A Relational Model of Types-and-Effects in Higher-Order Concurrent Separation Logic
Technical Appendix

October 24, 2016

Contents

1 The Language and Typing Rules

1.1 Syntax and Operational Semantics of $\lambda_{\mathit{ref,conc}}$

The syntax of $\lambda_{\mathit{ref,conc}}$ is shown in Figure **??** and the operational semantics is presented in Figure **??**. We assume given denumerably infinte sets of variables VAR, ranged over by x, y, f, and locations LOC, ranged over by l. We use v to range over the set of values, VAL, and e to range over the set of expressions, EXP. Note that expressions do not include types.

$$
\begin{array}{rl}
\textsc{Val}\ v ::= & () \mid n \mid (v,v) \mid \mathsf{inj}_i\ v \mid \mathsf{rec}\ f(x).e \mid x \mid l \\
\textsc{Exp}\ e ::= & v \mid e = e \mid e\ e \mid (e,e) \mid \mathsf{prj}_i\ e \mid \mathsf{inj}_i\ e \mid e + e \\
\mid & \mathsf{case}(e, \mathsf{inj}_1\ x \Rightarrow e, \mathsf{inj}_2\ y \Rightarrow e) \\
\mid & \mathsf{new}\ e \mid !e \mid e := e \mid \mathsf{CAS}(e,e,e) \mid e \,||\, e
\end{array}
$$

Figure 1: Syntax of $\lambda_{\mathit{ref,conc}}$.

Heaps are finite partial maps from LOC to VAL and a thread-pool is a finite partial map from thread identifiers, modelled by natural numbers $\mathbb{N}$, to expressions EXP.

The operational semantics is defined by a small-step relation between configurations consisting of a heap and a thread-pool, where each individual step of the system is either a reduction on a thread or the forking of a new thread. The semantics is defined in terms of evaluation contexts, $K \in$ ECTX. We use $K[e]$ to denote the expression obtained by plugging e into the context K and $e[v/x]$ to denote capture-avoiding substitution of value v for variable x in expressio e.

$$
\begin{aligned}
&\textsc{Heap}\ h \ \in\ \textsc{Loc} \xrightarrow{\text{fin}} \textsc{Val}\\
&\textsc{ECtx}\ K ::= [\,] \mid K = e \mid v = K \mid K\ e \mid v\ K \mid (K, e) \mid (v, K)\\
&\mid\ \ \mathsf{prj}_i\ K \mid \mathsf{inj}_i\ K \mid K + e \mid v + K \mid \mathsf{case}(K, \mathsf{inj}_1\ x \Rightarrow e, \mathsf{inj}_2\ y \Rightarrow e)\\
&\mid\ \ \mathsf{new}\ K \mid\ !K \mid K\ :=\ e \mid v\ :=\ K \mid K \,||\, e \mid e \,||\, K\\
&\mid\ \ \mathsf{CAS}(K, e, e) \mid \mathsf{CAS}(v, K, e) \mid \mathsf{CAS}(v, v, K)
\end{aligned}
$$

Pure reduction $\boxed{e \overset{\text{pure}}{\to} e'}$

$$(\mathsf{rec}\ f(x).e)\ v \overset{\text{pure}}{\to} e[v/x, \mathsf{rec}\ f(x).e/f]$$

$$\mathsf{case}(\mathsf{inj}_i\ v, \mathsf{inj}_1\ x \Rightarrow e_1, \mathsf{inj}_2\ x \Rightarrow e_2) \overset{\text{pure}}{\to} e_i[v/x]$$

$$v_1 \,||\, v_2 \overset{\text{pure}}{\to} (v_1, v_2) \qquad \mathsf{prj}_i\ (v_1, v_2) \overset{\text{pure}}{\to} v_i \qquad v_1 + v_2 \overset{\text{pure}}{\to} v_3 \quad \text{where } v_3 = v_1 + v_2$$

$$v = v \overset{\text{pure}}{\to} \mathsf{true} \qquad v_1 = v_2 \overset{\text{pure}}{\to} \mathsf{false} \qquad \text{where } v_1 \neq v_2$$

Reduction $\boxed{h; e \to h'; e'}$

$$
\begin{aligned}
h; e &\to h; e' && \text{if } e \overset{\text{pure}}{\to} e'\\
h; \mathsf{new}\ \ v &\to h \uplus [l \mapsto v]; l\\
h; !l &\to h; v && \text{if } h(l) = v\\
h[l \mapsto -]; l\ :=\ v &\to h[l \mapsto v]; ()\\
h; \mathsf{CAS}(l, v_o, v_n) &\to h; \mathsf{false} && \text{if } h(l) \neq v_o\\
h[l \mapsto v_o]; \mathsf{CAS}(l, v_o, v_n) &\to h[l \mapsto v_n]; \mathsf{true}\\
h; K[e] &\to h'; K[e'] && \text{if } h; e \to h'; e'
\end{aligned}
$$

Figure 2: Operational semantics of $\lambda_{ref,conc}$.

1.2 Typing rules

We assume a denumerably infinite set RegVar of region variables, ranged over by ρ. An atomic effect on a region ρ is either a read effect, rd_ρ, a write effect, wr_ρ, or an allocation effect, al_ρ. An effect ε is a finite set of atomic effects. The set of types is defined by the following grammar:

$$\textsc{Type}\ \tau ::= \mathbf{1} \mid \mathsf{int} \mid \mathsf{ref}_\rho\ \tau \mid \tau \times \tau \mid \tau + \tau \mid \tau \to_{\varepsilon}^{\Pi,\Lambda} \tau$$

where Π and Λ are finite sequences of region variables. Typing judgments take the form

$$\Pi \mid \Lambda \mid \Gamma \vdash e : \tau, \varepsilon$$

$$\frac{}{\Pi \mid \Lambda \mid \Gamma, x : \tau \vdash x : \tau, \emptyset} \qquad \frac{}{\Pi \mid \Lambda \mid \Gamma \vdash () : \mathbf{1}, \emptyset} \qquad \frac{v \in \{\textsf{true}, \textsf{false}\}}{\Pi \mid \Lambda \mid \Gamma \vdash v : \textsf{B}, \emptyset} \qquad \frac{v \in \mathbb{N}}{\Pi \mid \Lambda \mid \Gamma \vdash v : \textsf{int}, \emptyset}$$

$$\frac{\Pi \mid \Lambda \mid \Gamma \vdash e : \tau_i, \varepsilon}{\Pi \mid \Lambda \mid \Gamma \vdash \textsf{inj}_i\ e : \tau_1 + \tau_2, \varepsilon} \qquad \frac{\Pi \mid \Lambda \mid \Gamma \vdash e_1 : \tau, \varepsilon_1 \qquad \Pi \mid \Lambda \mid \Gamma \vdash e_2 : \tau, \varepsilon_2 \qquad eq_{type}(\tau)}{\Pi \mid \Lambda \mid \Gamma \vdash e_1 = e_2 : \textsf{B}, \varepsilon_1 \cup \varepsilon_2}$$

$$\frac{\Pi \mid \Lambda \mid \Gamma \vdash e : \tau_1 + \tau_2, \varepsilon \qquad \Pi \mid \Lambda \mid \Gamma, x_i : \tau_i \vdash e_i : \tau, \varepsilon_i}{\Pi \mid \Lambda \mid \Gamma \vdash \textsf{case}(e, \textsf{inj}_1\ x_1 \Rightarrow e_1, \textsf{inj}_2\ x_2 \Rightarrow e_2) : \textsf{B}, \varepsilon \cup \varepsilon_1 \cup \varepsilon_2} \qquad \frac{\Pi \mid \Lambda \mid \Gamma \vdash e : \tau_1 \times \tau_2, \varepsilon}{\Pi \mid \Lambda \mid \Gamma \vdash \textsf{prj}_i\ e : \tau_i, \varepsilon}$$

$$\frac{\Pi \mid \Lambda \mid \Gamma \vdash e_1 : \textsf{int}, \varepsilon_1 \qquad \Pi \mid \Lambda \mid \Gamma \vdash e_2 : \textsf{int}, \varepsilon_2}{\Pi \mid \Lambda \mid \Gamma \vdash e_1 + e_2 : \textsf{int}, \varepsilon_1 \cup \varepsilon_2} \qquad \frac{\Pi \mid \Lambda \mid \Gamma \vdash e_1 : \tau_1, \varepsilon_1 \qquad \Pi \mid \Lambda \mid \Gamma \vdash e_2 : \tau_2, \varepsilon_2}{\Pi \mid \Lambda \mid \Gamma \vdash (e_1, e_2) : \tau_1 \times \tau_2, \varepsilon_1 \cup \varepsilon_2}$$

$$\frac{\Pi \mid \Lambda \mid \Gamma, f : \tau_1 \to_{\varepsilon}^{\Pi,\Lambda} \tau_2, x : \tau_1 \vdash e : \tau_2, \varepsilon}{\Pi \mid \Lambda \mid \Gamma \vdash \textsf{rec}\ f(x).e : \tau_1 \to_{\varepsilon}^{\Pi,\Lambda} \tau_2, \emptyset} \qquad \frac{\Pi \mid \Lambda \mid \Gamma \vdash e_1 : \tau_1 \to_{\varepsilon}^{\Pi,\Lambda} \tau_2, \varepsilon_1 \qquad \Pi \mid \Lambda \mid \Gamma \vdash e_2 : \tau_1, \varepsilon_2}{\Pi \mid \Lambda \mid \Gamma \vdash e_1\ e_2 : \tau_2, \varepsilon \cup \varepsilon_1 \cup \varepsilon_2}$$

$$\frac{\Pi \mid \Lambda \mid \Gamma \vdash e : \tau, \varepsilon \qquad \rho \in \Pi, \Lambda}{\Pi \mid \Lambda \mid \Gamma \vdash \textsf{new}\ e : \textsf{ref}_\rho\ \tau, \varepsilon \cup \{al_\rho\}} \qquad \frac{\Pi \mid \Lambda \mid \Gamma \vdash e_1 : \textsf{ref}_\rho\ \tau, \varepsilon_1 \qquad \Pi \mid \Lambda \mid \Gamma \vdash e_2 : \tau, \varepsilon_2}{\Pi \mid \Lambda \mid \Gamma \vdash e_1 := e_2 : \mathbf{1}, \varepsilon_1 \cup \varepsilon_2 \cup \{wr_\rho\}}$$

$$\frac{\Pi \mid \Lambda \mid \Gamma \vdash e : \textsf{ref}_\rho\ \tau, \varepsilon}{\Pi \mid \Lambda \mid \Gamma \vdash\ !e : \tau, \varepsilon \cup \{rd_\rho\}} \qquad \frac{\Pi \mid \Lambda, \rho \mid \Gamma \vdash e : \tau, \varepsilon \qquad \rho \notin FRV(\Gamma, \tau)}{\Pi \mid \Lambda \mid \Gamma \vdash e : \tau, \varepsilon - \rho}$$

$$\frac{\Pi, \Lambda_3 \mid \Lambda_1 \mid \Gamma_1 \vdash e_1 : \tau_1, \varepsilon_1 \qquad \Pi, \Lambda_3 \mid \Lambda_2 \mid \Gamma_2 \vdash e_2 : \tau_2, \varepsilon_2}{\Pi \mid \Lambda_1, \Lambda_2, \Lambda_3 \mid \Gamma_1, \Gamma_2 \vdash e_1 \mid\mid e_2 : \tau_1 \times \tau_2, \varepsilon_1 \cup \varepsilon_2}$$

$$\frac{\Pi \mid \Lambda \mid \Gamma \vdash e_1 : \textsf{ref}_\rho\ \tau, \varepsilon_1 \qquad \Pi \mid \Lambda \mid \Gamma \vdash e_2 : \tau, \varepsilon_2 \qquad \Pi \mid \Lambda \mid \Gamma \vdash e_3 : \tau, \varepsilon_3 \qquad eq_{type}(\tau)}{\Pi \mid \Lambda \mid \Gamma \vdash \textsf{CAS}(e_1, e_2, e_3) : \textsf{B}, \varepsilon_1 \cup \varepsilon_2 \cup \varepsilon_3 \cup \{wr_\rho, rd_\rho\}}$$

$$\frac{}{eq_{type}(\mathbf{1})} \qquad \frac{\Pi \mid \Lambda \mid \Gamma \vdash e : \tau_1, \varepsilon_1 \qquad \Pi, \Lambda \vdash \tau_1 \leq \tau_2 \qquad \varepsilon_1 \subseteq \varepsilon_2 \qquad FRV(\varepsilon_2) \in \Pi, \Lambda}{\Pi \mid \Lambda \mid \Gamma \vdash e : \tau_2, \varepsilon_2}$$

$$\frac{eq_{type}(\tau) \qquad eq_{type}(\sigma) \qquad op \in \{+, \times\}}{eq_{type}(\tau\ op\ \sigma)}$$

$$\frac{FRV(\tau) \in \Pi \cup \Lambda}{\Pi \cup \Lambda \vdash \tau \leq \tau} \qquad \frac{\Pi \cup \Lambda \vdash \tau_1 \leq \tau_1' \qquad \Pi \cup \Lambda \vdash \tau_2 \leq \tau_2'}{\Pi \cup \Lambda \vdash \tau_1 \times \tau_2 \leq \tau_1' \times \tau_2'}$$

$$\frac{\Pi \cup \Lambda \vdash \tau_1 \leq \tau_1' \qquad \Pi \cup \Lambda \vdash \tau_2 \leq \tau_2' \qquad \varepsilon_1 \subseteq \varepsilon_2 \qquad \Pi_1 \subseteq \Pi_2 \qquad \Lambda_1 \subseteq \Lambda_2}{\Pi \cup \Lambda \vdash \tau_1 \to_{\varepsilon_1}^{\Pi_1,\Lambda_1} \tau_2 \leq \tau_1' \to_{\varepsilon_2}^{\Pi_2,\Lambda_2} \tau_2'}$$

Figure 3: Typing and sub-typing inference rules. We write $FV(e)$ and $FRV(e)$ for the sets of free program variables and region variables respectively. For all typing judgments on the form $\Pi \mid \Lambda \mid \Gamma \vdash e : \tau, \varepsilon$ we always have $FRV(\Gamma, \tau, \varepsilon) \in \Pi \cup \Lambda$. The equality type predicate, eq_{type}, defines the types we may test for equality.

2 Monoids and Constructions

2.1 Evaluation Context Monoid

Extended expressions $\boxed{\mathcal{E} \in EExp}$

$$\begin{aligned}\mathcal{E} \in EExp ::= & \; a \mid () \mid n \mid x \mid l \mid \textsf{rec}\ f(x).e \mid \mathcal{E} = \mathcal{E} \mid \mathcal{E}\ \mathcal{E} \mid (\mathcal{E}, \mathcal{E}) \mid \mathcal{E} + \mathcal{E} \mid \textsf{prj}_i\ \mathcal{E} \mid \textsf{inj}_i\ \mathcal{E} \\ \mid & \; \textsf{case}(\mathcal{E}, \textsf{inj}_1\ x \Rightarrow e, \textsf{inj}_2\ y \Rightarrow e) \mid \textsf{new}\ \mathcal{E} \mid !\mathcal{E} \mid \mathcal{E} := \mathcal{E} \mid \textsf{CAS}(\mathcal{E}, \mathcal{E}, \mathcal{E}) \mid \mathcal{E} \,||\, \mathcal{E}\end{aligned}$$

where $a \in \mathcal{A}$ is an address.

Extended evaluation contexts $\boxed{\kappa \in EECtx}$

$$\begin{aligned}\kappa \in EECtx \quad ::= \quad & \bullet \mid \kappa = \mathcal{E} \mid v = \kappa \mid \kappa\ \mathcal{E} \mid v\ \kappa \mid (\kappa, \mathcal{E}) \mid (v, \kappa) \mid \kappa + \mathcal{E} \mid v + \kappa \\ \mid \quad & \textsf{prj}_i\ \kappa \mid \textsf{inj}_i\ \kappa \mid \textsf{case}(\kappa, \textsf{inj}_1\ x \Rightarrow e, \textsf{inj}_2\ y \Rightarrow e) \\ \mid \quad & \textsf{new}\ \kappa \mid !\kappa \mid \kappa := \mathcal{E} \mid v := \kappa \\ \mid \quad & \kappa||\mathcal{E} \mid \mathcal{E}||\kappa \mid \textsf{CAS}(\kappa, \mathcal{E}, \mathcal{E}) \mid \textsf{CAS}(v, \kappa, \mathcal{E}) \mid \textsf{CAS}(v, v, \kappa)\end{aligned}$$

Multi evaluation contexts $\boxed{MECtx \subseteq EExp}$

$$\begin{aligned}B \in MECtx \quad ::= \quad & a \mid e \mid B = e \mid v = B \mid B\ e \mid v\ B \mid (B, e) \mid (v, B) \mid B + e \mid v + B \\ \mid \quad & \textsf{prj}_i\ B \mid \textsf{inj}_i\ B \mid \textsf{case}(B, \textsf{inj}_1\ x \Rightarrow e, \textsf{inj}_2\ y \Rightarrow e) \\ \mid \quad & \textsf{new}\ B \mid !B \mid B := e \mid v := B \\ \mid \quad & B||B \mid \textsf{CAS}(B, e, e) \mid \textsf{CAS}(v, B, e) \mid \textsf{CAS}(v, v, B)\end{aligned}$$

Free addresses $\boxed{FA : EExp \rightharpoonup \mathcal{P}(\mathcal{A})}$

$$\begin{aligned}FA(a) &\triangleq \{a\} \\ FA(()) = FA(x) = FA(l) = FA(\textsf{rec}\ f(x).e) &\triangleq \emptyset \\ FA(\textsf{prj}_i\ \mathcal{E}) = FA(\textsf{inj}_i\ \mathcal{E}) = FA(\textsf{new}\ \mathcal{E}) = FA(!\mathcal{E}) &\triangleq FA(\mathcal{E}) \\ FA(\textsf{case}(\kappa, \textsf{inj}_1\ x \Rightarrow e_1, \textsf{inj}_2\ y \Rightarrow e_2)) &\triangleq FA(\mathcal{E}) \\ FA(\mathcal{E}_1 = \mathcal{E}_2) = FA(\mathcal{E}_1\ \mathcal{E}_2) FA(\mathcal{E}_1 := \mathcal{E}_2) = FA(\mathcal{E}_1 \,||\, \mathcal{E}_2) &\triangleq FA(\mathcal{E}_1) \uplus FA(\mathcal{E}_2) \\ FA((\mathcal{E}_1, \mathcal{E}_2)) = FA(\mathcal{E}_1 + \mathcal{E}_2) &\triangleq FA(\mathcal{E}_1) \uplus FA(\mathcal{E}_2) \\ FA(\textsf{CAS}(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3)) &\triangleq FA(\mathcal{E}_1) \uplus FA(\mathcal{E}_2) \uplus FA(\mathcal{E}_3)\end{aligned}$$

where $A \uplus B$ is the union of A and B, but is only defined if A and B are disjoint.

Evaluation context monoid $\boxed{\textsc{ECtx}}$

$$\textsc{ECtx} \triangleq (\{f : \mathcal{A} \rightharpoonup_{fin} MECtx \mid \forall a \in \mathrm{dom}(f).\, \forall b \in FA(f(a)).\, a <_{\mathcal{A}} b\}, \cdot, [])$$

where $<_{\mathcal{A}}$ is strict ordering on addresses and monoid composition is defined as follows

$$f \cdot g \triangleq \begin{cases} \bot & \text{if } \mathrm{dom}(f) \cap \mathrm{dom}(g) \neq \emptyset \\ f \cup g & \text{otherwise} \end{cases}$$

Hereditarily free addresses $\boxed{FA : EExp \times |\text{ECTX}| \rightharpoonup \mathcal{P}(\mathcal{A})}$

$$FA(\mathcal{E}, f) \triangleq FA(\mathcal{E}) \uplus \biguplus\{FA(f(a), f \setminus \{a\}) \mid a \in FA(\mathcal{E}) \cap \text{dom}(f)\}$$

The $FA(\mathcal{E}, f)$ function is defined by recursively on the size of (the domain of) f.

Address substitution $\boxed{subst : EExp \times |\text{ECTX}| \to EExp}$

$$\begin{aligned}
subst(a)(f) &\triangleq \begin{cases} subst(f(a), f \setminus \{a\}) & \text{if } a \in \text{dom}(f) \\ a & \text{otherwise} \end{cases} \\
subst(e, f) &\triangleq e \\
subst(\mathcal{E}_1 = \mathcal{E}_2, f) &\triangleq subst(\mathcal{E}_1, f) = subst(\mathcal{E}_2, f) \\
subst(\mathcal{E}_1\ \mathcal{E}_2, f) &\triangleq subst(\mathcal{E}_1, f)\ subst(\mathcal{E}_2, f) \\
subst((\mathcal{E}_1, \mathcal{E}_2), f) &\triangleq (subst(\mathcal{E}_1, f), subst(\mathcal{E}_2, f)) \\
subst(\mathcal{E}_1 + \mathcal{E}_2, f) &\triangleq subst(\mathcal{E}_1, f) + subst(\mathcal{E}_2, f) \\
subst(\mathbf{prj}_i\ \mathcal{E}, f) &\triangleq \mathbf{prj}_i\ subst(\mathcal{E}, f) \\
subst(\mathbf{inj}_i\ \mathcal{E}, f) &\triangleq \mathbf{inj}_i\ subst(\mathcal{E}, f) \\
subst(\mathbf{case}(\kappa, \mathbf{inj}_1\ x \Rightarrow e_1, \mathbf{inj}_2\ y \Rightarrow e_2), f) &\triangleq \mathbf{case}(subst(\kappa, f), \mathbf{inj}_1\ x \Rightarrow e_1, \mathbf{inj}_2\ y \Rightarrow e_2) \\
subst(\mathbf{new}\ \mathcal{E}, f) &\triangleq \mathbf{new}\ subst(\mathcal{E}, f) \\
subst(!\mathcal{E}, f) &\triangleq\ !subst(\mathcal{E}, f) \\
subst(\mathcal{E}_1 := \mathcal{E}_2, f) &\triangleq subst(\mathcal{E}_1, f) := subst(\mathcal{E}_2, f) \\
subst(\mathbf{CAS}(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3), f) &\triangleq \mathbf{CAS}(subst(\mathcal{E}_1, f), subst(\mathcal{E}_2, f), subst(\mathcal{E}_3, f)) \\
subst(\mathcal{E}_1 || \mathcal{E}_2, f) &\triangleq subst(\mathcal{E}_1, f) || subst(\mathcal{E}_2, f)
\end{aligned}$$

The $subst(\mathcal{E}, f)$ function is defined by lexicographic recursion on the size of f and $\mathcal{E}$.

Extended context substitution $\boxed{-[=] : EECtx \times Exp \to MECtx}$

The extended context substitution function, $\kappa[e]$, substitues the expression e for the $\bullet$ in κ in the obvious way.

Lemma 1.

$$\forall \mathcal{E}.\, \forall f \in |\text{ECTX}|.\, \forall a \in FA(subst(\mathcal{E}, f)).\, \exists b \in FA(\mathcal{E}).\, b \leq_{\mathcal{A}} a$$

Proof. By lexicographic induction on $|f|$ and the size of $\mathcal{E}$.

- Case $\mathcal{E} = c$: if $c \in \text{dom}(f)$ then $subst(\mathcal{E}, f) = subst(f(c), f \setminus \{c\})$ and it follows by the induction hypothesis that there exists a $b \in FA(f(c))$ such that $b \leq_{\mathcal{A}} a$. Furthermore, by definition of $|\text{ECTX}|$ it follows that $c < b$ and thus by transitivity that $c <_{\mathcal{A}} a$ and $c \in FA(\mathcal{E})$.

  Conversely, if $c \notin \text{dom}(f)$ then $subst(\mathcal{E}, f) = \mathcal{E}$ and it follows trivially by choosing $b = a$.

- All remaining cases follow directly from the induction hypothesis.

□

Lemma 2.

$$\forall \mathcal{E}.\, subst(\mathcal{E}, []) = \mathcal{E}$$

Lemma 3.

$\forall \mathcal{E}. \forall f_1, f_2 \in |\text{ECtx}|.$
$(\forall a \in \mathit{FA}(\mathcal{E}). \forall b \geq_{\mathcal{A}} a. (b \in \mathit{dom}(f_1) \Leftrightarrow b \in \mathit{dom}(f_2)) \wedge f_1(b) = f_2(b)) \Rightarrow \mathit{subst}(\mathcal{E}, f_1) = \mathit{subst}(\mathcal{E}, f_2)$

Proof. By lexicographic induction on $|f_1|$ and the size of $\mathcal{E}$.

- Case $\mathcal{E} \cong a$: then $a \in \mathit{FA}(\mathcal{E})$. If $a \in \text{dom}(f_1)$ then $a \in \text{dom}(f_2)$, $f_1(a) = f_2(a)$ and thus,

$$\mathit{subst}(\mathcal{E}, f_1) = \mathit{subst}(f_1(a), f_1) \stackrel{IH}{=} \mathit{subst}(f_1(a), f_2) = \mathit{subst}(f_2(a), f_2) = \mathit{subst}(\mathcal{E}, f_2)$$

  and if $a \notin \text{dom}(f_1)$, then $a \notin \text{dom}(f_2)$ and thus $\mathit{subst}(\mathcal{E}, f_1) = a = \mathit{subst}(\mathcal{E}, f_2)$.

- All the remaining cases follow directly from the induction hypothesis.

□

Definition 1.

$$f =_a g \triangleq \forall b >_{\mathcal{A}} a. (b \in \mathit{dom}(f) \Leftrightarrow b \in \mathit{dom}(g)) \wedge f(b) = g(b)$$

Lemma 4.

$$\forall f, g. \forall a, b. a < b \wedge f =_a g \Rightarrow f =_b g$$

Proof. Let $c \in \mathcal{A}$ such that $b <_{\mathcal{A}} c$. Then by transitivity of $<_{\mathcal{A}}$ it follows that $a <_{\mathcal{A}} c$ and thus $c \in \text{dom}(f) \Leftrightarrow c \in \text{dom}(g)$ and $f(c) = g(c)$, as required. □

Corollary 1.

$$\begin{aligned}&\forall \mathcal{E}. \forall f, f_1, f_2 \in |\text{ECtx}|. \forall a.\\ &\quad a \in \mathit{dom}(f) \wedge f_1 =_a f_2 \Rightarrow \mathit{subst}(f(a), f_1) = \mathit{subst}(f(a), f_2)\end{aligned}$$

Proof. By Lemma **??** it suffices to prove that

$$b \in \text{dom}(f_1) \Leftrightarrow b \in \text{dom}(f_2) \qquad\qquad f_1(b) = f_2(b)$$

for all $b \in \mathit{FA}(f(a))$. To that end, let $b \in \mathit{FA}(f(a))$. By definition of $|\text{ECtx}|$ it follows that $a < b$ and thus by the $f_1 =_a f_2$ assumption it follows that $f_1(b) = f_2(b)$ and $b \in \text{dom}(f_1) \Leftrightarrow b \in \text{dom}(f_2)$, as required. □

Lemma 5.

$$\forall f \in |\text{ECtx}|. \forall a \in \mathcal{A}. f =_a (f \setminus \{a\})$$

Proof. Let $b \in \mathcal{A}$ such that $a < b$. Then $a \neq b$ and thus $b \in \text{dom}(f) \Leftrightarrow b \in \text{dom}(f \setminus \{a\})$ and $f(b) = (f \setminus \{a\})(b)$. □

Lemma 6.

$$\forall f, g \in |\text{ECtx}|. g \subseteq f \Rightarrow \mathit{subst}(\mathcal{E}, f) = \mathit{subst}(\mathit{subst}(\mathcal{E}, g), f)$$

Proof. By lexicographic induction on $|g|$ and the size of $\mathcal{E}$.

- Case $\mathcal{E} = a$: if $a \in \text{dom}(g)$ then

$$\begin{aligned}\mathit{subst}(\mathit{subst}(\mathcal{E}, g), f) &= \mathit{subst}(\mathit{subst}(g(a), g \setminus \{a\}), f) \stackrel{IH}{=} \mathit{subst}(g(a), f)\\ &= \mathit{subst}(f(a), f)\\ &= \mathit{subst}(f(a), f \setminus \{a\})\\ &= \mathit{subst}(\mathcal{E}, f)\end{aligned}$$

  where the second to last equality follows from Corollary **??** and Lemma **??**. If $a \notin \text{dom}(g)$ then

$$\mathit{subst}(\mathit{subst}(\mathcal{E}, g), f) = \mathit{subst}(\mathcal{E}, f)$$

- All the remaining cases follow directly from the induction hypothesis.

$\square$

Lemma 7.

$$\begin{aligned}&\forall \mathcal{E} \in EExp. \forall f \in |\textsc{ECtx}|. \, FA(\mathcal{E}) \text{ defined } \Rightarrow \\ &\quad FA(subst(\mathcal{E}, f)) = (FA(\mathcal{E}) \setminus dom(f)) \cup \bigcup \{FA(f(a)) \mid a \in FA(\mathcal{E}) \cap dom(f)\}\end{aligned}$$

Lemma 8.

$$\forall \mathcal{E}. \forall \kappa. \forall f. \, subst(\kappa[\mathcal{E}], f) = subst(\kappa[subst(\mathcal{E}, f)], f)$$

Proof. By induction on the structure of κ.

- Case $\kappa \equiv \bullet$: then $subst(\mathcal{E}, f) = subst(subst(\mathcal{E}, f), f)$ by Lemma **??**.
- Cse $\kappa \equiv \kappa_1 = \mathcal{E}'$: then

$$\begin{aligned}subst(\kappa_1[\mathcal{E}] = \mathcal{E}', f) &= (subst(\kappa_1[\mathcal{E}], f) = subst(\mathcal{E}', f)) \\ &\stackrel{IH}{=} (subst(\kappa_1[subst(\mathcal{E}, f)], f) = subst(\mathcal{E}', f)) \\ &= subst(\kappa_1[subst(\mathcal{E}, f)] = \mathcal{E}', f) \\ &= subst(\kappa[subst(\mathcal{E}, f)], f)\end{aligned}$$

- All remaining cases follow directly from the induction hypothesis.

$\square$

Lemma 9.

$$\begin{aligned}&\forall \mathcal{E}. \forall f. \forall j. \forall \kappa. \forall e \in \textsc{Exp}. \forall k \notin dom(f). \\ &\quad f(j) = \kappa[e] \land j < k \land FA(\mathcal{E}, f) = dom(f) \\ &\qquad \Rightarrow \; subst(\mathcal{E}, f) = subst(\mathcal{E}, f[j \mapsto \kappa[k], k \mapsto e])\end{aligned}$$

Proof. By lexicographic induction on $|f|$ and the size of $\mathcal{E}$.

- Case $\mathcal{E} = a$: Since $a \in FA(\mathcal{E}, f) = \mathrm{dom}(f)$ and $k \notin \mathrm{dom}(f)$ it follows that $a \neq k$. If $a = j$ then

$$\begin{aligned}&subst(\mathcal{E}, f[j \mapsto \kappa[k], k \mapsto e]) \\ &\quad = subst(\kappa[k], (f \setminus \{j\})[k \mapsto e]) \\ &\quad = subst(subst(\kappa[k], [k \mapsto e]), (f \setminus \{j\})[k \mapsto e]) \\ &\quad = subst(subst(\kappa[subst(k, [k \mapsto e])], [k \mapsto e]), (f \setminus \{j\})[k \mapsto e]) \\ &\quad = subst(subst(\kappa[e], [k \mapsto e]), (f \setminus \{j\})[k \mapsto e]) \\ &\quad = subst(\kappa[e], (f \setminus \{j\})[k \mapsto e]) \\ &\quad = subst(\kappa[e], f \setminus \{j\}) \\ &\quad = subst(\mathcal{E}, f)\end{aligned}$$

  and if $a \neq j$ then

$$\begin{aligned}subst(\mathcal{E}, f[j \mapsto \kappa[k], k \mapsto e]) &= subst(f(a), (f \setminus \{a\})[j \mapsto \kappa[k], k \mapsto e]) \\ &\stackrel{IH}{=} subst(f(a), f \setminus \{a\})) \\ &= subst(\mathcal{E}, f)\end{aligned}$$

- All remaining cases follow directly from induction hypothesis.

□

Lemma 10.

$$\begin{aligned}&\forall \mathcal{E}. \forall f. \forall j, k \in \mathit{dom}(f). \forall \kappa. \forall e \in \textsc{Exp}.\\ &\quad f(j) = \kappa[k] \wedge f(k) = e \wedge j \neq k \wedge \mathit{FA}(\mathcal{E}, f) = \mathit{dom}(f)\\ &\qquad \Rightarrow \; \mathit{subst}(\mathcal{E}, f) = \mathit{subst}(\mathcal{E}, f[j \mapsto \kappa[e], k \mapsto \bot])\end{aligned}$$

Proof. By lexicographic induction on $|f|$ and $|\mathcal{E}|$.

- Case $\mathcal{E} = a$: If $a = j$ then

$$\begin{aligned}\mathit{subst}(\mathcal{E}, f) &= \mathit{subst}(\kappa[k], f \setminus \{j\})\\ &= \mathit{subst}(\mathit{subst}(\kappa[k], [k \mapsto e]), f \setminus \{j\})\\ &= \mathit{subst}(\mathit{subst}(\kappa[\mathit{subst}(k, [k \mapsto e])], [k \mapsto e]), f \setminus \{j\})\\ &= \mathit{subst}(\kappa[e], f \setminus \{j\})\\ &= \mathit{subst}(\kappa[e], f[k \mapsto \bot] \setminus \{j\})\\ &= \mathit{subst}(\mathcal{E}, f[j \mapsto \kappa[e], k \mapsto \bot])\end{aligned}$$

  where the second to last equality follows from the fact that $k \notin \mathit{FA}(\kappa[e])$.

  If $a = k$ then $\mathrm{dom}(f) = \mathit{FA}(\mathcal{E}, f) = \{a\} \uplus \mathit{FA}(e) = \{a\}$, which is a contradiction, as $k, j \in \mathrm{dom}(f)$ and $k \neq j$.

  Lastly, if $a \neq k$ and $a \neq j$ then

$$\begin{aligned}\mathit{subst}(\mathcal{E}, f) &= \mathit{subst}(f(a), f \setminus \{a\})\\ &\overset{IH}{=} \mathit{subst}(f(a), f \setminus \{a\}[j \mapsto \kappa[e], k \mapsto \bot])\\ &= \mathit{subst}(f(a), (f[j \mapsto \kappa[e], k \mapsto \bot]) \setminus \{a\})\\ &= \mathit{subst}(\mathcal{E}, f[j \mapsto \kappa[e], k \mapsto \bot])\end{aligned}$$

- All remaining cases follow directly from the induction hypothesis.

□

Lemma 11.

$$\forall \kappa. \forall k. \forall e \in \textsc{Exp}. \; \mathit{FA}(\kappa[k]) = \mathit{FA}(\kappa[e]) \uplus \{k\}$$

Proof. By induction on κ.

- Case $\kappa = \bullet$: then $\mathit{FA}(\kappa[k]) = \mathit{FA}(k) = \{k\} = \mathit{FA}(\kappa[e]) \uplus \{k\}$.
- Case $\kappa = \kappa_1 || \mathcal{E}$: then

$$\mathit{FA}(\kappa[k]) = \mathit{FA}(\kappa_1[k]) \uplus \mathit{FA}(\mathcal{E}) \overset{IH}{=} \mathit{FA}(\kappa_1[e]) \uplus \{k\} \uplus \mathit{FA}(\mathcal{E}) = \mathit{FA}(\kappa[e]) \uplus \{k\}$$

- All remaining cases should follow directly from the induction hypothesis.

□

Lemma 12.

$$\begin{aligned}&\forall \kappa. \forall f. \forall k \in \mathit{dom}(f). \forall e \in \textsc{Exp}.\\ &\quad \mathit{FA}(\kappa[k], f) = \mathit{FA}(\kappa[e], f) \uplus \{k\} \uplus \mathit{FA}(f(k), f \setminus \{k\})\end{aligned}$$

Proof. By induction on the structure of κ.

- Case $\kappa = \bullet$: then

$$\begin{aligned} FA(\kappa[k], f) &= FA(k, f) = \{k\} \uplus FA(f(k), f \setminus \{k\}) \\ &= FA(\kappa[e], f) \uplus \{k\} \uplus FA(f(k), f \setminus \{k\}) \end{aligned}$$

- Case $\kappa = \kappa_1 || \mathcal{E}$: then

$$\begin{aligned} FA(\kappa[k], f) &= FA(\kappa_1[k]) \uplus FA(\mathcal{E}) \uplus \biguplus \{FA(f(a), f \setminus \{a\}) \mid a \in FA(\kappa_1[k]) \uplus FA(\mathcal{E})\} \\ &= FA(\kappa_1[e]) \uplus \{k\} \uplus FA(\mathcal{E}) \uplus FA(f(k), f \setminus \{k\}) \uplus \\ &\quad \biguplus \{FA(f(a), f \setminus \{a\}) \mid a \in FA(\kappa_1[e]) \uplus FA(\mathcal{E})\} \\ &= FA(\kappa_1[e], f) \uplus \{k\} \uplus FA(f(k), f \setminus \{k\}) \end{aligned}$$

- All remaining cases should follow directly from the induction hypothesis.

