\chi}[\sigma_0/\zeta][(\mathbf{i+k-j})/\epsilon]$ we have that $\mathcal{R}[\![\chi]\!]\rho \subseteq \mathcal{R}[\![\hat{\chi}[\sigma_0/\zeta][(\mathbf{i+k-j})/\epsilon]]\!]\rho$.
  Therefore, it remains to show that $\mathcal{R}[\![\hat{\chi}[\sigma_0/\zeta][(\mathbf{i+k-j})/\epsilon]]\!]\rho \subseteq \mathcal{R}[\![\hat{\chi}]\!]\rho'$.
  Next, we examine two cases based on the value of $\hat{\mathbf{q}}$:

Case $\hat{\mathbf{q}} = \mathbf{i_{ra}}$ Hence, from the premise $\Delta \vdash \hat{\chi} \setminus \hat{\mathbf{q}}$, we have that $\Delta \vdash \hat{\chi}$. Therefore, note that

$$\mathcal{R}[\![\hat{\chi}[\sigma_0/\zeta][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]]\!]\rho \equiv \mathcal{R}[\![\hat{\chi}]\!]\rho \quad \text{since } \zeta, \epsilon \notin \text{ftv}(\hat{\chi}) \equiv \mathcal{R}[\![\hat{\chi}]\!]\rho' \quad \text{by Lemma 1.13}$$

which suffices to show what we needed.

Case $\hat{\mathbf{q}} = \mathbf{r_{ra}}$ Hence, from the premise $\Delta \vdash \hat{\chi} \setminus \hat{\mathbf{q}}$, we actually have that $\Delta \vdash \hat{\chi} \setminus \mathbf{r_{ra}}$.
Hence, it follows that $\mathcal{R}[\![(\hat{\chi}[\sigma_0/\zeta][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]) \setminus \mathbf{r_{ra}}]\!]\rho \equiv \mathcal{R}[\![(\hat{\chi}) \setminus \mathbf{r_{ra}}]\!]\rho'$.
Therefore, it remains to show the following for the remaining register $\mathbf{r_{ra}}$, whose type by our premises must be $\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}$ where $\Delta \vdash \tau$:

$$\mathcal{R}[\![\mathbf{r_{ra}}:\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'[\sigma_0/\zeta]\}^{\epsilon[(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]}]\!]\rho \subseteq \mathcal{R}[\![\mathbf{r_{ra}}:\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$$

Therefore, we must show for arbitrary
$(W^*, \mathbf{R}_1^*\restriction, \mathbf{R}_2^*\restriction) \in \mathcal{R}[\![\mathbf{r_{ra}}:\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'[\sigma_0/\zeta]\}^{\epsilon[(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]}]\!]\rho$ that $(W^*, \mathbf{R}_1^*\restriction, \mathbf{R}_2^*\restriction) \in \mathcal{R}[\![\mathbf{r_{ra}}:\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$. Hence, it suffices to show that

$$(W^*, \mathbf{R}_1^*(\mathbf{r_{ra}}), \mathbf{R}_2^*(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'.$$

Note, from our most recent assumption, we have
$(W^*, \mathbf{R}_1^*(\mathbf{r_{ra}}), \mathbf{R}_2^*(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'[\sigma_0/\zeta]\}^{\epsilon[(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]}]\!]\rho$. By the substitution (Lemmas 1.15 and 1.16), the latter is equivalent to $(W^*, \mathbf{R}_1^*(\mathbf{r_{ra}}), \mathbf{R}_2^*(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho^*$ where $\rho^* = \rho[\zeta \mapsto (\rho_1(\sigma_0), \rho_2(\sigma_0), \mathcal{S}[\![\sigma_0]\!]\rho), \epsilon \mapsto (\mathbf{i}+\mathbf{k}-\mathbf{j}, \mathbf{i}+\mathbf{k}-\mathbf{j})]$.
To show $(W^*, \mathbf{R}_1^*(\mathbf{r_{ra}}), \mathbf{R}_2^*(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$, consider arbitrary $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W^*(i_{\text{box}}))$ such that $\widetilde{W} \sqsupset W^*$.
Instantiating $(W^*, \mathbf{R}_1^*(\mathbf{r_{ra}}), \mathbf{R}_2^*(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho^*$, we end up in a position where we have to show that

$$\mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho^* \;\subseteq\; \mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$$

The latter follows by expanding the definitions and noting that it suffices to prove the following three facts:

- For any world W', $\text{currentMR}(W'(i_{\text{reg}})) \in_{W'} \mathcal{R}[\![\mathbf{r}:\tau]\!]\rho'$ implies $\text{currentMR}(W'(i_{\text{reg}})) \in_{W'} \mathcal{R}[\![\mathbf{r}:\tau]\!]\rho*$ since both are equal to $\text{currentMR}(W'(i_{\text{reg}})) \in_{W'} \mathcal{R}[\![\mathbf{r}:\tau]\!]\rho$ because $\Delta \vdash \tau$.
- For any world W', given that $\text{currentMR}(W'(i_{\text{stk}})) \in_{W'} \mathcal{S}[\![\hat{\sigma}']\!]\rho'$ we claim that $\text{currentMR}(W'(i_{\text{reg}})) \in_{W'} \mathcal{S}[\![\hat{\sigma}']\!]\rho^*$.
  Note that $\hat{\sigma}' = \tau_0' :: \cdots :: \tau_k' :: \zeta$, and from the premise $\Delta \vdash \hat{\sigma}'[\sigma_0/\zeta]$, we know that $\zeta \notin \text{ftv}(\tau_n')$ for $n \in \{0, \ldots, k\}$. Therefore, it suffices to show that

  $$\mathcal{S}[\![\zeta]\!]\rho' \subseteq \mathcal{S}[\![\zeta]\!]\rho^* \equiv \varphi_S \subseteq \mathcal{S}[\![\sigma_0]\!]\rho$$

  which is immediate from our choice of φ_S above.
- Finally, we note that $\tau_r; \sigma_R =_{\rho'} \text{ret-type}(\epsilon, \{\mathbf{r}:\tau\}, \hat{\sigma}')$. (We show the latter in detail later in the proof so we won't duplicate it here.) Therefore, note that $\mathcal{E}[\![\epsilon \vdash \tau_r; \sigma_r]\!]\rho^* = \mathcal{E}[\![\mathbf{i}+\mathbf{k}-\mathbf{j} \vdash \tau_r; \sigma_r]\!]\rho' = \mathcal{E}[\![\mathbf{i}+\mathbf{k}-\mathbf{j} \vdash \tau_r; \sigma_r]\!]\rho$.

This completes our proof of the claim marked (†).

- Note that $\text{currentMR}((\triangleright W)(i_{\text{reg}})) \in_{\triangleright W} \mathcal{R}[\![\hat{\chi}]\!]\rho'$, which follows from $\text{currentMR}(W(i_{\text{reg}})) \in_{\triangleright W} \mathcal{R}[\![\hat{\chi}]\!]$.
- We claim that $\text{currentMR}(W(i_{\text{stk}})) \in_{\triangleright W} \mathcal{S}[\![\hat{\sigma}]\!]\rho'$ (‡)
  To show this, consider arbitrary $(\widetilde{W}, M_1^*, M_2^*) \in \text{currentMR}(W(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W$. We must show that

  $$(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{S}[\![\hat{\sigma}]\!]\rho'.$$

  Recall that above we had $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \text{currentMR}(W(i_{\text{stk}}))$. Therefore, by definition of the i_{stk} island, it must be that $M_1^* = \mathbf{S_1}\restriction$ and $M_2^* = \mathbf{S_2}\restriction$. Hence, it remains for us to show:

  $$(\widetilde{W}, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathcal{S}[\![\hat{\sigma}]\!]\rho'$$

where we recall that

$$\begin{aligned}
&\mathbf{S_1} = \mathbf{w_{10}} :: \cdots :: \mathbf{w_{1j}} :: \mathbf{S_{10}} \\
&\mathbf{S_2} = \mathbf{w_{20}} :: \cdots :: \mathbf{w_{2j}} :: \mathbf{S_{20}} \\
&\hat{\boldsymbol{\sigma}} = \boldsymbol{\tau_0} :: \cdots :: \boldsymbol{\tau_j} :: \boldsymbol{\zeta} \\
&\text{and } \rho' = \rho[\boldsymbol{\zeta} \mapsto (\rho_1(\boldsymbol{\sigma_0}), \rho_2(\boldsymbol{\sigma_0}), \varphi_S), \boldsymbol{\epsilon} \mapsto (\mathbf{i}+\mathbf{k}-\mathbf{j}, \mathbf{i}+\mathbf{k}-\mathbf{j})] \\
&\text{with } \varphi_S = \{(\widetilde{W}, \mathbf{S_{10}}\restriction, \mathbf{S_{20}}\restriction) | \widetilde{W} \sqsupseteq \triangleright W\}.
\end{aligned}$$

Thus, to show $(\widetilde{W}, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathcal{S}[\![\hat{\boldsymbol{\sigma}}]\!]\rho'$, it suffices to show

- $(\widetilde{W}, \mathbf{w_{1n}}, \mathbf{w_{2n}}) \in \mathcal{W}[\![\boldsymbol{\tau_n}]\!]\rho'$ for $n \in \{0, \ldots, j\}$, which follows from $(\triangleright W, \mathbf{w_{1n}}, \mathbf{w_{2n}}) \in \mathcal{W}[\![\boldsymbol{\tau_n}]\!]$ by monotonicity (Lemma 1.8).
- $(\widetilde{W}, \mathbf{S_{10}}, \mathbf{S_{20}}) \in \mathcal{S}[\![\boldsymbol{\zeta}]\!]\rho'$, which is immediate from $\mathcal{S}[\![\boldsymbol{\zeta}]\!]\rho' = \varphi_S$ (by definition) and our choice of φ_S above.

- Note that $\text{currentMR}((\triangleright W)(i_{\text{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\hat{\boldsymbol{\sigma}}]\!]\rho'$, which follows from $\text{currentMR}(W(i_{\text{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\hat{\boldsymbol{\sigma}}]\!]\rho'$.

Hence, we can conclude that

$$(\triangleright W, (\mathbf{I_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}][\rho_1(\boldsymbol{\sigma_0})/\boldsymbol{\zeta}][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\boldsymbol{\epsilon}], \cdot), (\mathbf{I_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}][\rho_2(\boldsymbol{\sigma_0})/\boldsymbol{\zeta}][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\boldsymbol{\epsilon}], \cdot)) \in \mathcal{E}[\![\hat{\mathbf{q}} \vdash \boldsymbol{\tau}; \hat{\boldsymbol{\sigma}}']\!]\rho'$$

Next, we instantiate the latter with E_1 and E_2, for which we need to show the following:

$$(\triangleright W, E_1, E_2) \in \mathcal{K}[\![\hat{\mathbf{q}} \vdash \boldsymbol{\tau}; \hat{\boldsymbol{\sigma}}']\!]\rho'$$

Consider arbitrary W', $\hat{\mathbf{q}}'$, $\mathbf{r_1}$, $\mathbf{r_2}$ such that

1. $W' \sqsupseteq_{\text{pub}} \triangleright W$,
2. $(\hat{\mathbf{q}} =_{\rho'} \hat{\mathbf{q}}' =_{\rho'} \mathbf{end}\{\hat{\boldsymbol{\tau}}; \hat{\boldsymbol{\sigma}}'\}) \vee$
   $(\exists \mathbf{r_0}.\hat{\mathbf{q}}' = \mathbf{r_0} \wedge \text{ret-addr}_1(\triangleright W, \rho_1'(\hat{\mathbf{q}})) = W'.\mathbf{R_1}(\mathbf{r_0}) \wedge \text{ret-addr}_2(\triangleright W, \rho_2'(\hat{\mathbf{q}})) = W'.\mathbf{R_2}(\mathbf{r_0}) \wedge$
   $\text{ret-reg}_1(W', \mathbf{r_0}) = \mathbf{r_1} \wedge \text{ret-reg}_2(W', \mathbf{r_0}) = \mathbf{r_2})$
3. $(\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho'$
4. $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\hat{\boldsymbol{\sigma}}']\!]\rho'$

We are required to show

$$(W', (\mathtt{ret}\ \rho_1(\hat{\mathbf{q}}')\ \{\mathbf{r_1}\}, \cdot), (\mathtt{ret}\ \rho_2(\hat{\mathbf{q}}')\ \{\mathbf{r_2}\}, \cdot)) \in \mathcal{O}$$

Next, we collect some facts before we proceed:

- Note that from assumption (4) above, it follows that $\triangleright W'$ is defined, which means that $W'.k > 0$.
- Recall from above that either $\hat{\mathbf{q}} = \mathbf{r_{ra}}$ or $\hat{\mathbf{q}} = \mathbf{i_{ra}}$. This fact lets us refine (3) above—that is, since $\hat{\mathbf{q}} \neq_{\rho'} \mathbf{end}\{\hat{\boldsymbol{\tau}}; \hat{\boldsymbol{\sigma}}'\}$, we know that

$$\exists \mathbf{r_0}.\hat{\mathbf{q}}' = \mathbf{r_0} \wedge \text{ret-addr}_1(\triangleright W, \rho_1'(\hat{\mathbf{q}})) = W'.\mathbf{R_1}(\mathbf{r_0}) \wedge \text{ret-addr}_2(\triangleright W, \rho_2'(\hat{\mathbf{q}})) = W'.\mathbf{R_2}(\mathbf{r_0})) \wedge$$
$$\text{ret-reg}_1(W', \mathbf{r_0})) = \mathbf{r_1} \wedge \text{ret-reg}_2(W', \mathbf{r_0})) = \mathbf{r_2})$$

Hence, $\rho_i(\hat{\mathbf{q}}') = \rho_i(\mathbf{r_0}) = \mathbf{r_0}$. Therefore, it suffices to show

$$(W', E_1[(\texttt{ret}\ \mathbf{r_0}\ \{\mathbf{r_1}\}, \cdot)], E_2[(\texttt{ret}\ \mathbf{r_0}\ \{\mathbf{r_2}\}, \cdot)]) \in \mathcal{O}$$

Consider arbitrary $(M_1', M_2') : W'$. We must show that for $i \in \{1, 2\}$, either both configurations $\langle M_i' \mid E_1[(\texttt{ret}\ \mathbf{r_0}\ \{\mathbf{r_i}\}, \cdot)]\rangle$ terminate or both are running at $W'.k$.

Next, we establish that $(\triangleright W, W'.\mathbf{R_1}(\mathbf{r_0}), W'.\mathbf{R_2}(\mathbf{r_0})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon]\!]\rho'$ by considering the two cases of $\hat{\mathbf{q}}$:

Case $\hat{\mathbf{q}} = \mathbf{r_{ra}}$: Hence, by the definition of ret-addr-type we have

$$\begin{aligned}\text{ret-addr-type}(\hat{\mathbf{q}}, \hat{\boldsymbol{\chi}}, \hat{\boldsymbol{\sigma}}) &= \text{ret-addr-type}(\mathbf{r_{ra}}, \hat{\boldsymbol{\chi}}, \hat{\boldsymbol{\sigma}}) \\ &= \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon \text{ where } \hat{\boldsymbol{\chi}}(\mathbf{r_{ra}}) = \mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon\end{aligned}$$

Since $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \text{currentMR}(W(i_{\text{reg}}))$ (from above) and $\text{currentMR}(W(i_{\text{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\hat{\boldsymbol{\chi}}]\!]\rho'$ († from above), it follows that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in \mathcal{R}[\![\hat{\boldsymbol{\chi}}]\!]\rho'$. From the latter, since $\mathbf{r_{ra}} : \mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon \in \hat{\boldsymbol{\chi}}$, we have

$$(\triangleright W, \mathbf{R_1}(\mathbf{r_{ra}}), \mathbf{R_2}(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon]\!]\rho'.$$

Since $\mathbf{R_i} = W.\mathbf{R_i} = \triangleright W.\mathbf{R_i}$, the above is equivalent to

$$(\triangleright W, \triangleright W.\mathbf{R_1}(\mathbf{r_{ra}}), \triangleright W.\mathbf{R_2}(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon]\!]\rho'.$$

Moreover, note that we have the following equalities

$$\begin{aligned}&\text{ret-addr}_i(\triangleright W, \hat{\mathbf{q}}) \\ &= \text{ret-addr}_i(\triangleright W, \mathbf{r_{ra}}) && \text{since } \hat{\mathbf{q}} = \mathbf{r_{ra}} \\ &= (\triangleright W).\mathbf{R_i}(\mathbf{r_{ra}}) && \text{by definition of ret-addr}_i \\ &= W'.\mathbf{R_i}(\mathbf{r_0}) && \text{since ret-addr}_i(\triangleright W, \hat{\mathbf{q}}) = W'.\mathbf{R_i}(\mathbf{r_0})\end{aligned}$$

Hence, we have

$$(\triangleright W, W'.\mathbf{R_1}(\mathbf{r_0}), W'.\mathbf{R_2}(\mathbf{r_0})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon]\!]\rho'.$$

Case $\hat{\mathbf{q}} = \mathbf{i_{ra}}$: Hence, by the definition of ret-addr-type we have

$$\begin{aligned}\text{ret-addr-type}(\hat{\mathbf{q}}, \hat{\boldsymbol{\chi}}, \hat{\boldsymbol{\sigma}}) &= \text{ret-addr-type}(\mathbf{i_{ra}}, \hat{\boldsymbol{\chi}}, \hat{\boldsymbol{\sigma}}) \\ &= \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon \text{ where } \hat{\boldsymbol{\sigma}}(\mathbf{i_{ra}}) = \mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon\end{aligned}$$

Since $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \text{currentMR}(W(i_{\text{stk}}))$ (from above) and $\text{currentMR}(W(i_{\text{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\hat{\boldsymbol{\sigma}}]\!]\rho'$ (‡ from above), it follows that $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathcal{S}[\![\hat{\boldsymbol{\sigma}}]\!]\rho'$. From the latter, since $\mathbf{i_{ra}} : \mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon \in \hat{\boldsymbol{\sigma}}$, we have

$$(\triangleright W, \mathbf{S_1}(\mathbf{i_{ra}}), \mathbf{S_2}(\mathbf{i_{ra}})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon]\!]\rho'.$$

Since $\mathbf{S_i} = W.\mathbf{S_i} = \triangleright W.\mathbf{S_i}$, the above is equivalent to

$$(\triangleright W, \triangleright W.\mathbf{S_1}(\mathbf{i_{ra}}), \triangleright W.\mathbf{S_2}(\mathbf{i_{ra}})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon]\!]\rho'.$$

Moreover, note that we have the following equalities

$$\begin{aligned}&\text{ret-addr}_i(\triangleright W, \hat{\mathbf{q}}) \\ &= \text{ret-addr}_i(\triangleright W, \mathbf{i_{ra}}) && \text{since } \hat{\mathbf{q}} = \mathbf{i_{ra}} \\ &= (\triangleright W).\mathbf{S_i}(\mathbf{i_{ra}}) && \text{by definition of ret-addr}_i \\ &= W'.\mathbf{R_i}(\mathbf{r_0}) && \text{since ret-addr}_i(\triangleright W, \hat{\mathbf{q}}) = W'.\mathbf{R_i}(\mathbf{r_0})\end{aligned}$$

Hence, we have

$$(\triangleright W, W'.\mathbf{R_1}(\mathbf{r_0}), W'.\mathbf{R_2}(\mathbf{r_0})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r} : \tau; \hat{\boldsymbol{\sigma}}'\}^\epsilon]\!]\rho'.$$

Since $W' \sqsupseteq \triangleright W$, by monotonicity we have

$$(W', W'.\mathbf{R_1}(\mathbf{r_0}), W'.\mathbf{R_2}(\mathbf{r_0})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'.$$

From the above, we have that $W'.\Psi_1;\cdot \vdash W'.\mathbf{R_1}(\mathbf{r_0}) : \rho_1'(\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon})$ and $W'.\Psi_2;\cdot \vdash W'.\mathbf{R_2}(\mathbf{r_0}) : \rho_2'(\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon})$. These facts put together with $W' \in$ World and ret-reg$_1(W', \mathbf{r_0})$ allow us to conclude $\mathbf{r} = \mathbf{r_1} = \mathbf{r_2}$.

Next, let $M_i' = (\mathbf{H_i'}, \mathbf{R_i'}, \mathbf{S_i'})$.

From $(M_1', M_2') : W'$, since $W'.k > 0$, we have $(\triangleright W', M_1', M_2') \in \bigotimes\{\,\text{currentMR}(\theta) \mid \theta \in W'.\Theta\,\}$. From the latter, we have three facts, one each for islands i_{reg}, i_{stk}, and i_{box}.

First, we have that $(\triangleright W', \mathbf{R_1'}\restriction, \mathbf{R_2'}\restriction) \in \text{currentMR}(W'(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i'} = W'.\mathbf{R_i}$ and, hence, we have $(\triangleright W', \mathbf{R_1'}(\mathbf{r_0}), \mathbf{R_1'}(\mathbf{r_0})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$. From the latter, it must be that $\mathbf{R_i'}(\mathbf{r_0}) = \ell_i'[\overline{\omega_i'}]$.

Second, we have $(\triangleright W', \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction) \in \text{currentMR}(W'(i_{\text{stk}}))$. Hence, we can instantiate assumption (5) from above, i.e., currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\hat{\sigma}']\!]\rho'$, with $(\triangleright W', \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction)$, noting $\triangleright W' \sqsupseteq W'$ (by Lemma 1.6), which allows us to conclude that $(\triangleright W', \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction) \in \mathcal{S}[\![\hat{\sigma}']\!]\rho'$. From the premise $\hat{\sigma}' = \tau_0' :: \cdots :: \tau_k' :: \zeta$, it follows that $\mathbf{S_1'} = \mathbf{w_{10}'} :: \cdots :: \mathbf{w_{1k}'} :: \mathbf{S_{10}'}$, $\mathbf{S_2'} = \mathbf{w_{20}'} :: \cdots :: \mathbf{w_{2l}'} :: \mathbf{S_{20}'}$, $(\triangleright W', \mathbf{w_{1n}'}, \mathbf{w_{2n}'}) \in \mathcal{W}[\![\tau_n']\!]\rho'$ for $n \in \{0, \ldots, k\}$, and $(\triangleright W', \mathbf{S_{10}'}\restriction, \mathbf{S_{20}'}\restriction) \in \mathcal{S}[\![\zeta]\!]\rho'$. From the latter, since $\mathcal{S}[\![\zeta]\!]\rho' = \varphi_S$, it follows that $\mathbf{S_{10}'} = \mathbf{S_{10}}$ and $\mathbf{S_{20}'} = \mathbf{S_{20}}$.

Third, we have that there exist some $\mathbf{H_{b1}'} \subseteq \mathbf{H_1'}$ and $\mathbf{H_{b2}'} \subseteq \mathbf{H_2'}$ such that $(\triangleright W', \mathbf{H_{b1}'}\restriction, \mathbf{H_{b2}'}\restriction) \in \text{currentMR}(W'(i_{\text{box}}))$.

Instantiate $(W', \ell_1'[\overline{\omega_1'}], \ell_1'[\overline{\omega_1'}]) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$ with $(\triangleright W', \mathbf{H_{b1}'}\restriction, \mathbf{H_{b2}'}\restriction) \in \text{currentMR}(W'(i_{\text{box}}))$, noting that $\triangleright W' \sqsupset W'$ by Lemma 1.6. Hence, we have that

- $\mathbf{H_{bi}'}(\ell_i') = \mathbf{code}[\overline{\beta_i'}]\{\chi_i';\sigma_i'\}^{\mathbf{q_i'}}.\mathbf{I_i'}$,
- $\rho_i'(\mathbf{r}:\tau) = \chi_i'[\overline{\omega_i'/\beta_i'}]$,
- $\rho_i'(\hat{\sigma}') = \sigma_i'[\overline{\omega_i'/\beta_i'}]$,
- $\rho_i'(\epsilon) = \mathbf{q_i'}[\overline{\omega_i'/\beta_i'}]$, and
- $(\triangleright W', (\mathbf{code}[]\{\chi_1';\sigma_1'\}^{\mathbf{q_1'}}.\mathbf{I_1'})[\overline{\omega_1'/\beta_1'}], (\mathbf{code}[]\{\chi_2';\sigma_2'\}^{\mathbf{q_2'}}.\mathbf{I_2'})[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$

Hence, we know that $\hat{\mathbf{R}}_i'(\mathbf{r_0}) = \ell_i'[\overline{\omega_i'}]$ and $\mathbf{H_i'}(\ell_i') = \mathbf{code}[\overline{\beta_i'}]\{\chi_i';\sigma_i'\}^{\mathbf{q_i'}}.\mathbf{I_i'}$, and therefore

$$\langle(\mathbf{H_i'}, \mathbf{R_i'}, \mathbf{S_i'}) \mid E_i[(\mathbf{ret}\ \mathbf{r_0}\ \{\mathbf{r_i}\}, \cdot)]\rangle \longmapsto^1 \langle(\mathbf{H_i'}, \mathbf{R_i'}, \mathbf{S_i'}) \mid E_i[(\mathbf{I_i'}[\overline{\omega_i'/\beta_i'}], \cdot)]\rangle$$

Therefore, it suffices to show that for $i \in \{1, 2\}$, either both configurations $\langle M_i' \mid E_i[(\mathbf{I_i'}[\overline{\omega_i'/\beta_i'}], \cdot)]\rangle$ terminate or both are running at $W'.k - 1$.

We proceed by noting that

$$\begin{aligned}
&(\triangleright W', (\mathbf{code}[]\{\chi_1';\sigma_1'\}^{\mathbf{q_1'}}.\mathbf{I_1'})[\overline{\omega_1'/\beta_1'}], (\mathbf{code}[]\{\chi_2';\sigma_2'\}^{\mathbf{q_2'}}.\mathbf{I_2'})[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho' \\
\equiv\ &(\triangleright W', \mathbf{code}[]\{\chi_1'[\overline{\omega_1'/\beta_1'}];\sigma_1'[\overline{\omega_1'/\beta_1'}]\}^{\mathbf{q_1'}[\overline{\omega_1'/\beta_1'}]}.\mathbf{I_1'}[\overline{\omega_1'/\beta_1'}], \\
&\qquad \mathbf{code}[]\{\chi_2'[\overline{\omega_2'/\beta_2'}];\sigma_2'[\overline{\omega_2'/\beta_2'}]\}^{\mathbf{q_2'}[\overline{\omega_2'/\beta_2'}]}.\mathbf{I_2'}[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho' \\
\equiv\ &(\triangleright W', \mathbf{code}[]\{\rho_1'(\mathbf{r}:\tau);\rho_1'(\hat{\sigma}')\}^{\rho_1'(\epsilon)}.\mathbf{I_1'}[\overline{\omega_1'/\beta_1'}], \\
&\qquad \mathbf{code}[]\{\rho_2'(\mathbf{r}:\tau);\rho_2'(\hat{\sigma}')\}^{\rho_2'(\epsilon)}.\mathbf{I_2'}[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho' \\
\equiv\ &(\triangleright W', \mathbf{code}[]\{\mathbf{r}:\rho_1'(\tau);\rho_1'(\hat{\sigma}')\}^{\mathbf{i}+\mathbf{k}-\mathbf{j}}.\mathbf{I_1'}[\overline{\omega_1'/\beta_1'}], \\
&\qquad \mathbf{code}[]\{\mathbf{r}:\rho_2'(\tau);\rho_2'(\hat{\sigma}')\}^{\mathbf{i}+\mathbf{k}-\mathbf{j}}.\mathbf{I_2'}[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'
\end{aligned}$$

Instantiate the latter with $\triangleright W'$, $\emptyset \in \mathcal{D}[\![\cdot]\!]$, $\tau_{\mathbf{r}}$, and $\sigma_{\mathbf{r}}$.

We note the following:

- We have $\triangleright W' \sqsupseteq \triangleright W'$ by reflexivity.
- We claim that $\boldsymbol{\tau_r}; \boldsymbol{\sigma_r} =_{\rho'} \text{ret-type}(\epsilon, \{\mathbf{r} : \boldsymbol{\tau}\}, \hat{\boldsymbol{\sigma}}')$. It suffices to show for $i \in \{1, 2\}$:

$$\begin{aligned}
&\rho_i'(\boldsymbol{\tau_r}); \rho_i'(\boldsymbol{\sigma_r}) = \text{ret-type}(\rho_i'(\epsilon), \rho_i'(\{\mathbf{r} : \boldsymbol{\tau}\}), \rho_i'(\hat{\boldsymbol{\sigma}}')) \\
&\equiv \rho_i'(\boldsymbol{\tau_r}); \rho_i'(\boldsymbol{\sigma_r}) = \text{ret-type}(\mathbf{i} + \mathbf{k} - \mathbf{j}, \rho_i'(\{\mathbf{r} : \boldsymbol{\tau}\}), \rho_i'(\boldsymbol{\tau_0} :: \cdots :: \boldsymbol{\tau_j} :: \boldsymbol{\zeta})) \\
&\equiv \rho_i'(\boldsymbol{\tau_r}); \rho_i'(\boldsymbol{\sigma_r}) = \text{ret-type}(\mathbf{i} + \mathbf{k} - \mathbf{j}, \rho_i'(\{\mathbf{r} : \boldsymbol{\tau}\}), \rho_i'(\boldsymbol{\tau_0}) :: \cdots :: \rho_i'(\boldsymbol{\tau_j}) :: \rho_i'(\boldsymbol{\zeta})) \\
&\equiv \rho_i'(\boldsymbol{\tau_r}); \rho_i'(\boldsymbol{\sigma_r}) = \text{ret-type}(\mathbf{i} + \mathbf{k} - \mathbf{j}, \rho_i'(\{\mathbf{r} : \boldsymbol{\tau}\}), \rho_i'(\boldsymbol{\tau_0}) :: \cdots :: \rho_i'(\boldsymbol{\tau_j}) :: \rho_i(\boldsymbol{\sigma_0}))
\end{aligned}$$

  Recall that $\boldsymbol{\tau_r}; \boldsymbol{\sigma_r} = \text{ret-type}(\mathbf{i}, \chi, \boldsymbol{\sigma})$ where $\boldsymbol{\sigma} = \boldsymbol{\tau_0} :: \cdots :: \boldsymbol{\tau_j} :: \boldsymbol{\sigma_0}$. Hence, $FTV(\boldsymbol{\tau_r}; \boldsymbol{\sigma_r}) \subseteq \boldsymbol{\Delta}$ and $\boldsymbol{\sigma_0}(\mathbf{i} - \mathbf{j} - 1) = \mathbf{box}\, \forall [].\{\mathbf{r}' : \boldsymbol{\tau_r}; \boldsymbol{\sigma_r}\}^{\mathbf{q}'}$ for some $\mathbf{r}'$ and $\mathbf{q}'$.
  Putting these facts together, we have that

$$\begin{aligned}
\rho_i'(\hat{\boldsymbol{\sigma}}'(\mathbf{i} + \mathbf{k} - \mathbf{j})) &= \rho_i'(\boldsymbol{\sigma_0}(\mathbf{i} + \mathbf{k} - \mathbf{j} - (\mathbf{k} + 1))) \\
&= \rho_i(\boldsymbol{\sigma_0}(\mathbf{i} - \mathbf{j} - 1)) \\
&= \rho_i(\mathbf{box}\, \forall [].\{\mathbf{r}' : \boldsymbol{\tau_r}; \boldsymbol{\sigma_r}\}^{\mathbf{q}'})
\end{aligned}$$

  which means that $\rho_i(\boldsymbol{\tau_r}); \rho_i(\boldsymbol{\sigma_r}) = \text{ret-type}(\mathbf{i} + \mathbf{k} - \mathbf{j}, \rho_i'(\{\mathbf{r} : \boldsymbol{\tau}\}), \rho_i'(\hat{\boldsymbol{\sigma}}'))$ as we needed to show.
- We claim that $\text{currentMR}((\triangleright W')(i_{\text{reg}})) \Subset_{\triangleright W'} \mathcal{R}[\![\mathbf{r} : \boldsymbol{\tau}]\!]\rho'$.
  To show this, consider arbitrary $(\widetilde{W}, M_1^*, M_2^*) \in \text{currentMR}((\triangleright W')(i_{\text{reg}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W'$. We must show that

$$(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{R}[\![\mathbf{r} : \boldsymbol{\tau}]\!]\rho'$$

  Note that since $W'.k > 0$ (from above), $(\triangleright W').k = W'.k - 1$ and therefore

$$\text{currentMR}((\triangleright W')(i_{\text{reg}})) = \lfloor \text{currentMR}(W'(i_{\text{reg}})) \rfloor_{W'.k-1} \subseteq \text{currentMR}(W'(i_{\text{reg}}))$$

  Thus,$(\widetilde{W}, M_1^*, M_2^*) \in \text{currentMR}(W'(i_{\text{reg}}))$. Moreover, since we already have $(\triangleright W', \mathbf{R}_1'\restriction, \mathbf{R}_2'\restriction) \in \text{currentMR}(W'(i_{\text{reg}}))$, by the definition of island i_{reg}, it must be that $M_i^* = \mathbf{R_i'}$. Therefore, we are required to show

$$(\widetilde{W}, \mathbf{R}_1'\restriction, \mathbf{R}_2'\restriction) \in \mathcal{R}[\![\mathbf{r} : \boldsymbol{\tau}]\!]\rho'.$$

  It suffices to show

$$(\widetilde{W}, \mathbf{R}_1'(\mathbf{r}), \mathbf{R}_2'(\mathbf{r})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho'$$

  which follows by monotonicity (Lemma 1.8) from our earlier assumption (4), namely $(\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho'$ since $\mathbf{r} = \mathbf{r_1} = \mathbf{r_2}$ (from above) and since $W'.\mathbf{R_1} = \mathbf{R_1'}$ and $W'.\mathbf{R_2} = \mathbf{R_2'}$.
- We claim that $\text{currentMR}((\triangleright W')(i_{\text{stk}})) \Subset_{\triangleright W'} \mathcal{S}[\![\hat{\boldsymbol{\sigma}}']\!]\rho'$.
  To show this, consider arbitrary $(\widetilde{W}, M_1^*, M_2^*) \in \text{currentMR}((\triangleright W')(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W'$. We must show that

$$(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{S}[\![\hat{\boldsymbol{\sigma}}']\!]\rho'.$$

  Note that since $W'.k > 0$ (from above), $(\triangleright W).k = W.k - 1$ and therefore

$$\text{currentMR}((\triangleright W')(i_{\text{stk}})) = \lfloor \text{currentMR}(W'(i_{\text{stk}})) \rfloor_{W'.k-1} \subseteq \text{currentMR}(W'(i_{\text{stk}}))$$

  Thus,$(\widetilde{W}, M_1^*, M_2^*) \in \text{currentMR}(W'(i_{\text{stk}}))$. Moreover, since we already have $(\triangleright W', \mathbf{S}_1'\restriction, \mathbf{S}_2'\restriction) \in \text{currentMR}(W'(i_{\text{stk}}))$, by the definition of island i_{stk}, it must be that $M_i^* = \mathbf{S_i'}$. Therefore, we are required to show

$$(\widetilde{W}, \mathbf{S}_1'\restriction, \mathbf{S}_2'\restriction) \in \mathcal{S}[\![\hat{\boldsymbol{\sigma}}']\!]\rho'.$$

  Since $\hat{\boldsymbol{\sigma}}' = \boldsymbol{\tau_0'} :: \cdots :: \boldsymbol{\tau_k'} :: \boldsymbol{\zeta}$, with $\mathbf{S_1'} = \mathbf{w_{10}'} :: \cdots :: \mathbf{w_{1k}'} :: \mathbf{S_{10}'}$ and $\mathbf{S_2'} = \mathbf{w_{20}'} :: \cdots :: \mathbf{w_{2l}'} :: \mathbf{S_{20}'}$, the above follows from

– $(\widetilde{W}, \mathbf{w'_{1n}}, \mathbf{w'_{2n}}) \in \mathcal{W}[\![\tau'_n]\!]\rho'$ for $n \in \{0, \ldots, k\}$, which follow by monotonicity (Lemma 1.8) from $(\triangleright W', \mathbf{w'_{1n}}, \mathbf{w'_{2n}}) \in \mathcal{W}[\![\tau'_n]\!]\rho'$, and

– $(\widetilde{W}, \mathbf{S'_{10}}\restriction, \mathbf{S'_{20}}\restriction) \in \mathcal{S}[\![\zeta]\!]\rho'$, which follows from $\mathcal{S}[\![\zeta]\!]\rho' = \varphi_S$ and the definition of φ_S since $\mathbf{S'_{10}} = \mathbf{S_{10}}$ and $\mathbf{S'_{20}} = \mathbf{S_{20}}$.

Hence, we can conclude that

$$(\triangleright W', (\mathbf{I'_1}[\overline{\omega'_1/\beta'_1}], \cdot), (\mathbf{I'_2}[\overline{\omega'_2/\beta'_2}], \cdot)) \in \mathcal{E}[\![\epsilon \vdash \tau_r; \sigma_r]\!]\rho'$$

By Lemma 1.16, and noting that $FTV(\tau_r; \sigma_r) \subseteq \mathbf{\Delta}$ we have

$$(\triangleright W', (\mathbf{I'_1}[\overline{\omega'_1/\beta'_1}], \cdot), (\mathbf{I'_2}[\overline{\omega'_2/\beta'_2}], \cdot)) \in \mathcal{E}[\![\mathbf{i + k - j} \vdash \tau_r; \sigma_r]\!]\rho. \tag{18}$$

Near the beginning of this proof, we had assumed $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{i} \vdash \tau_r; \sigma_r]\!]\rho$.

We now apply Lemma 1.10 (monotonicity for evaluation contexts) to $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{i} \vdash \tau_r; \sigma_r]\!]\rho$, noting the following:

- $\triangleright W' \sqsupseteq_{\text{pub}} W$, which follows by transitivity of $\sqsupseteq_{\text{pub}}$ and the following $\triangleright W' \sqsupseteq_{\text{pub}} W' \sqsupseteq_{\text{pub}} \triangleright W \sqsupseteq_{\text{pub}} W$ (which we have from above and from Lemma 1.6).
- $\text{ret-addr}_1(W, \mathbf{i}) = \text{ret-addr}_1(\triangleright W', \mathbf{i + k - j})$ and $\text{ret-addr}_2(W, \mathbf{i}) = \text{ret-addr}_2(\triangleright W', \mathbf{i + k - j})$, which follow from:

$$\begin{aligned} \text{ret-addr}_1(W, \mathbf{i}) &= W.\mathbf{S_1(i)} \\ &= (\mathbf{w_{10} :: \cdots :: w_{1j} :: S_{10}})(\mathbf{i}) \\ &= \mathbf{S_{10}(i - j + 1)} \end{aligned}$$

and

$$\begin{aligned} \text{ret-addr}_1(\triangleright W', \mathbf{i + k - j}) &= W'.\mathbf{S_1(i + k - j)} \\ &= (\mathbf{w'_{10} :: \cdots :: w'_{1k} :: S_{10}})(\mathbf{i + k - j}) \\ &= \mathbf{S_{10}(i + k - j - (k + 1))} \\ &= \mathbf{S_{10}(i - j - 1)} \end{aligned}$$

and analogously for ret-addr_2.

Hence, we have that $(\triangleright W', E_1, E_2) \in \mathcal{K}[\![\mathbf{i + k - j} \vdash \tau_r; \sigma_r]\!]\rho$.

Instantiating 18 with the above, we have $(\triangleright W', E_1[(\mathbf{I'_1}[\overline{\omega'_1/\beta'_1}], \cdot)], E_2[(\mathbf{I'_2}[\overline{\omega'_2/\beta'_2}], \cdot)]) \in \mathcal{O}$.

By instantiating the latter with M'_1 and M'_2, noting $(M'_1, M'_2) : \triangleright W'$, we have that $\langle M'_1 \mid E_1[(\mathbf{I'_1}[\overline{\omega'_1/\beta'_1}], \cdot)]\rangle$ and $\langle M'_2 \mid E_2[(\mathbf{I'_2}[\overline{\omega'_2/\beta'_2}], \cdot)]\rangle$ either both terminate or are both running at $W'.k - 1$, as we needed to show.

Hence, we conclude that

$$(\triangleright W, E_1[(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\sigma_0)/\zeta][\mathbf{q_1}/\epsilon], \cdot)], E_2[(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\sigma_0)/\zeta][\mathbf{q_2}/\epsilon], \cdot)]) \in \mathcal{O}$$

Now instantiate the above with M_1 and M_2, noting that we have $(M_1, M_2) : \triangleright W$ by Lemma 1.6 since $(M_1, M_2) : W$. Hence, we have that for $i \in \{1, 2\}$, either both configurations $\langle M_i \mid E_1[(\mathbf{I_i}[\overline{\omega_i/\beta_i}][\rho_i(\sigma_0)/\zeta][\mathbf{q_i}/\epsilon], \cdot)]\rangle$ terminate or both are running at $W.k - 1$, which is exactly what we needed to show!

□

Lemma 1.64 (Call from Top Level)
Given the following:

- $\mathbf{\Psi}; \mathbf{\Delta}; \chi \vdash \mathbf{u_1} \approx_u \mathbf{u_2} : \mathbf{box}\, \forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{q}}$,

- ret-addr-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \forall[].\{\mathbf{r} : \tau; \hat{\sigma}'\}^{\epsilon}$,
- $\Delta \vdash \sigma_0$,
- $\Delta \vdash \forall[].\{\hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]; \hat{\sigma}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]\}^{\hat{\mathbf{q}}}$,
- $\Delta \vdash \chi \leq \hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]$,
- $\sigma = \overline{\tau} :: \sigma_0$,
- $\hat{\sigma} = \overline{\tau} :: \zeta$, and
- $\hat{\sigma}' = \overline{\tau'} :: \zeta$,

we have that $\Psi; \Delta; \chi; \sigma; \mathbf{end}\{\tau^*; \sigma^*\} \vdash \texttt{call}\ \mathbf{u_1}\ \{\sigma_0, \mathbf{end}\{\tau^*; \sigma^*\}\} \approx_{\mathbf{I}} \texttt{call}\ \mathbf{u_2}\ \{\sigma_0, \mathbf{end}\{\tau^*; \sigma^*\}\}$.

Proof

Clearly, $\Psi; \Delta; \chi; \sigma; \mathbf{end}\{\tau^*; \sigma^*\} \vdash \texttt{call}\ \mathbf{u_1}\ \{\sigma_0, \mathbf{end}\{\tau^*; \sigma^*\}\}$ and $\Psi; \Delta; \chi; \sigma; \mathbf{end}\{\tau^*; \sigma^*\} \vdash \texttt{call}\ \mathbf{u_2}\ \{\sigma_0, \mathbf{end}\{\tau^*; \sigma^*\}\}$ follow from the premises.

Consider arbitrary W,γ, and ρ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1((\texttt{call}\ \mathbf{u_1}\ \{\sigma_0, \mathbf{end}\{\tau^*; \sigma^*\}\}, \cdot))), \rho_2(\gamma_2((\texttt{call}\ \mathbf{u_2}\ \{\sigma_0, \mathbf{end}\{\tau^*; \sigma^*\}\}, \cdot))))\\ &= (W, (\texttt{call}\ \rho_1(\mathbf{u_1})\ \{\rho_1(\sigma_0), \mathbf{end}\{\rho_1(\tau^*); \rho_1(\sigma^*)\}\}, \cdot), (\texttt{call}\ \rho_2(\mathbf{u_2})\ \{\rho_2(\sigma_0), \mathbf{end}\{\rho_1(\tau^*); \rho_1(\sigma^*)\}\}, \cdot))\\ &\qquad \in \mathcal{E}[\![\mathbf{end}\{\tau^*; \sigma^*\} \vdash \tau^*; \sigma^*]\!]\rho.\end{aligned}$$

Note that if $W.k = 0$ then we are done, since for any evaluation contexts E_i and memories M_i, we can immediately show that running$(0, \langle M_i \mid E_i[e_i]\rangle)$.

In the following, assume $W.k > 0$. Also, let $\mathbf{q_i} = \mathbf{end}\{\rho_i(\tau^*); \rho_i(\sigma^*)\}$

Consider arbitrary $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau^*; \sigma^*\} \vdash \tau^*; \sigma^*]\!]\rho$. We need to show that

$$(W, E_1[(\texttt{call}\ \rho_1(\mathbf{u_1})\ \{\rho_1(\sigma_0), \mathbf{q_1}\}, \cdot)], E_2[(\texttt{call}\ \rho_2(\mathbf{u_2})\ \{\rho_2(\sigma_0), \mathbf{q_2}\}, \cdot)]) \in \mathcal{O}$$

Consider arbitrary $(M_1, M_2) : W$. We must show that for $i \in \{1, 2\}$, either both configurations $\langle M_i \mid E_i[(\texttt{call}\ \rho_i(\mathbf{u_i})\ \{\rho_i(\sigma_0), \mathbf{q_i}\}, \cdot)]\rangle$ terminate or both are running at $W.k$.

Instantiate the first premise with W and ρ, noting $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$. Thus we have that $(W, W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1})), W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u_2}))) \in \mathcal{W}[\![\mathbf{box}\,\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathbf{q}}}]\!]\rho$. From the definition of the latter, we have that $W.\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) = \ell_{\mathbf{i}}[\overline{\omega_{\mathbf{i}}}]$.

Next, let $M_i = (\mathbf{H_i}, \mathbf{R_i}, \mathbf{S_i})$.

From $(M_1, M_2) : W$, since $W.k > 0$, we have $(\triangleright W, M_1, M_2) \in \bigotimes\{\,\text{currentMR}(\theta) \mid \theta \in W.\Theta\,\}$. From the latter, we have three facts, one each for islands i_{reg}, i_{stk}, and i_{box}.

First, we have that $(\triangleright W, \mathbf{R_1}\restriction, \mathbf{R_2}\restriction) \in$ currentMR$(W(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i} = W.\mathbf{R_i}$ and, hence, $\hat{\mathbf{R}}_{\mathbf{i}}(\rho_i(\mathbf{u_i})) = \ell_{\mathbf{i}}[\overline{\omega_{\mathbf{i}}}]$.

Second, we have $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in$ currentMR$(W(i_{\text{stk}}))$. From the latter and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$, it follows that $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathcal{S}[\![\sigma]\!]\rho$. From the premise $\sigma = \tau_0 :: \cdots :: \tau_{\mathbf{j}} :: \sigma_0$, it follows that $\mathbf{S_1} = \mathbf{w_{10}} :: \cdots :: \mathbf{w_{1j}} :: \mathbf{S_{10}}$, $\mathbf{S_2} = \mathbf{w_{20}} :: \cdots :: \mathbf{w_{2j}} :: \mathbf{S_{20}}$, $(\triangleright W, \mathbf{w_{1n}}, \mathbf{w_{2n}}) \in \mathcal{W}[\![\tau_{\mathbf{n}}]\!]\rho$ for $n \in \{0, \ldots, j\}$, and $(\triangleright W, \mathbf{S_{10}}\restriction, \mathbf{S_{20}}\restriction) \in \mathcal{S}[\![\sigma_0]\!]\rho$.

Third, we have that there exist some $\mathbf{H_{b1}} \subseteq \mathbf{H_1}$ and $\mathbf{H_{b2}} \subseteq \mathbf{H_2}$ such that $(\triangleright W, \mathbf{H_{b1}}\restriction, \mathbf{H_{b2}}\restriction) \in$ currentMR$(W(i_{\text{box}}))$. We use the latter to instantiate $(W, \ell_1[\overline{\omega_1}], \ell_2[\overline{\omega_2}]) \in \mathcal{W}[\![\mathbf{box}\,\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathbf{q}}}]\!]\rho$, noting that $\triangleright W \sqsupset W$, which allows us to conclude:

- $\mathbf{H_{bi}}(\ell_{\mathbf{i}}) = \mathbf{code}[\overline{\beta_{\mathbf{i}}}, \zeta, \epsilon]\{\chi_{\mathbf{i}}; \sigma_{\mathbf{i}}\}^{\mathbf{q_i}}.\mathbf{I_i}$,

- $\rho_i(\hat{\chi}) = \chi_i[\overline{\omega_i/\beta_i}]$,
- $\rho_i(\hat{\sigma}) = \sigma_i[\overline{\omega_i/\beta_i}]$,
- $\rho_i(\hat{\mathbf{q}}) = \mathbf{q}_i[\overline{\omega_i/\beta_i}]$, and
- $(\triangleright W, (\mathbf{code}[\zeta, \epsilon]\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\omega_1/\beta_1}], (\mathbf{code}[\zeta, \epsilon]\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathbf{q}}}]\!]\rho$

Hence, we know that $\hat{\mathbf{R}}_i(\rho_i(\mathbf{u}_i)) = \ell_i[\overline{\omega_i}]$ and $\mathbf{H}_i(\ell_i) = \mathbf{code}[\overline{\beta_i}, \zeta, \epsilon]\{\chi_i; \sigma_i\}^{\mathbf{q}_i}.\mathbf{I}_i$, and therefore

$$\langle (\mathbf{H}_i, \mathbf{R}_i, \mathbf{S}_i) \mid E_i[(\texttt{call}\ \rho_i(\mathbf{u}_i)\ \{\rho_i(\sigma_0), \mathbf{q}_i\}, \cdot)]\rangle \longmapsto^1 \langle (\mathbf{H}_i, \mathbf{R}_i, \mathbf{S}_i) \mid E_i[(\mathbf{I}_i[\overline{\omega_i/\beta_i}][\rho_i(\sigma_0)/\zeta][\mathbf{q}_i/\epsilon], \cdot)]\rangle$$

Therefore, it suffices to show that for $i \in \{1, 2\}$, either both configurations $\langle M_i \mid E_i[(\mathbf{I}_i[\overline{\omega_i/\beta_i}][\rho_i(\sigma_0)/\zeta][\mathbf{q}_i/\epsilon], \cdot)]\rangle$ terminate or both are running at $W.k - 1$.

We proceed by noting that from the premise ret-addr-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \forall[].\{\mathbf{r} : \tau; \hat{\sigma}'\}^{\epsilon}$, by definition of ret-addr-type, it must be that either $\hat{\mathbf{q}} = \mathbf{r}_{\mathbf{ra}}$ or $\hat{\mathbf{q}} = \mathbf{i}_{\mathbf{ra}}$.

Further, we note that we have

$$\begin{aligned}
&(\triangleright W, (\mathbf{code}[\zeta, \epsilon]\{\chi_1; \sigma_1\}^{\mathbf{q}_1}.\mathbf{I}_1)[\overline{\omega_1/\beta_1}], \\
&\qquad (\mathbf{code}[\zeta, \epsilon]\{\chi_2; \sigma_2\}^{\mathbf{q}_2}.\mathbf{I}_2)[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathbf{q}}}]\!]\rho \\
\equiv\ &(\triangleright W, \mathbf{code}[\zeta, \epsilon]\{\chi_1[\overline{\omega_1/\beta_1}]; \sigma_1[\overline{\omega_1/\beta_1}]\}^{\mathbf{q}_1[\overline{\omega_1/\beta_1}]}.\mathbf{I}_1[\overline{\omega_1/\beta_1}], \\
&\qquad \mathbf{code}[\zeta, \epsilon]\{\chi_2[\overline{\omega_2/\beta_2}]; \sigma_2[\overline{\omega_2/\beta_2}]\}^{\mathbf{q}_2[\overline{\omega_2/\beta_2}]}.\mathbf{I}_2[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathbf{q}}}]\!]\rho \\
\equiv\ &(\triangleright W, \mathbf{code}[\zeta, \epsilon]\{\rho_1(\hat{\chi}); \rho_1(\hat{\sigma})\}^{\rho_1(\hat{\mathbf{q}})}.\mathbf{I}_1[\overline{\omega_1/\beta_1}], \\
&\qquad \mathbf{code}[\zeta, \epsilon]\{\rho_2(\hat{\chi}); \rho_2(\hat{\sigma})\}^{\rho_2(\hat{\mathbf{q}})}.\mathbf{I}_2[\overline{\omega_2/\beta_2}]) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathbf{q}}}]\!]\rho
\end{aligned}$$

Instantiate the latter with $\triangleright W$, ρ^*, τ, and $\hat{\sigma}'$, where

$$\begin{aligned}
&\rho^* = \{\zeta \mapsto (\rho_1(\sigma_0), \rho_2(\sigma_0), \varphi_S), \epsilon \mapsto (\mathbf{q}_1, \mathbf{q}_2)\} \text{ and} \\
&\varphi_S = \{(\widetilde{W}, \mathbf{S}_{10}\restriction, \mathbf{S}_{20}\restriction) \mid \widetilde{W} \sqsupseteq \triangleright W\}
\end{aligned}$$

We note the following:

- We have $\triangleright W \sqsupseteq \triangleright W$ by reflexivity.
- Note that $\rho^* \in \mathcal{D}[\![\zeta, \epsilon]\!]$, which follows by the definition of $\mathcal{D}[\![\cdot]\!]$ and by applying Lemma 1.18 to $(\triangleright W, \mathbf{S}_{10}\restriction, \mathbf{S}_{20}\restriction) \in \mathcal{S}[\![\sigma_0]\!]\rho$.
- Let $\rho' = \rho \cup \rho^*$.
- Note that $\tau; \hat{\sigma}' =_{\rho'}$ ret-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma})$. This follows by applying the substitutions ρ'_1 and ρ'_2 to ret-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \tau; \hat{\sigma}'$, which in turn follows from the premise ret-addr-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \forall[].\{\mathbf{r} : \tau; \hat{\sigma}'\}^{\epsilon}$.
- We claim that currentMR$(W(i_{\text{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\hat{\chi}]\!]\rho'$. (†)

  To show this, consider arbitrary $(\widetilde{W}, M_1^*, M_2^*) \in$ currentMR$(W(i_{\text{reg}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W$. We must show that
  $$(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{R}[\![\hat{\chi}]\!]\rho'$$
  Instantiate currentMR$(W(i_{\text{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\chi]\!]\rho$ with $(\widetilde{W}, M_1^*, M_2^*) \in$ currentMR$(W(i_{\text{reg}}))$, noting that $\widetilde{W} \sqsupseteq \triangleright W$, which gives us $(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{R}[\![\chi]\!]\rho$. Finally, by Lemma 1.19 (register-file subtyping implies inclusion) applied to the premise $\mathbf{\Delta} \vdash \chi \leq \hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]$ we have that $\mathcal{R}[\![\chi]\!]\rho \subseteq \mathcal{R}[\![\hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]]\!]\rho$.
  Therefore, it remains to show that $\mathcal{R}[\![\hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]]\!]\rho \subseteq \mathcal{R}[\![\hat{\chi}]\!]\rho'$.
  Next, we examine two cases based on the value of $\hat{\mathbf{q}}$:

Case $\hat{\mathbf{q}} = \mathbf{i_{ra}}$ Hence, from the premise $\Delta \vdash \hat{\chi} \setminus \hat{\mathbf{q}}$, we have that $\Delta \vdash \hat{\chi}$. Therefore, note that

$$\mathcal{R}[\![\hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*;\sigma^*\}/\epsilon]]\!]\rho \equiv \mathcal{R}[\![\hat{\chi}]\!]\rho \quad \text{since } \zeta, \epsilon \notin \mathrm{ftv}(\hat{\chi}) \equiv \mathcal{R}[\![\hat{\chi}]\!]\rho' \quad \text{by Lemma 1.13}$$

which suffices to show what we needed.

