A Logical Relation for Monadic Encapsulation of State
Proving contextual equivalences in the presence of runST

Technical Appendix

AMIN TIMANY, imec-Distrinet, KU-Leuven
LÉO STEFANESCO, ENS Lyon, Université de Lyon
MORTEN KROGH-JESPERSEN, Aarhus University
LARS BIRKEDAL, Aarhus University

ACM Reference format:
Amin Timany, Léo Stefanesco, Morten Krogh-Jespersen, and Lars Birkedal. 2017. A Logical Relation for Monadic Encapsulation of State. *PACM Progr. Lang.* 1, 1, Article 1 (January 2017), 47 pages.
DOI: 10.1145/nnnnnnn.nnnnnnn

1 PRELIMINARIES

To lighten the notations, we make the convention that some (meta)variable names implicitly range over some sets, as indicated in the table bellow. If a (meta)variables m ranges over a set S, so does m', m'', m_1, m_2, m'_1, …

Variables	Set	Description
τ, ρ	*Types*	Types
X	*Tvar*	Type variables
x, y	*Var*	Program variables
$\gamma, \gamma_h, \gamma_{rel}, \gamma_{bij} \ldots$	*Names*	Monoid names
v, w	*Val*	Program values
e	*Expr*	Program expression
l	*Loc*	Heap locations
Ξ	$\mathcal{P}(Tvar)$	Type context
Γ	$Var \rightharpoonup^{\text{fin}} Types$	Variable environment
r	$(Loc \times Loc) \rightharpoonup^{\text{fin}} (\textsc{Ag}(Names))$	See §5

Remark 1.1. *In the paper we define the IC predicate and IC-triples (see blow) in which in the postcondition can only mention the value that the computation converges to. Here we define a slightly stronger version which allows the postcondition to also mention the number steps the computation takes. This stronger version is only used in constructing a particular logical relation (the NN-logical relation) which in turn only appears as part of the proof of rec hoisting.*

2 THE LANGUAGE: STLang

2.1 Statics

We note the set of heap locations $Loc \triangleq \mathbb{N}$.

2017. 2475-1421/2017/1-ART1 $15.00
DOI: 10.1145/nnnnnnn.nnnnnnn

$$
\begin{aligned}
\circledcirc &::= \; + \mid - \mid * \mid = \mid < \\
e &::= x \mid () \mid \texttt{true} \mid \texttt{false} \mid n \mid \ell \mid (e,e) \mid \texttt{inj}_i\, e \mid \texttt{rec}\, f(x) = e \mid \Lambda\, e \mid \texttt{fold}\, e \mid \texttt{unfold}\, e \mid e\; e \\
&\quad \mid e\; \_ \mid \pi_i\, e \mid \texttt{match}\, e\, \texttt{with}\, \texttt{inj}_i\, x \Rightarrow e_i\, \texttt{end} \mid \texttt{if}\, e\, \texttt{then}\, e\, \texttt{else}\, e \mid e \circledcirc e \\
&\quad \mid \texttt{ref}(e) \mid !\, e \mid e \leftarrow e \mid e == e \mid \texttt{bind}\, e\, \texttt{in}\, e \mid \texttt{return}\, e \mid \texttt{runST}\ \{e\} \\
v &::= () \mid \texttt{true} \mid \texttt{false} \mid n \mid \ell \mid (v,v) \mid \texttt{inj}_i\, v \\
&\quad \mid \texttt{rec}\, f(x) = e \mid \Lambda\, e \mid \texttt{fold}\, v \mid \texttt{ref}(v) \mid !\, v \mid v \leftarrow v \mid \texttt{bind}\, v\, \texttt{in}\, v \mid \texttt{return}\, v \\
\tau &::= X \mid \rho \mid \mathbf{1} \mid \mathbb{B} \mid \mathbb{N} \mid \tau \times \tau \mid \tau + \tau \mid \tau \to \tau \mid \forall X.\, \tau \mid \mu X.\, \tau \mid \mathsf{ref}(\tau) \mid \mathsf{ST}\ \rho\ \tau
\end{aligned}
$$

2.1.1 Typing. We use two contexts type context (Ξ) and term context (Γ). $\Xi \subseteq \mathit{Tvar}$ is a set of type variables, we write $\cdot$ for the empty set and Ξ, X for the disjoint union $\Xi \uplus \{X\}$. Γ is a partial map from variables to types, we write $\cdot$ for the partial function defined nowhere, and, for $x \in \mathit{Var}$ and $\tau \in \mathit{Types}$, we denote by $\Gamma, x : \tau$ the disjoint union $\Gamma \uplus \{(x,\tau)\}$, where we identify partial functions and their graphs.