□

Lemma 13.

$$\begin{aligned} &\forall f. \forall j. \forall \kappa. \forall k \notin dom(f). \forall e. \\ &\quad f(j) = \kappa[e] \wedge FA(\mathcal{E}, f) = dom(f) \Rightarrow FA(\mathcal{E}, f[j \mapsto \kappa[k], k \mapsto e]) = dom(f[j \mapsto \kappa[k], k \mapsto e]) \end{aligned}$$

Proof. By lexicographic induction on $|f|$ and the size of $\mathcal{E}$. Let $f' = f[j \mapsto \kappa[k], k \mapsto e]$.

- Case $\mathcal{E} = a$: If $a = k$ then $a \in FA(\mathcal{E}, f) = \mathrm{dom}(f)$ and thus $k \in \mathrm{dom}(f)$, which is a contradiction. If $a = j$ then

$$\begin{aligned} FA(\mathcal{E}, f') &= \{j\} \uplus FA(\kappa[k], (f \setminus \{j\})[k \mapsto e]) \\ &= \{j\} \uplus FA(\kappa[e], (f \setminus \{j\})[k \mapsto e]) \uplus \{k\} \uplus FA(e, f[k \mapsto e]) \\ &= \{j, k\} \uplus FA(\kappa[e], (f \setminus \{j\})[k \mapsto e]) \\ &= \{j, k\} \uplus FA(\kappa[e], f \setminus \{j\}) \\ &= \{k\} \uplus FA(\mathcal{E}, f) \\ &= \{k\} \uplus \mathrm{dom}(f) \\ &= \mathrm{dom}(f') \end{aligned}$$

Lastly, if $a \neq k$ and $a \neq j$ then

$$\begin{aligned} FA(\mathcal{E}, f') &= \{a\} \uplus FA(f'(a), f' \setminus \{a\}) \\ &= \{a\} \uplus FA(f(a), (f \setminus \{a\})[j \mapsto \kappa[k], k \mapsto e]) \\ &\overset{IH}{=} \{a\} \uplus \mathrm{dom}((f \setminus \{a\})[j \mapsto \kappa[k], k \mapsto e]) \\ &= \{a\} \uplus (\mathrm{dom}(f[j \mapsto \kappa[k], k \mapsto e]) \setminus \{a\}) \\ &= \mathrm{dom}(f') \end{aligned}$$

- All the remaining cases should follow directly from the induction hypothesis.

□

Lemma 14.

$$\begin{aligned} &\forall f. \forall j, k \in dom(f). \forall \kappa. \forall e. \\ &\quad f(j) = \kappa[k] \wedge f(k) = e \wedge j \neq k \wedge FA(\mathcal{E}, f) = dom(f) \\ &\quad\quad \Rightarrow \; FA(\mathcal{E}, f[j \mapsto \kappa[e], k \mapsto \bot]) = dom(f[j \mapsto \kappa[e], k \mapsto \bot]) \end{aligned}$$

Proof. By lexicographic induction on $|f|$ and the size of $\mathcal{E}$. Let $f' = f[j \mapsto \kappa[e], k \mapsto \bot]$.

- Case $\mathcal{E} = a$: If $a = k$ then $\mathrm{dom}(f) \in \mathit{FA}(\mathcal{E}, f) = \{k\} \uplus \mathit{FA}(e, f \setminus \{k\}) = \{k\}$, which is a contradiction as $k, j \in \mathrm{dom}(f)$ and $k \neq j$. If $a = j$ then

$$\begin{aligned}
\mathit{FA}(\mathcal{E}, f') &= \{j\} \uplus \mathit{FA}(\kappa[e], (f \setminus \{j\})[k \mapsto \bot]) \\
&= \{j\} \uplus \mathit{FA}(\kappa[e], f \setminus \{j\}) \\
&= \{j\} \uplus (\mathit{FA}(\kappa[k], f \setminus \{j\}) \setminus \{k\}) \\
&= \mathit{FA}(\mathcal{E}, f) \setminus \{k\} \\
&= \mathrm{dom}(f) \setminus \{k\} \\
&= \mathrm{dom}(f')
\end{aligned}$$

  Lastly, if $a \neq k$ and $a \neq j$ then

$$\begin{aligned}
\mathit{FA}(\mathcal{E}, f') &= \{a\} \uplus \mathit{FA}(f'(a), f' \setminus \{a\}) \\
&= \{a\} \uplus \mathit{FA}(f(a), (f \setminus \{a\})[j \mapsto \kappa[e], k \mapsto \bot]) \\
&\overset{IH}{=} \{a\} \uplus \mathrm{dom}((f \setminus \{a\})[j \mapsto \kappa[e], k \mapsto \bot]) \\
&= \{a\} \uplus (\mathrm{dom}(f[j \mapsto \kappa[e], k \mapsto \bot]) \setminus \{a\}) \\
&= \mathrm{dom}(f')
\end{aligned}$$

- All the remaining cases should follow directly from the induction hypothesis.

$\square$

Lemma 15.

$$\forall f. \forall \mathcal{E}. \forall a \in \mathit{dom}(f). \, a \notin \mathit{FA}(\mathcal{E}, f) \Rightarrow \mathit{FA}(\mathcal{E}, f) = \mathit{FA}(\mathcal{E}, f[a \mapsto \bot])$$

Proof. By lexicographic induction on $|f|$ and $|\mathcal{E}|$.

- Case $\mathcal{E} = b$: since $a \notin \mathit{FA}(\mathcal{E}, f) = \{b\} \uplus \mathit{FA}(f(b), f \setminus \{b\})$ it follows that $a \neq b$. We thus have,

$$\begin{aligned}
\mathit{FA}(\mathcal{E}, f) &= \{b\} \uplus \mathit{FA}(f(b), f \setminus \{b\}) \\
&\overset{IH}{=} \{b\} \uplus \mathit{FA}(f(b), (f \setminus \{b\})[a \mapsto \bot]) \\
&= \{b\} \uplus \mathit{FA}(f(b), (f[a \mapsto \bot]) \setminus \{b\}) \\
&= \mathit{FA}(\mathcal{E}, f[a \mapsto \bot])
\end{aligned}$$

- All the remaining cases follow directly from the induction hypothesis.

$\square$

Lemma 16.

$$\forall f. \forall \mathcal{E}. \forall a \in \mathit{dom}(f). \, a \notin \mathit{FA}(\mathcal{E}, f) \Rightarrow \mathit{subst}(\mathcal{E}, f) = \mathit{subst}(\mathcal{E}, f[a \mapsto \bot])$$

Proof. By lexicographic induction on $|f|$ and $|\mathcal{E}|$.

- Case $\mathcal{E} = b$: since $a \notin \mathit{FA}(\mathcal{E}, f) = \{b\} \uplus \mathit{FA}(f(b), f \setminus \{b\})$ it follows that $a \neq b$. We thus have,

$$\begin{aligned}
\mathit{subst}(\mathcal{E}, f) &= \mathit{subst}(f(b), f \setminus \{b\}) \\
&\overset{IH}{=} \mathit{subst}(f(b), (f \setminus \{b\})[a \mapsto \bot]) \\
&= \mathit{subst}(f(b), (f[a \mapsto \bot] \setminus \{b\})) \\
&= \mathit{subst}(\mathcal{E}, f[a \mapsto \bot])
\end{aligned}$$

- All the remaining cases follow directly from the induction hypothesis.

□

Lemma 17.

$$\forall \mathcal{E}.\, \forall f.\, \forall j \in \mathit{dom}(f).\, \mathit{FA}(\mathcal{E}, f) = \mathit{dom}(f) \land \mathit{FA}(f(j)) = \emptyset$$
$$\Rightarrow\ \exists K.\, \forall e \in \textsc{Exp}.\, \mathit{subst}(\mathcal{E}, f[j \mapsto e]) = K[e]$$

Proof. By lexicographic induction on $|f|$ and $|\mathcal{E}|$.

- Case $\mathcal{E} = a$: if $a = j$ then $\mathrm{dom}(f) = \mathit{FA}(\mathcal{E}, f) = \mathit{FA}(f(a)) \uplus \{j\} = \{j\}$. We thus take $K = \bullet$. Then, for every $e \in \textsc{Exp}$ we have

  $$\mathit{subst}(\mathcal{E}, f[j \mapsto e]) = \mathit{subst}(e, []) = e = K[e]$$

  If $a \neq j$ then $\mathit{FA}(f(a), f \setminus \{a\}) = \mathrm{dom}(f \setminus \{a\})$ and by the induction hypothesis, there exists a K such that $\mathit{subst}(f(a), (f \setminus \{a\})[j \mapsto e]) = K[e]$. We simply pick this K:

  $$\mathit{subst}(\mathcal{E}, f[j \mapsto e]) = \mathit{subst}(f(a), (f \setminus \{a\})[j \mapsto e]) = K[e]$$

- Case $\mathcal{E} = \mathcal{E}_1\ \mathcal{E}_2$: we know that $j \in \mathrm{dom}(f) = \mathit{FA}(\mathcal{E}, f) = \mathit{FA}(\mathcal{E}_1, f) \uplus \mathit{FA}(\mathcal{E}_2, f)$. By Lemma **??** it follows that $\mathit{FA}(\mathcal{E}_1, f) = \mathit{FA}(\mathcal{E}_1, f \setminus \mathit{FA}(\mathcal{E}_2, f))$ and $\mathit{FA}(\mathcal{E}_2, f) = \mathit{FA}(\mathcal{E}_2, f \setminus \mathit{FA}(\mathcal{E}_1, f))$ and more importantly,

  $$\mathit{FA}(\mathcal{E}_1, f \setminus \mathit{FA}(\mathcal{E}_2, f)) = \mathrm{dom}(f \setminus \mathit{FA}(\mathcal{E}_2, f)) \quad \mathit{FA}(\mathcal{E}_2, f \setminus \mathit{FA}(\mathcal{E}_1, f)) = \mathrm{dom}(f \setminus \mathit{FA}(\mathcal{E}_1, f))$$

  If $j \in \mathit{FA}(\mathcal{E}_1, f)$ then by the induction hypothesis, there exists a K such that

  $$\mathit{subst}(\mathcal{E}_1, (f \setminus \mathit{FA}(\mathcal{E}_2, f))[j \mapsto e]) = K[e]$$

  for all expressions e. We thus simply pick $K\ \mathit{subst}(\mathcal{E}_2, f)$ as our context, such that

  $$\begin{aligned} \mathit{subst}(\mathcal{E}, f[j \mapsto e]) &= \mathit{subst}(\mathcal{E}_1, f[j \mapsto e])\ \mathit{subst}(\mathcal{E}_2, f[j \mapsto e]) \\ &= \mathit{subst}(\mathcal{E}_1, (f \setminus \mathit{FA}(\mathcal{E}_2, f))[j \mapsto e])\ \mathit{subst}(\mathcal{E}_2, f) \\ &= K[e]\ \mathit{subst}(\mathcal{E}_2, f) \end{aligned}$$

  for all expressions e. Here the second equality follows by Lemma **??**.

  The case of $j \in \mathit{FA}(\mathcal{E}_2, f)$ is symmetric.

- All other cases follow a similar pattern: on binary expression formers, do a case-analysis on which sub-expression j "appears" in and appeal to the induction hypothesis for that sub-expression.

□

Definition 2.

$$j \overset{\zeta}{\Rrightarrow}_S B \triangleq \boxed{\circ[j \mapsto B] : \textsc{Auth}(\textsc{ECtx})}^{\textsc{Exp}(\zeta)}$$
$$\mathit{mctx}(e, \zeta) \triangleq \exists f \in |\textsc{ECtx}|.\, \boxed{\bullet f : \textsc{Auth}(\textsc{ECtx})}^{\textsc{Exp}(\zeta)} *$$
$$\mathit{subst}(0, f) = e * \mathit{FA}(0, f) = \mathit{dom}(f)$$

Lemma 18.

$$\mathit{mctx}(e, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \kappa[e'] \Rrightarrow \exists k.\, \mathit{mctx}(e, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \kappa[k] * k \overset{\zeta}{\Rrightarrow}_S e'$$

Proof.

$$
\begin{aligned}
mctx(e, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \kappa[e'] &= \exists f.\, j \overset{\zeta}{\Rrightarrow}_S \kappa[e'] * \boxed{\bullet f}^{\zeta} * subst(0, f) = e * FA(0, f) = \mathrm{dom}(f) \\
&\Rightarrow j \overset{\zeta}{\Rrightarrow}_S \kappa[e'] * \boxed{\bullet f}^{\zeta} * subst(0, f') = e * FA(0, f) = \mathrm{dom}(f) \\
&\Rightarrow j \overset{\zeta}{\Rrightarrow}_S \kappa[e'] * \boxed{\bullet f}^{\zeta} * subst(0, f') = e * FA(0, f') = \mathrm{dom}(f') \\
&\Rrightarrow j \overset{\zeta}{\Rrightarrow}_S \kappa[k] * k \overset{\zeta}{\Rrightarrow}_S e' * \boxed{\bullet f'}^{\zeta} * subst(0, f') = e * FA(0, f') = \mathrm{dom}(f') \\
&\Rightarrow \exists k.\, j \overset{\zeta}{\Rrightarrow}_S \kappa[k] * k \overset{\zeta}{\Rrightarrow}_S e' * mctx(e, \zeta)
\end{aligned}
$$

where $f' = f[j \mapsto \kappa[k], k \mapsto e']$, the first implication follows by Lemma **??** and the second implication by Lemma **??**. ☐

Lemma 19.

$$mctx(e, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \kappa[k] * k \overset{\zeta}{\Rrightarrow}_S e' \Rrightarrow mctx(e, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \kappa[e']$$

Proof.

$$
\begin{aligned}
mctx(e, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \kappa[k] * k \overset{\zeta}{\Rrightarrow}_S e' &= \exists f.\, j \overset{\zeta}{\Rrightarrow}_S \kappa[k] * k \overset{\zeta}{\Rrightarrow}_S e' * \boxed{\bullet f}^{\zeta} * subst(0, f) = e * FA(0, f) = \mathrm{dom}(f) \\
&\Rightarrow j \overset{\zeta}{\Rrightarrow}_S \kappa[k] * k \overset{\zeta}{\Rrightarrow}_S e' * \boxed{\bullet f}^{\zeta} * subst(0, f') = e * FA(0, f) = \mathrm{dom}(f) \\
&\Rightarrow j \overset{\zeta}{\Rrightarrow}_S \kappa[k] * k \overset{\zeta}{\Rrightarrow}_S e' * \boxed{\bullet f}^{\zeta} * subst(0, f') = e * FA(0, f') = \mathrm{dom}(f') \\
&\Rrightarrow j \overset{\zeta}{\Rrightarrow}_S \kappa[e'] * \boxed{\bullet f'}^{\zeta} * subst(0, f') = e * FA(0, f') = \mathrm{dom}(f') \\
&\Rightarrow j \overset{\zeta}{\Rrightarrow}_S \kappa[e'] * mctx(e, \zeta)
\end{aligned}
$$

where $f' = f[j \mapsto \kappa[e'], k \mapsto \bot]$, the first implication follows by Lemma **??** and the second implication by Lemma **??**. ☐

Lemma 20.

$$mctx(e, \zeta) * 0 \overset{\zeta}{\Rrightarrow}_S e' \Rightarrow mctx(e, \zeta) * 0 \overset{\zeta}{\Rrightarrow}_S e' * e = e'$$

Proof. By unfolding the syntactic sugar, it follows that $subst(e', f) = e$ and since $FA(e') = \emptyset$ we have $e = e'$ as required. ☐

Lemma 21.

$$
\begin{aligned}
&\forall e, e', e_1, e_1'.\, \forall h, h'.\, \forall j. \\
&\quad mctx(e, \zeta) * j \overset{\zeta}{\Rrightarrow}_S e_1 * (h; e_1 \to h'; e_1') \Rrightarrow \exists e'.\, mctx(e', \zeta) * j \overset{\zeta}{\Rrightarrow}_S e_1' * (h; e \to h'; e')
\end{aligned}
$$

Proof. If $j = 0$ then it follows by Lemma **??** that $e = e_1$ and the conclusion thus follows easily by taking $e' = e_1'$.

Otherwise, $j \neq 0$ and by unfolding the syntactic sugar there exists an f such that

$$\boxed{\bullet f}^{\zeta} * e = subst(0, f) * FA(0, f) = \mathrm{dom}(f) * \boxed{\circ [j \mapsto e_1]}^{\zeta} * (h; e_1 \to h'; e_1')$$

By Lemma **??** there exists a K such that

$$subst(0, f[j \mapsto e'']) = K[e'']$$

for all expressions e''. Hence, in particular, $e = \mathit{subst}(0, f[j \mapsto e_1]) = K[e_1]$. We thus have

$$
\begin{aligned}
&\boxed{\bullet\, f}^{\zeta} * e = \mathit{subst}(0, f) * \mathit{FA}(0, f) = \mathrm{dom}(f) * \boxed{\circ\, [j \mapsto e_1]}^{\zeta} * (h; e_1 \to h'; e_1') \\
&\Rightarrow\ \boxed{\bullet\, f}^{\zeta} * K[e_1'] = \mathit{subst}(0, f[j \mapsto e_1']) * \mathit{FA}(0, f[j \mapsto e_1']) = \mathrm{dom}(f[j \mapsto e_1']) \\
&\quad * \ \boxed{\circ\, [j \mapsto e_1]}^{\zeta} * (h; K[e_1] \to h'; K[e_1']) \\
&\Rrightarrow \boxed{\bullet\, f[j \mapsto e_1']}^{\zeta} * K[e_1'] = \mathit{subst}(0, f[j \mapsto e_1']) * \mathit{FA}(0, f[j \mapsto e_1']) = \mathrm{dom}(f[j \mapsto e_1']) \\
&\quad * \ \boxed{\circ\, [j \mapsto e_1']}^{\zeta} * (h; K[e_1] \to h'; K[e_1']) \\
&\Rightarrow \mathit{mctx}(K[e_1'], \zeta) * j \overset{\zeta}{\Rrightarrow}_S e_1' * (h; e \to h'; K[e_1'],)
\end{aligned}
$$

$\square$

2.2 Other Monoids

Standard Iris Monoids

$$
\begin{aligned}
\textsc{AHeap} &\triangleq \textsc{Auth}(\textsc{FpFun}(\textsc{Loc}, \textsc{Val})) \\
\textsc{Sr} &\triangleq \textsc{Frac}(\{*\}) \\
\textsc{Reg} &\triangleq \textsc{FpFun}(\mathcal{RN}, \textsc{Frac}(X + (\{A \in \mathcal{P}(X) \mid |A| = 2\} \times \textsc{Heap}))) \quad \text{where } X \triangleq \mathsf{list}\ Name \\
\textsc{AFHeap} &\triangleq \textsc{Auth}(\textsc{FpFun}(\textsc{Loc}, \textsc{Frac}(\textsc{Val}))) \\
\textsc{EfReg} &\triangleq \textsc{FpFun}(\mathbb{N}, \textsc{Frac}(\{*\})) \\
\textsc{EfRegLoc} &\triangleq \textsc{FpFun}(\textsc{Loc}, \textsc{Ex}(\{*\})) \\
\textsc{AllocHeap} &\triangleq \textsc{Frac}(\mathcal{P}(\textsc{Loc}) \times \mathcal{P}(\textsc{Loc}))
\end{aligned}
$$

Disjoint Monoid

Assume a countably infinite set X, define:

$$\textsc{Disjoint} \triangleq (\mathcal{P}(X), \circ, \emptyset)$$

where

$$x \circ y \triangleq x \cup y \text{ if } x \# y$$

2.3 Syntactic Sugar

LR$_{\mathbf{ML}}$

$$
\begin{aligned}
heap(h) &\triangleq \boxed{\bullet\, h : \textsc{AHeap}}^{\pi_1(\gamma)} \\
l \mapsto v &\triangleq \boxed{\circ\, [l \mapsto v] : \textsc{AHeap}}^{\pi_1(\gamma)}
\end{aligned}
$$

LR$_{\mathbf{Eff}}$

$$
\begin{aligned}
heap(h) &\triangleq \boxed{\bullet\, h : \textsc{AHeap}}^{\pi_1(\gamma)} \\
l \mapsto v &\triangleq \boxed{\circ\, [l \mapsto v] : \textsc{AHeap}}^{\pi_1(\gamma)} \\
[\textsc{Rd}]^{\pi}_{r} &\triangleq \boxed{[r \mapsto (\pi, *)] : \textsc{EfReg}}^{\pi_2(\gamma)} \\
[\textsc{Wr}]^{\pi}_{r} &\triangleq \boxed{[r \mapsto (\pi, *)] : \textsc{EfReg}}^{\pi_3(\gamma)} \\
[\textsc{Al}]^{\pi}_{r} &\triangleq \boxed{[r \mapsto (\pi, *)] : \textsc{EfReg}}^{\pi_4(\gamma)} \\
rheap(h, r) &\triangleq \boxed{\bullet\, \widehat{h} : \textsc{AFHeap}}^{R(r)} \\
x \overset{\pi}{\hookrightarrow}_{r} v &\triangleq \boxed{\circ\, [l \mapsto v] : \textsc{AFHeap}}^{R(r)} \\
[\textsc{Rd}(x)]_{r} &\triangleq \boxed{[x \mapsto *] : \textsc{EfRegLoc}}^{\textsc{Rd}(r)} \\
[\textsc{NoRd}(x)]_{r} &\triangleq \boxed{[x \mapsto *] : \textsc{EfRegLoc}}^{\textsc{No}(r)} \\
[\textsc{Wr}(x)]_{r} &\triangleq \boxed{[x \mapsto *] : \textsc{EfRegLoc}}^{\textsc{Wr}(r)} \\
[\textsc{Al}(h)]^{\pi}_{r} &\triangleq \boxed{(\pi, \mathrm{dom}(h)) : \textsc{AllocHeap}}^{\textsc{Al}(r)}
\end{aligned}
$$

$\mathbf{LR_{Bin}}$

$$
\begin{aligned}
heap_I(h) &\triangleq \boxed{\bullet\, h : \textsc{AHeap}}^{\pi_1(\gamma)} \\
l \mapsto_I v &\triangleq \boxed{\circ\, [l \mapsto v] : \textsc{AHeap}}^{\pi_1(\gamma)} \\
heap_S(h) &\triangleq \boxed{\bullet\, h : \textsc{AHeap}}^{\pi_2(\gamma)} \\
l \mapsto_S v &\triangleq \boxed{\circ\, [l \mapsto v] : \textsc{AHeap}}^{\pi_2(\gamma)} \\
[\textsc{Rd}]^{\pi}_{r} &\triangleq \boxed{[r \mapsto (\pi, *)] : \textsc{EfReg}}^{\pi_5(\gamma)} \\
[\textsc{Wr}]^{\pi}_{r} &\triangleq \boxed{[r \mapsto (\pi, *)] : \textsc{EfReg}}^{\pi_6(\gamma)} \\
[\textsc{Al}]^{\pi}_{r} &\triangleq \boxed{[r \mapsto (\pi, *)] : \textsc{EfReg}}^{\pi_7(\gamma)} \\
mctx(f) &\triangleq \boxed{\bullet\, f : \textsc{Auth}(\textsc{ECtx})}^{\pi_8(\gamma)} \\
j \Rightarrow_S e &\triangleq \boxed{\circ\, [j \mapsto e] : \textsc{Auth}(\textsc{ECtx})}^{\pi_8(\gamma)}
\end{aligned}
$$

$$
\begin{aligned}
rheap_X(h, r) &\triangleq \boxed{\bullet\, \widehat{h} : \textsc{AFHeap}}^{X(r)} \\
x \overset{\pi}{\hookrightarrow}_{X,r} v &\triangleq \boxed{\circ\, [l \mapsto v] : \textsc{AFHeap}}^{X(r)} \\
[\textsc{Rd}(x)]_r &\triangleq \boxed{[x \mapsto *] : \textsc{EfRegLoc}}^{\textsc{Rd}(r)} \\
[\textsc{NoRd}(x)]_r &\triangleq \boxed{[x \mapsto *] : \textsc{EfRegLoc}}^{\textsc{No}(r)} \\
[\textsc{Wr}(x)]_r &\triangleq \boxed{[x \mapsto *] : \textsc{EfRegLoc}}^{\textsc{Wr}(r)} \\
[\textsc{Al}(h_1, h_2)]^{\pi}_{r} &\triangleq \boxed{(\pi, (\mathrm{dom}(h_1), \mathrm{dom}(h_2))) : \textsc{AllocHeap}}^{\textsc{Al}(r)}
\end{aligned}
$$

$\mathbf{LR_{Par}}$

$$
\begin{aligned}
heap_I(h) &\triangleq \boxed{\bullet\, h : \text{AH}\textsc{eap}}^{\pi_1(\gamma)}\\
l \mapsto_I v &\triangleq \boxed{\circ\, [l \mapsto v] : \text{AH}\textsc{eap}}^{\pi_1(\gamma)}\\
[\text{M}\textsc{u}(r, \{\zeta\})]^\pi &\triangleq \boxed{[r \mapsto (\pi, \textbf{inj}_1\ \zeta)] : \text{R}\textsc{eg}}^{\pi_2(\gamma)}\\
[\text{I}\textsc{m}(r, \zeta s, h)]^\pi &\triangleq \boxed{[r \mapsto (\pi, \textbf{inj}_2\ (\zeta s, h))] : \text{R}\textsc{eg}}^{\pi_2(\gamma)}\\
[Y]_H &\triangleq \boxed{Y : \text{D}\textsc{isjoint}}^{\pi_3(\gamma)}\\
[\text{R}\textsc{d}]^\pi_r &\triangleq \boxed{[r \mapsto (\pi, *)] : \text{E}\textsc{f}\text{R}\textsc{eg}}^{\pi_4(\gamma)}\\
[\text{W}\textsc{r}]^\pi_r &\triangleq \boxed{[r \mapsto (\pi, *)] : \text{E}\textsc{f}\text{R}\textsc{eg}}^{\pi_5(\gamma)}\\
[\text{A}\textsc{l}]^\pi_r &\triangleq \boxed{[r \mapsto (\pi, *)] : \text{E}\textsc{f}\text{R}\textsc{eg}}^{\pi_6(\gamma)}
\end{aligned}
$$

$$
\begin{aligned}
heap_S(h, \zeta) &\triangleq \boxed{\bullet\, h : \text{AH}\textsc{eap}}^{\pi_1(\zeta)}\\
l \mapsto_S^\zeta v &\triangleq \boxed{\circ\, [l \mapsto v] : \text{AH}\textsc{eap}}^{\pi_1(\zeta)}\\
mctx(f) &\triangleq \boxed{\bullet\, f : \text{A}\textsc{uth}(\text{EC}\textsc{tx})}^{\pi_2(\zeta)}\\
j \overset{\zeta}{\Rightarrow}_S e &\triangleq \boxed{\circ\, [j \mapsto e] : \text{A}\textsc{uth}(\text{EC}\textsc{tx})}^{\pi_2(\zeta)}\\
[\text{S}\textsc{r}]^\pi_\zeta &\triangleq \boxed{(\pi, *) : \text{S}\textsc{r}}^{\pi_3(\zeta)}
\end{aligned}
$$

$$
\begin{aligned}
rheap_X(h, r) &\triangleq \boxed{\bullet\, \widehat{h} : \text{AFH}\textsc{eap}}^{X(r)}\\
x \overset{\pi}{\hookrightarrow}_{X,r} v &\triangleq \boxed{\circ\, [l \mapsto v] : \text{AFH}\textsc{eap}}^{X(r)}\\
[\text{R}\textsc{d}(x)]_r &\triangleq \boxed{[x \mapsto *] : \text{E}\textsc{f}\text{R}\textsc{eg}\text{L}\textsc{oc}}^{\text{R}\textsc{d}(r)}\\
[\text{N}\textsc{o}\text{R}\textsc{d}(x)]_r &\triangleq \boxed{[x \mapsto *] : \text{E}\textsc{f}\text{R}\textsc{eg}\text{L}\textsc{oc}}^{\text{N}\textsc{o}(r)}\\
[\text{W}\textsc{r}(x)]_r &\triangleq \boxed{[x \mapsto *] : \text{E}\textsc{f}\text{R}\textsc{eg}\text{L}\textsc{oc}}^{\text{W}\textsc{r}(r)}\\
[\text{A}\textsc{l}(h_1, h_2)]^\pi_r &\triangleq \boxed{(\pi, (\text{dom}(h_1), \text{dom}(h_2))) : \text{A}\textsc{lloc}\text{H}\textsc{eap}}^{\text{A}\textsc{l}(r)}
\end{aligned}
$$

The function $\widehat{\ }$ embeds a partial finite function into a full fractional partial finite function, formally, it is pairwise applied where each map is computed as so:

$$\widehat{x \mapsto v} = x \mapsto (1, v)$$

Utility functions for invariant names

Throughout the entire paper we assume a constant invariant name HP and functions SP, RG and RF that maps simulation identifiers, region identifiers and locations into Iris names respectively. We assume each function is injective, that the images of each pair of functions is disjoint and does not contain HP.

3 The $\mathrm{LR}_{\mathrm{ML}}$ relation

We assume a list of monoid-names γ to be defined globally.

$$\begin{aligned}
\textsc{Heap} &\triangleq \exists h.\ heap(h) * \lfloor h \rfloor \\
\textsc{Ref}(\phi, x) &\triangleq \exists v.\ x \mapsto v * \phi(v)
\end{aligned}$$

$$\begin{aligned}
[\![\mathbf{1}]\!] &\triangleq \lambda x.\, x = () \\
[\![\mathsf{int}]\!] &\triangleq \lambda x.\, x \in \mathbb{N} \\
[\![\tau_1 \times \tau_2]\!] &\triangleq \lambda x.\, \exists y_1, y_2.\ x = (y_1, y_2)\ \wedge \triangleright y_1 \in [\![\tau_1]\!] \wedge \triangleright y_2, \in [\![\tau_2]\!] \\
[\![\tau_1 + \tau_2]\!] &\triangleq \lambda x.\, (\triangleright \exists y \in [\![\tau_1]\!].\ x = \mathsf{inj}_1\ y)\ \vee (\triangleright \exists y \in [\![\tau_2]\!].\ x = \mathsf{inj}_2\ y) \\
[\![\tau_1 \to \tau_2]\!] &\triangleq \lambda x.\, \Box \forall y.\ (\triangleright y \in [\![\tau_1]\!])\ \Rightarrow \mathcal{E}([\![\tau_2]\!])(x\ y) \\
[\![\mathsf{ref}\ \tau]\!] &\triangleq \lambda x.\, \boxed{\textsc{Ref}([\![\tau]\!], x)}^{\textsc{Rf}(x)}
\end{aligned}$$

$$\mathcal{E}(\phi) \triangleq \lambda x.\, \left\{\boxed{\textsc{Heap}}^{\textsc{Hp}}\right\}\ x\ \left\{v.\ \phi(v)\right\}_{\top}$$

Logical relatedness

$$\overline{x : \tau} \models_{\mathrm{ML}} e : \tau \triangleq\ \ \vdash_{\mathrm{Iris}} \forall \overline{x'}.\ \overline{[\![\tau]\!](x')}\ \Longrightarrow\ \mathcal{E}([\![\tau]\!])(e[x'/x])$$

Theorem 1 (Fundamental Theorem)**.** *If* $\Pi \mid \Delta \mid \Gamma \vdash e : \tau, \varepsilon$ *then* $\Pi \mid \Delta \mid \Gamma \models_{\mathrm{ML}} e : \tau, \varepsilon$

Proof. Proof omitted. ☐

4 The $\mathrm{LR}_{\mathbf{Eff}}$ relation

We assume a list of monoid-names γ to be defined globally.

$$\textsc{Heap} \triangleq \exists h.\ heap(h) * \lfloor h \rfloor$$

$$\textsc{Ref}(r, \phi, x) \triangleq \exists v.\ x \overset{\frac{1}{2}}{\hookrightarrow}_r v * \mathit{effs}(r, \phi, x, v)$$

$$\textsc{Reg}(r) \triangleq locs(r) * tokens(r)$$

where

$$M : \mathcal{RV} \xrightarrow{\text{fin}} MonoidName\ \mathsf{list}$$

$$\begin{aligned}
\mathit{effs}(r, \phi, x, v) &\triangleq ([\textsc{Wr}(x)]_r \vee x \overset{\frac{1}{2}}{\hookrightarrow}_r v) * ([\textsc{Rd}(x)]_r \vee (\phi(v) * [\textsc{NoRd}(x)]_r)) \\
locs(r) &\triangleq \exists h.\ rheap(h, r) * alloc(h, r) * \circledast_{(l,v) \in h} l \mapsto v * \circledast_{\{x \mid x \in Loc \setminus \mathrm{dom}(h)\}} [\textsc{NoRd}(x)]_r \\
toks(r) &\triangleq ([\textsc{Wr}]_r^{\pi_{wr}} \vee \circledast_{x \in Loc} [\textsc{Wr}(x)]_r) * ([\textsc{Rd}]_r^{\pi_{rd}} \vee \circledast_{x \in Loc} [\textsc{Rd}(x)]_r) \\
alloc(h, r) &\triangleq ([\textsc{Al}(r)]_1 * [\textsc{Al}(h)]_r^{\frac{1}{2}}) \vee [\textsc{Al}(h)]_r^1
\end{aligned}$$

$$\begin{aligned}
[\![\mathbf{1}]\!]^M &\triangleq \lambda x.\ x = () \\
[\![\mathsf{int}]\!]^M &\triangleq \lambda x.\ x \in \mathbb{N} \\
[\![\tau_1 \times \tau_2]\!]^M &\triangleq \lambda x.\ \exists y_1, y_2.\ x = (y_1, y_2)\ \wedge \triangleright y_1 \in [\![\tau_1]\!]^M \wedge \triangleright y_2, \in [\![\tau_2]\!]^M \\
[\![\tau_1 + \tau_2]\!]^M &\triangleq \lambda x.\ (\triangleright \exists y \in [\![\tau_1]\!]^M.\ x = \mathsf{inj}_1\ y)\ \vee (\triangleright \exists y \in [\![\tau_2]\!]^M.\ x = \mathsf{inj}_2\ y) \\
[\![\tau_1 \to_\varepsilon^{\Pi,\Lambda} \tau_2]\!]^M &\triangleq \lambda x.\ \Box \forall y.\ (\triangleright y \in [\![\tau_1]\!]^M)\ \Rightarrow \mathcal{E}_{\varepsilon,M}^{\Pi;\Lambda}([\![\tau_2]\!]^M)(x\ y)) \\
[\![\mathsf{ref}_\rho\ \tau]\!]^M &\triangleq \lambda x.\ \boxed{\textsc{Ref}(M(\rho), [\![\tau]\!]^M, x)}^{\textsc{Rf}(x)} * \boxed{\textsc{Reg}(M(\rho))}^{\textsc{Rg}(M(\rho))}
\end{aligned}$$

$$\begin{aligned}
P_{toks}(\rho, r, \pi, \varepsilon) &\triangleq (\rho \notin \mathsf{rds}\ \varepsilon \vee [\textsc{Rd}]_r^\pi) * (\rho \notin \mathsf{wrs}\ \varepsilon \vee [\textsc{Wr}]_r^\pi) * (\rho \notin \mathsf{als}\ \varepsilon \vee [\textsc{Al}]_r^\pi) \\
P_{reg}(R, g, \varepsilon, M) &\triangleq \circledast_{\rho \in R} P_{toks}(\rho, M(\rho), g(\rho), \varepsilon) * \boxed{\textsc{Reg}(M(\rho))}^{\textsc{Rg}(M(\rho))}
\end{aligned}$$

$$\begin{aligned}
\mathcal{E}_{\varepsilon,M}^{\Pi;\Lambda}(\phi) \triangleq \lambda x.\ &\forall g \in \Pi \to Perm. \\
&\Big\{\boxed{\textsc{Heap}}^{\textsc{Hp}} * P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M) * P_{reg}(\Pi, g, \varepsilon, M)\Big\} \\
&\quad x \\
&\{v.\ \phi(v) * P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M) * P_{reg}(\Pi, g, \varepsilon, M)\}_\top
\end{aligned}$$

Logical relatedness

$$\begin{aligned}
&\Pi \mid \Lambda \mid \overline{x : \tau} \models_{\textsc{Eff}} e : \tau, \varepsilon \triangleq \\
&\quad \vdash_{\textsc{Iris}} \forall M. \forall \overline{x'}.\ \overline{[\![\tau]\!]^M(x')} \implies \mathcal{E}_{\varepsilon,M}^{\Pi;\Lambda}([\![\tau]\!]^M)(e[x'/x])
\end{aligned}$$

Theorem 2 (Fundamental Theorem)**.** *If* $\Pi \mid \Delta \mid \Gamma \vdash e : \tau, \varepsilon$ *then* $\Pi \mid \Delta \mid \Gamma \models_{\textsc{Eff}} e : \tau, \varepsilon$

Proof. Proof omitted. □

4.1 Example: Type violating assignments

The code below illustrates the possibility to temporarily break the type-constraints for references in private regions.

$$x := (); x := \mathsf{True}$$

The above example clearly violates the type of the parameter x, however, we would still like to show:

$$\cdot \mid \cdot \mid \textsf{\textbf{ref}}_\rho\ \textsf{\textbf{B}} \vdash x := (); x := \textsf{True} : \mathbf{1}, \{wr_\rho, rd_\rho\}$$

which means we would have to show for $M = M'[\rho \mapsto r]$:

$$\mathcal{E}^{\cdot;\rho}_{\{wr_\rho, rd_\rho\},M}(\llbracket \mathbf{1} \rrbracket^M)(x := (); x := \textsf{True})$$

We define the following evaluation context:

$$K^1 \quad \triangleq \quad []; x := \textsf{True}$$

Lemmas

Lemma 22.

$$\forall r.\ \triangleright\textsc{Reg}(r) \iff \textsc{Reg}(r)$$

Proof. $\triangleright$ can be removed by VSTimeless since ghost resources are timeless. $\square$

Lemma 23.

$$\forall r, \phi, x.\ \triangleright\textsc{Ref}(r, \phi, x) \iff \textsc{Ref}(r, \triangleright\phi, x)$$

Lemma 24 (Trade write tokens)**.**

$$\forall h, r.\ \mathit{tokens}(h, 1, 1, r) * [\textsc{Wr}]^1_r \iff \mathit{tokens}(h, 1, 1, r) * \circledast_{x \in Loc}[\textsc{Wr}(x)]_r$$

Lemma 25 (Trade read tokens)**.**

$$\forall h, r.\ \mathit{tokens}(h, 1, 1, r) * [\textsc{Rd}]^1_r \iff \mathit{tokens}(h, 1, 1, r) * \circledast_{x \in Loc}[\textsc{Rd}(x)]_r$$

Lemma 26 (Trade region points-to)**.**

$$\forall r, \phi, x, v.\ \mathit{effs}(r, \phi, x, v) * [\textsc{Wr}(x)]_r \Leftrightarrow \mathit{effs}(r, \phi, x, v) * x \overset{\frac{1}{2}}{\hookrightarrow}_r v$$

Lemma 27 (Trade Read for NoRead)**.**

$$\forall r, \phi, x, v.\ \mathit{effs}(r, \phi, x, v) * [\textsc{Rd}(x)]_r \Leftrightarrow \mathit{effs}(r, \phi, x, v) * \phi(v) * [\textsc{NoRd}(x)]_r$$

Lemma 28 (Region heap has mapping)**.**

$$\forall h, x, v, \pi, r.\ \mathit{locs}(h, r) * x \overset{\pi}{\hookrightarrow}_r v \Rightarrow \exists h'.\ h = h'[x \mapsto v]$$

Proof. By owning an authorative fragment $x \overset{\pi}{\hookrightarrow}_r v$ it must be that for $\mathit{regheap}(\hat{h}, r)$, $\hat{h}$ contains $[x \mapsto v]$ since this is the corresponding authorative element. Since the hat function is just an injection from a partial map to one with a full fragment, there exists some h' such that $h = h'[x \mapsto v]$. $\square$

Lemma 29 (Obtain points-to)**.**

$$\forall h, h', r, x, v.\ h = h'[x \mapsto v] * \mathit{locs}(h, r) \Leftrightarrow \mathit{regheap}(\hat{h}, r) * \mathit{alloc}(h, r) * \circledast_{(l,v') \in h'} l \mapsto v' * x \mapsto v$$

Lemma 30 (Update concrete heap)**.**

$$\begin{aligned} \forall x, v.\ \boxed{\textsc{Heap}}^{\textsc{Hp}} \vdash\ & \{x \mapsto -\} \\ & \quad x := v \\ & \{v'.\ v' = () * x \mapsto v\} \end{aligned}$$

Proof.