Case $\hat{\mathbf{q}} = \mathbf{r_{ra}}$ Hence, from the premise $\Delta \vdash \hat{\chi} \setminus \hat{\mathbf{q}}$, we actually have that $\Delta \vdash \hat{\chi} \setminus \mathbf{r_{ra}}$.
Hence, it follows that $\mathcal{R}[\![(\hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*;\sigma^*\}/\epsilon]) \setminus \mathbf{r_{ra}}]\!]\rho \equiv \mathcal{R}[\![(\hat{\chi}) \setminus \mathbf{r_{ra}}]\!]\rho'$.
Therefore, it remains to show the following for the remaining register $\mathbf{r_{ra}}$, whose type by our premises must be $\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}$ where $\Delta \vdash \tau$:

$$\mathcal{R}[\![\mathbf{r_{ra}}:\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'[\sigma_0/\zeta]\}^{\epsilon[\mathbf{end}\{\tau^*;\sigma^*\}/\epsilon]}]\!]\rho \subseteq \mathcal{R}[\![\mathbf{r_{ra}}:\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$$

Therefore, we must show for arbitrary $(W^*, \mathbf{R_1^*}\restriction, \mathbf{R_2^*}\restriction) \in \mathcal{R}[\![\mathbf{r_{ra}}:\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'[\sigma_0/\zeta]\}^{\epsilon[\mathbf{end}\{\tau^*;\sigma^*\}/\epsilon]}]\!]\rho$ that $(W^*, \mathbf{R_1^*}\restriction, \mathbf{R_2^*}\restriction) \in \mathcal{R}[\![\mathbf{r_{ra}}:\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$. Hence, it suffices to show that

$$(W^*, \mathbf{R_1^*}(\mathbf{r_{ra}}), \mathbf{R_2^*}(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'.$$

Note, from our most recent assumption, we have
$(W^*, \mathbf{R_1^*}(\mathbf{r_{ra}}), \mathbf{R_2^*}(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'[\sigma_0/\zeta]\}^{\epsilon[\mathbf{end}\{\tau^*;\sigma^*\}/\epsilon]}]\!]\rho$. By substitution (Lemmas 1.15 and 1.16), the latter is equivalent to $(W^*, \mathbf{R_1^*}(\mathbf{r_{ra}}), \mathbf{R_2^*}(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho^*$ where $\rho^* = \rho[\zeta \mapsto (\rho_1(\sigma_0), \rho_2(\sigma_0), \mathcal{S}[\![\sigma_0]\!]\rho), \epsilon \mapsto (\mathbf{q_1}, \mathbf{q_2})]$.
To show $(W^*, \mathbf{R_1^*}(\mathbf{r_{ra}}), \mathbf{R_2^*}(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$, consider arbitrary $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W^*(i_{\mathrm{box}}))$ such that $\widetilde{W} \sqsupset W^*$.
Instantiating $(W^*, \mathbf{R_1^*}(\mathbf{r_{ra}}), \mathbf{R_2^*}(\mathbf{r_{ra}})) \in \mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho^*$, we end up in a position where we have to show that

$$\mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho^* \;\subseteq\; \mathcal{HV}[\![\forall[].\{\mathbf{r}:\tau;\hat{\sigma}'\}^{\epsilon}]\!]\rho'$$

The latter follows by expanding the definitions and noting that it suffices to prove the following three facts:

- For any world W', $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\mathbf{r}:\tau]\!]\rho'$ implies $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\mathbf{r}:\tau]\!]\rho*$ since both are equal to $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\mathbf{r}:\tau]\!]\rho$ because $\Delta \vdash \tau$.
- For any world W', given that $\mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\hat{\sigma}']\!]\rho'$ we claim that $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{S}[\![\hat{\sigma}']\!]\rho^*$.
  Note that $\hat{\sigma}' = \tau_0' :: \cdots :: \tau_k' :: \zeta$, and from the premise $\Delta \vdash \hat{\sigma}'[\sigma_0/\zeta]$, we know that $\zeta \notin \mathrm{ftv}(\tau_n')$ for $n \in \{0, \ldots, k\}$. Therefore, it suffices to show that

  $$\mathcal{S}[\![\zeta]\!]\rho' \subseteq \mathcal{S}[\![\zeta]\!]\rho^* \equiv \varphi_S \subseteq \mathcal{S}[\![\sigma_0]\!]\rho$$

  which is immediate from our choice of φ_S above.
- Finally, we note that $\tau^*;\sigma^* =_{\rho'} \text{ret-type}(\epsilon, \{\mathbf{r}:\tau\}, \hat{\sigma}')$. Therefore, note that $\mathcal{E}[\![\epsilon \vdash \tau^*;\sigma^*]\!]\rho^* = \mathcal{E}[\![\mathbf{end}\{\tau^*;\sigma^*\} \vdash \tau^*;\sigma^*]\!]\rho' = \mathcal{E}[\![\mathbf{end}\{\tau^*;\sigma^*\} \vdash \tau^*;\sigma^*]\!]\rho$.

This completes our proof of the claim marked (†).

- Note that $\mathrm{currentMR}((\triangleright W)(i_{\mathrm{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\hat{\chi}]\!]\rho'$, which follows from $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\hat{\chi}]\!]$.
- We claim that $\mathrm{currentMR}(W(i_{\mathrm{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\hat{\sigma}]\!]\rho'$ (‡)
  To show this, consider arbitrary $(\widetilde{W}, M_1^*, M_2^*) \in \mathrm{currentMR}(W(i_{\mathrm{stk}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W$. We must show that

  $$(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{S}[\![\hat{\sigma}]\!]\rho'.$$

  Recall that above we had $(\triangleright W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathrm{currentMR}(W(i_{\mathrm{stk}}))$. Therefore, by definition of the i_{stk} island, it must be that $M_1^* = \mathbf{S_1}\restriction$ and $M_2^* = \mathbf{S_2}\restriction$. Hence, it remains for us to show:

  $$(\widetilde{W}, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathcal{S}[\![\hat{\sigma}]\!]\rho'$$

where we recall that

$$\begin{aligned}
&\mathbf{S_1} = \mathbf{w_{10}} :: \cdots :: \mathbf{w_{1j}} :: \mathbf{S_{10}}\\
&\mathbf{S_2} = \mathbf{w_{20}} :: \cdots :: \mathbf{w_{2j}} :: \mathbf{S_{20}}\\
&\hat{\boldsymbol{\sigma}} = \boldsymbol{\tau_0} :: \cdots :: \boldsymbol{\tau_j} :: \boldsymbol{\zeta}\\
&\text{and } \rho' = \rho[\boldsymbol{\zeta} \mapsto (\rho_1(\boldsymbol{\sigma_0}), \rho_2(\boldsymbol{\sigma_0}), \varphi_S), \boldsymbol{\epsilon} \mapsto (\mathbf{q_1}, \mathbf{q_2})]\\
&\text{with } \varphi_S = \{(\widetilde{W}, \mathbf{S_{10}}\restriction, \mathbf{S_{20}}\restriction) | \widetilde{W} \sqsupseteq \triangleright W\}.
\end{aligned}$$

Thus, to show $(\widetilde{W}, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathcal{S}[\![\hat{\boldsymbol{\sigma}}]\!]\rho'$, it suffices to show

- $(\widetilde{W}, \mathbf{w_{1n}}, \mathbf{w_{2n}}) \in \mathcal{W}[\![\boldsymbol{\tau_n}]\!]\rho'$ for $n \in \{0, \ldots, j\}$, which follows from $(\triangleright W, \mathbf{w_{1n}}, \mathbf{w_{2n}}) \in \mathcal{W}[\![\boldsymbol{\tau_n}]\!]$ by monotonicity (Lemma 1.8).
- $(\widetilde{W}, \mathbf{S_{10}}, \mathbf{S_{20}}) \in \mathcal{S}[\![\boldsymbol{\zeta}]\!]\rho'$, which is immediate from $\mathcal{S}[\![\boldsymbol{\zeta}]\!]\rho' = \varphi_S$ (by definition) and our choice of φ_S above.

- Note that $\text{currentMR}((\triangleright W)(i_{\text{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\hat{\boldsymbol{\sigma}}]\!]\rho'$, which follows from $\text{currentMR}(W(i_{\text{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\hat{\boldsymbol{\sigma}}]\!]\rho'$.

Hence, we can conclude that

$$(\triangleright W, (\mathbf{I_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}][\rho_1(\boldsymbol{\sigma_0})/\boldsymbol{\zeta}][\mathbf{q_1}/\boldsymbol{\epsilon}], \cdot), (\mathbf{I_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}][\rho_2(\boldsymbol{\sigma_0})/\boldsymbol{\zeta}][\mathbf{q_2}/\boldsymbol{\epsilon}], \cdot)) \in \mathcal{E}[\![\hat{\mathbf{q}} \vdash \boldsymbol{\tau}; \hat{\boldsymbol{\sigma}}']\!]\rho'$$

Next, we instantiate the latter with E_1 and E_2, for which we need to show the following:

$$(\triangleright W, E_1, E_2) \in \mathcal{K}[\![\hat{\mathbf{q}} \vdash \boldsymbol{\tau}; \hat{\boldsymbol{\sigma}}']\!]\rho'$$

Consider arbitrary W', $\hat{\mathbf{q}}'$, $\mathbf{r_1}$, $\mathbf{r_2}$ such that

1. $W' \sqsupseteq_{\text{pub}} \triangleright W$,
2. $(\hat{\mathbf{q}} =_{\rho'} \hat{\mathbf{q}}' =_{\rho'} \mathbf{end}\{\hat{\boldsymbol{\tau}}; \hat{\boldsymbol{\sigma}}'\}) \vee$
   $(\exists \mathbf{r_0}.\hat{\mathbf{q}}' = \mathbf{r_0} \ \wedge\ \text{ret-addr}_1(\triangleright W, \rho_1'(\hat{\mathbf{q}})) = W'.\mathbf{R_1}(\mathbf{r_0}) \ \wedge\ \text{ret-addr}_2(\triangleright W, \rho_2'(\hat{\mathbf{q}})) = W'.\mathbf{R_2}(\mathbf{r_0}) \ \wedge$
   $\text{ret-reg}_1(W', \mathbf{r_0}) = \mathbf{r_1} \ \wedge\ \text{ret-reg}_2(W', \mathbf{r_0}) = \mathbf{r_2})$
3. $(\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho'$
4. $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\hat{\boldsymbol{\sigma}}']\!]\rho'$

We are required to show

$$(W', E_1[(\mathtt{ret}\ \rho_1(\hat{\mathbf{q}}')\ \{\mathbf{r_1}\}, \cdot)], E_2[(\mathtt{ret}\ \rho_2(\hat{\mathbf{q}}')\ \{\mathbf{r_2}\}, \cdot)]) \in \mathcal{O}$$

Next, we collect some facts before we proceed:

- Note that from assumption (4) above, it follows that $\triangleright W'$ is defined, which means that $W'.k > 0$.
- Recall from above that either $\hat{\mathbf{q}} = \mathbf{r_{ra}}$ or $\hat{\mathbf{q}} = \mathbf{i_{ra}}$. This fact lets us refine (3) above—that is, since $\hat{\mathbf{q}} \neq_{\rho'} \mathbf{end}\{\hat{\boldsymbol{\tau}}; \hat{\boldsymbol{\sigma}}'\}$, we know that

  $$\begin{aligned}\exists \mathbf{r_0}.\hat{\mathbf{q}}' = \mathbf{r_0} \ \wedge\ &\text{ret-addr}_1(\triangleright W, \rho_1'(\hat{\mathbf{q}})) = W'.\mathbf{R_1}(\mathbf{r_0}) \ \wedge\ \text{ret-addr}_2(\triangleright W, \rho_2'(\hat{\mathbf{q}})) = W'.\mathbf{R_2}(\mathbf{r_0})) \ \wedge\\ &\text{ret-reg}_1(W', \mathbf{r_0})) = \mathbf{r_1} \ \wedge\ \text{ret-reg}_2(W', \mathbf{r_0})) = \mathbf{r_2})\end{aligned}$$

Hence, $\rho_i(\hat{\mathbf{q}}') = \rho_i(\mathbf{r_0}) = \mathbf{r_0}$. Therefore, it suffices to show

$$(W', E_1[(\mathtt{ret}\ \mathbf{r_0}\ \{\mathbf{r_1}\}, \cdot)], E_2[(\mathtt{ret}\ \mathbf{r_0}\ \{\mathbf{r_2}\}, \cdot)]) \in \mathcal{O}$$

Consider arbitrary $(M_1', M_2') : W'$. We must show that for $i \in \{1, 2\}$, either both configurations $\langle M_i' \mid E_i[(\mathtt{ret}\ \mathbf{r_0}\ \{\mathbf{r_i}\}, \cdot)]\rangle$ terminate or both are running at $W'.k$.

Next, we establish that $(\triangleright W, W'.\mathbf{R_1}(\mathbf{r_0}), W'.\mathbf{R_2}(\mathbf{r_0})) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r} : \boldsymbol{\tau}; \hat{\boldsymbol{\sigma}}'\}^{\epsilon}]\!]\rho'$ by considering the two cases of $\hat{\mathbf{q}}$:

Case $\hat{\mathbf{q}} = \mathbf{r_{ra}}$: Hence, by the definition of ret-addr-type we have

$$\begin{aligned}\text{ret-addr-type}(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) &= \text{ret-addr-type}(\mathbf{r_{ra}}, \hat{\chi}, \hat{\sigma}) \\ &= \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon} \text{ where } \hat{\chi}(\mathbf{r_{ra}}) = \mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}\end{aligned}$$

Since $(\triangleright W, \mathbf{R_1}\uparrow, \mathbf{R_2}\uparrow) \in \text{currentMR}(W(i_{\text{reg}}))$ (from above) and $\text{currentMR}(W(i_{\text{reg}})) \Subset_{\triangleright W} \mathcal{R}[\![\hat{\chi}]\!]\rho'$ († from above), it follows that $(\triangleright W, \mathbf{R_1}\uparrow, \mathbf{R_2}\uparrow) \in \mathcal{R}[\![\hat{\chi}]\!]\rho'$. From the latter, since $\mathbf{r_{ra}} : \mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon} \in \hat{\chi}$, we have

$$(\triangleright W, \mathbf{R_1(r_{ra})}, \mathbf{R_2(r_{ra})}) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}]\!]\rho'.$$

Since $\mathbf{R_i} = W.\mathbf{R_i} = \triangleright W.\mathbf{R_i}$, the above is equivalent to

$$(\triangleright W, \triangleright W.\mathbf{R_1(r_{ra})}, \triangleright W.\mathbf{R_2(r_{ra})}) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}]\!]\rho'.$$

Moreover, note that we have the following equalities

$$\begin{aligned}&\text{ret-addr}_i(\triangleright W, \hat{\mathbf{q}}) \\ &= \text{ret-addr}_i(\triangleright W, \mathbf{r_{ra}}) && \text{since } \hat{\mathbf{q}} = \mathbf{r_{ra}} \\ &= (\triangleright W).\mathbf{R_i(r_{ra})} && \text{by definition of ret-addr}_i \\ &= W'.\mathbf{R_i(r_0)} && \text{since ret-addr}_i(\triangleright W, \hat{\mathbf{q}}) = W'.\mathbf{R_i(r_0)}\end{aligned}$$

Hence, we have

$$(\triangleright W, W'.\mathbf{R_1(r_0)}, W'.\mathbf{R_2(r_0)}) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}]\!]\rho'.$$

Case $\hat{\mathbf{q}} = \mathbf{i_{ra}}$: Hence, by the definition of ret-addr-type we have

$$\begin{aligned}\text{ret-addr-type}(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) &= \text{ret-addr-type}(\mathbf{i_{ra}}, \hat{\chi}, \hat{\sigma}) \\ &= \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon} \text{ where } \hat{\sigma}(\mathbf{i_{ra}}) = \mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}\end{aligned}$$

Since $(\triangleright W, \mathbf{S_1}\uparrow, \mathbf{S_2}\uparrow) \in \text{currentMR}(W(i_{\text{stk}}))$ (from above) and $\text{currentMR}(W(i_{\text{stk}})) \Subset_{\triangleright W} \mathcal{S}[\![\hat{\sigma}]\!]\rho'$ (‡ from above), it follows that $(\triangleright W, \mathbf{S_1}\uparrow, \mathbf{S_2}\uparrow) \in \mathcal{S}[\![\hat{\sigma}]\!]\rho'$. From the latter, since $\mathbf{i_{ra}} : \mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon} \in \hat{\sigma}$, we have

$$(\triangleright W, \mathbf{S_1(i_{ra})}, \mathbf{S_2(i_{ra})}) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}]\!]\rho'.$$

Since $\mathbf{S_i} = W.\mathbf{S_i} = \triangleright W.\mathbf{S_i}$, the above is equivalent to

$$(\triangleright W, \triangleright W.\mathbf{S_1(i_{ra})}, \triangleright W.\mathbf{S_2(i_{ra})}) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}]\!]\rho'.$$

Moreover, note that we have the following equalities

$$\begin{aligned}&\text{ret-addr}_i(\triangleright W, \hat{\mathbf{q}}) \\ &= \text{ret-addr}_i(\triangleright W, \mathbf{i_{ra}}) && \text{since } \hat{\mathbf{q}} = \mathbf{i_{ra}} \\ &= (\triangleright W).\mathbf{S_i(i_{ra})} && \text{by definition of ret-addr}_i \\ &= W'.\mathbf{R_i(r_0)} && \text{since ret-addr}_i(\triangleright W, \hat{\mathbf{q}}) = W'.\mathbf{R_i(r_0)}\end{aligned}$$

Hence, we have

$$(\triangleright W, W'.\mathbf{R_1(r_0)}, W'.\mathbf{R_2(r_0)}) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}]\!]\rho'.$$

Since $W' \sqsupseteq \triangleright W$, by monotonicity we have

$$(W', W'.\mathbf{R_1(r_0)}, W'.\mathbf{R_2(r_0)}) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r}:\tau;\hat{\sigma'}\}^{\epsilon}]\!]\rho'.$$

From the above, we have that $W'.\Psi_1;\cdot \vdash W'.\mathbf{R_1(r_0)} : \rho_1'(\mathbf{box}\ \forall[].\{\mathbf{r:\tau;\hat{\sigma}'}\}^{\epsilon})$ and $W'.\Psi_2;\cdot \vdash W'.\mathbf{R_2(r_0)} : \rho_2'(\mathbf{box}\ \forall[].\{\mathbf{r:\tau;\hat{\sigma}'}\}^{\epsilon})$. These facts put together with $W' \in \text{World}$ and $\text{ret-reg}_1(W', \mathbf{r_0})$ allow us to conclude $\mathbf{r = r_1 = r_2}$.

Next, let $M_i' = (\mathbf{H_i', R_i', S_i'})$.

From $(M_1', M_2') : W'$, since $W'.k > 0$, we have $(\triangleright W', M_1', M_2') \in \bigotimes\{\,\text{currentMR}(\theta) \mid \theta \in W'.\Theta\,\}$. From the latter, we have three facts, one each for islands i_{reg}, i_{stk}, and i_{box}.

First, we have that $(\triangleright W', \mathbf{R_1'}\restriction, \mathbf{R_2'}\restriction) \in \text{currentMR}(W'(i_{\text{reg}}))$. From the latter it follows that $\mathbf{R_i'} = W'.\mathbf{R_i}$ and, hence, we have $(\triangleright W', \mathbf{R_1'(r_0)}, \mathbf{R_1'(r_0)}) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r:\tau;\hat{\sigma}'}\}^{\epsilon}]\!]\rho'$. From the latter, it must be that $\mathbf{R_i'(r_0)} = \ell_i'[\overline{\omega_i'}]$.

Second, we have $(\triangleright W', \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction) \in \text{currentMR}(W'(i_{\text{stk}}))$. Hence, we can instantiate assumption (5) from above, i.e., $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\hat{\sigma}']\!]\rho'$, with $(\triangleright W', \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction)$, noting $\triangleright W' \sqsupseteq W'$ (by Lemma 1.6), which allows us to conclude that $(\triangleright W', \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction) \in \mathcal{S}[\![\hat{\sigma}']\!]\rho'$. From the premise $\hat{\sigma}' = \tau_0' :: \cdots :: \tau_k' :: \zeta$, it follows that $\mathbf{S_1'} = \mathbf{w_{10}'} :: \cdots :: \mathbf{w_{1k}'} :: \mathbf{S_{10}'}$, $\mathbf{S_2'} = \mathbf{w_{20}'} :: \cdots :: \mathbf{w_{2l}'} :: \mathbf{S_{20}'}$, $(\triangleright W', \mathbf{w_{1n}'}, \mathbf{w_{2n}'}) \in \mathcal{W}[\![\tau_n']\!]\rho'$ for $n \in \{0, \ldots, k\}$, and $(\triangleright W', \mathbf{S_{10}'}\restriction, \mathbf{S_{20}'}\restriction) \in \mathcal{S}[\![\zeta]\!]\rho'$. From the latter, since $\mathcal{S}[\![\zeta]\!]\rho' = \varphi_S$, it follows that $\mathbf{S_{10}' = S_{10}}$ and $\mathbf{S_{20}' = S_{20}}$.

Third, we have that there exist some $\mathbf{H_{b1}'} \subseteq \mathbf{H_1'}$ and $\mathbf{H_{b2}'} \subseteq \mathbf{H_2'}$ such that $(\triangleright W', \mathbf{H_{b1}'}\restriction, \mathbf{H_{b2}'}\restriction) \in \text{currentMR}(W'(i_{\text{box}}))$.

Instantiate $(W', \ell_1'[\overline{\omega_1'}], \ell_1'[\overline{\omega_1'}]) \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathbf{r:\tau;\hat{\sigma}'}\}^{\epsilon}]\!]\rho'$ with $(\triangleright W', \mathbf{H_{b1}'}\restriction, \mathbf{H_{b2}'}\restriction) \in \text{currentMR}(W'(i_{\text{box}}))$, noting that $\triangleright W' \sqsupseteq W'$ by Lemma 1.6. Hence, we have that

- $\mathbf{H_{bi}'}(\ell_i') = \mathbf{code}[\overline{\beta_i'}]\{\chi_i'; \sigma_i'\}^{\mathbf{q_i'}}.\mathbf{I_i'}$,
- $\rho_i'(\mathbf{r:\tau}) = \chi_i'[\overline{\omega_i'/\beta_i'}]$,
- $\rho_i'(\hat{\sigma}') = \sigma_i'[\overline{\omega_i'/\beta_i'}]$,
- $\rho_i'(\epsilon) = \mathbf{q_i'}[\overline{\omega_i'/\beta_i'}]$, and
- $(\triangleright W', (\mathbf{code}[]\{\chi_1'; \sigma_1'\}^{\mathbf{q_1'}}.\mathbf{I_1'})[\overline{\omega_1'/\beta_1'}], (\mathbf{code}[]\{\chi_2'; \sigma_2'\}^{\mathbf{q_2'}}.\mathbf{I_2'})[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r:\tau;\hat{\sigma}'}\}^{\epsilon}]\!]\rho'$

Hence, we know that $\hat{\mathbf{R}}_i'(\mathbf{r_0}) = \ell_i'[\overline{\omega_i'}]$ and $\mathbf{H_i'}(\ell_i') = \mathbf{code}[\overline{\beta_i'}]\{\chi_i'; \sigma_i'\}^{\mathbf{q_i'}}.\mathbf{I_i'}$, and therefore

$$\langle (\mathbf{H_i', R_i', S_i'}) \mid E_i[(\mathtt{ret}\ \mathbf{r_0}\ \{\mathbf{r_i}\}, \cdot)]\rangle \longmapsto^1 \langle (\mathbf{H_i', R_i', S_i'}) \mid E_i[(\mathbf{I_i'}[\overline{\omega_i'/\beta_i'}], \cdot)]\rangle$$

Therefore, it suffices to show that for $i \in \{1, 2\}$, either both configurations $\langle M_i' \mid E_i[(\mathbf{I_i'}[\overline{\omega_i'/\beta_i'}], \cdot)]\rangle$ terminate or both are running at $W'.k - 1$.

We proceed by noting that

$$\begin{aligned}
&(\triangleright W', (\mathbf{code}[]\{\chi_1'; \sigma_1'\}^{\mathbf{q_1'}}.\mathbf{I_1'})[\overline{\omega_1'/\beta_1'}], (\mathbf{code}[]\{\chi_2'; \sigma_2'\}^{\mathbf{q_2'}}.\mathbf{I_2'})[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r:\tau;\hat{\sigma}'}\}^{\epsilon}]\!]\rho' \\
\equiv\ &(\triangleright W', \mathbf{code}[]\{\chi_1'[\overline{\omega_1'/\beta_1'}]; \sigma_1'[\overline{\omega_1'/\beta_1'}]\}^{\mathbf{q_1'}[\overline{\omega_1'/\beta_1'}]}.\mathbf{I_1'}[\overline{\omega_1'/\beta_1'}], \\
&\quad \mathbf{code}[]\{\chi_2'[\overline{\omega_2'/\beta_2'}]; \sigma_2'[\overline{\omega_2'/\beta_2'}]\}^{\mathbf{q_2'}[\overline{\omega_2'/\beta_2'}]}.\mathbf{I_2'}[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r:\tau;\hat{\sigma}'}\}^{\epsilon}]\!]\rho' \\
\equiv\ &(\triangleright W', \mathbf{code}[]\{\rho_1'(\mathbf{r:\tau}); \rho_1'(\hat{\sigma}')\}^{\rho_1'(\epsilon)}.\mathbf{I_1'}[\overline{\omega_1'/\beta_1'}], \\
&\quad \mathbf{code}[]\{\rho_2'(\mathbf{r:\tau}); \rho_2'(\hat{\sigma}')\}^{\rho_2'(\epsilon)}.\mathbf{I_2'}[\overline{\omega_2'/\beta_2'}]) \in \mathcal{HV}[\![\forall[].\{\mathbf{r:\tau;\hat{\sigma}'}\}^{\epsilon}]\!]\rho'
\end{aligned}$$

Instantiate the latter with $\triangleright W'$, $\emptyset \in \mathcal{D}[\![\cdot]\!]$, τ^*, and σ^*.

We note the following:

- We have $\triangleright W' \sqsupseteq \triangleright W'$ by reflexivity.
- We claim that $\tau^*; \sigma^* =_{\rho'} \text{ret-type}(\epsilon, \{\mathbf{r:\tau}\}, \hat{\sigma}')$. It suffices to show for $i \in \{1, 2\}$:

$$\begin{aligned}
&\rho_i'(\tau^*); \rho_i'(\sigma^*) = \text{ret-type}(\rho_i'(\epsilon), \rho_i'(\{\mathbf{r:\tau}\}), \rho_i'(\hat{\sigma}')) \\
&\equiv \rho_i'(\tau^*); \rho_i'(\sigma^*) = \text{ret-type}(\rho_i'(\mathbf{end}\{\tau^*; \sigma^*\}), \rho_i'(\{\mathbf{r:\tau}\}), \rho_i'(\tau_0 :: \cdots :: \tau_j :: \zeta))
\end{aligned}$$

  Note that $FTV(\tau^*; \sigma^*) \subseteq \mathbf{\Delta}$.

- We claim that currentMR$((\triangleright W')(i_{\text{reg}})) \Subset_{\triangleright W'} \mathcal{R}[\![\mathbf{r} : \tau]\!]\rho'$.

  To show this, consider arbitrary $(\widetilde{W}, M_1^*, M_2^*) \in$ currentMR$((\triangleright W')(i_{\text{reg}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W'$. We must show that
  $$(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{R}[\![\mathbf{r} : \tau]\!]\rho'$$
  Note that since $W'.k > 0$ (from above), $(\triangleright W').k = W'.k - 1$ and therefore
  $$\text{currentMR}((\triangleright W')(i_{\text{reg}})) = \lfloor \text{currentMR}(W'(i_{\text{reg}})) \rfloor_{W'.k-1} \subseteq \text{currentMR}(W'(i_{\text{reg}}))$$
  Thus,$(\widetilde{W}, M_1^*, M_2^*) \in$ currentMR$(W'(i_{\text{reg}}))$. Moreover, since we already have $(\triangleright W', \mathbf{R_1'}\restriction, \mathbf{R_2'}\restriction) \in$ currentMR$(W'(i_{\text{reg}}))$, by the definition of island i_{reg}, it must be that $M_i^* = \mathbf{R_i'}$. Therefore, we are required to show
  $$(\widetilde{W}, \mathbf{R_1'}\restriction, \mathbf{R_2'}\restriction) \in \mathcal{R}[\![\mathbf{r} : \tau]\!]\rho'.$$
  It suffices to show
  $$(\widetilde{W}, \mathbf{R_1'(r)}, \mathbf{R_2'(r)}) \in \mathcal{W}[\![\tau]\!]\rho'$$
  which follows by monotonicity (Lemma 1.8) from our earlier assumption (4), namely $(\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\tau]\!]\rho'$ since $\mathbf{r} = \mathbf{r_1} = \mathbf{r_2}$ (from above) and since $W'.\mathbf{R_1} = \mathbf{R_1'}$ and $W'.\mathbf{R_2} = \mathbf{R_2'}$.
- We claim that currentMR$((\triangleright W')(i_{\text{stk}})) \Subset_{\triangleright W'} \mathcal{S}[\![\hat{\sigma}']\!]\rho'$.

  To show this, consider arbitrary $(\widetilde{W}, M_1^*, M_2^*) \in$ currentMR$((\triangleright W')(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq \triangleright W'$. We must show that
  $$(\widetilde{W}, M_1^*, M_2^*) \in \mathcal{S}[\![\hat{\sigma}']\!]\rho'.$$
  Note that since $W'.k > 0$ (from above), $(\triangleright W).k = W.k - 1$ and therefore
  $$\text{currentMR}((\triangleright W')(i_{\text{stk}})) = \lfloor \text{currentMR}(W'(i_{\text{stk}})) \rfloor_{W'.k-1} \subseteq \text{currentMR}(W'(i_{\text{stk}}))$$
  Thus,$(\widetilde{W}, M_1^*, M_2^*) \in$ currentMR$(W'(i_{\text{stk}}))$. Moreover, since we already have $(\triangleright W', \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction) \in$ currentMR$(W'(i_{\text{stk}}))$, by the definition of island i_{stk}, it must be that $M_i^* = \mathbf{S_i'}$. Therefore, we are required to show
  $$(\widetilde{W}, \mathbf{S_1'}\restriction, \mathbf{S_2'}\restriction) \in \mathcal{S}[\![\hat{\sigma}']\!]\rho'.$$
  Since $\hat{\sigma}' = \tau_0' :: \cdots :: \tau_k' :: \zeta$, with $\mathbf{S_1'} = \mathbf{w_{10}'} :: \cdots :: \mathbf{w_{1k}'} :: \mathbf{S_{10}'}$ and $\mathbf{S_2'} = \mathbf{w_{20}'} :: \cdots :: \mathbf{w_{2l}'} :: \mathbf{S_{20}'}$, the above follows from
  - $(\widetilde{W}, \mathbf{w_{1n}'}, \mathbf{w_{2n}'}) \in \mathcal{W}[\![\tau_n']\!]\rho'$ for $n \in \{0, \ldots, k\}$, which follow by monotonicity (Lemma 1.8) from $(\triangleright W', \mathbf{w_{1n}'}, \mathbf{w_{2n}'}) \in \mathcal{W}[\![\tau_n']\!]\rho'$, and
  - $(\widetilde{W}, \mathbf{S_{10}'}\restriction, \mathbf{S_{20}'}\restriction) \in \mathcal{S}[\![\zeta]\!]\rho'$, which follows from $\mathcal{S}[\![\zeta]\!]\rho' = \varphi_S$ and the definition of φ_S since $\mathbf{S_{10}'} = \mathbf{S_{10}}$ and $\mathbf{S_{20}'} = \mathbf{S_{20}}$.

Hence, we can conclude that
$$(\triangleright W', (\mathbf{I_1'}[\overline{\omega_1'/\beta_1'}], \cdot), (\mathbf{I_2'}[\overline{\omega_2'/\beta_2'}], \cdot)) \in \mathcal{E}[\![\epsilon \vdash \tau_r; \sigma_r]\!]\rho'$$
By Lemma 1.16, and noting that $FTV(\tau^*; \sigma^*) \subseteq \mathbf{\Delta}$ we have
$$(\triangleright W', (\mathbf{I_1'}[\overline{\omega_1'/\beta_1'}], \cdot), (\mathbf{I_2'}[\overline{\omega_2'/\beta_2'}], \cdot)) \in \mathcal{E}[\![\mathbf{end}\{\tau^*; \sigma^*\} \vdash \tau^*; \sigma^*]\!]\rho. \tag{19}$$

Near the beginning of this proof, we had assumed $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau^*; \sigma^*\} \vdash \tau^*; \sigma^*]\!]\rho$. We now apply Lemma 1.10 (monotonicity for evaluation contexts) to $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau^*; \sigma^*\} \vdash \tau^*; \sigma^*]\!]\rho$, noting the following:

- $\triangleright W' \sqsupseteq_{\text{pub}} W$, which follows by transitivity of $\sqsupseteq_{\text{pub}}$ and the following $\triangleright W' \sqsupseteq_{\text{pub}} W' \sqsupseteq_{\text{pub}} \triangleright W \sqsupseteq_{\text{pub}} W$ (which we have from above and from Lemma 1.6).
- $\mathbf{end}\{\tau^*; \sigma^*\} =_\rho \mathbf{end}\{\tau^*; \sigma^*\}$.

Hence, we have that $(\triangleright W', E_1, E_2) \in \mathcal{K}[\![\mathbf{end\{\tau^*; \sigma^*\}} \vdash \tau^*; \sigma^*]\!]\rho$.

Instantiating 19 with the above, we have $(\triangleright W', E_1[(\mathbf{I'_1}[\overline{\omega'_1/\beta'_1}], \cdot)], E_2[(\mathbf{I'_2}[\overline{\omega'_2/\beta'_2}], \cdot)]) \in \mathcal{O}$.

By instantiating the latter with M'_1 and M'_2, noting $(M'_1, M'_2) : \triangleright W'$, we have that $\langle M'_1 \mid E_1[(\mathbf{I'_1}[\overline{\omega'_1/\beta'_1}], \cdot)]\rangle$ and $\langle M'_2 \mid E_2[(\mathbf{I'_2}[\overline{\omega'_2/\beta'_2}], \cdot)]\rangle$ either both terminate or both are running at $W'.k - 1$, which gives us what we needed to show.

Hence, we conclude that

$$(\triangleright W, E_1[(\mathbf{I_1}[\overline{\omega_1/\beta_1}][\rho_1(\boldsymbol{\sigma_0})/\zeta][\mathbf{q_1}/\epsilon], \cdot)], E_2[(\mathbf{I_2}[\overline{\omega_2/\beta_2}][\rho_2(\boldsymbol{\sigma_0})/\zeta][\mathbf{q_2}/\epsilon], \cdot)]) \in \mathcal{O}$$

Now instantiate the above with M_1 and M_2, noting that we have $(M_1, M_2) : \triangleright W$ by Lemma 1.6 since $(M_1, M_2) : W$. Hence, we have that for $i \in \{1, 2\}$, either both configurations $\langle M_i \mid E_1[(\mathbf{I_i}[\overline{\omega_i/\beta_i}][\rho_i(\boldsymbol{\sigma_0})/\zeta][\mathbf{q_i}/\epsilon], \cdot)]\rangle$ terminate or both are running at $W.k - 1$, which is exactly what we needed to show!

□

2 Functional language: F

2.1 Syntax and Semantics

$$
\begin{array}{rcl}
\tau & ::= & \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid (\overline{\tau}) \to \tau \mid \mu\alpha.\tau \mid \langle \overline{\tau} \rangle \\
\mathsf{e} & ::= & \mathsf{t} \\
\mathsf{t} & ::= & \mathsf{x} \mid () \mid \mathsf{n} \mid \mathsf{t}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{t}\ \mathsf{t} \mid \lambda(\overline{\mathsf{x}:\tau}).\mathsf{t} \mid \mathsf{t}\ \overline{\mathsf{t}} \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t} \mid \mathsf{unfold}\ \mathsf{t} \mid \langle \overline{\mathsf{t}} \rangle \mid \pi_i(\mathsf{t}) \\
\mathsf{p} & ::= & + \mid - \mid * \\
\mathsf{v} & ::= & () \mid \mathsf{n} \mid \lambda(\overline{\mathsf{x}:\tau}).\mathsf{t} \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v} \mid \langle \overline{\mathsf{v}} \rangle \\
\mathsf{E} & ::= & [\cdot] \mid \mathsf{E}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{v}\ \mathsf{p}\ \mathsf{E} \mid \mathsf{if0}\ \mathsf{E}\ \mathsf{t}\ \mathsf{t} \mid \mathsf{E}\ \overline{\mathsf{t}} \mid \mathsf{v}\ \overline{\mathsf{v}}\ \mathsf{E}\ \overline{\mathsf{t}} \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{E} \mid \mathsf{unfold}\ \mathsf{E} \mid \langle \overline{\mathsf{v}}, \mathsf{E}, \overline{\mathsf{t}} \rangle \mid \pi_i(\mathsf{E}) \\
\Delta & ::= & \cdot \mid \Delta, \alpha \\
\Gamma & ::= & \cdot \mid \Gamma, \mathsf{x}:\tau
\end{array}
$$

2.1.1 Well-Formed Type $\boxed{\Delta \vdash \tau}$

$$
\frac{\alpha \in \Delta}{\Delta \vdash \alpha} \qquad \frac{}{\Delta \vdash \mathsf{unit}} \qquad \frac{}{\Delta \vdash \mathsf{int}} \qquad \frac{\overline{\Delta \vdash \tau} \qquad \Delta \vdash \tau'}{\Delta \vdash (\overline{\tau}) \to \tau'} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \mu\alpha.\tau} \qquad \frac{\Delta \vdash \tau_1 \ \cdots \ \Delta \vdash \tau_n}{\Delta \vdash \langle \tau_1, \ldots, \tau_n \rangle}
$$

2.1.2 Well-Formed Type Environment $\boxed{\vdash \Gamma}$

$$
\frac{}{\vdash \cdot} \qquad \frac{\vdash \Gamma \qquad \cdot \vdash \tau}{\vdash \Gamma, \mathsf{x}:\tau}
$$

2.1.3 Well-Typed Component $\boxed{\Gamma \vdash \mathsf{e}:\tau}$

$$
\frac{\mathsf{x}:\tau \in \Gamma}{\Gamma \vdash \mathsf{x}:\tau} \qquad \frac{}{\Gamma \vdash ():\mathsf{unit}} \qquad \frac{}{\Gamma \vdash \mathsf{n}:\mathsf{int}} \qquad \frac{\Gamma \vdash \mathsf{t}_1:\mathsf{int} \qquad \Gamma \vdash \mathsf{t}_2:\mathsf{int}}{\Gamma \vdash \mathsf{t}_1\ \mathsf{p}\ \mathsf{t}_2:\mathsf{int}}
$$

$$
\frac{\Gamma \vdash \mathsf{t}_1:\mathsf{int} \qquad \Gamma \vdash \mathsf{t}_2:\tau \qquad \Gamma \vdash \mathsf{t}_3:\tau}{\Gamma \vdash \mathsf{if0}\ \mathsf{t}_1\ \mathsf{t}_2\ \mathsf{t}_3:\tau} \qquad \frac{\Gamma, \overline{\mathsf{x}:\tau} \vdash \mathsf{t}:\tau'}{\Gamma \vdash \lambda(\overline{\mathsf{x}:\tau}).\mathsf{t}:(\overline{\tau}) \to \tau'} \qquad \frac{\Gamma \vdash \mathsf{t}_0:(\overline{\tau_1}) \to \tau_2 \qquad \Gamma \vdash \overline{\mathsf{t}}:\overline{\tau_1}}{\Gamma \vdash \mathsf{t}_0\ \overline{\mathsf{t}}:\tau_2}
$$

$$
\frac{\Gamma \vdash \mathsf{t}:\tau[\mu\alpha.\tau/\alpha]}{\Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t}:\mu\alpha.\tau} \qquad \frac{\Gamma \vdash \mathsf{t}:\mu\alpha.\tau}{\Gamma \vdash \mathsf{unfold}\ \mathsf{t}:\tau[\mu\alpha.\tau/\alpha]} \qquad \frac{\Gamma \vdash \mathsf{t}_1:\tau_1 \qquad \cdots \qquad \Gamma \vdash \mathsf{t}_n:\tau_n}{\Gamma \vdash \langle \mathsf{t}_1, \ldots, \mathsf{t}_n \rangle:\langle \tau_1, \ldots, \tau_n \rangle}
$$

$$
\frac{\Gamma \vdash \mathsf{t}:\langle \tau_1, \ldots, \tau_n \rangle}{\Gamma \vdash \pi_i(\mathsf{t}):\tau_i}
$$

2.1.4 Reduction Relation $\boxed{\mathsf{e} \longmapsto \mathsf{e}'}$

$$
\begin{array}{lll}
\mathsf{E}[\mathsf{n}_1\ \mathsf{p}\ \mathsf{n}_2] & \longmapsto \mathsf{E}[\mathrm{prim}(\mathsf{p}, \mathsf{n}_1, \mathsf{n}_2)] & \\
\mathsf{E}[\mathsf{if0}\ 0\ \mathsf{t}_1\ \mathsf{t}_2] & \longmapsto \mathsf{E}[\mathsf{t}_1] & \\
\mathsf{E}[\mathsf{if0}\ \mathsf{n}\ \mathsf{t}_1\ \mathsf{t}_2] & \longmapsto \mathsf{E}[\mathsf{t}_2] & \mathsf{n} \neq 0 \\
\mathsf{E}[\lambda(\overline{\mathsf{x}:\tau}).\mathsf{t}\ \overline{\mathsf{v}}] & \longmapsto \mathsf{E}[\mathsf{t}[\overline{\mathsf{v}}/\overline{\mathsf{x}}]] & \\
\mathsf{E}[\mathsf{unfold}\ (\mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v})] & \longmapsto \mathsf{E}[\mathsf{v}] & \\
\mathsf{E}[\pi_i(\langle \mathsf{v}_1, \ldots, \mathsf{v}_n \rangle)] & \longmapsto \mathsf{E}[\mathsf{v}_i] &
\end{array}
$$

3 Multi-Language: F+T

3.1 Syntax and Semantics

$$
\begin{array}{rcl}
\tau & ::= & \cdots \mid (\overline{\tau}) \xrightarrow{\phi;\phi} \tau' \\
\mathbf{t} & ::= & \cdots \mid {}^{\tau}\mathcal{FT}\,\mathbf{e} \mid \lambda^{\phi}_{\phi}(\overline{\mathbf{x}:\tau}).\mathbf{t} \mid \mathbf{t}\,\overline{\mathbf{t}'} \\
\mathbf{v} & ::= & \cdots \mid \lambda^{\phi}_{\phi}(\overline{\mathbf{x}:\tau}).\mathbf{t} \\
\mathbf{E} & ::= & \cdots \mid {}^{\tau}\mathcal{FT}\,\mathbf{E} \\
\mathbf{q} & ::= & \cdots \mid \mathtt{out} \\
\iota & ::= & \cdots \mid \mathtt{protect}\ \phi,\zeta \mid \mathtt{import}\ \mathbf{r_d}, {}^{\sigma}\mathcal{T}\mathcal{F}^{\tau}\,\mathbf{e} \\
\mathbf{E_I} & ::= & \cdots \mid \mathtt{import}\ \mathbf{r_d}, {}^{\sigma}\mathcal{T}\mathcal{F}^{\tau}\,\mathbf{E};\mathbf{I} \\
\phi & ::= & \cdot \mid \tau :: \phi \\
\sigma & ::= & \zeta \mid \bullet \mid \phi :: \sigma
\end{array}
\qquad
\begin{array}{rcl}
\tau & ::= & \tau \mid \tau \\
e & ::= & \mathbf{e} \mid \mathbf{e} \\
v & ::= & \mathbf{v} \mid \mathbf{v} \\
E & ::= & \mathbf{E} \mid \mathbf{E} \\
\Delta & ::= & \cdot \mid \Delta,\alpha \mid \Delta,\alpha \mid \Delta,\zeta \mid \Delta,\epsilon
\end{array}
$$

3.1.1 Boundary Type Translation

$$
\begin{array}{rcl}
\alpha^{\mathcal{T}} & = & \alpha \\
\mathbf{unit}^{\mathcal{T}} & = & \mathbf{unit} \qquad \mu\alpha.\tau^{\mathcal{T}} = \mu\alpha.(\tau^{\mathcal{T}}) \\
\mathbf{int}^{\mathcal{T}} & = & \mathbf{int} \qquad \langle\tau_1,\ldots,\tau_n\rangle^{\mathcal{T}} = \mathbf{box}\,\langle\tau_1{}^{\mathcal{T}},\ldots,\tau_n{}^{\mathcal{T}}\rangle \\
(\tau_1,\ldots,\tau_n) \to \tau'^{\mathcal{T}} & = & \mathbf{box}\,\forall[\zeta,\epsilon].\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}};\zeta\}^{\epsilon};\sigma'\}^{\mathtt{ra}} \\
 & & \text{where } \sigma' = \tau_n{}^{\mathcal{T}} :: \cdots :: \tau_1{}^{\mathcal{T}} :: \zeta \\
(\tau_1,\ldots,\tau_n) \xrightarrow{\phi_i;\phi_o} \tau'^{\mathcal{T}} & = & \mathbf{box}\,\forall[\zeta,\epsilon].\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}};\phi_o :: \zeta\}^{\epsilon};\sigma'\}^{\mathtt{ra}} \\
 & & \text{where } \sigma' = \tau_n{}^{\mathcal{T}} :: \cdots :: \tau_1{}^{\mathcal{T}} :: \phi_i :: \zeta
\end{array}
$$

NOTE: FT inherits any judgments of F or T not mentioned here explicitly.

3.1.2 Well-Typed Heap Value $\boxed{\Psi \vdash \mathbf{h} :^{\nu} \psi}$

$$
\frac{\cdot \vdash \forall[\Delta].\{\chi;\sigma\}^{\mathbf{q}} \qquad \Psi;\Delta;\cdot;\chi;\sigma;\mathbf{q} \vdash \mathbf{I}}{\Psi \vdash \mathbf{code}[\Delta]\{\chi;\sigma\}^{\mathbf{q}}.\mathbf{I} :^{\mathbf{box}} \forall[\Delta].\{\chi;\sigma\}^{\mathbf{q}}}
\qquad
\frac{\Psi;\cdot \vdash \mathbf{w_0} : \tau_0 \qquad \cdots \qquad \Psi;\cdot \vdash \mathbf{w_n} : \tau_n}{\Psi \vdash \langle \mathbf{w_0},\ldots,\mathbf{w_n}\rangle :^{\nu} \langle\tau_0,\ldots,\tau_n\rangle}
$$

3.1.3 Well-Typed Instruction Sequence $\boxed{\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash \mathbf{I}}$

To the corresponding rules of T, amend the side-condition to forbid $\mathbf{q} = \mathbf{out}$ as well as $\mathbf{q} = \epsilon$ and add the environment Γ.