A type τ is said to be well defined in a context Ξ whenever:

$$\Xi \vdash \tau \quad \triangleq \quad \mathsf{FV}(\tau) \subseteq \Xi.$$

$\boxed{\Xi \mid \Gamma \vdash e : \tau}$

$$
\textsc{TVar}\ \ \Xi \mid \Gamma, x : \tau \vdash x : \tau
\qquad
\textsc{TUnit}\ \ \Xi \mid \Gamma \vdash () : \mathbf{1}
\qquad
\textsc{TTrue}\ \ \Xi \mid \Gamma \vdash \texttt{true} : \mathbb{B}
\qquad
\textsc{TFalse}\ \ \Xi \mid \Gamma \vdash \texttt{false} : \mathbb{B}
\qquad
\textsc{TNat}\ \ \Xi \mid \Gamma \vdash n : \mathbb{N}
$$

$$
\textsc{TPair}\ \frac{\Xi \mid \Gamma \vdash e_1 : \tau_1 \qquad \Xi \mid \Gamma \vdash e_2 : \tau_2}{\Xi \mid \Gamma \vdash (e_1, e_2) : \tau_1 \times \tau_2}
\qquad
\textsc{TInj}\ \frac{\Xi \mid \Gamma \vdash e : \tau_i \qquad i \in \{1,2\}}{\Xi \mid \Gamma \vdash \texttt{inj}_i\, e : \tau_1 + \tau_2}
\qquad
\textsc{TRec}\ \frac{\Xi \mid \Gamma, x : \tau_1, f : \tau_1 \to \tau_2 \vdash e : \tau_2}{\Xi \mid \Gamma \vdash \texttt{rec}\, f(x) = e : \tau_1 \to \tau_2}
$$

$$
\textsc{TAbs}\ \frac{\Xi, X \mid \Gamma \vdash e : \tau}{\Xi \mid \Gamma \vdash \Lambda\, e : \forall X.\, \tau}
\qquad
\textsc{TFold}\ \frac{\Xi \mid \Gamma \vdash e : \tau[\mu X.\, \tau / X]}{\Xi \mid \Gamma \vdash \texttt{fold}\, e : \mu X.\, \tau}
\qquad
\textsc{TUnfold}\ \frac{\Xi \mid \Gamma \vdash e : \mu X.\, \tau}{\Xi \mid \Gamma \vdash \texttt{unfold}\, e : \tau[\mu X.\, \tau / X]}
$$

$$
\textsc{TApp}\ \frac{\Xi \mid \Gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Xi \mid \Gamma \vdash e_2 : \tau_1}{\Xi \mid \Gamma \vdash e_1\; e_2 : \tau_2}
\qquad
\textsc{TInst}\ \frac{\Xi \mid \Gamma \vdash e : \forall X.\, \tau \qquad \Xi \vdash \tau'}{\Xi \mid \Gamma \vdash e\; \_ : \tau[\tau'/X]}
\qquad
\textsc{TProj}\ \frac{\Xi \mid \Gamma \vdash e : \tau_1 \times \tau_2 \qquad i \in \{1,2\}}{\Xi \mid \Gamma \vdash \pi_i\, e : \tau_i}
$$

$$
\textsc{TMatch}\ \frac{\Xi \mid \Gamma \vdash e : \tau_1 + \tau_2 \qquad \Xi \mid \Gamma, x : \tau_1 \vdash e_1 : \tau \qquad \Xi \mid \Gamma, x : \tau_2 \vdash e_2 : \tau}{\Xi \mid \Gamma \vdash \texttt{match}\, e\, \texttt{with}\, \texttt{inj}_i\, x \Rightarrow e_i\, \texttt{end} : \tau}
$$