Context: $x, v, \boxed{\textsc{Heap}}^{\textsc{Hp}}$

$\{x \mapsto -\}_{\{\textsc{Hp}\}}$

Open Hp

$\{\triangleright \textsc{Heap} * x \mapsto -\}$

$\{\textsc{Heap} * x \mapsto -\}$

$\{\exists h.\ \mathit{heap}(h[x \mapsto -], \gamma) * \lfloor h[x \mapsto -] \rfloor * x \mapsto -\}$

$\quad x := v$

$\{v'.\ v' = () * \exists h.\ \mathit{heap}(h[x \mapsto v], \gamma) * \lfloor h[x \mapsto v] \rfloor * x \mapsto v\}$

$\{v'.\ v' = () * \textsc{Heap} * x \mapsto v\}$

$\{v'.\ v' = () * x \mapsto v\}_{\{\textsc{Hp}\}}$

$\square$

Lemma 31 (Make type-violating assignment)**.**

$$\begin{aligned}
&\forall r, x, v, \phi.\ \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)}, \boxed{\textsc{Ref}(r, \phi, x)}^{\textsc{Rf}(x)} \vdash \\
&\quad \big\{[\textsc{Wr}]_r^1 * [\textsc{Rd}]_r^1\big\} \\
&\qquad x := v \\
&\quad \big\{v'.\ v' = () * [\textsc{Wr}]_r^1 * \circledast_{x' \in Loc \setminus \{x\}} [\textsc{Rd}(x')]_r * [\textsc{NoRd}(x)]_r\big\}
\end{aligned}$$

Proof.

Context: $r, x, v, \phi, \boxed{\text{HEAP}}^{\text{HP}}, \boxed{\text{REG}(r)}^{\text{RG}(r)}, \boxed{\text{REF}(x,\phi,x)}^{\text{RF}(x)}$

$\{[\text{WR}]_r^1 * [\text{RD}]_r^1\}_{\{\text{HP},\text{RG}(r),\text{RF}(x)\}}$

Open $\text{RG}(r), \text{RF}(x)$

$\{\triangleright\text{REG}(r) * \triangleright\text{REF}(r,\phi,x) * [\text{WR}]_r^1 * [\text{RD}]_r^1\}_{\{\text{HP}\}}$

By Lemma ?? and Lemma ??

$\{\text{REG}(r) * \text{REF}(r,\triangleright\phi,x) * [\text{WR}]_r^1 * [\text{RD}]_r^1\}_{\{\text{HP}\}}$

By Lemma ?? and Lemma ??

$$\left\{\begin{array}{l}\exists h.\ \mathit{locs}(h,r) * \mathit{tokens}(h,1,1,r) * \text{REF}(r,\triangleright\phi,x) * \\ \circledast_{x'\in Loc\setminus\{x\}}([\text{WR}(x')]_r * [\text{RD}(x')]_r) * [\text{WR}(x)]_r * [\text{RD}(x)]_r\end{array}\right\}_{\{Hp\}}$$

FRAME

$\{\exists h.\ \mathit{locs}(h,r) * \text{REF}(r,\triangleright\phi,x) * [\text{WR}(x)]_r * [\text{RD}(x)]_r\}_{\{\text{HP}\}}$

$$\left\{\exists h.\ \mathit{locs}(h,r) * x \overset{\frac{1}{2}}{\hookrightarrow}_r - * \mathit{effs}(r,\phi,x,-) * [\text{WR}(x)]_r * [\text{RD}(x)]_r\right\}_{\{\text{HP}\}}$$

By Lemma ??, Lemma ?? and Lemma ??

$$\left\{\exists h.\ \mathit{locs}(h[x\mapsto -],r) * x \overset{1}{\hookrightarrow}_r - * \mathit{effs}(r,\phi,x,-) * [\text{NORD}(x)]_r\right\}_{\{\text{HP}\}}$$

By Lemma ??

$$\left\{\begin{array}{l}\exists h.\ \mathit{regheap}(h[x \hat{\mapsto} -],r) * \mathit{alloc}(h[x\mapsto -],r) * \circledast_{(l,w)\in h} l \mapsto w * x \mapsto - * \\ x \overset{1}{\hookrightarrow}_r - * \mathit{effs}(r,\phi,x,-) * [\text{NORD}(x)]_r\end{array}\right\}_{\{\text{HP}\}}$$

FRAME

$\{x \mapsto -\}_{\{\text{HP}\}}$

$x := v$

$\{v'.\ v' = () * x \mapsto -\}_{\{\text{HP}\}}$ By Lemma ??

$$\left\{\begin{array}{l}v'.\ v' = () * \exists h.\ \mathit{regheap}(h[x \hat{\mapsto} -],r) * \mathit{alloc}(h[x\mapsto -],r) * \circledast_{(l,w)\in h} l \mapsto w * \\ x \mapsto v * x \overset{1}{\hookrightarrow}_r - * \mathit{effs}(r,\phi,x,-) * [\text{NORD}(x)]_r\end{array}\right\}_{\{\text{HP}\}}$$

Updated region points-to by having full fraction and having both the full and the fragmental authorative parts by AFHEAPUPD.

$$\left\{\begin{array}{l}v'.\ v' = () * \exists h.\ \mathit{regheap}(h[x \hat{\mapsto} v],r) * \mathit{alloc}(h[x\mapsto -],r) * \circledast_{(l,w)\in h} l \mapsto w * \\ x \mapsto v * x \overset{1}{\hookrightarrow}_r v * \mathit{effs}(r,\phi,x,v) * [\text{NORD}(x)]_r\end{array}\right\}_{\{\text{HP}\}}$$

$$\left\{v'.\ v' = () * \exists h.\ \mathit{locs}(h,r) * x \overset{\frac{1}{2}}{\hookrightarrow}_r v * x \overset{\frac{1}{2}}{\hookrightarrow}_r v * \mathit{effs}(r,\phi,x,v) * [\text{NORD}(x)]_r\right\}_{\{\text{HP}\}}$$

By Lemma ??

$\{v'.\ v' = () * \exists h.\ \mathit{locs}(h,r) * \text{REF}(r,\phi,x) * [\text{WR}(x)]_r * [\text{NORD}(x)]_r\}_{\{\text{HP}\}}$

$$\left\{\begin{array}{l}v'.\ v' = () * \exists h.\ \mathit{locs}(h,r) * \mathit{tokens}(h,1,1,r) * \text{REF}(r,\phi,x) * \\ \circledast_{x'\in Loc\setminus\{x\}}([\text{WR}(x')]_r * [\text{RD}(x')]_r) * [\text{WR}(x)]_r * [\text{NORD}(x)]_r\end{array}\right\}_{\{Hp\}}$$

By Lemma ??

$\{v'.\ v' = () * \text{REG}(r) * \text{REF}(r,\phi,x) * [\text{WR}]_r^1 * \circledast_{x'\in Loc\setminus\{x\}}[\text{RD}(x')]_r * [\text{NORD}(x)]_r\}_{\{\text{HP}\}}$

$\{v'.\ v' = () * [\text{WR}]_r^1 * \circledast_{x'\in Loc\setminus\{x\}}[\text{RD}(x')]_r * [\text{NORD}(x)]_r\}_{\{\text{HP},\text{RG}(r),\text{RF}(x)\}}$

□

Lemma 32 (Make type-respecting assignment)**.**

$$\forall r,x,v,\phi.\ \boxed{\text{HEAP}}^{\text{HP}}, \boxed{\text{REG}(r)}^{\text{RG}(r)}, \boxed{\text{REF}(r,\phi,x)}^{\text{RF}(x)}, \phi(v) \vdash$$
$$\{[\text{WR}]_r^1 * \circledast_{x'\in Loc\setminus\{x\}}[\text{RD}(x')]_r * [\text{NORD}(x)]_r\}$$
$$x := v$$
$$\{v'.\ v' = () * [\text{WR}]_r^1 * [\text{RD}]_r^1\}$$

Proof. The proof follows the same outline as above, except for the last line, before closing $\textsc{Rg}(r), \textsc{Rf}(x)$, by having $\phi(v) * [\textsc{NoRd}(x)]_r$ we can use Lemma **??** to obtain $\circledast_{x' \in Loc}[\textsc{Rd}(x')]_r$ to which we can use Lemma **??** to obtain $[\textsc{Rd}]^1_r$ □

Proof

Context: $\rho, M, y, \boxed{\textsc{Heap}}^{\textsc{Hp}}, \triangleright[\![\mathbf{ref}_\rho\ \mathbf{B}]\!]^M(y)$

$\{P_{reg}(\rho, \mathbf{1}, \{wr_\rho, rd_\rho\}, M)\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

$e[y/x]$

$\left\{[\textsc{Wr}]^1_{M(\rho)} * [\textsc{Rd}]^1_{M(\rho)} * \boxed{\textsc{Reg}(M(\rho))}^{\textsc{Rg}(M(\rho))}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

Context: $\rho, M, y, \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Reg}(M(\rho))}^{\textsc{Rg}(M(\rho))}, \boxed{\textsc{Ref}(M(\rho, [\![\mathbf{B}]\!]^M, y))}^{\textsc{Rf}(y)}$

Bind on $K^1[y := ()]$

$\left\{[\textsc{Wr}]^1_{M(\rho)} * [\textsc{Rd}]^1_{M(\rho)}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

Lemma ??

$\left\{[\textsc{Wr}]^1_{M(\rho)} * [\textsc{Rd}]^1_{M(\rho)}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

$x := ()$

$\left\{\begin{array}{l} v^1.\ v^1 = () * [\textsc{Wr}]^1_{M(\rho)} * \circledast_{x \in Loc \setminus \{y\}}[\textsc{Rd}(x)]_{M(\rho)} * \\ [\textsc{NoRd}(y)]_{M(\rho)} \end{array}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

$\forall v^1.\ \left\{\begin{array}{l} v^1 = () * [\textsc{Wr}]^1_{M(\rho)} * \circledast_{x \in Loc \setminus \{y\}}[\textsc{Rd}(x)]_{M(\rho)} * \\ [\textsc{NoRd}(y)]_{M(\rho)} \end{array}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

Lemma ??

$\left\{[\textsc{Wr}]^1_{M(\rho)} * \circledast_{x \in Loc \setminus \{y\}}[\textsc{Rd}(x)]_{M(\rho)} * [\textsc{NoRd}(y)]_{M(\rho)}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

$\left\{\begin{array}{l} [\textsc{Wr}]^1_{M(\rho)} * \circledast_{x \in Loc \setminus \{y\}}[\textsc{Rd}(x)]_{M(\rho)} * [\textsc{NoRd}(y)]_{M(\rho)} * \\ \mathsf{True} \in [\![\mathbf{B}]\!]^M \end{array}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

$x := \mathsf{True}$

$\left\{v^2.\ v^2 = () * [\textsc{Wr}]^1_{M(\rho)} * [\textsc{Rd}]^1_{M(\rho)}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

$\left\{v^2.\ v^2 = () * [\textsc{Wr}]^1_{M(\rho)} * [\textsc{Rd}]^1_{M(\rho)}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

$\left\{v^2.\ v^2 = () * [\textsc{Wr}]^1_{M(\rho)} * [\textsc{Rd}]^1_{M(\rho)} * \boxed{\textsc{Reg}(M(\rho))}^{\textsc{Rg}(M(\rho))}\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

$\left\{v^2.\ v^2 = () * P_{reg}(\rho, \mathbf{1}, \{wr_\rho, rd_\rho\}, M)\right\}_{\{\textsc{Rg}(M(\rho)), \textsc{Rf}(y), \textsc{Hp}\}}$

5 The $\mathrm{LR}_{\mathbf{Bin}}$ relation

For a pair $x \triangleq (x_1, x_2)$ we have $x_I \triangleq \pi_1(x)$ and $x_S \triangleq \pi_2(x)$ when x_I and x_S is not defined in the context. Similarly, for a pair $X = (X_1, X_2)$, we have $X_\Pi \triangleq \pi_1(X)$ and $X_\Lambda \triangleq \pi_2(X)$.

$$\begin{aligned}
\textsc{Heap} &\triangleq \exists h.\ \mathit{heap}(h, \gamma) * \lfloor h \rfloor \\
\textsc{Spec}(h_0, e_0) &\triangleq \exists h, e.\ \mathit{heap}_S(h) * \mathit{mctx}(e, \gamma) * (h_0, e_0) \to^* (h, e) \\
\textsc{Ref}(r, \phi, x) &\triangleq \exists v.\ x_I \overset{\frac{1}{2}}{\hookrightarrow}_{I,r} v_I * x_S \overset{\frac{1}{2}}{\hookrightarrow}_{S,r} v_S * \mathit{effs}(r, \phi, x, v) \\
\textsc{Reg}(r) &\triangleq \mathit{locs}(r) * \mathit{tokens}(r)
\end{aligned}$$

where

$$\begin{aligned}
\mathit{effs}(r, \phi, x, v) &\triangleq ([\textsc{Wr}(x)]_r \lor (x_I \overset{\frac{1}{2}}{\hookrightarrow}_{I,r} _ * x_S \overset{\frac{1}{2}}{\hookrightarrow}_{S,r} _)) * ([\textsc{Rd}(x)]_r \lor ((v_I, v_S) \in \phi * [\textsc{NoRd}(x)]_r)) \\
\mathit{locs}(r) &\triangleq \exists h.\ \mathit{rheap}_I(h_I, r) * \mathit{rheap}_S(h_S, r) * \mathit{alloc}(h, r) * \circledast_{(l,v) \in h_I} l \mapsto_I v * \circledast_{(l,v) \in h_S} l \mapsto_S^\gamma v * \\
&\qquad \circledast_{\{x | x \in (\mathit{Loc} \setminus \mathrm{dom}(h_I)) \times (\mathit{Loc} \setminus \mathrm{dom}(h_S))\}} [\textsc{NoRd}(x)]_r \\
\mathit{tokens}(r) &\triangleq ([\textsc{Wr}]_r^{\pi_{wr}} \lor \circledast_{x \in \mathit{Loc}^2} [\textsc{Wr}(x)]_r) * ([\textsc{Rd}]_r^{\pi_{rd}} \lor \circledast_{x \in \mathit{Loc}^2} [\textsc{Rd}(x)]_r) \\
\mathit{alloc}(h, r) &\triangleq ([\textsc{Al}]_r^1 * [\textsc{Al}(h_I, h_S)]_r^{\frac{1}{2}}) \lor [\textsc{Al}((h_I, h_S))]_r^1
\end{aligned}$$

For $M \triangleq \mathcal{RN} \overset{\text{fin}}{\rightharpoonup} \mathit{MonoidName}$ list:

$$\begin{aligned}
[\![\mathbf{1}]\!]^M &\triangleq \lambda x.\ x_I = x_S = () \\
[\![\mathsf{int}]\!]^M &\triangleq \lambda x.\ x_I, x_S \in \mathbb{N} \land x_I = x_S \\
[\![\tau_1 \times \tau_2]\!]^M &\triangleq \lambda x.\ \exists y_1, y_2, z_1, z_2.\ x_I = (y_1, y_2) \land x_S = (z_1, z_2) \ \land \\
&\qquad \triangleright(y_1, z_1) \in [\![\tau_1]\!]^M \land \triangleright(y_2, z_2) \in [\![\tau_2]\!]^M \\
[\![\tau_1 + \tau_2]\!]^M &\triangleq \lambda x.\ (\triangleright\exists(y_I, y_S) \in [\![\tau_1]\!]^M.\ x_I = \mathsf{inj}_1\ y_I \land x_S = \mathsf{inj}_1\ y_S) \ \lor \\
&\qquad (\triangleright\exists(y_I, y_S) \in [\![\tau_2]\!]^M.\ x_I = \mathsf{inj}_2\ y_I \land x_S = \mathsf{inj}_2\ y_S) \\
[\![\tau_1 \to_\varepsilon^{\Pi,\Lambda} \tau_2]\!]^M &\triangleq \lambda x.\ \Box\forall y_I, y_S.\ (\triangleright(y_I, y_S) \in [\![\tau_1]\!]^M) \Rightarrow \mathcal{E}_{\varepsilon,M}^{\Pi;\Lambda}([\![\tau_2]\!]^M)(x_I\ y_I, x_S\ y_S) \\
[\![\mathsf{ref}_\rho\ \tau]\!]^M &\triangleq \lambda x.\ \boxed{\textsc{Ref}(M(\rho), [\![\tau]\!]^M, x_I, x_S)}^{\textsc{Rf}(x_I, x_S)} * \boxed{\textsc{Reg}(M(\rho))}^{\textsc{Rg}(M(\rho))}
\end{aligned}$$

$$\begin{aligned}
P_{toks}(\rho, r, \pi, \varepsilon) &\triangleq (\rho \notin \mathsf{rds}\ \varepsilon \lor [\textsc{Rd}]_r^\pi) * (\rho \notin \mathsf{wrs}\ \varepsilon \lor [\textsc{Wr}]_r^\pi) * (\rho \notin \mathsf{als}\ \varepsilon \lor [\textsc{Al}]_r^\pi) \\
P_{reg}(R, g, \varepsilon, M) &\triangleq \mathop{\circledast}_{\rho \in R} P_{toks}(\rho, M(\rho), g(\rho), \varepsilon) * \boxed{\textsc{Reg}(M(\rho))}^{\textsc{Rg}(M(\rho))}
\end{aligned}$$

$$\begin{aligned}
&\mathcal{E}_{\varepsilon,M}^{\Pi;\Lambda}(\phi)(e_I, e_S) \triangleq \forall g \in \Pi \to \mathit{Perm}, j : \mathcal{A}, e_0 : \textsc{Exp}, \textsc{Hp}, \textsc{Sp}, h_0. \\
&\quad \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0)}^{\textsc{Sp}} \vdash \{j \Rightarrow_S e_S * P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M) * P_{reg}(\Pi, g, \varepsilon, M)\} \\
&\qquad\qquad e_I \\
&\qquad\qquad \{v_I.\ \exists v_S.\ j \Rightarrow_S v_S * \phi(v_I, v_S) * P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M) * P_{reg}(\Pi, g, \varepsilon, M)\}_\top
\end{aligned}$$

Logical relatedness

$$\begin{aligned}
&\Pi \mid \Lambda \mid \overline{x : \tau} \models_{\textsc{Bin}} e_1 \leq_{log} e_2 : \tau, \varepsilon \triangleq \\
&\quad \vdash_{\textsc{Iris}} \forall M.\forall \overline{x_I}, \overline{x_S}.\ \overline{[\![\tau]\!]^M(x_I, x_S)} \\
&\qquad \Longrightarrow \mathcal{E}_{\varepsilon,M}^{\Pi;\Lambda}([\![\tau]\!]^M)(e_1[x_I/x], e_2[x_S/x])
\end{aligned}$$

Theorem 3 (Fundamental Theorem)**.** *If* $\Pi \mid \Delta \mid \Gamma \vdash e : \tau, \varepsilon$ *then* $\Pi \mid \Delta \mid \Gamma \models_{\textsc{Bin}} e \leq_{log} e : \tau, \varepsilon$

Proof. Proof omitted. $\square$

Theorem 4 (Soundness). *If* $\Pi \mid \Delta \mid \Gamma \models_{\textsc{Bin}} e_I \leq_{log} e_S : \tau, \varepsilon$ *then* $\Pi \mid \Delta \mid \Gamma \vdash e_I \leq_{ctx} e_S : \tau, \varepsilon$.

Proof. Proof omitted. $\square$

5.1 Example: Type violating assignments

Consider the following two programs:

$$e_1 \triangleq (x := (); x := \textbf{true}) \qquad e_2 \triangleq x := \textbf{true}$$

We would like to show the following:

$$\cdot \mid \rho \mid x : \textbf{ref}_\rho\ \textbf{B} \models_{\textsc{Bin}} e_1 \preceq e_2 : \mathbf{1}, \{wr_\rho, rd_\rho\}$$

which means that we have to show:

$$\mathcal{E}^{\Pi;\Lambda}_{\{wr_\rho, rd_\rho\}, M}([\![\mathbf{1}]\!]^M)(e_1, e_2)$$

Lemma 33.

$$\forall r.\ \textsc{Reg}(r) * [\textsc{Rd}]^1_r \iff \textsc{Reg}(r) * \circledast_{x \in \textsc{Loc}^2} [\textsc{Rd}(x)]_r$$

Lemma 34.

$$\begin{array}{l}\forall r, \pi, \phi, x, v.\\ \quad \{[\textsc{Wr}]^\pi_r * [\textsc{Rd}(x)]_r * \textsc{Ref}(r, \triangleright\phi, x) * \textsc{Reg}(r) * \textsc{Heap}\}\\ \qquad x := v\\ \quad \{w.\ w = () * [\textsc{Wr}]^\pi_r * [\textsc{NoRd}(x)]_r * \textsc{Ref}(r, \phi, x) * \textsc{Reg}(r) * \textsc{Heap}\}\end{array}$$

Proof. Follows from view-shifts shown in the article and appendix $\square$

Lemma 35.

$$\begin{array}{l}\forall j, r, \pi, \phi, x, v.\\ \quad \{j \Rightarrow_S x_S := v_S * [\textsc{Wr}]^\pi_r * [\textsc{NoRd}(x)]_r * \textsc{Ref}(r, \triangleright\phi, x) * \textsc{Reg}(r) * \textsc{Heap} * \phi(v_I, v_S)\}\\ \qquad x := v_I\\ \quad \{w.\ w = () * j \Rightarrow_S () * [\textsc{Wr}]^\pi_r * [\textsc{Rd}(x)]_r * \textsc{Ref}(r, \phi, x) * \textsc{Reg}(r) * \textsc{Heap}\}\end{array}$$

Proof. Follows from view-shifts shown in the article and appendix $\square$

Context: $x, j, M, \rho, \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}}^{\textsc{Sp}}$
`// Let` $r = M(\rho)$ `and` $R = \{\texttt{Hp}, \texttt{Sp}, \texttt{Rf}(x), \texttt{Rg}(r)\}$

$$\left\{ j \Rightarrow_S x_S := \textbf{true} * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * \boxed{\textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x)}^{\textsc{Rf}(x)} * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} \right\}_R$$

Bind on $x_I := (); x_I := \textbf{true}$

$$\left\{ j \Rightarrow_S x_S := \textbf{true} * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * \boxed{\textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x)}^{\textsc{Rf}(x)} * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} \right\}_R$$

Open R

$$\left\{ j \Rightarrow_S x_S := \textbf{true} * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * \triangleright\textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x) * \triangleright\textsc{Reg}(r) * \triangleright\textsc{Heap} * \triangleright\textsc{Spec} \right\}$$

`// Follows from VSTimeless`

$$\left\{ j \Rightarrow_S x_S := \textbf{true} * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * \textsc{Ref}(r, \triangleright[\![\mathbf{1}]\!]^M, x) * \textsc{Reg}(r) * \textsc{Heap} * \textsc{Spec} \right\}$$

`// Follows from Lemma ??`

$$\left\{ \begin{array}{l} j \Rightarrow_S x_S := \textbf{true} * [\textsc{Wr}]^1_r * \textsc{Ref}(r, \triangleright[\![\mathbf{1}]\!]^M, x) * \textsc{Reg}(r) * \textsc{Heap} * \textsc{Spec} * \\ \circledast_{x \in \textsc{Loc}^2} [\textsc{Rd}(x)]_r \end{array} \right\}$$

$x := ()$

`// Follows from Lemma ??`

$$\left\{ \begin{array}{l} w.\ w = () * j \Rightarrow_S x_S := \textbf{true} * [\textsc{Wr}]^1_r * \textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x) * \textsc{Reg}(r) * \textsc{Heap} * \textsc{Spec} * \\ \circledast_{y \in \textsc{Loc}^2 \setminus \{x\}} [\textsc{Rd}(y)]_r * [\textsc{NoRd}(x)]_r \end{array} \right\}$$

$$\left\{ \begin{array}{l} w.\ w = () * j \Rightarrow_S x_S := \textbf{true} * [\textsc{Wr}]^1_r * \boxed{\textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x)}^{\textsc{Rf}(x)} * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ \circledast_{y \in \textsc{Loc}^2 \setminus \{x\}} [\textsc{Rd}(y)]_r * [\textsc{NoRd}(x)]_r \end{array} \right\}_R$$

Open R

$$\left\{ \begin{array}{l} j \Rightarrow_S x_S := \textbf{true} * [\textsc{Wr}]^1_r * \textsc{Ref}(r, \triangleright[\![\mathbf{1}]\!]^M, x) * \textsc{Reg}(r) * \textsc{Heap} * \textsc{Spec} * \\ \circledast_{y \in \textsc{Loc}^2 \setminus \{x\}} [\textsc{Rd}(y)]_r * [\textsc{NoRd}(x)]_r \end{array} \right\}$$

$x := \textbf{true}$

`// Follows from Lemma ??`

$$\left\{ \begin{array}{l} w'.\ w' = () * j \Rightarrow_S () * [\textsc{Wr}]^1_r * \textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x) * \textsc{Reg}(r) * \textsc{Heap} * \textsc{Spec} * \\ \circledast_{y \in \textsc{Loc}^2 \setminus \{x\}} [\textsc{Rd}(y)]_r * [\textsc{Rd}(x)]_r \end{array} \right\}$$

$$\left\{ \begin{array}{l} w'.\ w' = () * j \Rightarrow_S () * [\textsc{Wr}]^1_r * \textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x) * \textsc{Reg}(r) * \textsc{Heap} * \textsc{Spec} * \\ \circledast_{y \in \textsc{Loc}^2} [\textsc{Rd}(y)]_r \end{array} \right\}$$

`// Follows from Lemma ??`

$$\left\{ w'.\ w' = () * j \Rightarrow_S () * [\textsc{Wr}]^1_r * \textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x) * \textsc{Reg}(r) * \textsc{Heap} * \textsc{Spec} * [\textsc{Rd}]^1_r \right\}$$

$$\left\{ w'.\ w' = () * j \Rightarrow_S () * [\textsc{Wr}]^1_r * \boxed{\textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x)}^{\textsc{Rf}(x)} * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Rd}]^1_r \right\}_R$$

$$\left\{ w'.\ \exists w_S.\ j \Rightarrow_S w_S * [\textsc{Wr}]^1_r * \boxed{\textsc{Ref}(r, [\![\mathbf{1}]\!]^M, x)}^{\textsc{Rf}(x)} * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Rd}]^1_r * [\![\mathbf{1}]\!]^M(w', w_S) \right\}_R$$

5.2 Example: Local state

We have intensionally defined our logical relations to support local state that is not tracked by the type-and-effect system. This means that we can for instance prove that a pure expression approximates an impure expression at a pure effect type, because the impure expression uses untracked local state. To illustrate, consider the following two functions:

$$e_1 \triangleq \textbf{true} \qquad e_2 \triangleq \textbf{let}\ x = \textbf{new true in}\ !x$$

thus we would like to show:

$$\cdot \mid \cdot \mid \cdot \models_{\textsc{Eff}} e_1 \preceq e_2 : \mathbf{B}, \emptyset$$

Context: $\boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}}^{\textsc{Sp}}$

$\{j \Rightarrow_S e_2\}$

Open Sp

$\{\textsc{Spec} * j \Rightarrow_S e_2\}$

$\{\textsc{Spec} * \exists v_S.\ j \Rightarrow_S\ !v_S * v_S \mapsto_S \textsf{true}\}$

$\{\textsc{Spec} * \exists v_S, v'_S.\ j \Rightarrow_S v'_S * v_S \mapsto_S \textsf{true} * v'_S = \textsf{true}\}$

$\{\exists v_S, v'_S.\ j \Rightarrow_S v'_S * v'_S = \textsf{true}\}$

true

$\{v_I.\ v_I = \textsf{true} * \exists v_S, v'_S.\ j \Rightarrow_S v'_S * v'_S = \textsf{true}\}$

$\left\{v_I.\ \exists v'_S.\ j \Rightarrow_S v'_S * (v_I, v'_S) \in [\![\textsf{B}]\!]^M\right\}$

As a consequence of this choice to allow local state not tracked by the type-and-effect system, it is possible to have non-determinism in expressions that we deem semantically pure. For instance, the following expression returns 1 or 2 non-deterministically, but can be proven to be semantically pure, because it only uses local state.

$$e \triangleq \textsf{let}\ x = \textsf{new}\ 0\ \textsf{in}\ x \ := \ 1 \,||\, x \ := \ 2; !x$$

6 The $\mathrm{LR}_{\mathbf{Par}}$ relation

For a pair $x \triangleq (x_1, x_2)$ we have $x_I \triangleq \pi_1(x)$ and $x_S \triangleq \pi_2(x)$ when x_I and x_S is not defined in the context. Similarly, for a pair $X = (X_1, X_2)$, we have $X_\Pi \triangleq \pi_1(X)$ and $X_\Lambda \triangleq \pi_2(X)$. We assume a list of monoid-names γ to be defined globally. A spec can either be active ($\pi < 1$) or finished ($\pi = 1$).

$$\begin{aligned}
\textsc{Heap} &\triangleq \exists h_I.\ \mathit{heap}_I(h_I) * \lfloor h_I \rfloor \\
\textsc{Ref}(r, \phi, x) &\triangleq \exists v.\ \mathit{ref}(r, \phi, x, v) \\
\textsc{Reg}(r) &\triangleq \exists h.\ \mathit{locs}(h, r) * \mathit{toks}(1, 1, r)
\end{aligned}$$

$$\textsc{Spec}(h_0, e_0, \zeta) \triangleq \exists h, e.\ \mathit{heaps}_S(h, \zeta) * \mathit{mctx}(e, \zeta) * (h_0, e_0) \to^* (h, e) * ([\textsc{Sr}]^1_\zeta \vee ([\textsc{Sr}]^{\frac{1}{2}}_\zeta * \mathit{disj}_H(h_0, h)))$$

where

$$\begin{aligned}
\mathit{ref}(r, \phi, x, v) &\triangleq x_I \overset{\frac{1}{2}}{\hookrightarrow}_{I,r} v_I * x_S \overset{\frac{1}{2}}{\hookrightarrow}_{S,r} v_S * \mathit{effs}(r, \phi, x, v) \\
\mathit{effs}(r, \phi, x, v) &\triangleq ([\textsc{Wr}(x)]_r \vee (x_I \overset{\frac{1}{2}}{\hookrightarrow}_{I,r} _ * x_S \overset{\frac{1}{2}}{\hookrightarrow}_{S,r} _)) * \\
&\qquad ([\textsc{Rd}(x)]_r \vee (\phi(v_I, v_S) * [\textsc{NoRd}(x)]_r)) \\
\mathit{locs}(h, r) &\triangleq \exists \zeta s.\ \mathit{locs}(h, r, \zeta s, \zeta s) \\
\mathit{locs}(h, r, \zeta s, \zeta s') &\triangleq \mathit{rheap}_I(h_I, r) * \mathit{rheap}_S(h_S, r) * \mathit{alloc}(h, r) * \\
&\qquad \mathit{slink}(r, \zeta s, h_S, \tfrac{1}{2}, \tfrac{1}{4}) * \circledast_{(l,v) \in h_I} l \mapsto v * \circledast_{\zeta \in \zeta s'} \circledast_{(l,v) \in h_S} l \mapsto^\zeta_S v * \\
&\qquad \circledast_{x \in (\mathit{Loc} \setminus \mathrm{dom}(h_I)) \times (\mathit{Loc} \setminus \mathrm{dom}(h_S))} [\textsc{NoRd}(x)]_r \\
\mathit{slink}(r, \zeta s, h, \pi, \pi') &\triangleq ([\textsc{Mu}(r, \zeta s)]^\pi \vee [\textsc{Im}(r, \zeta s, h)]^{\pi'}) \\
\mathit{toks}(\pi_{rd}, \pi_{wr}, r) &\triangleq ([\textsc{Wr}]^{\pi_{wr}}_r \vee \circledast_{x \in \mathit{Loc}^2} [\textsc{Wr}(x)]_r) * ([\textsc{Rd}]^{\pi_{rd}}_r \vee \circledast_{x \in \mathit{Loc}^2} [\textsc{Rd}(x)]_r) \\
\mathit{alloc}(h, r) &\triangleq ([\textsc{Al}]^1_r * [\textsc{Al}(h_I, h_S)]^{\frac{1}{2}}_r) \vee [\textsc{Al}(h_I, h_S)]^1_r \\
\mathit{disj}_H(h_0, h) &\triangleq \exists h_Y.\ [h_Y]_H \wedge \mathrm{dom}(h_0) \cap h_Y = \emptyset \wedge (\mathrm{dom}(h) \setminus \mathrm{dom}(h_0)) \subset h_Y
\end{aligned}$$

$$\begin{aligned}
[\![\mathbf{1}]\!]^M &\triangleq \lambda x.\ x_I = x_S = () \\
[\![\mathbf{int}]\!]^M &\triangleq \lambda x.\ x_I, x_S \in \mathbb{N} \wedge x_I = x_S \\
[\![\tau_1 \times \tau_2]\!]^M &\triangleq \lambda x.\ \exists y_1, y_2, z_1, z_2.\ x_I = (y_1, y_2) \wedge x_S = (z_1, z_2) \ \wedge \\
&\qquad \triangleright(y_1, z_1) \in [\![\tau_1]\!]^M \wedge \triangleright(y_2, z_2) \in [\![\tau_2]\!]^M \\
[\![\tau_1 + \tau_2]\!]^M &\triangleq \lambda x.\ (\triangleright\exists(y_I, y_S) \in [\![\tau_1]\!]^M.\ x_I = \mathbf{inj}_1\ y_I \wedge x_S = \mathbf{inj}_1\ y_S) \ \vee \\
&\qquad (\triangleright\exists(y_I, y_S) \in [\![\tau_2]\!]^M.\ x_I = \mathbf{inj}_2\ y_I \wedge x_S = \mathbf{inj}_2\ y_S) \\
[\![\tau_1 \to^{\Pi,\Lambda}_\varepsilon \tau_2]\!]^M &\triangleq \lambda x.\ \Box\forall y_I, y_S.\ (\triangleright(y_I, y_S) \in [\![\tau_1]\!]^M) \Rightarrow \mathcal{E}^{\Pi;\Lambda}_{\varepsilon,M}([\![\tau_2]\!]^M)(x_I\ y_I, x_S\ y_S) \\
[\![\mathbf{ref}_\rho\ \tau]\!]^M &\triangleq \lambda x.\ \boxed{\textsc{Ref}(M(\rho), [\![\tau]\!]^M, x)}^{\textsc{Rf}(x)} * \boxed{\textsc{Reg}(M(\rho))}^{\textsc{Rg}(M(\rho))}
\end{aligned}$$

$$
\begin{aligned}
P_{par}(R,g,\varepsilon,M,\zeta) &\triangleq \mathop{\circledast}_{\rho \in mutable(R,g,\varepsilon)} [\textsc{Mu}(M(\rho),\{\zeta\})]^{g(\rho)} \ast \\
&\qquad \mathop{\circledast}_{\rho \in R \setminus mutable(R,g,\varepsilon)} \exists \zeta s.\ slink(M(\rho),\{\zeta\} \uplus \zeta s, h, g(\rho), g(\rho)) \\
P_{toks}(\rho,r,\pi,\varepsilon) &\triangleq (\rho \notin \mathsf{rds}\ \varepsilon \vee [\textsc{Rd}]^{\pi}_{r}) \ast (\rho \notin \mathsf{wrs}\ \varepsilon \vee [\textsc{Wr}]^{\pi}_{r}) \ast (\rho \notin \mathsf{als}\ \varepsilon \vee [\textsc{Al}]^{\pi}_{r}) \\
P_{reg}(R,g,\varepsilon,M,\zeta) &\triangleq P_{par}(R,\tfrac{\mathbf{1}}{\mathbf{2}} \circ g,\varepsilon,M,\zeta) \ast \mathop{\circledast}_{\rho \in R} P_{toks}(\rho,M(\rho),g(\rho),\varepsilon) \ast \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} \\
mutable(R,g,\varepsilon) &\triangleq \mathsf{wrs}\ \varepsilon \cup \mathsf{als}\ \varepsilon \cup \left\{\rho \mid \rho \in R \wedge g(\rho) = \tfrac{1}{2}\right\}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{E}^{\Pi;\Lambda}_{\varepsilon,M}(\phi)(e_I,e_S) \triangleq{} & \forall g \in \Pi \to Perm, j \in \mathcal{A}, e_0 \in \textsc{Exp}, h_0, \pi, \zeta. \\
& \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(e_0,h_0,\zeta)}^{\textsc{Sp}(\zeta)} \vdash \\
& \quad \left\{ j \overset{\zeta}{\Rightarrow}_S e_S \ast [\textsc{Sr}]^{\pi}_{\zeta} \ast P_{reg}(\Lambda,\mathbf{1},\varepsilon,M,\zeta) \ast P_{reg}(\Pi,g,\varepsilon,M,\zeta) \right\} \\
& \qquad e_I \\
& \quad \left\{ v_I.\ \exists v_S.\ j \overset{\zeta}{\Rightarrow}_S v_S \ast [\textsc{Sr}]^{\pi}_{\zeta} \ast P_{reg}(\Lambda,\mathbf{1},\varepsilon,M,\zeta) \ast P_{reg}(\Pi,g,\varepsilon,M,\zeta) \ast \phi(v_I,v_S) \right\}_{\top}
\end{aligned}
$$

Logical relatedness

$$
\begin{aligned}
&\Pi \mid \Lambda \mid \overline{x:\tau} \models_{\textsc{Par}} e_1 \leq_{log} e_2 : \tau, \varepsilon \triangleq \\
&\quad \vdash_{\textsc{Iris}} \forall M. \forall \overline{x_I}, \overline{x_S}.\ \overline{[\![\tau]\!]^M(x_I,x_S)} \\
&\qquad \implies \mathcal{E}^{\Pi;\Lambda}_{\varepsilon,M}([\![\tau]\!]^M)(e_1[x_I/x], e_2[x_S/x])
\end{aligned}
$$

Theorem 5 (Soundness)**.** *If* $\Pi \mid \Delta \mid \Gamma \models_{\textsc{Bin}} e_I \leq_{log} e_S : \tau, \varepsilon$ *then* $\Pi \mid \Delta \mid \Gamma \vdash e_I \leq_{ctx} e_S : \tau, \varepsilon$.