3.1.4 Well-Typed Instruction $\boxed{\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash \iota \Rightarrow \Delta';\chi';\sigma';\mathbf{q}'}$

To the corresponding rules of T, amend the side-condition to forbid $\mathbf{q} = \mathbf{out}$ as well as $\mathbf{q} = \epsilon$, add the environment Γ, and add the following rules:

$$
\frac{\sigma = \tau_0 :: \cdots :: \tau_j :: \sigma_0 \qquad \sigma' = \tau'_0 :: \cdots :: \tau'_k :: \sigma_0}{\Psi;\Delta,\zeta;\Gamma;\chi;(\tau_0 :: \cdots :: \tau_j :: \zeta);\mathbf{out} \vdash \mathbf{e} : \tau;(\tau'_0 :: \cdots :: \tau'_k :: \zeta) \qquad \mathbf{q} = \mathbf{i} > \mathbf{j} \text{ or } \mathbf{q} = \mathbf{end}\{\hat{\tau};\hat{\sigma}\}}{\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash \mathtt{import}\ \mathbf{r_d}, {}^{\sigma_0}\mathcal{T}\mathcal{F}^{\tau}\,\mathbf{e} \Rightarrow \Delta;(\mathbf{r_d} : \tau^{\mathcal{T}});\sigma';\mathrm{inc}(\mathbf{q},\mathbf{k}-\mathbf{j})}
$$

$$
\frac{\sigma = \phi :: \sigma_0 \qquad \sigma' = \phi :: \zeta}{\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash \mathtt{protect}\ \phi,\zeta \Rightarrow \Delta,\zeta;\chi;\sigma';\mathbf{q}}
$$

3.1.5 Well-Typed Component $\boxed{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash e : \tau; \sigma'}$

To the corresponding rules of T, add the environment Γ and add the following rules:

$$\frac{\mathbf{x} : \tau \in \Gamma}{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \mathbf{x} : \tau; \sigma} \qquad \frac{}{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash () : \mathbf{unit}; \sigma} \qquad \frac{}{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \mathbf{n} : \mathbf{int}; \sigma}$$

$$\frac{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{t}_1 : \mathbf{int}; \sigma_1 \qquad \Psi; \Delta; \Gamma; \chi; \sigma_1; \mathrm{out} \vdash \mathbf{t}_2 : \mathbf{int}; \sigma_2}{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{t}_1\ \mathbf{p}\ \mathbf{t}_2 : \mathbf{int}; \sigma_2}$$

$$\frac{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{t}_1 : \mathbf{int}; \sigma_1 \qquad \Psi; \Delta; \Gamma; \chi; \sigma_1; \mathrm{out} \vdash \mathbf{t}_2 : \tau; \sigma_2 \qquad \Psi; \Delta; \Gamma; \chi; \sigma_1; \mathrm{out} \vdash \mathbf{t}_3 : \tau; \sigma_2}{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{if0}\ \mathbf{t}_1\ \mathbf{t}_2\ \mathbf{t}_3 : \tau; \sigma_2}$$

$$\frac{\Psi; \Delta, \zeta; \Gamma, \overline{\mathbf{x} : \tau}; \chi; \zeta; \mathrm{out} \vdash \mathbf{t} : \tau'; \zeta}{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \lambda(\overline{\mathbf{x} : \tau}).\mathbf{t} : (\overline{\tau}) \to \tau'; \sigma} \qquad \frac{\Psi; \Delta, \zeta; \Gamma, \overline{\mathbf{x} : \tau}; \chi; \phi_{\mathrm{i}} :: \zeta; \mathrm{out} \vdash \mathbf{t} : \tau'; \phi_{\mathrm{o}} :: \zeta}{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \lambda^{\phi_{\mathrm{i}}}_{\phi_{\mathrm{o}}}(\overline{\mathbf{x} : \tau}).\mathbf{t} : (\overline{\tau}) \xrightarrow{\phi_{\mathrm{i}}; \phi_{\mathrm{o}}} \tau'; \sigma}$$

$$\frac{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \mathbf{t} : (\tau_1 \cdots \tau_{\mathrm{n}}) \to \tau'; \sigma_0 \qquad \Psi; \Delta; \Gamma; \chi; \sigma_{\mathrm{i}-1}; \mathrm{out} \vdash \mathbf{t}_{\mathrm{i}} : \tau_{\mathrm{i}}; \sigma_{\mathrm{i}}}{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \mathbf{t}\ \mathbf{t}_1 \cdots \mathbf{t}_{\mathrm{n}} : \tau'; \sigma_{\mathrm{n}}}$$

$$\frac{\begin{array}{c}\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \mathbf{t} : (\tau_1 \cdots \tau_{\mathrm{n}}) \xrightarrow{\phi_{\mathrm{i}}; \phi_{\mathrm{o}}} \tau'; \sigma_0 \\ \Psi; \Delta; \Gamma; \chi; \sigma_{\mathrm{i}-1}; \mathrm{out} \vdash \mathbf{t}_{\mathrm{i}} : \tau_{\mathrm{i}}; \sigma_{\mathrm{i}} \qquad \sigma_{\mathrm{n}} = \phi_{\mathrm{i}} :: \hat{\sigma} \qquad \sigma' = \phi_{\mathrm{o}} :: \hat{\sigma}'\end{array}}{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \mathbf{t}\ \mathbf{t}_1 \cdots \mathbf{t}_{\mathrm{n}} : \tau'; \sigma'}$$

$$\frac{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{t} : \tau[\mu\alpha.\tau/\alpha]; \sigma_1}{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{t} : \mu\alpha.\tau; \sigma_1} \qquad \frac{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{t} : \mu\alpha.\tau; \sigma_1}{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{unfold}\ \mathbf{t} : \tau[\mu\alpha.\tau/\alpha]; \sigma_1}$$

$$\frac{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{t}_1 : \tau_1; \sigma_1 \qquad \cdots \qquad \Psi; \Delta; \Gamma; \chi; \sigma_{\mathrm{n}-1}; \mathrm{out} \vdash \mathbf{t}_{\mathrm{n}} : \tau_{\mathrm{n}}; \sigma_{\mathrm{n}}}{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \langle \mathbf{t}_1, \ldots, \mathbf{t}_{\mathrm{n}} \rangle : \langle \tau_1, \ldots, \tau_{\mathrm{n}} \rangle; \sigma_{\mathrm{n}}}$$

$$\frac{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \mathbf{t} : \langle \tau_1, \ldots, \tau_{\mathrm{n}} \rangle; \sigma_1}{\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathrm{out} \vdash \pi_{\mathrm{i}}(\mathbf{t}) : \tau_{\mathrm{i}}; \sigma_1} \qquad \frac{\Psi; \Delta; \Gamma; \cdot; \sigma; \mathrm{end}\{\tau^{\mathcal{T}}; \sigma'\} \vdash \mathrm{e} : \tau^{\mathcal{T}}; \sigma'}{\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash {}^{\tau}\mathcal{FT}\,\mathrm{e} : \tau; \sigma'}$$

3.1.6 Value Translation

$$
\begin{aligned}
\mathbf{TF}^{\mathsf{unit}}((), \mathrm{M}) &= ((), \mathrm{M}) \\
\mathbf{TF}^{\mathsf{int}}(\mathbf{n}, \mathrm{M}) &= (\mathbf{n}, \mathrm{M}) \\
\mathbf{TF}^{\mu\alpha.\tau}(\mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{v}, \mathrm{M}) &= (\mathbf{fold}_{\mu\alpha.\tau\mathcal{T}}\ \mathrm{v}, \mathrm{M}') \qquad \text{where } \mathbf{TF}^{\tau[\mu\alpha.\tau/\alpha]}(\mathbf{v}, \mathrm{M}) = (\mathrm{v}, \mathrm{M}') \\
\mathbf{TF}^{(\overline{\tau}) \to \tau'}(\boldsymbol{\lambda}(\overline{\mathbf{x}:\tau}).\mathbf{t}, \mathrm{M}) &= (\ell, (\mathrm{M}, \ell \mapsto \mathrm{h})) \\
&\quad \text{where } \mathrm{h} = \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}}; \zeta\}^{\epsilon}; \overline{\tau^{\mathcal{T}}} :: \zeta\}^{\mathrm{ra}}. \\
&\qquad\qquad \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{ra}; \mathtt{import}\ \mathtt{r}_1, {}^{\zeta}\mathcal{T}\mathcal{F}^{\tau'}\ \mathbf{e}; \mathtt{sld}\ \mathtt{ra}, 0; \mathtt{sfree}\ \mathrm{n}{+}1; \mathtt{ret}\ \mathtt{ra}\ \{\mathtt{r1}\} \\
&\quad\quad \mathbf{e} = (\boldsymbol{\lambda}(\overline{\mathbf{x}:\tau}).\mathbf{t})^{\tau}\mathcal{F}\mathcal{T}\ ((\mathtt{sld}\ \mathtt{r1}, \mathrm{n}{+}1{-}\mathrm{i}; \mathtt{ret}\ \mathbf{end}\{\tau^{\mathcal{T}}; \sigma\}\ \{\mathtt{r1}\}), \cdot) \\
&\quad\quad \sigma = \forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}}; \zeta\}^{\epsilon} :: \overline{\tau^{\mathcal{T}}} :: \zeta \\
\mathbf{TF}^{(\overline{\tau}) \xrightarrow{\phi_i;\phi_o} \tau'}(\boldsymbol{\lambda}^{\phi_i}_{\phi_o}(\overline{\mathbf{x}:\tau}).\mathbf{t}, \mathrm{M}) &= (\ell, (\mathrm{M}, \ell \mapsto \mathrm{h})) \\
&\quad \text{where } \mathrm{h} = \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\epsilon}; \overline{\tau^{\mathcal{T}}} :: \phi_i :: \zeta\}^{\mathrm{ra}}. \\
&\qquad\qquad \mathtt{salloc}\ 1{+}|\phi_i|; \mathtt{sst}\ |\phi_i|, \mathtt{ra}; \\
&\qquad\qquad \mathtt{sld}\ \mathtt{r1}, |\phi_i| + \mathrm{n}; \mathtt{sst}\ 1, \mathtt{r1}; \ldots; \mathtt{sld}\ \mathtt{r1}, |\phi_i| + \mathrm{n} + |\phi_i| - 1; \mathtt{sst}\ |\phi_i|, \mathtt{r1}; \\
&\qquad\qquad \mathtt{import}\ \mathtt{r}_1, {}^{\zeta}\mathcal{T}\mathcal{F}^{\tau'}\ \mathbf{e}; \\
&\qquad\qquad \mathtt{sld}\ \mathtt{ra}, |\phi_o|; \\
&\qquad\qquad \mathtt{sld}\ \mathtt{r2}, |\phi_o|{-}1; \mathtt{sst}\ |\phi_o|{+}\mathrm{n}{+}|\phi_i| - 1, \mathtt{r2}; \ldots; \mathtt{sld}\ \mathtt{r2}, 0; \mathtt{sst}\ |\phi_o|{+}\mathrm{n}{+}|\phi_i|{-}|\mathbf{pref}_o|, \mathtt{r2}; \\
&\qquad\qquad \mathtt{sfree}\ \mathrm{n}{+}|\phi_o|{+}1; \mathtt{ret}\ \mathtt{ra}\ \{\mathtt{r1}\} \\
&\quad\quad \mathbf{e} = (\boldsymbol{\lambda}^{\phi_i}_{\phi_o}(\overline{\mathbf{x}:\tau}).\mathbf{t})^{\tau_1}\mathcal{F}\mathcal{T}\ ((\mathtt{sld}\ \mathtt{r1}, |\phi_i| + \mathrm{n}; \mathtt{ret}\ \mathbf{end}\{{\tau_1}^{\mathcal{T}}; \sigma\}\ \{\mathtt{r1}\}), \cdot) \\
&\qquad\qquad \ldots \\
&\qquad\qquad {}^{\tau_n}\mathcal{F}\mathcal{T}\ ((\mathtt{sld}\ \mathtt{r1}, |\phi_i| + 1; \mathtt{ret}\ \mathbf{end}\{{\tau_n}^{\mathcal{T}}; \sigma\}\ \{\mathtt{r1}\}), \cdot) \\
&\quad\quad \sigma = \forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}}; \zeta\}^{\epsilon} :: \overline{\tau^{\mathcal{T}}} :: \phi_i :: \zeta \\
\mathbf{TF}^{\langle\tau_1, \ldots, \tau_n\rangle}(\langle \mathbf{v_0}, \ldots, \mathbf{v_n}\rangle, \mathrm{M}) &= (\ell, (\mathrm{M}_{n+1}, \ell \mapsto \langle \mathrm{w_0}, \ldots, \mathrm{w_n}\rangle)) \quad \mathrm{M_0} = \mathrm{M}, \text{ and } \mathbf{TF}^{\tau_i}(\mathbf{v_i}, \mathrm{M_i}) = (\mathrm{w_i}, \mathrm{M_{i+1}})
\end{aligned}
$$

$$
\begin{aligned}
{}^{\mathsf{unit}}\mathbf{FT}((), \mathrm{M}) &= ((), \mathrm{M}) \\
{}^{\mathsf{int}}\mathbf{FT}(\mathrm{n}, \mathrm{M}) &= (\mathbf{n}, \mathrm{M}) \\
{}^{\mu\alpha.\tau}\mathbf{FT}(\mathbf{fold}_{\mu\alpha.\tau\mathcal{T}}\ \mathrm{w}) &= (\mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{v}, \mathrm{M}') \qquad \text{where } {}^{\tau[\mu\alpha.\tau/\alpha]}\mathbf{FT}(\mathrm{w}, \mathrm{M}) = (\mathbf{v}, \mathrm{M}') \\
{}^{(\overline{\tau_n}) \to \tau'}\mathbf{FT}(\mathrm{w}, \mathrm{M}) &= (\mathbf{v}, (\mathrm{M}, \ell_{\mathbf{end}} \mapsto \mathrm{h}_{\mathbf{end}})) \\
&\quad \text{where } \mathbf{v} = \boldsymbol{\lambda}(\overline{\mathbf{x_n}:\tau_n}).{}^{\tau'}\mathcal{F}\mathcal{T}\ (\mathtt{protect}\ \cdot, \zeta; \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{T}\mathcal{F}^{\tau_1}\ \mathbf{x_1}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \ldots; \\
&\qquad\qquad (\mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{T}\mathcal{F}^{\tau_n}\ \mathbf{x_n}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \\
&\qquad\qquad \mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\zeta]; \mathtt{jmp}\ \mathrm{w}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}]), \cdot) \\
&\quad\quad \mathrm{h}_{\mathbf{end}} = \mathbf{code}[\zeta]\{\mathtt{r1}:\tau'^{\mathcal{T}}; \zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}}.\mathtt{ret}\ \mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}\ \{\mathtt{r1}\} \\
{}^{(\overline{\tau_n}) \xrightarrow{\phi_i;\phi_o} \tau'}\mathbf{FT}(\mathrm{w}, \mathrm{M}) &= (\mathbf{v}, (\mathrm{M}, \ell_{\mathbf{end}} \mapsto \mathrm{h}_{\mathbf{end}})) \\
&\quad \text{where } \mathbf{v} = \boldsymbol{\lambda}^{\phi_i}_{\phi_o}(\overline{\mathbf{x_n}:\tau_n}).{}^{\tau'}\mathcal{F}\mathcal{T}\ (\mathtt{protect}\ \phi_i, \zeta; \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{T}\mathcal{F}^{\tau_1}\ \mathbf{x_1}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \ldots; \\
&\qquad\qquad (\mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{T}\mathcal{F}^{\tau_n}\ \mathbf{x_n}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \\
&\qquad\qquad \mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\phi_o :: \zeta]; \mathtt{jmp}\ \mathrm{w}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}]), \cdot) \\
&\quad\quad \mathrm{h}_{\mathbf{end}} = \mathbf{code}[\zeta]\{\mathtt{r1}:\tau'^{\mathcal{T}}; \zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}}.\mathtt{ret}\ \mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}\ \{\mathtt{r1}\} \\
{}^{\langle\tau_0, \ldots, \tau_n\rangle}\mathbf{FT}(\ell, \mathrm{M}) &= (\langle \mathbf{v_0}, \ldots, \mathbf{v_n}\rangle, \mathrm{M}_{n+1}) \qquad \text{where } \mathrm{M}(\ell) = \langle \mathrm{w_0}, \ldots, \mathrm{w_n}\rangle, \\
&\qquad\qquad \mathrm{M_0} = \mathrm{M}, \text{ and } {}^{\tau_i}\mathbf{FT}(\mathrm{w_i}, \mathrm{M_i}) = (\mathbf{v_i}, \mathrm{M_{i+1}})
\end{aligned}
$$

3.1.7 Reduction Relation $\boxed{\langle \mathbf{M} \mid e \rangle \longmapsto \langle \mathbf{M'} \mid e' \rangle}$

Lift the individual language reduction relations to obtain a multilanguage reduction relation, noting that the contexts are untyped, as for T, we may reach intermediate states with different types and return markers $\mathbf{q}$. This means that a proof of type safety would not be possible using progress and preservation, and we would instead have to use a unary logical relation in the style of [**?**]. We have not done this, but do not anticipate any problems, since the form of this logical relation would be a special case of the binary logical relation for equivalence that we have used.

$$\frac{\mathbf{e} \longmapsto \mathbf{e'}}{\langle \mathbf{M} \mid E[\mathbf{e}] \rangle \longmapsto \langle \mathbf{M} \mid E[\mathbf{e'}] \rangle} \qquad \frac{\langle \mathbf{M} \mid \mathbf{e} \rangle \longmapsto \langle \mathbf{M'} \mid \mathbf{e'} \rangle}{\langle \mathbf{M} \mid E[\mathbf{e}] \rangle \longmapsto \langle \mathbf{M'} \mid E[\mathbf{e'}] \rangle}$$

Add the reduction rules for boundaries:

$$\begin{array}{lll} \langle \mathbf{M} \mid E[{}^{\tau}\mathcal{FT}\ (\mathtt{ret}\ \mathbf{end}\{\tau^{\mathcal{T}}; \sigma\}\ \{\mathbf{r}\}, \cdot)] \rangle & \longmapsto \langle \mathbf{M'} \mid E[\mathbf{v}] \rangle & \text{if } {}^{\tau}\mathbf{FT}(\mathbf{M.R(r)}, \mathbf{M}) = (\mathbf{v}, \mathbf{M'}) \\ \langle \mathbf{M} \mid E[(\mathtt{import}\ \mathbf{r_d}, {}^{\sigma'}\mathcal{TF}^{\tau}\ \mathbf{v}; \mathbf{I}, \cdot)] \rangle & \longmapsto \langle \mathbf{M'} \mid E[(\mathtt{mv}\ \mathbf{r_d}, \mathbf{w}; \mathbf{I}, \cdot)] \rangle & \text{if } \mathbf{TF}^{\tau}(\mathbf{v}, \mathbf{M}) = (\mathbf{w}, \mathbf{M'}) \end{array}$$

Finally, add beta reduction for the new lambda form, which is identical to normal beta reduction:

$$\langle \mathbf{M} \mid E[(\lambda^{\phi_i}_{\phi_o}(\overline{\mathbf{x}:\tau}).\mathbf{t})\ \overline{\mathbf{t'}}] \rangle \quad \longmapsto \langle \mathbf{M} \mid E[\mathbf{t}[\overline{\mathbf{t'}/\mathbf{x}}]] \rangle$$

3.1.8 Reduction Relation $\boxed{\langle \mathbf{M} \mid I \rangle \longmapsto \langle \mathbf{M'} \mid I' \rangle}$

Add instruction reduction for stack protection, which has no operational consequence:

$$\langle (\mathbf{H}, \mathbf{R}, \mathbf{S}) \mid \mathtt{protect}\ \phi, \zeta; \mathbf{I} \rangle \longrightarrow \langle (\mathbf{H}, \mathbf{R}, \mathbf{S}) \mid \mathbf{I} \rangle$$

3.2 General Contexts and Contextual Equivalence

$$
\begin{aligned}
\mathsf{C} ::= {} & [\cdot] \mid \mathsf{C}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{t}\ \mathsf{p}\ \mathsf{C} \mid \mathsf{if0}\ \mathsf{C}\ \mathsf{t}\ \mathsf{t} \\
& \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{C}\ \mathsf{t} \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{t}\ \mathsf{C} \mid \lambda(\overline{\mathsf{x}:\tau}).\mathsf{C} \\
& \mid \lambda^{\phi_i}_{\phi_o}(\overline{\mathsf{x}:\tau}).\mathsf{C} \mid \mathsf{C}\ \overline{\mathsf{t}} \mid \mathsf{t}\ \overline{\mathsf{t}}\ \mathsf{C}\ \overline{\mathsf{t}} \\
& \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{C} \mid \mathsf{unfold}\ \mathsf{C} \mid \langle \overline{\mathsf{t}}, \mathsf{C}, \overline{\mathsf{t}} \rangle \\
& \mid \pi_i(\mathsf{C}) \mid {}^{\tau}\mathcal{FT}\ \mathsf{C}
\end{aligned}
\qquad
\begin{aligned}
\mathbf{C} &::= (\mathbf{C_I}, \mathbf{H}) \mid (\mathbf{I}, \mathbf{C_H}) \\
\mathbf{C_I} &::= [\cdot] \mid \mathtt{import}\ \mathbf{r_d}, {}^{\sigma}\mathcal{T}\mathcal{F}^{\tau}\ \mathbf{C}; \mathbf{I} \mid \iota; \mathbf{C_I} \\
\mathbf{C_H} &::= \mathbf{C_H}, \ell \mapsto \mathbf{h} \mid \mathbf{H}, \ell \mapsto \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{C_I}
\end{aligned}
$$

$$C ::= \mathsf{C} \mid \mathbf{C}$$

3.2.1 Plug Function $\boxed{C[e]}$

$$
\begin{aligned}
[\cdot][\mathsf{e}] &= \mathsf{e} \\
(\mathsf{C}\ \mathsf{p}\ \mathsf{t})[e] &= (\mathsf{C}[e])\ \mathsf{p}\ \mathsf{t} \\
(\mathsf{t}\ \mathsf{p}\ \mathsf{C})[e] &= \mathsf{t}\ \mathsf{p}\ (\mathsf{C}[e]) \\
(\mathsf{if0}\ \mathsf{C}\ \mathsf{t}_1\ \mathsf{t}_2)[e] &= \mathsf{if0}\ (\mathsf{C}[e])\ \mathsf{t}_1\ \mathsf{t}_2 \\
(\mathsf{if0}\ \mathsf{t}_0\ \mathsf{C}\ \mathsf{t}_2)[e] &= \mathsf{if0}\ \mathsf{t}_0\ (\mathsf{C}[e])\ \mathsf{t}_2 \\
(\mathsf{if0}\ \mathsf{t}_0\ \mathsf{t}_1\ \mathsf{C})[e] &= \mathsf{if0}\ \mathsf{t}_0\ \mathsf{t}_1\ (\mathsf{C}[e]) \\
(\lambda(\overline{\mathsf{x}:\tau}).\mathsf{C})[e] &= \lambda(\overline{\mathsf{x}:\tau}).(\mathsf{C}[e]) \\
(\lambda^{\phi_i}_{\phi_o}(\overline{\mathsf{x}:\tau}).\mathsf{C})[e] &= \lambda^{\phi_i}_{\phi_o}(\overline{\mathsf{x}:\tau}).(\mathsf{C}[e]) \\
(\mathsf{C}\ \overline{\mathsf{t}})[e] &= (\mathsf{C}[e])\ \overline{\mathsf{t}} \\
(\mathsf{t}'\ \overline{\mathsf{t}}\ \mathsf{C}\ \overline{\mathsf{t}})[e] &= \mathsf{t}'\ \overline{\mathsf{t}}\ (\mathsf{C}[e])\ \overline{\mathsf{t}} \\
(\mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{C})[e] &= \mathsf{fold}_{\mu\alpha.\tau}\ (\mathsf{C}[e]) \\
(\mathsf{unfold}\ \mathsf{C})[e] &= \mathsf{unfold}\ (\mathsf{C}[e]) \\
(\langle \overline{\mathsf{t}}, \mathsf{C}, \overline{\mathsf{t}'} \rangle)[e] &= \langle \overline{\mathsf{t}}, (\mathsf{C}[e]), \overline{\mathsf{t}'} \rangle \\
(\pi_i(\mathsf{C}))[e] &= \pi_i(\mathsf{C}[e]) \\
({}^{\tau}\mathcal{FT}\ \mathsf{C})[e] &= {}^{\tau}\mathcal{FT}\ (\mathsf{C}[e])
\end{aligned}
$$

$$
(\mathbf{C_I}, \mathbf{H})[e] = \begin{cases} (\mathbf{C_I}[\mathbf{I}], (\mathbf{H}, \mathbf{H}')) & e = (\mathbf{I}, \mathbf{H}') \wedge \mathbf{C_I} \text{ contains no language boundaries} \\ (\mathbf{C_I}[e], \mathbf{H}) & \text{otherwise} \end{cases}
$$

$$
(\mathbf{I}, \mathbf{C_H})[e] = \begin{cases} (\mathbf{I}, (\mathbf{C_H}[\mathbf{I}], \mathbf{H}')) & e = (\mathbf{I}, \mathbf{H}') \wedge \mathbf{C_H} \text{ contains no language boundaries} \\ (\mathbf{I}, \mathbf{C_H}[e]) & \text{otherwise} \end{cases}
$$

$$
\begin{aligned}
[\cdot][\mathbf{I}] &= \mathbf{I} \\
(\mathtt{import}\ \mathbf{r_d}, {}^{\sigma}\mathcal{T}\mathcal{F}^{\tau}\ \mathbf{C}; \mathbf{I})[e] &= \mathtt{import}\ \mathbf{r_d}, {}^{\sigma}\mathcal{T}\mathcal{F}^{\tau}\ (\mathbf{C}[e]); \mathbf{I}
\end{aligned}
$$

$$
\begin{aligned}
(\iota; \mathbf{C_I})[e] &= \iota; \mathbf{C_I}[e] \\
(\mathbf{C_H}, \ell \mapsto \mathbf{h})[e] &= (\mathbf{C_H}[e]), \ell \mapsto \mathbf{h} \\
(\mathbf{H}, \ell \mapsto \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{C_I})[e] &= \mathbf{H}, \ell \mapsto \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.(\mathbf{C_I}[e])
\end{aligned}
$$

3.2.2 Well-Typed Context $\boxed{\vdash C : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{q}' \vdash \tau'; \sigma_1)}$

$$\frac{\Psi \subseteq \Psi' \qquad \Delta \subseteq \Delta' \qquad \Gamma \subseteq \Gamma' \qquad \Delta \vdash \chi' \leq \chi}{\vdash [\cdot] : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{out} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma; \mathrm{out} \vdash \tau; \sigma')}$$

$$\frac{\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{int}; \sigma_1) \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_1; \mathrm{out} \vdash \mathsf{t} : \mathsf{int}; \sigma_2}{\vdash \mathsf{C}\ \mathsf{p}\ \mathsf{t} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{int}; \sigma_2)}$$

$$\frac{\Psi'; \Delta'; \Gamma'; \cdot; \sigma_0; \mathrm{out} \vdash \mathsf{t} : \mathsf{int}; \sigma_1 \qquad \vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_1; \mathrm{out} \vdash \mathsf{int}; \sigma_2)}{\vdash \mathsf{t}\ \mathsf{p}\ \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{int}; \sigma_2)}$$

$$\frac{\begin{array}{c}\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{int}; \sigma_1) \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_1; \mathrm{out} \vdash \mathsf{t}_1 : \tau; \sigma_2 \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_1; \mathrm{out} \vdash \mathsf{t}_2 : \tau; \sigma_2\end{array}}{\vdash \mathsf{if0}\ \mathsf{C}\ \mathsf{t}_1\ \mathsf{t}_2 : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau; \sigma_2)}$$

$$\frac{\begin{array}{c}\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{t}_0 : \mathsf{int}; \sigma_1 \\ \vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_1; \mathrm{out} \vdash \tau; \sigma_2) \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_1; \mathrm{out} \vdash \mathsf{t}_2 : \tau; \sigma_2\end{array}}{\vdash \mathsf{if0}\ \mathsf{t}_0\ \mathsf{C}\ \mathsf{t}_2 : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau; \sigma_2)}$$

$$\frac{\begin{array}{c}\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{t}_0 : \mathsf{int}; \sigma_1 \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_1; \mathrm{out} \vdash \mathsf{t}_1 : \tau; \sigma_2 \qquad \vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_1; \mathrm{out} \vdash \tau; \sigma_2)\end{array}}{\vdash \mathsf{if0}\ \mathsf{t}_0\ \mathsf{t}_1\ \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau; \sigma_2)}$$

$$\frac{\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; (\Delta', \zeta); (\Gamma', \overline{\mathsf{x} : \tau}); \chi'; \zeta; \mathrm{out} \vdash \tau'; \zeta)}{\vdash \lambda(\overline{\mathsf{x} : \tau}).\mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash (\overline{\tau}) \to \tau'; \sigma_0)}$$

$$\frac{\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; (\Delta', \zeta); (\Gamma', \overline{\mathsf{x} : \tau}); \chi'; \phi_\mathrm{i} :: \zeta; \mathrm{out} \vdash \tau'; \phi_\mathrm{o} :: \zeta)}{\vdash \lambda^{\phi_\mathrm{i}}_{\phi_\mathrm{o}}(\overline{\mathsf{x} : \tau}).\mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash (\overline{\tau}) \xrightarrow{\phi_\mathrm{i}; \phi_\mathrm{o}} \tau'; \sigma_0)}$$

$$\frac{\begin{array}{c}\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash (\tau_1, \ldots, \tau_\mathrm{n}) \to \tau'; \sigma_0) \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{\mathrm{i}-1}; \mathrm{out} \vdash \mathsf{t}_\mathrm{i} : \tau_\mathrm{i}; \sigma_\mathrm{i}\end{array}}{\vdash \mathsf{C}\ \mathsf{t}_1 \cdots \mathsf{t}_\mathrm{n} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau; \sigma_\mathrm{n})}$$

$$\frac{\begin{array}{c}\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash (\tau_1, \ldots, \tau_\mathrm{n}) \xrightarrow{\phi_\mathrm{i}; \phi_\mathrm{o}} \tau'; \sigma_0) \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{\mathrm{i}-1}; \mathrm{out} \vdash \mathsf{t}_\mathrm{i} : \tau_\mathrm{i}; \sigma_\mathrm{i} \qquad \sigma_\mathrm{n} = \phi_\mathrm{i} :: \hat{\sigma} \qquad \sigma' = \phi_\mathrm{o} :: \hat{\sigma}\end{array}}{\vdash \mathsf{C}\ \mathsf{t}_1 \cdots \mathsf{t}_\mathrm{n} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau; \sigma')}$$

$$\frac{\begin{array}{c}\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{t} : (\tau_1, \ldots, \tau_\mathrm{n}) \to \tau'; \sigma_0 \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{t}_1 : \tau_1; \sigma_1 \qquad \cdots \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{\mathrm{i}-1}; \mathrm{out} \vdash \mathsf{t}_\mathrm{i} : \tau_\mathrm{i}; \sigma_\mathrm{i} \\ \vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_\mathrm{i}; \mathrm{out} \vdash \tau_{\mathrm{i}+1}; \sigma_{\mathrm{i}+1}) \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{\mathrm{i}+1}; \mathrm{out} \vdash \mathsf{t}_{\mathrm{i}+2} : \tau_{\mathrm{i}+2}; \sigma_{\mathrm{i}+2} \qquad \cdots \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{\mathrm{n}-1}; \mathrm{out} \vdash \mathsf{t}_\mathrm{n} : \tau_\mathrm{n}; \sigma_\mathrm{n}\end{array}}{\vdash \mathsf{t}\ \mathsf{t}_1 \cdots \mathsf{t}_\mathrm{i}\ \mathsf{C}\ \mathsf{t}_{\mathrm{i}+2} \cdots \mathsf{t}_\mathrm{n} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau'; \sigma_\mathrm{n})}$$

$$\frac{\begin{array}{c}\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{t} : (\tau_1, \ldots, \tau_\mathrm{n}) \xrightarrow{\phi_\mathrm{i}; \phi_\mathrm{o}} \tau'; \sigma_0 \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{t}_1 : \tau_1; \sigma_1 \qquad \cdots \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{\mathrm{i}-1}; \mathrm{out} \vdash \mathsf{t}_\mathrm{i} : \tau_\mathrm{i}; \sigma_\mathrm{i} \\ \vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_\mathrm{i}; \mathrm{out} \vdash \tau_{\mathrm{i}+1}; \sigma_{\mathrm{i}+1}) \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{\mathrm{i}+1}; \mathrm{out} \vdash \mathsf{t}_{\mathrm{i}+2} : \tau_{\mathrm{i}+2}; \sigma_{\mathrm{i}+2} \\ \cdots \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{\mathrm{n}-1}; \mathrm{out} \vdash \mathsf{t}_\mathrm{n} : \tau_\mathrm{n}; \sigma_\mathrm{n} \qquad \sigma_\mathrm{n} = \phi_\mathrm{i} :: \hat{\sigma} \qquad \sigma' = \phi_\mathrm{o} :: \hat{\sigma}\end{array}}{\vdash \mathsf{t}\ \mathsf{t}_1 \cdots \mathsf{t}_\mathrm{i}\ \mathsf{C}\ \mathsf{t}_{\mathrm{i}+2} \cdots \mathsf{t}_\mathrm{n} : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau'; \sigma')}$$

$$\frac{\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau[\mu\alpha.\tau/\alpha]; \sigma_1)}{\vdash \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mu\alpha.\tau; \sigma_1)}$$

$$\frac{\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mu\alpha.\tau; \sigma_1)}{\vdash \mathsf{unfold}\ \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau[\mu\alpha.\tau/\alpha]; \sigma_1)}$$

$$\frac{\begin{array}{c}\Psi'; \Delta'\Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \mathsf{t_1} : \tau_1; \sigma_1 \qquad \cdots \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{i-1}; \mathrm{out} \vdash \mathsf{t_i} : \tau_i; \sigma_i \\ \vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_i; \mathrm{out} \vdash \tau_{i+1}; \sigma_{i+1}) \\ \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{i+1}; \mathrm{out} \vdash \mathsf{t_{i+2}} : \tau_{i+2}; \sigma_{i+2} \qquad \cdots \qquad \Psi'; \Delta'; \Gamma'; \chi'; \sigma_{n-1}; \mathrm{out} \vdash \mathsf{t_n} : \tau_n; \sigma_n\end{array}}{\vdash \langle \mathsf{t_1}, \ldots, \mathsf{t_i}, \mathsf{C}, \mathsf{t_{i+2}}, \ldots, \mathsf{t_n} \rangle : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \langle \tau_1, \ldots, \tau_n \rangle; \sigma_n)}$$

$$\frac{\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \langle \tau_1, \ldots, \tau_n \rangle; \sigma_1)}{\vdash \pi_i(\mathsf{C}) : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau_i; \sigma_1)}$$

$$\frac{\vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{end}\{\tau^{\mathcal{T}}; \sigma_1\} \vdash \tau^{\mathcal{T}}; \sigma_1)}{\vdash {}^{\tau}\mathcal{FT}\ \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathrm{out} \vdash \tau; \sigma_1)}$$

$$\frac{\begin{array}{c}\Psi' \vdash \mathrm{H} : \Psi \\ \text{ret-type}(q', \chi', \sigma_0) = \tau; \sigma_1 \qquad \vdash \mathrm{C_I} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow ((\Psi', \Psi); \Delta'; \Gamma'; \chi'; \sigma_0; q')\end{array}}{\vdash (\mathrm{C_I}, \mathrm{H}) : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; q' \vdash \tau; \sigma_1)}$$

$$\frac{\begin{array}{c}\vdash \mathrm{C_H} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi' \vdash \Psi) \\ \text{ret-type}(q', \chi', \sigma_0) = \tau; \sigma_1 \qquad (\Psi', \Psi); \Delta'; \Gamma'; \chi'; \sigma_0; q' \vdash \mathrm{I}\end{array}}{\vdash (\mathrm{I}, \mathrm{C_H}) : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; q' \vdash \tau; \sigma_1)}$$

$$\frac{\Psi \subseteq \Psi' \qquad \Delta \subseteq \Delta' \qquad \Gamma \subseteq \Gamma' \qquad \Delta \vdash \chi' \leq \chi \qquad \text{ret-type}(q, \chi, \sigma) = \tau; \sigma'}{\vdash [\cdot] : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma; q)}$$

$$\frac{\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; q' \vdash \iota \Rightarrow \Delta''; \chi''; \sigma_1; q'' \qquad \vdash \mathrm{C_I} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta''; \Gamma'; \chi''; \sigma_1; q'')}{\vdash \iota; \mathrm{C_I} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; q')}$$

$$\frac{\begin{array}{c}\sigma_0 = \tau_0 :: \ldots :: \tau_j :: \sigma'' \\ \vdash \mathsf{C} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; (\Delta', \zeta); \Gamma'; \chi'; \tau_0 :: \ldots :: \tau_j :: \zeta; \mathrm{out} \vdash \tau; \tau'_0 :: \ldots :: \tau'_k :: \zeta) \\ q' = i > j \text{ or } q' = \mathrm{end}\{\hat{\tau}; \hat{\sigma}\} \qquad \Psi'; \Delta'; \Gamma'; (r_d : \tau^{\mathcal{T}}); \tau'_0 :: \ldots :: \tau'_k :: \sigma''; \mathrm{inc}(q', k{-}j) \vdash \mathrm{I}\end{array}}{\vdash (\mathtt{import}\ r_d, {}^{\sigma''}\mathcal{TF}^{\tau}\ \mathsf{C}); \mathrm{I} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; q')}$$

$$\frac{\begin{array}{c}\mathrm{H} = \ell_1 \mapsto h_1, \ldots, \ell_n \mapsto h_n \qquad \mathrm{H}' = \ell'_1 \mapsto h'_1, \ldots, \ell'_m \mapsto h'_n \\ \Psi_1 = \{\ell_1 : \psi_1, \ldots, \ell_n : \psi_n, \ell : \forall[\Delta'].\{\chi'; \sigma_0\}^{q'}, \ell'_1 : \psi'_1, \ldots, \ell'_m : \psi'_m\} \qquad \cdot \vdash \psi_1 \ \cdots \ \cdot \vdash \psi_n \\ \Psi_0, \Psi_1 \vdash h_1 : {}^{\psi_1} \ \cdots \ \Psi_0, \Psi_1 \vdash h_n : {}^{\psi_n} \qquad \vdash \mathrm{C_I} : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow ((\Psi_0, \Psi_1); \Delta'; \cdot; \chi'; \sigma_0; q') \\ \cdot \vdash \psi'_1 \ \cdots \ \cdot \vdash \psi'_m \qquad \Psi, \Psi_1 \vdash h'_1 : {}^{\psi'_1} \ \cdots \ \Psi, \Psi_1 \vdash h'_m : {}^{\psi'_m}\end{array}}{\vdash \mathrm{H}, \ell \mapsto \mathrm{code}[\Delta']\{\chi'; \sigma_0\}^{q'}.\mathrm{C_I}, \mathrm{H}' : (\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \tau; \sigma') \rightsquigarrow (\Psi_0 \vdash \Psi_1)}$$

3.2.3 Contextual Equivalence

$$
\begin{aligned}
&\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash e_1 \approx^{ctx} e_2 : \tau;\hat{\sigma} \stackrel{\text{def}}{=} \\
&\quad \Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash e_1 : \tau;\hat{\sigma} \ \wedge\ \Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash e_2 : \tau;\hat{\sigma} \ \wedge \\
&\quad \forall C, \mathbf{M}, \Psi', \chi', \sigma', \mathbf{q}', \tau', \hat{\sigma}'. \\
&\qquad \vdash C : (\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash \tau;\hat{\sigma}) \rightsquigarrow (\Psi';\cdot;\cdot;\chi';\sigma';\mathbf{q}' \vdash \tau';\hat{\sigma}') \ \wedge\ \vdash \mathbf{M} : (\Psi', \chi', \sigma') \\
&\qquad \Longrightarrow\ (\langle \mathbf{M} \mid C[e_1] \rangle \downarrow \iff \langle \mathbf{M} \mid C[e_2] \rangle \downarrow)
\end{aligned}
$$

3.2.4 CIU Equivalence

$$
\begin{aligned}
&\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash e_1 \approx^{ciu} e_2 : \tau;\hat{\sigma} \stackrel{\text{def}}{=} \\
&\quad \Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash e_1 : \tau;\hat{\sigma} \ \wedge\ \Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q} \vdash e_2 : \tau;\hat{\sigma} \ \wedge \\
&\quad \forall \delta, \gamma, E, \mathbf{M}, \Psi', \mathbf{q}', \tau', \hat{\sigma}'. \\
&\qquad \cdot \vdash \delta : \Delta \ \wedge\ \Psi';\cdot;\cdot;\cdot;\bullet;\mathbf{out} \vdash \gamma : \Gamma;\bullet \ \wedge \\
&\qquad \vdash E : (\Psi;\cdot;\cdot;\chi;\sigma;\mathbf{q} \vdash \tau;\hat{\sigma}) \rightsquigarrow (\Psi';\cdot;\cdot;\chi;\sigma;\mathbf{q}' \vdash \tau';\hat{\sigma}') \ \wedge\ \vdash \mathbf{M} : (\Psi', \chi, \sigma) \\
&\qquad \Longrightarrow\ (\langle \mathbf{M} \mid E[\delta(\gamma(e_1))] \rangle \downarrow \iff \langle \mathbf{M} \mid E[\delta(\gamma(e_2))] \rangle \downarrow)
\end{aligned}
$$

3.3 Logical Relation

NOTE: We used curr-S(W) $\Subset X$ as shorthand for currentMR($W(i_{\text{stk}})$) $\Subset_W X$ and curr-R(W) $\Subset X$ as shorthand for currentMR($W(i_{\text{reg}})$) $\Subset_W X$ in the accompanying paper. This shorthand does not appear in this technical report.

Worlds and Auxiliary Definitions Worlds consist of a sequence of islands that describe the current state of the memories (and how they are related) of the two computations we wish to relate. The essential idea here is that the islands θ in the sequence Θ will specify constraints on *disjoint* parts of memory. We obtain constraints on the entire memory via a disjoint union of the memories specified by the islands.

Therefore, we begin with some simple definitions for memory objects that we will make use of in islands. We need to be able to lift various pieces of memory to a full program memory $\mathbf{M} = (\mathbf{H}, \mathbf{R}, \mathbf{S})$. In many cases, we may not want to impose a constraint on the register file and stack, so we allow $\bot$ to appear in those positions. Since disjoint heap fragments can be merged, the heap can be left unconstrained just by using an empty heap.

$$\begin{aligned} \text{Regs}_\bot &= \{\mathbf{R}\} \cup \{\bot\} \\ \text{Stack}_\bot &= \{\mathbf{S}\} \cup \{\bot\} \end{aligned} \qquad \begin{aligned} \{\cdot\} &\stackrel{\text{def}}{=} (\{\cdot\}, \bot, \bot) \\ \mathbf{H}\restriction &\stackrel{\text{def}}{=} (\mathbf{H}, \bot, \bot) \\ \mathbf{R}\restriction &\stackrel{\text{def}}{=} (\{\cdot\}, \mathbf{R}, \bot) \\ \mathbf{S}\restriction &\stackrel{\text{def}}{=} (\{\cdot\}, \bot, \mathbf{S}) \end{aligned}$$

A world W consists of a step index k, a pair of heap types $\mathbf{\Psi_1}$ and $\mathbf{\Psi_2}$, and a sequence Θ of islands θ. Each island expresses invariants on certain parts of memory by encoding a state transition system and a memory relation MR that establishes which pairs of memories are acceptable in each state. (See Dreyer *et al.* [1] for details.)

The first three islands in Θ are distinguished: they track the register file, the stack, and the immutable contents of the heap, respectively. We assign these islands the indices i_{reg}, i_{stk}, and i_{box}, respectively. Further islands can be added to a world to encode invariants about mutable data.

$$\begin{aligned}
\text{World}_n &\stackrel{\text{def}}{=} \{\, W = (k, \mathbf{\Psi_1}, \mathbf{\Psi_2}, \Theta) \mid k < n \ \wedge\ \exists m \geq 3.\ \Theta \in \text{Island}_k^m \ \wedge \\
&\quad (\exists s_{\text{reg}}.\ \Theta(i_{\text{reg}}) = \text{island}_{\text{reg}}(s_{\text{reg}}, k) \ \wedge\ \mathbf{\Psi_1} \vdash s_{\text{reg}}.\mathbf{R_1} : s_{\text{reg}}.\boldsymbol{\chi_1} \ \wedge\ \mathbf{\Psi_2} \vdash s_{\text{reg}}.\mathbf{R_2} : s_{\text{reg}}.\boldsymbol{\chi_2}) \wedge \\
&\quad (\exists s_{\text{stk}}.\ \Theta(i_{\text{stk}}) = \text{island}_{\text{stk}}(s_{\text{stk}}, k) \ \wedge\ \mathbf{\Psi_1} \vdash s_{\text{stk}}.\mathbf{S_1} : s_{\text{stk}}.\boldsymbol{\sigma_1} \ \wedge\ \mathbf{\Psi_2} \vdash s_{\text{stk}}.\mathbf{S_2} : s_{\text{stk}}.\boldsymbol{\sigma_2}) \wedge \\
&\quad (\exists s_{\text{box}}.\ \Theta(i_{\text{box}}) = \text{island}_{\text{box}}(s_{\text{box}}, k) \ \wedge \mathbf{\Psi_1^{ref}} \vdash s_{\text{box}}.\mathbf{H_1} : \mathbf{\Psi_1^{box}} \ \wedge\ \mathbf{\Psi_2^{ref}} \vdash s_{\text{box}}.\mathbf{H_2} : \mathbf{\Psi_2^{box}})\} \\
\text{Island}_n &\stackrel{\text{def}}{=} \{\, \theta = (s, S, \delta, \pi, \text{MR}, \text{bij}) \mid \ s \in S \ \wedge\ S \in \text{Set} \ \wedge\ \delta \subseteq S \times S \ \wedge\ \pi \subseteq \delta \ \wedge \\
&\quad \delta, \pi \text{ reflexive} \wedge \delta, \pi \text{ transitive} \wedge \text{MR} \in S \to \text{MemRel}_n \ \wedge\ \text{bij} \in S \to \mathbb{P}(\text{Val} \times \text{Val}) \,\}
\end{aligned}$$

$$\text{MemAtom}_n \stackrel{\text{def}}{=} \{\, (W, \mathbf{M_1}, \mathbf{M_2}) \mid \ W \in \text{World}_n \wedge\ \mathbf{M_1}, \mathbf{M_2} \in \text{Heap} \times \text{Regs}_\bot \times \text{Stack}_\bot \,\}$$

$$\text{MemRel}_n \stackrel{\text{def}}{=} \{\, \varphi_M \subseteq \text{MemAtom}_n \mid \ \forall (W, \mathbf{M_1}, \mathbf{M_2}) \in \varphi_M.\ \forall W' \sqsupseteq W.\ (W', \mathbf{M_1}, \mathbf{M_2}) \in \varphi_M \,\}$$

The transition systems for θ_{reg} and θ_{stk} encode the current contents of each side's register file and stack, respectively. They may transition freely between states, since the register file and stack are fairly free in how they can change during program execution. The states of θ_{box} encode the contents of the immutable part of

the heap on each side. This island is allowed to transition only by adding more immutable data to the heap.

$$
\begin{aligned}
i_{\text{reg}} &= 1 \\
S_{\text{reg}} &= \{\, (\mathbf{R_1}, \boldsymbol{\chi_1}, \mathbf{R_2}, \boldsymbol{\chi_2}) \,\} \\
\text{island}_{\text{reg}}(s,k) &= (s, S_{\text{reg}}, S_{\text{reg}} \times S_{\text{reg}}, S_{\text{reg}} \times S_{\text{reg}}, \lambda s.\{(W, s.\mathbf{R_1}\restriction, s.\mathbf{R_2}\restriction) \mid W \in \text{World}_k\}, \lambda s.\emptyset)
\end{aligned}
$$

$$
\begin{aligned}
i_{\text{stk}} &= 2 \\
S_{\text{stk}} &= \{\, (\mathbf{S_1}, \boldsymbol{\sigma_1}, \mathbf{S_2}, \boldsymbol{\sigma_2}) \,\} \\
\text{island}_{\text{stk}}(s,k) &= (s, S_{\text{stk}}, S_{\text{stk}} \times S_{\text{stk}}, S_{\text{stk}} \times S_{\text{stk}}, \lambda s.\{(W, s.\mathbf{S_1}\restriction, s.\mathbf{S_2}\restriction) \mid W \in \text{World}_k\}, \lambda s.\emptyset)
\end{aligned}
$$

$$
\begin{aligned}
i_{\text{box}} &= 3 \\
S_{\text{box}} &= \{\, (\mathbf{H_1}, \mathbf{H_2}) \,\} \\
\delta_{\text{box}} &= \{((\mathbf{H_1}, \mathbf{H_2}), (\mathbf{H_1'}, \mathbf{H_2'})) \mid \mathbf{H_1} \subseteq \mathbf{H_1'} \wedge \mathbf{H_2} \subseteq \mathbf{H_2'}\} \\
\text{island}_{\text{box}}(s,k) &= (s, S_{\text{box}}, \delta_{\text{box}}, \delta_{\text{box}}, \lambda s.\{(W, (s.\mathbf{H_1})\restriction, (s.\mathbf{H_2})\restriction) \mid W \in \text{World}_k\}, \lambda s.\emptyset)
\end{aligned}
$$

Two memory objects that describe disjoint parts of memory can be merged into one compound memory object via the $\otimes$ operator.

$\boxed{\mathbf{M_1} \otimes \mathbf{M_2}}$ where $\mathbf{M_1}, \mathbf{M_2} \in (\{\mathbf{H}\} \times \text{Regs}_\bot \times \text{Stack}_\bot)$

$$
(\mathbf{H_1}, \mathbf{R_1}, \mathbf{S_1}) \otimes (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2}) = \begin{cases} (\mathbf{H_1} \uplus \mathbf{H_2}, \mathbf{R}, \mathbf{S}) & \text{where } \mathbf{R} = \mathbf{R_1} \text{ if } \mathbf{R_2} = \bot; \mathbf{R} = \mathbf{R_2} \text{ if } \mathbf{R_1} = \bot \\ & \qquad \mathbf{S} = \mathbf{S_1} \text{ if } \mathbf{S_2} = \bot; \mathbf{S} = \mathbf{S_2} \text{ if } \mathbf{S_1} = \bot \\ \text{undefined} & \text{otherwise} \end{cases}
$$

$$
\varphi_M \otimes \varphi'_M \;=\; \{\, (W, \mathbf{M_1} \otimes \mathbf{M_1'}, \mathbf{M_2} \otimes \mathbf{M_2'}) \mid (W, \mathbf{M_1}, \mathbf{M_2}) \in \varphi_M \;\wedge\; (W, \mathbf{M_1'}, \mathbf{M_2'}) \in \varphi'_M \,\}
$$

These are standard operations for dealing with step indexing: we can approximate a world or relation to a given number of steps with $\lfloor \cdot \rfloor_k$, and we can expend a step using the $\triangleright$ operator (read "later").

$$
\begin{aligned}
\lfloor (\theta_1, \ldots, \theta_m) \rfloor_k &\stackrel{\text{def}}{=} (\lfloor \theta_1 \rfloor_k, \ldots, \lfloor \theta_m \rfloor_k) \\
\lfloor (s, S, \delta, \pi, \text{MR}, \text{bij}) \rfloor_k &\stackrel{\text{def}}{=} (s, S, \delta, \pi, \lfloor \text{MR} \rfloor_k, \text{bij}) \\
\lfloor \text{MR} \rfloor_k &\stackrel{\text{def}}{=} \lambda s.\ \lfloor \text{MR}(s) \rfloor_k \\
\lfloor \varphi_M \rfloor_k &\stackrel{\text{def}}{=} \{\, (W, \mathbf{M_1}, \mathbf{M_2}) \in \varphi_M \mid\ W.k < k \,\}
\end{aligned}
$$

$$
\begin{aligned}
\triangleright(k+1, \boldsymbol{\Psi_1}, \boldsymbol{\Psi_2}, \Theta) &\stackrel{\text{def}}{=} (k, \boldsymbol{\Psi_1}, \boldsymbol{\Psi_2}, \lfloor \Theta \rfloor_k) \\
\triangleright\varphi_e &\stackrel{\text{def}}{=} \{\, (W, e_1, e_2) \mid W.k > 0 \implies (\triangleright W, e_1, e_2) \in \varphi_e \,\} \\
\triangleright\varphi_v &\stackrel{\text{def}}{=} \{\, (W, v_1, v_2) \mid W.k > 0 \implies (\triangleright W, v_1, v_2) \in \varphi_v \,\} \\
\triangleright\varphi_w &\stackrel{\text{def}}{=} \{\, (W, w_1, w_2) \mid W.k > 0 \implies (\triangleright W, w_1, w_2) \in \varphi_w \,\}
\end{aligned}
$$

Future worlds W' of a given world W, written $W' \sqsupseteq W$, may differ from W in any or all of the following ways: they may have expended steps, allocated additional memory, added new islands, or taken transitions in existing islands. Public future worlds $W' \sqsupseteq_{\text{pub}} W$ are similar, but must have taken public transitions

from the island states in W.

$$(k', \Psi_1', \Psi_2', \Theta') \sqsupseteq (k, \Psi_1, \Psi_2, \Theta) \stackrel{\text{def}}{=} k' \le k \ \wedge\ \Psi_1' \supseteq \Psi_1 \ \wedge\ \Psi_2' \supseteq \Psi_2 \ \wedge\ \Theta' \sqsupseteq \lfloor \Theta \rfloor_{k'} \ \wedge\ (k, \Psi_1, \Psi_2, \Theta) \in \text{World} \ \wedge\ (k', \Psi_1', \Psi_2', \Theta') \in \text{World}$$

$$(\theta_1', \ldots, \theta_{m'}') \sqsupseteq (\theta_1, \ldots, \theta_m) \stackrel{\text{def}}{=} m' \ge m \ \wedge\ \forall j \in \{1, \ldots, m\}.\ \theta_j' \sqsupseteq \theta_j$$

$$(s', S', \delta', \pi', \text{MR}', \text{bij}') \sqsupseteq (s, S, \delta, \pi, \text{MR}, \text{bij}) \stackrel{\text{def}}{=} (S', \delta', \pi', \text{MR}', \text{bij}') = (S, \delta, \pi, \text{MR}, \text{bij}) \ \wedge\ (s, s') \in \delta$$

$$W' \sqsupset W \stackrel{\text{def}}{=} W'.k < W.k \ \wedge\ W' \sqsupseteq W$$

$$(k', \Psi_1', \Psi_2', \Theta') \sqsupseteq_{\text{pub}} (k, \Psi_1, \Psi_2, \Theta) \stackrel{\text{def}}{=} k' \le k \ \wedge\ \Psi_1' \supseteq \Psi_1 \ \wedge\ \Psi_2' \supseteq \Psi_2 \ \wedge\ \Theta' \sqsupseteq_{\text{pub}} \lfloor \Theta \rfloor_{k'} \ \wedge\ (k, \Psi_1, \Psi_2, \Theta) \in \text{World} \ \wedge\ (k', \Psi_1', \Psi_2', \Theta') \in \text{World}$$

$$(\theta_1', \ldots, \theta_{m'}') \sqsupseteq_{\text{pub}} (\theta_1, \ldots, \theta_m) \stackrel{\text{def}}{=} m' \ge m \ \wedge\ \forall j \in \{1, \ldots, m\}.\ \theta_j' \sqsupseteq_{\text{pub}} \theta_j$$

$$(s', S', \delta', \pi', \text{MR}', \text{bij}') \sqsupseteq_{\text{pub}} (s, S, \delta, \pi, \text{MR}, \text{bij}) \stackrel{\text{def}}{=} (S', \delta', \pi', \text{MR}', \text{bij}') = (S, \delta, \pi, \text{MR}, \text{bij}) \ \wedge\ (s, s') \in \pi$$

Given a world W, we often need to talk about future worlds of W where the only change is that new immutable memory has been allocated. We use this notation to capture this:

$$W \boxplus (\mathbf{H_1}, \mathbf{H_2}) \stackrel{\text{def}}{=} (W.k, W.\Psi_1 \uplus \Psi_1, W.\Psi_2 \uplus \Psi_2, W.\Theta[i_{\text{box}} \mapsto \text{island}_{\text{box}}(W(i_{\text{box}}).s \uplus (\mathbf{H_1}, \mathbf{H_2}),\ W.k)])$$
$$\text{if } W.\Psi_1 \vdash \mathbf{H_1} : \Psi_1 \ \wedge\ W.\Psi_2 \vdash \mathbf{H_2} : \Psi_2 \ \wedge\ \text{boxheap}(\Psi_1) \ \wedge\ \text{boxheap}(\Psi_2).$$

The following are convenient shorthands for frequently-used pieces of a world:

$$\text{currentMR}(\theta) \stackrel{\text{def}}{=} \theta.\text{MR}(\theta.s) \qquad W(i) \stackrel{\text{def}}{=} W.\Theta(i)$$

$$W.\mathbf{R_1} \stackrel{\text{def}}{=} W.\Theta(i_{\text{reg}}).s.\mathbf{R_1} \quad W.\mathbf{S_1} \stackrel{\text{def}}{=} W.\Theta(i_{\text{stk}}).s.\mathbf{S_1} \quad W.\chi_1 \stackrel{\text{def}}{=} W.\Theta(i_{\text{reg}}).s.\chi_1 \quad W.\sigma_1 \stackrel{\text{def}}{=} W.\Theta(i_{\text{stk}}).s.\sigma_1$$
$$W.\mathbf{R_2} \stackrel{\text{def}}{=} W.\Theta(i_{\text{reg}}).s.\mathbf{R_2} \quad W.\mathbf{S_2} \stackrel{\text{def}}{=} W.\Theta(i_{\text{stk}}).s.\mathbf{S_2} \quad W.\chi_2 \stackrel{\text{def}}{=} W.\Theta(i_{\text{reg}}).s.\chi_2 \quad W.\sigma_2 \stackrel{\text{def}}{=} W.\Theta(i_{\text{stk}}).s.\sigma_2$$

$$W.\Phi_1 \stackrel{\text{def}}{=} (W.\Psi_1, W.\chi_1, W.\sigma_1) \qquad W.\Phi_2 \stackrel{\text{def}}{=} (W.\Psi_2, W.\chi_2, W.\sigma_2)$$

Atoms are well-formed worlds together with a pair of components or values that are well-typed at the indicated type under the appropriate memory type of the world.

$$\text{TermAtom}_n[(\mathbf{q_1} \vdash \tau_1; \sigma_1), (\mathbf{q_2} \vdash \tau_2; \sigma_2)] \stackrel{\text{def}}{=}$$
$$\{ (W, e_1, e_2) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1; \cdot; \cdot; W.\chi_1; W.\sigma_1; \mathbf{q_1} \vdash e_1 : \tau_1; \sigma_1 \ \wedge\ W.\Psi_2; \cdot; \cdot; W.\chi_2; W.\sigma_2; \mathbf{q_2} \vdash e_2 : \tau_2; \sigma_2 \}$$
$$\text{ValAtom}_n[\tau_1, \tau_2] \stackrel{\text{def}}{=} \{ (W, \mathbf{v_1}, \mathbf{v_2}) \in \text{TermAtom}_n[(\mathbf{out} \vdash \tau_1; W.\sigma_1), (\mathbf{out} \vdash \tau_2; W.\sigma_2)] \}$$
$$\text{WvalAtom}_n[\tau_1, \tau_2] \stackrel{\text{def}}{=} \{ (W, \mathbf{w_1}, \mathbf{w_2}) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1; \cdot; \cdot \vdash \mathbf{w_1} : \tau_1 \ \wedge\ W.\Psi_2; \cdot; \cdot \vdash \mathbf{w_2} : \tau_2 \}$$
$$\text{StackAtom}_n[\sigma_1, \sigma_2] \stackrel{\text{def}}{=} \{ (W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1 \vdash \mathbf{S_1} : \sigma_1 \ \wedge\ W.\Psi_2 \vdash \mathbf{S_2} : \sigma_2 \}$$
$$\text{HvalAtom}_n[\psi_1, \psi_2] \stackrel{\text{def}}{=} \{ (W, \mathbf{h_1}, \mathbf{h_2}) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1 \vdash \mathbf{h_1} : {}^{\nu}\psi_1 \ \wedge\ W.\Psi_2 \vdash \mathbf{h_2} : {}^{\nu}\psi_2 \}$$
$$\text{ContAtom}[(\mathbf{q_1} \vdash \tau_1; \sigma_1), (\mathbf{q_2} \vdash \tau_2; \sigma_2)] \rightsquigarrow [(\mathbf{q_1'} \vdash \tau_1'; \sigma_1'), (\mathbf{q_2'} \vdash \tau_2'; \sigma_2')] \stackrel{\text{def}}{=}$$
$$\{(W, E_1, E_2) \mid W \in \text{World} \ \wedge$$
$$\vdash E_1 : (W.\Psi_1; \cdot; \cdot; W.\chi_1; W.\sigma_1; \mathbf{q_1} \vdash \tau_1; \sigma_1) \rightsquigarrow (W.\Psi_1; \cdot; \cdot; W.\chi_1; W.\sigma_1; \mathbf{q_1'} \vdash \tau_1'; \sigma_1') \ \wedge$$
$$\vdash E_2 : (W.\Psi_2; \cdot; \cdot; W.\chi_2; W.\sigma_2; \mathbf{q_2} \vdash \tau_2; \sigma_2) \rightsquigarrow (W.\Psi_2; \cdot; \cdot; W.\chi_2; W.\sigma_2; \mathbf{q_2'} \vdash \tau_2'; \sigma_2')\}$$
$$\text{ContAtom}[(\mathbf{q_1} \vdash \tau_1; \sigma_1), (\mathbf{q_2} \vdash \tau_2; \sigma_2)] \stackrel{\text{def}}{=}$$
$$\{(W, E_1, E_2) \mid \exists \mathbf{q_1'}, \mathbf{q_2'}, \tau_1', \tau_2', \sigma_1', \sigma_2'.$$
$$(W, E_1, E_2) \in \text{ContAtom}[(\mathbf{q_1} \vdash \tau_1; \sigma_1), (\mathbf{q_2} \vdash \tau_2; \sigma_2)] \rightsquigarrow [(\mathbf{q_1'} \vdash \tau_1'; \sigma_1'), (\mathbf{q_2'} \vdash \tau_2'; \sigma_2')]\}$$

$$
\begin{aligned}
\mathrm{WvalRel}[\tau_1, \tau_2] &\stackrel{\text{def}}{=} \{\, \varphi_w \subseteq \mathrm{WvalAtom}[\tau_1, \tau_2] \mid \forall (W, \mathbf{w_1}, \mathbf{w_2}) \in \varphi_w.\ \forall W' \sqsupseteq W.\ (W', \mathbf{w_1}, \mathbf{w_2}) \in \varphi_w \} \\
\mathrm{TValRel} &\stackrel{\text{def}}{=} \{\, \mathrm{VR} = (\tau_1, \tau_2, \varphi_w) \mid \varphi_w \in \mathrm{WvalRel}[\tau_1, \tau_2] \,\} \\
\mathrm{StackRel}[\sigma_1, \sigma_2] &\stackrel{\text{def}}{=} \{\, \varphi_S \subseteq \mathrm{StackAtom}[\sigma_1, \sigma_2] \,\} \\
\mathrm{TStackRel} &\stackrel{\text{def}}{=} \{\, \mathrm{SR} = (\sigma_1, \sigma_2, \varphi_S) \mid\ \varphi_S \in \mathrm{StackRel}[\sigma_1, \sigma_2] \,\}
\end{aligned}
$$

The set $\mathcal{D}[\![\Delta]\!]$ ensures that an environment ρ mapping type variables to value relations is well-formed.

$$
\begin{aligned}
\mathcal{D}[\![\cdot]\!] &\stackrel{\text{def}}{=} \{\, \emptyset \,\} \\
\mathcal{D}[\![\Delta, \alpha]\!] &\stackrel{\text{def}}{=} \{\, \rho[\alpha \mapsto \mathrm{VR}] \mid\ \rho \in \mathcal{D}[\![\Delta]\!]\ \wedge\ \mathrm{VR} \in \mathrm{TValRel} \,\} \\
\mathcal{D}[\![\Delta, \zeta]\!] &\stackrel{\text{def}}{=} \{\, \rho[\zeta \mapsto \mathrm{SR}] \mid\ \rho \in \mathcal{D}[\![\Delta]\!]\ \wedge\ \mathrm{SR} \in \mathrm{TStackRel} \,\} \\
\mathcal{D}[\![\Delta, \epsilon]\!] &\stackrel{\text{def}}{=} \{\, \rho[\epsilon \mapsto (\mathbf{q_1}, \mathbf{q_2})] \mid\ \rho \in \mathcal{D}[\![\Delta]\!]\ \wedge\ \mathrm{ftv}(\mathbf{q_1}) = \emptyset\ \wedge\ \mathrm{ftv}(\mathbf{q_2}) = \emptyset \,\}
\end{aligned}
$$

We use ρ_1 and ρ_2 to denote the substitutions formed by mapping variables in $\mathrm{dom}\,\rho$ to the first and second components, respectively, of the tuples they map to.