$$
\textsc{TIf}\ \frac{\Xi \mid \Gamma \vdash e : \mathbb{B} \qquad \Xi \mid \Gamma \vdash e_1 : \tau \qquad \Xi \mid \Gamma \vdash e_2 : \tau}{\Xi \mid \Gamma \vdash \texttt{if}\, e\, \texttt{then}\, e_1\, \texttt{else}\, e_2 : \tau}
\qquad
\textsc{TNatBinop}\ \frac{\Xi \mid \Gamma \vdash e : \mathbb{N} \qquad \Xi \mid \Gamma \vdash e' : \mathbb{N} \qquad \circledcirc \in \{+,-,*\}}{\Xi \mid \Gamma \vdash e \circledcirc e : \mathbb{N}}
$$

$$
\textsc{TBoolBinop}\ \frac{\Xi \mid \Gamma \vdash e : \mathbb{N} \qquad \Xi \mid \Gamma \vdash e' : \mathbb{N} \qquad \circledcirc \in \{=,<\}}{\Xi \mid \Gamma \vdash e \circledcirc e : \mathbb{B}}
$$

$$\textsc{TNew}\quad \frac{\Xi \mid \Gamma \vdash e : \tau \qquad \Xi \vdash \rho}{\Xi \mid \Gamma \vdash \texttt{ref}(e) : \mathsf{ST}\ \rho\ (\mathsf{STRef}\ \rho\ \tau)} \qquad \textsc{TDeref}\quad \frac{\Xi \mid \Gamma \vdash e : \mathsf{STRef}\ \rho\ \tau}{\Xi \mid \Gamma \vdash\ !e : \mathsf{ST}\ \rho\ \tau} \qquad \textsc{TGets}\quad \frac{\Xi \mid \Gamma \vdash e : \mathsf{STRef}\ \rho\ \tau \qquad \Xi \mid \Gamma \vdash e' : \tau}{\Xi \mid \Gamma \vdash e \leftarrow e' : \mathsf{ST}\ \rho\ \mathbf{1}}$$

$$\textsc{TRefEq}\quad \frac{\Xi \mid \Gamma \vdash e : \mathsf{STRef}\ \rho\ \tau \qquad \Xi \mid \Gamma \vdash e' : \mathsf{STRef}\ \rho\ \tau}{\Xi \mid \Gamma \vdash e == e' : \mathbb{B}} \qquad \textsc{TBind}\quad \frac{\Xi \mid \Gamma \vdash e : \mathsf{ST}\ \rho\ \tau \qquad \Xi \mid \Gamma \vdash e' : \tau \to (\mathsf{ST}\ \rho\ \tau')}{\Xi \mid \Gamma \vdash \texttt{bind}\, e\, \texttt{in}\, e' : \mathsf{ST}\ \rho\ \tau'}$$

$$\textsc{TReturn}\quad \frac{\Xi \mid \Gamma \vdash e : \tau \qquad \Xi \vdash \rho}{\Xi \mid \Gamma \vdash \texttt{return}\, e : \mathsf{ST}\ \rho\ \tau} \qquad \textsc{TRunST}\quad \frac{\Xi, X \mid \Gamma \vdash e : \mathsf{ST}\ X\ \tau \qquad \Xi \vdash \tau}{\Xi \mid \Gamma \vdash \texttt{runST}\ \{e\} : \tau}$$

Lemma 2.1 (Context typing correct).

$$C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau') \wedge \Xi \mid \Gamma \vdash e : \tau \Rightarrow \Xi' \mid \Gamma' \vdash C[e] : \tau'$$

Proof. By induction on derivation $C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')$. □

Lemma 2.2 (Typing substitution).

$$\Xi \mid \Gamma, x : \tau' \vdash e : \tau \wedge \Xi \mid \Gamma \vdash e' : \tau' \Rightarrow \Xi \mid \Gamma \vdash e[e'/x] : \tau$$

Proof. By induction on derivation $\Xi \mid \Gamma, x : \tau' \vdash e : \tau$. □

Lemma 2.3 (Well-typed closed).

$$\Xi \mid \Gamma \vdash e : \tau \Rightarrow \mathsf{FV}(e) \subseteq \mathrm{dom}(\Gamma) \wedge \Xi \vdash \tau$$

Proof. By induction on derivation $\Xi \mid \Gamma \vdash e : \tau$. □

2.2 Well-typed contexts

We define well-typed contexts and their typing.