Proof. Proof in end of appendix. □

6.1 Fundamental Theorem

Theorem 6 (Fundamental Theorem)**.** *If* $\Pi \mid \Delta \mid \Gamma \vdash e : \tau, \varepsilon$ *then* $\Pi \mid \Delta \mid \Gamma \models_{\textsc{Bin}} e \leq_{log} e : \tau, \varepsilon$

Proof. Hard cases are shown below □

We will use the predicates below to make proving specific properties about their internal state easier. The intended meaning and naming remains.

$$\begin{aligned}\textsc{Spec}(h_0, h, e_0, e, \pi, \zeta) &\triangleq heap_S(h, \zeta) * mctx(e, \zeta) * (h_0, e_0) \to^* (h, e) * [\textsc{Sr}]^{\pi}_{\zeta} * \\ &\qquad (\pi = 1 \vee (\pi < 1 * disj_H(h_0, h))) \\ \textsc{Spec}(h_0, e_0, \zeta) &\triangleq \exists h, e.\ \textsc{Spec}(h_0, h, e_0, e, \frac{1}{2}, \zeta)\end{aligned}$$

$$\begin{aligned}S(\zeta, j, h_0, e_0, e, \pi, R, g, \varepsilon, M) \triangleq{}& \boxed{\textsc{Spec}(e_0, h_0, \zeta)}^{\textsc{Sp}(\zeta)} * j \overset{\zeta}{\Rrightarrow}_S e * [\textsc{Sr}]^{\pi}_{\zeta} * P_{reg}(R_{\Lambda}, \mathbf{1}, \varepsilon, M, \zeta) * \\ & P_{reg}(R_{\Pi}, g, \varepsilon, M, \zeta)\end{aligned}$$

Open invariants

Lemma 36 (Can remove $\triangleright$)**.**

$$\triangleright\textsc{Heap} \Rrightarrow \textsc{Heap} \tag{1}$$
$$\forall \zeta.\ \triangleright\textsc{Spec}(h_0, e_0, \zeta) \Rrightarrow \textsc{Spec}(h_0, e_0, \zeta) \tag{2}$$
$$\forall r.\ \triangleright\textsc{Reg}(r) \Rrightarrow \textsc{Reg}(r) \tag{3}$$
$$\forall r, \phi, x.\ \triangleright\textsc{Ref}(r, \phi, x) \Rrightarrow \textsc{Ref}(r, \triangleright\phi, x) \tag{4}$$

Proof. $\triangleright$ commute over $*$ and all assertions inside are either ghost-resource or pure statements thus we can use Timeless to remove the $\triangleright$. □

Specification reduction

Lemma 37 (Specification reduction / no allocation)**.**

$$\begin{aligned}&\forall j, e_0, e, e_1, e_1', e_1', \pi, \pi', h_0, h, h', K, \zeta. \\ &\qquad (heap_S(h, \zeta) * disj_H(h_0, h) \Rrightarrow heap_S(h', \zeta) * disj_H(h_0, h') \Rightarrow \\ &\qquad \textsc{Spec}(h_0, h, e_0, e, \pi, \zeta) * [\textsc{Sr}]^{\pi'}_{\zeta} * j \overset{\zeta}{\Rrightarrow}_S K[e_1] * (h, e_1) \to (h', e_1') \\ \Rrightarrow\ &\qquad \exists e'.\ \textsc{Spec}(h_0, h', e_0, e, \pi, \zeta) * [\textsc{Sr}]^{\pi'}_{\zeta} * j \overset{\zeta}{\Rrightarrow}_S K[e_1']\end{aligned}$$

Proof.

$$
\begin{aligned}
& \textsc{Spec}(h_0, h, e_0, e, \pi, \zeta) * [\textsc{Sr}]_{\zeta}^{\pi'} * j \overset{\zeta}{\Rrightarrow}_S K[e_1] * (h, e_1) \to (h', e_1') \\
(\text{unfold}) \Rrightarrow \quad & heap_S(h, \zeta) * mctx(e, \zeta) * (h_0, e_0) \to^* (h, e) * [\textsc{Sr}]_{\zeta}^{\pi} * \\
& (\pi = 1 \vee (\pi < 1 * disj_H(h_0, h))) * [\textsc{Sr}]_{\zeta}^{\pi'} * j \overset{\zeta}{\Rrightarrow}_S K[e_1] * (h, e_1) \to (h', e_1') \\
\Rrightarrow \quad & heap_S(h, \zeta) * mctx(e, \zeta) * (h_0, e_0) \to^* (h, e) * [\textsc{Sr}]_{\zeta}^{\pi+\pi'} * disj_H(h_0, h) * \\
& j \overset{\zeta}{\Rrightarrow}_S K[e_1] * (h, e_1) \to (h', e_1') \\
(\textit{Lemma } \mathbf{??}) \Rrightarrow \quad & \exists k.\ heap_S(h, \zeta) * mctx(e, \zeta) * (h_0, e_0) \to^* (h, e) * [\textsc{Sr}]_{\zeta}^{\pi+\pi'} * disj_H(h_0, h) * \\
& j \overset{\zeta}{\Rrightarrow}_S K[k] * (h, e_1) \to (h', e_1') * k \overset{\zeta}{\Rrightarrow}_S e_1 \\
(\textit{Lemma } \mathbf{??}) \Rrightarrow \quad & \exists k, e'.\ heap_S(h, \zeta) * mctx(e', \zeta) * (h_0, e_0) \to^* (h', e') * [\textsc{Sr}]_{\zeta}^{\pi+\pi'} * disj_H(h_0, h) * \\
& j \overset{\zeta}{\Rrightarrow}_S K[k] * (h, e_1) \to (h', e_1') * k \overset{\zeta}{\Rrightarrow}_S e_1' \\
(\textit{ass}) \Rrightarrow \quad & \exists k, e'.\ heap_S(h', \zeta) * mctx(e', \zeta) * (h_0, e_0) \to^* (h', e') * [\textsc{Sr}]_{\zeta}^{\pi+\pi'} * disj_H(h_0, h') * \\
& j \overset{\zeta}{\Rrightarrow}_S K[k] * (h, e_1) \to (h', e_1') * k \overset{\zeta}{\Rrightarrow}_S e_1' \\
(\textit{Lemma } \mathbf{??}) \Rrightarrow \quad & \exists k, e'.\ heap_S(h', \zeta) * mctx(e', \zeta) * (h_0, e_0) \to^* (h', e') * [\textsc{Sr}]_{\zeta}^{\pi+\pi'} * disj_H(h_0, h') * \\
& j \overset{\zeta}{\Rrightarrow}_S K[e_1'] * (h, e_1) \to (h', e_1') \\
(\text{fold}) \Rrightarrow \quad & \exists e'.\ \textsc{Spec}(h_0, h', e_0, e', \pi, \zeta) * [\textsc{Sr}]_{\zeta}^{\pi'} * j \overset{\zeta}{\Rrightarrow}_S K[e_1']
\end{aligned}
$$

□

Lemma 38 (Spec pure reduction step)**.**

$$
\begin{aligned}
& \forall e_1, e_1', h, K, \pi.\ (h, e_1) \to (h, e_1') \Rightarrow \\
& \quad \forall \zeta, j.\ (\boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)} * j \overset{\zeta}{\Rrightarrow}_S K[e_1] * [\textsc{Sr}]_{\zeta}^{\pi} \Rrightarrow_{\textsc{Sp}(\zeta)} \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)} * j \overset{\zeta}{\Rrightarrow}_S K[e_1'] * [\textsc{Sr}]_{\zeta}^{\pi})
\end{aligned}
$$

Proof.

$$
\begin{aligned}
& \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)} * j \overset{\zeta}{\Rrightarrow}_S K[e_1] * [\textsc{Sr}]_{\zeta}^{\pi} \\
(\textsc{VSInv})\ {}^{\textsc{Sp}(\zeta)}\!\Rrightarrow^{\emptyset} \quad & \triangleright \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S K[e_1] * [\textsc{Sr}]_{\zeta}^{\pi} \\
(\textit{Lemma } \mathbf{??}) \Rrightarrow \quad & \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S K[e_1] * [\textsc{Sr}]_{\zeta}^{\pi} \\
(\text{unfold}) \Rightarrow \quad & \exists h, e.\ heap_S(h, \zeta) * mctx(e, \zeta) * (h_0, e_0) \to^* (h, e) * ([\textsc{Sr}]_{\zeta}^{1} \vee ([\textsc{Sr}]_{\zeta}^{\frac{1}{2}} * \\
& disj_H(h_0, h))) * j \overset{\zeta}{\Rrightarrow}_S K[e_1] * [\textsc{Sr}]_{\zeta}^{\pi} \\
(\textit{Lemma } \mathbf{??}) \Rightarrow \quad & \exists h, e'.\ heap_S(h, \zeta) * mctx(e', \zeta) * (h_0, e_0) \to^* (h, e') * ([\textsc{Sr}]_{\zeta}^{1} \vee ([\textsc{Sr}]_{\zeta}^{\frac{1}{2}} * \\
& disj_H(h_0, h))) * j \overset{\zeta}{\Rrightarrow}_S K[e_1'] * [\textsc{Sr}]_{\zeta}^{\pi} \\
(\text{fold}) \Rightarrow \quad & \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S K[e_1'] * [\textsc{Sr}]_{\zeta}^{\pi} \\
(\textsc{VSClose}) \quad & \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)} * j \overset{\zeta}{\Rrightarrow}_S K[e_1'] * [\textsc{Sr}]_{\zeta}^{\pi}
\end{aligned}
$$

□

Function abstraction

Lemma 39. *If*

$$[\![\tau_1 \to^{\Pi,\Lambda}_{\varepsilon} \tau_2]\!]^M(f_I, f_S) \vdash \mathcal{E}^{\Pi;\Lambda}_{\varepsilon,M}(\tau_2)(e_I, e_S) \quad (H1)$$

then

$$[\![\tau_1 \to^{\Pi,\Lambda}_{\varepsilon} \tau_2]\!]^M(\textbf{\textit{rec}}\ f(x).e_I, \textbf{\textit{rec}}\ f(x).e_S)$$

Proof. Löb-induction, thus we have to show:

$$\square \forall y_I, y_S.\ (\triangleright(y_I, y_S) \in [\![\tau_1]\!]^M) \Rightarrow \mathcal{E}^{\Pi;\Lambda}_{\varepsilon,M}([\![\tau_2]\!]^M)(\textbf{rec}\ f(x).e_I\ y_I, \textbf{rec}\ f(x).e_S\ y_S)$$

under the assumption $\triangleright([\![\tau_1 \to^{\Pi,\Lambda}_{\varepsilon} \tau_2]\!]^M(\textbf{rec}\ f(x).e_I, \textbf{rec}\ f(x).e_S))$:

Context: $h_0, e_0, j, \zeta, \pi, g, \triangleright([\![\tau_1]\!]^M(y_I, y_S)), \triangleright([\![\tau_1 \to^{\Pi,\Lambda}_{\varepsilon} \tau_2]\!]^M(f_I, f_S)), \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}$

$$\left\{j \overset{\zeta}{\Rightarrow}_S \textbf{rec}\ f(x).e_S\ y_S * [\textsc{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M, \zeta) * P_{reg}(\Pi, g, \varepsilon, M, \zeta)\right\}_{\{\textsc{Hp},\textsc{Sp}(\zeta)\}}$$

$$\textbf{rec}\ f(x).e_I\ y_I$$

$$\left\{v_I.\ \exists v_S.\ [\![\tau_2]\!]^M(v_I, v_S) * j \overset{\zeta}{\Rightarrow}_S v_S * [\textsc{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M, \zeta) * P_{reg}(\Pi, g, \varepsilon, M, \zeta)\right\}_{\{\textsc{Hp},\textsc{Sp}(\zeta)\}}$$

We can take a step, thereby remove the $\triangleright$ from the context

Context: $h_0, e_0, j, \zeta, \pi, g, [\![\tau_1]\!]^M(y_I, y_S), [\![\tau_1 \to^{\Pi,\Lambda}_{\varepsilon} \tau_2]\!]^M(f_I, f_S), \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}$

$$\left\{j \overset{\zeta}{\Rightarrow}_S e_S[y_S/x, f_S/f] * [\textsc{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M, \zeta) * P_{reg}(\Pi, g, \varepsilon, M, \zeta)\right\}_{\{\textsc{Hp},\textsc{Sp}(\zeta)\}}$$

$$e_I[y_I/x, f_I/f]$$

$$\left\{v_I.\ \exists v_S.\ [\![\tau_2]\!]^M(v_I, v_S) * j \overset{\zeta}{\Rightarrow}_S v_S * [\textsc{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M, \zeta) * P_{reg}(\Pi, g, \varepsilon, M, \zeta)\right\}_{\{\textsc{Hp},\textsc{Sp}(\zeta)\}}$$

Now we can apply $H1$ with y_I and y_S.

□

Function application

Lemma 40.

$$\begin{aligned}
&\forall v_1, v_2, j, \pi, \Lambda, \Pi, \varepsilon, h_0, e_0, \zeta, M.\\
&\quad \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}, [\![\tau_1 \to^{\Pi,\Lambda}_{\varepsilon} \tau_2]\!]^M(v_{1I}, v_{1S}), [\![\tau_1]\!]^M(v_{2I}, v_{2S}) \ \vdash\\
&\quad \left\{j \overset{\zeta}{\Rightarrow}_S v_{1S}\ v_{2S} * [\textsc{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda, \boldsymbol{1}, \varepsilon, M, \zeta) * P_{reg}(\Pi, g, \varepsilon, M, \zeta)\right\}\\
&\qquad v_{1I}\ v_{2I}\\
&\quad \left\{v_I.\ \exists v_S.\ j \overset{\zeta}{\Rightarrow}_S v_S * [\![\tau_2]\!]^M(v_I, v_S) * [\textsc{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda, \boldsymbol{1}, \varepsilon, M, \zeta) * P_{reg}(\Pi, g, \varepsilon, M, \zeta)\right\}_{\{\textsc{Hp},\textsc{Sp}(\zeta)\}}
\end{aligned}$$

Proof. Unfolding $[\![\tau_1 \to^{\Pi,\Lambda}_{\varepsilon} \tau_2]\!]^M(v_{1I}, v_{1S})$ and apply that the computations are related, thus we have to show $[\![\tau_1]\!]^M(v_{2I}, v_{2S})$, which we have from our assumption. □

Par

$$\mathsf{regs}(\varepsilon) \triangleq \{r \mid r \in \mathsf{rds}\ \varepsilon \cup \mathsf{wrs}\ \varepsilon \cup \mathsf{als}\ \varepsilon\}$$

Lemma 41 (Splitting region)**.**

$$\begin{array}{ll} & \forall R_1, R_2, g, \varepsilon_1, \varepsilon_2, M, \zeta. \\ & \quad P_{reg}(R_1 \uplus R_2, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * \textsf{\textit{regs}}(\varepsilon_1) \subseteq R_1 * \textsf{\textit{regs}}(\varepsilon_2) \subseteq R_2 \\ \Rrightarrow & \quad P_{reg}(R_1, g, \varepsilon_1, M, \zeta) * P_{reg}(R_2, g, \varepsilon_2, M, \zeta) \end{array}$$

Lemma 42 (Assembling regions)**.**

$$\begin{array}{ll} & \forall R_1, R_2, g, \varepsilon_1, \varepsilon_2, M, \zeta. \\ & \quad P_{reg}(R_1, g, \varepsilon_1, M, \zeta) * P_{reg}(R_2, g, \varepsilon_2, M, \zeta) \\ \Rrightarrow & \quad P_{reg}(R_1 \uplus R_2, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{array}$$

Lemma 43 (Changing region)**.**

$$\begin{array}{ll} & \forall R, g, \varepsilon_1, \varepsilon_2, M, \zeta. \\ & \quad P_{reg}(R, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \\ \Longleftrightarrow & \quad P_{reg}(R, \frac{g}{2}, \varepsilon_1, M, \zeta) * P_{reg}(R, \frac{g}{2}, \varepsilon_2, M, \zeta) * P_{reg}(R, \frac{g}{2}, \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2, M, \zeta) \end{array}$$

where

$$\frac{g}{2}(\rho) \triangleq \begin{cases} \frac{g(\rho)}{2} & \rho \in dom(g) \\ \bot & otherwise \end{cases}$$

Lemma 44 (New expressions in evaluation contexts)**.**

$$\forall j, e_1, e_2.\ j \overset{\zeta}{\Rrightarrow}_S e_1 \,||\, e_2 \Rrightarrow \exists k_1, k_2.\ j \overset{\zeta}{\Rrightarrow}_S k_1 \,||\, k_2 * k_1 \overset{\zeta}{\Rrightarrow}_S e_1 * k_2 \overset{\zeta}{\Rrightarrow}_S e_2$$

Proof. Follows from Lemma **??**. ☐

Lemma 45 (Substituting expressions in evaluation contexts)**.**

$$\forall j, k_1, j_2, v_1, v_2.\ j \overset{\zeta}{\Rrightarrow}_S k_1 \,||\, k_2 * k_1 \overset{\zeta}{\Rrightarrow}_S v_1 * k_2 \overset{\zeta}{\Rrightarrow}_S v_2 \Rrightarrow j \overset{\zeta}{\Rrightarrow}_S v_1 \,||\, v_2$$

Proof. Follows from Lemma **??**. ☐

Lemma 46 (Par)**.**

$$\begin{array}{l} \forall j, h_0, e_0, e_1, e_2, \zeta, \pi, \Lambda_1, \Lambda_2, \Lambda_3, \Pi, \varepsilon_1, \varepsilon_2, M, g, \tau_1, \tau_2. \\ \quad \textsf{\textit{regs}}(\varepsilon_1) \subseteq \Lambda_1 \cup \Lambda_3 \cup \Pi \wedge \textsf{\textit{regs}}(\varepsilon_2) \subseteq \Lambda_2 \cup \Lambda_3 \cup \Pi \Rightarrow \\ \quad (\mathcal{E}^{(\Pi,\Lambda_3);\Lambda_1}_{\varepsilon_1,M}(\llbracket \tau_1 \rrbracket^M)(e_{1I}, e_{1S}), \mathcal{E}^{(\Pi,\Lambda_3);\Lambda_2}_{\varepsilon_2,M}(\llbracket \tau_2 \rrbracket^M)(e_{2I}, e_{2S}), \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)} \vdash \\ \qquad \mathcal{E}^{\Pi,(\Lambda_1,\Lambda_2,\Lambda_3)}_{\varepsilon_1 \cup \varepsilon_2, M}(\llbracket \tau_1 \times \tau_2 \rrbracket^M)(e_{1I} \,||\, e_{2I}, e_{1S} \,||\, e_{2S})) \end{array}$$

Proof.

Context: $j, h_0, e_0, e_1, e_2, \zeta, \pi, \Lambda_1, \Lambda_2, \Lambda_3, \Pi, \varepsilon_1, \varepsilon_2, M, g, \tau_1, \tau_2$
Context: $\mathcal{E}^{(\Pi,\Lambda_3);\Lambda_1}_{\varepsilon_1,M}(\llbracket\tau_1\rrbracket^M)(e_{1I}, e_{1S}), \mathcal{E}^{(\Pi,\Lambda_3);\Lambda_2}_{\varepsilon_2,M}(\llbracket\tau_2\rrbracket^M)(e_{2I}, e_{2S}), \boxed{\text{Heap}}^{\text{Hp}}, \boxed{\text{Spec}(h_0, e_0, \zeta)}^{\text{Sp}(\zeta)}$

$$\left\{ j \overset{\zeta}{\Rrightarrow}_S e_{1S} \,||\, e_{2S} * [\text{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda_1 \uplus \Lambda_2 \uplus \Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * P_{reg}(\Pi, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

`// Lemma ??`

$$\left\{ \begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S e_{1S} \,||\, e_{2S} * [\text{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * \\ P_{reg}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * P_{reg}(\Pi, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

`// Lemma ??`

$$\left\{ \begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S e_{1S} \,||\, e_{2S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * \\ P_{reg}(\Lambda_3, \frac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_3, \frac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3, \frac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2, M, \zeta) * \\ P_{reg}(\Pi, \frac{g}{2}, \varepsilon_1, M, \zeta) * P_{reg}(\Pi, \frac{g}{2}, \varepsilon_2, M, \zeta) * P_{reg}(\Pi, \frac{g}{2}, \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

`// Let` $g'(r) \triangleq \begin{cases} \frac{g}{2} & r \in \Pi \\ \frac{1}{2} & r \in \Lambda_3 \\ \bot & \texttt{otherwise} \end{cases}$

$$\left\{ \begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S e_{1S} \,||\, e_{2S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * \\ P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

`// Lemma ??`

$$\left\{ \begin{array}{l} \exists k_1, k_2.\ j \overset{\zeta}{\Rrightarrow}_S k_1 \,||\, k_2 * k_1 \overset{\zeta}{\Rrightarrow}_S e_{1S} * k_2 \overset{\zeta}{\Rrightarrow}_S e_{2S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * \\ P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_2, M, \zeta) * \\ P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

Frame

$$\left\{ \begin{array}{l} \exists k_1, k_2.\ k_1 \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1, M, \zeta) * \\ k_2 \overset{\zeta}{\Rrightarrow}_S e_{2S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

$e_{1I} \,||\, e_{2I}$

$$\left\{ \exists k_1.\ k_1 \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1, M, \zeta) \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

e_{1I}

$$\left\{ \begin{array}{l} v_{1I}.\ \exists k_1, v_{1S}.\ k_1 \overset{\zeta}{\Rrightarrow}_S v_{1S} * \llbracket\tau_1\rrbracket^M(v_{1I}, v_{1S}) * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * \\ P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

$$\left\{ \exists k_2.\ k_2 \overset{\zeta}{\Rrightarrow}_S e_{2S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_2, M, \zeta) \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

e_{2I}

$$\left\{ \begin{array}{l} v_{2I}.\ \exists k_2, v_{2S}.\ k_2 \overset{\zeta}{\Rrightarrow}_S v_{2S} * \llbracket\tau_2\rrbracket^M(v_{2I}, v_{2S}) * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * \\ P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

$$\left\{ \begin{array}{l} v_I.\ \exists k_1, k_2, v_{1S}, v_{2S}.\ v_I = (v_{1I}, v_{2I}) * \llbracket\tau_1\rrbracket^M(v_{1I}, v_{1S}) * \llbracket\tau_2\rrbracket^M(v_{2I}, v_{2S}) * \\ k_1 \overset{\zeta}{\Rrightarrow}_S v_{1S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1, M, \zeta) * \\ k_2 \overset{\zeta}{\Rrightarrow}_S v_{2S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

$$\left\{ \begin{array}{l} v_I.\ \exists k_1, k_2, v_{1S}, v_{2S}.\ v_I = (v_{1I}, v_{2I}) * \llbracket\tau_1\rrbracket^M(v_{1I}, v_{1S}) * \llbracket\tau_2\rrbracket^M(v_{2I}, v_{2S}) * \\ j \overset{\zeta}{\Rrightarrow}_S v_{1S} \,||\, v_{2S} * k_1 \overset{\zeta}{\Rrightarrow}_S v_{1S} * k_2 \overset{\zeta}{\Rrightarrow}_S v_{2S} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * [\text{Sr}]^{\frac{\pi}{2}}_{\zeta} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * \\ P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_2, M, \zeta) * \\ P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{Hp},\text{Sp}(\zeta)\}}$$

// Lemma ??

$$\begin{Bmatrix} v_I.\ \exists v_{1S}, v_{2S}.\ v_I = (v_{1I}, v_{2I}) * [\![\tau_1]\!]^M(v_{1I}, v_{1S}) * [\![\tau_2]\!]^M(v_{2I}, v_{2S}) * \\ j \overset{\zeta}{\Rightarrow}_S v_{1S} \,||\, v_{2S} * [\mathrm{SR}]_\zeta^{\frac{\pi}{2}} * [\mathrm{SR}]_\zeta^{\frac{\pi}{2}} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * \\ P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_2, M, \zeta) * \\ P_{reg}(\Lambda_3 \uplus \Pi, g', \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2, M, \zeta) \end{Bmatrix}_{\{\mathrm{HP}, \mathrm{SP}(\zeta)\}}$$

// Lemma ??

$$\begin{Bmatrix} v_I.\ \exists v_{1S}, v_{2S}.\ v_I = (v_{1I}, v_{2I}) * [\![\tau_1]\!]^M(v_{1I}, v_{1S}) * [\![\tau_2]\!]^M(v_{2I}, v_{2S}) * \\ j \overset{\zeta}{\Rightarrow}_S v_{1S} \,||\, v_{2S} * [\mathrm{SR}]_\zeta^{\frac{\pi}{2}} * [\mathrm{SR}]_\zeta^{\frac{\pi}{2}} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * \\ P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * P_{reg}(\Pi, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{Bmatrix}_{\{\mathrm{HP}, \mathrm{SP}(\zeta)\}}$$

// From $\mathsf{regs}(\varepsilon_1) \notin \Lambda_2$ and $\mathsf{regs}(\varepsilon_2) \notin \Lambda_1$

$$\begin{Bmatrix} v_I.\ \exists v_{1S}, v_{2S}.\ v_I = (v_{1I}, v_{2I}) * [\![\tau_1]\!]^M(v_{1I}, v_{1S}) * [\![\tau_2]\!]^M(v_{2I}, v_{2S}) * \\ j \overset{\zeta}{\Rightarrow}_S v_{1S} \,||\, v_{2S} * [\mathrm{SR}]_\zeta^{\pi} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * \\ P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2 \cup \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * P_{reg}(\Pi, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{Bmatrix}_{\{\mathrm{HP}, \mathrm{SP}(\zeta)\}}$$

$$\begin{Bmatrix} v_I.\ \exists v_{1S}, v_{2S}.\ v_I = (v_{1I}, v_{2I}) * [\![\tau_1]\!]^M(v_{1I}, v_{1S}) * [\![\tau_2]\!]^M(v_{2I}, v_{2S}) * \\ j \overset{\zeta}{\Rightarrow}_S v_{1S} \,||\, v_{2S} * [\mathrm{SR}]_\zeta^{\pi} * P_{reg}(\Lambda_1 \uplus \Lambda_2 \uplus \Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * \\ P_{reg}(\Pi, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{Bmatrix}_{\{\mathrm{HP}, \mathrm{SP}(\zeta)\}}$$

// Pure step

$$\begin{Bmatrix} v_I.\ \exists v_{1S}, v_{2S}.\ v_I = (v_{1I}, v_{2I}) * [\![\tau_1]\!]^M(v_{1I}, v_{1S}) * [\![\tau_2]\!]^M(v_{2I}, v_{2S}) * \\ j \overset{\zeta}{\Rightarrow}_S (v_{1S}, v_{2S}) * [\mathrm{SR}]_\zeta^{\pi} * P_{reg}(\Lambda_1 \uplus \Lambda_2 \uplus \Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * \\ P_{reg}(\Pi, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{Bmatrix}_{\{\mathrm{HP}, \mathrm{SP}(\zeta)\}}$$

$$\begin{Bmatrix} v_I.\ \exists v_S.\ j \overset{\zeta}{\Rightarrow}_S v_S * [\![\tau_1 \times \tau_2]\!]^M(v_I, v_S) * [\mathrm{SR}]_\zeta^{\pi} * P_{reg}(\Lambda_1 \uplus \Lambda_2 \uplus \Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * \\ P_{reg}(\Pi, g, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{Bmatrix}_{\{\mathrm{HP}, \mathrm{SP}(\zeta)\}}$$

□

Read

Lemma 47 (Trade read tokens)**.**

$$\forall r, \iota, \pi.\ \boxed{\mathrm{REG}(r)}^{\iota} \vdash [\mathrm{RD}]_r^{\pi} \ {}^{\{\iota\}}\!\!\Longleftrightarrow^{\emptyset} \exists h.\ locs(h, r) * toks(\pi, 1, r) * \circledast_{x \in Loc^2} [\mathrm{RD}(x)]_r$$
$$\forall r, \iota.\ \boxed{\mathrm{REG}(r)}^{\iota} \vdash [\mathrm{RD}]_r^{1} \ {}^{\{\iota\}}\!\!\Longleftrightarrow^{\{\iota\}} \circledast_{x \in Loc^2} [\mathrm{RD}(x)]_r$$

Lemma 48 (Read effect ensures well-typedness)**.**

$$\begin{aligned} \forall r, \phi, x, v. \quad & effs(r, \phi, x, v) * [\mathrm{RD}(x)]_r \\ \Rightarrow \quad & effs(r, \phi, x, v) * [\mathrm{RD}(x)]_r * v \in \phi \end{aligned}$$

Lemma 49.

$$\forall h, r, x, y, \pi.\, locs(h, r) * x \overset{\pi}{\hookrightarrow}_{I,r} y \Rightarrow locs(h, r) * x \overset{\pi}{\hookrightarrow}_{I,r} y * h_I(x) = y$$

Lemma 50.

$$\forall h, r, x, y, \pi.\, locs(h, r) * x \overset{\pi}{\hookrightarrow}_{S,r} y \Rightarrow locs(h, r) * x \overset{\pi}{\hookrightarrow}_{S,r} y * h_S(x) = y$$

Lemma 51.

$$\begin{aligned} & \forall h, r, \zeta, \pi. \\ & \quad locs(h, r) * [\mathrm{MU}(r, \{\zeta\})]^{\pi} \\ \Rightarrow \quad & locs(h, r, \{\zeta\}, \{\zeta\}) * [\mathrm{MU}(r, \{\zeta\})]^{\pi} \end{aligned}$$

Lemma 52.

$$\begin{array}{ll} & \forall h, h_R, r, \zeta s, \pi. \\ & \quad \mathit{locs}(h, r) * [\textsc{Im}(r, \zeta s, h_R)]^{\pi} \\ \Rightarrow & \quad \mathit{locs}(h, r, \zeta s, \zeta s) * [\textsc{Im}(r, \zeta s, h_R)]^{\pi} * h_S = h_R \end{array}$$

Lemma 53.

$$\begin{array}{ll} & \forall h, r, y, \zeta, \zeta s, \zeta s', \pi. \\ & \quad \mathit{locs}(h, r, \zeta s', \{\zeta\} \uplus \zeta s) \\ \Leftrightarrow & \quad \mathit{locs}(h, r, \zeta s', \zeta s) * \circledast_{(l,v) \in h_S} l \mapsto_S^{\zeta} v \end{array}$$

Lemma 54 (Implementation dereference)**.**

$$\begin{array}{l} \forall r, x, v, h, \pi. \\ \quad \left\{\textsc{Heap} * x \xhookrightarrow{\pi}_{I,r} v * \mathit{locs}(h, r)\right\} \\ \quad\quad !x \\ \quad \left\{v'.\ \textsc{Heap} * x \xhookrightarrow{\pi}_{I,r} v * \mathit{locs}(h, r) * v' = v\right\} \end{array}$$

Proof. By Lemma **??** and definition of *locs*. □

Lemma 55 (Specification dereference)**.**

$$\begin{array}{ll} & \forall h_0, h_S, e_0, e, \pi, \pi', \zeta, x, v, j. \\ & \quad \textsc{Spec}(h_0, h_S, e_0, e, \pi, \zeta) * x \mapsto_S^{\zeta} v * j \overset{\zeta}{\Rrightarrow}_S !x * [\textsc{Sr}]_{\zeta}^{\pi'} \\ \Rrightarrow & \quad \textsc{Spec}(h_0, h_S, e_0, e, \pi, \zeta) * x \mapsto_S^{\zeta} v * j \overset{\zeta}{\Rrightarrow}_S v * [\textsc{Sr}]_{\zeta}^{\pi'} \end{array}$$

Proof. $x \mapsto_S^{\zeta} v$ asserts $h_S[x \mapsto v]$. From our operational semantics we have $(h_S[x \mapsto v], !x) \to (h_S[x \mapsto v], v)$ and since we do not change the heap the update of ghost-state follows from Lemma **??**. □

Lemma 56 (Specification dereference for region)**.**

$$\begin{array}{ll} & \forall j, x, v, r, h, h_R, \zeta, \zeta s, \pi, \pi', \pi''. \\ & \quad \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S !x * [\textsc{Sr}]_{\zeta}^{\pi''} * x \xhookrightarrow{\frac{1}{2}}_{S,r} v * \mathit{locs}(h, r) * \mathit{slink}(r, \zeta s, h_R, \pi, \pi') * \zeta \in \zeta s \\ \Rrightarrow & \quad \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S v * [\textsc{Sr}]_{\zeta}^{\pi''} * x \xhookrightarrow{\frac{1}{2}}_{S,r} v * \mathit{locs}(h, r) * \mathit{slink}(r, \zeta s, h_R, \pi, \pi') \end{array}$$

Proof. By Lemma **??**, Lemma **??** and Lemma **??**. □

Lemma 57.

$$\begin{array}{l} \forall r, \phi, x, \zeta, \zeta s, j, h, \pi, \pi', \pi''. \\ \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}, \boxed{\textsc{Ref}(r, \phi, x)}^{\textsc{Rf}(x)} \ \vdash \\ \left\{j \overset{\zeta}{\Rrightarrow}_S !x_S * [\textsc{Sr}]_{\zeta}^{\pi''} * \mathit{locs}(h, r) * [\textsc{Rd}(x)]_r * \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h_S, \pi, \pi')\right\} \\ \quad !x_I \\ \left\{\begin{array}{l} v_I.\ \exists v_S.\ j \overset{\zeta}{\Rrightarrow}_S v_S * [\textsc{Sr}]_{\zeta}^{\pi''} * \mathit{locs}(h, r) * [\textsc{Rd}(x)]_r \ * \\ \quad \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h_S, \pi, \pi') * (v_I, v_S) \in \phi \end{array}\right\}_{\{\textsc{Hp}, \textsc{Sp}(\zeta), \textsc{Rf}(x)\}} \end{array}$$

Proof.