We also use some shorthands for referring to atoms of a particular type in terms of an environment ρ:

$$
\begin{aligned}
\mathrm{TermAtom}[\mathbf{q} \vdash \tau; \sigma]\rho &\stackrel{\text{def}}{=} \mathrm{TermAtom}[(\rho_1(\mathbf{q}) \vdash \rho_1(\tau); \rho_1(\sigma)), (\rho_2(\mathbf{q}) \vdash \rho_2(\tau); \rho_2(\sigma))] \\
\mathrm{ValAtom}[\tau]\rho &\stackrel{\text{def}}{=} \mathrm{ValAtom}[\rho_1(\tau), \rho_2(\tau)] \\
\mathrm{WvalAtom}[\tau]\rho &\stackrel{\text{def}}{=} \mathrm{WvalAtom}[\rho_1(\tau), \rho_2(\tau)] \\
\mathrm{HvalAtom}[\psi]\rho &\stackrel{\text{def}}{=} \mathrm{HvalAtom}[\rho_1(\psi), \rho_2(\psi)] \\
\mathrm{ContAtom}[\mathbf{q} \vdash \tau; \sigma]\rho \rightsquigarrow [\mathbf{q'} \vdash \tau'; \sigma']\rho' &\stackrel{\text{def}}{=} \mathrm{ContAtom}[(\rho_1(\mathbf{q}) \vdash \rho_1(\tau); \rho_1(\sigma)), (\rho_2(\mathbf{q}) \vdash \rho_2(\tau); \rho_2(\sigma))] \\
&\qquad \rightsquigarrow [(\rho'_1(\mathbf{q'}) \vdash \rho'_1(\tau'); \rho'_1(\sigma')), (\rho'_2(\mathbf{q'}) \vdash \rho'_2(\tau'); \rho'_2(\sigma'))]
\end{aligned}
$$

The following relation says that a memory relation φ_M satisfies the constraints imposed by a memory relation φ'_M in all worlds accessible from W.

$$
\varphi_M \Subset_W \varphi'_M \stackrel{\text{def}}{=} \forall (\widetilde{W}, \mathbf{M_1}, \mathbf{M_2}) \in \varphi_M.\ \widetilde{W} \sqsupseteq W \implies (\widetilde{W}, \mathbf{M_1}, \mathbf{M_2}) \in \varphi'_M
$$

$$
\begin{aligned}
\mathcal{V}[\![\mathbf{unit}]\!]\rho &= \{\, (W, (), ()) \in \mathrm{ValAtom}[\mathbf{unit}]\rho \,\} \\
\mathcal{V}[\![\mathbf{int}]\!]\rho &= \{\, (W, \mathbf{n}, \mathbf{n}) \in \mathrm{ValAtom}[\mathbf{int}]\rho \,\} \\
\mathcal{V}[\![\mu\alpha.\tau]\!]\rho &= \{\, (W, \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{v_1}, \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{v_2}) \in \mathrm{ValAtom}[\mu\alpha.\tau]\rho \mid \\
&\qquad (W, \mathbf{v_1}, \mathbf{v_2}) \in \triangleright \mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho \,\} \\
\mathcal{V}[\![\langle \tau_1, \ldots, \tau_n \rangle]\!]\rho &= \{\, (W, \langle \mathbf{v_{11}}, \ldots, \mathbf{v_{1n}} \rangle, \langle \mathbf{v_{21}}, \ldots, \mathbf{v_{2n}} \rangle) \in \mathrm{ValAtom}[\langle \tau_1, \ldots, \tau_n \rangle]\rho \mid \\
&\qquad \forall \mathbf{j} \in \{\mathbf{1}, \ldots, \mathbf{n}\}.\ (W, \mathbf{v_{1j}}, \mathbf{v_{2j}}) \in \mathcal{V}[\![\tau_j]\!]\rho \,\} \\
\mathcal{V}[\![(\overline{\tau}) \to \tau']\!]\rho &= \{\, (W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[(\overline{\tau}) \to \tau']\rho \mid \\
&\qquad \forall W' \sqsupseteq W.\ \forall \mathrm{SR} \in \mathrm{TStackRel}.\ \forall \overline{\mathbf{v'_1}}, \overline{\mathbf{v'_2}}. \\
&\qquad\quad \text{let } \rho' = \rho[\zeta \mapsto \mathrm{SR}] \text{ in} \\
&\qquad\quad\ \mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\zeta]\!]\rho'\ \wedge\ \overline{(W', \mathbf{v'_1}, \mathbf{v'_2}) \in \mathcal{V}[\![\tau]\!]\rho'} \\
&\qquad\quad \implies (W', \mathbf{v_1}\ \overline{\mathbf{v'_1}}, \mathbf{v_2}\ \overline{\mathbf{v'_2}}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \zeta]\!]\rho' \,\} \\
\mathcal{V}[\![(\overline{\tau}) \xrightarrow{\phi_i; \phi_o} \tau']\!]\rho &= \{\, (W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[(\overline{\tau}) \xrightarrow{\phi_i; \phi_o} \tau']\rho \mid \\
&\qquad \forall W' \sqsupseteq W.\ \forall \mathrm{SR} \in \mathrm{TStackRel}.\ \forall \overline{\mathbf{v'_1}}, \overline{\mathbf{v'_2}}. \\
&\qquad\quad \text{let } \rho' = \rho[\zeta \mapsto \mathrm{SR}] \text{ in} \\
&\qquad\quad\ \mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\phi_i :: \zeta]\!]\rho'\ \wedge\ \overline{(W', \mathbf{v'_1}, \mathbf{v'_2}) \in \mathcal{V}[\![\tau]\!]\rho'} \\
&\qquad\quad \implies (W', \mathbf{v_1}\ \overline{\mathbf{v'_1}}, \mathbf{v_2}\ \overline{\mathbf{v'_2}}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \phi_o :: \zeta]\!]\rho' \,\}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{W}[\![\boldsymbol{\alpha}]\!]\rho &= \rho(\boldsymbol{\alpha}).\varphi_w \\
\mathcal{W}[\![\mathbf{unit}]\!]\rho &= \{\, (W, (), ()) \in \mathrm{WvalAtom}[\mathbf{unit}]\rho \,\} \\
\mathcal{W}[\![\mathbf{int}]\!]\rho &= \{\, (W, \mathbf{n}, \mathbf{n}) \in \mathrm{WvalAtom}[\mathbf{int}]\rho \,\} \\
\mathcal{W}[\![\exists\boldsymbol{\alpha}.\boldsymbol{\tau}]\!]\rho &= \{\, (W, \mathbf{pack}\langle\boldsymbol{\tau_1},\mathbf{w_1}\rangle\ \mathbf{as}\ \rho_1(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}), \mathbf{pack}\langle\boldsymbol{\tau_2},\mathbf{w_2}\rangle\ \mathbf{as}\ \rho_2(\exists\boldsymbol{\alpha}.\boldsymbol{\tau})) \in \mathrm{WvalAtom}[\exists\boldsymbol{\alpha}.\boldsymbol{\tau}]\rho \mid \\
&\qquad \exists\varphi_w \in \mathrm{WvalRel}[\boldsymbol{\tau_1}, \boldsymbol{\tau_2}].\ (W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto (\boldsymbol{\tau_1}, \boldsymbol{\tau_2}, \varphi_w)] \,\} \\
\mathcal{W}[\![\boldsymbol{\mu\alpha}.\boldsymbol{\tau}]\!]\rho &= \{\, (W, \mathbf{fold}_{\rho_1(\boldsymbol{\mu\alpha}.\boldsymbol{\tau})}\ \mathbf{w_1}, \mathbf{fold}_{\rho_2(\boldsymbol{\mu\alpha}.\boldsymbol{\tau})}\ \mathbf{w_2}) \in \mathrm{WvalAtom}[\boldsymbol{\mu\alpha}.\boldsymbol{\tau}]\rho \mid \\
&\qquad (W, \mathbf{w_1}, \mathbf{w_2}) \in \triangleright\mathcal{W}[\![\boldsymbol{\tau}[\boldsymbol{\mu\alpha}.\boldsymbol{\tau}/\boldsymbol{\alpha}]]\!]\rho \,\} \\
\mathcal{W}[\![\mathbf{ref}\ \boldsymbol{\psi}]\!]\rho &= \{\, (W, \boldsymbol{\ell_1}, \boldsymbol{\ell_2}) \in \mathrm{WvalAtom}[\mathbf{ref}\ \boldsymbol{\psi}]\rho \mid \exists i.\ \forall W' \sqsupseteq W. \\
&\qquad (\boldsymbol{\ell_1}, \boldsymbol{\ell_2}) \in W'(i).\mathrm{bij}(W'(i).s) \wedge \\
&\qquad \exists\varphi_M.\ \mathrm{currentMR}(W'(i)) = \varphi_M \otimes \\
&\qquad\qquad \{\, (\widetilde{W}, \{\boldsymbol{\ell_1} \mapsto \mathbf{h_1}\}\restriction, \{\boldsymbol{\ell_2} \mapsto \mathbf{h_2}\}\restriction) \in \mathrm{MemAtom} \mid\ (\widetilde{W}, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\boldsymbol{\psi}]\!])\rho \,\} \,\} \\
\mathcal{W}[\![\mathbf{box}\,\langle\boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n}\rangle]\!]\rho &= \{\, (W, \boldsymbol{\ell_1}, \boldsymbol{\ell_2}) \in \mathrm{WvalAtom}[\mathbf{box}\,\langle\boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n}\rangle]\rho \mid \\
&\qquad \forall(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}})).\ \widetilde{W} \sqsupset W \\
&\qquad\quad \Longrightarrow\ (\widetilde{W}, M_1(\boldsymbol{\ell_1}), M_2(\boldsymbol{\ell_2})) \in \mathcal{HV}[\![\langle\boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n}\rangle]\!]\rho \,\} \\
\mathcal{W}[\![\mathbf{box}\,\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^{\mathbf{q}}]\!]\rho &= \{(W, \boldsymbol{\ell_1}[\overline{\boldsymbol{\omega_1}}], \boldsymbol{\ell_2}[\overline{\boldsymbol{\omega_2}}]) \in \mathrm{WvalAtom}[\mathbf{box}\,\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^{\mathbf{q}}]\rho \mid \\
&\qquad \forall(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}})).\ \widetilde{W} \sqsupset W \\
&\qquad\quad \Longrightarrow\ (\, M_1(\boldsymbol{\ell_1}) = \mathbf{code}[\overline{\boldsymbol{\beta_1}}, \boldsymbol{\Delta}]\{\boldsymbol{\chi_1};\boldsymbol{\sigma_1}\}^{\mathbf{q_1}}.\mathbf{I_1} \wedge \\
&\qquad\qquad \rho_1(\boldsymbol{\chi}) = \boldsymbol{\chi_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}]\ \wedge\ \rho_1(\boldsymbol{\sigma}) = \boldsymbol{\sigma_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}]\ \wedge\ \rho_1(\mathbf{q}) = \mathbf{q_1}[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}] \wedge \\
&\qquad\qquad M_2(\boldsymbol{\ell_2}) = \mathbf{code}[\overline{\boldsymbol{\beta_2}}, \boldsymbol{\Delta}]\{\boldsymbol{\chi_2};\boldsymbol{\sigma_2}\}^{\mathbf{q_2}}.\mathbf{I_2} \wedge \\
&\qquad\qquad \rho_2(\boldsymbol{\chi}) = \boldsymbol{\chi_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}]\ \wedge\ \rho_2(\boldsymbol{\sigma}) = \boldsymbol{\sigma_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}]\ \wedge\ \rho_2(\mathbf{q}) = \mathbf{q_2}[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}] \wedge \\
&\qquad\qquad (\widetilde{W}, (\mathbf{code}[\boldsymbol{\Delta}]\{\boldsymbol{\chi_1};\boldsymbol{\sigma_1}\}^{\mathbf{q_1}}.\mathbf{I_1})[\overline{\boldsymbol{\omega_1}/\boldsymbol{\beta_1}}], \\
&\qquad\qquad\quad (\mathbf{code}[\boldsymbol{\Delta}]\{\boldsymbol{\chi_2};\boldsymbol{\sigma_2}\}^{\mathbf{q_2}}.\mathbf{I_2})[\overline{\boldsymbol{\omega_2}/\boldsymbol{\beta_2}}]) \in \mathcal{HV}[\![\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^{\mathbf{q}}]\!]\rho\,) \,\}
\end{aligned}
$$

$$
\begin{aligned}
&\mathcal{HV}[\![\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^{\mathbf{q}}]\!]\rho = \\
&\quad \{(W, \mathbf{code}[\boldsymbol{\Delta}]\{\rho_1(\boldsymbol{\chi});\rho_1(\boldsymbol{\sigma})\}^{\rho_1(\mathbf{q})}.\mathbf{I_1}, \mathbf{code}[\boldsymbol{\Delta}]\{\rho_2(\boldsymbol{\chi});\rho_2(\boldsymbol{\sigma})\}^{\rho_2(\mathbf{q})}.\mathbf{I_2}) \in \mathrm{HvalAtom}[\forall[\boldsymbol{\Delta}].\{\boldsymbol{\chi};\boldsymbol{\sigma}\}^{\mathbf{q}}]\rho \mid \\
&\quad\ \forall W' \sqsupseteq W.\ \forall\rho^* \in \mathcal{D}[\![\boldsymbol{\Delta}]\!].\ \forall\boldsymbol{\tau}, \boldsymbol{\sigma'}.\ \ \mathrm{let}\ \rho' = \rho \cup \rho^*\ \mathrm{in}\ \boldsymbol{\tau};\boldsymbol{\sigma'} =_{\rho'} \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma})\ \wedge \\
&\qquad \mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho'\ \wedge\ \mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho' \\
&\qquad \Longrightarrow\ (W', (\rho_1^*(\mathbf{I_1}), \cdot), (\rho_2^*(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathbf{q} \vdash \boldsymbol{\tau};\boldsymbol{\sigma'}]\!]\rho' \,\}
\end{aligned}
$$

$$
\begin{aligned}
\boldsymbol{\tau};\boldsymbol{\sigma'} =_{\rho} \text{ret-type}(\mathbf{q}, \boldsymbol{\chi}, \boldsymbol{\sigma}) \ \stackrel{\text{def}}{=}\ & \rho_1(\boldsymbol{\tau});\rho_1(\boldsymbol{\sigma'}) = \text{ret-type}(\rho_1(\mathbf{q}), \rho_1(\boldsymbol{\chi}), \rho_1(\boldsymbol{\sigma}))\ \wedge \\
& \rho_2(\boldsymbol{\tau});\rho_2(\boldsymbol{\sigma'}) = \text{ret-type}(\rho_2(\mathbf{q}), \rho_2(\boldsymbol{\chi}), \rho_2(\boldsymbol{\sigma}))
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{HV}[\![\langle\boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n}\rangle]\!]\rho = \{\, & (W, \langle\mathbf{w_{11}}, \ldots, \mathbf{w_{1n}}\rangle, \langle\mathbf{w_{21}}, \ldots, \mathbf{w_{2n}}\rangle) \in \mathrm{HvalAtom}[\langle\boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n}\rangle]\rho \mid \\
& \forall\mathbf{j} \in \{\mathbf{1}, \ldots, \mathbf{n}\}.\ (W, \mathbf{w_{1j}}, \mathbf{w_{2j}}) \in \mathcal{W}[\![\boldsymbol{\tau_j}]\!]\rho \,\}
\end{aligned}
$$

$$(\mathbf{M_1}, \mathbf{M_2}) : W \quad \stackrel{\text{def}}{=} \vdash \mathbf{M_1} : W.\Phi_1 \ \wedge \ \vdash \mathbf{M_2} : W.\Phi_2 \ \wedge$$
$$(W.k > 0 \implies (\triangleright W, \mathbf{M_1}, \mathbf{M_2}) \in \bigotimes \{ \, \mathrm{currentMR}(\theta) \mid \ \theta \in W.\Theta \, \})$$
$$\mathrm{running}(k, \langle \mathbf{M} \mid e \rangle) \quad \stackrel{\text{def}}{=} \exists \mathbf{M'}, e'. \ \langle \mathbf{M} \mid e \rangle \longmapsto^k \langle \mathbf{M'} \mid e' \rangle$$
$$\mathcal{O} = \{ \, (W, e_1, e_2) \mid \ \forall (\mathbf{M_1}, \mathbf{M_2}) : W. \ (\langle \mathbf{M_1} \mid e_1 \rangle \downarrow \ \wedge \ \langle \mathbf{M_2} \mid e_2 \rangle \downarrow) \vee$$
$$(\mathrm{running}(W.k, \langle \mathbf{M_1} \mid e_1 \rangle) \ \wedge \ \mathrm{running}(W.k, \langle \mathbf{M_2} \mid e_2 \rangle)) \, \}$$

NOTE: Our continuations are untyped. See the operational semantics (3.1.7) for more detail.

$$\begin{aligned}
\mathcal{K}[\![\mathbf{out} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho \quad &= \{\, (W, E_1, E_2) \mid \forall W', \mathbf{v_1}, \mathbf{v_2}. \\
&\quad W' \sqsupseteq_{\text{pub}} W \;\wedge\; (W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho \;\wedge\; \text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho \\
&\quad \implies (W', E_1[\mathbf{v_1}], E_2[\mathbf{v_1}]) \in \mathcal{O} \,\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{K}[\![\mathbf{q} \vdash \boldsymbol{\tau}; \boldsymbol{\sigma}]\!]\rho \quad &= \{\, (W, E_1, E_2) \mid \forall W', \mathbf{q'}, \mathbf{r_1}, \mathbf{r_2}. \\
&\quad W' \sqsupseteq_{\text{pub}} W \;\wedge\; (\mathbf{q} =_\rho \mathbf{q'} =_\rho \mathbf{end}\{\boldsymbol{\tau}; \boldsymbol{\sigma}\} \vee \\
&\quad (\exists \mathbf{r}. \mathbf{q'} = \mathbf{r} \;\wedge\; \text{ret-addr}_1(W, \rho_1(\mathbf{q})) = W'.\mathbf{R_1}(\mathbf{r}) \;\wedge\; \text{ret-addr}_2(W, \rho_2(\mathbf{q})) = W'.\mathbf{R_2}(\mathbf{r}) \;\wedge \\
&\qquad\qquad \text{ret-reg}_1(W', \mathbf{r}) = \mathbf{r_1} \;\wedge\; \text{ret-reg}_2(W', \mathbf{r}) = \mathbf{r_2}) \wedge \\
&\quad (\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho \;\wedge\; \text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho \\
&\quad \implies (W', E_1[(\mathtt{ret}\ \rho_1(\mathbf{q'})\ \{\mathbf{r_1}\}, \cdot)], E_2[(\mathtt{ret}\ \rho_2(\mathbf{q'})\ \{\mathbf{r_2}\}, \cdot)]) \in \mathcal{O} \,\}
\end{aligned}$$

$$\mathbf{q} =_\rho \mathbf{q'} \quad \stackrel{\text{def}}{=} \quad \rho_1(\mathbf{q}) = \rho_1(\mathbf{q'}) \;\wedge\; \rho_2(\mathbf{q}) = \rho_2(\mathbf{q'})$$

$$\begin{aligned}
&\text{ret-addr}_1(W, \mathbf{r}) = W.\mathbf{R_1}(\mathbf{r}) \qquad \text{ret-addr}_1(W, \mathbf{i}) = W.\mathbf{S_1}(\mathbf{i}) \\
&\text{ret-addr}_2(W, \mathbf{r}) = W.\mathbf{R_2}(\mathbf{r}) \qquad \text{ret-addr}_2(W, \mathbf{i}) = W.\mathbf{S_2}(\mathbf{i})
\end{aligned}$$

$$\begin{aligned}
&\text{ret-reg}_1(W, \mathbf{r}) = \mathbf{r'} \qquad \text{if } W.\chi_1(\mathbf{r}) = \mathbf{box}\,\forall[].\{\mathbf{r'} : \boldsymbol{\tau}; \boldsymbol{\sigma'}\}^{\mathbf{q}} \\
&\text{ret-reg}_2(W, \mathbf{r}) = \mathbf{r'} \qquad \text{if } W.\chi_2(\mathbf{r}) = \mathbf{box}\,\forall[].\{\mathbf{r'} : \boldsymbol{\tau}; \boldsymbol{\sigma'}\}^{\mathbf{q}}
\end{aligned}$$

$$\begin{aligned}
\mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho \quad &= \{\, (W, e_1, e_2) \in \text{TermAtom}[\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\rho \mid \\
&\quad \forall E_1, E_2.\ (W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho \implies (W, E_1[e_1], E_2[e_2]) \in \mathcal{O} \,\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{G}[\![\cdot]\!]\rho \quad &\stackrel{\text{def}}{=} \{\, (W, \emptyset) \mid W \in \text{World} \,\} \\
\mathcal{G}[\![\boldsymbol{\Gamma}, \mathbf{x} : \boldsymbol{\tau}]\!]\rho \quad &\stackrel{\text{def}}{=} \{\, (W, \gamma[\mathbf{x} \mapsto (\mathbf{v_1}, \mathbf{v_2})] \mid\ (W, \gamma) \in \mathcal{G}[\![\boldsymbol{\Gamma}]\!]\rho \;\wedge\; (W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho \,\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{H}[\![\{\cdot\}]\!] \quad &= \text{World} \\
\mathcal{H}[\![\boldsymbol{\Psi}, \boldsymbol{\ell} : {}^{\text{ref}}\psi]\!] \quad &= \mathcal{H}[\![\boldsymbol{\Psi}]\!] \cap \{\, W \in \text{World} \mid\ (W, \boldsymbol{\ell}, \boldsymbol{\ell}) \in \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\emptyset \,\} \\
\mathcal{H}[\![\boldsymbol{\Psi}, \boldsymbol{\ell} : {}^{\text{box}}\psi]\!] \quad &= \mathcal{H}[\![\boldsymbol{\Psi}]\!] \cap \{\, W \in \text{World} \mid\ (W, \boldsymbol{\ell}, \boldsymbol{\ell}) \in \mathcal{W}[\![\mathbf{box}\ \psi]\!]\emptyset \,\}
\end{aligned}$$

$$\mathcal{R}[\![\chi]\!]\rho \quad = \{\, (W, \mathbf{R_1}\!\uparrow, \mathbf{R_2}\!\uparrow) \mid\ \forall(\mathbf{r} : \boldsymbol{\tau}) \in \chi.\ (W, \mathbf{R_1}(\mathbf{r}), \mathbf{R_2}(\mathbf{r})) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho \,\}$$

$$\begin{aligned}
\mathcal{S}[\![\zeta]\!]\rho \quad &= \rho(\zeta).\varphi_S \\
\mathcal{S}[\![\bullet]\!]\rho \quad &= \{\, (W, \mathbf{nil}\!\uparrow, \mathbf{nil}\!\uparrow) \mid\ W \in \text{World} \,\} \\
\mathcal{S}[\![\boldsymbol{\tau} :: \boldsymbol{\sigma}]\!]\rho \quad &= \{\, (W, (\mathbf{w_1} :: \mathbf{S_1})\!\uparrow, (\mathbf{w_2} :: \mathbf{S_2})\!\uparrow) \mid (W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho \;\wedge\; (W, \mathbf{S_1}\!\uparrow, \mathbf{S_2}\!\uparrow) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho \,\}
\end{aligned}$$

$$\begin{aligned}\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q}\vdash e_1\approx e_2:\tau;\sigma' \stackrel{\text{def}}{=}\ & \Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q}\vdash e_1:\tau;\sigma' \ \wedge\ \Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q}\vdash e_2:\tau;\sigma' \ \wedge\\ & \forall W,\gamma,\rho.\ W\in\mathcal{H}[\![\Psi]\!]\ \wedge\ \rho\in\mathcal{D}[\![\Delta]\!]\ \wedge(W,\gamma)\in\mathcal{G}[\![\Gamma]\!]\rho\ \wedge\\ & \qquad \text{currentMR}(W(i_{\text{reg}}))\Subset_W \mathcal{R}[\![\chi]\!]\rho\ \wedge\\ & \qquad \text{currentMR}(W(i_{\text{stk}}))\Subset_W \mathcal{S}[\![\sigma]\!]\rho\\ & \qquad \implies (W,\rho_1(\gamma_1(e_1)),\rho_2(\gamma_2((e_2)))\in\mathcal{E}[\![\mathbf{q}\vdash\tau;\sigma']\!]\rho\end{aligned}$$

3.3.1 Other Logical Equivalences

To simplify the structure of the Lemmas in subsequent chapters, we define the following notions of logical equivalence for heaps, values, and instruction sequences:

Definition 3.1 (Logical Equivalence for Heaps)

$$\Psi\vdash \mathbf{H_1}\approx_{\text{H}}\mathbf{H_2}:\Psi' \stackrel{\text{def}}{=} \Psi\vdash\mathbf{H_1}:\Psi'\ \wedge\ \Psi\vdash\mathbf{H_2}:\Psi'\ \wedge\ \forall(\ell:^{\nu}\psi)\in\Psi'.\ \Psi,\Psi'\vdash\mathbf{H_1}(\ell)\approx_{\text{hv}}\mathbf{H_2}(\ell):^{\nu}\psi$$

$$\Psi\vdash \mathbf{h_1}\approx_{\text{hv}}\mathbf{h_2}:^{\nu}\psi \stackrel{\text{def}}{=} \Psi\vdash\mathbf{h_1}:^{\nu}\psi\ \wedge\ \Psi\vdash\mathbf{h_2}:^{\nu}\psi\ \wedge\ \forall W\in\mathcal{H}[\![\Psi]\!].\ (W,\mathbf{h_1},\mathbf{h_2})\in\mathcal{HV}[\![\psi]\!]\emptyset$$

Definition 3.2 (Logical Equivalence for Small Values)

$$\begin{aligned}\Psi;\Delta\vdash\mathbf{w_1}\approx_{\text{w}}\mathbf{w_2}:\tau \stackrel{\text{def}}{=}\ & \Psi;\Delta\vdash\mathbf{w_1}:\tau\ \wedge\ \Psi;\Delta\vdash\mathbf{w_2}:\tau\ \wedge\\ & \forall W\in\mathcal{H}[\![\Psi]\!].\ \forall\rho\in\mathcal{D}[\![\Delta]\!].\ (W,\rho_1(\mathbf{w_1}),\rho_2(\mathbf{w_2}))\in\mathcal{W}[\![\tau]\!]\rho\end{aligned}$$

$$\begin{aligned}\Psi;\Delta;\chi\vdash\mathbf{u_1}\approx_{\text{u}}\mathbf{u_2}:\tau \stackrel{\text{def}}{=}\ & \Psi;\Delta;\chi\vdash\mathbf{u_1}:\tau\ \wedge\ \Psi;\Delta;\chi\vdash\mathbf{u_1}:\tau\ \wedge\\ & \forall W\in\mathcal{H}[\![\Psi]\!].\ \forall\rho\in\mathcal{D}[\![\Delta]\!].\ \text{currentMR}(W(i_{\text{reg}}))\Subset_W\mathcal{R}[\![\chi]\!]\rho\\ & \qquad\implies (W,W.\hat{\mathbf{R}}_1(\rho_1(\mathbf{u_1})),W.\hat{\mathbf{R}}_2(\rho_2(\mathbf{u_2})))\in\mathcal{W}[\![\tau]\!]\rho\end{aligned}$$

Definition 3.3 (Logical Equivalence for Instruction Sequences)

$$\begin{aligned}\Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q}\vdash\mathbf{I_1}\approx_{\text{I}}\mathbf{I_2} \stackrel{\text{def}}{=}\ & \Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q}\vdash\mathbf{I_1}\ \wedge\ \Psi;\Delta;\Gamma;\chi;\sigma;\mathbf{q}\vdash\mathbf{I_2}\ \wedge\\ & \forall W\in\mathcal{H}[\![\Psi]\!].\ \forall\rho\in\mathcal{D}[\![\Delta]\!].\ \forall\gamma\in\mathcal{G}[\![\Gamma]\!]\rho.\\ & \quad\text{currentMR}(W(i_{\text{reg}}))\Subset_W\mathcal{R}[\![\chi]\!]\rho\ \wedge\ \text{currentMR}(W(i_{\text{stk}}))\Subset_W\mathcal{S}[\![\sigma]\!]\rho\\ & \quad\implies (W,\rho_1(\gamma_1((\mathbf{I_1},\cdot))),\rho_2(\gamma_2((\mathbf{I_2},\cdot))))\in\mathcal{E}[\![\mathbf{q}\vdash\text{ret-type}(\mathbf{q},\chi,\sigma)]\!]\rho\end{aligned}$$

3.4 Basic Properties

3.4.1 Operations on Worlds

Lemma 3.4 (World Extension is Reflexive and Transitive)
For any $W, W', W'' \in \text{World}$, we have

1. $W \sqsupseteq W$
2. $W \sqsupseteq_{\text{pub}} W$
3. if $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$, then $W'' \sqsupseteq W$
4. if $W'' \sqsupseteq_{\text{pub}} W'$ and $W' \sqsupseteq_{\text{pub}} W$, then $W'' \sqsupseteq_{\text{pub}} W$.

Proof

1. By definition of $\sqsupseteq$ for worlds and islands, and by the reflexivity of transition relations δ in the definition of World.
2. By definition of $\sqsupseteq_{\text{pub}}$ for worlds and islands, and by the reflexivity of public transition relations π in the definition of World.
3. By definition of $\sqsupseteq$ for worlds and islands, and by the transitivity of transition relations δ in the definition of World.
4. By definition of $\sqsupseteq_{\text{pub}}$ for worlds and islands, and by the transitivity of public transition relations π in the definition of World.

□

Lemma 3.5 (Properties of $\boxplus$)

1. If $(M_1, M_2) : W$ and $M_1' = (\mathbf{H_1}, \bot, \bot)$, $M_2' = (\mathbf{H_2}, \bot, \bot)$, then
$$(M_1 \uplus M_1', M_2 \uplus M_2') : W \boxplus (\mathbf{H_1}, \mathbf{H_2}).$$
2. $(W \boxplus (H_1, H_2)) \boxplus (H_1', H_2') = W \boxplus (H_1 \uplus H_1', H_2 \uplus H_2')$.
3. If $W \in \text{World}$ and $(W \boxplus (H_1, H_2))$ is defined, then $(W \boxplus (H_1, H_2)) \sqsupseteq W$ and $(W \boxplus (H_1, H_2)) \sqsupseteq_{\text{pub}} W$.

Proof

1. By definition of $W(i_{\text{box}})$.
2. By definition of $W(i_{\text{box}})$.
3. By definition of $\sqsupseteq$, $\sqsupseteq_{\text{pub}}$, and $\text{island}_{\text{box}}$.

□

Lemma 3.6 (Properties of $\triangleright$ and $\sqsupset$)
For any $W \in \text{World}$, we have

1. $\triangleright W \sqsupseteq W$
2. $\triangleright W \sqsupseteq_{\text{pub}} W$
3. If $(M_1, M_2) : W$, then $(M_1, M_2) : \triangleright W$.
4. If $W' \sqsupset W$, then $W' \sqsupseteq W$.
5. If $W' \sqsupset W$, then $W' \sqsupseteq \triangleright W$.

Proof

1. By definition of $\triangleright$ and $\sqsupseteq$, it suffices to show that $\lfloor \theta \rfloor_{W.k-1} \sqsupseteq \lfloor \theta \rfloor_{W.k-1}$ for each island $\theta \in W.\Theta$. But this relation is reflexive, so we are done.

2. Similar.
3. Note that if $W.k = 0$, there is nothing to show. Otherwise, the claim follows from the definitions of MemRel and $\lfloor \varphi_M \rfloor_k$.
4. Immediate from the definition of $\sqsupset$.
5. From the definition of $\sqsupset$ we have $W'.k < W.k$ and $W' \sqsupseteq W$. The latter implies that $W' \in \text{World}$, which gives us $0 \leq W'.k$. Hence, $0 < W.k$.
   Let $W = (k+1, \Psi_1, \Psi_2, \Theta)$. We have that:
   $$(W'.k, W'.\Psi_1, W'.\Psi_2, W'.\Theta) \sqsupset (k+1, \Psi_1, \Psi_2, \Theta)$$
   We must show that:
   $$(W'.k, W'.\Psi_1, W'.\Psi_2, W'.\Theta) \sqsupseteq (k, \Psi_1, \Psi_2, \lfloor \Theta \rfloor_k)$$
   It suffices to show the following:
   - $W'.k \leq (\triangleright W).k$: this follows from $W'.k < W.k$ and $(\triangleright W).k = W.k - 1$.
   - $W'.\Psi_i \supseteq \Psi_i$: by (4) we have $W' \sqsupseteq W$, from which this fact is immediate.
   - $W'.\Theta \sqsupseteq \lfloor \lfloor \Theta \rfloor_k \rfloor_{W'.k}$: From above we have that $W'.\Theta' \sqsupseteq \lfloor \Theta \rfloor_{k'}$. Furthermore, since $W'.k \leq (\triangleright W).k = W.k - 1 = k$, we have that $\lfloor \lfloor \Theta \rfloor_k \rfloor_{W'.k} = \lfloor \Theta \rfloor_{W'.k}$ so we are done.

□

3.4.2 Properties of the Observation Relation

Lemma 3.7 ($\mathcal{O}$ Closed under Anti-Reduction)
Given $W' \sqsupseteq W$, if $W.k \leq W'.k + k_1$, $W.k \leq W'.k + k_2$, and

$$\forall (M_1, M_2) : W.\ \exists (M_1', M_2') : W'.\ \langle M_1 \mid e_1 \rangle \longmapsto^{k_1} \langle M_1' \mid e_1' \rangle \ \wedge\ \langle M_2 \mid e_2 \rangle \longmapsto^{k_2} \langle M_2' \mid e_2' \rangle,$$

then

$$(W', e_1', e_2') \in \mathcal{O} \implies (W, e_1, e_2) \in \mathcal{O}.$$

Proof

Let $(M_1, M_2) : W$. Then, by our assumption, $\langle M_1 \mid e_1 \rangle \longmapsto^{k_1} \langle M_1' \mid e_1' \rangle$ and $\langle M_2 \mid e_2 \rangle \longmapsto^{k_2} \langle M_2' \mid e_2' \rangle$ for some $(M_1', M_2') : W'$. Since $(W', e_1', e_2') \in \mathcal{O}$, we have either that $\langle M_1' \mid e_1' \rangle \downarrow$ and $\langle M_2' \mid e_2' \rangle \downarrow$ or that running$(W'.k, \langle M_1' \mid e_1' \rangle)$ and running$(W'.k, \langle M_2' \mid e_2' \rangle)$.

In the former case, we have $\langle M_1 \mid e_1 \rangle \downarrow$ and $\langle M_2 \mid e_2 \rangle \downarrow$ by assumption. In the latter case, we have running$(W'.k + k_1, \langle M_1 \mid e_1 \rangle)$ and running$(W'.k + k_2, \langle M_2 \mid e_2 \rangle)$. Since we have assumptions that both of these are more steps than needed, we have the result. □

3.4.3 Monotonicity and Reduction

Lemma 3.8 (Monotonicity)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, where $\Delta \vdash \boldsymbol{\tau}$, $\Delta \vdash \boldsymbol{\psi}$, and $\Delta \vdash \boldsymbol{\tau}$. If $W' \sqsupseteq W$, then

1. $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho \implies (W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$
2. $(W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho \implies (W', \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\boldsymbol{\tau}]\!]\rho$.
3. $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho \implies (W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho$.

Proof

1. Proved by induction on $W'.k$ and on the structure of $\boldsymbol{\tau}$, simultaneously with Claim 2.
   In each case, we will need to show $(W', \mathbf{w_1}, \mathbf{w_2}) \in \text{WvalAtom}[\boldsymbol{\tau}]\rho$. This amounts to showing that $W'.\Psi_i; \cdot \vdash \mathbf{w_i} : \boldsymbol{\tau}$ for $i \in \{1, 2\}$. We have by assumption that $W.\Psi_i; \cdot \vdash \mathbf{w_i} : \boldsymbol{\tau}$. By definition of world extension, $W'.\Psi_i \supseteq W.\Psi_i$, so this property holds.
   To complete the proof, consider the possible cases of $\boldsymbol{\tau}$:

Case α Follows from $\rho(\alpha).\varphi_v^T \in \mathrm{WvalRel}[\rho(\alpha).\tau_1, \rho(\alpha).\tau_2]$, which holds by $\rho(\alpha) \in \mathrm{TValRel}$.

Case $\mathbf{unit}$ Immediate.

Case $\mathbf{int}$ Immediate.

Case $\exists\alpha.\tau'$ Follows from the induction hypothesis for the type.

Case $\mu\alpha.\tau'$ Follows from the induction hypothesis for the step index.

Case $\mathbf{ref}\ \psi$ We need to show that $(W', \ell_1, \ell_2) \in \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\rho$. Let $W'' \sqsupseteq W'$. By transitivity of world extension, $W'' \sqsupseteq W$. Thus everything we need holds by our assumption that $(W, \ell_1, \ell_2) \in \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\rho$.

Case $\mathbf{box}\,\langle\tau_1, \ldots, \tau_n\rangle$ We need to show that $(W', \ell_1, \ell_2) \in \mathcal{W}[\![\mathbf{box}\,\langle\tau_1, \ldots, \tau_n\rangle]\!]\rho$.
Let $(\widetilde{W}, M_1', M_2') \in \mathrm{currentMR}(W'(i_{\mathrm{box}}))$ such that $\widetilde{W} \sqsupset W'$. By definition of $\mathrm{island}_{\mathrm{box}}$, $M_1' = (W'(i_{\mathrm{box}}).s.H_1)\restriction$ and $M_2' = (W'(i_{\mathrm{box}}).s.H_2)\restriction$. By our assumption, to show

$$(\widetilde{W}, M_1'(\ell_1), M_2'(\ell_2)) \in \mathcal{HV}[\![\langle\tau_1, \ldots, \tau_n\rangle]\!]\rho$$

it suffices to find some M_1 and M_2 such that $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$, $M_1(\ell_1) = M_1'(\ell_1)$, and $M_2(\ell_2) = M_2'(\ell_2)$, noting that $\widetilde{W} \sqsupset W$ follows from $\widetilde{W} \sqsupset W' \sqsupseteq W$.
We claim that $M_1 = (W(i_{\mathrm{box}}).s.H_1)\restriction$ and $M_2 = (W(i_{\mathrm{box}}).s.H_2)\restriction$ are suitable. The first condition holds immediately by definition of $\mathrm{island}_{\mathrm{box}}$. Since $W' \sqsupseteq W$, we know that $W'(i_{\mathrm{box}}) \sqsupseteq \lfloor W(i_{\mathrm{box}})\rfloor_{W'.k}$. Thus $((H_1, H_2), (H_1', H_2')) \in \delta_{\mathrm{box}}$, that is, $H_1 \subseteq H_1'$ and $H_2 \subseteq H_2'$. Since ℓ_1 and ℓ_2 must be in the domain of H_1 and H_2, we have the desired property that $M_1(\ell_1) = M_1'(\ell_1)$ and $M_2(\ell_2) = M_2'(\ell_2)$.

Case $\mathbf{box}\,\forall[\Delta].\{\chi;\sigma\}^{\mathsf{q}}$ Let $(\widetilde{W}, M_1', M_2') \in \mathrm{currentMR}(W'(i_{\mathrm{box}}))$ such that $\widetilde{W} \sqsupset W'$. It suffices to find some M_1 and M_2 such that $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$, $M_1(\ell_1) = M_1'(\ell_1)$, and $M_2(\ell_2) = M_2'(\ell_2)$, noting that $\widetilde{W} \sqsupset W$. This can be done exactly as in the previous case.

2. Proved simultaneously with Claim 1.

   In both cases, we need to show that $(W', \mathbf{h}_1, \mathbf{h}_2) \in \mathrm{HvalAtom}[\psi]\rho$. This amounts to showing that $W'.\Psi_i \vdash \mathbf{h}_i : {}^{\nu}\psi$ for $i \in \{1, 2\}$. We have by assumption that $W.\Psi_i \vdash \mathbf{h}_i : {}^{\nu}\psi$. By definition of world extension, $W'.\Psi_i \supseteq W.\Psi_i$, so this property holds.

   Consider the possible cases of ψ:

   Case $\forall[\Delta].\{\chi;\sigma\}^{\mathsf{q}}$ We need to show that $(W', \mathbf{h}_1, \mathbf{h}_2) \in \mathcal{HV}[\![\forall[\Delta].\{\chi;\sigma\}^{\mathsf{q}}]\!]\rho$. Let $W'' \sqsupseteq W'$. By transitivity of world extension, $W'' \sqsupseteq W$. Thus everything we need holds by our assumption that $(W, \mathbf{h}_1, \mathbf{h}_2) \in \mathcal{HV}[\![\forall[\Delta].\{\chi;\sigma\}^{\mathsf{q}}]\!]\rho$.

   Case $\langle\tau_1, \ldots, \tau_n\rangle$ Follows from Claim 1 using the induction hypothesis for the type.

3. Proved by induction on $W'.k$ and on the structure of τ.

   In each case, we will need to show $(W', \mathbf{v}_1, \mathbf{v}_2) \in \mathrm{ValAtom}[\tau]\rho$. This amounts to showing that $W'.\Psi_i; \cdot; \cdot; W'.\chi_i; W'.\sigma_i; \mathbf{out} \vdash \mathbf{v}_i : \tau; W'.\sigma_i$ for $i \in \{1, 2\}$. We have by assumption that $W.\Psi_i; \cdot; \cdot; W.\chi_i; W.\sigma_i; \mathbf{out} \vdash \mathbf{v}_i : \tau; W.\sigma_i$. By definition of world extension, $W'.\Psi_i \supseteq W.\Psi_i$. However, note that $W'.\chi_i$ and $W'.\sigma_i$ may be arbitrarily different from $W.\chi_i$ and $W.\sigma_i$. But note that the only place where there are non-trivial dependencies of the typing on either of those are past the ${}^{\tau}\mathcal{FT}\,\cdot$ boundaries. Note first that at the boundary, what is inside is restricted to type under the empty register file typing, so any changes to the typing outside the boundary is irrelevant. Note secondly that since we are dealing with values, the only place an ${}^{\tau}\mathcal{FT}\,\cdot$ boundary can occur is within a lambda. The typing rule for lambdas requires that the body types under a fresh ζ variable for the stack typing, both in and out, which means that any changes that are made to the stack typing outside of the lambda are irrelevant.

   To complete the proof, consider the possible cases of τ:

   Case $\mathbf{unit}$ No proof obligations beyond what was shown above.

   Case $\mathbf{int}$ No proof obligations beyond what was shown above.

   Case $\mu\alpha.\tau$ This follows from the induction hypothesis.

Case $\langle \overline{\tau} \rangle$ This follows from the induction hypothesis.

Case $(\overline{\tau}) \to \tau'$ The obligations in this case follow trivially from the transitivity of world extension, since with any future world $W^* \sqsupseteq W'$ we can instantiate what we are given.

Case $(\overline{\tau}) \xrightarrow{\phi_i;\phi_o} \tau'$ This case is the same as the other arrow case.

□

Lemma 3.9 (Monotonicity for Heaps)
If $W' \sqsupseteq W$ and $W \in \mathcal{H}[\![\Psi]\!]$, then $W' \in \mathcal{H}[\![\Psi]\!]$.

Proof

We use induction on the structure of Ψ. If $\Psi = \{\cdot\}$ then there is nothing to show.

If $\Psi = \Psi', \ell : {}^{\mathrm{ref}}\psi$, then by the induction hypothesis, $W' \in \mathcal{H}[\![\Psi']\!]$, and it remains to show that $(W', \ell, \ell) \in \mathcal{W}[\![\mathbf{ref}\ \psi]\!]\emptyset$. But this follows from $W \in \mathcal{H}[\![\Psi', \ell : {}^{\mathrm{ref}}\psi]\!]$ and Lemma 3.8.

If $\Psi = \Psi', \ell : {}^{\mathrm{box}}\psi$, then by the induction hypothesis, $W' \in \mathcal{H}[\![\Psi']\!]$, and it remains to show that $(W', \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\ \psi]\!]\emptyset$. But this follows from $W \in \mathcal{H}[\![\Psi', \ell : {}^{\mathrm{box}}\psi]\!]$ and Lemma 3.8. □

Lemma 3.10 (Monotonicity for F Evaluation Contexts)
If $W' \sqsupseteq_{\mathrm{pub}} W$, then

$$(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{out} \vdash \tau; \sigma]\!]\rho \implies (W', E_1, E_2) \in \mathcal{K}[\![\mathbf{out} \vdash \tau; \sigma]\!]\rho.$$

Proof

Follows from the transitivity of $\sqsupseteq_{\mathrm{pub}}$. □

Lemma 3.11 (Monotonicity for T Evaluation Contexts)
If $W' \sqsupseteq_{\mathrm{pub}} W$ and if either $\mathbf{q} =_\rho \mathbf{q}' =_\rho \mathbf{end}\{\tau; \sigma\}$ or $\text{ret-addr}_1(W, \rho_1(\mathbf{q})) = \text{ret-addr}_1(W', \rho_1(\mathbf{q}'))$ and $\text{ret-addr}_2(W, \rho_2(\mathbf{q})) = \text{ret-addr}_2(W', \rho_2(\mathbf{q}'))$, then

$$(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho \implies (W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q}' \vdash \tau; \sigma]\!]\rho.$$

Proof

Follows from the transitivity of $\sqsupseteq_{\mathrm{pub}}$ and our hypotheses about the relationship between $\mathbf{q}$ and $\mathbf{q}'$. □

Lemma 3.12 ($\mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho$ Closed under Type-Preserving Anti-Reduction)
Let $(W, e_1, e_2) \in \text{TermAtom}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho$. Given $W' \sqsupseteq_{\mathrm{pub}} W$, $W.k \leq W'.k + k_1$, $W.k \leq W'.k + k_2$, and if $\mathbf{q} =_\rho \mathbf{q}' =_\rho \mathbf{end}\{\tau; \sigma\}$ or $\mathbf{q} =_\rho \mathbf{q}' =_\rho \mathbf{out}$ or if $\text{ret-addr}_1(W, \rho_1(\mathbf{q})) = \text{ret-addr}_1(W', \rho_1(\mathbf{q}'))$ and $\text{ret-addr}_2(W, \rho_2(\mathbf{q})) = \text{ret-addr}_2(W', \rho_2(\mathbf{q}'))$, and if

$$\forall (M_1, M_2) : W.\ \exists (M_1', M_2') : W'.\ \langle M_1 \mid e_1 \rangle \longmapsto^{k_1} \langle M_1' \mid e_1' \rangle \ \wedge\ \langle M_2 \mid e_2 \rangle \longmapsto^{k_2} \langle M_2' \mid e_2' \rangle,$$

then

$$(W', e_1', e_2') \in \mathcal{E}[\![\mathbf{q}' \vdash \tau; \sigma]\!]\rho \implies (W, e_1, e_1) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho.$$

Proof

Now let $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho$. We need to show that $(W, E_1[e_1], E_2[e_2]) \in \mathcal{O}$.