$$\begin{aligned} C ::= & [\,] \mid (C, e) \mid (e, C) \mid \texttt{inj}_i\, C \mid \texttt{fold}\, C \mid \texttt{unfold}\, C \mid \texttt{rec}\, f(x) = C \mid C\ e \mid v\ C \mid \Lambda\, C \mid C\ \_ \\ & \mid \pi_i\, C \mid \texttt{match}\, C\, \texttt{with}\, \texttt{inj}_i\, x \Rightarrow e_i\, \texttt{end} \mid (\texttt{match}\, e\, \texttt{with}\, \texttt{inj}_1\, x \Rightarrow C \mid \texttt{inj}_2\, x \Rightarrow e_2\, \texttt{end}) \\ & \mid (\texttt{match}\, e\, \texttt{with}\, \texttt{inj}_1\, x \Rightarrow e_1 \mid \texttt{inj}_2\, x \Rightarrow C\, \texttt{end}) \mid \texttt{if}\, C\, \texttt{then}\, e\, \texttt{else}\, e \\ & \mid \texttt{if}\, e\, \texttt{then}\, C\, \texttt{else}\, e \mid \texttt{if}\, e\, \texttt{then}\, e\, \texttt{else}\, C \\ & \mid C \circledcirc e \mid e \circledcirc C \mid \texttt{ref}(C) \mid\ !C \mid C \leftarrow e \mid v \leftarrow C \\ & \mid C == e \mid e == C \mid \texttt{bind}\, C\, \texttt{in}\, e \mid \texttt{bind}\, e\, \texttt{in}\, C \mid \texttt{return}\, C \mid \texttt{runST}\ \{C\} \end{aligned}$$

$$\boxed{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}$$

$$\textsc{CT-hole}\quad [\,] : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi \mid \Gamma; \tau)$$

$$\textsc{CT-rec}\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma', x : \tau', f : \tau' \to \tau''; \tau'')}{\texttt{rec}\, f(x) = C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' \to \tau'')}$$

$$\textsc{CT-app}_1\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau') \qquad \Xi \mid \Gamma \vdash e : \tau' \to \tau''}{e\; C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau'')}$$

$$\textsc{CT-app}_2\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' \to \tau'') \qquad \Xi' \mid \Gamma' \vdash e : \tau'}{C\; e : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau'')}$$

$$\textsc{CT-abs}\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi', X \mid \Gamma'; \tau')}{\Lambda\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \forall X.\, \tau')}$$

$$\textsc{CT-inst}\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \forall X.\, \tau') \qquad \Xi' \vdash \tau''}{C\; \_ : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau'[\tau''/X])}$$

$$\textsc{CT-fold}\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}{\texttt{fold}\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mu X.\, \tau')}$$

$$\textsc{CT-unfold}\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mu X.\, \tau')}{\texttt{unfold}\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau'[\mu X.\, \tau'/X])}$$

$$\textsc{CT-if}_1\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{B}) \qquad \Xi' \mid \Gamma' \vdash e_2 : \tau' \qquad \Xi' \mid \Gamma' \vdash e_3 : \tau'}{\texttt{if}\, C\, \texttt{then}\, e_2\, \texttt{else}\, e_3 : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}$$

$$\textsc{CT-if}_2\quad \frac{\Xi' \mid \Gamma' \vdash e_1 : \mathbb{B} \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau') \qquad \Xi' \mid \Gamma' \vdash e_3 : \tau'}{\texttt{if}\, e_1\, \texttt{then}\, C\, \texttt{else}\, e_3 : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}$$

$$\textsc{CT-if}_3\quad \frac{\Xi' \mid \Gamma' \vdash e_1 : \mathbb{B} \qquad \Xi' \mid \Gamma' \vdash e_2 : \tau' \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}{\texttt{if}\, e_1\, \texttt{then}\, e_2\, \texttt{else}\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}$$

$$\textsc{CT-prod}_1\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau') \qquad \Xi' \mid \Gamma' \vdash e : \tau''}{(C, e) : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' \times \tau'')}$$

$$\textsc{CT-proj}_1\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' \times \tau'')}{\pi_1\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}$$

$$\textsc{CT-prod}_2\quad \frac{\Xi' \mid \Gamma' \vdash e : \tau' \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau'')}{(e, C) : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' \times \tau'')}$$

$$\textsc{CT-proj}_2\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' \times \tau'')}{\pi_2\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau'')}$$

$$\textsc{CT-inj}_1\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}{\texttt{inj}_1\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' + \tau'')}$$