Context: $r, \phi, x, \zeta, \zeta s, j, h, \pi, \pi', \pi''$, $\boxed{\text{HEAP}}^{\text{HP}}$, $\boxed{\text{SPEC}(h_0, e_0, \zeta)}^{\text{SP}(\zeta)}$, $\boxed{\text{REF}(r, \phi, x)}^{\text{RF}(x)}$

$$\left\{ j \overset{\zeta}{\Rrightarrow}_S \, !x_S * [\text{SR}]_\zeta^{\pi''} * \mathit{locs}(h, r) * [\text{RD}(x)]_r * \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h_S, \pi, \pi') \right\}_{\{\text{HP},\text{SP}(\zeta),\text{RF}(x)\}}$$

Open HP, SP(ζ), RF(x)

```
// ▷ moved by Lemma ??
```

$$\left\{ \begin{array}{l} \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \, !x_S * [\text{SR}]_\zeta^{\pi''} * \exists v.\ \mathit{ref}(r, \triangleright\phi, x, v) * \mathit{locs}(h, r) * [\text{RD}(x)]_r \, * \\ \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h_S, \pi, \pi') \end{array} \right\}_\emptyset$$

$!x_I$

```
// Unfold ref and apply Lemma ??
```

$$\left\{ \begin{array}{l} v_I^2.\ \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \, !x_S * [\text{SR}]_\zeta^{\pi''} * \exists v.\ \mathit{ref}(r, \phi, x, v) * \mathit{locs}(h, r) \, * \\ [\text{RD}(x)]_r * v_I = v_I^2 * \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h_S, \pi, \pi') \end{array} \right\}_\emptyset$$

```
// Lemma ??
```

$$\left\{ \begin{array}{l} v_I^2.\ \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * \exists v.\ j \overset{\zeta}{\Rrightarrow}_S v_S * [\text{SR}]_\zeta^{\pi''} * \mathit{ref}(r, \phi, x, v) * \mathit{locs}(h, r) \, * \\ [\text{RD}(x)]_r * v_I = v_I^2 * \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h_S, \pi, \pi') \end{array} \right\}_\emptyset$$

```
// Lemma ??
```

$$\left\{ \begin{array}{l} v_I^2.\ \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * \exists v.\ j \overset{\zeta}{\Rrightarrow}_S v_S * [\text{SR}]_\zeta^{\pi''} * \mathit{ref}(r, \phi, x, v) * (v_I^2, v_S) \in \phi \, * \\ \mathit{locs}(h, r) * [\text{RD}(x)]_r * \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h_S, \pi, \pi') \end{array} \right\}_\emptyset$$

$$\left\{ \begin{array}{l} v_I^2.\ \exists v_S.\ j \overset{\zeta}{\Rrightarrow}_S v_S * [\text{SR}]_\zeta^{\pi''} * \mathit{locs}(h, r) * [\text{RD}(x)]_r \, * \\ \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h_S, \pi, \pi') * (v_I^2, v_S) \in \phi \end{array} \right\}_{\{\text{HP},\text{SP}(\zeta),\text{RF}(x)\}}$$

□

Lemma 58.

$$\forall r, \zeta, \pi, \pi', h.\ [\text{MU}(r, \{\zeta\})]^\pi \Leftrightarrow \mathit{slink}(r, \{\zeta\}, h, \pi, \pi')$$

Lemma 59 (Read)**.**

$\forall r, \phi, x, \pi, \pi', \pi'', \pi''', j, \zeta, \zeta s, h.$

$\boxed{\text{HEAP}}^{\text{HP}}, \boxed{\text{SPEC}(h_0, e_0, \zeta)}^{\text{SP}(\zeta)}, \boxed{\text{REG}(r)}^{\text{RG}(r)}, \boxed{\text{REF}(r, \phi, x)}^{\text{RF}(x)} \vdash$

$\left\{ j \overset{\zeta}{\Rrightarrow}_S \, !x_S * [\text{SR}]_\zeta^{\pi'''} * [\text{RD}]_r^\pi * \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h, \pi', \pi'') \right\}$

$!x_I$

$\left\{ v_I.\ \exists v_S.\ j \overset{\zeta}{\Rrightarrow}_S v_S * [\text{SR}]_\zeta^{\pi'''} * [\text{RD}]_r^\pi * \mathit{slink}(r, \{\zeta\} \uplus \zeta s, h, \pi', \pi'') * (v_I, v_S) \in \phi \right\}_{\{\text{HP},\text{SP}(\zeta),\text{RG}(r),\text{RF}(x)\}}$

Proof. By Lemma **??** and Lemma **??**. □

Write

Lemma 60 (Trade write tokens)**.**

$$\forall r, \iota, \pi.\ \boxed{\text{REG}(r)}^\iota \vdash [\text{WR}]_r^\pi \ {}^{\{\iota\}}\!\!\Longleftrightarrow^{\emptyset} \exists h.\ \mathit{locs}(h, r) * \mathit{toks}(1, \pi, r) * \circledast_{x \in Loc^2} [\text{WR}(x)]_r$$

$$\forall r, \iota.\ \boxed{\text{REG}(r)}^\iota \vdash [\text{WR}]_r^1 \ {}^{\{\iota\}}\!\!\Longleftrightarrow^{\{\iota\}} \circledast_{x \in Loc^2} [\text{WR}(x)]_r$$

Lemma 61 (Assign in concrete code)**.**

$\forall x, v.$

$\{\text{HEAP} * x \mapsto -\}$

$x := v$

$\{v'.\ v' = () * \text{HEAP} * x \mapsto v\}$

Lemma 62 (Assign in specification code)**.**

$$\begin{array}{ll} & \forall h_0, e_0, \pi, \pi', \zeta, j, e, x, v. \\ & \quad \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S x := v * [\textsc{Sr}]_\zeta^{\pi'} * x \mapsto_S^\zeta - \\ \Rrightarrow & \quad \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S () * [\textsc{Sr}]_\zeta^{\pi'} * x \mapsto_S^\zeta v \end{array}$$

Proof. $x \mapsto_S^\zeta -$ asserts $h_S[x \mapsto -]$. From the operational semantics we have $(h_S[x \mapsto -], x := v) \to (h_S[x \mapsto v], ())$ and since we do not change the domain of the heap, the update of ghost-state follows from Lemma **??**. $\square$

Lemma 63 (Exclusive ownership of region-references)**.**

$$\begin{array}{ll} & \forall r, \phi, x, v. \\ & \quad \mathit{ref}(r, \phi, x, v) * [\textsc{Wr}(x)]_r \\ \Longleftrightarrow & \quad [\textsc{Wr}(x)]_r * x_I \overset{1}{\hookrightarrow}_{I,r} v_I * x_S \overset{1}{\hookrightarrow}_{S,r} v_S * ([\textsc{Rd}(x)]_r \vee (v \in \phi * [\textsc{NoRd}(x)]_r)) \end{array}$$

Lemma 64 (Update related locations with related values)**.**

$$\begin{array}{ll} & \forall r, \phi, x, v. \\ & \quad x_I \overset{1}{\hookrightarrow}_{I,r} v_I' * x_S \overset{1}{\hookrightarrow}_{S,r} v_S' * v \in \phi * ([\textsc{Rd}(x)]_r \vee (v' \in \phi * [\textsc{NoRd}(x)]_r)) \\ \Rrightarrow & \quad \mathit{ref}(r, \phi, x, v) \end{array}$$

Lemma 65 (Assignment)**.**

$$\begin{array}{l} \forall r, \phi, x, v, h, j, \zeta, \pi, \pi'. \\ \quad \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}, \boxed{\textsc{Ref}(r, \phi, x)}^{\textsc{Rf}(x)} \\ \vdash \left\{ j \overset{\zeta}{\Rrightarrow}_S x_S := v_S * [\textsc{Sr}]_\zeta^{\pi'} * \mathit{locs}(h, r) * [\textsc{Wr}(x)]_r * [\textsc{Mu}(r, \{\zeta\})]^\pi * \phi(v) \right\} \\ \qquad x_I := v_I \\ \quad \left\{ v'.\ v' = () * j \overset{\zeta}{\Rrightarrow}_S () * [\textsc{Sr}]_\zeta^{\pi'} * \mathit{locs}(h, r) * [\textsc{Wr}(x)]_r * [\textsc{Mu}(r, \{\zeta\})]^\pi \right\}_{\{\textsc{Hp}, \textsc{Sp}(\zeta), \textsc{Rf}(x)\}} \end{array}$$

Proof.

Context: $r, \phi, x, v, h, j, \zeta, \pi, \pi', \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}, \boxed{\textsc{Ref}(r, \phi, x)}^{\textsc{Rf}(x)}, \phi(v)$

$$\left\{ j \overset{\zeta}{\Rrightarrow}_S x_S := v_S * [\textsc{Sr}]_\zeta^{\pi'} * \mathit{locs}(h, r) * [\textsc{Wr}(x)]_r * [\textsc{Mu}(r, \{\zeta\})]^\pi \right\}_{\{\textsc{Hp},\textsc{Sp}(\zeta),\textsc{Rf}(x)\}}$$

Open $\textsc{Hp}, \textsc{Sp}(\zeta), \textsc{Rf}(x)$

$$\left\{ \begin{array}{l} \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * \textsc{Ref}(r, \phi, x) * j \overset{\zeta}{\Rrightarrow}_S x_S := v_S * [\textsc{Sr}]_\zeta^{\pi'} * \mathit{locs}(h, r) * \\ [\textsc{Wr}(x)]_r * [\textsc{Mu}(r, \{\zeta\})]^\pi \end{array} \right\}_\emptyset$$

// Lemma ??.

$$\left\{ \begin{array}{l} \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S x_S := v_S * [\textsc{Sr}]_\zeta^{\pi'} * \mathit{locs}(h, r) * [\textsc{Wr}(x)]_r * x_I \overset{1}{\hookrightarrow}_{I,r} - * \\ x_S \overset{1}{\hookrightarrow}_{S,r} - * ([\textsc{Rd}(x)]_r \vee ((-, -) \in \phi * [\textsc{NoRd}(x)]_r)) * [\textsc{Mu}(r, \{\zeta\})]^\pi \end{array} \right\}_\emptyset$$

// Lemma ?? and Lemma ?? and unfolding of *locs*

$$\left\{ \begin{array}{l} \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S x_S := v_S * [\textsc{Sr}]_\zeta^{\pi'} * \exists h'_I, h'_S.\ h_I = h'_I \uplus [x_I \mapsto -] * \\ h_S = h'_S \uplus [x_S \mapsto -] * \mathit{slink}(r, \{\zeta\}, h_S, \tfrac{1}{2}, \tfrac{1}{4}) * \mathit{rheap}_I(h_I, r) * \mathit{rheaps}_S(h_S, r) * \mathit{alloc}(h, r) * \\ \circledast_{(l,v) \in h'_I} l \mapsto v * x_I \mapsto - * \circledast_{(l,v) \in h'_S} l \mapsto_S^\zeta v * x_S \mapsto_S^\zeta - * [\textsc{Wr}(x)]_r * x_I \overset{1}{\hookrightarrow}_{I,r} - * \\ x_S \overset{1}{\hookrightarrow}_{S,r} - * ([\textsc{Rd}(x)]_r \vee [\textsc{NoRd}(x)]_r) * [\textsc{Mu}(r, \{\zeta\})]^\pi \end{array} \right\}_\emptyset$$

Frame

$$\left\{ \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S x_S := v_S * [\textsc{Sr}]_\zeta^{\pi'} * x_I \mapsto - * x_S \mapsto_S^\zeta - \right\}_\emptyset$$

$x_I := v_I$

$$\left\{ v_I^1.\ v_I^1 = () * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S x_S := v_S * [\textsc{Sr}]_\zeta^{\pi'} * x_I \mapsto v_I * x_S \mapsto_S^\zeta - \right\}_\emptyset$$

// Lemma ??

$$\left\{ v_I^1.\ v_I^1 = () * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S () * [\textsc{Sr}]_\zeta^{\pi'} * x_I \mapsto v_I * x_S \mapsto_S^\zeta v_S \right\}_\emptyset$$

$$\left\{ \begin{array}{l} v_I^1.\ v_I^1 = () * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S () * [\textsc{Sr}]_\zeta^{\pi'} * \exists h'_I, h'_S.\ h_I = h'_I[x_I \mapsto -] * \\ h_S = h'_S[x_S \mapsto -] * \mathit{slink}(r, \{\zeta\}, h_S, \tfrac{1}{2}, \tfrac{1}{4}) * \mathit{rheap}_I(h_I, r) * \mathit{rheaps}_S(h_S, r) * \mathit{alloc}(h, r) * \\ \circledast_{(l,v) \in h'_I} l \mapsto v * x_I \mapsto v_I * \circledast_{(l,v) \in h'_S} l \mapsto_S^\zeta v * x_S \mapsto_S^\zeta v_S * [\textsc{Wr}(x)]_r * x_I \overset{1}{\hookrightarrow}_{I,r} - * \\ x_S \overset{1}{\hookrightarrow}_{S,r} - * ([\textsc{Rd}(x)]_r \vee [\textsc{NoRd}(x)]_r) * [\textsc{Mu}(r, \{\zeta\})]^\pi \end{array} \right\}_\emptyset$$

// Updated region points-to by having full fraction and having both the full and the fragmental authorative parts by AFHeapUpd.

$$\left\{ \begin{array}{l} v_I^1.\ v_I^1 = () * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S () * [\textsc{Sr}]_\zeta^{\pi'} * \exists h'. \\ h' = (h_I[x_I \mapsto v_I], h_S[x_S \mapsto v_S]) * \mathit{locs}(h', r) * [\textsc{Wr}(x)]_r * x_I \overset{1}{\hookrightarrow}_{I,r} v_I * x_S \overset{1}{\hookrightarrow}_{S,r} v_S * \\ ([\textsc{Rd}(x)]_r \vee (\phi(v_I, v_S) * [\textsc{NoRd}(x)]_r)) * [\textsc{Mu}(r, \{\zeta\})]^\pi \end{array} \right\}_\emptyset$$

// Lemma ?? and folding of Ref predicate.

$$\left\{ \begin{array}{l} v_I^1.\ \exists h', v_S^1.\ v_I^1 = () * v_S^1 = () * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S v_S^1 * [\textsc{Sr}]_\zeta^{\pi'} * \\ \mathit{locs}(h', r) * [\textsc{Wr}(x)]_r * \textsc{Ref}(r, \phi, x) * [\textsc{Mu}(r, \{\zeta\})]^\pi \end{array} \right\}_\emptyset$$

$$\left\{ v_I^1.\ \exists h', v_S^1.\ j \overset{\zeta}{\Rrightarrow}_S v_S^1 * [\textsc{Sr}]_\zeta^{\pi'} * \mathit{locs}(h', r) * [\textsc{Wr}(x)]_r * [\textsc{Mu}(r, \{\zeta\})]^\pi * [\![\mathbf{1}]\!]^M(v_I^1, v_S^1) \right\}_{\{\textsc{Hp},\textsc{Sp}(\zeta),\textsc{Rf}(x)\}}$$

□

Lemma 66 (Write)**.**

$$\begin{array}{ll} & \forall r, \phi, x, \zeta, j, \pi, \pi', v. \\ & \quad \boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}, \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)}, \boxed{\textsc{Ref}(r, \phi, x)}^{\textsc{Rf}(x)} \\ \vdash & \quad \left\{ j \overset{\zeta}{\Rrightarrow}_S x_S := v_S * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Mu}(r, \{\zeta\})]^\pi * [\textsc{Wr}]_r^\pi * \phi(v) \right\} \\ & \quad\quad x_I := v_I \\ & \quad \left\{ ().\ j \overset{\zeta}{\Rrightarrow}_S () * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Mu}(r, \{\zeta\})]^\pi * [\textsc{Wr}]_r^\pi * [\![\mathbf{1}]\!]^M((), ()) \right\}_{\{\textsc{Hp},\textsc{Sp}(\zeta),\textsc{Rg}(r),\textsc{Rf}(x)\}} \end{array}$$

Proof. By Lemma **??** and Lemma **??**. □

Allocate

Lemma 67 (New location in disjoint domain)**.**

$$\begin{array}{rl} & \forall v, h_0, h, \zeta. \\ & \quad \mathit{heaps}_S(h,\zeta) * \mathit{disj}_H(h_0,h) \\ \Rrightarrow & \quad \exists h', x.\ h' = h \uplus [x \mapsto (1,v)] * \mathit{heaps}_S(h',\zeta) * \mathit{disj}_H(h_0,h') * x \mapsto_S^{\zeta} v \end{array}$$

Proof.

$$\begin{array}{rl} & \mathit{heaps}_S(h,\zeta) * \mathit{disj}_H(h_0,h) \\ \text{(unfold)} \Rrightarrow & \exists h_Y.\ \mathit{heaps}_S(h,\zeta) * [h_Y]_H \wedge \mathrm{dom}(h_0) \cap h_Y = \emptyset \wedge (\mathrm{dom}(h) \setminus \mathrm{dom}(h_0)) \subset h_Y \\ \text{(below)} \Rrightarrow & \exists h_Y, x.\ \mathit{heaps}_S(h,\zeta) * [h_Y]_H \wedge \mathrm{dom}(h_0) \cap h_Y = \emptyset \wedge (\mathrm{dom}(h) \setminus \mathrm{dom}(h_0)) \subset h_Y * \\ & x \notin \mathrm{dom}(h) * x \in \mathrm{dom}(h_Y) \\ \text{(rewrite)} \Rrightarrow & \exists h_Y, x, h'.\ h' = h \uplus [x \mapsto (1,v)] * \mathit{heaps}_S(h,\zeta) * [h_Y]_H \wedge \mathrm{dom}(h_0) \cap h_Y = \emptyset \wedge \\ & (\mathrm{dom}(h') \setminus \mathrm{dom}(h_0)) \subset h_Y * x \notin \mathrm{dom}(h) \\ \text{(fold)} \Rrightarrow & \exists x, h'.\ h' = h \uplus [x \mapsto (1,v)] * \mathit{heaps}_S(h,\zeta) * \mathit{disj}_H(h_0,h') \\ (\textsc{FpAlloc}) \Rrightarrow & \exists x, h'.\ h' = h \uplus [x \mapsto (1,v)] * \mathit{heaps}_S(h',\zeta) * \mathit{disj}_H(h_0,h') * x \mapsto_S^{\zeta} v \end{array}$$

From h_Y being enumerable and $\mathrm{dom}(h)$ being finite, we can pick an x such that $x \notin \mathrm{dom}(h)$ and $x \in \mathrm{dom}(h_Y)$.

□

Lemma 68 (Trade allocate token)**.**

$$\forall h, r, \pi.\ \mathit{alloc}(h,r) * [\textsc{Al}]_r^{\pi} \ \Leftrightarrow [\textsc{Al}]_r^{\pi} * [\textsc{Al}(h_I, h_S)]_r^{1}$$
$$\forall h, r.\ \mathit{alloc}(h,r) * [\textsc{Al}]_r^{1} \Longleftrightarrow \mathit{alloc}(h,r) * [\textsc{Al}(h_I, h_S)]_r^{\frac{1}{2}}$$

Lemma 69 (Allocate in concrete code)**.**

$$\begin{array}{l} \forall x, v. \\ \quad \{\textsc{Heap}\} \\ \quad\quad \textbf{new}\ v \\ \quad \{l.\ \textsc{Heap} * l \mapsto v\} \end{array}$$

Lemma 70 (Allocate in specification code)**.**

$$\begin{array}{rl} & \forall e_0, h_0, j, x, v, \zeta, \pi. \\ & \quad \textsc{Spec}(h_0, e_0, \zeta) * [\textsc{Sr}]_{\zeta}^{\pi} * j \overset{\zeta}{\Rrightarrow}_S \textbf{new}\ v \\ \Rrightarrow & \quad \textsc{Spec}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S () * [\textsc{Sr}]_{\zeta}^{\pi} * \exists x.\ x \mapsto_S^{\zeta} v \end{array}$$

Proof.

$$
\begin{array}{rl}
 & \textsc{Spec}(h_0, e_0, \zeta) * [\textsc{Sr}]^{\pi}_{\zeta} * j \overset{\zeta}{\Rrightarrow}_S \textsf{new}\ v \\
\Rrightarrow & \exists h, e, \pi'.\ \textsc{Spec}(h_0, h, e_0, e, \pi', \zeta) * [\textsc{Sr}]^{\pi}_{\zeta} * j \overset{\zeta}{\Rrightarrow}_S \textsf{new}\ v \\
\Rrightarrow & \exists h, e, \pi'.\ \mathit{heap}_S(h, \zeta) * \mathit{mctx}(e, \zeta) * (h_0, e_0) \to^* (h, e) * [\textsc{Sr}]^{\pi'+\pi}_{\zeta} * \mathit{disj}_H(h_0, h) * \\
 & j \overset{\zeta}{\Rrightarrow}_S \textsf{new}\ v \\
(\textit{Lemma}\ \textbf{??}) \Rrightarrow & \exists h, h', e, \pi'.\ \mathit{heap}_S(h', \zeta) * \mathit{mctx}(e, \zeta) * (h_0, e_0) \to^* (h, e) * [\textsc{Sr}]^{\pi'+\pi}_{\zeta} * \mathit{disj}_H(h_0, h') * \\
 & j \overset{\zeta}{\Rrightarrow}_S \textsf{new}\ v * x \mapsto^{\zeta}_S v * h' = h \uplus [x \mapsto (1, v)] \\
(\textit{Lemma}\ \textbf{??}) \Rrightarrow & \exists h', e', \pi'.\ \mathit{heap}_S(h', \zeta) * \mathit{mctx}(e, \zeta) * (h_0, e_0) \to^* (h', e') * [\textsc{Sr}]^{\pi'+\pi}_{\zeta} * \mathit{disj}_H(h_0, h') * \\
 & j \overset{\zeta}{\Rrightarrow}_S () * x \mapsto^{\zeta}_S v \\
(\text{fold}) \Rrightarrow & \exists h', e', \pi'.\ \textsc{Spec}(h_0, h', e_0, e', \pi', \zeta) * [\textsc{Sr}]^{\pi}_{\zeta} * j \overset{\zeta}{\Rrightarrow}_S () * x \mapsto^{\zeta}_S v \\
(\text{fold}) \Rrightarrow & \textsc{Spec}(h_0, e_0, \zeta) * [\textsc{Sr}]^{\pi}_{\zeta} * j \overset{\zeta}{\Rrightarrow}_S () * x \mapsto^{\zeta}_S v
\end{array}
$$

We can take the step $(h, \textsf{new}\ v) \to (h'[x \mapsto v], ())$ since we have $x \notin \mathrm{dom}(h)$.

□

Lemma 71 (Extending region heap)**.**

$$
\begin{array}{rl}
 & \forall x, v, \pi, r, \pi, \iota.\ \boxed{\textsc{Reg}(r)}^{\iota} \\
\vdash & x_I \mapsto v_I * x_S \mapsto^{\zeta}_S v_S * [\textsc{Al}]^{\pi}_r * [\textsc{Mu}(r, \{\zeta\})]^{\pi} \\
{}^{\{i\}}\Rrightarrow^{\{i\}} & x_I \overset{1}{\hookrightarrow}_{I,r} v_I * x_S \overset{1}{\hookrightarrow}_{S,r} v_S * [\textsc{NoRd}(x)]_r * [\textsc{Al}]^{\pi}_r * [\textsc{Mu}(r, \{\zeta\})]^{\pi}
\end{array}
$$

Proof. By VSInv we obtain $\triangleright(\exists h.\ \mathit{locs}(h, r) * \mathit{toks}(1, 1, r))$ and we can remove the later by Lemma **??**. By having $\mathit{locs}(h, r)$, $x_I \mapsto v_I$ and $x_S \mapsto^{\zeta}_S v_S$ it is the case $x_I \notin \mathrm{dom}(h_I)$ and $x_S \notin \mathrm{dom}(h_S)$. By AFHeapAdd we obtain $x_I \overset{1}{\hookrightarrow}_{I,r} v_I$ and $x_S \overset{1}{\hookrightarrow}_{S,r} v_S$. By Lemma **??** we obtain the exclusive token guarding the domains of h_I and h_S and we can do a frame-preserving update and we also obtain $[\textsc{NoRd}(x)]_r$. We can fold $\exists h'.\ \mathit{locs}(h', r)$ since we have provided all spec points to required by *slink*, which we know since we own $[\textsc{Mu}(r, \{\zeta\})]^{\pi}$. □

Lemma 72 (Allocating region reference)**.**

$$
\begin{array}{rl}
 & \forall x, v, \phi, r. \\
 & \quad x_I \overset{1}{\hookrightarrow}_{I,r} v_I * x_S \overset{1}{\hookrightarrow}_{S,r} v_S * v \in \phi * [\textsc{NoRd}(x)]_r \\
{}^{\emptyset}\Rrightarrow^{\{\textsc{Rf}(x)\}} & \quad \boxed{\textsc{Ref}(r, \phi, x)}^{\textsc{Rf}(x)}
\end{array}
$$

Proof.

$$
\begin{array}{rl}
 & x_I \overset{1}{\hookrightarrow}_{I,r} v_I * x_S \overset{1}{\hookrightarrow}_{S,r} v_s * v \in \phi * [\textsc{NoRd}(x)]_r \\
\Longleftrightarrow & x_I \overset{\frac{1}{2}}{\hookrightarrow}_{I,r} v_I * x_I \overset{\frac{1}{2}}{\hookrightarrow}_{I,r} v_I * \mathit{effs}(r, \phi, x, v) \\
\Rrightarrow & \mathit{ref}(r, \phi, x, v) \\
\Rrightarrow^{\{\textsc{Rf}(x)\}} & \boxed{\textsc{Ref}(r, \phi, x)}^{\textsc{Rf}(x)}
\end{array}
$$

□

Lemma 73 (Allocate)**.**

$$\forall r, \zeta, j, v, \phi, \pi, \pi', \pi''.\ \boxed{\text{HEAP}}^{\text{Hp}}, \boxed{\text{SPEC}(h_0, e_0, \zeta)}^{\text{Sp}(\zeta)}, \boxed{\text{REG}(r)}^{\text{Rg}(r)}$$

$$\vdash \quad \left\{ j \overset{\zeta}{\Rrightarrow}_S \textbf{new}\ v_S * [\text{SR}]^{\pi''}_{\zeta} * [\text{AL}]^{\pi}_r * [\text{MU}(r, \{\zeta\})]^{\pi'} * v \in \phi \right\}$$

$$\textbf{new}\ v_I$$

$$\left\{ l_I.\ \exists l_S.\ j \overset{\zeta}{\Rrightarrow}_S l_S * [\text{SR}]^{\pi''}_{\zeta} * [\text{AL}]^{\pi}_r * [\text{MU}(r, \{\zeta\})]^{\pi'} * \boxed{\text{REF}(r, \phi, (l_I, l_S))}^{\text{Rf}(l_I, l_S)} \right\}_{\{\text{Hp}, \text{Sp}(\zeta), \text{Rg}(r)\}}$$

Proof.

Context $r, \zeta, j, v, \phi, \pi, \pi', \pi''$, $\boxed{\text{HEAP}}^{\text{Hp}}, \boxed{\text{SPEC}(h_0, e_0, \zeta)}^{\text{Sp}(\zeta)}, \boxed{\text{REG}(r)}^{\text{Rg}(r)}$

$$\left\{ j \overset{\zeta}{\Rrightarrow}_S \textbf{new}\ v_S * [\text{SR}]^{\pi''}_{\zeta} * [\text{AL}]^{\pi}_r * [\text{MU}(r, \{\zeta\})]^{\pi'} * v \in \phi \right\}_{\{\text{Hp}, \text{Sp}(\zeta), \text{Rg}(r)\}}$$

Open Hp, Sp(ζ)

$$\left\{ \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \textbf{new}\ v_S * [\text{SR}]^{\pi''}_{\zeta} \right\}_{\{\text{Rg}(r)\}}$$

$$\textbf{new}\ v_I$$

`// Lemma ??`

$$\left\{ l_I.\ \text{HEAP} * l_I \mapsto v_I * \text{SPEC}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S \textbf{new}\ v_S \right\}_{\{\text{Rg}(r)\}}$$

`// Lemma ??`

$$\left\{ l_I.\ \exists l_S.\ \text{HEAP} * l_I \mapsto v_I * \text{SPEC}(h_0, e_0, \zeta) * j \overset{\zeta}{\Rrightarrow}_S l_S * [\text{SR}]^{\pi''}_{\zeta} * l_S \mapsto^{\zeta}_S v_S \right\}_{\{\text{Rg}(r)\}}$$

$$\left\{ l_I.\ \exists l_S.\ j \overset{\zeta}{\Rrightarrow}_S l_S * l_I \mapsto v_I * l_S \mapsto^{\zeta}_S v_S * [\text{SR}]^{\pi''}_{\zeta} * [\text{AL}]^{\pi}_r * [\text{MU}(r, \{\zeta\})]^{\pi'} * v \in \phi \right\}_{\{\text{Hp}, \text{Sp}(\zeta), \text{Rg}(r)\}}$$

`// Lemma ?? and Lemma ??`

$$\left\{ l_I.\ \exists l_S.\ j \overset{\zeta}{\Rrightarrow}_S l_S * [\text{SR}]^{\pi''}_{\zeta} * [\text{AL}]^{\pi}_r * [\text{MU}(r, \{\zeta\})]^{\pi'} * \boxed{\text{REF}(r, \phi, (l_I, l_S))}^{\text{Rf}(l_I, l_S)} \right\}_{\{\text{Hp}, \text{Sp}(\zeta), \text{Rg}(r)\}}$$

□

Masking

Lemma 74.

$$\forall \Pi, \Lambda, \varepsilon, M_1, M_2, \zeta, g.\ (\forall \rho \in \Pi, \Lambda.\ M_1(\rho) = M_2(\rho)) \;\Rightarrow$$
$$P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M_1, \zeta) * P_{reg}(\Pi, g, \varepsilon, M_1, \zeta) = P_{reg}(\Lambda, \mathbf{1}, \varepsilon, M_2, \zeta) * P_{reg}(\Pi, g, \varepsilon, M_2, \zeta)$$

Proof. Unfolding shows syntactic equality between ghost-resources. □

Lemma 75.

$$\forall \Pi, \Lambda, M_1, M_2, e, \phi, \psi, \varepsilon.\ (\forall \rho \in \Pi, \Lambda.\ M_1(\rho) = M_2(\rho) \wedge \phi = \psi) \Rightarrow \mathcal{E}^{\Pi,\Lambda,M_1}_{\varepsilon,M}(\phi)(e) = \mathcal{E}^{\Pi,\Lambda,M_2}_{\varepsilon,M}(\psi)(e)$$

Proof. Follows by Lemma **??** and by $\phi = \psi$. □

Lemma 76.

$$\forall \tau, M_1, M_2.\ (\forall \rho \in FRV(\tau).\ M_1(\rho) = M_2(\rho)) \Rightarrow [\![\tau]\!]^{M_1} = [\![\tau]\!]^{M_2}$$

Proof. Induction on τ. The simple types are straight forward even for the binary case. Arrow type follows by Lemma **??**. To remind the reader, the following is the definition of reference types:

$$[\![\textbf{ref}_\rho\ \tau]\!]^M \triangleq \lambda x.\ \boxed{\text{REF}(M(\rho), [\![\tau]\!]^M, x)}^{\text{Rf}(x)} * \boxed{\text{REG}(M(\rho))}^{\text{Rg}(M(\rho))}$$

From $M_1(\rho) = M_2(\rho)$ we have $\boxed{\text{REG}(M_1(\rho))}^{\text{Rg}(M_1(\rho))} = \boxed{\text{REG}(M_2(\rho))}^{\text{Rg}(M_2(\rho))}$. Similarly, we have to show $\boxed{\text{REF}(M_1(\rho), [\![\tau]\!]^M, x)}^{\text{Rf}(x)} = \boxed{\text{REF}(M_2(\rho), [\![\tau]\!]^M, x)}^{\text{Rf}(x)}$ which follows directly from $M_1(\rho) = M_2(\rho)$ and the induction hypothesis. □

Lemma 77 (Creating monoids)**.**

$$\top \Rrightarrow \exists r.\ locs(\emptyset, r) * toks(1, 1, r) * r \notin dom(M)$$

Proof. Follows by repeated application of NewGhost. $\square$

Lemma 78.

$$\top \Rrightarrow \exists r.\ \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * [\textsc{Al}]^1_r$$

Proof. Follows by Lemma **??** and NewInv for creating $\exists r.\ \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)}$. $\square$

6.2 Soundness

Definition 3. $\Pi \mid \Lambda \mid \Gamma \vdash e_1 \leq_{ctx} e_2 : \tau, \varepsilon$ *iff for all contexts* C*, values* v*, and heaps* h_1 *such that* $C : (\Pi \mid \Lambda \mid \Gamma \vdash \tau, \varepsilon) \rightsquigarrow (- \mid - \mid - \vdash \boldsymbol{B}, \emptyset)$ *and* $[]; C[e_1] \to^* h_1; v$ *there exists a heap* h_2 *such that* $[]; C[e_2] \to^* h_2; v$.

Theorem 7 (Iris soundness)**.** *For all* $p \in Props$*,* $e \in Exp$*,* $q : Val \to Props$*,* $n, k \in \mathbb{N}$*,* $v \in Val$*,* $r \in Res$*,* $\sigma, \sigma' \in State$*,* $W \in World$*, and* $\mathcal{E} \in Mask$*, if*

$$valid(\{p\}\ e\ \{q\}_{\mathcal{E}}) \qquad e, \sigma \to^n v, \sigma' \qquad (n+k+1, r) \in p(W) \qquad (n+k+1, \sigma) \in \lfloor r \rfloor^W_{\mathcal{E}}$$

then there exists a $W' \geq W$ *and* $r' \in Res$ *such that*

$$(k+1, r') \in q(v)(W') \qquad\qquad (k+1, \sigma') \in \lfloor r' \rfloor^{W'}_{\mathcal{E}}$$

Lemma 79. *If* $\Pi \mid \Lambda \mid \Gamma \models_{\mathrm{PAR}} e_1 \leq_{log} e_2 : \tau, \varepsilon$ *and* $C : (\Pi \mid \Lambda \mid \Gamma \vdash \tau, \varepsilon) \rightsquigarrow (\Pi' \mid \Lambda' \mid \Gamma' \vdash \tau', \varepsilon')$ *then* $\Pi' \mid \Delta' \mid \Gamma' \models_{\mathrm{PAR}} C[e_1] \leq_{log} C[e_2] : \tau', \varepsilon'$.

Lemma 80. *If* $- \mid - \mid - \models_{\mathrm{PAR}} e_1 \leq_{log} e_2 : \tau, \varepsilon$ *then*

$$\vdash \{\top\}\ e_1\ \{\lambda v_1.\, \exists h_2.\, \exists v_2.\, (v_1, v_2) \in [\![\tau]\!] * []; e_2 \to^* h_2; v_2\}$$

Proof.

$\{\top\}$

$\left\{\exists \zeta.\ \boxed{\textsc{Spec}([], e_2, \zeta)}^{\textsc{Sp}(\zeta)} * 0 \overset{\zeta}{\Rrightarrow}_S e_2\right\}$

e_1

$\left\{v_1.\, \exists \zeta.\ \boxed{\textsc{Spec}([], e_2, \zeta)}^{\textsc{Sp}(\zeta)} * \exists v_2.\ [\![\tau]\!](v_1, v_2) * 0 \overset{\zeta}{\Rrightarrow}_S v_2\right\}$

$\{v_1.\, \exists v_2.\, [\![\tau]\!](v_1, v_2) * \exists h.\ []; e_2 \to^* h; v_2\}$

∎

Lemma 81. *If* $- \mid - \mid - \models_{\mathrm{PAR}} e_1 \leq_{log} e_2 : \boldsymbol{B}, \varepsilon$ *and* $[]; e_1 \to^* h_1; v_1$ *then there exists an* h_2 *such that* $[]; e_2 \to^* h_2; v_1$.

Proof.

- from the $- \mid - \mid - \vdash e_1 \leq_{log} e_2 : \mathbf{B}, \varepsilon$ assumption it follows by Lemma **??** that

$$\vdash \{\top\}\ e_1\ \{\lambda v_1.\, \exists h_2.\, \exists v_2.\, v_1 = v_2 * []; e_2 \to^* h_2; v_2\}$$

- hence, by Theorem **??**, it follows that there exists W and r such that

$$(2, r') \in (\lambda v_1.\, \exists h_2.\, \exists v_2.\, v_1 = v_2 * []; e_2 \to^* h_2; v_2)(v_1)(W)$$

  and $(2, h_I) \in \lfloor r' \rfloor^W_{\mathcal{E}}$

- hence, there exists v_2, h_2 such that $v_1 = v_2$ and $[]; e_2 \to^* h_2; v_2$.

∎

Theorem 8 (Soundness of $\mathrm{LR}_{\mathrm{PAR}}$)**.** *If* $\Pi \mid \Delta \mid \Gamma \models_{\mathrm{PAR}} e_1 \leq_{log} e_2 : \tau, \varepsilon$ *then* $\Pi \mid \Delta \mid \Gamma \vdash e_1 \leq_{ctx} e_2 : \tau, \varepsilon$

Proof.