We can use Lemma 3.11 and Lemma 3.10 to conclude that $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{q}' \vdash \tau; \sigma]\!]\rho$. Instantiating the latter with $(W', e_1', e_2') \in \mathcal{E}[\![\mathbf{q}' \vdash \tau; \sigma]\!]\rho$ gives us $(W', E_1[e_1'], E_2[e_2']) \in \mathcal{O}$.

By inspection of the operational semantics and by assumption, for any $(M_1, M_2) : W$, there is an $(M_1', M_2') : W'$ such that

$$\langle M_1 \mid E_1[e_1] \rangle \longmapsto^{k_1} \langle M_1' \mid E_1[e_1'] \rangle \quad \text{and} \quad \langle M_2 \mid E_2[e_2] \rangle \longmapsto^{k_2} \langle M_2' \mid E_2[e_2'] \rangle.$$

The rest of this case follows by Lemma 3.7.

□

Lemma 3.13 ($\mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho$ Closed under Memory-Preserving Anti-Reduction)
Let $(W, e_1, e_2) \in \mathrm{TermAtom}[\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\rho$.

If

$$\forall (M_1, M_2) : W.\ \langle M_1 \mid e_1 \rangle \longmapsto^* \langle M_1 \mid e_1' \rangle \ \wedge\ \langle M_2 \mid e_2 \rangle \longmapsto^* \langle M_2 \mid e_2' \rangle,$$

then

$$(W, e_1', e_2') \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho \implies (W, e_1, e_1) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho.$$

Proof

This follows fram Lemma . □

3.4.4 Substitution

The next lemma is a simple property, but its proof shows the induction structure by which properties of the mutually-dependent parts of the logical relation can be proved.

Definition 3.14

$\xi \ ::= \boldsymbol{\alpha} \mid \boldsymbol{\zeta} \mid \boldsymbol{\epsilon}$

$\mathrm{AR} ::= \mathrm{VR} \mid \mathrm{SR} \mid \mathrm{QR}$

Lemma 3.15
[Weakening] If $\rho[\xi \mapsto \mathrm{AR}] \in \mathcal{D}[\![\Delta, \xi]\!]$ and $\xi \notin \mathrm{ftv}(\tau)$, $\xi \notin \mathrm{ftv}(\tau)$ $\xi \notin \mathrm{ftv}(\boldsymbol{\sigma})$, $\xi \notin \mathrm{ftv}(\chi)$, $\xi \notin \mathrm{ftv}(\psi)$, then

1. $\mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho = \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
2. $\mathcal{R}[\![\chi]\!]\rho = \mathcal{R}[\![\chi]\!]\rho[\xi \mapsto \mathrm{AR}]$
3. $\mathcal{W}[\![\tau]\!]\rho = \mathcal{W}[\![\tau]\!]\rho[\xi \mapsto \mathrm{AR}]$
4. $\mathcal{HV}[\![\psi]\!]\rho = \mathcal{HV}[\![\psi]\!]\rho[\xi \mapsto \mathrm{AR}]$
5. $\mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho = \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
6. $\mathcal{K}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho = \mathcal{K}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$.
7. $\mathcal{V}[\![\tau]\!]\rho = \mathcal{V}[\![\tau]\!]\rho[\xi \mapsto \mathrm{AR}]$
8. $\mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho = \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
9. $\mathcal{K}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho = \mathcal{K}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$.

Proof

Assume $\xi \notin \mathrm{ftv}(\tau)$ and $\xi \notin \mathrm{ftv}(\boldsymbol{\sigma})$. We will need to prove the following:

1. (a) $(W, \mathbf{S_1}, \mathbf{S_2}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho \implies (W, \mathbf{S_1}, \mathbf{S_2}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{S_1}, \mathbf{S_2}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{S_1}, \mathbf{S_2}) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$
2. (a) $(W, \mathbf{R_1}, \mathbf{R_2}) \in \mathcal{R}[\![\chi]\!]\rho \implies (W, \mathbf{R_1}, \mathbf{R_2}) \in \mathcal{R}[\![\chi]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{R_1}, \mathbf{R_2}) \in \mathcal{R}[\![\chi]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{R_1}, \mathbf{R_2}) \in \mathcal{R}[\![\chi]\!]\rho$
3. (a) $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho \implies (W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho$
4. (a) $(W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\psi]\!]\rho \implies (W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\psi]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\psi]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\psi]\!]\rho$
5. (a) $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho \implies (W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho$
6. (a) $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho \implies (W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \boldsymbol{\sigma}]\!]\rho[\xi \mapsto \mathrm{AR}]$

(b) $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho$.

7. (a) $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho \implies (W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$
8. (a) $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho \implies (W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho$
9. (a) $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho \implies (W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho[\xi \mapsto \mathrm{AR}]$
   (b) $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho[\xi \mapsto \mathrm{AR}] \implies (W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma]\!]\rho$.

We will prove all these claims simultaneously, by induction on $W.k$ and τ.

1. We use an additional induction and case analysis on the structure of σ.

   Case ζ Immediate, since $\xi \neq \zeta$.

   Case $\bullet$ Immediate.

   Case $\tau :: \sigma$ For part (a), we have $\mathbf{S_1} = \mathbf{w_1} :: \mathbf{S_1'}$, $\mathbf{S_2} = \mathbf{w_2} :: \mathbf{S_2'}$, $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho$, and $(W, \mathbf{S_1'}, \mathbf{S_2'}) \in \mathcal{S}[\![\sigma]\!]\rho$. We need to show that $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho[\xi \mapsto \mathrm{AR}]$ and $(W, \mathbf{S_1'}, \mathbf{S_2'}) \in \mathcal{S}[\![\sigma]\!]\rho[\xi \mapsto \mathrm{AR}]$. The latter holds by the induction hypothesis for σ and the former holds by claim 3.
   Part (b) is similar.

2. Follows from claim 3.

3. Consider the possible cases of τ:

   Case α Immediate, since $\alpha \neq \xi$.

   Case $\mathbf{unit}$ Immediate.

   Case $\mathbf{int}$ Immediate.

   Case $\exists \alpha.\tau$ By the induction hypothesis for τ.

   Case $\mu\alpha.\tau$ By the induction hypothesis for $W.k$.

   Case $\mathbf{ref}\ \langle \tau_1, \ldots, \tau_n \rangle$ Follows from claim 4.

   Case $\mathbf{box}\ \langle \tau_1, \ldots, \tau_n \rangle$ Follows from claim 4.

   Case $\mathbf{box}\ \forall[\Delta].\{\chi; \sigma'\}^{\mathbf{q}'}$ Follows from claim 4.

4. Consider the two possible cases of ψ:

   Case $\forall[\Delta].\{\chi; \sigma'\}^{\mathbf{q}'}$ Follows from claims 1 and 2 (using the induction hypothesis for τ) and from claim 5 (using the induction hypothesis for $W.k$).

   Case $\langle \tau_1, \ldots, \tau_n \rangle$ Follows from claim 3 (using the induction hypothesis for τ).

5. Follows from claim 6.

6. Follows from claims 1 and 3.

7. Consider the possible cases of τ that are defined in $\mathcal{V}[\![\cdot]\!]\rho$:

   Case $()$ Immediate.

   Case $\mathbf{int}$ Immediate.

   Case $\mu\alpha.\tau$ By the induction hypothesis for $W.k$.

   Case $\langle \overline{\tau} \rangle$ By the induction hypothesis for $\overline{\tau}$.

   Case $(\overline{\tau}) \to \tau$ Follows from claim 1 (using induction hypothesis for τ), and from claim 8 (using induction hypothesis for $W.k$.

   Case $(\overline{\tau}) \xrightarrow{\phi_i;\phi_o} \tau$ Same as other arrow case.

8. Follows from claim 9.

9. Follows from claims 1 and 7.

□

Lemma 3.16 (Substitution)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, $\alpha \notin \Delta$, $\Delta \vdash \tau'$, and $\Delta, \alpha \vdash \tau$, $\Delta, \alpha \vdash \sigma$, $\Delta, \alpha \vdash \chi$, $\Delta, \alpha \vdash \psi$. Then

1. $\mathcal{S}[\![\sigma]\!]\rho[\alpha \mapsto (\rho_1(\tau'), \rho_2(\tau'), \mathcal{W}[\![\tau']\!]\rho)] = \mathcal{S}[\![\sigma[\tau'/\alpha]]\!]\rho$
2. $\mathcal{R}[\![\chi]\!]\rho[\alpha \mapsto (\rho_1(\tau'), \rho_2(\tau'), \mathcal{W}[\![\tau']\!]\rho)] = \mathcal{R}[\![\chi[\tau'/\alpha]]\!]\rho$
3. $\mathcal{W}[\![\tau]\!]\rho[\alpha \mapsto (\rho_1(\tau'), \rho_2(\tau'), \mathcal{W}[\![\tau']\!]\rho)] = \mathcal{W}[\![\tau[\tau'/\alpha]]\!]\rho$
4. $\mathcal{HV}[\![\psi]\!]\rho[\alpha \mapsto (\rho_1(\tau'), \rho_2(\tau'), \mathcal{W}[\![\tau']\!]\rho)] = \mathcal{HV}[\![\psi[\tau'/\alpha]]\!]\rho$
5. $\mathcal{E}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\alpha \mapsto (\rho_1(\tau'), \rho_2(\tau'), \mathcal{W}[\![\tau']\!]\rho)] = \mathcal{E}[\![\mathrm{q}[\tau'/\alpha] \vdash \tau[\tau'/\alpha]; \sigma[\tau'/\alpha]]\!]\rho$
6. $\mathcal{K}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\alpha \mapsto (\rho_1(\tau'), \rho_2(\tau'), \mathcal{W}[\![\tau']\!]\rho)] = \mathcal{K}[\![\mathrm{q}[\tau'/\alpha] \vdash \tau[\tau'/\alpha]; \sigma[\tau'/\alpha]]\!]\rho$.

Proof

Follows the structure of the proof of Lemma 3.15, aside from the cases about source types, since they cannot have free type variables. The only case that depends on ρ is in claim 3, in the case where $\tau = \beta$. But the needed equality is immediate in this case, whether $\alpha = \beta$ or not. □

Lemma 3.17 (Substitution for Stack Types)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, $\zeta \notin \Delta$, $\Delta \vdash \sigma'$, and $\Delta, \zeta \vdash \tau$, $\Delta, \zeta \vdash \sigma$, $\Delta, \zeta \vdash \chi$, $\Delta, \zeta \vdash \psi$. Then

1. $\mathcal{S}[\![\sigma]\!]\rho[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{S}[\![\sigma[\sigma'/\zeta]]\!]\rho$
2. $\mathcal{R}[\![\chi]\!]\rho[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{R}[\![\chi[\sigma'/\zeta]]\!]\rho$
3. $\mathcal{W}[\![\tau]\!]\rho[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{W}[\![\tau[\sigma'/\zeta]]\!]\rho$
4. $\mathcal{HV}[\![\psi]\!]\rho[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{HV}[\![\psi[\sigma'/\zeta]]\!]\rho$
5. $\mathcal{E}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{E}[\![\mathrm{q}[\sigma'/\zeta] \vdash \tau[\sigma'/\zeta]; \sigma[\sigma'/\zeta]]\!]\rho$
6. $\mathcal{K}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)] = \mathcal{K}[\![\mathrm{q}[\sigma'/\zeta] \vdash \tau[\sigma'/\zeta]; \sigma[\sigma'/\zeta]]\!]\rho$.
7. $\mathcal{E}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho = \mathcal{E}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)]$
8. $\mathcal{K}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho = \mathcal{K}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\zeta \mapsto (\rho_1(\sigma'), \rho_2(\sigma'), \mathcal{S}[\![\sigma']\!]\rho)]$.

Proof

Follows the structure of the proof of Lemma 3.15. The only case that depends on $\rho(\zeta)$ is in claim 1, in the case where $\sigma = \zeta'$. But the needed equality is immediate, whether $\zeta = \zeta'$ or not. □

Lemma 3.18 (Substitution for Return Markers)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, $\Delta \vdash \mathrm{q}'$, and $\Delta, \epsilon \vdash \tau$, $\Delta, \epsilon \vdash \sigma$, $\Delta, \epsilon \vdash \chi$, $\Delta, \epsilon \vdash \psi$. Then

1. $\mathcal{S}[\![\sigma]\!]\rho[\epsilon \mapsto (\rho_1(\mathrm{q}'), \rho_2(\mathrm{q}'))] = \mathcal{S}[\![\sigma[\mathrm{q}'/\epsilon]]\!]\rho$
2. $\mathcal{R}[\![\chi]\!]\rho[\epsilon \mapsto (\rho_1(\mathrm{q}'), \rho_2(\mathrm{q}'))] = \mathcal{R}[\![\chi[\mathrm{q}'/\epsilon]]\!]\rho$
3. $\mathcal{W}[\![\tau]\!]\rho[\epsilon \mapsto (\rho_1(\mathrm{q}'), \rho_2(\mathrm{q}'))] = \mathcal{W}[\![\tau[\mathrm{q}'/\epsilon]]\!]\rho$
4. $\mathcal{HV}[\![\psi]\!]\rho[\epsilon \mapsto (\rho_1(\mathrm{q}'), \rho_2(\mathrm{q}'))] = \mathcal{HV}[\![\psi[\mathrm{q}'/\epsilon]]\!]\rho$
5. $\mathcal{E}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\epsilon \mapsto (\rho_1(\mathrm{q}'), \rho_2(\mathrm{q}'))] = \mathcal{E}[\![\mathrm{q}[\mathrm{q}'/\epsilon] \vdash \tau[\mathrm{q}'/\epsilon]; \sigma[\mathrm{q}'/\epsilon]]\!]\rho$
6. $\mathcal{K}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\epsilon \mapsto (\rho_1(\mathrm{q}'), \rho_2(\mathrm{q}'))] = \mathcal{K}[\![\mathrm{q}[\mathrm{q}'/\epsilon] \vdash \tau[\mathrm{q}'/\epsilon]; \sigma[\mathrm{q}'/\epsilon]]\!]\rho$.
7. $\mathcal{E}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\epsilon \mapsto (\rho_1(\mathrm{q}'), \rho_2(\mathrm{q}'))] = \mathcal{E}[\![\mathrm{q}[\mathrm{q}'/\epsilon] \vdash \tau; \sigma[\mathrm{q}'/\epsilon]]\!]\rho$
8. $\mathcal{K}[\![\mathrm{q} \vdash \tau; \sigma]\!]\rho[\epsilon \mapsto (\rho_1(\mathrm{q}'), \rho_2(\mathrm{q}'))] = \mathcal{K}[\![\mathrm{q}[\mathrm{q}'/\epsilon] \vdash \tau; \sigma[\mathrm{q}'/\epsilon]]\!]\rho$.

Proof

Followed the structure of the proof of Lemma 3.15. There are no interesting cases. □

3.4.5 Properties of Semantic Interpretations

Lemma 3.19
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \tau$, then $\mathcal{W}[\![\tau]\!]\rho \in \mathrm{WvalRel}[\rho_1(\tau), \rho_2(\tau)]$.

Proof

Follows from monotonicity. □

Lemma 3.20
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \sigma$, then $\mathcal{S}[\![\sigma]\!]\rho \in \mathrm{StackRel}[\rho_1(\sigma), \rho_2(\sigma)]$.

Proof

Proceed by induction on the structure of σ.

Case ζ From $\Delta \vdash \sigma$ we have that $\zeta \in \Delta$. Since $\rho \in \mathcal{D}[\![\Delta]\!]$, it follows that $\mathcal{S}[\![\zeta]\!]\rho = \rho(\zeta).\varphi_S \in \mathrm{StackRel}[\rho_1(\zeta), \rho_2(\zeta)]$.

Case $\bullet$ In this case, $\mathcal{S}[\![\bullet]\!]\rho = \{\, (W, \mathbf{nil}\uparrow, \mathbf{nil}\uparrow) \mid W \in \mathrm{World} \,\} \in \mathrm{StackRel}[\bullet, \bullet]$ is immediate from the definition of StackRel.

Case $\tau :: \sigma$ For any $(W, \mathbf{w_1} :: \mathbf{S_1}\uparrow, \mathbf{w_2} :: \mathbf{S_2}\uparrow) \in \mathcal{S}[\![\tau :: \sigma]\!]\rho$, we need that $W.\Psi_i \vdash \mathbf{w_i} :: \mathbf{S_i} : \rho_i(\tau :: \sigma)$. From the definition of $\mathcal{S}[\![\tau :: \sigma]\!]\rho$ we have $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho$ and $(W, \mathbf{S_1}\uparrow, \mathbf{S_2}\uparrow) \in \mathcal{S}[\![\sigma]\!]\rho$, from which we have that $W.\Psi_i; \cdot \vdash \mathbf{w_i} : \rho_i(\tau)$ and $W.\Psi_i \vdash \mathbf{S_i} : \rho_i(\sigma)$, which gives us what we need.

□

Lemma 3.21 (Register File Subtyping Implies Inclusion)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \chi \leq \chi'$. Then $\mathcal{R}[\![\chi]\!]\rho \subseteq \mathcal{R}[\![\chi']\!]\rho$.

Proof

Consider arbitrary $(W, M_1, M_2) \in \mathcal{R}[\![\chi]\!]\rho$. Note that $M_1 = \mathbf{R_1}\uparrow$ and $M_2 = \mathbf{R_2}\uparrow$. We must show that $(W, M_1, M_2) = (W, \mathbf{R_1}\uparrow, \mathbf{R_2}\uparrow) \in \mathcal{R}[\![\chi']\!]\rho$.

Consider $(\mathbf{r} : \tau) \in \chi'$. We must show $(W, \mathbf{R_1(r)}, \mathbf{R_2(r)}) \in \mathcal{W}[\![\tau]\!]\rho$. From the hypothesis $\Delta \vdash \chi \leq \chi'$, it follows that $\mathbf{r} : \tau \in \chi$. We use the latter to instantiate $(W, \mathbf{R_1}\uparrow, \mathbf{R_2}\uparrow) \in \mathcal{R}[\![\chi]\!]\rho$, which gives us what we needed to show. □

Lemma 3.22 (World Updates that Respect Register-File Relation)
Let $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$ and $W' \sqsupseteq W$.

1. If $W'(i_{\mathrm{reg}}) = W(i_{\mathrm{reg}})$, then $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\chi]\!]\rho$.
2. Let $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\mathrm{reg}} \mapsto \mathrm{island}_{\mathrm{reg}}(s, W.k)])$, where $s = (W.\mathbf{R_1}[\mathbf{r_d} \mapsto \mathbf{w_1}], W.\chi_1[\mathbf{r_d} : \rho_1(\tau)], W.\mathbf{R_2}[\mathbf{r_d} \mapsto \mathbf{w_2}], W.\chi_2[\mathbf{r_d} : \rho_2(\tau)])$. If $(W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau]\!]\rho$, then $\mathrm{currentMR}(W'(i_{\mathrm{reg}})) \Subset_{W'} \mathcal{R}[\![\chi[\mathbf{r_d} : \tau]]\!]\rho$.

Proof

1. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W'(i_{\mathrm{reg}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\chi]\!]\rho$.

   Instantiate the first premise with $(\widetilde{W}, M_1, M_2)$, noting that the latter is in $\mathrm{currentMR}(W(i_{\mathrm{reg}}))$ since $W'(i_{\mathrm{reg}}) = W(i_{\mathrm{reg}})$, and noting that $\widetilde{W} \sqsupseteq W$ by transitivity of $\sqsupseteq$. Hence, $(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\chi]\!]\rho$ as we needed to show.
2. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W'(i_{\mathrm{reg}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{R}[\![\chi]\!]\rho$. Note that M_i must be of the form $\mathbf{R_i}\uparrow$ and $\mathbf{R_i} = W'.\mathbf{R_i}$.

   Consider arbitrary $(\mathbf{r} : \tau') \in \chi[\mathbf{r_d} : \tau]$. We must show that $(\widetilde{W}, \mathbf{R_1(r)}, \mathbf{R_2(r)}) \in \mathcal{W}[\![\tau']\!]\rho$.

Case $\mathbf{r} = \mathbf{r_d}$: Then $\boldsymbol{\tau'} = \boldsymbol{\tau}$ and $\mathbf{R_i(r)} = \mathbf{w_i}$, which means that it suffices to show $(\widetilde{W}, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$. This latter is immediate from the premise $(W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$ using monotonicity (Lemma 3.8).

Case $\mathbf{r} \neq \mathbf{r_d}$: Then $\mathbf{R_i(r)} = W'.\mathbf{R_i(r)} = W.\mathbf{R_i(r)}$, which means that it suffices to show $(\widetilde{W}, W.\mathbf{R_1(r)}, W.\mathbf{R_2(r)}) \in \mathcal{W}[\![\boldsymbol{\tau'}]\!]\rho$. Instantiate the first premise with $(\widetilde{W}, W.\mathbf{R_1}\restriction, W.\mathbf{R_2}\restriction)$ noting that the latter is in currentMR$(W(i_{\text{reg}}))$ by the definition of island$_{\text{reg}}$. Also note that $\widetilde{W} \sqsupseteq W$ by transitivity of $\sqsupseteq$. Hence, we have that $(\widetilde{W}, W.\mathbf{R_1}\restriction, W.\mathbf{R_2}\restriction) \in \mathcal{R}[\![\boldsymbol{\chi}]\!]\rho$. Instantiating the latter with $(\mathbf{r} : \boldsymbol{\tau'}) \in \boldsymbol{\chi}$ gives us $(\widetilde{W}, W.\mathbf{R_1(r)}, W.\mathbf{R_2(r)}) \in \mathcal{W}[\![\boldsymbol{\tau'}]\!]\rho$ as we needed to show.

□

Lemma 3.23 (World Updates that Respect Stack Relation)
Let currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ and $W' \sqsupseteq W$.

1. If $W'(i_{\text{stk}}) = W(i_{\text{stk}})$, then currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$.
2. Let $W.S_1 = w_{11} :: \cdots :: w_{1n} :: S'_1$, $W.S_2 = w_{21} :: \cdots :: w_{2n} :: S'_2$, $\sigma = \tau_1 :: \cdots :: \tau_n :: \sigma'$ and $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\text{stk}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$, where $s = (S'_1, \sigma', S'_2, \sigma')$. currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\sigma'}]\!]\rho$.
3. Let $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\text{stk}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$, where $s = (w_{11} :: \cdots :: w_{1n} :: S_1, \tau_1 :: \cdots :: \tau_n :: \sigma, w_{21} :: \cdots :: w_{2n} :: S_2, \tau_1 :: \cdots :: \tau_n :: \sigma)$. If $(W', \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\boldsymbol{\tau}_i]\!]\rho$, then currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\tau_1} :: \cdots :: \boldsymbol{\tau_n} :: \boldsymbol{\sigma}]\!]\rho$.
4. Let $W.S_1 = w_{11} :: \cdots :: w_{1n} :: S'_1$, $W.S_2 = w_{21} :: \cdots :: w_{2n} :: S'_2$, $\sigma = \tau_1 :: \cdots :: \tau_n :: \sigma'$ and $W' = (W.k, W.\Psi_1, W.\Psi_2, W.\Theta[i_{\text{stk}} \mapsto \text{island}_{\text{reg}}(s, W.k)])$, where $s = (w_{11} :: \cdots :: w_{1n-1} :: w'_1 :: S'_1, \tau_1 :: \cdots :: \tau_{n-1} :: \tau' :: \sigma', w_{21} :: \cdots :: w_{2n-1} :: w'_2 :: S'_2, \tau_1 :: \cdots :: \tau_{n-1} :: \tau' :: \sigma')$. If $(W', \mathbf{w'_1}, \mathbf{w'_2}) \in \mathcal{W}[\![\boldsymbol{\tau'}]\!]\rho$, then currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\boldsymbol{\tau_1} :: \cdots :: \boldsymbol{\tau_{n-1}} :: \boldsymbol{\tau'} :: \boldsymbol{\sigma}]\!]\rho$.

Proof

1. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in$ currentMR$(W'(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$.

   Instantiate the first premise with $(\widetilde{W}, M_1, M_2)$, noting that the latter is in currentMR$(W(i_{\text{stk}}))$ since $W'(i_{\text{stk}}) = W(i_{\text{stk}})$, and noting that $\widetilde{W} \sqsupseteq W$ by transitivity of $\sqsupseteq$. Hence, $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$ as we needed to show.
2. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in$ currentMR$(W'(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\sigma']\!]\rho$. Note that M_i must be of the form $\mathbf{S'_i}\restriction$ and $\mathbf{S'_i} = W'.\mathbf{S_i}$. The desired result follows directly from monotonicity (Lemma 3.8) after unfolding currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho$.
3. Consider arbitrary $(\widetilde{W}, M_1, M_2) \in$ currentMR$(W'(i_{\text{stk}}))$ such that $\widetilde{W} \sqsupseteq W'$. We must show that $(\widetilde{W}, M_1, M_2) \in \mathcal{S}[\![\tau_1 :: \cdots :: \tau_n :: \sigma]\!]\rho$. Note that M_i must be of the form $\mathbf{w_{j1}} :: \cdots :: \mathbf{w_{jn}} :: \mathbf{S_j}\restriction$ and $\mathbf{w_{j1}} :: \cdots :: \mathbf{w_{jn}} :: \mathbf{S_j} = W'.\mathbf{S_j}$. The desired result follows directly from monotonicity (Lemma 3.8) after unfolding currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\boldsymbol{\tau_1} :: \cdots :: \boldsymbol{\tau_n} :: \boldsymbol{\sigma}]\!]\rho$ and premise $(W', \mathbf{w_{1i}}, \mathbf{w_{2i}}) \in \mathcal{W}[\![\boldsymbol{\tau}_i]\!]\rho$.
4. Let $\sigma' = \boldsymbol{\tau_1} :: \cdots :: \boldsymbol{\tau_n} :: \boldsymbol{\sigma}$. Consider arbitrary $1 \leq k \leq |\sigma'|$ such that such that $(\boldsymbol{\sigma'(k)} = \tau_k)$. We must show that $(\widetilde{W}, \mathbf{W'.S_1(k)}, \mathbf{W'.S_2(k)}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$.

   Case $\mathbf{k} = \mathbf{n}$: Then $\boldsymbol{\tau'} = \boldsymbol{\tau_k}$ and $\mathbf{W'.S_j(k)} = \mathbf{w'_j}$, which means that it suffices to show $(\widetilde{W}, \mathbf{w'_1}, \mathbf{w'_2}) \in \mathcal{W}[\![\boldsymbol{\tau'}]\!]\rho$. This latter is immediate from the premise $(W', \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\boldsymbol{\tau}]\!]\rho$ using monotonicity (Lemma 3.8).

   Case $\mathbf{k} \neq \mathbf{n}$: Then $\mathbf{W'.S_j(k)} = W.\mathbf{S_j(k)}$, which means that it suffices to show $(\widetilde{W}, W.\mathbf{S_1(k)}, W.\mathbf{S_2(k)}) \in \mathcal{W}[\![\boldsymbol{\tau_k}]\!]\rho$. Instantiate the first premise with $(\widetilde{W}, W.\mathbf{S_1}\restriction, W.\mathbf{S_2}\restriction)$ noting that the latter is in currentMR$(W(i_{\text{reg}}))$ by the definition of island$_{\text{reg}}$. Also note that $\widetilde{W} \sqsupseteq W$ by transitivity of $\sqsupseteq$. Hence, we have that $(\widetilde{W}, W.\mathbf{S_1}\restriction, W.\mathbf{S_2}\restriction) \in \mathcal{R}[\![\boldsymbol{\sigma}]\!]\rho$. Instantiating the latter with $(\boldsymbol{\tau_k}) = \boldsymbol{\sigma}(k)$ gives us $(\widetilde{W}, W.\mathbf{S_1(k)}, W.\mathbf{S_2(k)}) \in \mathcal{W}[\![\boldsymbol{\tau_k}]\!]\rho$ as we needed to show.

□

Lemma 3.24 (Heap Interpretation Extension with Boxheap)
If $W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$, $\mathbf{\Psi} \vdash \mathbf{H_1} \approx_{\mathrm{H}} \mathbf{H_2} : \mathbf{\Psi'}$, and boxheap($\mathbf{\Psi'}$), then $W \boxplus (\mathbf{H_1}, \mathbf{H_2}) \in \mathcal{H}[\![\mathbf{\Psi}, \mathbf{\Psi'}]\!]$.

Proof

By induction on $W.k$.

To show $W \boxplus (\mathbf{H_1}, \mathbf{H_2}) \in \mathcal{H}[\![\mathbf{\Psi}, \mathbf{\Psi'}]\!]$, it suffices to show

$$\forall (\ell :^{\nu} \psi) \in (\mathbf{\Psi}, \mathbf{\Psi'}).\ (W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \ell, \ell) \in \mathcal{W}[\![\nu\ \psi]\!]\emptyset$$

where ν is $\mathbf{box}$ or $\mathbf{ref}$.

Consider arbitrary $(\ell :^{\nu} \psi) \in (\mathbf{\Psi}, \mathbf{\Psi'})$. If $\ell \in \mathrm{dom}(\mathbf{\Psi})$, for any value of $W.k$, it follows from the first premise that $(W, \ell, \ell) \in \mathcal{W}[\![\nu\ \psi]\!]\emptyset$. By Lemma 3.5 we have that $W \boxplus (\mathbf{H_1}, \mathbf{H_2}) \sqsupseteq W$, so by monotonicity we have $(W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \ell, \ell) \in \mathcal{W}[\![\nu\ \psi]\!]\emptyset$.

Therefore, it remains for us to show that if $\ell \in \mathrm{dom}(\mathbf{\Psi'})$ then $(W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\ \psi]\!]\emptyset$.

Case $W.k = 0$: Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}((W \boxplus (\mathbf{H_1}, \mathbf{H_2}))(i_{\mathrm{box}}))$ such that $\widetilde{W} \sqsupset (W \boxplus (\mathbf{H_1}, \mathbf{H_2}))$. But the latter implies $\widetilde{W}.k < W.k = 0$ which leads to a contradiction since $\widetilde{W} \in \mathrm{World}$ which requires that $\widetilde{W}.k \geq 0$. So we are done.

Case $W.k = n + 1$ for $n \geq 0$: By the induction hypothesis we know that the lemma we wish to prove holds for any W such that $W.k = n$. We must prove it for any W such that $W.k = n + 1$.

We have that $\ell \in \mathrm{dom}(\mathbf{\Psi'})$ and must show that $(W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\ \psi]\!]\emptyset$.

Consider arbitrary $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}((W \boxplus (\mathbf{H_1}, \mathbf{H_2}))(i_{\mathrm{box}}))$ such that $\widetilde{W} \sqsupset (W \boxplus (\mathbf{H_1}, \mathbf{H_2}))$. Note that it must be the case that $M_1 = (W(i_{\mathrm{box}}).s.H_1 \uplus \mathbf{H_1})\restriction$ and $M_2 = (W(i_{\mathrm{box}}).s.H_2 \uplus \mathbf{H_2})\restriction$. Also, since $\ell \in \mathrm{dom}(\mathbf{\Psi'})$, from the second premise it follows that $\ell \in \mathrm{dom}(\mathbf{H_1})$ and $\ell \in \mathrm{dom}(\mathbf{H_2})$. Regardless of whether ψ is a code type or tuple type, it suffices to show:

$$\begin{aligned} &(\widetilde{W}, M_1(\ell), M_2(\ell)) \in \mathcal{HV}[\![\psi]\!]\emptyset \\ \equiv\ &(\widetilde{W}, \mathbf{H_1}(\ell), \mathbf{H_2}(\ell)) \in \mathcal{HV}[\![\psi]\!]\emptyset \end{aligned}$$

From the second premise, since $(\ell :^{\mathbf{box}} \psi) \in \mathbf{\Psi'}$, it follows that:

$$\mathbf{\Psi}, \mathbf{\Psi'} \vdash \mathbf{H_1}(\ell) \approx_{\mathrm{hv}} \mathbf{H_2}(\ell) : {}^{\mathbf{box}}\psi. \tag{20}$$

Since $\triangleright W \in \mathcal{H}[\![\mathbf{\Psi}]\!]$ by heap monototonicity (Lemma 3.9) and since $(\triangleright W).k = n$, by the induction hypothesis we have that $(\triangleright W \boxplus (\mathbf{H_1}, \mathbf{H_2})) \in \mathcal{H}[\![\mathbf{\Psi}, \mathbf{\Psi'}]\!]$. Thus, we can instantiate (20) with $\triangleright W \boxplus (\mathbf{H_1}, \mathbf{H_2})$, which allows us to conclude that

$$(\triangleright W \boxplus (\mathbf{H_1}, \mathbf{H_2}), \mathbf{H_1}(\ell), \mathbf{H_2}(\ell)) \in \mathcal{HV}[\![\psi]\!]\emptyset$$

Now, since $\widetilde{W} \sqsupset (W \boxplus (\mathbf{H_1}, \mathbf{H_2}))$, we can use by Lemma 3.6 to conclude $\widetilde{W} \sqsupseteq \triangleright(W \boxplus (\mathbf{H_1}, \mathbf{H_2}))$. Hence, by monotonicity, we have $(\widetilde{W}, \mathbf{H_1}(\ell), \mathbf{H_2}(\ell)) \in \mathcal{HV}[\![\psi]\!]\emptyset$ as we needed to show.

□

3.5 Bridge Lemmas

Lemma 3.25 (F Values are F Expressions)
If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$ and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$ then $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma]\!]$.

Proof

Consider arbitrary E_1, E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{out} \vdash \tau; \sigma]\!]\rho$.

We need to show that $(W, E_1[\mathbf{v_1}], E_2[\mathbf{v_2}]) \in \mathcal{O}$. But we can instantiate the $\mathcal{K}[\![\cdot]\!]$ relation with our hypotheses, noting $W \sqsupseteq_{\text{pub}} W$ by reflexivity, to get the result. □

Lemma 3.26 (Monadic Bind F To F)
If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma]\!]\rho$, $(W, E_1, E_2) \in \text{ContAtom}[\mathbf{out} \vdash \tau; \sigma]\rho \rightsquigarrow [\mathbf{out} \vdash \tau^*; \sigma^*]$, and $\forall W' \sqsupseteq_{\text{pub}} W. \forall \mathbf{v_1}, \mathbf{v_2}. (W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho \wedge \text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$
$\implies (W', E_1[\mathbf{v_1}], E_2[\mathbf{v_2}]) \in \mathcal{E}[\![\mathbf{out} \vdash \tau^*; \sigma^*]\!]\rho^*$, then
$(W, E_1[\mathbf{e_1}], E_2[\mathbf{e_2}]) \in \mathcal{E}[\![\mathbf{out} \vdash \tau^*; \sigma^*]\!]\rho^*$

Proof

Consider arbitrary E_1', E_2' such that $(W, E_1', E_2') \in \mathcal{K}[\![\mathbf{out} \vdash \tau^*; \sigma^*]\!]\rho^*$.

It suffices to show that $(W, E_1'[E_1], E_2'[E_2]) \in \mathcal{K}[\![\mathbf{out} \vdash \tau; \sigma]\!]\rho$.

In order to do that, consider arbitrary $W', \mathbf{v_1}, \mathbf{v_2}$ where $W' \sqsupseteq_{\text{pub}} W$, $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$ and currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$. We need to show that $(W', E_1'[E_1[\mathbf{v_1}]], E_2'[E_2[\mathbf{v_2}]]) \in \mathcal{O}$.

From the hypothesis, we know that $(W', E_1[\mathbf{v_1}], E_2[\mathbf{v_2}]) \in \mathcal{E}[\![\mathbf{out} \vdash \tau^*; \sigma^*]\!]$. We can then instantiate that with (W', E_1', E_2'), which, appealing to Lemma 3.10, we know are in $\mathcal{K}[\![\mathbf{out} \vdash \tau^*; \sigma^*]\!]\rho^*$, which yields the result that we need.

□

Lemma 3.27 (Monadic Bind T to F)
If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{end}\{\tau^{\mathcal{T}}; \sigma\} \vdash \tau^{\mathcal{T}}; \sigma]\!]\rho$, $(W, E_1, E_2) \in \text{ContAtom}[\mathbf{end}\{\tau^{\mathcal{T}}; \sigma\} \vdash \tau^{\mathcal{T}}; \sigma]\rho \rightsquigarrow [\mathbf{out} \vdash \tau; \sigma_1]$,
and
$\forall W' \sqsupseteq_{\text{pub}} W. \forall \mathbf{r_1}, \mathbf{r_2}. (\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\tau^{\mathcal{T}}]\!]\rho \wedge \text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$
$\implies (W', E_1[\texttt{ret}\ \mathbf{end}\{\rho_1(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_1}\}], E_2[\texttt{ret}\ \mathbf{end}\{\rho_2(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_2}\}]) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]\rho$, then
$(W, E_1[\mathbf{e_1}], E_2[\mathbf{e_2}]) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]\rho$

Proof

Consider arbitrary E_1', E_2' such that $(W, E_1', E_2') \in \mathcal{K}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]\rho$.

It suffices to show that $(W, E_1'[E_1], E_2'[E_2]) \in \mathcal{K}[\![\mathbf{end}\{\tau^{\mathcal{T}}; \sigma\} \vdash \tau^{\mathcal{T}}; \sigma]\!]\rho$.

In order to do that, consider arbitrary $W', q', \mathbf{r_1}, \mathbf{r_2}$ such that the following hold, noting that based on the form of the return marker, $q' =_\rho \mathbf{end}\{\tau^{\mathcal{T}}; \sigma\}$, rather than possibly being a register.

- $W' \sqsupseteq_{\text{pub}} W$
- $(W', E_1'[E_1], E_2'[E_2]) \in \text{ContAtom}[q' \vdash \tau^{\mathcal{T}}; \sigma]\rho \rightsquigarrow [\mathbf{q}^* \vdash \tau^*; \sigma^*]\rho^*$
- $q' =_\rho \mathbf{end}\{\tau^{\mathcal{T}}; \sigma\}$
- $(\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\tau^{\mathcal{T}}]\!]\rho$
- currentMR$(W(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$

Given the above, we must show that $(W', (E_1'[E_1[\texttt{ret}\ \rho_1(\mathbf{q}')\ \{\mathbf{r_1}\}]], \cdot), (E_2'[E_2[\texttt{ret}\ \rho_2(\mathbf{q}')\ \{\mathbf{r_2}\}]], \cdot)) \in \mathcal{O}$.

From the hypothesis, we know that

$(W', E_1[\texttt{ret}\ \rho_1(\mathbf{end}\{\tau^{\mathcal{T}}; \sigma\})\ \{\mathbf{r_1}\}], E_2[\texttt{ret}\ \rho_2(\mathbf{end}\{\tau^{\mathcal{T}}; \sigma\})\ \{\mathbf{r_2}\}])$
$= (W', E_1[\texttt{ret}\ \rho_1(\mathbf{q}')\ \{\mathbf{r_1}\}], E_2[\texttt{ret}\ \rho_2(\mathbf{q}')\ \{\mathbf{r_2}\}])$
$\in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]$

We can then instantiate that with (W', E_1', E_2'), which, appealing to Lemma 3.10, we know are in $\mathcal{K}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]\rho$, which yields the result that we need.

□

Lemma 3.28 (Bridge Lemma)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \tau$.

1. (a) If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{end}\{\tau^{\mathcal{T}}; \sigma\} \vdash \tau^{\mathcal{T}}; \sigma]\!]\rho$ then $(W, {}^{\rho_1(\tau)}\mathcal{FT}\,\mathbf{e_1}, {}^{\rho_2(\tau)}\mathcal{FT}\,\mathbf{e_2}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]\rho$.

   (b) If the following hold
   - $\forall \text{SR} \in \text{TStackRel}.(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \tau_0' :: \cdots :: \tau_k' :: \zeta]\!]\rho[\zeta \mapsto \text{SR}]$
   - $\Delta \vdash \sigma$
   - $\sigma' = \tau_0' :: \cdots :: \tau_k' :: \sigma_0$
   - $q = i > j$ or $q = \mathbf{end}\{\hat{\tau}; \hat{\sigma}\}$
   - $W \in \mathcal{H}[\![\Psi]\!]$
   - $\text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma']\!]\rho$
   - $\Psi; \Delta; \Gamma; \chi[\mathbf{r_d} : \tau^{\mathcal{T}}]; \sigma'; \text{inc}(\mathbf{q}, \mathbf{k} - \mathbf{j}) \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$
   - $\text{ret-type}(\mathbf{q}, \chi, \sigma) = \hat{\tau}; \hat{\sigma}$

   then $(W, \mathtt{import}\ \mathbf{r_d}, {}^{\rho_1(\sigma_0)}\mathcal{T}\mathcal{F}^{\rho_1(\tau)}\,\mathbf{e_1}; \rho_1(\mathbf{I_1}), \mathtt{import}\ \mathbf{r_d}, {}^{\rho_2(\sigma_0)}\mathcal{T}\mathcal{F}^{\rho_2(\tau)}\,\mathbf{e_2}; \rho_2(\mathbf{I_2})) \in \mathcal{E}[\![\mathbf{q} \vdash \hat{\tau}; \hat{\sigma}]\!]\rho$.

2. (a) If the following hold
   - $(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau^{\mathcal{T}}]\!]\rho$
   - $(M_1, M_2) : W$
   - ${}^{\rho_1(\tau)}\mathbf{FT}((\mathbf{w_1}, \mathbf{M_1})) = (\mathbf{v_1}, M_1 \uplus M_1')$
   - ${}^{\rho_2(\tau)}\mathbf{FT}((\mathbf{w_2}, \mathbf{M_2})) = (\mathbf{v_2}, M_2 \uplus M_2')$

   then $(W \boxplus (M_1', M_2'), \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$

   (b) If the following hold
   - $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$
   - $(M_1, M_2) : W$
   - $\mathbf{TF}^{\rho_1(\tau)}((\mathbf{v_1}, \mathbf{M_1})) = (\mathbf{w_1}, M_1 \uplus M_1')$
   - $\mathbf{TF}^{\rho_2(\tau)}((\mathbf{v_2}, \mathbf{M_2})) = (\mathbf{w_2}, M_2 \uplus M_2')$

   then $(W \boxplus (M_1', M_2'), \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau^{\mathcal{T}}]\!]\rho$

Proof

1. (a) Appeal to Lemma 3.27, letting $E_i = {}^{\rho_i(\tau)}\mathcal{FT}\,[\cdot]$.
   From 3.27 we are given registers $\mathbf{r_1}, \mathbf{r_2}$, and world $W' \sqsupseteq_{\text{pub}} W$ such that
   - $(\triangleright W', W'.\mathbf{R_1}(\mathbf{r_1}), W'.\mathbf{R_2}(\mathbf{r_2})) \in \mathcal{W}[\![\tau^{\mathcal{T}}]\!]\rho$
   - $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma]\!]\rho$

   and need to show that

   $$(W', {}^{\rho_1(\tau)}\mathcal{FT}\,\mathtt{ret}\ \mathbf{end}\{\rho_1(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_1}\}, {}^{\rho_2(\tau)}\mathcal{FT}\,\mathtt{ret}\ \mathbf{end}\{\rho_2(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_2}\}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]\rho$$

   In order to do that, consider arbitrary E_1, E_2 such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]$. We need to show that

   $$(W, E_1[{}^{\rho_1(\tau)}\mathcal{FT}\,\mathtt{ret}\ \mathbf{end}\{\rho_1(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_1}\}], E_2[{}^{\rho_2(\tau)}\mathcal{FT}\,\mathtt{ret}\ \mathbf{end}\{\rho_2(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_2}\}]) \in \mathcal{O}$$

   Consider arbitrary $(\mathbf{M_1}, \mathbf{M_2}) : W$. We take one step

$$\langle \mathbf{M_i} \mid E_1[^{\rho_1(\tau)}\mathcal{FT}\ \mathtt{ret}\ \mathbf{end}\{\rho_1(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_1}\}]\rangle \longmapsto \langle \mathbf{M_i} \uplus \mathbf{M'_i} \mid E_i[\mathbf{v_i}]\rangle$$

where ${}^{\tau}\mathbf{FT}(\mathbf{M_i.R(r_i)}, \mathbf{M_i}) = (\mathbf{v_i}, \mathbf{M_i} \uplus \mathbf{M'_i})$
From part 2(a) we have that $(\triangleright W' \boxplus (\mathbf{M'_1}, \mathbf{M'_2}), \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$, noting from Lemmas 3.4,3.5,3.6, that

$$(\mathbf{M_1}, \mathbf{M_2}) : \triangleright W' \text{ and } \triangleright W' \boxplus (\mathbf{M'_1}, \mathbf{M'_2}) \sqsupseteq_{\text{pub}} W'$$

This means we can instantiate E_1, E_2 to get that

$$(\triangleright W' \boxplus (\mathbf{M'_1}, \mathbf{M'_2}), E_1[\mathbf{v_1}], E_2[\mathbf{v_2}]) \in \mathcal{O}$$

which is sufficient to prove that

$$(W', E_1[^{\rho_1(\tau)}\mathcal{FT}\ \mathtt{ret}\ \mathbf{end}\{\rho_1(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_1}\}], E_2[^{\rho_2(\tau)}\mathcal{FT}\ \mathtt{ret}\ \mathbf{end}\{\rho_2(\tau^{\mathcal{T}}); \sigma\}\ \{\mathbf{r_2}\}]) \in \mathcal{O}$$

since each took exactly one reduction step.

(b) We must show that

$$(W, \mathtt{import}\ \mathbf{r_d}, {}^{\rho_1(\sigma_0)}\mathcal{TF}^{\rho_1(\tau)}\ \mathbf{e_1}; \rho_1(\mathbf{I_1}), \mathtt{import}\ \mathbf{r_d}, {}^{\rho_2(\sigma_0)}\mathcal{TF}^{\rho_2(\tau)}\ \mathbf{e_2}; \rho_2(\mathbf{I_2})) \in \mathcal{E}[\![\mathbf{q} \vdash \hat{\tau}; \hat{\sigma}]\!]\rho$$

In order to do that, consider arbitrary E_1, E_2, such that $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \hat{\tau}; \sigma]\!]\rho$.
We are required to show that

$$(W, E_1[\mathtt{import}\ \mathbf{r_d}, {}^{\rho_1(\sigma_0)}\mathcal{TF}^{\rho_1(\tau)}\ \mathbf{e_1}; \rho_1(\mathbf{I_1})], E_2[\mathtt{import}\ \mathbf{r_d}, {}^{\rho_2(\sigma_0)}\mathcal{TF}^{\rho_2(\tau)}\ \mathbf{e_2}; \rho_2(\mathbf{I_2})]) \in \mathcal{O}$$

Consider arbitrary $(M_1, M_2) : W$. From the premise, we know that there exist $\mathbf{S_1}$ and $\mathbf{S_2}$ such that $(W, \mathbf{S_1}\restriction, \mathbf{S_2}\restriction) \in \mathcal{S}[\![\sigma']\!]\rho$
Since $\sigma' = \tau_0 :: \cdots :: \tau_j :: \sigma_0$, there exist $\mathbf{S_{10}}$ and $\mathbf{S_{20}}$ such that $(W, \mathbf{S_{10}}, \mathbf{S_{20}} \in \mathcal{S}[\![\sigma_0]\!]$.
We can instantiate the first premise with $SR = (\rho_1(\sigma_0), \rho_2(\sigma_0), \varphi_S)$ where $\varphi_S = \{(\widetilde{W}, \mathbf{S_{10}}, \mathbf{S_{20}}) \mid \widetilde{W} \sqsupseteq W\}$.
Let $\rho^* = \rho[\zeta \mapsto SR]$. Hence, $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma']\!]\rho^*$.
We can instantiate this with evaluation contexts

- $E'_1 = E_1[\mathtt{import}\ \mathbf{r_d}, \rho_1^*(\sigma_0)\mathcal{TF}^{\tau}\ [\cdot]; \mathbf{I_1}]$
- $E'_2 = E_2[\mathtt{import}\ \mathbf{r_d}, \rho_2^*(\sigma_0)\mathcal{TF}^{\tau}\ [\cdot]; \mathbf{I_2}]$

It now suffices to show that

$$(W, E'_1, E'_2) \in) \in \mathcal{K}[\![\mathbf{out} \vdash \tau; \sigma']\!]\rho^*$$

Consider arbitrary $W', \mathbf{v_1}, \mathbf{v_2}$ such that $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho^*$, currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma']\!]\rho^*$.
We need to show that

$$(W', E'_1[\mathbf{v_1}], E'_2[\mathbf{v_2}]) = (W', E_1[\mathtt{import}\ \mathbf{r_d}, \rho_1^*(\sigma_0)\mathcal{TF}^{\tau}\ \mathbf{v_1}; \mathbf{I_1}], E_2[\mathtt{import}\ \mathbf{r_d}, \rho_2^*(\sigma_0)\mathcal{TF}^{\tau}\ \mathbf{v_2}; \mathbf{I_2}]) \in \mathcal{O}$$

Consider arbitrary $(\mathbf{M_1}, \mathbf{M_2}) : W'$. We first take one step

$$\langle \mathbf{M_i} \mid E_i[\mathtt{import}\ \mathbf{r_d}, \rho_i^*(\sigma_0)\mathcal{TF}^{\tau}\ \mathbf{v_i}; \mathbf{I_i}]\rangle \longmapsto \langle \mathbf{M_i} \uplus \mathbf{M'_i} \mid E_i[\mathtt{mv}\ \mathbf{r_d}, \mathbf{w_i}; \mathbf{I_i}]\rangle$$

where $\mathbf{TF}^{\tau}(\mathbf{v_i}, \mathbf{M_i}) = (\mathbf{w_i}, \mathbf{M_i} \uplus \mathbf{M'_i})$ Noting from part 2(b), we have that $(W' \boxplus (\mathbf{M'_1}, \mathbf{M'_2}), \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\tau^{\mathcal{T}}]\!]\rho^*$, and from Lemma 3.5, $W' \boxplus (\mathbf{M'_1}, \mathbf{M'_2}) \sqsupseteq_{\text{pub}} W'$.
Then we take another step

$$\langle \mathbf{M_i} \uplus \mathbf{M'_i} \mid E_i[\mathtt{mv}\ \mathbf{r_d}, \mathbf{w_i}; \mathbf{I_i}]\rangle \longmapsto \langle \mathbf{M_i} \uplus \mathbf{M'_i}[\mathbf{r_d} \mapsto (\mathbf{w_1}, \mathbf{w_2})] \mid E_i[\mathbf{I_i}]\rangle$$

We now apply our hypothesis about $\mathbf{I_i}$, noting that the results above and choice of ρ^* fulfill the requirements for the stack and heap.
We can now instantiate the resulting $\mathcal{E}[\![\cdot]\!]$ with E_1, E_2, which gives us that

$$(W' \boxplus \mathbf{M_i} \uplus \mathbf{M_i'}[\mathbf{r_d} \mapsto (\mathbf{w_1}, \mathbf{w_2})], E_1[\mathbf{I_1}], E_2[\mathbf{I_2}]) \in \mathcal{O}$$

from which the result follows, since in

$$(W', E_1[\texttt{import } \mathbf{r_d}, \rho_1^*(\sigma_0)\mathcal{T}\mathcal{F}^\tau \mathbf{v_1}; \mathbf{I_1}], E_2[\texttt{import } \mathbf{r_d}, \rho_2^*(\sigma_0)\mathcal{T}\mathcal{F}^\tau \mathbf{v_2}; \mathbf{I_2}]) \in \mathcal{O}$$

each took exactly two steps to reach the above.

2. (a) Proceed by induction first on the step index $W.k$ and then on the structure of $\boldsymbol{\tau}$.

Case **unit** Follows trivially from the value translation and $\mathcal{W}[\![\textbf{unit}]\!]\rho$ and $\mathcal{V}[\![\textbf{unit}]\!]\rho$.

Case **int** Follows trivially from the value translation and $\mathcal{W}[\![\textbf{int}]\!]\rho$ and $\mathcal{V}[\![\textbf{int}]\!]\rho$.

Case $\boldsymbol{\mu\alpha.\tau}$ We're given that

$$(W, \textbf{fold}_{\mu\alpha.\tau}\tau\ \mathbf{w_1}, \textbf{fold}_{\mu\alpha.\tau}\tau\ \mathbf{w_2}) \in \mathcal{W}[\![\mu\alpha.\tau^{\mathcal{T}}]\!]\rho$$

which is translated to $(\textbf{fold}_{\mu\alpha.\tau}\ \mathbf{v_i}, \mathbf{M_i} \uplus \mathbf{M_i'})$.
From this, we know that

$$(W, \mathbf{w_1}, \mathbf{w_2}) \in \triangleright\mathcal{W}[\![\tau^{\mathcal{T}}[\mu\alpha.\tau^{\mathcal{T}}/\alpha]]\!]\rho$$

Since we are inducting on the step index $W.k$, we can use this, along with the value translations that we have from the hypothesis to get that

$$(W \boxplus (\mathbf{M_1'}, \mathbf{M_2'}), \mathbf{v_1}, \mathbf{v_2}) \in \triangleright\mathcal{V}[\![\tau^{\mathcal{T}}[\mu\alpha.\tau^{\mathcal{T}}/\alpha]]\!]\rho$$

which, when combined with the typing rules, yields the required result.