$$\textsc{CT-inj}_2\quad \frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau'')}{\texttt{inj}_2\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' + \tau'')}$$

$$\textsc{CT-natbinop}_1\quad \frac{\Xi' \mid \Gamma' \vdash e : \mathbb{N} \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{N})}{C \circledcirc e : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{N})}$$

$$\textsc{CT-natbinop}_2\quad \frac{\Xi' \mid \Gamma' \vdash e : \mathbb{N} \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{N})}{e \circledcirc C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{N})}$$

$$\textsc{CT-boolbinop}_1\quad \frac{\Xi' \mid \Gamma' \vdash e : \mathbb{N} \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{N})}{C \circledcirc e : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{B})}$$

$$\textsc{CT-boolbinop}_2\quad \frac{\Xi' \mid \Gamma' \vdash e : \mathbb{N} \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{N})}{e \circledcirc C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{B})}$$

CT-Match$_1$

$$\frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' + \tau'') \qquad \Xi' \mid \Gamma', x : \tau' \vdash e_1 : \tau_2 \qquad \Xi' \mid \Gamma', x : \tau'' \vdash e_2 : \tau_2}{\texttt{match}\, C\, \texttt{with}\, \texttt{inj}_1\, x \Rightarrow e_1 \mid \texttt{inj}_2\, x \Rightarrow e_2\, \texttt{end} : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau_2)}$$

CT-Match$_2$

$$\frac{\Xi' \mid \Gamma' \vdash e : \tau' + \tau'' \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma', x : \tau'; \tau_2) \qquad \Xi' \mid \Gamma', x : \tau'' \vdash e_2 : \tau_2}{\texttt{match}\, e\, \texttt{with}\, \texttt{inj}_1\, x \Rightarrow C \mid \texttt{inj}_2\, x \Rightarrow e_2\, \texttt{end} : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau_2)}$$

CT-Match$_3$

$$\frac{\Xi' \mid \Gamma' \vdash e : \tau' + \tau'' \qquad \Xi' \mid \Gamma', x : \tau' \vdash e_1 : \tau_2 \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma', x : \tau''; \tau_2)}{\texttt{match}\, e\, \texttt{with}\, \texttt{inj}_1\, x \Rightarrow e_1 \mid \texttt{inj}_2\, x \Rightarrow C\, \texttt{end} : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau_2)}$$

CT-New

$$\frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau') \qquad \Xi' \vdash \rho}{\texttt{ref}(C) : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{STRef}\ \rho\ \tau')}$$

CT-Deref

$$\frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{STRef}\ \rho\ \tau')}{!\,C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{ST}\ \rho\ \tau')}$$

CT-Gets$_1$

$$\frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{STRef}\ \rho\ \tau') \qquad \Xi' \mid \Gamma' \vdash e : \tau'}{C \leftarrow e : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{ST}\ \rho\ \mathbf{1})}$$

CT-Gets$_2$

$$\frac{\Xi' \mid \Gamma' \vdash e : \mathsf{STRef}\ \rho\ \tau' \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}{e \leftarrow C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{ST}\ \rho\ \mathbf{1})}$$

CT-Bind$_1$

$$\frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{ST}\ \rho\ \tau') \qquad \Xi' \mid \Gamma' \vdash e : \tau' \to (\mathsf{ST}\ \rho\ \tau'')}{\texttt{bind}\, C\, \texttt{in}\, e : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{ST}\ \rho\ \tau'')}$$

CT-Bind$_2$

$$\frac{\Xi' \mid \Gamma' \vdash e : \mathsf{ST}\ \rho\ \tau' \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau' \to (\mathsf{ST}\ \rho\ \tau''))}{\texttt{bind}\, e\, \texttt{in}\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{ST}\ \rho\ \tau'')}$$

CT-RefEq$_1$

$$\frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{STRef}\ \rho\ \tau') \qquad \Xi' \mid \Gamma' \vdash e : \mathsf{STRef}\ \rho\ \tau'}{C == e' : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{B})}$$

CT-RefEq$_2$

$$\frac{\Xi' \mid \Gamma' \vdash e : \mathsf{STRef}\ \rho\ \tau' \qquad C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{STRef}\ \rho\ \tau')}{e == C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathbb{B})}$$

CT-Return

$$\frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau') \qquad \Xi' \vdash \rho}{\texttt{return}\, C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \mathsf{ST}\ \rho\ \tau')}$$

CT-RunST

$$\frac{C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi', X \mid \Gamma'; \mathsf{ST}\ X\ \tau') \qquad \Xi' \vdash \tau}{\texttt{runST}\ \{C\} : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')}$$

2.3 Dynamics

We define two small step semantics to our language. They only differ on whether heap allocation is deterministic or not. We begin by the non-deterministic version, which we consider to be the actual semantics of the language.