- let $C : (\Pi \mid \Delta \mid \Gamma \vdash \tau, \varepsilon) \rightsquigarrow (- \mid - \mid - \vdash \mathbf{B}, \emptyset)$ and assume that $[]; C[e_1] \to^* h_1; v$
- by Lemma **??** it follows that $- \mid - \mid - \vdash C[e_1] \leq_{log} C[e_2] : \mathbf{B}, \emptyset$
- and thus, by Lemma **??**, there exists h_2 such that $[]; C[e_1] \to^* h_2; v$

∎

6.3 Effect-dependent transformations

6.3.1 Parallelization

Theorem 9 (Parallelization)**.** *Assuming*

1. $\Lambda_3 \mid \Lambda_1 \mid \Gamma \vdash e_1 : \tau_1, \varepsilon_1$
2. $\Lambda_3 \mid \Lambda_2 \mid \Gamma \vdash e_2 : \tau_2, \varepsilon_2$
3. $\mathsf{als}\, \varepsilon_1 \cup \mathsf{wrs}\, \varepsilon_1 \subseteq \Lambda_1$ *and* $\mathsf{als}\, \varepsilon_2 \cup \mathsf{wrs}\, \varepsilon_2 \subseteq \Lambda_2$
4. $\mathsf{rds}\, \varepsilon_1 \subseteq \Lambda_1 \cup \Lambda_3$ *and* $\mathsf{rds}\, \varepsilon_2 \subseteq \Lambda_2 \cup \Lambda_3$

then

$$\Pi \mid \Lambda_1, \Lambda_2, \Lambda_3 \mid \Gamma \vdash e_1 \,||\, e_2 \preceq (e_1, e_2) : \tau_1 \times \tau_2, \varepsilon_1 \cup \varepsilon_2$$

The two next lemmas provides the base of the proof:

Lemma 82 (Framed heap)**.** *If for all heaps h, h', h_F and expression e, e':*

$$(h; e) \to^* (h'; e) \wedge h_F \# h \wedge h_f \# h'$$

then

$$(h_F \uplus h; e) \to^* (h_F \uplus h'; e')$$

Proof. By induction. □

Lemma 83 (New disjoint range)**.**

$$\forall f, g, h.\, disj_H(f, g) \Rrightarrow disj_H(f, g) * disj_H(h, h,)$$

Lemma 84 (*disjoint* ensures disjointness)**.**

$$\begin{aligned}&\forall f_1, f_2, g, h, Z.\\ &\quad disj_H(f_1, g \uplus f_2) * disj_H(f_2, h) \Rrightarrow disj_H(f_1, g \uplus h)\end{aligned}$$

We define the following short-hand notations:

$$\begin{aligned}I(R) &\triangleq \{\mathrm{R{\scriptsize G}}(r) \mid r \in R\}\\ \mathit{HRef}(h, r) &\triangleq \exists \zeta s.\, locs(h, r, \zeta s, \emptyset) * toks(1, 1, r)\\ heaps(\zeta s, h) &\triangleq \circledast_{\zeta \in \zeta s} \circledast_{(l,v) \in h}\, l \mapsto_S^{\zeta} v\\ P_f(\Lambda, M, \zeta, \zeta_1, \zeta_2, \varepsilon_1, \varepsilon_2, h_1, h_2, h_3, h_{3R}) &\triangleq h_3 = \uplus_{r \in M(\Lambda)} h_{3R}(r) * heaps(\{\zeta\}, h_1 \uplus h_2 \uplus h_3) *\\ &\qquad \circledast_{\rho \in \mathsf{rds}\, \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2} [\mathrm{R{\scriptsize D}}]^{\frac{1}{2}}_{M(\rho)} *\\ &\qquad \circledast_{r \in M(\Lambda)} [\mathrm{I{\scriptsize M}}(r, \{\zeta_1, \zeta_2\}, h_{3R}(r))]^{\frac{1}{4}}\end{aligned}$$

Lemma 85.

$$\begin{aligned}&\forall r, \zeta s, \pi, \pi', r, y.\, \boxed{\mathrm{R{\scriptsize EG}}(r)}^{\mathrm{R{\scriptsize G}}(r)} \vdash\\ &\quad slink(r, \zeta s, y, \pi, \pi')\ {}^{\{\mathrm{R{\scriptsize G}}(r)\}}\!\!\Rrightarrow^{\emptyset} \exists h.\, \mathit{HRef}(h, r) * slink(r, \zeta s, h, \pi, \pi') * heaps(\zeta s, h)\end{aligned}$$

Lemma 86.

$$\begin{aligned}&\forall r, \zeta s, r.\, \boxed{\mathrm{R{\scriptsize EG}}(r)}^{\mathrm{R{\scriptsize G}}(r)} \vdash\\ &\quad slink(r, \zeta s, h, \tfrac{1}{2}, \tfrac{3}{4}) * \mathit{HRef}(h, r) * heaps(\zeta s', h)\ {}^{\emptyset}\!\!\Rrightarrow^{\{\mathrm{R{\scriptsize G}}(r)\}} slink(r, \zeta s', h, \tfrac{1}{2}, \tfrac{3}{4})\end{aligned}$$

Lemma 87 (Create branching specification invariant)**.**

$$\begin{array}{ll} & \forall h, e. \\ & \quad disj_H(h,h) \\ \Rrightarrow & \exists \zeta.\, \textsc{Spec}(h,e,\zeta) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta} * 0 \overset{\zeta}{\Rrightarrow}_S e * heaps(\{\zeta\}, h) \end{array}$$

Lemma 88 (Prepare None-interference parallelization)**.**

$$\begin{array}{ll} & \forall j, e_1, e_2, \Lambda_1, \Lambda_2, \Lambda_3, \varepsilon_1, \varepsilon_2, M, \zeta, h_0, h_S, T_0, T.\ R = I(M(\Lambda_1 \uplus \Lambda_2 \uplus \Lambda_3)) \Rightarrow \\ & \quad P_{reg}(\Lambda_1, \boldsymbol{1}, \varepsilon_1, M, \{\zeta\}) * P_{reg}(\Lambda_2, \boldsymbol{1}, \varepsilon_2, M, \{\zeta\}) * \\ & \quad P_{reg}(\Lambda_3, \boldsymbol{1}, \varepsilon_1 \cup \varepsilon_2, M, \{\zeta\}) * disj_H(h_0, h_S) \\ {}^{R}\Rrightarrow^{R \cup \{\textsc{Sp}(\zeta_1), \textsc{Sp}(\zeta_2)\}} & \quad \exists \zeta_1, \zeta_2, h_1, h_2, h_3, h_{3R}.\ S(\zeta_1, 0, h_1 \uplus h_3, e_1, e_1, \frac{1}{2}, (\Lambda_1, \Lambda_3), \boldsymbol{\frac{1}{2}}, \varepsilon_1, M) * \\ & \quad S(\zeta_2, 0, h_2 \uplus h_3, e_2, e_2, \frac{1}{2}, (\Lambda_2, \Lambda_3), \boldsymbol{\frac{1}{2}}, \varepsilon_2, M) * disj_H(h_0, h_S) * \\ & \quad P_f(\Lambda_3, M, \zeta, \zeta_1, \zeta_2, \varepsilon_1, \varepsilon_2, h_1, h_2, h_3, h_{3R}) \end{array}$$

Proof.

$$\left\{P_{reg}(\Lambda_1,\mathbf{1},\varepsilon_1,M,\{\zeta\}) * P_{reg}(\Lambda_2,\mathbf{1},\varepsilon_2,M,\{\zeta\}) * P_{reg}(\Lambda_3,\mathbf{1},\varepsilon_1\cup\varepsilon_2,M,\{\zeta\}) * disj_H(h_0,h_S)\right\}_R$$

$$\left\{\begin{array}{l} P_{regs}(\Lambda_1\cup\Lambda_2\cup\Lambda_3,M) * P_{effs}(\Lambda_1,\mathbf{1},\varepsilon_1,M) * P_{effs}(\Lambda_2,\mathbf{1},\varepsilon_2,M) * P_{effs}(\Lambda_3,\mathbf{1},\varepsilon_1\cup\varepsilon_2,M) \\ P_{par}(\Lambda_1,\mathbf{1},\varepsilon_1,M,\{\zeta\}) * P_{par}(\Lambda_2,\mathbf{1},\varepsilon_2,M,\{\zeta\}) * P_{par}(\Lambda_3,\mathbf{1},\varepsilon_1\cup\varepsilon_2,M,\{\zeta\}) * disj_H(h_0,h_S)\end{array}\right\}_R$$

Frame

$$\{P_{par}(\Lambda_1,\mathbf{1},\varepsilon_1,M,\{\zeta\}) * P_{par}(\Lambda_2,\mathbf{1},\varepsilon_2,M,\{\zeta\}) * P_{par}(\Lambda_3,\mathbf{1},\varepsilon_1\cup\varepsilon_2,M,\{\zeta\}) * disj_H(h_0,h_S)\}_R$$

$$\left\{\circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3}[\textsc{Mu}(M(\rho),\{\zeta\})]^{\frac{1}{2}} * disj_H(h_0,h_S)\right\}_R$$

`// Lemma ??`

$$\left\{\circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3}\exists h.\ HRef(h,M(\rho)) * [\textsc{Mu}(M(\rho),\{\zeta\})]^{\frac{1}{2}} * heaps(\{\zeta\},h) * disj_H(h_0,h_S)\right\}_\emptyset$$

$$\left\{\exists h.\ \circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3} HRef(h(\rho),M(\rho)) * [\textsc{Mu}(M(\rho),\{\zeta\})]^{\frac{1}{2}} * heaps(\{\zeta\},h(\rho)) * disj_H(h_0,h_S)\right\}_\emptyset$$

Let $h_i = \prod_{\rho\in\Lambda_i} h(\rho)$ for $i\in\{1,2,3\}$

`// Follows from Lemma ??`

$$\left\{\begin{array}{l}\exists h.\ \circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3} HRef(h(\rho),M(\rho)) * [\textsc{Mu}(M(\rho),\{\zeta\})]^{\frac{1}{2}} * heaps(\{\zeta\},h(\rho)) * disj_H(h_0,h_S) \\ disj_H(h_1\uplus h_3, h_1\uplus h_3) * disj_H(h_2\uplus h_3, h_2\uplus h_3)\end{array}\right\}_\emptyset$$

`// Follows from Lemma ??`

$$\left\{\begin{array}{l}\circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3}\ HRef(h(\rho),M(\rho)) * [\textsc{Mu}(M(\rho),\{\zeta\})]^{\frac{1}{2}} * heaps(\{\zeta\},h(\rho)) * disj_H(h_0,h_S) \\ \exists\zeta_1.\ \textsc{Spec}(h_1\uplus h_3,e_1,\zeta_1) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_1} * 0 \overset{\zeta_1}{\Longrightarrow}_S e_1 * heaps(\{\zeta_1\},h_1\uplus h_3) \\ \exists\zeta_2.\ \textsc{Spec}(h_2\uplus h_3,e_2,\zeta_2) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_2} * 0 \overset{\zeta_2}{\Longrightarrow}_S e_2 * heaps(\{\zeta_2\},h_2\uplus h_3)\end{array}\right\}_\emptyset$$

Let $E(\zeta_1,\zeta_2) = \textsc{Spec}(h_1\uplus h_3,e_1,\zeta_1) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_1} * 0 \overset{\zeta_1}{\Longrightarrow}_S e_1 *$
$\textsc{Spec}(h_2\uplus h_3,e_2,\zeta_2) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_2} * 0 \overset{\zeta_2}{\Longrightarrow}_S e_2$

$$\left\{\begin{array}{l}\exists\zeta_1,\zeta_2.\ E(\zeta_1,\zeta_2) * disj_H(h_0,h_S) * \circledast_{\rho\in\Lambda_1}[\textsc{Mu}(M(\rho),\{\zeta_1\})]^{\frac{1}{2}} * \circledast_{\rho\in\Lambda_2}[\textsc{Mu}(M(\rho),\{\zeta_2\})]^{\frac{1}{2}} * \\ \circledast_{\rho\in\Lambda_3}[\textsc{Im}(M(\rho),\{\zeta_1,\zeta_2\},h(\rho))]^{\frac{3}{4}} * \circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3} heaps(\{\zeta\},h(\rho))\end{array}\right\}_R$$

$$\left\{\begin{array}{l}\exists\zeta_1,\zeta_2.\ E(\zeta_1,\zeta_2) * disj_H(h_0,h_S) * P_{regs}((\Lambda_1,\Lambda_2,\Lambda_3),M) * P_{effs}(\Lambda_1,\mathbf{1},\varepsilon_1,M) * \\ P_{effs}(\Lambda_1,\mathbf{1},\varepsilon_2,M) * P_{effs}(\Lambda_3,\mathbf{1},\varepsilon_1\cup\varepsilon_2,M) * \circledast_{\rho\in\Lambda_1}[\textsc{Mu}(M(\rho),\{\zeta_1\})]^{\frac{1}{2}} * \\ \circledast_{\rho\in\Lambda_2}[\textsc{Mu}(M(\rho),\{\zeta_2\})]^{\frac{1}{2}} * \circledast_{\rho\in\Lambda_3}[\textsc{Im}(M(\rho),\{\zeta_1,\zeta_2\},h(\rho))]^{\frac{3}{4}} * \circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3} heaps(\{\zeta\},h(\rho))\end{array}\right\}_R$$

$$\left\{\begin{array}{l}\exists\zeta_1,\zeta_2.\ E(\zeta_1,\zeta_2) * disj_H(h_0,h_S) * P_{reg}(\Lambda_1,\mathbf{1},\varepsilon_1,M,\{\zeta_1\}) * P_{reg}(\Lambda_2,\mathbf{1},\varepsilon_2,M,\{\zeta_2\}) \\ P_{reg}(\Lambda_3,\frac{1}{4},\varepsilon_1,M,\{\zeta_1\}) * P_{reg}(\Lambda_3,\frac{1}{4},\varepsilon_2,M,\{\zeta_2\}) * \circledast_{\rho\in\Lambda_3}[\textsc{Im}(M(\rho),\{\zeta_1,\zeta_2\},h(\rho))]^{\frac{1}{4}} * \\ \circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3} heaps(\{\zeta\},h(\rho))\ \circledast_{\rho\in\Lambda_3\cap(\mathsf{rds}\ ((\varepsilon_1\cup\varepsilon_2)\setminus(\varepsilon_1\cap\varepsilon_2)))}\ [\textsc{Rd}]^{\frac{1}{2}}_{M(\rho)}\end{array}\right\}_R$$

$$\left\{\begin{array}{l}\exists\zeta_1,\zeta_2.\ disj_H(h_0,h_S) * S(\zeta_1,0,h_1,e_1,e_1,\frac{1}{2},(\Lambda_1,\Lambda_3),\mathbf{\tfrac{1}{2}},\varepsilon_1,M) * \\ S(\zeta_2,0,h_2,e_2,e_2,\frac{1}{2},(\Lambda_2,\Lambda_3),\mathbf{\tfrac{1}{2}},\varepsilon_2,M) * \circledast_{\rho\in\Lambda_3}[\textsc{Im}(M(\rho),\{\zeta_1,\zeta_2\},h(\rho))]^{\frac{1}{4}} * \\ \circledast_{\rho\in\Lambda_1,\Lambda_2,\Lambda_3} heaps(\{\zeta\},h(\rho)) * \circledast_{\rho\in\Lambda_3\cap(rds\ ((\varepsilon_1\cup\varepsilon_2)\setminus(\varepsilon_1\cap\varepsilon_2)))}[\textsc{Rd}]^{\frac{1}{2}}_{M(\rho)}\end{array}\right\}_{R\cup\{\textsc{Sp}(\zeta_1),\textsc{Sp}(\zeta_2)\}}$$

$$\left\{\begin{array}{l}S(\zeta_1,0,h_1,e_1,e_1,\frac{1}{2},(\Lambda_1,\Lambda_3),\mathbf{\tfrac{1}{2}},\varepsilon_1,M) * S(\zeta_2,0,h,2e_2,e_2,\frac{1}{2},(\Lambda_2,\Lambda_3),\mathbf{\tfrac{1}{2}},\varepsilon_2,M) * \\ P_f(\Lambda_3,M,\zeta,\zeta_1,\zeta_2,\varepsilon_1,\varepsilon_2,h_1,h_2,h_3,h) * disj_H(h_0,h_S)\end{array}\right\}_{R\cup\{\textsc{Sp}(\zeta_1),\textsc{Sp}(\zeta_2)\}}$$

$\square$

Lemma 89 (Combine shared part with frame)**.**

$$\begin{array}{ll} & \forall \Lambda, \varepsilon_1, \varepsilon_2, M, \zeta_1, \zeta_2, h. \\ & \quad (\mathsf{wrs}\,(\varepsilon_1 \cup \varepsilon_2) \cup \mathsf{als}\,(\varepsilon_1 \cup \varepsilon_2)) \cap \Lambda = \emptyset \Rightarrow \\ & \quad P_{reg}(\Lambda, \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M, \zeta_1) * P_{reg}(\Lambda, \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M, \zeta_2) * \circledast_{\rho \in \mathsf{rds}\ \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2} [\mathrm{RD}]^{\frac{1}{2}}_{M(\rho)} * \\ & \quad \circledast_{r \in M(\Lambda)} \left[\mathrm{IM}(r, \{\zeta_1, \zeta_2\}, h(r))\right]^{\frac{1}{4}} \\ \Rrightarrow & \quad \circledast_{r \in M(\Lambda)} \left[\mathrm{IM}(r, \{\zeta_1, \zeta_2\}, h(r))\right]^{\frac{3}{4}} * P_{\mathit{effs}}(\Lambda, \mathbf{\mathit{1}}, \varepsilon_1 \cup \varepsilon_2, M) * P_{\mathit{regs}}(\Lambda, M) \end{array}$$

Lemma 90.

$$\begin{array}{ll} & \forall \zeta, j, e_0, e, h, h_0.\ \boxed{\mathrm{SPEC}(h_0, e_0, \zeta)}^{\mathrm{SP}(\zeta)} \vdash \\ & \quad j \overset{\zeta}{\Rrightarrow}_S e * heaps(h, \{\zeta\}) \\ {}^{\{\mathrm{SP}(\zeta)\}}\!\Rrightarrow^{\emptyset} & \quad \exists h_S, e'.\ \mathrm{SPEC}(h_0, h \uplus h_S, e_0, e', \tfrac{1}{2}, \zeta) * j \overset{\zeta}{\Rrightarrow}_S e * heaps(h, \{\zeta\}) \end{array}$$

Lemma 91 (Frozen regions are frames)**.**

$$\begin{array}{l} \forall h, h_f, \zeta, r, \pi.\ \boxed{\mathrm{REG}(r)}^{\mathrm{RG}(r)}, \zeta \in \zeta s \vdash \\ \quad heap_S(h, \zeta) * [\mathrm{IM}(r, \zeta s, h_f)]^{\pi}\ {}^{\{\mathrm{RG}(r)\}}\!\Rrightarrow^{\emptyset}\ \exists h'.\ heap_S(h' \uplus h_f, \zeta) * [\mathrm{IM}(r, \zeta s, h_f)]^{\pi} \end{array}$$

Proof. Follows Lemma **??** for each region. □

Lemma 92 (Obtain disjoint token by trading specification runner)**.**

$$\begin{array}{ll} & \forall h_0, h, e_0, e, \tfrac{1}{2}, \zeta. \\ & \quad \mathrm{SPEC}(h_0, h, e_0, e, \tfrac{1}{2}, \zeta) * [\mathrm{SR}]^{\frac{1}{2}}_{\zeta} \\ \Rrightarrow & \quad \mathrm{SPEC}(h_0, h, e_0, e, 1, \zeta) * disj_H(h_0, h) * (h_0, e_0) \to^* (h, e) \end{array}$$

Lemma 93 (Combining new specs with old spec)**.**

$$\begin{array}{ll} & \forall h_0, h_S, h_1, h_1', e_0, e, e_1, e_1', \zeta, \zeta'. \\ & \quad \mathrm{SPEC}(h_1, h_1', e_1, e_1', \tfrac{1}{2}, \zeta') * [\mathrm{SR}]^{\frac{1}{2}}_{\zeta'} * \\ & \quad \mathrm{SPEC}(h_0, h_S \uplus h_1, e_0, e, \tfrac{1}{2}, \zeta) * [\mathrm{SR}]^{\pi}_{\zeta} * j \overset{\zeta}{\Rrightarrow}_S e_1 * heaps(\{\zeta\}, h_1) \\ \Rrightarrow & \quad \exists e''.\ \mathrm{SPEC}(h_1, h_1', e_1, e_1', 1, \zeta') * \\ & \quad \mathrm{SPEC}(h_0, h_S \uplus h_1', e_0, e'', \tfrac{1}{2}, \zeta) * [\mathrm{SR}]^{\pi}_{\zeta} * j \overset{\zeta}{\Rrightarrow}_S e_1' * heaps(\{\zeta\}, h_1') \end{array}$$

Proof.
By Lemma **??** we obtain $disj_H(h_1, h_1') * (h_1, e_1) \to^* (h_1', e_1')$ for simulation in ζ'. By Lemma **??** we have that $h_S' \# h_1'$ thus we allocate $\mathrm{dom}(h_1') \setminus \mathrm{dom}(h_1)$ with the values specifically in h_1'. For all values in h_1 we own the points to predicate thus we can just update it directly. To update the stepping relation we use Lemma **??** and Lemma **??**. □

Lemma 94 (Swap immutable to mutable for regions)**.**

$$\begin{array}{l} \forall R_1, R_2, R_3, h_1, h_2, h_3, \zeta, \zeta_1, \zeta_2, h_{3R}.\ \circledast_{r \in R_1 \uplus R_2 \uplus R_3} \left(\boxed{\mathrm{REG}(r)}^{\mathrm{RG}(r)}, h_3 = \uplus_{r \in R_3} h_{3R}(r)\right) \vdash \\ \quad heap_S(h_1 \uplus h_3, \zeta_1) * heap_S(h_2 \uplus h_3, \zeta_2) * \circledast_{i \in \{1,2\}} \circledast_{r \in R_i} [\mathrm{MU}(r, \{\zeta_i\})]^{\frac{1}{2}} * \\ \quad \circledast_{r \in R_3} \left(\mathrm{REG}(r) * [\mathrm{IM}(r, \{\zeta_1, \zeta_2\}, h_{3R}(r))]^{\frac{3}{4}}\right) * \circledast_{(l,v) \in h_1 \uplus h_2 \uplus h_3} l \mapsto^{\zeta}_{S} v \\ {}^{\{\mathrm{RG}(r) \mid r \in R_1 \uplus R_2\}}\!\Rrightarrow^{\{\mathrm{RG}(r) \mid r \in R_1 \uplus R_2 \uplus R_3\}} \\ \quad heap_S(h_1 \uplus h_3, \zeta_1) * heap_S(h_2 \uplus h_3, \zeta_2) * \circledast_{r \in R_1 \uplus R_2 \uplus R_3} [\mathrm{MU}(r, \{\zeta\})]^{\frac{1}{2}} \end{array}$$

Lemma 95 (Complete Non-interference parallelization)**.**

$$\begin{array}{ll}
& \forall \zeta, \zeta_1, \zeta_2, \Lambda_1, \Lambda_2, \Lambda_3, M, e_1, e_2, v_1, v_2, j, h_1, h_2, h_3, h_{3R}, \pi, \varepsilon_1, \varepsilon_2, R, S. \\
& \quad R = I(M(\Lambda_1 \uplus \Lambda_2 \uplus \Lambda_3)), S = \{\textsc{Sp}(\zeta), \textsc{Sp}(\zeta_1), \textsc{Sp}(\zeta_2)\} \vdash \\
& \qquad S(\zeta_1, 0, h_1, e_1, v_1, \tfrac{1}{2}, (\Lambda_1, \Lambda_3), \boldsymbol{\tfrac{1}{2}}, \varepsilon_1, M) * S(\zeta_2, 0, h_2, e_2, v_2, \tfrac{1}{2}, (\Lambda_2, \Lambda_3), \boldsymbol{\tfrac{1}{2}}, \varepsilon_2, M) \; * \\
& \qquad P_f(\Lambda_3, M, \zeta, \zeta_1, \zeta_2, \varepsilon_1, \varepsilon_2, h_1, h_2, h_3, h_{3R}) * j \overset{\zeta}{\Rightarrow}_S (e_1, e_2) * [\textsc{Sr}]^{\pi}_{\zeta} * \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)} \\
\Rrightarrow_{R \uplus S} & j \overset{\zeta}{\Rightarrow}_S (v_1, v_2) * [\textsc{Sr}]^{\pi}_{\zeta} * P_{reg}(\Lambda_1, \boldsymbol{1}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_2, \boldsymbol{1}, \varepsilon_2, M, \zeta) \; * \\
& P_{reg}(\Lambda_3, \boldsymbol{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) * \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}
\end{array}$$

Proof.

$$\text{Context: } \zeta, \zeta_1, \zeta_2, R, \Lambda_1, \Lambda_2, \Lambda_3, M, e_0, e_1, e_2, v_1, v_2, j, h_0, h_1, h_2, h_3, h_{3R}, \pi, \varepsilon_1, \varepsilon_2$$

$$S(\zeta_1, 0, h_1, e_1, v_1, \tfrac{1}{2}, (\Lambda_1, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M) * S(\zeta_2, 0, h_2, e_2, v_2, \tfrac{1}{2}, (\Lambda_2, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M) *$$

$$P_f(\Lambda_3, M, \zeta, \zeta_1, \zeta_2, \varepsilon_1, \varepsilon_2, h_1, h_2, h_3, h_{3R}) * j \overset{\zeta}{\Rrightarrow}_S (e_1, e_2) * [\textsc{Sr}]^{\pi}_{\zeta} * \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}$$

$\Rrightarrow_{R \uplus \{\textsc{Sp}(\zeta), \textsc{Sp}(\zeta_1), \textsc{Sp}(\zeta_2)\}}$ `// Unfold` S `and` P_f

$$\text{Context: } \boxed{\textsc{Spec}(h_1, e_1, \zeta_1)}^{\textsc{Sp}(\zeta_1)}, \boxed{\textsc{Spec}(h_2, e_2, \zeta_2)}^{\textsc{Sp}(\zeta_2)}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}$$

$$0 \overset{\zeta_1}{\Rrightarrow}_S v_1 * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_1} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta_1) * P_{reg}(\Lambda_3, \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M, \zeta_1) *$$

$$0 \overset{\zeta_2}{\Rrightarrow}_S v_2 * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_2} * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta_2) * P_{reg}(\Lambda_3, \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M, \zeta_2) *$$

$$h_3 = \uplus_{r \in M(\Lambda_3)} h_{3R}(r) * \mathit{heaps}(\{\zeta\}, h_1 \uplus h_2 \uplus h_3) * \circledast_{\rho \in \mathsf{rds}\ \varepsilon_1 \cup \varepsilon_2 \setminus \varepsilon_1 \cap \varepsilon_2} [\textsc{Rd}]^{\frac{1}{2}}_{M(\rho)} *$$

$$\circledast_{r \in M(\Lambda_3)} [\textsc{Im}(r, \{\zeta_1, \zeta_2\}, h_{3R}(r))]^{\frac{1}{4}} * j \overset{\zeta}{\Rrightarrow}_S (e_1, e_2) * [\textsc{Sr}]^{\pi}_{\zeta}$$

$\Rrightarrow_{R \uplus \{\textsc{Sp}(\zeta), \textsc{Sp}(\zeta_1), \textsc{Sp}(\zeta_2)\}}$ `// Lemma ??`

$$0 \overset{\zeta_1}{\Rrightarrow}_S v_1 * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_1} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta_1) * 0 \overset{\zeta_2}{\Rrightarrow}_S v_2 * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_2} * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta_2) *$$

$$h_3 = \uplus_{r \in M(\Lambda_3)} h_{3R}(r) * \mathit{heaps}(\{\zeta\}, h_1 \uplus h_2 \uplus h_3) * \circledast_{r \in M(\Lambda_3)} [\textsc{Im}(r, \{\zeta_1, \zeta_2\}, h(r))]^{\frac{3}{4}} *$$

$$P_{\mathit{effs}}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M) * P_{\mathit{regs}}(\Lambda_3, M) * j \overset{\zeta}{\Rrightarrow}_S (e_1, e_2) * [\textsc{Sr}]^{\pi}_{\zeta}$$

$\Rrightarrow_R$ `// Lemma ??`

$$\exists h_0, h_S, e_0, e_S, e_1, e_2, h_1', h_2', v_1, v_2.\ \textsc{Spec}(h_0, h_S \uplus h_1 \uplus h_2 \uplus h_3, e_0, e_S, \tfrac{1}{2}, \zeta) *$$

$$\textsc{Spec}(h_1 \uplus h_3, h_1', e_1, v_1, \tfrac{1}{2}, \zeta_1) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_1} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta_1) *$$

$$\textsc{Spec}(h_2 \uplus h_3, h_2', e_2, v_2, \tfrac{1}{2}, \zeta_2) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_2} * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta_2) *$$

$$h_3 = \uplus_{r \in M(\Lambda_3)} h_{3R}(r) * \mathit{heaps}(\{\zeta\}, h_1 \uplus h_2 \uplus h_3) * \circledast_{r \in M(\Lambda_3)} [\textsc{Im}(r, \{\zeta_1, \zeta_2\}, h_{3R}(r))]^{\frac{3}{4}} *$$

$$P_{\mathit{effs}}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M) * P_{\mathit{regs}}(\Lambda_3, M) * j \overset{\zeta}{\Rrightarrow}_S (e_1, e_2) * [\textsc{Sr}]^{\pi}_{\zeta}$$

$\Rrightarrow_{\{\textsc{Rg}(r) | r \in M(\Lambda_1 \uplus \Lambda_2)\}}$ `// Lemma ??`

$$\exists h_0, h_S, e_0, e_S, e_1, e_2, h_1', h_2', v_1, v_2.\ \textsc{Spec}(h_0, h_S \uplus h_1 \uplus h_2 \uplus h_3, e_0, e_S, \tfrac{1}{2}, \zeta) *$$

$$\textsc{Spec}(h_1 \uplus h_3, h_1' \uplus h_3, e_1, v_1, \tfrac{1}{2}, \zeta_1) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_1} * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta_1) *$$

$$\textsc{Spec}(h_2 \uplus h_3, h_2' \uplus h_3, e_2, v_2, \tfrac{1}{2}, \zeta_2) * [\textsc{Sr}]^{\frac{1}{2}}_{\zeta_2} * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta_2) *$$

$$h_3 = \uplus_{r \in M(\Lambda_3)} h_{3R}(r) * \mathit{heaps}(\{\zeta\}, h_1 \uplus h_2 \uplus h_3) * \circledast_{r \in M(\Lambda_3)} [\textsc{Im}(r, \{\zeta_1, \zeta_2\}, h_{3R}(r))]^{\frac{3}{4}} *$$

$$P_{\mathit{effs}}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M) * \circledast_{r \in M(\Lambda_3)} \textsc{Reg}(r) * j \overset{\zeta}{\Rrightarrow}_S (e_1, e_2) * [\textsc{Sr}]^{\pi}_{\zeta}$$

$\Rrightarrow_{\{\textsc{Rg}(r) | r \in M(\Lambda_1 \uplus \Lambda_2)\}}$ `// Lemma ?? with` $k_1 \overset{\zeta}{\Rrightarrow}_S e_1$ `and Lemma ?? with` $k_2 \overset{\zeta}{\Rrightarrow}_S e_2$

$$\exists h_0, h_S, e_0, e_S', e_1, e_2, h_1', h_2', v_1, v_2.\ \textsc{Spec}(h_0, h_S \uplus h_1' \uplus h_2' \uplus h_3, e_0, e_S', \tfrac{1}{2}, \zeta) *$$

$$\textsc{Spec}(h_1 \uplus h_3, h_1' \uplus h_3, e_1, v_1, 1, \zeta_1) * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta_1) *$$

$$\textsc{Spec}(h_2 \uplus h_3, h_2' \uplus h_3, e_2, v_2, 1, \zeta_2) * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta_2) *$$

$$h_3 = \uplus_{r \in M(\Lambda_3)} h_{3R}(r) * \mathit{heaps}(\{\zeta\}, h_1' \uplus h_2' \uplus h_3) * \circledast_{r \in M(\Lambda_3)} [\textsc{Im}(r, \{\zeta_1, \zeta_2\}, h_{3R}(r))]^{\frac{3}{4}} *$$

$$P_{\mathit{effs}}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M) * \circledast_{r \in M(\Lambda_3)} \textsc{Reg}(r) * j \overset{\zeta}{\Rrightarrow}_S (v_1, v_2) * [\textsc{Sr}]^{\pi}_{\zeta}$$

$\Rrightarrow_R$ `// Lemma ??`

$\exists h_0, h_S, e_0, e'_S, e_1, e_2, h'_1, h'_2, v_1, v_2.\ \textsc{Spec}(h_0, h_S \uplus h'_1 \uplus h'_2 \uplus h_3, e_0, e'_S, \frac{1}{2}, \zeta) \ast$
$\textsc{Spec}(h_1 \uplus h_3, h'_1 \uplus h_3, e_1, v_1, 1, \zeta_1) \ast P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) \ast$
$\textsc{Spec}(h_2 \uplus h_3, h'_2 \uplus h_3, e_2, v_2, 1, \zeta_2) \ast P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) \ast$
$\circledast_{r \in M(\Lambda_3)} [\textsc{Mu}(r, \{\zeta\})]^{\frac{3}{4}} \ast \circledast_{r \in M(\Lambda)} \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} \ast P_{effs}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M) \ast j \overset{\zeta}{\Rrightarrow}_S (v_1, v_2) \ast [\textsc{Sr}]^{\pi}_{\zeta}$

$\Rrightarrow_{R \uplus \{\textsc{Sp}(\zeta), \textsc{Sp}(\zeta_1), \textsc{Sp}(\zeta_2)\}}$
$\boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)} \ast P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) \ast P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) \ast P_{reg}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \ast$
$j \overset{\zeta}{\Rrightarrow}_S (v_1, v_2) \ast [\textsc{Sr}]^{\pi}_{\zeta}$

$\square$

Proof of Parallelization.