Case $\langle\tau_1, \ldots, \tau_n\rangle$ From the definition of $\mathcal{W}[\![\textbf{box}\ \langle\tau_1, \ldots, \tau_n\rangle]\!]\rho$ we know that

$$(W, M_1(\mathbf{w_1}), M_2(\mathbf{w_2})) \in \mathcal{HV}[\![\langle\tau_1{}^{\mathcal{T}}, \ldots, \tau_n{}^{\mathcal{T}}\rangle]\!]\rho$$

where $M_i(\mathbf{w_i}) = \langle\mathbf{w_{i1}}, \ldots, \mathbf{w_{in}}\rangle$.
From the definition of $\mathcal{HV}[\![\cdot]\!]$ we know that

$$(W, \mathbf{w_{1j}}, \mathbf{w_{2j}}) \in \mathcal{W}[\![\tau_j{}^{\mathcal{T}}]\!]\rho$$

By the value translation, ${}^{\rho_i(\tau_j)}\mathbf{FT}((\mathbf{w_{ij}}, \mathbf{M_{ij}})) = (\mathbf{v_{ij}}, \mathbf{M_{ij}} \uplus \mathbf{M'_{ij}})$, where

- $\mathbf{M_{i0}} = \mathbf{M}$
- $\mathbf{M_{ij}} = \mathbf{M_{i(j-1)}} \uplus \mathbf{M'_{i(j-1)}}$
- $\mathbf{M_i'} = \cup_j \mathbf{M'_{ij}}$

We know that $(\mathbf{M_{1n}}, \mathbf{M_{2n}}) : W$ since $(\mathbf{M_{10}}, \mathbf{M_{20}}) : W$ and the only changes to the memory are additions.
We can use the inductive hypothesis to conclude that

$$(W \boxplus (\mathbf{M_1'}, \mathbf{M_2'}), \mathbf{v_{1j}}, \mathbf{v_{2j}}) \in \mathcal{V}[\![\tau_j{}^{\mathcal{T}}]\!]\rho$$

which combined with the typing rules, yields what we need.

Case $\boldsymbol{(\overline{\tau}) \to \tau'}$ Given some $W' \sqsupseteq W \boxplus (\ell_{1end} \mapsto \mathbf{h_{end}}, \ell_{2end} \mapsto \mathbf{h_{end}})$, where

- $\mathbf{h_{end}} = \textbf{code}[\zeta]\{\mathbf{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\textbf{end}\{\tau'^{\mathcal{T}}; \zeta\}}.\mathbf{ret}\ \textbf{end}\{\tau'^{\mathcal{T}}; \zeta\}\ \{\mathbf{r1}\}$
- $SR \in TStackRel$
- $\rho' = \rho[\zeta \mapsto SR]$
- $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\zeta]\!]\rho'$
- $(W', v_{1j}, v_{2j}) \in \mathcal{V}[\![\tau_j]\!]\rho'$ for $j \in \{1..n\}$

we need to show that

$$(W', \mathbf{v_1 v_{10}} \ldots \mathbf{v_{1n}}, \mathbf{v_2 v_{20}} \ldots \mathbf{v_{2n}}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \zeta]\!]\rho$$

where

$$\begin{aligned}\mathbf{v_i} = \lambda(\overline{\mathbf{x_n} : \tau_n}).^{\tau'}\mathcal{FT}\ (&\mathtt{protect}\ \cdot, \zeta; \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_1}\ \mathbf{x_1}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \ldots;\\ &\mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_n}\ \mathbf{x_n}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1};\\ &\mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\zeta]; \mathtt{jmp}\ \mathbf{w}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}], \cdot)\end{aligned}$$

We proceed by appealing to Lemma 3.4.3.

Consider arbitrary $(M_1, M_2) : W'$. We first take one step

$$\begin{aligned}\langle \mathbf{M_i} \mid \mathbf{v_i v_{i0}} \ldots \mathbf{v_{in}} \rangle \longmapsto \langle \mathbf{M_i} \mid {}^{\tau'}\mathcal{FT}\ (&\mathtt{protect}\ \cdot, \zeta; \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_1}\ \mathbf{v_{i1}}; \quad \rangle\\ &\mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \ldots;\\ &\mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_n}\ \mathbf{v_{in}}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1};\\ &\mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\zeta]; \mathtt{jmp}\ \mathbf{w}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}]), \cdot)\end{aligned}$$

To show that this is in $\mathcal{E}[\![\mathbf{out} \vdash \tau'; \zeta]\!]$, it suffices to show that what is within the boundary is in $\mathcal{E}[\![\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\} \vdash \tau'^{\mathcal{T}}; \zeta]\!]$, as part 1(a) will then yield the result.

We now appeal to Lemma 3.4.3 again, noting we can take $3n + 1$ steps:

$$\begin{aligned}\langle \mathbf{M_i} \mid (&\mathtt{protect}\ \cdot, \zeta; \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_1}\ \mathbf{v_{i1}}; \quad \rangle \longmapsto {}^{3n}\langle \mathbf{M_i^*} \mid (\mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\zeta]; \quad \rangle\\ &\mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \ldots; \qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{jmp}\ \mathbf{w_i}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}], \cdot)\\ &\mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_n}\ \mathbf{v_{in}}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1};\\ &\mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\zeta]; \mathtt{jmp}\ \mathbf{w_i}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}], \cdot)\end{aligned}$$

Where

- $\mathbf{M_{i0a}} = \mathbf{M_i}$
- $\mathbf{TF}^{\tau_j}(\mathbf{v_{ij}}, \mathbf{M_{ija}}) = (\mathbf{w_{ij}}, \mathbf{M_{ijb}})$
- $\mathbf{M_{ijc}} = \mathbf{M_{ijb}}[\mathbf{r1} \mapsto \mathbf{w_{ij}}]$
- $\mathbf{M_{ijd}} = \mathbf{M_{ijc}}[() ::]$
- $\mathbf{M_{ije}} = \mathbf{M_{ijc}}[\mathbf{w_{ij}} ::]$
- $\mathbf{M_{i(j+1)a}} = \mathbf{M_{ije}}$
- $\mathbf{M_i^*} = \mathbf{M_{in}}$

We take one more step, resulting in:

$$\langle \mathbf{M_i^*}[\mathbf{ra} \mapsto \ell_{\mathbf{end}}[\zeta]] \mid (\mathtt{jmp}\ \mathbf{w_i}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}], \cdot)\rangle$$

We know

$$(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\mathbf{box}\ \forall[\zeta, \epsilon].\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\epsilon}; \sigma'\}^{\mathtt{ra}}]\!]\rho$$

where $\sigma' = \sigma' = \tau_n{}^{\mathcal{T}} :: \cdots :: \tau_1{}^{\mathcal{T}} :: \zeta$.
This means that

$$\begin{aligned}&(W, \mathbf{w_1}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}], \mathbf{w_1}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}])\\ &\quad \in \mathcal{W}[\![\mathbf{box}\ \forall[].\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}}; \zeta\}}; \sigma'\}^{\mathtt{ra}}]\!]\rho\end{aligned}$$

And thus $\mathbf{w_i}$ is a location that points to $\mathbf{code}[\zeta, \epsilon]\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}};\zeta\}^{\epsilon};\sigma'\}^{\mathtt{ra}}.\mathbf{I_i}$.
This means that the next reduction step results in:

$$\langle \mathbf{M_i^*}[\mathtt{ra} \mapsto \ell_{\mathbf{end}}[\zeta]] \mid (\mathbf{I_i}, \cdot)\rangle$$

From $\mathcal{W}[\![\mathbf{box}\,\forall[].\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}};\zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\};\sigma'\}^{\mathtt{ra}}]\!]\rho$ we know that

$$\begin{aligned}(W, &\mathbf{code}[]\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}};\zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\};\sigma'\}^{\mathtt{ra}}.\mathbf{I_1},\\ &\mathbf{code}[]\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}};\zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\};\sigma'\}^{\mathtt{ra}}.\mathbf{I_2})\\ &\in \mathcal{HV}[\![\forall[].\{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}};\zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\};\sigma'\}^{\mathtt{ra}}]\!]\rho\end{aligned}$$

This means that for any $W' \sqsupseteq W$, fulfilling the stack and register requirements, in particular, $W^* = W' \boxplus (\mathbf{M_1^*}\backslash\mathbf{M_1}, \mathbf{M_2^*}\backslash\mathbf{M_2})$, we have that $(W^*, (\mathbf{I_1}, \cdot), (\mathbf{I_2}, \cdot)) \in \mathcal{E}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}};\sigma']\!]\rho$.
Recall that what we need is that the reduced expression is in $\mathcal{E}[\![\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\} \vdash \tau'^{\mathcal{T}};\zeta]\!]\rho$.
In order to show that, consider arbitrary E_1, E_2 such that $(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\} \vdash \tau'^{\mathcal{T}};\zeta]\!]\rho$. We need to show that $(W', E_1[\mathbf{e_1}], E_2[\mathbf{e_2}]) \in \mathcal{O}$ where $\mathbf{e_i}$ are the reduced expressions. Note that this is equivalent to showing that $(W^*, E_1[\mathbf{e_1}], E_2[\mathbf{e_2}]) \in \mathcal{O}$, since $W^* \sqsupseteq W'$.
Since we know that $(W^*, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}};\sigma']\!]\rho$, we know that for any continuations E_1' and E_2' in $\mathcal{K}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}};\sigma']\!]\rho$, $(W^*, E_1'[\mathbf{e_1}], E_2'[\mathbf{e_2}]) \in \mathcal{O}$.
We argue that E_1 and E_2 are suitable choices for E_1' and E_2'. By the definition of the $\mathcal{K}[\![\cdot]\!]$ relation, we need that $(W^*, E_1[(\mathtt{ret}\,\mathtt{ra}\,\{\mathtt{r1}\}, \cdot)], E_2[(\mathtt{ret}\,\mathtt{ra}\,\{\mathtt{r1}\}, \cdot)]) \in \mathcal{O}$.
Since $\mathrm{currentMR}(W^*(i_{\mathrm{reg}})) \Subset_{W^*} \{\mathtt{ra}:\forall[].\{\mathtt{r1}:\tau'^{\mathcal{T}};\zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\}}\}$, this reduces, by the operational semantics, to $(W^*, E_1[(\mathbf{I_1^*}, \cdot)], E_2[(\mathbf{I_2^*}, \cdot)])$, where $(W^*, (\mathbf{I_1^*}, \cdot), (\mathbf{I_2^*}, \cdot)) \in \mathcal{E}[\![\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\} \vdash \tau'^{\mathcal{T}};\zeta]\!]\rho$
But this exactly means that $(W^*, E_1[(\mathbf{I_1^*}, \cdot)], E_2[(\mathbf{I_2^*}, \cdot)]) \in \mathcal{O}$, as $(W^*, E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\} \vdash \tau'^{\mathcal{T}};\zeta]\!]\rho$, so we are done.

Case $(\overline{\tau}) \xrightarrow{\phi_i;\phi_o} \tau'$

Given some $W' \sqsupseteq W \boxplus (\ell_{1\mathbf{end}} \mapsto \mathbf{h_{end}}, \ell_{2\mathbf{end}} \mapsto \mathbf{h_{end}})$, where

$$\begin{aligned}&\mathbf{h_{end}} = \mathbf{code}[\zeta]\{\mathtt{r1}:\tau'^{\mathcal{T}};\zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\}}.\mathtt{ret}\,\mathbf{end}\{\tau'^{\mathcal{T}};\zeta\}\,\{\mathtt{r1}\}\\ &SR \in TStackRel\\ &\rho' = \rho[\zeta \mapsto SR]\\ &\mathrm{currentMR}(W'(i_{\mathrm{stk}})) \Subset_{W'} \mathcal{S}[\![\phi_i :: \zeta]\!]\rho'\\ &(W', v_{1j}, v_{2j}) \in \mathcal{V}[\![\tau_j]\!]\rho' \text{ for } j \in \{1..n\}\end{aligned}$$

we need to show that
$(W', \mathbf{v_1 v_{10}} \ldots \mathbf{v_{1n}}, \mathbf{v_2 v_{20}} \ldots \mathbf{v_{2n}}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau';\phi_o :: \zeta]\!]\rho$
where

$$\begin{aligned}\mathbf{v_i} = \lambda^{\phi_i}_{\phi_o}(\overline{\mathtt{x_n}:\tau_n}).^{\tau'}\mathcal{FT}\,(&\mathtt{protect}\ \phi_i, \zeta; \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_1}\ \mathbf{x_1}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \ldots;\\ &\mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_n}\ \mathbf{x_n}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1};\\ &\mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\phi_o :: \zeta]; \mathtt{jmp}\ \mathbf{w}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}};\phi_o :: \zeta\}], \cdot)\end{aligned}$$

We proceed by appealing to Lemma 3.4.3.
Consider arbitrary $(M_1, M_2) : W'$. We first take one step

$$\begin{aligned}\langle \mathbf{M_i} \mid \mathbf{v_i v_{i0}} \ldots \mathbf{v_{in}}\rangle \longmapsto \langle \mathbf{M_i} \mid {}^{\tau'}\mathcal{FT}\,(&\mathtt{protect}\ \phi_i, \zeta; \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_1}\ \mathbf{v_{i1}}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1}; \ldots;\rangle\\ &\mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_n}\ \mathbf{v_{in}}; \mathtt{salloc}\ 1; \mathtt{sst}\ 0, \mathtt{r1};\\ &\mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\phi_o :: \zeta]; \mathtt{jmp}\ \mathbf{w}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}};\phi_o :: \zeta\}], \cdot)\end{aligned}$$

To show that this is in $\mathcal{E}[\![\mathbf{out} \vdash \tau'; \phi_o :: \zeta]\!]$, it suffices to show that what is within the boundary is in

$$\mathcal{E}[\![\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\} \vdash \tau'^{\mathcal{T}}; \phi_o :: \zeta]\!]$$

as part 1(a) will then yield the result.
We now appeal to Lemma 3.4.3 again, noting we can take $3n + 1$ steps:

$$\begin{aligned}
&\langle \mathbf{M_i} \mid (\mathtt{protect}\ \phi_i, \zeta; \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_1}\ \mathbf{v_{i1}}; \mathtt{salloc}\ \mathbf{1}; \mathtt{sst}\ \mathbf{0}, \mathtt{r1}; \ldots;\rangle \\
&\qquad \mathtt{import}\ \mathtt{r1}, {}^{\zeta}\mathcal{TF}^{\tau_n}\ \mathbf{v_{in}}; \mathtt{salloc}\ \mathbf{1}; \mathtt{sst}\ \mathbf{0}, \mathtt{r1}; \\
&\qquad \mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\phi_o :: \zeta]; \mathtt{jmp}\ \mathbf{w_i}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}], \cdot) \\
&\longmapsto {}^{3n}\langle \mathbf{M_i^*} \mid (\mathtt{mv}\ \mathtt{ra}, \ell_{\mathbf{end}}[\phi_o :: \zeta]; \qquad\qquad \rangle \\
&\qquad\qquad \mathtt{jmp}\ \mathbf{w_i}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}], \cdot)
\end{aligned}$$

Where $\mathbf{M_{i0a}} = \mathbf{M_i}$
$\mathbf{TF}^{\tau_j}(\mathbf{v_{ij}}, \mathbf{M_{ija}}) = (\mathbf{w_{ij}}, \mathbf{M_{ijb}})$
$\mathbf{M_{ijc}} = \mathbf{M_{ijb}}[\mathbf{r1} \mapsto \mathbf{w_{ij}}]$
$\mathbf{M_{ijd}} = \mathbf{M_{ijc}}[() ::]$
$\mathbf{M_{ije}} = \mathbf{M_{ijc}}[\mathbf{w_{ij}} ::]$
$\mathbf{M_{i(j+1)a}} = \mathbf{M_{ije}}$
$\mathbf{M_i^*} = \mathbf{M_{in}}$
We take one more step, resulting in:

$$\langle \mathbf{M_i^*}[\mathbf{ra} \mapsto \ell_{\mathbf{end}}[\phi_o :: \zeta]] \mid (\mathtt{jmp}\ \mathbf{w_i}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}], \cdot)\rangle$$

We know

$$(W, \mathbf{w_1}, \mathbf{w_2}) \in \mathcal{W}[\![\mathbf{box}\, \forall[\zeta, \epsilon].\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\epsilon}; \sigma'\}^{\mathtt{ra}}]\!]\rho$$

where $\sigma' = \sigma' = \tau_n{}^{\mathcal{T}} :: \cdots :: \tau_1{}^{\mathcal{T}} :: \phi_i :: \zeta$.
This means that

$$\begin{aligned}
&(W, \mathbf{w_1}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}], \\
&\quad \mathbf{w_1}[\zeta][\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}]) \\
&\qquad \in \mathcal{W}[\![\mathbf{box}\, \forall[].\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}; \sigma'\}^{\mathtt{ra}}]\!]\rho
\end{aligned}$$

And thus $\mathbf{w_i}$ is a location that points to $\mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\epsilon}; \sigma'\}^{\mathtt{ra}}.\mathbf{I_i}$.
This means that the next reduction step results in:

$$\langle \mathbf{M_i^*}[\mathbf{ra} \mapsto \ell_{\mathbf{end}}[\phi_o :: \zeta]] \mid (\mathbf{I_i}, \cdot)\rangle$$

From $\mathcal{W}[\![\mathbf{box}\, \forall[].\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}; \sigma'\}^{\mathtt{ra}}]\!]\rho$ we know that

$$\begin{aligned}
&(W, \mathbf{code}[]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}; \sigma'\}^{\mathtt{ra}}.\mathbf{I_1}, \\
&\quad \mathbf{code}[]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}; \sigma'\}^{\mathtt{ra}}.\mathbf{I_2}) \\
&\quad \in \mathcal{HV}[\![\forall[].\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}; \sigma'\}^{\mathtt{ra}}]\!]\rho
\end{aligned}$$

This means that for any $W' \sqsupseteq W$, fulfilling the stack and register requirements, in particular, $W^* = W' \boxplus (\mathbf{M_1^*} \backslash \mathbf{M_1}, \mathbf{M_2^*} \backslash \mathbf{M_2})$, we have that

$$(W^*, (\mathbf{I_1}, \cdot), (\mathbf{I_2}, \cdot)) \in \mathcal{E}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}}; \sigma']\!]\rho$$

Recall that what we need is that the reduced expression is in

$$\mathcal{E}[\![\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\} \vdash \tau'^{\mathcal{T}}; \phi_o :: \zeta]\!]\rho$$

In order to show that, consider arbitrary E_1, E_2 such that

$$(W', E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\} \vdash \tau'^{\mathcal{T}}; \phi_o :: \zeta]\!]\rho$$

We need to show that $(W', E_1[\mathbf{e_1}], E_2[\mathbf{e_2}]) \in \mathcal{O}$ where $\mathbf{e_i}$ are the reduced expressions. Note that this is equivalent to showing that $(W^*, E_1[\mathbf{e_1}], E_2[\mathbf{e_2}]) \in \mathcal{O}$, since $W^* \sqsupseteq W'$.
Since we know that $(W^*, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}}; \sigma']\!]\rho$, we know that for any continuations E_1' and E_2' in $\mathcal{K}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}}; \sigma']\!]\rho$, $(W^*, E_1'[\mathbf{e_1}], E_2'[\mathbf{e_2}]) \in \mathcal{O}$.
We argue that E_1 and E_2 are suitable choices for E_1' and E_2'. By the definition of the $\mathcal{K}[\![\cdot]\!]$ relation, we need that

$$(W^*, E_1[(\mathtt{ret\ ra\ \{r1\}}, \cdot)], E_2[(\mathtt{ret\ ra\ \{r1\}}, \cdot)]) \in \mathcal{O}$$

Since

$$\text{currentMR}(W^*(i_{\text{reg}})) \Subset_{W^*} \{\mathtt{ra} : \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\}\}$$

this reduces, by the operational semantics, to $(W^*, E_1[(\mathbf{I_1^*}, \cdot)], E_2[(\mathbf{I_2^*}, \cdot)])$, where

$$(W^*, (\mathbf{I_1^*}, \cdot), (\mathbf{I_2^*}, \cdot)) \in \mathcal{E}[\![\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\} \vdash \tau'^{\mathcal{T}}; \phi_o :: \zeta]\!]\rho$$

But this exactly means that

$$(W^*, E_1[(\mathbf{I_1^*}, \cdot)], E_2[(\mathbf{I_2^*}, \cdot)]) \in \mathcal{O}$$

as

$$(W^*, E_1, E_2) \in \mathcal{K}[\![\mathbf{end}\{\tau'^{\mathcal{T}}; \phi_o :: \zeta\} \vdash \tau'^{\mathcal{T}}; \phi_o :: \zeta]\!]\rho$$

so we are done.

(b) Proceed by induction first on the step index $W.k$ and then on the structure of τ.

Case **unit** Follows trivially from the value translation and the definitions of $\mathcal{W}[\![\mathbf{unit}]\!]\rho$ and $\mathcal{V}[\![\mathbf{unit}]\!]\rho$.

Case **int** Follows trivially from the value translation and the definitions of $\mathcal{W}[\![\mathbf{int}]\!]\rho$ and $\mathcal{V}[\![\mathbf{int}]\!]\rho$.

Case $\mu\alpha.\tau$
This case proceeds analogously to the $\mu\alpha.\tau$ case in the other direction.

Case $\langle\tau_1, \ldots, \tau_n\rangle$ To show that that (W, ℓ_1, ℓ_2) is in

$$\mathcal{W}[\![\langle\tau_1, \ldots, \tau_n\rangle^{\mathcal{T}}]\!]\rho = \mathcal{W}[\![\mathbf{box}\ \langle\tau_1{}^{\mathcal{T}}, \ldots, \tau_n{}^{\mathcal{T}}\rangle]\!]\rho$$

we need to show that

$$(W, \mathbf{M_1}(\ell_1), \mathbf{M_2}(\ell_2)) \in \mathcal{HV}[\![\langle\tau_1{}^{\mathcal{T}}, \ldots, \tau_n{}^{\mathcal{T}}\rangle]\!]\rho$$

for any $\mathbf{M_i}$ satisfying the box memory relation.
This, in turn, requires that for each j, $(W, \mathbf{w_{1j}}, \mathbf{w_{2j}}) \in \mathcal{W}[\![\tau_j{}^{\mathcal{T}}]\!]\rho$.
We're given that

$$(W, \langle\mathbf{v_{10}}, \ldots, \mathbf{v_{1n}}\rangle, \langle\mathbf{v_{10}}, \ldots, \mathbf{v_{1n}}\rangle) \in \mathcal{V}[\![\langle\tau_1, \ldots, \tau_n\rangle]\!]\rho$$

which means that $(W, \mathbf{v_{1j}}, \mathbf{v_{2j}}) \in \mathcal{V}[\![\tau_j]\!]\rho$.
From the value translation, we know that

- $\mathbf{TF}^{\rho_i(\tau_j)}((\mathbf{v_{ij}}, \mathbf{M_{ij}})) = (\mathbf{w_{ij}}$
- $\mathbf{M_{ij}} \uplus \mathbf{M'_{ij}})$

where

- $\mathbf{M_{i0}} = \mathbf{M_i}$
- $\mathbf{M_{ij}} = \mathbf{M_{i(j-1)}} \uplus \mathbf{M'_{i(j-1)}}$
- $\mathbf{M'_i} = \cup_j \mathbf{M'_{ij}}$

This follows from the fact that

$$\mathbf{TF}^{\rho_i(\langle \tau_0, \ldots, \tau_n \rangle)}((\mathbf{v_i}, \mathbf{M_i})) = (\mathbf{w_i}, \mathbf{M_i} \uplus \mathbf{M'_i})$$

Since $(\mathbf{M_{1j}}, \mathbf{M_{2j}}) : W$, as they are extensions of $\mathbf{M_1}$ and $\mathbf{M_2}$, we can use the induction hypotheses and conclude that $(W \boxplus (\mathbf{M'_1}, \mathbf{M'_2}), \mathbf{w_{1j}}, \mathbf{w_{2j}}) \in \mathcal{W}[\![\tau_j{}^{\mathcal{T}}]\!]\rho$. This, combined with the value translation placing these values in a tuple on the heap, yields the required result.

Case $(\overline{\tau}) \to \tau'$

To show that that (W, ℓ_1, ℓ_2) is in

$$\mathcal{W}[\![(\overline{\tau}) \to \tau'^{\mathcal{T}}]\!]\rho = \mathcal{W}[\![\mathbf{box}\, \forall[\zeta, \epsilon].\{\mathtt{ra} : \mathbf{box}\, \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\epsilon}; \sigma'\}^{\mathtt{ra}}]\!]\rho$$

where $\sigma' = \tau_n{}^{\mathcal{T}} :: \cdots :: \tau_1{}^{\mathcal{T}} :: \zeta$, we need to show that for any future world $\widetilde{W} \sqsupset W$, and any memories M_1, M_2 such that $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$, the following conditions hold:

- $M_i(\ell_i) = \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \rho_i(\tau'^{\mathcal{T}}); \zeta\}^{\epsilon}; \rho_i(\sigma')\}^{\mathtt{ra}}.\mathbf{I_i}$
- $(\widetilde{W}, M_1(\ell_1), M_2(\ell_2)) \in \mathcal{HV}[\![\forall[\zeta, \epsilon].\{\mathtt{ra} : \mathbf{box}\, \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\epsilon}; \sigma'\}^{\mathtt{ra}}]\!]\rho$

The latter requires that, in a further future world $W' \sqsupseteq \widetilde{W}$, with $\rho^* \in \mathcal{D}[\![\zeta, \epsilon]\!]$, letting $\rho' = \rho \cup \rho^*$, such that the world fulfills the following restrictions:

- $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\mathtt{ra} : \mathbf{box}\, \forall[].\{\mathtt{r1} : \rho_1(\tau'^{\mathcal{T}}); \zeta\}^{\epsilon}]\!]\rho'$
- $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma']\!]\rho'$

We must show that

$$(W', (\rho_1^*(\mathbf{I_1}), \cdot), (\rho_2^*(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}}; \zeta]\!]\rho'$$

Where $\mathbf{I_1}$ and $\mathbf{I_2}$ are defined by the value translation.
In order to do that, consider arbitrary E_1, E_2 such that

$$(W', E_1, E_2) \in \mathcal{K}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}}; \zeta]\!]\rho'$$

The definition of $\mathcal{E}[\![\cdot]\!]$ dictates we show that

$$(W', E_1[(\rho_1^*(\mathbf{I_1}), \cdot)], E_2[(\rho_2^*(\mathbf{I_2}), \cdot)]) \in \mathcal{O}$$

Expanding $\mathbf{I_i}$, we are considering:

$$E_i[(\mathtt{salloc}\ \mathbf{1}; \mathtt{sst}\ \mathbf{0}, \mathtt{ra}; \mathtt{import}\ \mathbf{r_1}, {}^{\rho_i^*(\zeta)}\mathcal{T}\mathcal{F}^{\rho_i^*(\tau')}\ \mathbf{e_i}; \mathtt{sld}\ \mathtt{ra}, \mathbf{0}; \mathtt{sfree}\ \mathbf{n{+}1}; \mathtt{ret}\ \mathtt{ra}\ \{\mathtt{r1}\}, \cdot)]$$

where

$$\mathbf{e_i} = \mathbf{v_i}^{\rho_i^*(\tau_i)}\mathcal{F}\mathcal{T}\ ((\mathtt{sld}\ \mathtt{r1}, \mathbf{n{-}j}; \mathtt{ret}\ \mathbf{end}\{\rho_i^*(\tau_j)^{\mathcal{T}}; \sigma\}\ \{\mathtt{r1}\}), \cdot)$$

and

$$\sigma = \rho_i^*(\forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\epsilon} :: \overline{\tau^{\mathcal{T}}} :: \zeta)$$

Consider arbitrary $(M_1, M_2) : W'$. From the definition of $\mathcal{O}$, we need to show that either both terms terminate or are both running after $W.k$ steps. From Lemma 3.7, we can take two steps and consider $\mathbf{M'_i}$ which is like $\mathbf{M_i}$ but has stack with type σ instead of σ', and W^* which has a corresponding stack island, noting that the values in the register $\mathtt{ra}$ are related from the condition on W', which means that $\text{currentMR}(W^*(i_{\text{stk}})) \Subset_{W^*} \mathcal{S}[\![\sigma]\!]\rho'$. Summarizing, we must now show:

$$(W^*, E_1[(\texttt{import r}_1, {}^{\rho_1^*(\zeta)}\mathcal{TF}^{\rho_1^*(\tau')}\ \mathbf{e_1}; \texttt{sld ra, 0; sfree n+1; ret ra \{r1\}}, \cdot)],\\ E_2[(\texttt{import r}_1, {}^{\rho_2^*(\zeta)}\mathcal{TF}^{\rho_2^*(\tau')}\ \mathbf{e_2}; \texttt{sld ra, 0; sfree n+1; ret ra \{r1\}}, \cdot)]) \in \mathcal{O}$$

Consider the sequence of evaluation contexts

$$E_i\left[\begin{array}{l}(\texttt{import r}_1, {}^{\rho_i^*(\zeta)}\mathcal{TF}^{\rho_i^*(\tau')}\ \mathbf{v_i}\overline{\mathbf{v_i'}} \\ \qquad\qquad {}^{\tau}\mathcal{FT}\ ([\cdot], \cdot) \\ \qquad\qquad \overline{{}^{\rho_i^*(\tau)}\mathcal{FT}\ ((\texttt{sld r1, n}-\texttt{j; ret end}\{\rho_i^*(\tau')^{\mathcal{T}}; \rho\}_i^*(\sigma)\ \{\texttt{r1}\}), \cdot)} \\ \texttt{sld ra, 0; sfree n+1; ret ra \{r1\}}, \cdot)\end{array}\right];$$

and target of reduction

$$\texttt{sld r1, n}-\texttt{j; ret end}\{\rho_i^*(\tau_j)^{\mathcal{T}}; \rho\}_i^*(\sigma)\ \{\texttt{r1}\}$$

where $\overline{\mathbf{v_i'}}$ starts empty and accumulates argument values in subsequent contexts. In order to step the target, we note that after one step the M_is have, in register r1, related values $\mathbf{w_{ji}}$ which have type $\rho_i^*(\tau_j)^{\mathcal{T}}$. This means that

$${}^{\rho_i^*(\tau_j)}\mathcal{FT}\ ((\texttt{ret end}\{\rho_i^*(\tau_j)^{\mathcal{T}}; \rho\}_i^*(\sigma)\ \{\texttt{r1}\}), \cdot)$$

reduces in another step to a $\mathbf{v_i'}$, defined and in $\mathcal{V}[\![\tau_j{}^{\mathcal{T}}]\!]\rho'$ by appealing to 2a on the structurally smaller type τ_j.
After 2n steps, we are in a world similar to W^*, denote W^{**} but with the register island having type $\tau_{n-1}{}^{\mathcal{T}}$ for register r1. We now must show that:

$$(W^{**}, E_1[(\texttt{import r}_1, {}^{\rho_1(\zeta)}\mathcal{TF}^{\rho_1(\tau')}\ \mathbf{v_1}\overline{\mathbf{v_1'}}; \texttt{sld ra, 0; sfree n+1; ret ra \{r1\}}, \cdot)],\\ E_2[(\texttt{import r}_1, {}^{\rho_2(\zeta)}\mathcal{TF}^{\rho_2(\tau')}\ \mathbf{v_2}\overline{\mathbf{v_2'}}; \texttt{sld ra, 0; sfree n+1; ret ra \{r1\}}, \cdot)]) \in \mathcal{O}$$

From $\mathbf{v_i}$ in the $\mathcal{V}[\![\cdot]\!]$ relation, we know that

$$\mathbf{v_i}\overline{\mathbf{v_i'}} \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \zeta]\!]\rho[\zeta \mapsto (\sigma, \sigma, \mathcal{S}[\![[\!]\sigma]\!]\rho)]$$

This means that for any chosen continuations E_1' and E_2' drawn from

$$\mathcal{K}[\![\mathbf{out} \vdash \tau'; \zeta]\!]\rho[\zeta \mapsto (\sigma, \sigma, \mathcal{S}[\![[\!]\sigma]\!]\rho)] = \mathcal{K}[\![\mathbf{out} \vdash \tau'; \sigma]\!]\rho$$

we will have that

$$(W^{**}, E_1'[\mathbf{v_1}\overline{\mathbf{v_1'}}], E_2'[\mathbf{v_2}\overline{\mathbf{v_2'}}]) \in \mathcal{O}$$

In particular, we will argue that

$$E_i' = E_i[(\texttt{import r}_1, {}^{\rho_1(\zeta)}\mathcal{TF}^{\rho_1(\tau')}\ [\cdot]; \texttt{sld ra, 0; sfree n+1; ret ra \{r1\}}, \cdot)]$$

are such continuations, which will complete the proof.
To show this, for any future world $W^f \sqsupseteq W^{**}$ such that

$$\text{currentMR}(W^f(i_{\text{stk}})) \Subset_{W^f} \mathcal{S}[\![\sigma]\!]\rho'$$

and any values $(W^f, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau']\!]\rho'$, we must show that

$$(W^f, E_1'[\mathtt{v_1}], E_2'[\mathtt{v_2}]) \in \mathcal{O}$$

In order to do that, consider $(M_1, M_2) : W^f$. The first step results in related values $\mathtt{w_1}$ and $\mathtt{w_2}$ being placed in register $\mathtt{r1}$, appealing to the inductive case of 2b for structurally smaller type τ'.
The next instruction results in register $\mathtt{ra}$ having, based on the stack island, related values with type $\forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\epsilon}$.
The next instruction results in the stack being composed of just ζ, which combined with the register typing means that we can appeal to the definition of E_i and get the desired result.

Case $(\overline{\tau}) \xrightarrow{\phi_i;\phi_o} \tau'$

To show that that (W, ℓ_1, ℓ_2) is in

$$\mathcal{W}[\![(\overline{\tau}) \xrightarrow{\phi_i;\phi_o} \tau'^{\mathcal{T}}]\!]\rho = \mathcal{W}[\![\mathbf{box}\,\forall[\zeta,\epsilon].\{\mathtt{ra} : \mathbf{box}\,\forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\epsilon}; \sigma'\}^{\mathtt{ra}}]\!]\rho$$

where $\sigma' = \tau_n{}^{\mathcal{T}} :: \cdots :: \tau_1{}^{\mathcal{T}} :: \phi_i :: \zeta$
we need to show that for any future world $\widetilde{W} \sqsupset W$, and any memories M_1, M_2 such that $(\widetilde{W}, M_1, M_2) \in \text{currentMR}(W(i_{\text{box}}))$, the following conditions hold:

- $M_i(\ell_i) = \mathbf{code}[\zeta,\epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \rho_i(\tau'^{\mathcal{T}}); \phi_o :: \zeta\}^{\epsilon}; \rho_i(\sigma')\}^{\mathtt{ra}}.\mathbf{I_i}$
- $(\widetilde{W}, M_1(\ell_1), M_2(\ell_2)) \in \mathcal{HV}[\![\forall[\zeta,\epsilon].\{\mathtt{ra} : \mathbf{box}\,\forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \phi_o :: \zeta\}^{\epsilon}; \sigma'\}^{\mathtt{ra}}]\!]\rho$

The latter requires that, in a further future world $W' \sqsupseteq \widetilde{W}$, with $\rho^* \in \mathcal{D}[\![\zeta,\epsilon]\!]$, letting $\rho' = \rho \cup \rho^*$, such that the world fulfills the following restrictions:

- $\text{currentMR}(W'(i_{\text{reg}})) \Subset_{W'} \mathcal{R}[\![\mathtt{ra} : \mathbf{box}\,\forall[].\{\mathtt{r1} : \rho_1(\tau'^{\mathcal{T}}); \phi_o :: \zeta\}^{\epsilon}]\!]\rho'$
- $\text{currentMR}(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\sigma']\!]\rho'$

We must show that

$$(W', (\rho_1^*(\mathbf{I_1}), \cdot), (\rho_2^*(\mathbf{I_2}), \cdot)) \in \mathcal{E}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}}; \phi_o :: \zeta]\!]\rho'$$

Where $\mathbf{I_1}$ and $\mathbf{I_2}$ are defined by the value translation.
In order to do that, consider arbitrary E_1, E_2 such that

$$(W', E_1, E_2) \in \mathcal{K}[\![\mathtt{ra} \vdash \tau'^{\mathcal{T}}; \phi_o :: \zeta]\!]\rho'$$

The definition of $\mathcal{E}[\![\cdot]\!]$ dictates we show that

$$(W', E_1[(\rho_1^*(\mathbf{I_1}), \cdot)], E_2[(\rho_2^*(\mathbf{I_2}), \cdot)]) \in \mathcal{O}$$

Expanding $\mathbf{I_i}$, we are considering:

$E_i[\mathtt{salloc}\ 1{+}|\phi_i|; \mathtt{sst}\ |\phi_i|, \mathtt{ra};$
$\mathtt{sld}\ \mathtt{r1}, |\phi_i| + \mathbf{n}; \mathtt{sst}\ \mathbf{1}, \mathtt{r1}; \ldots; \mathtt{sld}\ \mathtt{r1}, |\phi_i| + \mathbf{n} + |\phi_i| - \mathbf{1}; \mathtt{sst}\ |\phi_i|, \mathtt{r1};$
$\mathtt{import}\ \mathbf{r_1}, {}^{\zeta}\mathcal{T}\mathcal{F}^{\tau'}\ \mathbf{e};$
$\mathtt{sld}\ \mathtt{ra}, |\phi_o|;$
$\mathtt{sld}\ \mathtt{r2}, |\phi_o|{-}\mathbf{1}; \mathtt{sst}\ |\phi_o|{+}\mathbf{n}{+}|\phi_i| - \mathbf{1}, \mathtt{r2}; \ldots; \mathtt{sld}\ \mathtt{r2}, \mathbf{0}; \mathtt{sst}\ |\phi_o|{+}\mathbf{n}{+}|\phi_i|{-}|\mathbf{pref_o}|, \mathtt{r2};$
$\mathtt{sfree}\ \mathbf{n}{+}|\phi_o|{+}\mathbf{1}; \mathtt{ret}\ \mathtt{ra}\ \{\mathtt{r1}\}]$

where

$$\mathbf{e_i} = \mathbf{v_i}^{\overline{\rho_i^*(\tau_j)\mathcal{F}\mathcal{T}}}((\mathtt{sld}\ \mathtt{r1}, |\phi_i|{+}\mathbf{n}{-}\mathbf{j}; \mathtt{ret}\ \mathbf{end}\{\rho_i^*(\tau_j)^{\mathcal{T}}; \sigma\}\ \{\mathtt{r1}\}), \cdot)$$

and

$$\sigma = \rho_i^*(\phi_i :: \forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\epsilon} :: \overline{\tau^{\mathcal{T}}} :: \zeta)$$

Consider arbitrary $(M_1, M_2) : W'$. From the definition of $\mathcal{O}$, we need to show that either both terms terminate or are both running after $W.k$ steps. From Lemma 3.7, we can take $2 + 2 * |\phi_i|$ steps and consider $\mathbf{M_i'}$ which is like $\mathbf{M_i}$ but has stack with type $\boldsymbol{\sigma}$ instead of $\boldsymbol{\sigma'}$, and W^* which has a corresponding stack island, noting that the values in the register ra are related from the condition on W', and the rest of the instructions are moving related values from one point of the stack to another. This means that currentMR$(W^*(i_{\text{stk}})) \Subset_{W^*} \mathcal{S}[\![\boldsymbol{\sigma}]\!]\rho'$. Summarizing, we must now show:

$$(W^*, E_1[(\texttt{import r}_1, {}^{\rho_1^*(\zeta)}\mathcal{T}\mathcal{F}^{\rho_1^*(\tau')}\ \mathbf{e_1}; \ldots; \texttt{ret ra}\ \{\texttt{r1}\}, \cdot)],\\ E_2[(\texttt{import r}_1, {}^{\rho_2^*(\zeta)}\mathcal{T}\mathcal{F}^{\rho_2^*(\tau')}\ \mathbf{e_2}; \ldots; \texttt{ret ra}\ \{\texttt{r1}\}, \cdot)]) \in \mathcal{O}$$

Consider the sequence of evaluation contexts

$$E_i[(\texttt{import r}_1, {}^{\rho_i^*(\zeta)}\mathcal{T}\mathcal{F}^{\rho_i^*(\tau')}\ \mathbf{v_i}\overline{\mathbf{v_i'}}^{\tau}\mathcal{F}\mathcal{T}\ ([\cdot], \cdot)\overline{{}^{\rho_i^*(\tau)}\mathcal{F}\mathcal{T}\ ((\texttt{sld .,} \ldots; \texttt{ret end}\{\boldsymbol{\rho_i^*(\tau')}^{\mathcal{T}}; \boldsymbol{\rho_i^*(\sigma)}\}\ \{\texttt{r1}\}), \cdot)};$$

$$\ldots; \texttt{ret ra}\ \{\texttt{r1}\}, \cdot)]$$

and target of reduction

$$\texttt{sld r1}, |\phi_i| + \mathbf{n} - \mathbf{j}; \texttt{ret end}\{\boldsymbol{\rho_i^*(\tau_j)}^{\mathcal{T}}; \boldsymbol{\rho}\}_i^*(\boldsymbol{\sigma})\ \{\texttt{r1}\}$$

where $\overline{\mathbf{v_i'}}$ starts empty and accumulates argument values in subsequent contexts. In order to step the target, we note that after one step the M_is have, in register r1, related values $\mathbf{w_{ji}}$ which have type $\boldsymbol{\rho_i^*(\tau_j)}^{\mathcal{T}}$. This means that

$${}^{\rho_i^*(\tau_j)}\mathcal{F}\mathcal{T}\ ((\texttt{ret end}\{\boldsymbol{\rho_i^*(\tau_j)}^{\mathcal{T}}; \boldsymbol{\rho}\}_i^*(\boldsymbol{\sigma})\ \{\texttt{r1}\}), \cdot)$$

reduces in another step to a $\mathbf{v_i'}$, defined and in $\mathcal{V}[\![\boldsymbol{\tau_j}^{\mathcal{T}}]\!]\rho'$ by appealing to 2a on the structurally smaller type $\boldsymbol{\tau_j}$.
After 2n steps, we are in a world similar to W^*, denote W^{**} but with the register island having type $\boldsymbol{\tau_n}^{\mathcal{T}}$ for register r1. We now must show that:

$$(W^{**}, E_1[(\texttt{import r}_1, {}^{\rho_1(\zeta)}\mathcal{T}\mathcal{F}^{\rho_1(\tau')}\ \mathbf{v_1}\overline{\mathbf{v_1'}}; \ldots; \texttt{ret ra}\ \{\texttt{r1}\}, \cdot)],\\ E_2[(\texttt{import r}_1, {}^{\rho_2(\zeta)}\mathcal{T}\mathcal{F}^{\rho_2(\tau')}\ \mathbf{v_2}\overline{\mathbf{v_2'}}; \ldots; \texttt{ret ra}\ \{\texttt{r1}\}, \cdot)]) \in \mathcal{O}$$

From $\mathbf{v_i}$ in the $\mathcal{V}[\![\cdot]\!]$ relation, we know that

$$\mathbf{v_i}\overline{\mathbf{v_i'}} \in \mathcal{E}[\![\mathbf{out} \vdash \boldsymbol{\tau'}; \boldsymbol{\phi_o} :: \boldsymbol{\zeta}]\!]\rho[\boldsymbol{\zeta} \mapsto \text{SR}]$$

for any SR, and in particular, for $\text{SR} = (\boldsymbol{\sigma''}, \boldsymbol{\sigma''}, \mathcal{S}[\![\boldsymbol{\sigma''}]\!]\rho)$ where $\sigma'' = \forall[].\{\texttt{r1} : \boldsymbol{\tau'}^{\mathcal{T}}; \boldsymbol{\zeta}\}^{\epsilon} :: \overline{\boldsymbol{\tau}^{\mathcal{T}}} :: \boldsymbol{\zeta}$.
This means that for any chosen continuations E_1' and E_2' drawn from

$$\mathcal{K}[\![\mathbf{out} \vdash \boldsymbol{\tau'}; \boldsymbol{\phi_o} :: \boldsymbol{\zeta}]\!]\rho[\boldsymbol{\zeta} \mapsto (\boldsymbol{\sigma''}, \boldsymbol{\sigma''}, \mathcal{S}[\![\boldsymbol{\sigma''}]\!]\rho)] = \mathcal{K}[\![\mathbf{out} \vdash \boldsymbol{\tau'}; \boldsymbol{\phi_o} :: \boldsymbol{\sigma''}]\!]\rho$$

we will have that

$$(W^{**}, E_1'[\mathbf{v_1}\overline{\mathbf{v_1'}}], E_2'[\mathbf{v_2}\overline{\mathbf{v_2'}}]) \in \mathcal{O}$$

In particular, we will argue that

$$E_i' = E_i[(\texttt{import r}_1, {}^{\rho_1(\zeta)}\mathcal{T}\mathcal{F}^{\rho_1(\tau')}\ [\cdot];\\ \texttt{sld ra}, |\phi_o|;\\ \texttt{sld r2}, |\phi_o| - \mathbf{1}; \texttt{sst}\ |\phi_o| + \mathbf{n} + |\phi_i| - \mathbf{1}, \texttt{r2}; \ldots; \texttt{sld r2}, \mathbf{0}; \texttt{sst}\ |\phi_o| + \mathbf{n} + |\phi_i| - |\mathbf{pref_o}|, \texttt{r2};\\ \texttt{sfree}\ \mathbf{n} + |\phi_o| + \mathbf{1}; \texttt{ret ra}\ \{\texttt{r1}\}, \cdot)]$$

are such continuations, which will complete the proof.
To show this, for any future world $W^f \sqsupseteq W^{**}$ such that currentMR$(W^f(i_{\text{stk}})) \Subset_{W^f} \mathcal{S}[\![\phi_o :: \sigma'']\!]\rho'$, and any values $(W^f, \mathtt{v_1}, \mathtt{v_2}) \in \mathcal{V}[\![\tau']\!]\rho'$, we must show that

$$(W^f, E_1'[\mathtt{v_1}], E_2'[\mathtt{v_2}]) \in \mathcal{O}$$

In order to do that, consider $(M_1, M_2) : W^f$. The first step results in related values $\mathtt{w_1}$ and $\mathtt{w_2}$ being placed in register $\mathtt{r1}$, appealing to the inductive case of 2b for structurally smaller type τ'.
The next instruction results in register $\mathtt{ra}$ having, based on the stack island, related values with type $\forall[].\{\mathtt{r1} : \tau'^{\mathcal{T}}; \zeta\}^{\epsilon}$.
The next $2 * |\phi_o| + 1$ instructions result in the stack being composed of $\phi_o :: \zeta$, based on the related values on the stack specified by the constraint on the world, and the freeing of part of the stack.
Combined with the register typing, this means that we can appeal to the definition of E_i and get the desired result.

□

3.6 Compatibility Lemmas

NOTE: The proofs for TAL terms in the multi-language F+T are elided below since they are essentially the same as the proofs for the corresponding compatibility lemmas for T.