We define the call-by-value (non-deterministic) reduction and non-deterministic effectful reduction, $\longrightarrow$ and $\rightsquigarrow$ respectively bellow. We define these relations through the usual way of defining evaluation contexts and head reductions.

Evaluation contexts:

$$\begin{aligned} K ::= & [\,] \mid (K, e) \mid (v, K) \mid \mathtt{inj}_i\, K \mid \mathtt{fold}\, K \mid \mathtt{unfold}\, K \mid K\ e \mid v\ K \mid K\ \_ \\ & \mid \pi_i\, K \mid \mathtt{match}\, K\, \mathtt{with}\, \mathtt{inj}_i\, x \Rightarrow e_i\ \mathtt{end} \mid \mathtt{if}\, K\, \mathtt{then}\, e\, \mathtt{else}\, e \\ & \mid K \circledcirc e \mid v \circledcirc K \mid \mathtt{ref}(K) \mid\, !\, K \mid K \leftarrow e \mid v \leftarrow K \\ & \mid K == e \mid v == K \mid \mathtt{bind}\, K\, \mathtt{in}\, e \mid \mathtt{bind}\, v\, \mathtt{in}\, K \mid \mathtt{return}\, K \mid \mathtt{runST}\ \{K\} \end{aligned}$$

Reduction: $\boxed{\langle h, e\rangle \longrightarrow \langle h', e'\rangle}$ and head step: $\boxed{\langle h, e\rangle \longrightarrow_h \langle h', e'\rangle}$

$$\frac{\langle h, e\rangle \longrightarrow_h \langle h', e'\rangle}{\langle h, K[e]\rangle \longrightarrow \langle h', K[e']\rangle} \qquad \langle h, \mathtt{unfold}\, (\mathtt{fold}\, v)\rangle \longrightarrow_h \langle h, v\rangle$$

$$\langle h, (\mathtt{rec}\, f(x) = e)\ v\rangle \longrightarrow_h \langle h, e[v, \mathtt{rec}\, f(x) = e/x, f]\rangle \qquad \langle h, (\Lambda\, e)\ \_\rangle \longrightarrow_h \langle h, e\rangle \qquad \langle h, \pi_i\, (v_1, v_2)\rangle \longrightarrow_h \langle h, v_i\rangle$$

$$\langle h, \mathtt{match}\, \mathtt{inj}_i\, v\, \mathtt{with}\, \mathtt{inj}_i\, x \Rightarrow e_i\ \mathtt{end}\rangle \longrightarrow_h \langle h, e_i[v/x]\rangle \qquad \langle h, \mathtt{if}\, \mathtt{true}\, \mathtt{then}\, e_1\, \mathtt{else}\, e_2\rangle \longrightarrow_h \langle h, e_1\rangle$$

$$\langle h, \mathtt{if}\, \mathtt{false}\, \mathtt{then}\, e_1\, \mathtt{else}\, e_2\rangle \longrightarrow_h \langle h, e_2\rangle \qquad \frac{n + n' = m}{\langle h, n + n'\rangle \longrightarrow_h \langle h, m\rangle} \qquad \frac{n - n' = m}{\langle h, n - n'\rangle \longrightarrow_h \langle h, m\rangle}$$

$$\frac{n \times n' = m}{\langle h, n * n'\rangle \longrightarrow_h \langle h, m\rangle} \qquad \frac{n = n'}{\langle h, n = n'\rangle \longrightarrow_h \langle h, \mathtt{true}\rangle} \qquad \frac{n \neq n'}{\langle h, n = n'\rangle \longrightarrow_h \langle h, \mathtt{false}\rangle}$$

$$\frac{n < n'}{\langle h, n < n'\rangle \longrightarrow_h \langle h, \mathtt{true}\rangle} \qquad \frac{n \not< n'}{\langle h, n < n'\rangle \longrightarrow_h \langle h, \mathtt{false}\rangle} \qquad \frac{\ell = \ell'}{\langle h, \ell == \ell'\rangle \longrightarrow_h \langle h, \mathtt{true}\rangle}$$