Let $\Lambda = \Lambda_1, \Lambda_2, \Lambda_3$ and we have to show $\mathcal{E}^{\cdot;\Lambda}_{\varepsilon_1 \cup \varepsilon_2, M}(\tau_1 \times \tau_2)(e_{1I} \,||\, e_{2I}, (e_{1S}, e_{2S}))$:

Context: $j, \pi, \zeta, h_0, e_0, \boxed{\text{HEAP}}^{\text{HP}}, \boxed{\text{SPEC}(h_0, e_0, \zeta)}^{\text{SP}(\zeta)}$

$$\left\{ j \xRightarrow{\zeta}_S (e_{1S}, e_{2S}) * [\text{SR}]^{\pi}_{\zeta} * P_{reg}(\Lambda, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \right\}_{\{\text{HP},\text{SP}(\zeta)\}}$$

Open $\text{SP}(\zeta)$

$$\left\{ \begin{array}{l} j \xRightarrow{\zeta}_S (e_{1S}, e_{2S}) * [\text{SR}]^{\pi}_{\zeta} * \triangleright(\text{SPEC}(h_0, e_0, \zeta)) * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * \\ P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{HP}\}}$$

`// Lemma ??`

$$\left\{ \begin{array}{l} \exists \zeta_1, \zeta_2, h_1, h_2, h_3, h_{3R}.\ \text{SPEC}(h_0, e_0, \zeta) * j \xRightarrow{\zeta}_S (e_1, e_2) * [\text{SR}]^{\pi}_{\zeta} * \\ S(\zeta_1, 0, h_1 \uplus h_3, e_{1S}, e_{1S}, \tfrac{1}{2}, (\Lambda_1, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M) * \\ S(\zeta_2, 0, h_2 \uplus h_3, e_{2S}, e_{2S}, \tfrac{1}{2}, (\Lambda_2, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M) * \\ P_f(\Lambda_3, M, \zeta, \zeta_1, \zeta_2, \varepsilon_1, \varepsilon_2, h_1, h_2, h_3, h_{3R}) \end{array} \right\}_{\{\text{HP},\text{SP}(\zeta_1),\text{SP}(\zeta_2)\}}$$

$$\left\{ \begin{array}{l} \exists \zeta_1, \zeta_2, h_1, h_2, h_3, h_{3R}.\ S(\zeta_1, 0, h_1 \uplus h_3, e_{1S}, e_{1S}, \tfrac{1}{2}, (\Lambda_1, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M) * \\ S(\zeta_2, 0, h_2 \uplus h_3, e_{2S}, e_{2S}, \tfrac{1}{2}, (\Lambda_2, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M) * j \xRightarrow{\zeta}_S (e_1, e_2) * [\text{SR}]^{\pi}_{\zeta} * \\ P_f(\Lambda_3, M, \zeta, \zeta_1, \zeta_2, \varepsilon_1, \varepsilon_2, h_1, h_2, h_3, h_{3R}) \end{array} \right\}_{\{\text{HP},\text{SP}(\zeta),\text{SP}(\zeta_1),\text{SP}(\zeta_2)\}}$$

$e_1 \,||\, e_2$

$$\left\{ S(\zeta_1, 0, h_1 \uplus h_3, e_{1S}, e_{1S}, \tfrac{1}{2}, (\Lambda_1, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M) \right\}$$

e_{1I}

$$\left\{ v_{1I}.\ \exists v_{1S}.\ S(\zeta_1, 0, h_1 \uplus h_3, e_{1S}, v_{1S}, \tfrac{1}{2}, (\Lambda_1, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M) * [\![\tau_1]\!]^M(v_{1I}, v_{1S}) \right\}_{\{\text{HP},\text{SP}(\zeta),\text{SP}(\zeta_1),\text{SP}(\zeta_2)\}}$$

$$\left\{ S(\zeta_2, 0, h_2 \uplus h_3, e_{2S}, e_{2S}, \tfrac{1}{2}, (\Lambda_2, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M) \right\}$$

e_{2I}

$$\left\{ v_{2I}.\ \exists v_{2S}.\ S(\zeta_2, 0, h_2 \uplus h_3, e_{2S}, v_{2S}, \tfrac{1}{2}, (\Lambda_2, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M) * [\![\tau_2]\!]^M(v_{2I}, v_{2S}) \right\}_{\{\text{HP},\text{SP}(\zeta),\text{SP}(\zeta_1),\text{SP}(\zeta_2)\}}$$

$$\left\{ \begin{array}{l} v.\ v = (v_{1I}, v_{2I}) * \exists v_{1S}, v_{2S}.\ S(\zeta_1, 0, h_1 \uplus h_3, e_{1S}, v_{1S}, \tfrac{1}{2}, (\Lambda_1, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_1, M) * \\ S(\zeta_2, 0, h_2 \uplus h_3, e_{2S}, v_{2S}, \tfrac{1}{2}, (\Lambda_2, \Lambda_3), \tfrac{\mathbf{1}}{\mathbf{2}}, \varepsilon_2, M) * j \xRightarrow{\zeta}_S (e_1, e_2) * [\text{SR}]^{\pi}_{\zeta} * \\ P_f(\Lambda_3, M, \zeta, \zeta_1, \zeta_2, \varepsilon_1, \varepsilon_2, h_1, h_2, h_3, h_{3R}) * [\![\tau_1]\!]^M(v_{1I}, v_{1S}) * [\![\tau_2]\!]^M(v_{2I}, v_{2S}) \end{array} \right\}_{\{\text{HP},\text{SP}(\zeta),\text{SP}(\zeta_1),\text{SP}(\zeta_2)\}}$$

`// Lemma ??`

$$\left\{ \begin{array}{l} v.\ v = (v_{1I}, v_{2I}) * \exists v_{1S}, v_{2S}.\ j \xRightarrow{\zeta}_S (v_{1S}, v_{2S}) * [\text{SR}]^{\pi}_{\zeta} * [\![\tau_1]\!]^M(v_{1I}, v_{1S}) * \\ [\![\tau_2]\!]^M(v_{2I}, v_{2S}) * P_{reg}(\Lambda_1, \mathbf{1}, \varepsilon_1, M, \zeta) * P_{reg}(\Lambda_2, \mathbf{1}, \varepsilon_2, M, \zeta) * P_{reg}(\Lambda_3, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{HP},\text{SP}(\zeta)\}}$$

$$\left\{ \begin{array}{l} v.\ v = (v_{1I}, v_{2I}) * \exists v_{1S}, v_{2S}.\ j \xRightarrow{\zeta}_S (v_{1S}, v_{2S}) * [\![\tau_1 \times \tau_2]\!]^M((v_{1I}, v_{2I}), (v_{2I}, v_{2S})) * \\ [\text{SR}]^{\pi}_{\zeta} * P_{reg}(\Lambda, \mathbf{1}, \varepsilon_1 \cup \varepsilon_2, M, \zeta) \end{array} \right\}_{\{\text{HP},\text{SP}(\zeta)\}}$$

$\square$

6.3.2 Commuting

Assuming

1. $\Lambda_3 \mid \Lambda_1 \mid \Gamma \vdash e_1 : \tau_1, \varepsilon_1$
2. $\Lambda_3 \mid \Lambda_2 \mid \Gamma \vdash e_2 : \tau_2, \varepsilon_2$
3. $\mathsf{als}\ \varepsilon_1 \subseteq \Lambda_1$, $\mathsf{als}\ \varepsilon_2 \subseteq \Lambda_2$, $\mathsf{wrs}\ \varepsilon_1 \subseteq \Lambda_1$, $\mathsf{wrs}\ \varepsilon_2 \subseteq \Lambda_2$, $\mathsf{rds}\ \varepsilon_1 \subseteq \Lambda_1 \cup \Lambda_3$ and $\mathsf{rds}\ \varepsilon_2 \subseteq \Lambda_2 \cup \Lambda_3$

then

$$\cdot \mid \Lambda_1, \Lambda_2, \Lambda_3 \mid \Gamma \vdash (e_1, e_2) \preceq \textbf{let}\ x = e_2\ \textbf{in}\ (e_1, x) : \tau_1 \times \tau_2, \varepsilon_1 \cup \varepsilon_2$$

Proof. By parallelization, we have

$$\cdot \mid \Lambda_1, \Lambda_2, \Lambda_3 \mid \Gamma \vdash (e_1, e_2) \preceq e_1 \,||\, e_2 : \tau_1 \times \tau_2, \varepsilon_1 \cup \varepsilon_2$$

and by switching the parallel composition

$$\cdot \mid \Lambda_1, \Lambda_2, \Lambda_3 \mid \Gamma \vdash e_1 \,||\, e_2 \preceq \textsf{\textbf{let}}\ x = e_2 \,||\, e_1\ \textsf{\textbf{in}}\ (\pi_2(x), \pi_1(x)) : \tau_1 \times \tau_2, \varepsilon_1 \cup \varepsilon_2$$

now using parallel composition in the opposite direction

$$\cdot \mid \Lambda_1, \Lambda_2, \Lambda_3 \mid \Gamma \vdash \textsf{\textbf{let}}\ x = e_2 \,||\, e_1\ \textsf{\textbf{in}}\ (\pi_2(x), \pi_1(x)) \preceq \textsf{\textbf{let}}\ x = (e_2, e_1)\ \textsf{\textbf{in}}\ (\pi_2(x), \pi_1(x)) : \tau_1 \times \tau_2, \varepsilon_1 \cup \varepsilon_2$$

for which the post-condition easily follows

$$\cdot \mid \Lambda_1, \Lambda_2, \Lambda_3 \mid \Gamma \vdash \textsf{\textbf{let}}\ x = (e_2, e_1)\ \textsf{\textbf{in}}\ (\pi_2(x), \pi_1(x)) \preceq \textsf{\textbf{let}}\ x = e_2\ \textsf{\textbf{in}}\ (e_1, x) : \tau_1 \times \tau_2, \varepsilon_1 \cup \varepsilon_2$$

□

6.4 Example: Stacks

Consider the following two stack-modules:

Stack$_1$ has a single reference to a pure functional list, where the **cas** operation is used to update the entire list on push and pop.

$$
\begin{aligned}
\mathit{create}_1() &= \textbf{let } h = \textbf{new inj}_1\ () \textbf{ in } (\mathit{push}_1, \mathit{pop}_1)\\
\mathit{push}_1(n) &= \textbf{let } v = !h \textbf{ in}\\
&\qquad \textbf{let } v' = \textbf{inj}_2\ (n, v) \textbf{ in if } \textbf{CAS}(h, v, v') \textbf{ then } () \textbf{ else } \mathit{push}_1(n)\\
\mathit{pop}_1() &= \textbf{let } v = !h \textbf{ in}\\
&\qquad\quad \textbf{case}(v, \textbf{inj}_1\ () \Rightarrow \textbf{inj}_1\ (),\\
&\qquad\qquad\quad \textbf{inj}_2\ (n, v') \Rightarrow \textbf{if } \textbf{CAS}(h, v, v') \textbf{ then inj}_2\ n \textbf{ else } \mathit{pop}_1())
\end{aligned}
$$

Stack$_2$ uses a header-reference to a mutable linked list, where the **cas** operation is used to move the header back on pop and forth on push.

$$
\begin{aligned}
\mathit{create}_2() &= \textbf{let } t = \textbf{new inj}_1\ () \textbf{ in let } h = \textbf{new } t \textbf{ in } (\mathit{push}_2, \mathit{pop}_2)\\
\mathit{push}_2(n) &= \textbf{let } v = !h \textbf{ in}\\
&\qquad \textbf{let } v' = \textbf{new inj}_2\ (n, v) \textbf{ in if } \textbf{CAS}(h, v, v') \textbf{ then } () \textbf{ else } \mathit{push}_2(n)\\
\mathit{pop}_2() &= \textbf{let } v = !h \textbf{ in}\\
&\qquad \textbf{let } v' = !v \textbf{ in}\\
&\qquad\quad \textbf{case}(v', \textbf{inj}_1\ () \Rightarrow \textbf{inj}_1\ (),\\
&\qquad\qquad\quad \textbf{inj}_2\ (n, v'') \Rightarrow \textbf{if } \textbf{CAS}(h, v, v'') \textbf{ then inj}_2\ n \textbf{ else } \mathit{pop}_2())
\end{aligned}
$$

The physical footprint of the two modules differ, thus to show contextual equivalence we are required to establish an invariant that relates one location having a pure functional list to a collection of mutable heap-cells organized as a linked list. Such equivalences was not possible to show in 'A Concurrent Logical Relation' due to their more restrictive worlds allowing invariants to only relate values at two locations for a semantic type.

Theorem 10 (*Stack*$_1$ and *Stack*$_2$ are contextually equivalent)**.**

$$\forall \tau.\ \rho \mid \cdot \mid \cdot \vdash \mathit{create}_1 \cong_{ctx} \mathit{create}_2 : \mathbf{1} \to^{\rho|\cdot}_{al_\rho} (\tau \to^{\rho|\cdot}_{wr_\rho, rd_\rho, al_\rho} \mathbf{1} \times \mathbf{1} \to^{\rho|\cdot}_{wr_\rho, rd_\rho} \mathbf{1} + \tau), \emptyset$$

Proof. Contextual equivalence is defined as contextual approximation in both directions, thus we are to show:

$$\rho \mid \cdot \mid \cdot \vdash \mathit{create}_1 \leq_{ctx} \mathit{create}_2 : \mathbf{1} \to^{\rho|\cdot}_{al_\rho} (\tau \to^{\rho|\cdot}_{wr_\rho, rd_\rho, al_\rho} \mathbf{1} \times \mathbf{1} \to^{\rho|\cdot}_{wr_\rho, rd_\rho} \mathbf{1} + \tau), \emptyset \tag{5}$$

$$\rho \mid \cdot \mid \cdot \vdash \mathit{create}_2 \leq_{ctx} \mathit{create}_1 : \mathbf{1} \to^{\rho|\cdot}_{al_\rho} (\tau \to^{\rho|\cdot}_{wr_\rho, rd_\rho, al_\rho} \mathbf{1} \times \mathbf{1} \to^{\rho|\cdot}_{wr_\rho, rd_\rho} \mathbf{1} + \tau), \emptyset \tag{6}$$

(1) follows from Lemma **??** and soundness and (2) follows from Lemma **??** and soundness. □

Lemma 96 (*Stack*$_1$ logically refines *Stack*$_2$)**.**

$$\forall \tau.\ \rho \mid \cdot \mid \cdot \vdash \mathit{create}_1 \preceq \mathit{create}_2 : \mathbf{1} \to^{\rho|\cdot}_{al_\rho} (\tau \to^{\rho|\cdot}_{wr_\rho, rd_\rho, al_\rho} \mathbf{1} \times \mathbf{1} \to^{\rho|\cdot}_{wr_\rho, rd_\rho} \mathbf{1} + \tau), \emptyset$$

Proof. Proof follows directly from Lemma **??** and Lemma **??** □

Lemma 97 (*Stack*$_2$ logically refines *Stack*$_1$)**.**

$$\forall \tau.\ \rho \mid \cdot \mid \cdot \vdash \mathit{create}_2 \preceq \mathit{create}_1 : \mathbf{1} \to^{\rho|\cdot}_{al_\rho} (\tau \to^{\rho|\cdot}_{wr_\rho, rd_\rho, al_\rho} \mathbf{1} \times \mathbf{1} \to^{\rho|\cdot}_{wr_\rho, rd_\rho} \mathbf{1} + \tau), \emptyset$$

Proof. This direction is straight-forward, since any successful update from **cas** forces the shape of the linked list on the implementation side and we are required to make only a single heap update on the specification side for $Stack_1$: □

We choose the following relation to show equality:

$$\textsc{StackRel}(h, r, \phi) \triangleq \exists l, v, n.\ h_I \overset{1}{\hookrightarrow}_{I,r} v * h_S \overset{1}{\hookrightarrow}_{S,r} n * vals(l, v, \phi) * linked(l, n, r, \phi)$$
$$\textsc{StackInv}(h, r, \phi) \triangleq \exists \iota.\ \boxed{\textsc{StackRel}(h, r, \phi)}^{\textsc{Si}(\iota)}$$

where

$$vals(\mathsf{nil}, v, \phi) \triangleq v = \textbf{inj}_1\ ()$$
$$vals(x :: xs, v, \phi) \triangleq \exists v'.\ v = \textbf{inj}_2\ (x_I, v') * \phi(x) * vals(xs, v', \phi)$$

and

$$linked(\mathsf{nil}, n, r, \phi) \triangleq \exists v.\ n \overset{1}{\hookrightarrow}_{S,r} v * v = \textbf{inj}_1\ ()$$
$$linked(x :: xs, n, r, \phi) \triangleq \exists v, n'.\ n \overset{1}{\hookrightarrow}_{S,r} v * v = \textbf{inj}_2\ (x_S, n') * \phi(x) * linked(xs, n', r, \phi)$$

and the function $\textsc{Si}(\iota)$ ensures that the invariant identifier is disjoint from $\textsc{Hp}$,$\textsc{Sp}(\zeta)$ and $\textsc{Rg}(r)$ for all ζ and r.

Lemma 98 (Can create $\textsc{StackInv}$)**.**

$$\begin{array}{ll} & \forall h_I, h_S, l_S, r, \phi. \\ & \quad h_I \overset{1}{\hookrightarrow}_{I,r} \textbf{\textit{inj}}_1\ () * l_S \overset{1}{\hookrightarrow}_{S,r} \textbf{\textit{inj}}_1\ () * h_S \overset{1}{\hookrightarrow}_{S,r} l_S \\ \Rrightarrow^{\textsc{Si}(\iota)} & \quad \textsc{StackInv}((h_I, h_S), r, \phi) \end{array}$$

Proof. Intro h_I, h_S, l_S, r and ϕ.

$$\begin{array}{ll} & h_I \overset{1}{\hookrightarrow}_{I,r} \textbf{inj}_1\ () * l_S \overset{1}{\hookrightarrow}_{S,r} \textbf{inj}_1\ () * h_S \overset{1}{\hookrightarrow}_{S,r} l_S \\ \Rrightarrow & \exists v_I.\ v_I = \textbf{inj}_1\ () * h_I \overset{1}{\hookrightarrow}_{I,r} v_I * l_S \overset{1}{\hookrightarrow}_{S,r} \textbf{inj}_1\ () * h_S \overset{1}{\hookrightarrow}_{S,r} l_S * vals(\mathsf{nil}, v_I, \phi) \\ \Rrightarrow & \exists v_I, v_S.\ h_I \overset{1}{\hookrightarrow}_{I,r} v_I * h_S \overset{1}{\hookrightarrow}_{S,r} v_S * vals(\mathsf{nil}, v_I, \phi) * linked(\mathsf{nil}, v_S, \phi) \\ \Rrightarrow & \textsc{StackRel}((h_I, h_S), r, \phi) \\ \Rrightarrow^{\textsc{Si}(\iota)} & \exists \iota.\ \boxed{\textsc{StackRel}((h_I, h_S), r, \phi)}^{\textsc{Si}(\iota)} \\ \Rrightarrow & \textsc{StackInv}((h_I, h_S), r, \phi) \end{array}$$

□

Lemma 99. *$Stack_1$-push refines $Stack_2$-push*

$$\begin{array}{ll} & \forall \rho, M, h, n, m.\ V[\![\tau]\!]^M(n, m) \\ \Rightarrow & \textsc{StackInv}(h, M(\rho)) \vdash E^{\rho;\cdot}_{\{al_\rho, wr_\rho, rd_\rho\};M}(V[\![\mathbf{1}]\!]^M)(push_1(n), push_2(m)) \end{array}$$

Proof. We define the following short-hands:

$$e_{1I} \triangleq \textsf{let } v = !h_I \textsf{ in let } v' = \textsf{inj}_2\ (n, v) \textsf{ in if } \textsf{CAS}(h, v, v') \textsf{ then } () \textsf{ else } push_1(n)$$
$$e_{1S} \triangleq \textsf{let } v = !h_I \textsf{ in let } v' = \textsf{new inj}_2\ (m, v) \textsf{ in if } \textsf{CAS}(h, v, v') \textsf{ then } () \textsf{ else } push_2(m)$$
$$K_{1I} \triangleq \textsf{let } v = [] \textsf{ in let } v' = \textsf{inj}_2\ (n, v) \textsf{ in if } \textsf{CAS}(h, v, v') \textsf{ then } () \textsf{ else } push_1(n)$$
$$K_{2I} \triangleq \textsf{let } v' = [] \textsf{ in if } \textsf{CAS}(h, v_I^1, v') \textsf{ then } () \textsf{ else } push_1(n)$$
$$K_{3I} \triangleq \textsf{if } [] \textsf{ then } () \textsf{ else } push_1(n)$$
$$K_{1S} \triangleq \textsf{let } v = [] \textsf{ in let } v' = \textsf{new inj}_2\ (n, v) \textsf{ in if } \textsf{CAS}(h, v, v') \textsf{ then } () \textsf{ else } push_2(m)$$
$$K_{2S} \triangleq \textsf{let } v' = [] \textsf{ in if } \textsf{CAS}(h, v_S^1, v') \textsf{ then } () \textsf{ else } push_2(m)$$
$$K_{3S} \triangleq \textsf{if } [] \textsf{ then } () \textsf{ else } push_2(m)$$

and the following predicate to track the stacks:

$$\textsc{StackRel}(h, l, l', v, n, r, \phi) \triangleq h_I \overset{1}{\hookrightarrow}_{I,r} v * h_S \overset{1}{\hookrightarrow}_{S,r} n * vals(l, v, \phi) * linked(l', n, r, \phi)$$

and continue by Löb-induction.

Context: $g, j, \pi', e_0, h_0, \zeta, M, h, n, m$
Context: $\boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}, \textsc{StackInv}(h, M(\rho), V[\![\tau]\!]^M), V[\![\tau]\!]^M(n, m)$
Context: $\triangleright\left\{j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta)\right\}$

$push(n)$

$\left\{v_I^1.\ \exists v_S^1.\ j \overset{\zeta}{\Rrightarrow}_S v_S^1 * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta) * V[\![\mathbf{1}]\!]^M(v_I^1, v_S^1)\right\}_\top$

$\left\{j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta)\right\}_\top$

`// Let` $\pi = g(\rho)$, $r = M(\rho)$ `and` $R = \{\texttt{Hp}, \texttt{Sp}(\zeta), \texttt{Rg}(r)\}$

$\left\{j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}}\right\}_\top$

Bind on $K_{1I}[!h_I]$

`// Unfolding` $\textsc{StackInv}(h, r, V[\![\tau]\!]^M)$

$\left\{\begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \exists \iota.\ \boxed{\textsc{StackRel}(h, r, V[\![\tau]\!]^M)}^{\textsc{Si}(\iota)} \end{array}\right\}_\top$

Open $R, \textsc{Si}(\iota)$

$\left\{\begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \triangleright\textsc{Reg}(r) * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \triangleright\textsc{Heap} * \triangleright\textsc{Spec}(h_0, e_0, \zeta) * \triangleright\textsc{StackRel}(h, r, V[\![\tau]\!]^M) \end{array}\right\}_{\top \setminus R, \textsc{Si}(\iota)}$

$!h_I$

`// Follows from Lemma ??`

$\left\{\begin{array}{l} v_I^1.\ \exists l.\ vals(l, v_I^1, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \\ \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * \textsc{StackRel}(h, r, V[\![\tau]\!]^M) \end{array}\right\}_{\top \setminus R, \textsc{Si}(\iota)}$

$\left\{\begin{array}{l} v_I^1.\ \exists l.\ vals(l, v_I^1, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \\ \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h, r, V[\![\tau]\!]^M) \end{array}\right\}_\top$

Bind on $K_2[\textbf{inj}_2\ (n, v_I^1)]$

$$\forall v_I^1.\ \left\{\begin{array}{l}\exists l.\ \mathit{vals}(l, v_I^1, V[\![\tau]\!]^M) * j \stackrel{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \\ \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h, r, V[\![\tau]\!]^M)\end{array}\right\}_\top$$

$$\left\{\begin{array}{l}\exists l.\ \mathit{vals}(l, v_I^1, V[\![\tau]\!]^M) * j \stackrel{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \\ \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h, r, V[\![\tau]\!]^M)\end{array}\right\}_\top$$

$\textbf{inj}_2\ (n, v_I^1)$

$$\left\{\begin{array}{l}v_I^2.\ v_I^2 = \textbf{inj}_2\ (n, v_I^1) * \exists l.\ \mathit{vals}(l, v_I^1, V[\![\tau]\!]^M) * j \stackrel{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * \\ [\textsc{Al}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h, r, V[\![\tau]\!]^M)\end{array}\right\}_\top$$

$$\left\{\begin{array}{l}v_I^2.\ \exists l.\ \mathit{vals}(l, v_I^1, V[\![\tau]\!]^M) * \mathit{vals}((n, m) :: l, v_I^2, V[\![\tau]\!]^M) * j \stackrel{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * \\ [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h, r, V[\![\tau]\!]^M)\end{array}\right\}_\top$$

Bind on $K_3[\textbf{CAS}(h, v_I^1, v_I^2)]$

$$\forall v_I^2.\ \left\{\begin{array}{l}\exists l.\ \mathit{vals}(l, v_I^1, V[\![\tau]\!]^M) * \mathit{vals}((n, m) :: l, v_I^2, V[\![\tau]\!]^M) * j \stackrel{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * \\ [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h, r, V[\![\tau]\!]^M)\end{array}\right\}_\top$$

$$\left\{\begin{array}{l}\exists l, \iota.\ \mathit{vals}(l, v_I^1, V[\![\tau]\!]^M) * \mathit{vals}((n, m) :: l, v_I^2, V[\![\tau]\!]^M) * j \stackrel{\zeta}{\Rrightarrow}_S e_{1S} * \\ [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ \boxed{\textsc{StackRel}(h, r, V[\![\tau]\!]^M)}^{\textsc{Si}(\iota)}\end{array}\right\}_\top$$

Open $R, \textsc{Si}(\iota)$

$$\left\{\begin{array}{l}\exists l, l', v, n'.\ \mathit{vals}(l, v_I^1, V[\![\tau]\!]^M) * \mathit{vals}((n, m) :: l, v_I^2, V[\![\tau]\!]^M) * \\ j \stackrel{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \triangleright\textsc{Reg}(r) * \triangleright\textsc{Heap} * \\ \triangleright\textsc{Spec}(h_0, e_0, \zeta) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackRel}(h, l', l', v, n', r, V[\![\tau]\!]^M) * \\ ((v = v_I^1 \wedge l = l') \vee (v \neq v_I^1 \wedge l \neq l'))\end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$$

$\textbf{CAS}(h, v_I^1, v_I^2)$

```
// Follows from CAS (shown below)
```

$$\left\{\begin{array}{l}v_I^3.\ \exists l, l', v, n'.\ j \stackrel{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \\ \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * \\ ((v_I^3 = \textbf{true} * \textsc{StackRel}(h, (n, m) :: l, l, v_I^2, n', r, V[\![\tau]\!]^M)) \vee \\ (v_I^3 = \textbf{false} * \textsc{StackRel}(h, l, l, v, n', r, V[\![\tau]\!]^M)))\end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$$

```
// Follows from simulating on the right hand side (shown
below)
```

$$\left\{\begin{array}{l}v_I^3.\ \exists l, v, n', v_S^2, v_S^3.\ [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \textsc{Reg}(r) * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * ((v_I^3 = \textbf{true} * v_S^3 = \textbf{true} * \\ \textsc{StackRel}(h, (n, m) :: l, (n, m) :: l, v_I^2, v_S^2, r, V[\![\tau]\!]^M) * \\ j \stackrel{\zeta}{\Rrightarrow}_S K_{3S}[v_S^3]) \vee (v_I^3 = \textbf{false} * v_S^3 = \textbf{false} * \\ \textsc{StackRel}(h, l', l', v, n', r, V[\![\tau]\!]^M) * j \stackrel{\zeta}{\Rrightarrow}_S e_{1S}))\end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$$

$$\left\{\begin{array}{l}v_I^3.\ \exists v_S^3.\ [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ \textsc{StackInv}(h, r, V[\![\tau]\!]^M) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * ((v_I^3 = \textbf{true} * v_S^3 = \textbf{false} * \\ j \stackrel{\zeta}{\Rrightarrow}_S K_{3S}[v_S^3]) \vee (v_I^3 \neq \textbf{true} * v_S^3 = \textbf{false} * j \stackrel{\zeta}{\Rrightarrow}_S e_{1S}))\end{array}\right\}_\top$$

if v_I^3 **then**

$$\left\{\begin{array}{l}[\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * j \overset{\zeta}{\Rrightarrow}_S K_{3S}[()]\end{array}\right\}_\top$$

$()$

$$\left\{\begin{array}{l}v_I^4.\ \exists v_S^3.\ j \overset{\zeta}{\Rrightarrow}_S v_S^3 * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta) * \\ V[\![\mathbf{1}]\!]^M(v_I^4, v_S^3)\end{array}\right\}_\top$$

else

$$\left\{j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta)\right\}_\top$$

$push(n)$

```
// Follows from IH
```

$$\left\{\begin{array}{l}v_I^4.\ \exists v_S^3.\ j \overset{\zeta}{\Rrightarrow}_S v_S^3 * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta) * \\ V[\![\mathbf{1}]\!]^M(v_I^4, v_S^3)\end{array}\right\}_\top$$

We have to show we can perform the **cas** (open invariants are $R, \textsc{Si}(\iota)$):

$$\left\{\begin{array}{l}\exists l, l', v, n'.\ vals(l, v_I^1, V[\![\tau]\!]^M) * vals((n,m) :: l, v_I^2, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * \\ [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \triangleright\textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackRel}(h, l', l', v, n', r, V[\![\tau]\!]^M) * \\ \triangleright\textsc{Heap} * \triangleright\textsc{Spec}(h_0, e_0, \zeta) * ((v = v_I^1 \wedge l = l') \vee (v \neq v_I^1 \wedge l \neq l'))\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists l, l', v, n'.\ vals(l, v_I^1, V[\![\tau]\!]^M) * vals((n,m) :: l, v_I^2, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * \\ [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackRel}(h, l', l', v, n', r, V[\![\tau]\!]^M) * \\ \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * ((v = v_I^1 \wedge l = l') \vee (v \neq v_I^1 \wedge l \neq l'))\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists l, l', v, n'.\ vals(l, v_I^1, V[\![\tau]\!]^M) * vals((n,m) :: l, v_I^2, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * \\ [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \exists t.\ locs((t_I[h_I \mapsto v], t_S[h_S \mapsto n']), r) * toks(1,1,r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ \textsc{StackRel}(h, l, l, v, n', r, V[\![\tau]\!]^M) * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * ((v = v_I^1 \wedge l = l') \vee (v \neq v_I^1 \wedge l \neq l'))\end{array}\right\}$$

Frame

$\{\textsc{Heap} * h_I \mapsto_I v\}$

$\mathbf{CAS}(h_I, v_I^1, v_I^2)$

$\{v_I^3.\ \textsc{Heap} * ((v_I^3 = \textbf{true} * h_I \mapsto_I v_I^2) \vee (v_I^3 = \textbf{false} * h_I \mapsto_I v))\}$

// Updating $h \overset{1}{\hookrightarrow}_{I,r} v$ follows from having the authorative element and fragment

$$\left\{\begin{array}{l}v_I^3.\ \exists l, l', v, n'.\ j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * [\textsc{Al}]_r^\pi * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * \textsc{Reg}(r) * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * ((v_I^3 = \textbf{true} * \textsc{StackRel}(h, (n,m) :: l, l, v_I^2, n', r, V[\![\tau]\!]^M)) \vee \\ (v_I^3 = \textbf{false} * \textsc{StackRel}(h, l', l', v, n', r, V[\![\tau]\!]^M)))\end{array}\right\}$$

We also have to show that we could simulate on the right hand side, which consists of three parts - (1) reading the head pointer, (2) allocating a new location for the new node and (3) updating the head pointer:

$$\exists l, n'.\ j \xRightarrow{\zeta}_S e_{1S} * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Spec}(h_0, e_0, \zeta) *$$
$$\textsc{StackRel}(h, (n, m) :: l, l, v_I^2, n', r, V[\![\tau]\!]^M)$$

$$\Rrightarrow \quad \exists l, n'.\ j \xRightarrow{\zeta}_S K_{1S}[!h_S] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Spec}(h_0, e_0, \zeta) *$$
$$\textsc{StackRel}(h, (n, m) :: l, l, v_I^2, n', r, V[\![\tau]\!]^M)$$

`// Follows from Lemma ??`

$$\Rrightarrow \quad \exists l, n', v_S^1.\ j \xRightarrow{\zeta}_S K_{1S}[v_S^1] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Spec}(h_0, e_0, \zeta) *$$
$$\textsc{StackRel}(h, (n, m) :: l, l, v_I^2, v_S^1, r, V[\![\tau]\!]^M)$$

$$\Rrightarrow \quad \exists l, n', v_S^1.\ j \xRightarrow{\zeta}_S K_{2S}[\textbf{new inj}_2\ (n, v_S^1)] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) *$$
$$[\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Spec}(h_0, e_0, \zeta) * \textsc{StackRel}(h, (n, m) :: l, l, v_I^2, v_S^1, r, V[\![\tau]\!]^M)$$

`// Follows from Lemma ??`

$$\Rrightarrow \quad \exists l, n', v_S^1, v_S^2.\ j \xRightarrow{\zeta}_S K_{2S}[v_S^2] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} *$$
$$\textsc{Spec}(h_0, e_0, \zeta) * \textsc{StackRel}(h, (n, m) :: l, l, v_I^2, v_S^1, r, V[\![\tau]\!]^M) * v_S^2 \mapsto_S^{\zeta} \textbf{inj}_2\ (n, v_S^1)$$

`// Follows from Lemma ??`

$$\Rrightarrow \quad \exists l, n', v_S^1, v_S^2.\ j \xRightarrow{\zeta}_S K_{2S}[v_S^2] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} *$$
$$\textsc{Spec}(h_0, e_0, \zeta) * \textsc{StackRel}(h, (n, m) :: l, l, v_I^2, v_S^1, r, V[\![\tau]\!]^M) * v_S^2 \overset{1}{\hookrightarrow}_{S,r} \textbf{inj}_2\ (n, v_S^1)$$

$$\Rrightarrow \quad \exists l, n', v_S^1, v_S^2.\ j \xRightarrow{\zeta}_S K_{3S}[\textbf{CAS}(h_S, v_S^1, v_S^2)] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * \textsc{Spec}(h_0, e_0, \zeta) *$$
$$[\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackRel}(h, (n, m) :: l, l, v_I^2, v_S^1, r, V[\![\tau]\!]^M) * v_S^2 \overset{1}{\hookrightarrow}_{S,r} \textbf{inj}_2\ (n, v_S^1)$$

`// Follows from Lemma ??, Lemma ??`

$$\Rrightarrow \quad \exists l, n', v_S^1, v_S^2, v_S^3.\ v_S^3 = \textbf{true} * j \xRightarrow{\zeta}_S K_{3S}[v_S^3] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * \textsc{Spec}(h_0, e_0, \zeta) *$$
$$[\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^2 * vals((n, m) :: l, v_I^2, \phi, V[\![\tau]\!]^M) *$$
$$linked(l, v_S^1, r, V[\![\tau]\!]^M) * v_S^2 \overset{1}{\hookrightarrow}_{S,r} \textbf{inj}_2\ (n, v_S^1)$$

`// From` $V[\![\tau]\!]^M(n, m)$

$$\Rrightarrow \quad \exists l, n', v_S^1, v_S^2, v_S^3.\ v_S^3 = \textbf{true} * j \xRightarrow{\zeta}_S K_{3S}[v_S^3] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * \textsc{Spec}(h_0, e_0, \zeta) *$$
$$[\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^2 * vals((n, m) :: l, v_I^2, \phi, V[\![\tau]\!]^M) *$$
$$linked((n, m) :: l, v_S^2, r, V[\![\tau]\!]^M)$$

$$\Rrightarrow \quad \exists l, n', v_S^1, v_S^2, v_S^3.\ v_S^3 = \textbf{true} * j \xRightarrow{\zeta}_S K_{3S}[v_S^3] * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \textsc{Reg}(r) * \textsc{Spec}(h_0, e_0, \zeta) *$$
$$[\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackRel}(h, (n, m) :: l, (n, m) :: l, v_I^2, v_S^2, r, V[\![\tau]\!]^M)$$

□

Lemma 100. *$Stack_1$-pop refines $Stack_2$-pop*

$$\forall \rho, M, h.$$
$$\Rightarrow \quad \textsc{StackInv}(h, r, V[\![\tau]\!]^M) \vdash E^{\rho;\cdot}_{wr_\rho, rd_\rho; M}(V[\![\mathbf{1} + \tau]\!]^M)(pop_1(), pop_2())$$

Proof. We define the following short-hands:

$$\begin{aligned}
e_{1I} &\triangleq \textsf{let } v = !h_I \textsf{ in} \\
&\qquad \textsf{case}(v, \textsf{inj}_1\ () \Rightarrow \textsf{inj}_1\ (), \\
&\qquad\qquad\qquad \textsf{inj}_2\ (n_I, v') \Rightarrow \textsf{if } \textsf{CAS}(h_I, v, v') \textsf{ then } \textsf{inj}_2\ n_I \textsf{ else } pop_1()) \\
e_{1S} &\triangleq \textsf{let } v = !h_S \textsf{ in} \\
&\quad \textsf{let } v' = !v \textsf{ in} \\
&\qquad \textsf{case}(v', \textsf{inj}_1\ () \Rightarrow \textsf{inj}_1\ (), \\
&\qquad\qquad\qquad \textsf{inj}_2\ (n_S, v'') \Rightarrow \textsf{if } \textsf{CAS}(h_S, v, v'') \textsf{ then } \textsf{inj}_2\ n_S \textsf{ else } pop_2()) \\
K_{1I} &\triangleq \textsf{let } v = [] \textsf{ in } \textsf{case}(v, \textsf{inj}_1\ () \Rightarrow \textsf{inj}_1\ ()), \\
&\qquad\qquad\qquad\qquad\qquad \textsf{inj}_2\ (n_I, v') \Rightarrow \textsf{if } \textsf{CAS}(h_I, v, v') \textsf{ then } \textsf{inj}_2\ n_I \textsf{ else } pop_1() \\
K_{2I} &\triangleq \textsf{if } [] \textsf{ then } \textsf{inj}_2\ n_I \textsf{ else } pop_1() \\
K_{1S} &\triangleq \textsf{let } v = [] \textsf{ in} \\
&\quad \textsf{let } v' = !v \textsf{ in} \\
&\qquad \textsf{case}(v', \textsf{inj}_1\ () \Rightarrow \textsf{inj}_1\ (), \\
&\qquad\qquad\qquad \textsf{inj}_2\ (n_S, v'') \Rightarrow \textsf{if } \textsf{CAS}(h_S, v, v'') \textsf{ then } \textsf{inj}_2\ n_S \textsf{ else } pop_2()) \\
K_{2S} &\triangleq \textsf{let } v' = [] \textsf{ in} \\
&\qquad \textsf{case}(v', \textsf{inj}_1\ () \Rightarrow \textsf{inj}_1\ (), \\
&\qquad\qquad\qquad \textsf{inj}_2\ (n_S, v'') \Rightarrow \textsf{if } \textsf{CAS}(h_S, v_S^1, v'') \textsf{ then } \textsf{inj}_2\ n_S \textsf{ else } pop_2()) \\
K_{3S} &\triangleq \textsf{if } [] \textsf{ then } \textsf{inj}_2\ n_S \textsf{ else } pop_2()
\end{aligned}$$

Context: $g, j, \pi', e_0, h_0, \zeta, M, h$

Context: $\boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}, \textsc{StackInv}(h, r, V[\![\tau]\!]^M)$

Context: $\triangleright\left\{j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta)\right\}$

$$pop()$$

$$\left\{v_I^1.\ \exists v_S^1.\ j \overset{\zeta}{\Rrightarrow}_S v_S^1 * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta) * V[\![\mathbf{1} + \tau]\!]^M(v_I^1, v_S^1)\right\}_\top$$

$$\left\{j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta)\right\}_\top$$

`// Let` $\pi = g(\rho)$, $r = M(\rho)$ `and` $R = \{\texttt{Hp}, \texttt{Sp}(\zeta), \texttt{Rg}(r)\}$

$$\left\{j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}}\right\}_\top$$

Bind on $K_{1I}[!h_I]$

`// Unfolding` $\textsc{StackInv}(h, r, V[\![\tau]\!]^M)$

$$\left\{\begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \exists \iota.\ \boxed{\textsc{StackRel}(h, r, V[\![\tau]\!]^M)}^{\textsc{Si}(\iota)} \end{array}\right\}_\top$$

Open $R, \textsc{Si}(\iota)$

$$\left\{\begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * \triangleright\textsc{Reg}(r) * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \triangleright\textsc{Heap} * \triangleright\textsc{Spec}(h_0, e_0, \zeta) * \triangleright\textsc{StackRel}(h, r, V[\![\tau]\!]^M) \end{array}\right\}_{\top \setminus R, \textsc{Si}(\iota)}$$

$$!h_I$$

`// Follows from Lemma ??`

$$\left\{\begin{array}{l} v_I^1.\ \exists l.\ vals(l, v_I^1, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * \textsc{Reg}(r) * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * \textsc{StackRel}(h, r, V[\![\tau]\!]^M) \end{array}\right\}_{\top \setminus R, \textsc{Si}(\iota)}$$