Lemma 3.29 (Component)
If $\Psi \vdash \mathbf{H_1} \approx_{\mathrm{H}} \mathbf{H_2} : \Psi'$, boxheap($\Psi'$), ret-type$(\mathbf{q}, \chi, \sigma) = \tau; \sigma'$, and $(\Psi, \Psi'); \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathrm{I}} \mathbf{I_2}$, then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash (\mathbf{I_1}, \mathbf{H_1}) \approx (\mathbf{I_2}, \mathbf{H_2}) : \tau; \sigma'$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.30 (Heap Fragment)
Let $\cdot \vdash \psi_1, \ldots, \cdots \vdash \psi_n$ and $\Psi' = \ell_1 : {}^{\nu_1}\psi_1, \ldots, \ell_n : {}^{\nu_n}\psi_n$ such that $\mathrm{dom}(\Psi) \cap \mathrm{dom}(\Psi') = \emptyset$. If for each i, we have $\Psi, \Psi' \vdash \mathbf{h_{1i}} \approx_{\mathrm{hv}} \mathbf{h_{2i}} : {}^{\nu_i}\psi_i$, then $\Psi \vdash \ell_1 \mapsto \mathbf{h_{11}}, \ldots \ell_n \mapsto \mathbf{h_{1n}} \approx_{\mathrm{H}} \ell_1 \mapsto \mathbf{h_{21}}, \ldots \ell_n \mapsto \mathbf{h_{2n}} : \Psi'$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.31 (Code Block)
If $\cdot \vdash \forall[\Delta].\{\chi; \sigma\}^{\mathbf{q}}$ and $\Psi; \Delta; \cdot; \chi; \sigma; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathrm{I}} \mathbf{I_2}$, then
$\Psi \vdash \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{I_1} \approx_{\mathrm{hv}} \mathbf{code}[\Delta]\{\chi; \sigma\}^{\mathbf{q}}.\mathbf{I_2} : {}^{\mathbf{box}}\forall[\Delta].\{\chi; \sigma\}^{\mathbf{q}}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.32 (Tuple)
If for each i, we have $\Psi; \cdot \vdash \mathbf{w_{1i}} \approx_{\mathrm{w}} \mathbf{w_{2i}} : \tau_i$, then $\Psi \vdash \langle \mathbf{w_{10}}, \ldots, \mathbf{w_{1n}} \rangle \approx_{\mathrm{hv}} \langle \mathbf{w_{20}}, \ldots, \mathbf{w_{2n}} \rangle : {}^{\nu}\langle \tau_0, \ldots, \tau_n \rangle$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.33 (Unit)
$\Psi; \Delta \vdash () \approx_{\mathrm{w}} () : \mathbf{unit}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.34 (Integer)
$\Psi; \Delta \vdash \mathbf{n} \approx_{\mathrm{w}} \mathbf{n} : \mathbf{int}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.35 (Mutable Location)
If $\ell : {}^{\mathbf{ref}}\psi \in \Psi$, then $\Psi; \Delta \vdash \ell \approx_{\mathrm{w}} \ell : \mathbf{ref}\ \psi$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.36 (Immutable Location)
If $\ell : {}^{\mathbf{box}}\psi \in \Psi$, then $\Psi; \Delta \vdash \ell \approx_{\mathrm{w}} \ell : \mathbf{box}\ \psi$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.37 (Pack)
If $\Psi; \Delta \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \tau[\tau'/\alpha]$, then $\Psi; \Delta \vdash \mathbf{pack}\langle \tau', \mathbf{w_1} \rangle \,\mathbf{as}\, \exists \alpha.\tau \approx_{\mathrm{w}} \mathbf{pack}\langle \tau', \mathbf{w_2} \rangle \,\mathbf{as}\, \exists \alpha.\tau : \exists \alpha.\tau$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.38 (Fold)
If $\Psi; \Delta \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \tau[\mu\alpha.\tau/\alpha]$, then $\Psi; \Delta \vdash \mathbf{fold}_{\mu\alpha.\tau}\, \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{fold}_{\mu\alpha.\tau}\, \mathbf{w_2} : \mu\alpha.\tau$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.39 (Word Type Application)
If $\Psi; \Delta \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \mathbf{box}\, \forall[\alpha, \Delta'].\{\chi; \sigma\}^{\mathrm{q}}$ and $\Delta \vdash \tau$, then

$$\Psi; \Delta \vdash \mathbf{w_1}[\tau] \approx_{\mathrm{w}} \mathbf{w_2}[\tau] : \mathbf{box}\, \forall[\Delta'].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{\mathrm{q}[\tau/\alpha]}.$$

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.40 (Stack Type Application)
If $\Psi; \Delta \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \mathbf{box}\, \forall[\zeta, \Delta'].\{\chi; \sigma\}^{\mathrm{q}}$ and $\Delta \vdash \sigma'$, then

$$\Psi; \Delta \vdash \mathbf{w_1}[\sigma'] \approx_{\mathrm{w}} \mathbf{w_2}[\sigma'] : \mathbf{box}\, \forall[\Delta'].\{\chi[\sigma'/\zeta]; \sigma[\sigma'/\zeta]\}^{\mathrm{q}[\sigma'/\zeta]}.$$

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.41 (Return Marker Type Application)
If $\Psi; \Delta \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \mathbf{box}\, \forall[\epsilon, \Delta'].\{\chi; \sigma\}^{\mathrm{q}}$, $\mathrm{ftv}(\mathrm{q}') \subseteq \Delta$, and $\Delta \vdash \forall[\Delta'].\{\chi[\mathrm{q}'/\epsilon]; \sigma[\mathrm{q}'/\epsilon]\}^{\mathrm{q}[\mathrm{q}'/\epsilon]}$, then

$$\Psi; \Delta \vdash \mathbf{w_1}[\mathrm{q}'] \approx_{\mathrm{w}} \mathbf{w_2}[\mathrm{q}'] : \mathbf{box}\, \forall[\Delta'].\{\chi[\mathrm{q}'/\epsilon]; \sigma[\mathrm{q}'/\epsilon]\}^{\mathrm{q}[\mathrm{q}'/\epsilon]}.$$

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.42 (Word Value)
If $\Psi; \Delta \vdash \mathbf{w_1} \approx_{\mathrm{w}} \mathbf{w_2} : \tau$, then $\Psi; \Delta; \chi \vdash \mathbf{w_1} \approx_{\mathrm{u}} \mathbf{w_2} : \tau$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.43 (Register)
If $\mathbf{r} : \tau \in \chi$, then $\Psi; \Delta; \chi \vdash \mathbf{r} \approx_{\mathrm{u}} \mathbf{r} : \tau$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.44 (Pack)
If $\Psi; \Delta; \chi \vdash \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{u_2} : \tau[\tau'/\alpha]$, then $\Psi; \Delta; \chi \vdash \mathbf{pack}\langle \tau', \mathbf{u_1} \rangle \,\mathbf{as}\, \exists \alpha.\tau \approx_{\mathrm{u}} \mathbf{pack}\langle \tau', \mathbf{u_2} \rangle \,\mathbf{as}\, \exists \alpha.\tau : \exists \alpha.\tau$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.45 (Fold)
If $\Psi; \Delta; \chi \vdash \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{u_2} : \tau[\mu\alpha.\tau/\alpha]$, then $\Psi; \Delta; \chi \vdash \mathbf{fold}_{\mu\alpha.\tau}\, \mathbf{u_1} \approx_{\mathrm{u}} \mathbf{fold}_{\mu\alpha.\tau}\, \mathbf{u_2} : \mu\alpha.\tau$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.46 (Word Type Application)
If $\Psi; \Delta; \chi \vdash u_1 \approx_u u_2 : \mathbf{box}\,\forall[\alpha, \Delta'].\{\chi; \sigma\}^q$ and $\Delta \vdash \tau$, then

$$\Psi; \Delta; \chi \vdash u_1[\tau] \approx_u u_2[\tau] : \mathbf{box}\,\forall[\Delta'].\{\chi[\tau/\alpha]; \sigma[\tau/\alpha]\}^{q[\tau/\alpha]}.$$

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.47 (Stack Type Application)
If $\Psi; \Delta; \chi \vdash u_1 \approx_u u_2 : \mathbf{box}\,\forall[\zeta, \Delta'].\{\chi; \sigma\}^q$ and $\Delta \vdash \sigma'$, then

$$\Psi; \Delta; \chi \vdash u_1[\sigma'] \approx_u u_2[\sigma'] : \mathbf{box}\,\forall[\Delta'].\{\chi[\sigma'/\zeta]; \sigma[\sigma'/\zeta]\}^{q[\sigma'/\zeta]}.$$

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.48 (Return Marker Type Application)
If $\Psi; \Delta; \chi \vdash u_1 \approx_u u_2 : \mathbf{box}\,\forall[\epsilon, \Delta'].\{\chi; \sigma\}^q$, $\mathrm{ftv}(q') \subseteq \Delta$, and $\Delta \vdash \forall[\Delta'].\{\chi[q'/\epsilon]; \sigma[q'/\epsilon]\}^{q[q'/\epsilon]}$, then

$$\Psi; \Delta; \chi \vdash u_1[q'] \approx_u u_2[q'] : \mathbf{box}\,\forall[\Delta'].\{\chi[q'/\epsilon]; \sigma[q'/\epsilon]\}^{q[q'/\epsilon]}.$$

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.49 (Arithmetic Operation)
If $\Psi; \Delta; \chi \vdash r_{s1} \approx_u r_{s2} : \mathbf{int}$, $\Psi; \Delta; \chi \vdash u_1 \approx_u u_2 : \mathbf{int}$, $q \neq r_d$, and $\Psi; \Delta; \Gamma; \chi[r_d : \mathbf{int}]; \sigma; q \vdash I_1 \approx_I I_2$, then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathbf{aop}\ r_d, r_{s1}, u_1; I_1 \approx_I \mathbf{aop}\ r_d, r_{s2}, u_2; I_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.50 (Branch)
If $\Psi; \Delta; \chi \vdash r_1 \approx_u r_2 : \mathbf{int}$, $\Psi; \Delta; \chi \vdash u_1 \approx_u u_2 : \mathbf{box}\,\forall[].\{\chi'; \sigma\}^q$, $\Delta \vdash \chi \leq \chi'$, and $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash I_1 \approx_I I_2$, then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathtt{bnz}\ r_1, u_1; I_1 \approx_I \mathtt{bnz}\ r_2, u_2; I_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.51 (Load from Mutable Tuple)
If $\Psi; \Delta; \chi \vdash r_{s1} \approx_u r_{s2} : \mathbf{ref}\,\langle \tau_0, \ldots, \tau_n \rangle$, $0 \leq i \leq n$, $q \neq r_d$, and $\Psi; \Delta; \Gamma; \chi[r_d : \tau_i]; \sigma; q \vdash I_1 \approx_I I_2$, then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathtt{ld}\ r_d, r_{s1}[i]; I_1 \approx_I \mathtt{ld}\ r_d, r_{s2}[i]; I_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.52 (Load from Immutable Tuple)
If $\Psi; \Delta; \chi \vdash r_{s1} \approx_u r_{s2} : \mathbf{box}\,\langle \tau_0, \ldots, \tau_n \rangle$, $0 \leq i \leq n$, $q \neq r_d$, and $\Psi; \Delta; \Gamma; \chi[r_d : \tau_i]; \sigma; q \vdash I_1 \approx_I I_2$, then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathtt{ld}\ r_d, r_{s1}[i]; I_1 \approx_I \mathtt{ld}\ r_d, r_{s2}[i]; I_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.53 (Store to Mutable Tuple)
If $\Psi; \Delta; \chi \vdash \mathrm{r_{d1}} \approx_{\mathrm{u}} \mathrm{r_{d2}} : \mathrm{ref}\,\langle \tau_0, \ldots, \tau_n \rangle$, $0 \leq i \leq n$, $\Psi; \Delta; \chi \vdash \mathrm{r_{s1}} \approx_{\mathrm{u}} \mathrm{r_{s2}} : \tau_i$, and $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathrm{I_1} \approx_{\mathrm{I}} \mathrm{I_2}$, then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathtt{st}\,\mathrm{r_{d1}}[i], \mathrm{r_{s1}}; \mathrm{I_1} \approx_{\mathrm{I}} \mathtt{st}\,\mathrm{r_{d2}}[i], \mathrm{r_{s2}}; \mathrm{I_2}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.54 (Allocate Mutable Tuple)
If $\mathrm{len}(\overline{\tau}) = n$, $q \neq \mathrm{r_d}$, and $\Psi; \Delta; \Gamma; \chi[\mathrm{r_d} : \mathrm{ref}\,\langle \overline{\tau} \rangle]; \sigma; \mathrm{dec}(q, n) \vdash \mathrm{I_1} \approx_{\mathrm{I}} \mathrm{I_2}$,
then $\Psi; \Delta; \Gamma; \chi; \overline{\tau} :: \sigma; q \vdash \mathtt{ralloc}\,\mathrm{r_d}, n; \mathrm{I_1} \approx_{\mathrm{I}} \mathtt{ralloc}\,\mathrm{r_d}, n; \mathrm{I_2}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.55 (Allocate Immutable Tuple)
If $\mathrm{len}(\overline{\tau}) = n$, $q \neq \mathrm{r_d}$, and $\Psi; \Delta; \Gamma; \chi[\mathrm{r_d} : \mathrm{box}\,\langle \overline{\tau} \rangle]; \sigma; \mathrm{dec}(q, n) \vdash \mathrm{I_1} \approx_{\mathrm{I}} \mathrm{I_2}$,
then $\Psi; \Delta; \Gamma; \chi; \overline{\tau} :: \sigma; q \vdash \mathtt{balloc}\,\mathrm{r_d}, n; \mathrm{I_1} \approx_{\mathrm{I}} \mathtt{balloc}\,\mathrm{r_d}, n; \mathrm{I_2}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.56 (Move)
If $\Psi; \Delta; \chi \vdash u_1 \approx_{\mathrm{u}} u_2 : \tau$, $q \neq \mathrm{r_d}$, and $\Psi; \Delta; \Gamma; \chi[\mathrm{r_d} : \tau]; \sigma; q \vdash \mathrm{I_1} \approx_{\mathrm{I}} \mathrm{I_2}$,
then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathtt{mv}\,\mathrm{r_d}, u_1; \mathrm{I_1} \approx_{\mathrm{I}} \mathtt{mv}\,\mathrm{r_d}, u_2; \mathrm{I_2}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.57 (Move Return Address)
If $\chi(\mathrm{r_s}) = \tau$ and $\Psi; \Delta; \Gamma; \chi[\mathrm{r_d} : \tau]; \sigma; \mathrm{r_d} \vdash \mathrm{I_1} \approx_{\mathrm{I}} \mathrm{I_2}$, then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{r_s} \vdash \mathtt{mv}\,\mathrm{r_d}, \mathrm{r_s}; \mathrm{I_1} \approx_{\mathrm{I}} \mathtt{mv}\,\mathrm{r_d}, \mathrm{r_s}; \mathrm{I_2}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.58 (Unpack)
If $\Psi; \Delta; \chi \vdash u_1 \approx_{\mathrm{u}} u_2 : \exists \alpha.\tau$, $q \neq \mathrm{r_d}$, and $\Psi; \Delta, \alpha; \Gamma; \chi[\mathrm{r_d} : \tau]; \sigma; q \vdash \mathrm{I_1} \approx_{\mathrm{I}} \mathrm{I_2}$,
then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathtt{unpack}\,\langle \alpha, \mathrm{r_d} \rangle\ u_1; \mathrm{I_1} \approx_{\mathrm{I}} \mathtt{unpack}\,\langle \alpha, \mathrm{r_d} \rangle\ u_2; \mathrm{I_2}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.59 (Unfold)
If $\Psi; \Delta; \chi \vdash u_1 \approx_{\mathrm{u}} u_2 : \mu\alpha.\tau$, $q \neq \mathrm{r_d}$, and $\Psi; \Delta; \Gamma; \chi[\mathrm{r_d} : \tau[\mu\alpha.\tau/\alpha]]; \sigma; q \vdash \mathrm{I_1} \approx_{\mathrm{I}} \mathrm{I_2}$,
then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathtt{unfold}\,\mathrm{r_d}, u_1; \mathrm{I_1} \approx_{\mathrm{I}} \mathtt{unfold}\,\mathrm{r_d}, u_2; \mathrm{I_2}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.60 (Allocate Stack Space)
If $\Psi; \Delta; \Gamma; \chi; \mathrm{unit} :: \cdots^{n} :: \mathrm{unit} :: \sigma; \mathrm{inc}(q, n) \vdash \mathrm{I_1} \approx_{\mathrm{I}} \mathrm{I_2}$, then $\Psi; \Delta; \Gamma; \chi; \sigma; q \vdash \mathtt{salloc}\,n; \mathrm{I_1} \approx_{\mathrm{I}} \mathtt{salloc}\,n; \mathrm{I_2}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.61 (Free Stack Space)
If $\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{dec}(\mathrm{q}, \mathrm{n}) \vdash \mathrm{I}_1 \approx_{\mathrm{I}} \mathrm{I}_2$, then $\Psi; \Delta; \Gamma; \chi; \tau_0 :: \cdots :: \tau_{\mathrm{n}-1} :: \sigma; \mathrm{q} \vdash \mathtt{sfree}\ \mathrm{n}; \mathrm{I}_1 \approx_{\mathrm{I}} \mathtt{sfree}\ \mathrm{n}; \mathrm{I}_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.62 (Load from Stack)
If $\sigma(\mathrm{i}) = \tau$, $\mathrm{q} \neq \mathrm{r}_\mathrm{d}$, and $\Psi; \Delta; \Gamma; \chi[\mathrm{r}_\mathrm{d} : \tau_\mathrm{i}]; \sigma; \mathrm{q} \vdash \mathrm{I}_1 \approx_{\mathrm{I}} \mathrm{I}_2$, then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \mathtt{sld}\ \mathrm{r}_\mathrm{d}, \mathrm{i}; \mathrm{I}_1 \approx_{\mathrm{I}} \mathtt{sld}\ \mathrm{r}_\mathrm{d}, \mathrm{i}; \mathrm{I}_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.63 (Load Return Address from Stack)
If $\sigma(\mathrm{i}) = \tau_i$ and $\Psi; \Delta; \Gamma; \chi[\mathrm{r}_\mathrm{d} : \tau_\mathrm{i}]; \sigma; \mathrm{r}_\mathrm{d} \vdash \mathrm{I}_1 \approx_{\mathrm{I}} \mathrm{I}_2$, then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{i} \vdash \mathtt{sld}\ \mathrm{r}_\mathrm{d}, \mathrm{i}; \mathrm{I}_1 \approx_{\mathrm{I}} \mathtt{sld}\ \mathrm{r}_\mathrm{d}, \mathrm{i}; \mathrm{I}_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.64 (Store to Stack)
If $\Psi; \Delta; \chi \vdash \mathrm{r}_{\mathrm{s}1} \approx_{\mathrm{u}} \mathrm{r}_{\mathrm{s}2} : \tau'$, $\mathrm{q} \neq \mathrm{i}$, and $\Psi; \Delta; \Gamma; \chi; \tau_0 :: \cdots :: \tau_{\mathrm{i}-1} :: \tau' :: \sigma; \mathrm{q} \vdash \mathrm{I}_1 \approx_{\mathrm{I}} \mathrm{I}_2$,
then $\Psi; \Delta; \Gamma; \chi; \tau_0 :: \cdots :: \tau_\mathrm{i} :: \sigma; \mathrm{q} \vdash \mathtt{sst}\ \mathrm{i}, \mathrm{r}_{\mathrm{s}1}; \mathrm{I}_1 \approx_{\mathrm{I}} \mathtt{sst}\ \mathrm{i}, \mathrm{r}_{\mathrm{s}2}; \mathrm{I}_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.65 (Store Return Address to Stack)
If $\chi(\mathrm{r}_\mathrm{s}) = \tau'$ and $\Psi; \Delta; \Gamma; \chi; \tau_0 :: \cdots :: \tau_{\mathrm{i}-1} :: \tau' :: \sigma; \mathrm{i} \vdash \mathrm{I}_1 \approx_{\mathrm{I}} \mathrm{I}_2$,
then $\Psi; \Delta; \Gamma; \chi; \tau_0 :: \cdots :: \tau_\mathrm{i} :: \sigma; \mathrm{r}_\mathrm{s} \vdash \mathtt{sst}\ \mathrm{i}, \mathrm{r}_\mathrm{s}; \mathrm{I}_1 \approx_{\mathrm{I}} \mathtt{sst}\ \mathrm{i}, \mathrm{r}_\mathrm{s}; \mathrm{I}_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.66 (Return from Call)
If $\chi(\mathrm{r}) = \mathrm{box}\,\forall[].\{\mathrm{r}' : \tau; \sigma\}^{\mathrm{q}'}$ and $\chi(\mathrm{r}') = \tau$, then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{r} \vdash \mathtt{ret}\ \mathrm{r}\ \{\mathrm{r}'\} \approx_{\mathrm{I}} \mathtt{ret}\ \mathrm{r}\ \{\mathrm{r}'\}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.67 (Return at End)
If $\chi(\mathrm{r}) = \tau$, then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{end}\{\tau; \sigma\} \vdash \mathtt{ret}\ \mathrm{end}\{\tau; \sigma\}\ \{\mathrm{r}\} \approx_{\mathrm{I}} \mathtt{ret}\ \mathrm{end}\{\tau; \sigma\}\ \{\mathrm{r}\}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.68 (Jump)
If $\Psi; \Delta; \chi \vdash \mathrm{u}_1 \approx_{\mathrm{u}} \mathrm{u}_2 : \mathrm{box}\,\forall[].\{\chi'; \sigma\}^{\mathrm{q}}$, $\Delta \vdash \chi \leq \chi'$, and $\cdot[\Delta]; \chi; \sigma \vdash \mathrm{q}$,
then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathrm{q} \vdash \mathtt{jmp}\ \mathrm{u}_1 \approx_{\mathrm{I}} \mathtt{jmp}\ \mathrm{u}_2$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.69 (Call)
Given the following:

- $\Psi; \Delta; \chi \vdash \mathrm{u}_1 \approx_{\mathrm{u}} \mathrm{u}_2 : \mathrm{box}\,\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathrm{q}}}$,

- ret-addr-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \forall[].\{\mathbf{r} : \tau; \hat{\sigma}'\}^{\epsilon}$,
- $\Delta \vdash \sigma_0$,
- $\Delta \vdash \forall[].\{\hat{\chi}[\sigma_0/\zeta][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]; \hat{\sigma}[\sigma_0/\zeta][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]\}^{\hat{\mathbf{q}}}$,
- $\Delta \vdash \chi \leq \hat{\chi}[\sigma_0/\zeta][(\mathbf{i}+\mathbf{k}-\mathbf{j})/\epsilon]$,
- $\sigma = \tau_0 :: \cdots :: \tau_{\mathbf{j}} :: \sigma_0$,
- $\hat{\sigma} = \tau_0 :: \cdots :: \tau_{\mathbf{j}} :: \zeta$,
- $\mathbf{j} < \mathbf{i}$, and
- $\hat{\sigma}' = \tau'_0 :: \cdots :: \tau'_{\mathbf{k}} :: \zeta$,

we have that $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{i} \vdash \texttt{call}\ \mathbf{u}_1\ \{\sigma_0, \mathbf{i}+\mathbf{k}-\mathbf{j}\} \approx_{\mathbf{I}} \texttt{call}\ \mathbf{u}_2\ \{\sigma_0, \mathbf{i}+\mathbf{k}-\mathbf{j}\}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.70 (Call from Top Level)
Given the following:

- $\Psi; \Delta; \chi \vdash \mathbf{u}_1 \approx_{\mathrm{u}} \mathbf{u}_2 : \mathbf{box}\,\forall[\zeta, \epsilon].\{\hat{\chi}; \hat{\sigma}\}^{\hat{\mathbf{q}}}$,
- ret-addr-type$(\hat{\mathbf{q}}, \hat{\chi}, \hat{\sigma}) = \forall[].\{\mathbf{r} : \tau; \hat{\sigma}'\}^{\epsilon}$,
- $\Delta \vdash \sigma_0$,
- $\Delta \vdash \forall[].\{\hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]; \hat{\sigma}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]\}^{\hat{\mathbf{q}}}$,
- $\Delta \vdash \chi \leq \hat{\chi}[\sigma_0/\zeta][\mathbf{end}\{\tau^*; \sigma^*\}/\epsilon]$,
- $\sigma = \overline{\tau} :: \sigma_0$,
- $\hat{\sigma} = \overline{\tau} :: \zeta$, and
- $\hat{\sigma}' = \overline{\tau'} :: \zeta$,

we have that $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{end}\{\tau^*; \sigma^*\} \vdash \texttt{call}\ \mathbf{u}_1\ \{\sigma_0, \mathbf{end}\{\tau^*; \sigma^*\}\} \approx_{\mathbf{I}} \texttt{call}\ \mathbf{u}_2\ \{\sigma_0, \mathbf{end}\{\tau^*; \sigma^*\}\}$.

Proof

Analogous to proof of corresponding compatibility lemma for T. □

Lemma 3.71 (Import)
Given the following:

- $\Psi; \Delta; \Gamma; \chi; \tau_0 :: \cdots :: \tau_{\mathbf{j}} :: \zeta; \mathbf{out} \vdash \mathbf{e}_1 \approx \mathbf{e}_2 : \tau; \tau'_0 :: \cdots :: \tau'_{\mathbf{k}} :: \zeta$,
- $\sigma = \tau_0 :: \cdots :: \tau_{\mathbf{j}} :: \sigma_0$,
- $\sigma' = \tau'_0 :: \cdots :: \tau'_{\mathbf{k}} :: \sigma_0$,
- $\mathbf{q} = \mathbf{i} > \mathbf{j}$ or $\mathbf{q} = \mathbf{end}\{\hat{\tau}; \hat{\sigma}\}$,
- $\Psi; \Delta; \chi[\mathbf{r}_{\mathbf{d}} : \tau^{\tau}]; \sigma'; \mathrm{inc}(\mathbf{q}, \mathbf{k}-\mathbf{j}) \vdash \mathbf{I}_1 \approx_{\mathbf{I}} \mathbf{I}_2$,

we have that $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \texttt{import}\ \mathbf{r}_{\mathbf{d}}, {}^{\sigma_0}\mathcal{TF}^{\tau}\ \mathbf{e}_1; \mathbf{I}_1 \approx_{\mathbf{I}} \texttt{import}\ \mathbf{r}_{\mathbf{d}}, {}^{\sigma_0}\mathcal{TF}^{\tau}\ \mathbf{e}_2; \mathbf{I}_2$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$.

We need to show

$(W, \rho_1(\gamma_1((\texttt{import } \mathbf{r_d}, {}^{\sigma_0}\mathcal{TF}^{\tau}\ \mathbf{e_1}; \mathbf{I_1}, \cdot))), \rho_2(\gamma_2((\texttt{import } \mathbf{r_d}, {}^{\sigma_0}\mathcal{TF}^{\tau}\ \mathbf{e_2}; \mathbf{I_2}, \cdot))))$
$= (W, (\texttt{import } \mathbf{r_d}, {}^{\rho_1(\sigma_0)}\mathcal{TF}^{\rho_1(\tau)}\ \rho_1(\gamma_1(\mathbf{e_1})); \rho_1(\gamma_1(\mathbf{I_1})), \cdot), (\texttt{import } \mathbf{r_d}, {}^{\rho_2(\sigma_0)}\mathcal{TF}^{\rho_2(\tau)}\ \rho_2(\gamma_2(\mathbf{e_2})); \rho_2(\gamma_2(\mathbf{I_2})), \cdot))$
$\in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho$.

The result follows from Lemma 3.28, 1(b), using what is given in the hypotheses.

□

Lemma 3.72 (Protect)
Given the following:

- $\sigma = \phi :: \sigma'$
- $\Psi; \Delta, \zeta; \chi; \phi :: \zeta; \mathbf{q} \vdash \mathbf{I_1} \approx_{\mathbf{I}} \mathbf{I_2}$,

we have that $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \texttt{protect } \phi, \zeta; \mathbf{I_1} \approx_{\mathbf{I}} \texttt{protect } \phi, \zeta; \mathbf{I_2}$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$.

We need to show

$(W, \rho_1(\gamma_1((\texttt{protect } \phi, \zeta; \mathbf{I_1}, \cdot))), \rho_2(\gamma_2((\texttt{protect } \phi, \zeta; \mathbf{I_2}, \cdot))))$
$= (W, (\texttt{protect } \rho_1(\phi), \rho_1(\zeta); \rho_1(\gamma_1(\mathbf{I_1})), \cdot), (\texttt{protect } \rho_2(\phi), \rho_2(\zeta); \rho_2(\gamma_2(\mathbf{I_2})), \cdot))$
$\in \mathcal{E}[\![\mathbf{q} \vdash \text{ret-type}(\mathbf{q}, \chi, \sigma)]\!]\rho$.

Let $\rho' = \rho[\zeta \mapsto \mathcal{S}[\![\sigma']\!]]$, noting the latter exists due to last given. We can then instantiate the second hypothesis, since $\rho' \in \mathcal{D}[\![\Delta, \zeta]\!]$, and $\mathcal{S}[\![\sigma]\!]\rho = \mathcal{S}[\![\phi :: \sigma']\!]\rho = \mathcal{S}[\![\phi :: \zeta]\!]\rho'$ due to substitution. This gives us that:

$(W, \rho_1(\gamma_1((\mathbf{I_1}, \cdot))), \rho_1(\gamma_1((\mathbf{I_1}, \cdot)))) \in \mathcal{E}[\![q \vdash \text{ret-addr-type}(\mathbf{q}, \chi, \phi :: \zeta)]\!]\rho'$

With which the result can follow from Lemma 3.4.3, since the $\texttt{protect } \phi, \zeta$ instruction reduces without any operational consequences.

□

Lemma 3.73 (F Variable)
If $\mathbf{x} : \tau \in \Gamma$, then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{out} \vdash \mathbf{x} \approx \mathbf{x} : \tau; \sigma$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$.

We must show that $(W, \rho_1(\gamma_1(\mathbf{x})), \rho_2(\gamma_2(\mathbf{x}))) \in \mathcal{E}[\![\mathbf{out} \vdash \mathbf{int}; \sigma_2]\!]$

This follows immediately from the definition of $\mathcal{G}[\![\Gamma]\!]$ and Lemma 3.25.

□

Lemma 3.74 (F Unit)
$\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{out} \vdash () \approx () : \mathbf{unit}; \sigma$.

Proof

Immediate from Lemma 3.25. □

Lemma 3.75 (F Integer)
$\Psi; \Delta; \Gamma; \chi; \sigma; \mathsf{out} \vdash \mathsf{n} \approx \mathsf{n} : \mathsf{int}; \sigma$.

Proof

Immediate from Lemma 3.25. □

Lemma 3.76 (F Arith Op)
If $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathsf{out} \vdash \mathsf{t_1} \approx \mathsf{t_2} : \mathsf{int}; \sigma_1$, and $\Psi; \Delta; \Gamma; \chi; \sigma_1; \mathsf{out} \vdash \mathsf{t_1'} \approx \mathsf{t_2'} : \mathsf{int}; \sigma_2$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathsf{out} \vdash \mathsf{t_1\ p\ t_1'} \approx \mathsf{t_2\ p\ t_2'} : \mathsf{int}; \sigma_2$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma_0]\!]\rho$.

We must show that

$(W, \rho_1(\gamma_1(\mathsf{t_1\ p\ t_1'})), \rho_2(\gamma_2(\mathsf{t_2\ p\ t_2'}))) = (W, \rho_1(\gamma_1(\mathsf{t_1}))\ \mathsf{p}\ \rho_1(\gamma_1(\mathsf{t_1'})), \rho_2(\gamma_2(\mathsf{t_2}))\ \mathsf{p}\ \rho_2(\gamma_2(\mathsf{t_2'}))) \in \mathcal{E}[\![\mathsf{out} \vdash \mathsf{int}; \sigma_2]\!]$

We proceed by applying Lemma 3.26 twice, first with evaluation contexts $E_i = [\cdot]\ \mathsf{p}\ \rho_i(\gamma_i(\mathsf{t_i'}))$

and then with with $E_i = \mathsf{v_i\ p}\ [\cdot]$.

We then must show that $(W, \mathsf{v_1\ p\ v_1', v_2\ p\ v_2'}) \in \mathcal{E}[\![\mathsf{out} \vdash \mathsf{int}; \sigma_2]\!]$.

The result then follows from Lemma 3.13 and Lemma 3.25.

□

Lemma 3.77 (F If0)
If $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathsf{out} \vdash \mathsf{t_1} \approx \mathsf{t_1'} : \mathsf{int}; \sigma_1$, $\Psi; \Delta; \Gamma; \chi; \sigma_1; \mathsf{out} \vdash \mathsf{t_2} \approx \mathsf{t_2'} : \tau; \sigma_2$,
and $\Psi; \Delta; \Gamma; \chi; \sigma_1; \mathsf{out} \vdash \mathsf{t_3} \approx \mathsf{t_3'} : \tau; \sigma_2$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathsf{out} \vdash \mathsf{if0\ t_1\ t_2\ t_3} \approx \mathsf{if0\ t_1'\ t_2'\ t_3'} : \tau; \sigma_2$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma_0]\!]\rho$.

We must show that

$(W, \rho_1(\gamma_1(\mathsf{if0\ t_1\ t_2\ t_3})), \rho_2(\gamma_2(\mathsf{if0\ t_1'\ t_2'\ t_3'}))) \in \mathcal{E}[\![\mathsf{out} \vdash \tau; \sigma_2]\!]$.

After pushing in the substitutions, we apply Lemma 3.26 three times, which requires us to then show that:

$(W, \mathsf{if0\ v_1\ v_2\ v_3}, \mathsf{if0\ v_1'\ v_2'\ v_3'}) \in \mathcal{E}[\![\mathsf{out} \vdash \tau; \sigma_2]\!]$

Where $(W, \mathsf{v_1}, \mathsf{v_1'}) \in \mathcal{V}[\![\mathsf{int}]\!]\rho$,$(W, \mathsf{v_2}, \mathsf{v_2'}) \in \mathcal{V}[\![\tau]\!]\rho$, and $(W, \mathsf{v_3}, \mathsf{v_3'}) \in \mathcal{V}[\![\tau]\!]\rho$.

Inspecting the $\mathcal{V}[\![\mathsf{int}]\!]\rho$, we can see that $\mathsf{v_1}$ and $\mathsf{v_1'}$ are integer values which are either $\mathsf{0}$ or not.

In either case, we proceed by combination of Lemma 3.13 and Lemma 3.25. □

Lemma 3.78 (F Pure Function)
If $\Psi; \Delta, \zeta; \Gamma, \overline{\mathsf{x} : \tau}; \chi; \zeta; \mathsf{out} \vdash \mathsf{t_1} \approx \mathsf{t_2} : \tau'; \zeta$,
then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathsf{out} \vdash \lambda(\overline{\mathsf{x} : \tau}).\mathsf{t_1} \approx \lambda(\overline{\mathsf{x} : \tau}).\mathsf{t_1} : (\overline{\tau}) \to \tau'; \sigma$

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$.

We need to show that

$$(W, \rho_1(\gamma_1(\lambda(\overline{\mathbf{x}:\tau}).\mathbf{t_1})), \rho_2(\gamma_2(\lambda(\overline{\mathbf{x}:\tau}).\mathbf{t_2})))$$
$$= (W, \lambda(\overline{\mathbf{x}:\rho_1(\gamma_1(\tau))}).\rho_1(\gamma_1(\mathbf{t_1})), \lambda(\overline{\mathbf{x}:\rho_2(\gamma_2(\tau))}).\rho_2(\gamma_2(\mathbf{t_2}))) \in \mathcal{E}[\![\mathbf{out} \vdash (\overline{\tau}) \to \tau'\sigma]\!]\rho$$

Using Lemma 3.25, it suffices to show that $(W, \lambda(\overline{\mathbf{x}:\rho_1(\gamma_1(\tau))}).\rho_1(\gamma_1(\mathbf{t_1})), \lambda(\overline{\mathbf{x}:\rho_1(\gamma_1(\tau))}).\rho_2(\gamma_2(\mathbf{t_2}))) \in \mathcal{V}[\![(\overline{\tau}) \to \tau']\!]\rho$.

This means we must consider arbitrary $W' \sqsupseteq_{\text{pub}} W$, SR $\in$ TStackRel, $\overline{\mathbf{v_1'}}, \overline{\mathbf{v_2'}}$ such that currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\zeta]\!]\rho'$ where $\rho' = \rho[\zeta \mapsto \text{SR}]$ and $(\overline{W', \mathbf{v_1'}, \mathbf{v_2'}}) \in \mathcal{V}[\![\tau]\!]\rho'$.

Our obligation is to show that $(W', \lambda(\overline{\mathbf{x}:\rho_1(\gamma_1(\tau))}).\rho_1(\gamma_1(\mathbf{t_1}))\overline{\mathbf{v_1'}}, \lambda(\overline{\mathbf{x}:\rho_2(\gamma_2(\tau))}).\rho_2(\gamma_2(\mathbf{t_2}))\overline{\mathbf{v_2'}}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \zeta]\!]\rho'$.

We appeal to Lemma 3.13, which means we must show that

$(W', \rho_1(\gamma_1(\mathbf{t_1}))[\overline{\mathbf{v_1'}/\mathbf{x}}], \rho_2(\gamma_2(\mathbf{t_2}))[\overline{\mathbf{v_2'}/\mathbf{x}}]) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \zeta]\!]\rho'$.

Let $\gamma' = \gamma[\overline{\mathbf{x} \mapsto (\mathbf{v_1'}, \mathbf{v_2'})}]$. Note that $\gamma' \in \mathcal{G}[\![\Gamma, \overline{\mathbf{x}:\tau}]\!]\rho$, and that, appealing to substitution, the above is equivalent to $(W', \rho_1'(\gamma_1'(\mathbf{t_1})), \rho_2'(\gamma_2'(\mathbf{t_2}))) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \zeta]\!]\rho'$.

Which follows from our first hypothesis.

□

Lemma 3.79 (F Stack Modifying Function)
If $\Psi; \Delta, \zeta; \Gamma, \overline{\mathbf{x}:\tau}; \chi; \phi_{\text{i}} :: \zeta; \mathbf{out} \vdash \mathbf{t_1} \approx \mathbf{t_2} : \tau'; \phi_{\text{o}} :: \zeta$,
then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{out} \vdash \lambda^{\phi_{\text{i}}}_{\phi_{\text{o}}}(\overline{\mathbf{x}:\tau}).\mathbf{t_1} \approx \lambda^{\phi_{\text{i}}}_{\phi_{\text{o}}}(\overline{\mathbf{x}:\tau}).\mathbf{t_1} : (\overline{\tau}) \xrightarrow{\phi_{\text{i}};\phi_{\text{o}}} \tau'; \sigma$

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$.

We need to show that

$$(W, \rho_1(\gamma_1(\lambda^{\phi_{\text{i}}}_{\phi_{\text{o}}}(\overline{\mathbf{x}:\tau}).\mathbf{t_1})), \rho_2(\gamma_2(\lambda^{\phi_{\text{i}}}_{\phi_{\text{o}}}(\overline{\mathbf{x}:\tau}).\mathbf{t_2})))$$
$$= (W, \lambda^{\rho_1(\phi_{\text{i}})}_{\rho_1(\phi_{\text{o}})}(\overline{\mathbf{x}:\rho_1(\gamma_1(\tau))}).\rho_1(\gamma_1(\mathbf{t_1})), \lambda^{\rho_2(\phi_{\text{i}})}_{\rho_2(\phi_{\text{o}})}(\overline{\mathbf{x}:\rho_2(\gamma_2(\tau))}).\rho_2(\gamma_2(\mathbf{t_2}))) \in \mathcal{E}[\![\mathbf{out} \vdash (\overline{\tau}) \to \tau'\sigma]\!]\rho$$

Using Lemma 3.25, it suffices to show that $(W, \lambda^{\rho_1(\phi_{\text{i}})}_{\rho_1(\phi_{\text{o}})}(\overline{\mathbf{x}:\rho_1(\gamma_1(\tau))}).\rho_1(\gamma_1(\mathbf{t_1})), \lambda^{\rho_2(\phi_{\text{i}})}_{\rho_2(\phi_{\text{o}})}(\overline{\mathbf{x}:\rho_2(\gamma_2(\tau))}).\rho_2(\gamma_2(\mathbf{t_2}))) \in \mathcal{V}[\![(\overline{\tau}) \xrightarrow{\phi_{\text{i}};\phi_{\text{o}}} \tau']\!]\rho$.

This means we must consider arbitrary $W' \sqsupseteq_{\text{pub}} W$, SR $\in$ TStackRel, $\overline{\mathbf{v_1'}}, \overline{\mathbf{v_2'}}$ such that currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\phi_{\text{i}} :: \zeta]\!]\rho'$ where $\rho' = \rho[\zeta \mapsto \text{SR}]$ and $(\overline{W', \mathbf{v_1'}, \mathbf{v_2'}}) \in \mathcal{V}[\![\tau]\!]\rho'$.

Our obligation is to show that $(W', \lambda^{\rho_1(\phi_{\text{i}})}_{\rho_1(\phi_{\text{o}})}(\overline{\mathbf{x}:\rho_1(\gamma_1(\tau))}).\rho_1(\gamma_1(\mathbf{t_1}))\overline{\mathbf{v_1'}}, \lambda^{\rho_2(\phi_{\text{i}})}_{\rho_2(\phi_{\text{o}})}(\overline{\mathbf{x}:\rho_2(\gamma_2(\tau))}).\rho_2(\gamma_2(\mathbf{t_2}))\overline{\mathbf{v_2'}}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \phi_{\text{o}} :: \zeta]\!]\rho'$.

We appeal to Lemma 3.13, which means we must show that

$(W', \rho_1(\gamma_1(\mathbf{t_1}))[\overline{\mathbf{v_1'}/\mathbf{x}}], \rho_2(\gamma_2(\mathbf{t_2}))[\overline{\mathbf{v_2'}/\mathbf{x}}]) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \phi_{\text{o}} :: \zeta]\!]\rho'$.

Let $\gamma' = \gamma[\overline{\mathbf{x} \mapsto (\mathbf{v_1'}, \mathbf{v_2'})}]$. Note that $\gamma' \in \mathcal{G}[\![\Gamma, \overline{\mathbf{x}:\tau}]\!]\rho$, and that, appealing to substitution, the above is equivalent to $(W', \rho_1'(\gamma_1'(\mathbf{t_1})), \rho_2'(\gamma_2'(\mathbf{t_2}))) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \phi_{\text{o}} :: \zeta]\!]\rho'$.

Which follows from our first hypothesis.

□

Lemma 3.80 (F Pure Application)
If $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathbf{out} \vdash \mathbf{t} \approx \mathbf{t'} : (\tau_1 \cdots \tau_n) \to \tau'; \sigma_0$,
and $\Psi; \Delta; \Gamma; \chi; \sigma_{i-1}; \mathbf{out} \vdash \mathbf{t_i} \approx \mathbf{t'_i} : \tau_i; \sigma_i$ for $i \in \{1, \ldots, n\}$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathbf{out} \vdash \mathbf{t}\ \mathbf{t_1} \cdots \mathbf{t_n} \approx \mathbf{t'}\ \mathbf{t'_1} \cdots \mathbf{t'_n} : \tau'; \sigma_n$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma_0]\!]\rho$.

We need to show that

$$(W, \rho_1(\gamma_1(\mathbf{t}\ \mathbf{t_1} \cdots \mathbf{t_n})), \rho_2(\gamma_2(\mathbf{t'}\ \mathbf{t'_1} \cdots \mathbf{t'_n}))) \\ = (W, \rho_1(\gamma_1(\mathbf{t}))\ \rho_1(\gamma_1(\mathbf{t_1})) \cdots \rho_1(\gamma_1(\mathbf{t_n})), \rho_2(\gamma_2(\mathbf{t'}))\ \rho_2(\gamma_2(\mathbf{t'_1})) \cdots \rho_2(\gamma_2(\mathbf{t'_n}))) \\ \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \sigma_n]\!]\rho$$

We proceed by applying Lemma 3.26 $n+1$ times, with the first evaluation contexts being
$E_0 = [\cdot]\ \rho_1(\gamma_1(\mathbf{t_1})) \cdots \rho_1(\gamma_1(\mathbf{t_n}))$ and
$E'_0 = [\cdot]\ \rho_2(\gamma_2(\mathbf{t'_1})) \cdots \rho_2(\gamma_2(\mathbf{t'_n}))$
And the ith being
$E_i = \mathbf{v_0}\ \mathbf{v_1} \cdots \mathbf{v_{i-1}}[\cdot] \cdots \rho_1(\gamma_1(\mathbf{t_n}))$ and
$E'_i = \mathbf{v'_0}\ \rho_2(\gamma_2(\mathbf{v'_1})) \cdots \mathbf{v'_{i-1}}[\cdot] \cdots \rho_2(\gamma_2(\mathbf{t'_n}))$
Where $(W, \mathbf{v_0}, \mathbf{v'_0}) \in \mathcal{V}[\![(\tau_1 \cdots \tau_n) \to \tau']\!]\rho$ and $(W, \mathbf{v_i}, \mathbf{v'_i}) \in \mathcal{V}[\![\tau_i]\!]\rho$.
Once we show that

$$(W, E_n[\mathbf{v_n}], E'_n[\mathbf{v'_n}]) = (W, \mathbf{v_0}\ \mathbf{v_1} \cdots \mathbf{v_n}, \mathbf{v'_0}\ \mathbf{v'_1} \cdots \mathbf{v'_n}) \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \sigma_n]\!]\rho$$

all prior applications of Lemma 3.26 follow.
We instantiate $(W, \mathbf{v_0}, \mathbf{v'_0}) \in \mathcal{V}[\![(\tau_1 \cdots \tau_n) \to \tau']\!]\rho$ with W', SR $= (\rho_1(\sigma_n), \rho_2(\sigma_n), \mathcal{S}[\![\sigma_n]\!]\rho)$, $\overline{\mathbf{v}}$, $\overline{\mathbf{v'}}$ to yield the desired result.

□

Lemma 3.81 (F Stack Modifying Application)
If $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathbf{out} \vdash \mathbf{t} \approx \mathbf{t'} : (\tau_1 \cdots \tau_n) \xrightarrow{\phi_i; \phi_o} \tau'; \sigma_0$,
and $\Psi; \Delta; \Gamma; \chi; \sigma_{i-1}; \mathbf{out} \vdash \mathbf{t_i} \approx \mathbf{t'_i} : \tau_i; \sigma_i$ for $i \in \{1, \ldots, n\}$,
where $\sigma_n = \phi_i :: \hat{\sigma}$ and $\sigma' = \phi_o :: \hat{\sigma}$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathbf{out} \vdash \mathbf{t}\ \mathbf{t_1} \cdots \mathbf{t_n} \approx \mathbf{t'}\ \mathbf{t'_1} \cdots \mathbf{t'_n} : \tau'; \sigma'$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma_0]\!]\rho$.

We need to show that

$$(W, \rho_1(\gamma_1(\mathbf{t}\ \mathbf{t_1} \cdots \mathbf{t_n})), \rho_2(\gamma_2(\mathbf{t'}\ \mathbf{t'_1} \cdots \mathbf{t'_n}))) \\ = (W, \rho_1(\gamma_1(\mathbf{t}))\ \rho_1(\gamma_1(\mathbf{t_1})) \cdots \rho_1(\gamma_1(\mathbf{t_n})), \rho_2(\gamma_2(\mathbf{t'}))\ \rho_2(\gamma_2(\mathbf{t'_1})) \cdots \rho_2(\gamma_2(\mathbf{t'_n}))) \\ \in \mathcal{E}[\![\mathbf{out} \vdash \tau'; \sigma']\!]\rho$$

We proceed by applying Lemma 3.26 $n+1$ times, with the first evaluation contexts being

$E_0 = [\cdot]\, \rho_1(\gamma_1(\mathsf{t_1})) \cdots \rho_1(\gamma_1(\mathsf{t_n}))$ and

$E'_0 = [\cdot]\, \rho_2(\gamma_2(\mathsf{t'_1})) \cdots \rho_2(\gamma_2(\mathsf{t'_n}))$

And the ith being

$E_i = \mathsf{v_0\ v_1 \cdots v_{i-1}}[\cdot] \cdots \rho_1(\gamma_1(\mathsf{t_n}))$ and

$E'_i = \mathsf{v'_0}\, \rho_2(\gamma_2(\mathsf{v'_1})) \cdots \mathsf{v'_{i-1}}[\cdot] \cdots \rho_2(\gamma_2(\mathsf{t'_n}))$

Where $(W, \mathsf{v_0}, \mathsf{v'_0}) \in \mathcal{V}[\![(\tau_1 \cdots \tau_n) \to \tau']\!]\rho$ and $(W, \mathsf{v_i}, \mathsf{v'_i}) \in \mathcal{V}[\![\tau_i]\!]\rho$.

Once we show that

$$(W, E_n[\mathsf{v_n}], E'_n[\mathsf{v'_n}]) = (W, \mathsf{v_0\ v_1 \cdots v_n}, \mathsf{v'_0\ v'_1 \cdots v'_n}) \in \mathcal{E}[\![\mathsf{out} \vdash \tau'; \sigma']\!]\rho$$

all prior applications of Lemma 3.26 follow.

We instantiate $(W, \mathsf{v_0}, \mathsf{v'_0}) \in \mathcal{V}[\![(\tau_1 \cdots \tau_n) \xrightarrow{\phi_i;\phi_o} \tau']\!]\rho$ with W', SR $= (\rho_1(\sigma_n), \rho_2(\sigma_n), \mathcal{S}[\![\sigma_n]\!]\rho)$ (noting that $\sigma_n = \phi_i :: \zeta$), $\overline{\mathsf{v}}$, and $\overline{\mathsf{v'}}$ to yield the desired result.

□

Lemma 3.82 (F Fold)
If $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathsf{out} \vdash \mathsf{t_1} \approx \mathsf{t_2} : \tau[\mu\alpha.\tau/\alpha]; \sigma_1$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathsf{out} \vdash \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t_1} \approx \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t_2} : \mu\alpha.\tau; \sigma_1$

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma_0]\!]\rho$.

We proceed by applying Lemma 3.26, with evaluation contexts $E_i = \mathsf{fold}_{\mu\alpha.\tau}\ [\cdot]$.

Given $(W, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$, we must show $(W, \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v_1}, \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v_2}) \in \mathcal{E}[\![\mathsf{out} \vdash \mu\alpha.\tau; \sigma_1]\!]$.

From Lemma 3.8, noting that $\triangleright W \sqsupseteq W$, we have that $(W, \mathsf{v_1}, \mathsf{v_2}) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$, which means $(W, \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v_1}, \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v_2}) \in \mathcal{V}[\![\mu\alpha.\tau]\!]\rho$ and the result follows from Lemma 3.25.

□

Lemma 3.83 (F Unfold)
If $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathsf{out} \vdash \mathsf{t_1} \approx \mathsf{t_2} : \mu\alpha.\tau; \sigma_1$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathsf{out} \vdash \mathsf{unfold\ t_1} \approx \mathsf{unfold\ t_2} : \tau[\mu\alpha.\tau/\alpha]; \sigma_1$

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma_0]\!]\rho$.

We proceed by applying Lemma 3.26, with evaluation contexts $E_i = \mathsf{unfold}\ [\cdot]$.

Given $(W, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\mu\alpha.\tau]\!]\rho$, we must show $(W, \mathsf{unfold\ v_1}, \mathsf{unfold\ v_2}) \in \mathcal{E}[\![\mathsf{out} \vdash \tau[\mu\alpha.\tau/\alpha]; \sigma_1]\!]$.

From the definition of $\mathcal{V}[\![\mu\alpha.\tau]\!]\rho$, we know that the above is equivalent to $(W, \mathsf{unfold\ fold}_{\mu\alpha.\tau}\ \mathsf{v'_1}, \mathsf{unfold\ fold}_{\mu\alpha.\tau}\ \mathsf{v'_2}) \in \mathcal{E}[\![\mathsf{out} \vdash \tau[\mu\alpha.\tau/\alpha]; \sigma_1]\!]$ where $(W, \mathsf{v'_1}, \mathsf{v'_2}) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$.

And we can then appeal to Lemma 3.4.3, noting that Lemma 3.25 provides us with the needed condition once we take one reduction step.

□

Lemma 3.84 (F Tuple)
If $\Psi; \Delta; \Gamma; \chi; \sigma_{i-1}; \mathsf{out} \vdash \mathsf{t_i} \approx \mathsf{t'_i} : \tau_i; \sigma_i$ for $i \in \{1, \ldots, n\}$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_{n-1}; \mathsf{out} \vdash \langle \mathsf{t_1}, \ldots, \mathsf{t_n} \rangle \approx \langle \mathsf{t'_1}, \ldots, \mathsf{t'_n} \rangle : \langle \tau_1, \ldots, \tau_n \rangle; \sigma_n$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma_{n-1}]\!]\rho$.

We must show that

$(W, \rho_1(\gamma_1(\langle \mathbf{t_1}, \ldots, \mathbf{t_n} \rangle)), \rho_2(\gamma_2(\langle \mathbf{t'_1}, \ldots, \mathbf{t'_n} \rangle))) \in \mathcal{E}[\![\mathbf{out} \vdash \mathbf{int}; \sigma_2]\!]$

We proceed by pushing the substitutions in and applying Lemma 3.26 n times, with ith evaluation contexts $E_{1i} = \langle \mathbf{v_1}, \ldots, [\cdot], \ldots, \rho_1(\gamma_1(\mathbf{t_n})) \rangle$ and $E_{2i} = \langle \mathbf{v'_1}, \ldots, [\cdot], \ldots, \rho_2(\gamma_2(\mathbf{t'_n})) \rangle$

Where $(W, \mathbf{v_i}, \mathbf{v'_i}) \in \mathcal{V}[\![\tau_i]\!]\rho$.

We then must show that $(W, \langle \mathbf{v_1}, \ldots, \mathbf{v_n} \rangle, \langle \mathbf{v'_1}, \ldots, \mathbf{v'_n} \rangle) \in \mathcal{E}[\![\mathbf{out} \vdash \langle \tau_1, \ldots, \tau_n \rangle; \sigma_n]\!]\rho$.

But this follows from Lemma 3.25.

□

Lemma 3.85 (F Projection)
If $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathbf{out} \vdash \mathbf{t_1} \approx \mathbf{t_2} : \langle \tau_1, \ldots, \tau_n \rangle; \sigma_1$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathbf{out} \vdash \pi_i(\mathbf{t_1}) \approx \pi_i(\mathbf{t_2}) : \tau_i; \sigma_1$

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma_0]\!]\rho$.

We must show that

$(W, \rho_1(\gamma_1(\pi_i(\mathbf{t_1}))), \rho_2(\gamma_2(\pi_i(\mathbf{t_2})))) = (W, \pi_i(\rho_1(\gamma_1(\mathbf{t_1}))), \pi_i(\rho_2(\gamma_2(\mathbf{t_2})))) \in \mathcal{E}[\![\mathbf{out} \vdash \tau_i; \sigma_1]\!]\rho$

We appeal to Lemma 3.26, with $E_i = \pi_i([\cdot])$. We must show that

$(W, \pi_i(\mathbf{v_1}), \pi_i(\mathbf{v_2})) \in \mathcal{E}[\![\tau_i]\!]\rho$ given that $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\langle \tau_1, \ldots, \tau_n \rangle]\!]\rho$

We appeal to Lemma 3.13, noting that the definition of $\mathcal{V}[\![\langle \tau_1, \ldots, \tau_n \rangle]\!]\rho$ and Lemma 3.25 yields the desired result.

□

Lemma 3.86 (FT Boundary)
If $\Psi; \Delta; \Gamma; \cdot; \sigma_0; \mathbf{end}\{\tau^{\mathcal{T}}; \sigma_1\} \vdash \mathbf{e_1} \approx \mathbf{e_2} : \tau^{\mathcal{T}}; \sigma_1$,
then $\Psi; \Delta; \Gamma; \chi; \sigma_0; \mathbf{out} \vdash {}^{\tau}\mathcal{FT}\, \mathbf{e_1} \approx {}^{\tau}\mathcal{FT}\, \mathbf{e_2} : \tau; \sigma_1$.

Proof

Consider arbitrary W, ρ, and γ such that $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $\gamma \in \mathcal{G}[\![\Gamma]\!]$, currentMR$(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$, and currentMR$(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$.

We need to show that

$$(W, \rho_1(\gamma_1({}^{\tau}\mathcal{FT}\, \mathbf{e_1})), \rho_2(\gamma_2({}^{\tau}\mathcal{FT}\, \mathbf{e_2}))) = (W, {}^{\rho_1(\tau)}\mathcal{FT}\, \rho_1(\gamma_1(\mathbf{e_1})), {}^{\rho_2(\tau)}\mathcal{FT}\, \rho_2(\gamma_2(\mathbf{e_2}))) \in \mathcal{E}[\![\mathbf{out} \vdash \tau; \sigma_1]\!]$$

From the hypothesis, we know that $(W, \rho_1(\gamma_1(\mathbf{e_1})), \rho_2(\gamma_2(\mathbf{e_2}))) \in \mathcal{E}[\![\mathbf{end}\{\tau^{\mathcal{T}}; \sigma_1\} \vdash \tau^{\mathcal{T}}; \sigma_1]\!]$.

The result is then immediate from Lemma 3.28, 1(a).

□

3.7 Fundamental Property and Soundness

Lemma 3.87 (Fundamental Property)

- If $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e : \tau; \sigma'$ then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e \approx e : \tau; \sigma'$
- If $\Psi \vdash \mathbf{H} : \Psi'$ then $\Psi \vdash \mathbf{H} \approx_{\mathrm{H}} \mathbf{H} : \Psi'$
- If $\Psi \vdash \mathbf{h} : {}^{\nu}\psi$ then $\Psi \vdash \mathbf{h} \approx_{\mathrm{hv}} \mathbf{h} : {}^{\nu}\psi \stackrel{\text{def}}{=}$.
- If $\Psi; \Delta \vdash \mathbf{w} : \tau$ $\Psi; \Delta \vdash \mathbf{w} \approx_{\mathrm{w}} \mathbf{w} : \tau$
- If $\Psi; \Delta; \chi \vdash \mathbf{u} : \tau$ then $\Psi; \Delta; \chi \vdash \mathbf{u} \approx_{\mathrm{u}} \mathbf{u} : \tau$
- If $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \mathbf{I}$ then $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \mathbf{I} \approx_{\mathrm{I}} \mathbf{I}$

Proof

We prove all the claims simultaneously, by induction on the typing derivations, using the compatibility lemmas. □

Lemma 3.88 (Weakening)
If $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx e_2 : \tau; \sigma'$ and $\Psi \subseteq \Psi'$, $\Delta \subseteq \Delta'$, $\Gamma \subseteq \Gamma'$, $\chi \subseteq \chi'$, then $\Psi'; \Delta'; \Gamma'; \chi'; \sigma; \mathbf{q} \vdash e_1 \approx e_2 : \tau; \sigma'$.

Proof

Let $W \in \mathcal{H}[\![\Psi']\!]$, $\rho' \in \mathcal{D}[\![\Delta']\!]$, $(W, \gamma') \in \mathcal{G}[\![\Gamma']\!]\rho'$ such that $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi']\!]\rho'$ and $\mathrm{currentMR}(W(i_{\mathrm{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho'$.

Let $\rho = \rho'|_{\Delta}$ and $\gamma = \gamma'|_{\Gamma}$. Note that $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$ immediately.

We must further show:

- $\mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho$
- $\mathrm{currentMR}(W(i_{\mathrm{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho$
- $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$

Since the free type variables in χ are in Δ, $\mathcal{R}[\![\chi]\!]\rho' = \mathcal{R}[\![\chi]\!]\rho$, after which the first follows from the definition.

Similarly, the free type variables in σ are in Δ, after which the second follows.

Finally, we must show that $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. But clearly $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho'$ and since the free type variables in Γ are in Δ, $\mathcal{G}[\![\Gamma]\!]\rho' = \mathcal{G}[\![\Gamma]\!]\rho$, so we are done. □

Lemma 3.89 (Congruence)
If $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx e_2 : \tau; \sigma'$ and $\vdash C : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \tau; \sigma') \rightsquigarrow (\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathbf{q}' \vdash \tau'; \sigma_1)$, then $\Psi'; \Delta'; \Gamma'; \chi'; \sigma_0; \mathbf{q} \vdash C[e_1] \approx C[e_2] : \tau; \sigma_1$.

Proof

This follows by induction on the type derivation for C, using Lemma 3.88 for the cases when C is empty, and the compatibility lemmas in the rest of the cases. □

Lemma 3.90 (Canonical World)
If $\vdash \mathbf{M} = (\mathbf{H}, \mathbf{R}, \mathbf{S}) : (\Psi, \chi, \sigma)$, then for any $k, \exists W.\ W.k = k \wedge W \in \mathcal{H}[\![\psi]\!] \wedge \mathrm{currentMR}(W(i_{\mathrm{reg}})) \Subset_W \mathcal{R}[\![\chi]\!] \wedge \mathrm{currentMR}(W(i_{\mathrm{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!] \wedge (\mathbf{M}, \mathbf{M}) : W$.