$$\frac{\ell \neq \ell'}{\langle h, \ell == \ell'\rangle \longrightarrow_h \langle h, \mathtt{false}\rangle} \qquad \frac{\langle h, v\rangle \rightsquigarrow \langle h', e\rangle}{\langle h, \mathtt{runST}\ \{v\}\rangle \longrightarrow_h \langle h', \mathtt{runST}\ \{e\}\rangle} \qquad \langle h, \mathtt{runST}\ \{\mathtt{return}\, v\}\rangle \longrightarrow_h \langle h, v\rangle$$

Effectful evaluation contexts:

$$\mathbb{K} ::= [\,] \mid \mathtt{bind}\, \mathbb{K}\, \mathtt{in}\, v$$

Effectful reduction: $\boxed{\langle h, v\rangle \rightsquigarrow \langle h', e\rangle}$ and effectful head step: $\boxed{\langle h, v\rangle \rightsquigarrow_h \langle h', e\rangle}$

$$\frac{\langle h, v\rangle \rightsquigarrow_h \langle h', e\rangle}{\langle h, \mathbb{K}[v]\rangle \rightsquigarrow \langle h', \mathbb{K}[e]\rangle} \qquad \langle h, \texttt{bind}\,(\texttt{return}\,v)\,\texttt{in}\,v'\rangle \rightsquigarrow_h \langle h, v'\ v\rangle$$

Alloc

$$\frac{\ell \notin \mathrm{dom}(h)}{\langle h, \texttt{ref}(v)\rangle \rightsquigarrow_h \langle h \uplus \{\ell \mapsto v\}\,, \texttt{return}\,\ell\rangle} \qquad \langle h \uplus \{\ell \mapsto v\}\,, !\,\ell\rangle \rightsquigarrow_h \langle h \uplus \{\ell \mapsto v\}\,, \texttt{return}\,v\rangle$$

$$\langle h \uplus \{\ell \mapsto v'\}\,, \ell \leftarrow v\rangle \rightsquigarrow_h \langle h \uplus \{\ell \mapsto v\}\,, \texttt{return}\,()\rangle$$

The deterministic reduction relations, $\rightarrow_d$ and $\rightsquigarrow_d$, are defined by the same inference rules as $\rightarrow$ and $\rightsquigarrow$, except that the only non-deterministic rule, Alloc, is replaced by a deterministic one:

det-Alloc

$$\frac{\ell = \mathit{min}(\mathit{Loc} \setminus \mathrm{dom}(h))}{\langle h, \texttt{ref}(v)\rangle \rightsquigarrow_h \langle h \uplus \{\ell \mapsto v\}\,, \texttt{return}\,\ell\rangle}$$

If $\rightharpoonup$ is a relation, we note $\rightharpoonup^n$ its iterated self-composition and $\rightharpoonup^*$ its reflexive and transitive closure.

Lemma 2.4 (Properties of reduction). *Let $\rightharpoonup$ be either $\rightarrow$ or $\rightarrow_d$, then:*

(1) $\langle h, K[e]\rangle \rightharpoonup^n \langle h', v\rangle$ if and only if

$$\exists m, h'', v'.\ 0 \le m \le n \wedge \langle h, e\rangle \rightharpoonup^m \langle h'', v'\rangle \wedge \langle h'', K[v']\rangle \rightharpoonup^{n-m} \langle h', v\rangle$$

(2) $\langle h, \texttt{runST}\ \{\texttt{bind}\,v\,\texttt{in}\,v'\}\rangle \rightharpoonup^n \langle h', w\rangle$ if and only if

$$\exists m, h'', w'.\ 0 \le m \le n \wedge \langle h, \texttt{runST}\ \{v\}\rangle \rightharpoonup^m \langle h'', w'\rangle \wedge$$
$$\langle h'', \texttt{runST}\ \{v'\ w'\}\rangle \rightharpoonup^{n-m} \langle h', w\rangle$$

(3) $\langle h, \texttt{runST}\ \{e\}\rangle \rightharpoonup^n \langle h', v\rangle$ if and only if

$$\langle h, \texttt{runST}\ \{e\}\rangle \rightharpoonup^{n-1} \langle h'', \texttt{runST}\ \{\texttt{return}\,v\}\rangle$$