`// Follows from simulation on the right hand side`

$$\left\{\begin{array}{l} v_I^1.\ \exists l.\ vals(l, v_I^1, V[\![\tau]\!]^M) * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * \textsc{Reg}(r) * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackRel}(h, r, V[\![\tau]\!]^M) * ((v_I^1 = \mathsf{inj}_1\ () * j \overset{\zeta}{\Rrightarrow}_S \mathsf{inj}_1\ ()) \vee \\ (\exists n_I, n_S, v_I^2.\ v_I^1 = \mathsf{inj}_2\ (n_I, v_I^2) * l = (n, m) :: l' * j \overset{\zeta}{\Rrightarrow}_S e_{1S})) \end{array}\right\}_{\top \setminus R, \textsc{Si}(\iota)}$$

$$\left\{\begin{array}{l} v_I^1.\ \exists l.\ vals(l, v_I^1, V[\![\tau]\!]^M) * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^\pi * [\textsc{Wr}]_r^\pi * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h, r, V[\![\tau]\!]^M) * ((v_I^1 = \mathsf{inj}_1\ () * j \overset{\zeta}{\Rrightarrow}_S \mathsf{inj}_1\ ()) \vee (\exists n_I, n_S, v_I^2. \\ v_I^1 = \mathsf{inj}_2\ (n_I, v_I^2) * l = (n, m) :: l' * j \overset{\zeta}{\Rrightarrow}_S e_{1S})) \end{array}\right\}_\top$$

$$\forall v_I^1.\ \left\{\begin{array}{l}\exists l.\ vals(l, v_I^1, V[\![\tau]\!]^M) * [\mathrm{SR}]_\zeta^{\pi'} * [\mathrm{RD}]_r^\pi * [\mathrm{WR}]_r^\pi * \boxed{\mathrm{REG}(r)}^{\mathrm{RG}(r)} * \\ [\mathrm{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \mathrm{STACKINV}(h, r, V[\![\tau]\!]^M) * ((v_I^1 = \mathbf{inj}_1\ () * j \overset{\zeta}{\Rightarrow}_S \mathbf{inj}_1\ ()) \vee \\ (\exists n_I, v_I^2.\ v_I^1 = \mathbf{inj}_2\ (n_I, v_I^2) * l = (n, m) :: l' * j \overset{\zeta}{\Rightarrow}_S e_{1S}))\end{array}\right\}_\top$$

$\mathbf{case}\ v_I^1$

$\mathbf{inj}_1\ ()\ \Rrightarrow$

$$\left\{\begin{array}{l}\exists l.\ vals(l, v_I^1, V[\![\tau]\!]^M) * [\mathrm{SR}]_\zeta^{\pi'} * [\mathrm{RD}]_r^\pi * [\mathrm{WR}]_r^\pi * \boxed{\mathrm{REG}(r)}^{\mathrm{RG}(r)} * \\ [\mathrm{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \mathrm{STACKINV}(h, r, V[\![\tau]\!]^M) * v_I^1 = \mathbf{inj}_1\ () * j \overset{\zeta}{\Rightarrow}_S \mathbf{inj}_1\ ()\end{array}\right\}_\top$$

$\mathbf{inj}_1\ ()$

$$\left\{\begin{array}{l}v_I^3.\ v_I^3 = \mathbf{inj}_1\ () * \exists l.\ vals(l, v_I^1, V[\![\tau]\!]^M) * [\mathrm{SR}]_\zeta^{\pi'} * [\mathrm{RD}]_r^\pi * [\mathrm{WR}]_r^\pi * \boxed{\mathrm{REG}(r)}^{\mathrm{RG}(r)} * \\ [\mathrm{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \mathrm{STACKINV}(h, r, V[\![\tau]\!]^M) * v_I^1 = \mathbf{inj}_1\ () * j \overset{\zeta}{\Rightarrow}_S \mathbf{inj}_1\ ()\end{array}\right\}_\top$$

$$\left\{\begin{array}{l}v_I^3.\ \exists v_S^3.\ j \overset{\zeta}{\Rightarrow}_S v_S^3 * [\mathrm{SR}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta) * \\ V[\![\mathbf{1} + \tau]\!]^M(v_I^3, v_S^3)\end{array}\right\}_\top$$

$\mathbf{inj}_2\ (n_I, v_I^2)\ \Rrightarrow$

$$\left\{\begin{array}{l}\exists l, l', n_S.\ vals(l, v_I^1, V[\![\tau]\!]^M) * [\mathrm{SR}]_\zeta^{\pi'} * [\mathrm{RD}]_r^\pi * [\mathrm{WR}]_r^\pi * \boxed{\mathrm{REG}(r)}^{\mathrm{RG}(r)} * \\ [\mathrm{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \mathrm{STACKINV}(h, r, V[\![\tau]\!]^M) * v_I^1 = \mathbf{inj}_2\ (n_I, v_I^2) * l = (n, m) :: l' * \\ j \overset{\zeta}{\Rightarrow}_S e_{1S}\end{array}\right\}_\top$$

Bind on $K_{2I}[\mathbf{CAS}(h_I, v_I^1, v_I^2)]$

$$\left\{\begin{array}{l}\exists l, l', n_S, \iota.\ vals(l, v_I^1, V[\![\tau]\!]^M) * [\mathrm{SR}]_\zeta^{\pi'} * [\mathrm{RD}]_r^\pi * [\mathrm{WR}]_r^\pi * \boxed{\mathrm{REG}(r)}^{\mathrm{RG}(r)} * \\ [\mathrm{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \boxed{\mathrm{STACKREL}(h, r, V[\![\tau]\!]^M)}^{\mathrm{SI}(\iota)} * \\ v_I^1 = \mathbf{inj}_2\ (n_I, v_I^2) * l = (n, m) :: l' * j \overset{\zeta}{\Rightarrow}_S e_{1S}\end{array}\right\}_\top$$

Open R, $\mathrm{SI}(\iota)$

$$\left\{\begin{array}{l}\exists l, l', n_S.\ vals(l, v_I^1, V[\![\tau]\!]^M) * [\mathrm{SR}]_\zeta^{\pi'} * [\mathrm{RD}]_r^\pi * [\mathrm{WR}]_r^\pi * \triangleright\mathrm{HEAP} * \\ \triangleright\mathrm{SPEC} * \triangleright\mathrm{REG}(\mathrm{RG}(r)) * [\mathrm{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * j \overset{\zeta}{\Rightarrow}_S e_{1S} * \\ \triangleright\mathrm{STACKREL}(h, r, V[\![\tau]\!]^M) * v_I^1 = \mathbf{inj}_2\ (n_I, v_I^2) * l = (n, m) :: l'\end{array}\right\}_{\top\setminus R, \mathrm{SI}(\iota)}$$

$\mathbf{CAS}(h_I, v_I^1, v_I^2)$

```
// Follows from performing cas
```

$$\left\{\begin{array}{l}v_I^3.\ \exists l, l', n_S.\ [\mathrm{SR}]_\zeta^{\pi'} * [\mathrm{RD}]_r^\pi * [\mathrm{WR}]_r^\pi * \mathrm{REG}(\mathrm{RG}(r)) * \\ [\mathrm{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * l = (n, m) :: l' * \mathrm{HEAP} * \mathrm{SPEC} * j \overset{\zeta}{\Rightarrow}_S e_{1S} * \\ ((v_I^3 = \mathbf{true} * \exists n'.\ \mathrm{STACKREL}(h, l', l, v_I^2, n', r, V[\![\tau]\!]^M)) \vee \\ (v_I^3 = \mathbf{false} * \mathrm{STACKREL}(h, r, V[\![\tau]\!]^M)))\end{array}\right\}_{\top\setminus R, \mathrm{SI}(\iota)}$$

```
// Follows from simulating on the right hand side (below)
```

$$\left\{\begin{array}{l}v_I^3.\ [\mathrm{SR}]_\zeta^{\pi'} * [\mathrm{RD}]_r^\pi * [\mathrm{WR}]_r^\pi * \mathrm{REG}(\mathrm{RG}(r)) * \\ [\mathrm{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \mathrm{HEAP} * \mathrm{SPEC} * ((v_I^3 = \mathbf{true} * \\ \mathrm{STACKREL}(h, r, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rightarrow}_S K_{3S}[\mathbf{true}] * V[\![\tau]\!]^M(n, m)) \vee \\ (v_I^3 = \mathbf{false} * \mathrm{STACKREL}(h, r, V[\![\tau]\!]^M * j \overset{\zeta}{\Rightarrow}_S e_{1S})))\end{array}\right\}_{\top\setminus R, \mathrm{SI}(\iota)}$$

$$\left\{\begin{array}{l}v_I^3.\ [\mathrm{SR}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta) * \mathrm{STACKINV}(h, r, V[\![\tau]\!]^M) * \\ ((v_I^3 = \mathbf{true} * j \overset{\zeta}{\Rightarrow}_S K_{3S}[\mathbf{true}] * V[\![\tau]\!]^M(n, m)) \vee \\ (v_I^3 = \mathbf{false} * j \overset{\zeta}{\Rightarrow}_S e_{1S}))\end{array}\right\}_\top$$

if v_I^3 **then**

$$\left\{\begin{array}{l}[\mathrm{SR}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta) * \\ \textsc{StackInv}(h, r, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rightarrow}_S K_{3S}[\textbf{true}] * V[\![\tau]\!]^M(n, m)\end{array}\right\}_\top$$

inj$_2$ n_I

$$\left\{\begin{array}{l}v_I^4.\ \exists v_S^4.\ j \overset{\zeta}{\Rightarrow}_S v_S^4 * [\mathrm{SR}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta) * \\ V[\![\mathbf{1} + \tau]\!]^M(v_I^4, v_S^4)\end{array}\right\}_\top$$

else

$$\left\{\begin{array}{l}[\mathrm{SR}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta) * \\ \textsc{StackInv}(h, r, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rightarrow}_S e_{1S}\end{array}\right\}_\top$$

$push(h, n)$

```
// Follows from IH
```

$$\left\{\begin{array}{l}v_I^4.\ \exists v_S^4.\ j \overset{\zeta}{\Rightarrow}_S v_S^4 * [\mathrm{SR}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho, al_\rho\}, M, \zeta) * \\ V[\![\mathbf{1} + \tau]\!]^M(v_I^4, v_S^4)\end{array}\right\}_\top$$

We have to show we can perform the simulation on the right hand side:

$\exists l, l', n_S, n'.\ [\text{SR}]_\zeta^{\pi'} * [\text{WR}]_r^\pi * \text{REG}(\text{RG}(r)) * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} *$
$l = (n, m) :: l' * \text{SPEC} * j \overset{\zeta}{\Rrightarrow}_S e_{1S} \ * \text{STACKREL}(h, l', l, v_I^2, n', r, V[\![\tau]\!]^M)$

$\Rrightarrow$ $\exists l, l', n_S, n'.\ [\text{SR}]_\zeta^{\pi'} * [\text{WR}]_r^\pi * \text{REG}(\text{RG}(r)) * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} *$
$l = (n, m) :: l' * \text{SPEC} * j \overset{\zeta}{\Rrightarrow}_S K_{1S}[!h_S] \ * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * h_S \overset{1}{\hookrightarrow}_{I,r} n' *$
$vals(l', v_I^2, V[\![\tau]\!]^M) * linked(l, n', r, V[\![\tau]\!]^M)$
// Follows from Lemma ??

$\Rrightarrow$ $\exists l, l', n_S, v_S^1.\ [\text{SR}]_\zeta^{\pi'} * [\text{WR}]_r^\pi * \text{REG}(\text{RG}(r)) * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} *$
$l = (n, m) :: l' * \text{SPEC} * j \overset{\zeta}{\Rrightarrow}_S K_{1S}[v_S^1] \ * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * h_S \overset{1}{\hookrightarrow}_{I,r} v_S^1 *$
$vals(l', v_I^2, V[\![\tau]\!]^M) * linked(l, n', r, V[\![\tau]\!]^M)$
// Unfolding *linked*

$\Rrightarrow$ $\exists l, l', n_S, v_S^1, v_S^2, n''.\ [\text{SR}]_\zeta^{\pi'} * [\text{WR}]_r^\pi * \text{REG}(\text{RG}(r)) * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} *$
$l = (n, m) :: l' * \text{SPEC} * j \overset{\zeta}{\Rrightarrow}_S K_{2S}[!v_S^1] \ * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * h_S \overset{1}{\hookrightarrow}_{I,r} v_S^1 *$
$vals(l', v_I^2, V[\![\tau]\!]^M) * linked(l', n'', r, V[\![\tau]\!]^M) * v_S^1 \overset{1}{\hookrightarrow}_{I,r} v_S^2 * v_S^2 = \textbf{inj}_2\ (n_S, n'') *$
$V[\![\tau]\!]^M(n, m)$
// Follows from Lemma ??, Lemma ??

$\Rrightarrow$ $\exists l, l', n_S, v_S^1, v_S^2, n''.\ [\text{SR}]_\zeta^{\pi'} * [\text{WR}]_r^\pi * \text{REG}(\text{RG}(r)) * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} *$
$l = (n, m) :: l' * \text{SPEC} * j \overset{\zeta}{\Rrightarrow}_S K_{3S}[\textbf{CAS}(h_S, v_S^1, v_S^2)] \ * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * h_S \overset{1}{\hookrightarrow}_{I,r} v_S^1 *$
$vals(l', v_I^2, V[\![\tau]\!]^M) * linked(l', n'', r, V[\![\tau]\!]^M) * v_S^1 \overset{1}{\hookrightarrow}_{I,r} v_S^2 * v_S^2 = \textbf{inj}_2\ (n_S, n'') *$
$V[\![\tau]\!]^M(n, m)$
// Perform **CAS**

$\Rrightarrow$ $\exists l, l', n_S, v_S^1, v_S^2, n''.\ [\text{SR}]_\zeta^{\pi'} * [\text{WR}]_r^\pi * \text{REG}(\text{RG}(r)) * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} *$
$l = (n, m) :: l' * \text{SPEC} * j \overset{\zeta}{\Rrightarrow}_S K_{3S}[\textbf{true}] \ * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * h_S \overset{1}{\hookrightarrow}_{I,r} v_S^2 *$
$vals(l', v_I^2, V[\![\tau]\!]^M) * linked(l', n'', r, V[\![\tau]\!]^M) * v_S^1 \overset{1}{\hookrightarrow}_{I,r} v_S^2 * v_S^2 = \textbf{inj}_2\ (n_S, n'') *$
$V[\![\tau]\!]^M(n_I, n_S, n'')$
// Fold *linked*

$\Rrightarrow$ $\exists n_S, v_S^1, v_S^2.\ [\text{SR}]_\zeta^{\pi'} * [\text{WR}]_r^\pi * \text{REG}(\text{RG}(r)) * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} *$
$\text{SPEC} * j \overset{\zeta}{\Rrightarrow}_S \textbf{inj}_2\ n_S \ * \text{STACKREL}(h, r, V[\![\tau]\!]^M) * V[\![\tau]\!]^M(n, m)$

□

Lemma 101. *create*

$$\forall \rho, M.\ E^{\rho;\cdot}_{al_\rho;M}(V[\![\tau \rightarrow^{\rho|\cdot}_{wr_\rho, rd_\rho, al_\rho} \mathbf{1} \times \mathbf{1} \rightarrow^{\rho|\cdot}_{wr_\rho, rd_\rho} \mathbf{1} + \tau]\!]^M)(create_1(), create_2())$$

Proof.

Context: g, j, K, π', ζ, M

Context: $\boxed{\text{HEAP}}^{\text{HP}}, \boxed{\text{SPEC}(h_0, e_0, \zeta)}^{\text{SP}(\zeta)}$

$$\left\{j \overset{\zeta}{\Rrightarrow}_S \textbf{let } t = \textbf{new inj}_1\ ()\ \textbf{in let } h = \textbf{new } t \textbf{ in } (push_2, pop_2) * [\text{SR}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{al_\rho\}, M, \zeta)\right\}_\top$$

// Let $r = M(\rho)$ and $R = \{\text{HP}, \text{SP}(\zeta), r\}$

$$\left\{\begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S \textbf{let } t = \textbf{new inj}_1\ ()\ \textbf{in let } h = \textbf{new } t \textbf{ in } (push_2, pop_2) * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \\ \boxed{\text{REG}(r)}^{\text{RG}(r)} * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} \end{array}\right\}_\top$$

Bind on $(\textbf{let } h = []\ \textbf{in } (push_1, pop_1))[\textbf{new inj}_1\ ()]$

$$\left\{\begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S \textbf{let } t = \textbf{new inj}_1\ ()\ \textbf{in let } h = \textbf{new } t \textbf{ in } (push_2, pop_2) * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \\ \boxed{\text{REG}(r)}^{\text{RG}(r)} * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} \end{array}\right\}_\top$$

Open R

// Let $K_{1S} \triangleq \textbf{let } t = []\ \textbf{in let } h = \textbf{new } t \textbf{ in } (push_2, pop_2)$

// Let $K_{2S} \triangleq \textbf{let } h = \textbf{new } t \textbf{ in } (push_2, pop_2)$

$$\left\{\begin{array}{l} j \overset{\zeta}{\Rrightarrow}_S K_1[\textbf{new inj}_1\ ()] * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \boxed{\text{REG}(r)}^{\text{RG}(r)} * \\ [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \triangleright\text{HEAP} * \triangleright\text{SPEC}(h_0, e_0, \zeta) \end{array}\right\}_{\top\setminus R}$$

Frame

$\{\text{HEAP}\}_{\top\setminus R}$

new inj$_1$ $()$

// Follows from Lemma ??

$\{h_I.\ \text{HEAP} * h_I \mapsto_I \textbf{inj}_1\ ()\}_{\top\setminus R}$

$$\left\{\begin{array}{l} h_I.\ j \overset{\zeta}{\Rrightarrow}_S K_1[\textbf{new inj}_1\ ()] * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \boxed{\text{REG}(r)}^{\text{RG}(r)} * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * h_I \mapsto_I \textbf{inj}_1\ () \end{array}\right\}_{\top\setminus R}$$

// Follows from Lemma ??

$$\left\{\begin{array}{l} h_I.\ \exists l_S.\ j \overset{\zeta}{\Rrightarrow}_S K_{1S}[l_S] * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \boxed{\text{REG}(r)}^{\text{RG}(r)} * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * h_I \mapsto_I \textbf{inj}_1\ () * l_S \mapsto_S^\zeta \textbf{inj}_1\ () \end{array}\right\}_{\top\setminus R}$$

$$\left\{\begin{array}{l} h_I.\ \exists l_S.\ j \overset{\zeta}{\Rrightarrow}_S K_{2S}[\textbf{new } l_S] * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \boxed{\text{REG}(r)}^{\text{RG}(r)} * \\ [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * h_I \mapsto_I \textbf{inj}_1\ () * l_S \mapsto_S^\zeta \textbf{inj}_1\ () \end{array}\right\}_{\top\setminus R}$$

// Follows from Lemma ??

$$\left\{\begin{array}{l} h_I.\ \exists h_S, l_S.\ j \overset{\zeta}{\Rrightarrow}_S K_{2S}[h_S] * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \boxed{\text{REG}(r)}^{\text{RG}(r)} * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ \text{HEAP} * \text{SPEC}(h_0, e_0, \zeta) * h_I \mapsto_I \textbf{inj}_1\ () * l_S \mapsto_S^\zeta \textbf{inj}_1\ () * h_S \mapsto_S^\zeta l_S \end{array}\right\}_{\top\setminus R}$$

$$\left\{\begin{array}{l} h_I.\ \exists h_S, l_S.\ j \overset{\zeta}{\Rrightarrow}_S (push_2, pop_2) * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \boxed{\text{REG}(r)}^{\text{RG}(r)} * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ h_I \mapsto_I \textbf{inj}_1\ () * l_S \mapsto_S^\zeta \textbf{inj}_1\ () * h_S \mapsto_S^\zeta l_S \end{array}\right\}_\top$$

// Extending reg: Lemma ??

$$\left\{\begin{array}{l} h_I.\ \exists h_S, l_S.\ j \overset{\zeta}{\Rrightarrow}_S (push_2, pop_2) * [\text{SR}]_\zeta^{\pi'} * [\text{AL}]_r^\pi * \boxed{\text{REG}(r)}^{\text{RG}(r)} * [\text{MU}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ h_I \overset{1}{\hookrightarrow}_{I,r} \textbf{inj}_1\ () * l_S \overset{1}{\hookrightarrow}_{S,r} \textbf{inj}_1\ () * h_S \overset{1}{\hookrightarrow}_{S,r} l_S \end{array}\right\}_\top$$

$$
\begin{array}{l}
\texttt{// Fold into } \textsc{StackInv}((h_I, h_S), r, V[\![\tau]\!]^M) \texttt{ for the empty list by Lemma ??} \\
\left\{ \begin{array}{l} h_I.\ \exists h_S, l_S.\ j \overset{\zeta}{\Rrightarrow}_S (push_2, pop_2) * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ \textsc{StackInv}((h_I, h_S), r, V[\![\tau]\!]^M) \end{array} \right\}_{\top} \\
\forall h_I.\ \left\{ \begin{array}{l} \exists h_S, l_S.\ j \overset{\zeta}{\Rrightarrow}_S (push_2, pop_2) * [\textsc{Sr}]^{\pi'}_{\zeta} * [\textsc{Al}]^{\pi}_{r} * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \\ \textsc{StackInv}((h_I, h_S), r, V[\![\tau]\!]^M) \end{array} \right\}_{\top} \\
\quad (push_1, pop_1) \\
\left\{ \begin{array}{l} v^1_I.\ v^1_I = (push_1, pop_1) * \exists v^1_S.\ j \overset{\zeta}{\Rrightarrow}_S v^1_S * v^1_S = (push_2, pop_2) * [\textsc{Sr}]^{\pi'}_{\zeta} * \\ P_{reg}(\{\rho\}, g, \{al_\rho\}, M, \zeta) * \textsc{StackInv}((h_I, h_S), r, V[\![\tau]\!]^M) \end{array} \right\}_{\top} \\
\left\{ \begin{array}{l} v^1_I.\ \exists v^1_S.\ j \overset{\zeta}{\Rrightarrow}_S v^1_S * v^1_S = (push_2, pop_2) * [\textsc{Sr}]^{\pi'}_{\zeta} * P_{reg}(\{\rho\}, g, \{al_\rho\}, M, \zeta) * \\ \textsc{StackInv}(h, r, V[\![\tau]\!]^M) * V[\![\tau \to^{\rho|\cdot}_{wr_\rho, rd_\rho, al_\rho} \mathbf{1}]\!]^M (push_1, push_2) * \\ V[\![\mathbf{1} \to^{\rho|\cdot}_{wr_\rho, rd_\rho} \mathbf{1} + \tau]\!]^M (pop_1, pop_2) \end{array} \right\}_{\top} \\
\left\{ \begin{array}{l} v^1_I.\ \exists v^1_S.\ j \overset{\zeta}{\Rrightarrow}_S v^1_S * v^1_S = (push_2, pop_2) * [\textsc{Sr}]^{\pi'}_{\zeta} * P_{reg}(\{\rho\}, g, \{al_\rho\}, M, \zeta) * \\ \textsc{StackInv}(h, r, V[\![\tau]\!]^M) * \\ V[\![\tau \to^{\rho|\cdot}_{wr_\rho, rd_\rho, al_\rho} \mathbf{1} \times \mathbf{1} \to^{\rho|\cdot}_{wr_\rho, rd_\rho} \mathbf{1} + \tau]\!]^M ((push_1, pop_1), (push_2, pop_2)) \end{array} \right\}_{\top}
\end{array}
$$

$\square$

6.5 Example: Private Stacks

Consider the following two stack-modules:

$Stack_1$ has a single reference to a pure functional list, where the plain assignments updates the entire list on push and pop.

$$
\begin{aligned}
create_1() &= \textbf{let } h = \textbf{new inj}_1\ () \textbf{ in } (push_1, pop_1) \\
push_1(n) &= \textbf{let } v = !h \textbf{ in } h := \textbf{inj}_2\ (n, v) \\
pop_1() &= \textbf{let } v = !h \textbf{ in} \\
&\qquad \textbf{case}(v, \textbf{inj}_1\ () \Rightarrow \textbf{inj}_1\ (), \\
&\qquad\qquad \textbf{inj}_2\ (n, v') \Rightarrow h := v'; \textbf{inj}_2\ n)
\end{aligned}
$$

$Stack_2$ has a single reference to a pure functional list, where the **cas** operation is used to update the entire list on push and pop.

$$
\begin{aligned}
create_2() &= \textbf{let } h = \textbf{new inj}_1\ () \textbf{ in } (push_2, pop_2) \\
push_2(n) &= \textbf{let } v = !h \textbf{ in} \\
&\qquad \textbf{let } v' = \textbf{inj}_2\ (n, v) \textbf{ in if CAS}(h, v, v') \textbf{ then } () \textbf{ else } push_2(n) \\
pop_2() &= \textbf{let } v = !h \textbf{ in} \\
&\qquad \textbf{case}(v, \textbf{inj}_1\ () \Rightarrow \textbf{inj}_1\ (), \\
&\qquad\qquad \textbf{inj}_2\ (n, v') \Rightarrow \textbf{if CAS}(h, v, v') \textbf{ then inj}_2\ n \textbf{ else } pop_2())
\end{aligned}
$$

This example shows, that if we know the module is private to us, we can directly update the value without the need for doing compare-and-swap.

We choose the following relation to show equality:

$$
\begin{aligned}
\textsc{StackRel}(h, r, \phi) &\triangleq ([\textsc{Wr}]^1_r \vee (\exists l, v_I, v_S.\ h_I \overset{1}{\hookrightarrow}_{I,r} v_I * h_S \overset{1}{\hookrightarrow}_{S,r} v_S * vals(l, (v_I, v_S), \phi))) \\
\textsc{StackInv}(h) &\triangleq \exists \iota.\ \boxed{\textsc{StackRel}(h, V[\![\tau]\!]^M)}^{\textsc{Si}(\iota)}
\end{aligned}
$$

where

$$vals(\mathsf{nil}, v, \phi) \triangleq v_I = \mathbf{inj}_1\ () \land v_S = \mathbf{inj}_1\ ()$$
$$vals(x :: xs, v, \phi) \triangleq \exists v_I', v_S'.\ v_I = \mathbf{inj}_2\ (x_I, v_I') \land v_S = \mathbf{inj}_2\ (x_S, v_S') \land \phi(x) \land vals(xs, (v_I', v_S'), \phi)$$

We only show the refinement proof of push, the proof of pop is straight-forward.

Lemma 102. *$Stack_1$-push refines $Stack_2$-push*

$$\forall \rho, M, h, n, m.\ V[\![\tau]\!]^M(n, m)$$
$$\Rightarrow \quad \textsc{StackInv}(h, M(\rho)) \vdash E^{\rho;\cdot}_{wr_\rho, rd_\rho; M}(V[\![\mathbf{1}]\!]^M)(push_1(n), push_2(m))$$

Proof. We define the following short-hands:

$$e_{1I} \triangleq \textbf{let } v = !h \textbf{ in } h := \mathbf{inj}_2\ (n, v)$$
$$e_{1S} \triangleq \textbf{let } v = !h_I \textbf{ in let } v' = \mathbf{inj}_2\ (n, v) \textbf{ in if } \mathbf{CAS}(h, v, v') \textbf{ then } () \textbf{ else } push_2(n)$$
$$K_{1I} \triangleq \textbf{let } v = [] \textbf{ in } h := \mathbf{inj}_2\ (n, v)$$
$$K_{1S} \triangleq \textbf{let } v = [] \textbf{ in let } v' = \mathbf{inj}_2\ (n, v) \textbf{ in if } \mathbf{CAS}(h, v, v') \textbf{ then } () \textbf{ else } push_2(n)$$
$$K_{2S} \triangleq \textbf{let } v' = [] \textbf{ in if } \mathbf{CAS}(h, v_I^1, v') \textbf{ then } () \textbf{ else } push_1(n)$$
$$K_{3S} \triangleq \textbf{if } [] \textbf{ then } () \textbf{ else } push_2(n)$$

Context: $g, j, K, \pi', \zeta, M, h, n$

Context: $\boxed{\textsc{Heap}}^{\textsc{Hp}}, \boxed{\textsc{Spec}(h_0, e_0, \zeta)}^{\textsc{Sp}(\zeta)}, \textsc{StackInv}(h, M(\rho)), V[\![\tau]\!]^M(n, n)$

Context: $\triangleright\left\{j \overset{\zeta}{\Rightarrow}_S e_{1S} * [\textsc{Sr}]^{\pi'}_\zeta * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta)\right\}$

$push(n)$

$\left\{v_I^1.\ \exists v_S^1.\ j \overset{\zeta}{\Rightarrow}_S v_S^1 * [\textsc{Sr}]^{\pi'}_\zeta * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta) * V[\![\mathbf{1}]\!]^M(v_I^1, v_S^1)\right\}_\top$

$\left\{j \overset{\zeta}{\Rightarrow}_S e_{1S} * [\textsc{Sr}]^{\pi'}_\zeta * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta)\right\}_\top$

// Let $\pi = g(\rho)$, $r = M(\rho)$ and $R = \{\textsc{Hp}, \textsc{Sp}(\zeta), \textsc{Rg}(r)\}$

$\left\{j \overset{\zeta}{\Rightarrow}_S e_{1S} * [\textsc{Sr}]^{\pi'}_\zeta * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}}\right\}_\top$

Bind on $K_{1I}[!h_I]$

// Unfolding $\textsc{StackInv}(h, r)$

$\left\{\begin{array}{l} j \overset{\zeta}{\Rightarrow}_S e_{1S} * [\textsc{Sr}]^{\pi'}_\zeta * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \exists\iota.\ \boxed{\textsc{StackRel}(h, r, V[\![\tau]\!]^M)}^{\textsc{Si}(\iota)} \end{array}\right\}_\top$

Open $R, \textsc{Si}(\iota)$

$\left\{\begin{array}{l} j \overset{\zeta}{\Rightarrow}_S e_{1S} * [\textsc{Sr}]^{\pi'}_\zeta * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * \triangleright\textsc{Reg}(r) * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \triangleright\textsc{Heap} * \triangleright\textsc{Spec}(h_0, e_0, \zeta) * \triangleright\textsc{StackRel}(h, r, V[\![\tau]\!]^M) \end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$

$!h_I$

// Follows from Lemma ??

$\left\{\begin{array}{l} v_I^1.\ \exists l, v_S^1.\ vals(l, (v_I^1, v_S^1), V[\![\tau]\!]^M) * j \overset{\zeta}{\Rightarrow}_S e_{1S} * [\textsc{Sr}]^{\pi'}_\zeta * [\textsc{Rd}]^1_r * [\textsc{Wr}]^1_r * \\ \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * \textsc{StackRel}(h, r, V[\![\tau]\!]^M) \end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$

// Trade $[\textsc{Wr}]^1_r$ in $\textsc{StackRel}(h, r, V[\![\tau]\!]^M)$

$\left\{\begin{array}{l} v_I^1.\ \exists l, v_S^1.\ vals(l, (v_I^1, v_S^1), V[\![\tau]\!]^M) * j \overset{\zeta}{\Rightarrow}_S e_{1S} * [\textsc{Sr}]^{\pi'}_\zeta * [\textsc{Rd}]^1_r * \\ \textsc{Reg}(r) * [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * \\ \textsc{StackRel}(h, r, V[\![\tau]\!]^M) * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^1 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1 \end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$

$\left\{\begin{array}{l} v_I^1.\ \exists l, v_S^1.\ vals(l, (v_I^1, v_S^1), V[\![\tau]\!]^M) * j \overset{\zeta}{\Rightarrow}_S e_{1S} * [\textsc{Sr}]^{\pi'}_\zeta * [\textsc{Rd}]^1_r * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r, \{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h, r) * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^1 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1 \end{array}\right\}_\top$

$$\forall v_I^1.\ \left\{\begin{array}{l}\exists l, v_S^1.\ vals(l,(v_I^1,v_S^1),V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^1 * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h,r) * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^1 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1\end{array}\right\}_\top$$

Bind on $(h_I := [])[\textbf{inj}_2\ (n, v_I^1)]$

$$\left\{\begin{array}{l}\exists l, v_S^1.\ vals(l,(v_I^1,v_S^1),V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^1 * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h,r) * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^1 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1\end{array}\right\}_\top$$

$\textbf{inj}_2\ (n, v_I^1)$

$$\left\{\begin{array}{l}v_I^2.\ \exists l, v_S^1, v_S^2.\ v_S^2 = \textbf{inj}_2\ (n, v_S^1) * vals(l, v_I^1, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * \\ [\textsc{Rd}]_r^1 * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h,r) * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^1 * \\ h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1 * vals((n,n) :: l, (v_I^2, v_S^2), V[\![\tau]\!]^M)\end{array}\right\}_\top$$

$$\forall v_I^2.\ \left\{\begin{array}{l}\exists l, v_S^1, v_S^2.\ v_S^2 = \textbf{inj}_2\ (n, v_S^1) * vals(l, v_I^1, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * \\ [\textsc{Rd}]_r^1 * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h,r) * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^1 * \\ h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1 * vals((n,n) :: l, (v_I^2, v_S^2), V[\![\tau]\!]^M)\end{array}\right\}_\top$$

Bind on $K_3[\textbf{CAS}(h, v_I^1, v_I^2)]$

$$\left\{\begin{array}{l}\exists l, v_S^1, v_S^2, \iota.\ v_S^2 = \textbf{inj}_2\ (n, v_S^1) * vals(l, v_I^1, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * \\ [\textsc{Rd}]_r^1 * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^1 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1 * \\ vals((n,n) :: l, (v_I^2, v_S^2), V[\![\tau]\!]^M) * \boxed{\textsc{StackRel}(h,r,V[\![\tau]\!]^M)}^{\textsc{Si}(\iota)}\end{array}\right\}_\top$$

Open $R, \textsc{Si}(\iota)$

$$\left\{\begin{array}{l}\exists l, v_S^1, v_S^2.\ v_S^2 = \textbf{inj}_2\ (n, v_S^1) * vals(l, v_I^1, V[\![\tau]\!]^M) * j \overset{\zeta}{\Rrightarrow}_S e_{1S} * \\ [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^1 * \triangleright\textsc{Reg}(r) * \triangleright\textsc{Heap} * \triangleright\textsc{Spec}(h_0, e_0, \zeta) * [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \\ h_I \overset{1}{\hookrightarrow}_{I,r} v_I^1 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1 * vals((n,n) :: l, (v_I^2, v_S^2), V[\![\tau]\!]^M) * \\ \triangleright\textsc{StackRel}(h,r,V[\![int]\!]^M)\end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$$

$h_I := v_I^2$

$$\left\{\begin{array}{l}v_I^3.\ v_I^3 = () * \exists l, v_S^1, v_S^2.\ v_S^2 = \textbf{inj}_2\ (n, v_S^1) * vals(l, v_I^1, V[\![\tau]\!]^M) * \\ j \overset{\zeta}{\Rrightarrow}_S e_{1S} * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^1 * \textsc{Reg}(r) * [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \\ \textsc{Spec}(h_0, e_0, \zeta) * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1 * \textsc{StackRel}(h,r,V[\![int]\!]^M) * \\ vals((n,n) :: l, (v_I^2, v_S^2), V[\![\tau]\!]^M)\end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$$

// Follows from simulation on the right hand side. CAS succeeds because we have $h_S \overset{1}{\hookrightarrow}_{S,r} v_S^1$

$$\left\{\begin{array}{l}v_I^3.\ v_I^3 = () * \exists l, v_S^2, v_S^3.\ v_S^3 = () * j \overset{\zeta}{\Rrightarrow}_S v_S^3 * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^1 * \\ \textsc{Reg}(r) * [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * h_I \overset{1}{\hookrightarrow}_{I,r} v_I^2 * \\ h_S \overset{1}{\hookrightarrow}_{S,r} v_S^2 * vals((n,n) :: l, (v_I^2, v_S^2), V[\![\tau]\!]^M) * \\ \textsc{StackRel}(h,r,V[\![int]\!]^M)\end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$$

// We trade for $[\textsc{Wr}]_r^1$

$$\left\{\begin{array}{l}v_I^3.\ v_I^3 = () * \exists v_S^3.\ v_S^3 = () * j \overset{\zeta}{\Rrightarrow}_S v_S^3 * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^1 * \\ \textsc{Reg}(r) * [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \textsc{Heap} * \textsc{Spec}(h_0, e_0, \zeta) * [\textsc{Wr}]_r^1 * \\ \textsc{StackRel}(h,r,V[\![int]\!]^M)\end{array}\right\}_{\top\setminus R, \textsc{Si}(\iota)}$$

$$\left\{\begin{array}{l}v_I^3.\ \exists v_S^3.\ j \overset{\zeta}{\Rrightarrow}_S v_S^3 * [\textsc{Sr}]_\zeta^{\pi'} * [\textsc{Rd}]_r^1 * [\textsc{Wr}]_r^1 * \boxed{\textsc{Reg}(r)}^{\textsc{Rg}(r)} * \\ [\textsc{Mu}(r,\{\zeta\})]^{\frac{\pi}{2}} * \textsc{StackInv}(h) * V[\![\mathbf{1}]\!]^M(v_I^3, v_S^3)\end{array}\right\}_\top$$

$$\left\{v_I^3.\ \exists v_S^3.\ j \overset{\zeta}{\Rrightarrow}_S v_S^3 * [\textsc{Sr}]_\zeta^{\pi'} * P_{reg}(\{\rho\}, g, \{wr_\rho, rd_\rho\}, M, \zeta) * V[\![\mathbf{1}]\!]^M(v_I^3, v_S^3)\right\}_\top$$

$\square$