Proof

Say that $\Psi = \Psi', \ell_1 :^{\text{ref}} \psi_1, \ldots, \ell_n :^{\text{ref}} \psi_n$ where boxheap(Ψ'). Let

$$\theta_i = (\bullet, \{\bullet\}, \{\}, \{\}, \lambda s.\{(W', \mathbf{M_1}, \mathbf{M_2}) \in \text{MemAtom}_k | (W', \mathbf{M_1}(\ell_i), \mathbf{M_2}(\ell_i)) \in \mathcal{HV}[\![\psi_i]\!]\emptyset, \lambda s.\{(\ell_i, \ell_i)\})$$

for $1 \leq i \leq n$. We construct

$$W = (k, \Psi, \Psi, (\text{island}_{\text{reg}}((\mathbf{R}, \chi, \mathbf{R}, \chi), k), \text{island}_{\text{stk}}((\mathbf{S}, \sigma, \mathbf{S}, \sigma), k), \text{island}_{\text{box}}((\mathbf{H}|_{\Psi'}, \mathbf{H}|_{\Psi'}), k), \theta_1, \ldots, \theta_n)$$

We need to show the following:

- For each $\ell :^{\text{box}} \psi \in \Psi'$, $(W, \ell, \ell) \in \mathcal{W}[\![\mathbf{box}\, \psi]\!]\emptyset$,
- For each i, $(W, \ell_i, \ell_i) \in \mathcal{W}[\![\mathbf{ref}\, \psi]\!]\emptyset$
- currentMR($W(i_{\text{reg}})$) $\Subset_W \mathcal{R}[\![\chi]\!]$
- currentMR($W(i_{\text{stk}})$) $\Subset_W \mathcal{S}[\![\sigma]\!]$
- $(\mathbf{M}, \mathbf{M}) : W$

All of these follow from the respective definitions and the Fundamental Property for word and heap values.

□

Lemma 3.91 (Adequacy)
If $\Psi; \cdot; \cdot; \chi; \sigma; \mathbf{q} \vdash e_1 \approx e_2 : \tau; \sigma'$, $\vdash \mathbf{M} : (\Psi, \chi, \sigma)$, then $\langle \mathbf{M} \mid e_1 \rangle \downarrow$ if and only if $\langle \mathbf{M} \mid e_2 \rangle \downarrow$.

Proof

We show that $\langle \mathbf{M} \mid e_1 \rangle \downarrow$ implies $\langle \mathbf{M} \mid e_2 \rangle \downarrow$, and the converse holds by an identical argument.

Suppose $\langle \mathbf{M} \mid e_1 \rangle \downarrow^k$. By Lemma 3.90, there is some $W \in \mathcal{H}[\![\psi]\!]$ with currentMR($W(i_{\text{reg}})$) $\Subset_W \mathcal{R}[\![\chi]\!] \wedge$ currentMR($W(i_{\text{stk}})$) $\Subset_W \mathcal{S}[\![\sigma]\!]$ such that $(\mathbf{M}, \mathbf{M}) : W$ and $W.k \geq k$.

So by our assumption, $(W, e_1, e_2) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma']\!]\emptyset$. We claim that $(W, E, E) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma']\!]\emptyset$, where

$$E = \begin{cases} [\cdot] & \tau = \tau \\ ([\cdot], \cdot) & \tau = \tau \end{cases}$$

If the claim holds, then $(W, E[e_1], E[e_2]) = (W, e_1, e_2) \in \mathcal{O}$. Since running($W.k, \langle \mathbf{M} \mid e_1 \rangle$) contradicts our assumption, we must have $\langle \mathbf{M} \mid e_2 \rangle \downarrow$, as desired.

To prove the claim, we must consider the two types of continuations, depending on whether $\tau = \tau$ or $\tau = \tau$.

In the first case, let $W' \sqsupseteq_{\text{pub}} W$ and consider $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\emptyset$, such that currentMR($W'(i_{\text{stk}})$) $\Subset_{W'}$ $\mathcal{S}[\![\sigma]\!]\emptyset$. In that case

$$(W', E[\mathbf{v_1}], E[\mathbf{v_2}]) \in \mathcal{O}$$

trivially.

In the second case, the result is essentially as trivial, since while value forms are more complex in T, they are similarly observationally equivalent.

□

Lemma 3.92 (Logical Equivalence Implies Contextual Equivalence)
If $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx e_2 : \tau; \sigma'$ then
$\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx^{ctx} e_2 : \tau; \sigma'$.

Proof

Let $\vdash C : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \tau; \hat{\sigma}) \rightsquigarrow (\Psi'; \cdot; \cdot; \chi'; \sigma'; \mathbf{q}' \vdash \tau'; \hat{\sigma}')$ and $\vdash \mathbf{M} : (\Psi', \chi', \sigma')$.

By congruence (Lemma 3.89), $\Psi'; \cdot; \cdot; \chi; \sigma; \mathbf{q} \vdash C[e_1] \approx C[e_2] : \tau; \sigma'$.

By adequacy (Lemma 3.91), $\langle \mathbf{M} \mid C[e_1] \rangle \downarrow$ if and only if $\langle \mathbf{M} \mid C[e_2] \rangle \downarrow$, as desired.

□

3.8 Completeness

Lemma 3.93 (Contextual Equivalence Implies CIU Equivalence)
If $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx^{ctx} e_2 : \tau; \sigma'$ then
$\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx^{ciu} e_2 : \tau; \sigma'$.

Proof

We have that $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 : \tau; \sigma'$, $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_2 : \tau; \sigma'$, and

$$\forall C, \mathbf{M}, \Psi', \chi', \sigma', \mathbf{q}', \tau', \hat{\sigma}'. \quad \vdash C : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \tau; \hat{\sigma}) \rightsquigarrow (\Psi'; \cdot; \cdot; \chi'; \sigma'; \mathbf{q}' \vdash \tau'; \hat{\sigma}') \ \wedge \ \vdash \mathbf{M} : (\Psi', \chi', \sigma') \implies (\langle \mathbf{M} \mid C[e_1] \rangle \downarrow \iff \langle \mathbf{M} \mid C[e_2] \rangle \downarrow)$$

We need to show that

$$\forall \delta, \gamma, E, \mathbf{M}, \Psi'_{\mathbf{E}}, \mathbf{q}'_{\mathbf{E}}, \tau'_E, \hat{\sigma}'_{\mathbf{E}}. \quad \cdot \vdash \delta : \Delta \ \wedge \ \Psi'_{\mathbf{E}}; \cdot; \cdot; \cdot; \bullet; \mathbf{out} \vdash \gamma : \Gamma; \bullet \ \wedge \ \vdash E : (\Psi; \cdot; \cdot; \chi; \sigma; \mathbf{q} \vdash \tau; \hat{\sigma}) \rightsquigarrow (\Psi'_{\mathbf{E}}; \cdot; \cdot; \chi; \sigma; \mathbf{q}'_{\mathbf{E}} \vdash \tau'_E; \hat{\sigma}'_{\mathbf{E}}) \ \wedge \ \vdash \mathbf{M} : (\Psi'_{\mathbf{E}}, \chi, \sigma) \implies (\langle \mathbf{M} \mid E[\delta(\gamma(e_1))] \rangle \downarrow \iff \langle \mathbf{M} \mid E[\delta(\gamma(e_2))] \rangle \downarrow)$$

Assume all the premises in the implication. It suffices to find a C such that co-termination of $\langle \mathbf{M} \mid C[e_1] \rangle$ and $\langle \mathbf{M} \mid C[e_2] \rangle$ is equivalent to co-termination of $\langle \mathbf{M} \mid E[\delta(\gamma(e_1))] \rangle$ and $\langle \mathbf{M} \mid E[\delta(\gamma(e_2))] \rangle$.

We need a C such that:

$$\vdash C : (\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash \tau; \hat{\sigma}) \rightsquigarrow (\Psi'_{\mathbf{E}}; \cdot; \cdot; \chi'_{\mathbf{E}}; \sigma'_{\mathbf{E}}; \mathbf{q}'_{\mathbf{E}} \vdash \tau'_E; \hat{\sigma}'_{\mathbf{E}})$$

This amounts to constructing a syntactically valid C that accomplishes what $E[\delta(\gamma([\cdot]))]$ would do, were it a valid context, which is essentially an eta-expansion with boundaries inserted appropriately.

Let

$$\begin{aligned}
C_{inner} &= \begin{cases} [\cdot] & \text{if } \tau = \tau \\ {}^{\tau}\mathcal{FT}\,[\cdot] & \text{if } \tau = \tau^{\mathcal{T}} \end{cases} \\
C_{gamma} &= (\lambda(\mathrm{dom}(\Gamma)).C_{inner})\,\gamma(\mathrm{dom}(\Gamma)) \\
C_{delta} &= (\mathtt{jmp}\ \ell[\delta(\mathrm{dom}(\delta))], \\
&\qquad \ell \mapsto \mathbf{code}[\Delta]\{;\sigma\}^{\mathbf{q}}.\mathtt{import}\ r_d, {}^{\sigma}\mathcal{T}\mathcal{F}^{\tau}\ C_{gamma};) \\
&\qquad\qquad \mathtt{ret}\ q\ \{r_d\} \\
C_{outer} &= \begin{cases} C_{delta} & \text{if } \tau = \tau \\ {}^{\tau}\mathcal{FT}\,C_{delta} & \text{if } \tau = \tau \end{cases} \\
C &= E[C_{outer}]
\end{aligned}$$

By inspection of the operational semantics,

$\langle \mathbf{M} \mid C[e_i] \rangle \longmapsto {}^*\langle \mathbf{M} \mid E[C_{outer}[\texttt{import}\ \mathbf{r_d}, {}^{\sigma}\mathcal{T}\mathcal{F}^{\tau}\ (\delta(\gamma(C_{inner}[e_i])))\texttt{;}\ \texttt{ret}\ \mathbf{q}\ \{\mathbf{r_d}\}]] \rangle$

Since this is just a fixed sequence of boundary terms added to $E[\delta(\gamma(e_i))]$, we can see that this co-terminates as desired.

□

Lemma 3.94 (CIU Equivalence Implies Logical Equivalence)
If $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx^{ciu} e_2 : \tau; \sigma'$ then
$\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx e_2 : \tau; \sigma'$.

Proof

We have that $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 : \tau; \sigma'$, $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_2 : \tau; \sigma'$, and

$$\begin{aligned}\forall \delta, \gamma, E, \mathbf{M}, \Psi'_{\mathbf{E}}, \mathbf{q}'_{\mathbf{E}}, \tau'_E, \hat{\sigma}'_{\mathbf{E}}. \quad & \cdot \vdash \delta : \Delta \ \wedge\ \Psi'_{\mathbf{E}}; \cdot; \cdot; \cdot; \bullet; \mathbf{out} \vdash \gamma : \Gamma; \bullet \ \wedge \\ & \vdash E : (\Psi; \cdot; \cdot; \chi; \sigma; \mathbf{q} \vdash \tau; \hat{\sigma}) \rightsquigarrow (\Psi'_{\mathbf{E}}; \cdot; \cdot; \chi; \sigma; \mathbf{q}'_{\mathbf{E}} \vdash \tau'_E; \hat{\sigma}'_{\mathbf{E}}) \ \wedge\ \vdash \mathbf{M} : (\Psi'_{\mathbf{E}}, \chi, \sigma) \\ & \implies (\langle \mathbf{M} \mid E[\delta(\gamma(e_1))] \rangle \downarrow \iff \langle \mathbf{M} \mid E[\delta(\gamma(e_2))] \rangle \downarrow)\end{aligned}$$

We need to show that

$$\begin{aligned}\forall W, \rho.\ & W \in \mathcal{H}[\![\Psi]\!] \ \wedge\ \rho \in \mathcal{D}[\![\Delta]\!] \wedge \\ & \text{currentMR}(W(i_{\text{reg}})) \Subset_W \mathcal{R}[\![\chi]\!]\rho \ \wedge \\ & \text{currentMR}(W(i_{\text{stk}})) \Subset_W \mathcal{S}[\![\sigma]\!]\rho \\ & \implies (W, \rho_1(e_1), \rho_2(e_2)) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma']\!]\rho\end{aligned}$$

Assume all the premises of this implication.
Let $(W, E_1, E_2) \in \mathcal{K}[\![\mathbf{q} \vdash \tau; \sigma']\!]\rho$. We need to show that $(W, E_1[\rho_1(\gamma_1(e_1))], E_2[\rho_2(\gamma_2(e_2))]) \in \mathcal{O}$.
Let $(\mathbf{M_1}, \mathbf{M_2}) : W$. It suffices to show that

$$\langle \mathbf{M_1} \mid E_1[\rho_1(\gamma_1(e_1))] \rangle \downarrow \iff \langle \mathbf{M_2} \mid E_2[\rho_2(\gamma_2(e_2))] \rangle \downarrow .$$

By the Fundamental Property, $\Psi; \Delta; \chi; \sigma; \mathbf{q} \vdash e_1 \approx e_1 : \tau; \sigma'$. Therefore,

$$(W, \rho_1(\gamma_1(e_1)), \rho_2(\gamma_2(e_1))) \in \mathcal{E}[\![\mathbf{q} \vdash \tau; \sigma']\!]\rho$$

and thus

$$\langle \mathbf{M_1} \mid E_1[\rho_1(\gamma_1(e_1))] \rangle \downarrow \iff \langle \mathbf{M_2} \mid E_2[\rho_2(\gamma_2(e_1))] \rangle \downarrow .$$

It remains to show that

$$\langle \mathbf{M_1} \mid E_1[\rho_1(\gamma_1(e_1))] \rangle \downarrow \iff \langle \mathbf{M_2} \mid E_2[\rho_2(\gamma_2(e_2))] \rangle \downarrow .$$

But this follows from our hypothesis that $\Psi; \Delta; \Gamma; \chi; \sigma; \mathbf{q} \vdash e_1 \approx^{ciu} e_2 : \tau; \sigma'$.

□

3.9 Examples

In some of the following examples, we will use the following syntactic shorthands to improve readability:

$\mathsf{let\ x = e_1\ in\ e_2}$ means $(\lambda(\mathsf{x:t}).\mathsf{e_2})\mathsf{e_1}$ where $\mathsf{e_1 : t}$

$\mathsf{e_1; e_2}$ means $(\lambda(\mathsf{ignored : t_1, result : t_2}).\mathsf{result})\mathsf{e_1 e_2}$ where $\mathsf{e_1 : t_1}$ and $\mathsf{e_2 : t_2}$

Noting that for any well-typed term we can mechanically synthesize its type, so elliding them in this context introduces no ambiguity.

3.9.1 Calculations with Different Number of Basic T Blocks

$$f_1 = \lambda(\mathsf{x : int}).^{(\mathsf{int})\to\mathsf{int}}\mathcal{FT}\ (\mathtt{mv\ r1}, \ell; \mathtt{ret\ end}\{\mathsf{int}^{\mathcal{T}}; \cdot\}\ \{\mathtt{r1}\}, \mathbf{H_1})\ \mathsf{x}$$

where

$$\mathbf{H_1}(\ell) = \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon}; \mathsf{int}^{\mathcal{T}} :: \zeta\}^{\mathtt{ra}}.$$
$$\mathtt{sld\ r1, 0; +\ r1, r1, 1; +\ r1, r1, 1; sfree\ 1; ret\ ra\ \{r1\}}$$

$$f_2 = \lambda(\mathsf{x : int}).^{(\mathsf{int})\to\mathsf{int}}\mathcal{FT}\ (\mathtt{mv\ r1}, \ell; \mathtt{ret\ end}\{\mathsf{int}^{\mathcal{T}}; \cdot\}\ \{\mathtt{r1}\}, \mathbf{H_2})\ \mathsf{x}$$

where

$$\mathbf{H_2}(\ell) = \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon}; \mathsf{int}^{\mathcal{T}} :: \zeta\}^{\mathtt{ra}}.$$
$$\mathtt{sld\ r1, 0; +\ r1, r1, 1; sst\ 0, r1; jmp}\ \ell'[\zeta][\epsilon]$$
$$\mathbf{H_2}(\ell') = \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon}; \mathsf{int}^{\mathcal{T}} :: \zeta\}^{\mathtt{ra}}.$$
$$\mathtt{sld\ r1, 0; +\ r1, r1, 1; sfree\ 1; ret\ ra\ \{r1\}}$$

Claim 3.95
The two functions are equivalent, ie, $\cdot;\cdot;\cdot;\cdot;\cdot;\mathbf{out} \vdash f_1 \approx f_2 : (\mathsf{int}) \to \mathsf{int}; \cdot$, which shows that we can reason about assembly components that have similar externally visible behavior but different structure and control flow.

Proof

Expanding the definition of $\approx$, we see we need to show first that the terms are well-typed. This follows from the typing rules, noting in particular that:

$$^{(\mathsf{int})\to\mathsf{int}}\mathcal{FT}\ (\mathtt{mv\ r1}, \ell; \mathtt{ret\ end}\{\mathsf{int}^{\mathcal{T}}; \cdot\}\ \{\mathtt{r1}\}, \mathbf{H})$$

Requires that the inner component have translation type

$$(\mathsf{int}) \to \mathsf{int}^{\mathcal{T}} = \mathbf{box}\,\forall[\zeta, \epsilon].\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon}; \mathsf{int}^{\mathcal{T}} :: \zeta\}^{\mathtt{ra}}$$

And the heap must be well-typed, at the type that we'll denote $\mathbf{\Psi}$:

$$\cdot \vdash \mathbf{H} : \mathbf{\Psi}$$

For program $\mathsf{f_2}$, checking that the heap is well-typed involves checking the $\mathtt{jmp}\ \ell'[\zeta][\epsilon]$ instruction. At that point, the register file typing is the following:

$$\chi = \{\mathtt{r1} : \mathsf{int}, \mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}; \zeta\}^{\epsilon}\}$$

The full typing rule that we must satisfy at this point is:

$$\frac{\mathbf{\Psi}; \zeta, \epsilon; \chi \vdash \ell'[\zeta][\epsilon] : \mathbf{box}\,\forall[].\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}; \zeta\}^{\epsilon}; \mathsf{int} :: \zeta\}^{\mathtt{ra}} \quad \zeta, \epsilon \vdash \chi \le \{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}; \zeta\}^{\epsilon}\} \quad \cdot[\zeta, \epsilon]; \chi; \mathsf{int} :: \zeta \vdash \mathtt{ra}}{\mathbf{\Psi}; \zeta, \epsilon; \chi; \mathsf{int} :: \zeta; \mathtt{ra} \vdash \mathtt{jmp}\ \ell'[\zeta][\epsilon]}$$

Which can easily be seen to be true.

We further must show that given a suitable world W,

$$(W, \mathbf{f_1}, \mathbf{f_2}) \in \mathcal{E}[\![\mathbf{out} \vdash \mathbf{(int)} \to \mathbf{int}; \cdot]\!]$$

For this, we must show:

$$(E_1, E_2) \in \mathcal{K}[\![\mathbf{out} \vdash \mathbf{(int)} \to \mathbf{int}; \cdot]\!] \implies (W, E_1[\mathbf{f_1}], E_2[\mathbf{f_2}]) \in \mathcal{O}$$

From the definition of related contexts, it suffices to show $(W, \mathbf{f_1}, \mathbf{f_2}) \in \mathcal{V}[\![\mathbf{(int)} \to \mathbf{int}]\!]$.
In order to do this, given

- SR $\in TStackRel$
- $\rho = [\zeta \mapsto \text{SR}]$
- integer $\mathbf{v}$ (for which $(W, \mathbf{v}, \mathbf{v}) \in \mathcal{V}[\![\mathbf{int}]\!]\rho$ trivially)
- World W' such that $W' \sqsupseteq W$ and currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\zeta]\!]\rho$

We must show:

$$(W', \mathbf{f_1 v}, \mathbf{f_2 v}) \in \mathcal{E}[\![\mathbf{out} \vdash \mathbf{int}; \zeta]\!]\rho$$

As before, to do this we must show:

$$(W', E_1', E_2') \in \mathcal{K}[\![\mathbf{out} \vdash \mathbf{int}; \zeta]\!]\rho \implies (W', E_1'[\mathbf{f_1 v}], E_2'[\mathbf{f_2 v}]) \in \mathcal{O}$$

In order to do this, consider arbitrary memories $(\mathbf{M_1}, \mathbf{M_2}) : W'$.
We will then show that

$$\langle \mathbf{M_1} \mid \mathbf{f_1 v} \rangle \longmapsto \langle \mathbf{M_1'} \mid \mathbf{v_1} \rangle$$
$$\langle \mathbf{M_2} \mid \mathbf{f_2 v} \rangle \longmapsto \langle \mathbf{M_2'} \mid \mathbf{v_2} \rangle$$

Where $(\mathbf{M_1'}, \mathbf{M_2'}) : W^*$ for some $W^* \sqsupseteq W'$, which we can lift to contexts to show that:

$$\langle \mathbf{M_1} \mid E_1'[\mathbf{f_1 v}] \rangle \longmapsto \langle \mathbf{M_1'} \mid E_1'[\mathbf{v_1}] \rangle$$
$$\langle \mathbf{M_2} \mid E_2'[\mathbf{f_2 v}] \rangle \longmapsto \langle \mathbf{M_2'} \mid E_2'[\mathbf{v_2}] \rangle$$

We can then instantiate the contexts to show that $(W^*, E_1'[\mathbf{v_1}], E_2'[\mathbf{v_2}]) \in \mathcal{O}$, which we can then compose together to show that $(W', E_1'[\mathbf{f_1 v}], E_2'[\mathbf{f_2 v}]) \in \mathcal{O}$.
We argue the central reduction by appealing to the operational semantics, which will show that:

$$\langle \mathbf{M_1} \mid \mathbf{f_1 v} \rangle \longmapsto^{j_1} \langle \mathbf{M_1'} \mid \mathbf{v_1} \rangle$$
$$\langle \mathbf{M_2} \mid \mathbf{f_2 v} \rangle \longmapsto^{j_2} \langle \mathbf{M_2'} \mid \mathbf{v_2} \rangle$$

Consider the first program, letting $\mathbf{M_1} = (\mathbf{H}, \mathbf{R}, \mathbf{S})$. That is, we want to show that:

$$\langle \mathbf{M_1} \mid \mathbf{f_1 v} \rangle \longmapsto^{j_1} \langle \mathbf{M_1'} \mid \mathbf{v_1} \rangle$$

For some $\mathbf{v_1}$.

First we combine the heap fragment, reduce and then carry out the value translation for the T codeblock to an F function.

$$\begin{array}{l}\langle(\mathbf{H},\mathbf{R},\mathbf{S}) \mid \mathbf{f_1 v}\rangle \longmapsto^* \langle(\mathbf{H} \uplus \mathbf{H_1},\mathbf{R},\mathbf{S}) \mid \boldsymbol{\lambda}(\mathbf{x}:\mathbf{int}).^{\mathbf{int}}\mathcal{FT}\ (\mathtt{protect}\ \cdot, \zeta; \qquad\qquad \mathbf{v}\rangle \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{import\ r1}, {}^{\zeta}\mathcal{TF}^{\mathbf{int}}\ \mathbf{x}; \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{salloc\ 1; sst\ 0, r1;} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{mv\ ra}, \ell_{end}[\zeta]; \mathtt{jmp}\ \ell[\zeta][\mathbf{end}\{\mathbf{int}^{\mathcal{T}}; \zeta\}], \cdot)\end{array}$$

This further reduces:

$$\begin{array}{l}\langle(\mathbf{H} \uplus \mathbf{H_1},\mathbf{R},\mathbf{S}) \mid \boldsymbol{\lambda}(\mathbf{x}:\mathbf{int}).^{\mathbf{int}}\mathcal{FT}\ (\mathtt{protect}\ \cdot, \zeta; \qquad\qquad\qquad\qquad \mathbf{v}\rangle \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{import\ r1}, {}^{\zeta}\mathcal{TF}^{\mathbf{int}}\ \mathbf{x}; \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{salloc\ 1; sst\ 0, r1;} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{mv\ ra}, \ell_{end}[\zeta]; \mathtt{jmp}\ \ell[\zeta][\mathbf{end}\{\mathbf{int}^{\mathcal{T}}; \zeta\}], \cdot) \\ \longmapsto^* \\ \langle(\mathbf{H} \uplus \mathbf{H_1},\mathbf{R}[\mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathbf{end}}[\zeta]], \mathbf{v} :: \mathbf{S}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{jmp}\ \ell[\zeta][\mathbf{end}\{\mathbf{int}^{\mathcal{T}}; \zeta\}], \cdot)\rangle\end{array}$$

At which point the top of the stack contains the argument $\mathbf{v}$, the register $\mathtt{ra}$ contains the address of the return continuation created by the value translation, and we can jump to the code at ℓ.

This reduces as:

$$\begin{array}{l}\langle(\mathbf{H} \uplus \mathbf{H_1},\mathbf{R}[\mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathbf{end}}[\zeta]], \mathbf{v} :: \mathbf{S}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{jmp}\ \ell[\zeta][\mathbf{end}\{\mathbf{int}^{\mathcal{T}}; \zeta\}], \cdot)\rangle \\ \longmapsto^* \\ \langle(\mathbf{H} \uplus \mathbf{H_1},\mathbf{R}[\mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathbf{end}}[\zeta]], \mathbf{v} :: \mathbf{S}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{sld\ r1, 0;} \quad\ \rangle \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad + \mathtt{r1, r1, 1;} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad + \mathtt{r1, r1, 1;} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{sfree\ 1;} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{ret\ ra\ \{r1\}}, \cdot)\end{array}$$

Which we can then see will load the value $\mathbf{v}$ off the top of the stack, add two to it, and return:

$$\begin{array}{l}\langle(\mathbf{H} \uplus \mathbf{H_1},\mathbf{R}[\mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathbf{end}}[\zeta]], \mathbf{v} :: \mathbf{S}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{sld\ r1, 0;} \quad\ \rangle \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad + \mathtt{r1, r1, 1;} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad + \mathtt{r1, r1, 1;} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{sfree\ 1;} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \mathtt{ret\ ra\ \{r1\}}, \cdot) \\ \longmapsto^* \\ \langle(\mathbf{H} \uplus \mathbf{H_1},\mathbf{R}[\mathtt{r1} \mapsto \mathbf{v}{+}2, \mathtt{ra} \mapsto \ell_{\mathbf{end}}[\zeta]], \mathbf{S}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{ret\ ra\ \{r1\}}, \cdot)\rangle\end{array}$$

At which point, we jump to the return continuation, which then steps to $\mathtt{ret}\ \mathbf{end}\{\mathbf{int}; \zeta\}\ \{\mathtt{r1}\}$, which allows the boundary to cancel:

$$\langle(\mathbf{H} \uplus \mathbf{H}_1, \mathbf{R}[\mathtt{r1} \mapsto \mathsf{v}{+}2, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{S}) \mid {}^{\mathsf{int}}\mathcal{FT}\ (\mathtt{ret}\ \mathtt{ra}\ \{\mathtt{r1}\}, \cdot)\rangle$$
$$\longmapsto$$
$$\langle(\mathbf{H} \uplus \mathbf{H}_1, \mathbf{R}[\mathtt{r1} \mapsto \mathsf{v}{+}2, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{S}) \mid {}^{\mathsf{int}}\mathcal{FT}\ (\mathtt{ret}\ \mathtt{end}\{\mathsf{int}^{\mathcal{T}}; \zeta\}\ \{\mathtt{r1}\}, \cdot)\rangle$$
$$\longmapsto$$
$$\langle(\mathbf{H} \uplus \mathbf{H}_1, \mathbf{R}[\mathtt{r1} \mapsto \mathsf{v}{+}2, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{S}) \mid \mathsf{v}{+}2\rangle$$

Which completes the reduction of the first program.

The proof for the reduction of $\mathsf{f_2 v}$ proceeds similarly at first, but the first block jumps to the second with $\mathsf{v}{+}1$ stored at the top of the stack (replacing v). The second block is analogous to the first function, except it only adds 1 once, so the reduction proceeds as (here letting $\mathbf{M_2} = (\mathbf{H}, \mathbf{R}, \mathbf{S})$):

$\langle(\mathbf{H}, \mathbf{R}, \mathbf{S}) \mid \mathsf{f_2 v}\rangle \longmapsto \langle(\mathbf{H} \uplus \mathbf{H}_2, \mathbf{R}[\mathtt{r1} \mapsto \mathsf{v}{+}2, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{S}) \mid \mathsf{v}{+}2\rangle$.

$\mathsf{v}{+}2$ and $\mathsf{v}{+}2$ are trivially related, which means in the world W^* that the final memories fulfill (which only varies in private merged heaps and registers from the original W'),

$$(W^*, E_1'[\mathsf{v}{+}2], E_2'[\mathsf{v}{+}2]) \in \mathcal{O}$$

This can then be composed with the above reduction lifted to contexts (ie, $E_i'[\mathsf{f'v}] \longmapsto E_i'[\mathsf{v}{+}2]$) to yield the result.

□

3.9.2 Factorial Two Ways

$$\mathsf{fact_F} \quad = \lambda(\mathsf{x} : \mathsf{int}).(\mathsf{F}\ \mathsf{fold}_{\mu\alpha.(\alpha)\to\mathsf{int}}\ \mathsf{F})\ \mathsf{x}$$
where
$$\mathsf{F} = \lambda(\mathsf{f} : \mu\alpha.(\alpha) \to \mathsf{int}).\lambda(\mathsf{x} : \mathsf{int}).\mathsf{if0}\ \mathsf{x}\ 1\ ((\mathsf{unfold}\ \mathsf{f}\ \mathsf{f})\ (\mathsf{x} - 1)) * \mathsf{x}$$

$$\mathsf{fact_T} \quad = \lambda(\mathsf{x} : \mathsf{int}).{}^{(\mathsf{int})\to\mathsf{int}}\mathcal{FT}\ (\ell_{\mathrm{fact}}, \mathbf{H})\ \mathsf{x}$$
where
$$\mathbf{H}(\ell_{\mathrm{fact}}) = \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon}; \mathsf{int}^{\mathcal{T}} :: \zeta\}^{\mathtt{ra}}.$$
$$\mathtt{sld\ rn, 0; mv\ rr, 1; bnz\ rn, } \ell_{\mathrm{aux}}[\zeta][\epsilon]\mathtt{; sfree\ 1; ret\ ra\ \{rr\}}$$
$$\mathbf{H}(\ell_{\mathrm{aux}}) = \mathbf{code}[\zeta, \epsilon]\{\mathtt{rr} : \mathsf{int}, \mathtt{ri} : \mathsf{int}, \mathtt{rn} : \mathsf{int}, \mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon}; \mathsf{int}^{\mathcal{T}} :: \zeta\}^{\mathtt{ra}}.$$
$$\mathtt{* rr, rr, rn; - rn, rn, 1; bnz\ rn, } \ell_{\mathrm{aux}}[\zeta][\epsilon]\mathtt{; sfree\ 1; ret\ ra\ \{rr\}}$$

Claim 3.96
Here we again claim equivalence, this time showing how a high-level functional implementation can be shown equivalent to a low-level implementation implemented with direct jumps and register mutation. This is interesting because the the first program uses recursive types but the control flow mechanisms in T make this not necessary in the second program.

$\cdot; \cdot; \cdot; \cdot; \cdot; \mathsf{out} \vdash fact_F \approx fact_T : (\mathsf{int}) \to \mathsf{int}; \cdot$

Proof

To prove this equivalence, we use the same general approach as the (much simpler) programs with different numbers of basic blocks shown equivalent in the previous section.

First we note that both terms are well-typed, which follows from the typing rules.

We must next show that given a suitable world W,

$$(W, \mathsf{fact_F}, \mathsf{fact_T}) \in \mathcal{E}[\![\mathsf{out} \vdash (\mathsf{int}) \to \mathsf{int}; \cdot]\!]$$

For this, we must show:

$$(E_1, E_2) \in \mathcal{K}[\![\mathbf{out} \vdash \mathbf{(int)} \to \mathbf{int}; \cdot]\!] \implies (W, E_1[\mathbf{fact_F}], E_2[\mathbf{fact_T}]) \in \mathcal{O}$$

From the definition of related contexts, it suffices to show $(W, \mathbf{fact_F}, \mathbf{fact_T}) \in \mathcal{V}[\![\mathbf{(int)} \to \mathbf{int}]\!]$.

In order to do this, given

- SR $\in TStackRel$
- $\rho = [\zeta \mapsto \text{SR}]$
- integer $\mathbf{v}$ (for which $(W, \mathbf{v}, \mathbf{v}) \in \mathcal{V}[\![\mathbf{int}]\!]\rho$ trivially)
- World W' such that $W' \sqsupseteq W$ and currentMR$(W'(i_{\text{stk}})) \Subset_{W'} \mathcal{S}[\![\zeta]\!]\rho$

We must show:

$$(W', \mathbf{fact_F v}, \mathbf{fact_T v}) \in \mathcal{E}[\![\mathbf{out} \vdash \mathbf{int}; \zeta]\!]\rho$$

As before, to do this we must show:

$$(W', E_1', E_2') \in \mathcal{K}[\![\mathbf{out} \vdash \mathbf{int}; \zeta]\!]\rho \implies (W', E_1'[\mathbf{fact_F v}], E_2'[\mathbf{fact_T v}]) \in \mathcal{O}$$

At this point, deviating from the previous example, we consider two cases. In the case that $\mathbf{v} \geq 0$, we will prove this in a similar manner to the previous example, showing that:

$$\langle \mathbf{M_1} \mid \mathbf{fact_F v} \rangle \longmapsto \langle \mathbf{M_1'} \mid \mathbf{v_1} \rangle$$
$$\langle \mathbf{M_2} \mid \mathbf{fact_T v} \rangle \longmapsto \langle \mathbf{M_2'} \mid \mathbf{v_2} \rangle$$

Where $\mathbf{v_1}$ and $\mathbf{v_2}$ are related (in particular, are the same integer), at which point we will show that $(\mathbf{M_1'}, \mathbf{M_2'}) : W^*$ for some $W^* \sqsupseteq W'$, from which the rest follows as in the previous example.

If, on the other hand, $\mathbf{v} < 0$, both programs will diverge, so for arbitrary $W.k$ we will show that

$$\text{running}(k, \langle \mathbf{M_1} \mid \mathbf{fact_F v} \rangle) \wedge \text{running}(k, \langle \mathbf{M_2} \mid \mathbf{fact_T v} \rangle)$$

Which is equivalent to

$$\text{running}(k, \langle \mathbf{M_1} \mid E_1'[\mathbf{fact_F v}] \rangle) \wedge \text{running}(k, \langle \mathbf{M_2} \mid E_2'[\mathbf{fact_T v}] \rangle)$$

Which is sufficient to show membership in $\mathcal{O}$.

We will prove the first case in a similar way to the previous example, by appealing to the operational semantics.

$\langle \mathbf{M_1} \mid \mathbf{fact_F v} \rangle$
$\longmapsto^*$
$\langle \mathbf{M_1} \mid \mathbf{(\lambda (f : \mu\alpha.(\alpha) \to int).\lambda (x : int).if0\ x\ 1\ (unfold\ f\ f)\ (x - 1) * x)(fold_{\mu\alpha.(\alpha)\to int}\ F)\ v} \rangle$
$\longmapsto^*$
$\langle \mathbf{M_1} \mid \mathbf{if0\ v\ 1\ (unfold\ (fold_{\mu\alpha.(\alpha)\to int}\ F)\ (fold_{\mu\alpha.(\alpha)\to int}\ F)\ (v - 1)) * v} \rangle$

If $\mathbf{v}$ is 0, we can see this will reduce to 1, and otherwise it will step further:

$$\langle \mathbf{M_1} \mid \mathbf{if0\ v\ 1\ (unfold\ (fold}_{\mu\alpha.(\alpha)\to\mathbf{int}}\ \mathbf{F)\ (fold}_{\mu\alpha.(\alpha)\to\mathbf{int}}\ \mathbf{F)\ (v-1))} * \mathbf{v} \rangle$$
$$\longmapsto^*$$
$$\langle \mathbf{M_1} \mid \mathbf{if0\ (v-1)\ 1\ (unfold\ (fold}_{\mu\alpha.(\alpha)\to\mathbf{int}}\ \mathbf{F)\ (fold}_{\mu\alpha.(\alpha)\to\mathbf{int}}\ \mathbf{F)\ (v-2))} * \mathbf{(v-1)} * \mathbf{v} \rangle$$

Since we know $\mathbf{v} \geq 0$, this will eventually reduce to:

$$\langle \mathbf{M_1} \mid \mathbf{if0\ v\ 1\ (unfold\ (fold}_{\mu\alpha.(\alpha)\to\mathbf{int}}\ \mathbf{F)\ (fold}_{\mu\alpha.(\alpha)\to\mathbf{int}}\ \mathbf{F)\ (v-1))} * \mathbf{v} \rangle$$
$$\longmapsto^*$$
$$\langle \mathbf{M_1} \mid \mathbf{1} * \mathbf{2} * \ldots * \mathbf{(v-2)} * \mathbf{(v-1)} * \mathbf{v} \rangle$$

We now consider the second program, again for the case when $\mathbf{v} \geq 0$.

Let $(\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2}) = \mathbf{M_2}$.

As in the previous example, first we combine the heap fragment, reduce and then carry out the value translation for the T codeblock to an F function, stepping to the point of jumping into the first code block.

$$\langle (\mathbf{H_2}, \mathbf{R_2}, \mathbf{S_2}) \mid \mathbf{fact_T\ v} \rangle$$
$$\longmapsto^*$$
$$\langle (\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}, \mathbf{S_2}) \mid \boldsymbol{\lambda}\mathbf{(x : int).}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{protect}\ \cdot, \zeta;\ \mathtt{import\ r1}, {}^{\zeta}\mathcal{T}\mathcal{F}^{\mathbf{int}}\ \mathbf{x};\ \mathtt{salloc\ 1; sst\ 0, r1;}\ \mathtt{mv\ ra}, \ell_{end}[\zeta]; \mathtt{jmp}\ \ell_{fact}[\zeta][\mathbf{end\{int}^{\mathcal{T}}; \zeta\}], \cdot)\ \mathbf{v} \rangle$$
$$\longmapsto^*$$
$$\langle (\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{jmp}\ \ell_{fact}[\zeta][\mathbf{end\{int}^{\mathcal{T}}; \zeta\}], \cdot) \rangle$$

Once we jump, we load the argument off of the stack and then branch on it being zero.

$$\langle (\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{jmp}\ \ell_{fact}[\zeta][\mathbf{end\{int}^{\mathcal{T}}; \zeta\}], \cdot) \rangle$$
$$\longmapsto^*$$
$$\langle (\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{sld\ rn, 0; mv\ rr, 1;}\ \mathtt{bnz\ rn}, \ell_{\mathrm{aux}}[\zeta][\epsilon]; \mathtt{sfree\ 1; ret\ ra\ \{rr\}}) \rangle$$
$$\longmapsto^*$$
$$\langle (\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto \mathbf{v}, \mathtt{rr} \mapsto 1, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{bnz\ rn}, \ell_{\mathrm{aux}}[\zeta][\epsilon]; \mathtt{sfree\ 1; ret\ ra\ \{rr\}}) \rangle$$

As in the high-level version, if $\mathbf{v} = 0$ we can see that this reduces, via the same jump through the return continuation shown in the previous example, to 1.

Otherwise, we jump to the ℓ_{aux} codeblock:

$$\langle (\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto \mathbf{v}, \mathtt{rr} \mapsto 1, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (\mathtt{bnz\ rn}, \ell_{\mathrm{aux}}[\zeta][\epsilon]; \mathtt{sfree\ 1; ret\ ra\ \{rr\}}) \rangle$$
$$\longmapsto^*$$
$$\langle (\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto \mathbf{v}, \mathtt{rr} \mapsto 1, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathbf{int}}\mathcal{FT}\ (*\ \mathtt{rr, rr, rn; -\ rn, rn, 1;}\ \mathtt{bnz\ rn}, \ell_{\mathrm{aux}}[\zeta][\epsilon]; \mathtt{sfree\ 1; ret\ ra\ \{rr\}}) \rangle$$

This then steps by updating the return value register (rr) by multiplying it by $\mathbf{v}$ and then decreasing $\mathbf{v}$ by 1, before branching again on the updated value being 0.

$$\langle(\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto \mathbf{v}, \mathtt{rr} \mapsto 1, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathsf{int}}\mathcal{FT}\ (* \ \mathtt{rr}, \mathtt{rr}, \mathtt{rn}; - \ \mathtt{rn}, \mathtt{rn}, \mathbf{1};$$
$$\mathtt{bnz}\ \mathtt{rn}, \ell_{\mathrm{aux}}[\zeta][\epsilon];$$
$$\mathtt{sfree}\ \mathbf{1};$$
$$\mathtt{ret}\ \mathtt{ra}\ \{\mathtt{rr}\})$$
$$\longmapsto^*$$
$$\langle(\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto \mathbf{v}{-}1, \mathtt{rr} \mapsto 1{*}\mathbf{v}, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathsf{int}}\mathcal{FT}\ (\mathtt{bnz}\ \mathtt{rn}, \ell_{\mathrm{aux}}[\zeta][\epsilon];\rangle$$
$$\mathtt{sfree}\ \mathbf{1};$$
$$\mathtt{ret}\ \mathtt{ra}\ \{\mathtt{rr}\})$$

Since we know that $\mathbf{v} \geq 0$, this test will eventually succeed, at which point we will step to a return:

$$\langle(\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto 0, \mathtt{rr} \mapsto 1{*}\mathbf{v}{*}(\mathbf{v}-1){*}...{*}3{*}2, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{v} :: \mathbf{S_2}) \mid {}^{\mathsf{int}}\mathcal{FT}\ (\mathtt{bnz}\ \mathtt{rn}, \ell_{\mathrm{aux}}[\zeta][\epsilon];\rangle$$
$$\mathtt{sfree}\ \mathbf{1};$$
$$\mathtt{ret}\ \mathtt{ra}\ \{\mathtt{rr}\})$$
$$\longmapsto^*$$
$$\langle(\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto 0, \mathtt{rr} \mapsto 1{*}\mathbf{v}{*}(\mathbf{v}-1){*}...{*}3{*}2, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{S_2}) \mid {}^{\mathsf{int}}\mathcal{FT}\ (\mathtt{ret}\ \mathtt{ra}\ \{\mathtt{rr}\})\rangle$$

This steps through the return continuation to evaluate to:

$$\langle(\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto 0, \mathtt{rr} \mapsto 1{*}\mathbf{v}{*}(\mathbf{v}-1){*}...{*}3{*}2, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{S_2}) \mid {}^{\mathsf{int}}\mathcal{FT}\ (\mathtt{ret}\ \mathtt{ra}\ \{\mathtt{rr}\})\rangle$$
$$\longmapsto^*$$
$$\langle(\mathbf{H_2} \uplus \mathbf{H}, \mathbf{R_2}[\mathtt{rn} \mapsto 0, \mathtt{rr} \mapsto 1{*}\mathbf{v}{*}(\mathbf{v}-1){*}...{*}3{*}2, \mathtt{r1} \mapsto \mathbf{v}, \mathtt{ra} \mapsto \ell_{\mathrm{end}}[\zeta]], \mathbf{S_2}) \mid \mathbf{2{*}...{*}(v{-}1){*}v{*}1}\rangle$$

Which is the same as the value that the other program evaluated to.

Note that since the only changes to the memory were additions to the heap and register modifications, there exists a world $W^* \sqsupseteq W'$, which was the last piece we needed in this case.

In the second case, when $\mathbf{v} < 0$, we must show that for any k, we can show that both programs are still running after k steps.

We do this by noting that, based on the operational semantics, after the first 3 steps (which get to the if), the first program will call itself recursively with an argument 1 smaller every 4 steps. This means that for any k, after $ceil(k-3)/4+1$ iterations we will have taken more than k steps, which is sufficient.

The second program will jump to ℓ_{aux} after a small constant number of steps and then again every 3 steps, with rn decreased by 1 every time. This means that for any k, after ceil(k/3) + 1 jumps to ℓ_{aux} we will have taken more than k steps, which is sufficient to show the claim, and thus prove equivalence between the two programs.

□

3.9.3 Implementing a Mutable Reference

We can use inline T code to implement a basic mutable reference for use it F code. While the basic multi-language allows global mutable tuples, leading to trivial mutation of a statically defined value, in this case we show how we can dynamically allocate a new reference and access it from the functional language. While

multiple can be created, the stack-based nature means that only the most recently created can be accessed until the continuation for it returns.

$$
\begin{array}{l}
\textsf{withref} = \lambda(\mathit{init} : \mathit{int}, \qquad\qquad). \\
\quad k : (((\mathit{int}) \xrightarrow{\langle \mathbf{int} \rangle ; \langle \mathbf{int} \rangle} (),) \to \mathit{int} \\
\qquad (()) \xrightarrow{\langle \mathbf{int} \rangle ; \langle \mathbf{int} \rangle} \mathit{int}) \\
\quad {}^{()}\mathcal{FT}\,(\texttt{protect}\ \cdot, \zeta; \texttt{salloc}\ 1; \qquad\qquad ; \\
\qquad \texttt{import}\ \texttt{r1}, {}^{\zeta}\mathcal{TF}^{\textsf{int}}\ \textsf{init}; \\
\qquad \texttt{sst}\ 0, \texttt{r1}; \texttt{ralloc}\ \texttt{rc}, 1; \\
\qquad \texttt{salloc}\ 1; \texttt{sst}\ 0, \texttt{rc}; \texttt{mv}\ \texttt{r1}, (); \\
\qquad \texttt{ret}\ \textbf{end}\{\textbf{unit}; \langle \textbf{int} \rangle :: \zeta\}\ \{\texttt{r1}\}, \cdot) \\
\quad \textsf{let r} = \textsf{k}\,(\lambda^{\langle \mathbf{int} \rangle}_{\langle \mathbf{int} \rangle}(x : \mathit{int}). \qquad\qquad) \\
\qquad {}^{()}\mathcal{FT}\,(\texttt{protect}\ \langle \textbf{int} \rangle, \zeta; \\
\qquad\quad \texttt{sld}\ \texttt{r1}, 0; \\
\qquad\quad \texttt{import}\ \texttt{r2}, {}^{\langle \textbf{int} \rangle :: \zeta}\mathcal{TF}^{\textsf{int}}\ \textsf{x}; \\
\qquad\quad \texttt{st}\ \texttt{r1}[0], \texttt{r2}; \texttt{mv}\ \texttt{r1}, () \\
\qquad\quad \texttt{ret}\ \textbf{end}\{\textbf{unit}; \langle \textbf{int} \rangle :: \zeta\}\ \{\texttt{r1}\}, \cdot) \\
\qquad \lambda^{\langle \mathbf{int} \rangle}_{\langle \mathbf{int} \rangle}(). \\
\qquad {}^{\textsf{int}}\mathcal{FT}\,(\texttt{protect}\ \langle \textbf{int} \rangle, \zeta; \\
\qquad\quad \texttt{sld}\ \texttt{r1}, 0; \\
\qquad\quad \texttt{ld}\ \texttt{r2}, \texttt{r1}[0]; \\
\qquad\quad \texttt{ret}\ \textbf{end}\{\textbf{int}; \langle \textbf{int} \rangle :: \zeta\}\ \{\texttt{r2}\}, \cdot) \\
\textsf{in} \\
\quad {}^{()}\mathcal{FT}\,(\texttt{protect}\ \langle \textbf{int} \rangle, \zeta; \texttt{sfree}\ 1; \qquad\qquad ; \\
\qquad \texttt{mv}\ \texttt{r1}, (); \texttt{ret}\ \textbf{end}\{\textbf{unit}; \zeta\}\ \{\texttt{r1}\}, \cdot) \\
\quad \textsf{r}
\end{array}
$$

3.9.4 Higher Order

In this example we demonstrate how the multi-language supports higher order calls between languages.

$$
\begin{array}{l}
\tau = ((\mathsf{int}) \to \mathsf{int}) \to \mathsf{int} \\
\mathbf{g} = \lambda(\mathbf{h} : (\mathsf{int}) \to \mathsf{int}).\mathbf{h}\,\mathbf{1} \\
\mathbf{e} = ({}^{\mathsf{int}}\mathcal{FT}\ (\mathtt{mv}\,\mathtt{r1}, \ell; \qquad\qquad\qquad\qquad)\,\mathbf{g} \\
\qquad\qquad \mathtt{ret}\ \mathbf{end}\{(\tau) \to \mathsf{int}^{\mathcal{T}}; \bullet\}\ \{\mathtt{r1}\}, \\
\qquad\qquad \cdot) \\
\mathbf{H}(\ell) = \\
\quad \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon}; \tau^{\mathcal{T}} :: \zeta\}^{\mathtt{ra}}. \\
\qquad \mathtt{sld}\,\mathtt{r1}, \mathbf{0}; \mathtt{salloc}\,\mathbf{1}; \mathtt{sst}\,\mathbf{0}, \ell_{\mathbf{h}}; \mathtt{sst}\,\mathbf{1}, \mathtt{ra}; \\
\qquad \mathtt{mv}\,\mathtt{ra}, \ell_{\mathbf{gret}}[\zeta]; \mathtt{call}\,\mathtt{r1}\,\{\forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon} :: \zeta, \mathbf{0}\} \\
\mathbf{H}(\ell_{\mathbf{h}}) = \\
\quad \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\epsilon}; \mathsf{int}^{\mathcal{T}} :: \zeta\}^{\mathtt{ra}}. \\
\qquad \mathtt{sld}\,\mathtt{r1}, \mathbf{0}; \mathtt{sfree}\,\mathbf{1}; \mathtt{mul}\ \mathtt{r1}, \mathtt{r1}, \mathbf{2}; \mathtt{ret}\,\mathtt{ra}\,\{\mathtt{r1}\} \\
\mathbf{H}(\ell_{\mathbf{gret}}) = \\
\quad \mathbf{code}[\zeta]\{\mathtt{r1} : \mathbf{int}; \forall[].\{\mathtt{r1} : \mathsf{int}^{\mathcal{T}}; \zeta\}^{\mathbf{end}\{\mathbf{int}; \zeta\}} :: \zeta\}^{\mathbf{0}}. \\
\qquad \mathtt{sld}\,\mathtt{ra}, \mathbf{0}; \mathtt{sfree}\,\mathbf{1}; \mathtt{ret}\,\mathtt{ra}\,\{\mathtt{r1}\}
\end{array}
$$

3.9.5 Calls

This example shown the call/return structure of the `call` instruction.

$$
\begin{array}{l}
\mathbf{f} = (\mathtt{mv}\,\mathtt{ra}, \ell_{\mathbf{1ret}}; \mathtt{call}\,\ell_1\,\{\bullet, \mathbf{end}\{\mathbf{int}; \bullet\}\}, \mathbf{H}) \\
\mathbf{H}(\ell_1) = \\
\quad \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathbf{int}; \zeta\}^{\epsilon}; \zeta\}^{\mathtt{ra}}. \\
\qquad \mathtt{salloc}\,\mathbf{1}; \mathtt{sst}\,\mathbf{0}, \mathtt{ra}; \mathtt{mv}\,\mathtt{ra}, \ell_{\mathbf{2ret}}; \\
\qquad \mathtt{call}\,\ell_2\,\{\forall[].\{\mathtt{r1} : \mathbf{int}; \zeta\}^{\epsilon} :: \zeta, \mathbf{0}\} \\
\mathbf{H}(\ell_{\mathbf{1ret}}) = \quad \mathbf{code}[]\{\mathtt{r1} : \mathbf{int}; \bullet\}^{\mathbf{end}\{\mathbf{int}; \bullet\}}. \\
\qquad\qquad\qquad \mathtt{ret}\ \mathbf{end}\{\mathbf{int}; \bullet\}\ \{\mathtt{r1}\} \\
\mathbf{H}(\ell_2) = \quad \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathbf{int}; \zeta\}^{\epsilon}; \zeta\}^{\mathtt{ra}}. \\
\qquad\qquad\qquad \mathtt{mv}\,\mathtt{r1}, \mathbf{1}; \mathtt{jmp}\,\ell_{\mathbf{2aux}} \\
\mathbf{H}(\ell_{\mathbf{2aux}}) = \quad \mathbf{code}[\zeta, \epsilon]\{\mathtt{ra} : \forall[].\{\mathtt{r1} : \mathbf{int}; \zeta\}^{\epsilon}; \zeta\}^{\mathtt{ra}}. \\
\qquad\qquad\qquad \mathtt{mult}\ \mathtt{r1}, \mathtt{r1}, \mathbf{2}; \mathtt{ret}\,\mathtt{ra}\,\{\mathtt{r1}\} \\
\mathbf{H}(\ell_{\mathbf{2ret}}) = \\
\quad \mathbf{code}[]\{\mathtt{r1} : \mathbf{int}; \forall[].\{\mathtt{r1} : \mathbf{int}; \bullet\}^{\mathbf{end}\{\mathbf{int}; \bullet\}} :: \bullet\}^{\mathbf{0}}. \\
\qquad \mathtt{sld}\,\mathtt{ra}, \mathbf{0}; \mathbf{sfree1}; \mathtt{ret}\,\mathtt{ra}\,\{\mathtt{r1}\}
\end{array}
$$

References

[1] A. J. Ahmed. *Semantics of Types for Mutable State*. PhD thesis, Princeton University, Nov. 2004.

[2] D. Dreyer, G. Neis, and L. Birkedal. The impact of higher-order state and control effects on local relational reasoning. *Journal of Functional Programming*, 22(4&5):477–528, 2012.