As expected, $\rightarrow_d$ is deterministic, in particular:

(4) $\langle h, e\rangle \rightarrow_d^n \langle h', e'\rangle$ and $\langle h, e\rangle \rightarrow_d^n \langle h'', e''\rangle$ then

$$h' = h'' \wedge e' = e''$$

(5) $\langle h, e\rangle \rightarrow_d^* \langle h', v\rangle$ and $\langle h, e\rangle \rightarrow_d^* \langle h'', v'\rangle$

$$h' = h'' \wedge v = v'$$

(6) $\langle h, e\rangle \rightarrow_d^n \langle h', v\rangle$ and $\langle h, e\rangle \rightarrow_d^m \langle h'', v'\rangle$

$$h' = h'' \wedge v = v' \wedge n = m$$

Of course, the deterministic reduction relation is a subset of the non-deterministic one:

(7) $\rightarrow_d\ \subsetneq\ \rightarrow$ and $\rightsquigarrow_d\ \subsetneq\ \rightsquigarrow$.

Definition 2.5 (Contextual refinement).

$$\Xi \mid \Gamma \vDash e \preceq_{\mathsf{ctx}} e' : \tau \ \triangleq\ \Xi \mid \Gamma \vdash e : \tau\ \wedge\ \Xi \mid \Gamma \vdash e' : \tau\ \wedge$$
$$\forall h, h', C.\ \ C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\cdot \mid \cdot; \mathbf{1})\ \wedge\ (h, C[e])\downarrow\ \implies\ (h', C[e'])\downarrow$$

where

$$(h, e)\downarrow\ \triangleq\ \exists h', v.\ (h, e) \rightarrow^* (h', v)$$

3 IRIS

Iris was originally presented as a framework for higher-order (concurrent) separation logic, with built-in notions of invariants and weakest preconditions, useful for Hoare-style reasoning about higher-order concurrent imperative programs (Jung et al. 2015). Subsequently, Iris was extended with a notion of higher-order ghost state (Jung et al. 2016), i.e., the ability to store arbitrary higher-order separation-logic predicates in ghost variables. Recently, a simpler Iris *base logic* was defined and it was shown how that base logic suffices for defining the earlier built-in concepts of invariants, weakest preconditions, and higher-order ghost state (Krebbers et al. 2017a).

It is well-known that it is challenging to construct logical relations for languages with higher-order store because of the so-called type-world circularity (Ahmed 2004; Ahmed et al. 2002; Birkedal et al. 2011). Other recent work has shown how this challenge can be addressed by using the original Iris logic to define logical relations for languages with higher-order store (Krebbers et al. 2017b; Krogh-Jespersen et al. 2017). A key point is that Iris has enough logical features to give a direct inductive interpretation of the programming language types into Iris predicates. The binary relations in *loc. cit.* were defined using Iris's built-in notion of Hoare triple / weakest precondition. It turns out that this approach to representing logical relations is too abstract for our purposes: to prove the contextual refinements and equivalences for pure computations mentioned in the Introduction, we need to have more fine-grained control over how computations are related. In this paper we therefore use the Iris base logic to define a couple of new logical connectives which we use, instead of weakest preconditions, to define our binary logical relation. In this section we explain the bits we need and define the new logical connectives that we use in the next section to define our logical relation. We have to omit some details, which can be found in (Krebbers et al. 2017a).

3.1 Iris logic

The Iris logic is a higher-order logic, in which one can quantify over the Iris types κ:

$$\kappa ::= \mathbf{1} \mid \kappa \times \kappa \mid \kappa \to \kappa \mid \mathit{Expr} \mid \mathit{Val} \mid \mathbb{N} \mid \mathbb{B} \mid \kappa \overset{\text{fin}}{\rightharpoonup} \kappa \mid \mathsf{finset}(\kappa) \mid \mathit{Names} \mid \mathit{Monoid} \mid \mathit{iProp} \mid \ \ldots$$

Here *Expr* and *Val* are the types of syntactic expressions and values of STLang, $\kappa \rightharpoonup^{\text{fin}} \kappa$ is the type of finite functions, $\mathsf{finset}(\kappa)$ is the type of finite sets, $\mathbb{N}$ is the type of natural numbers, $\mathbb{B}$ is the type of booleans, *Names* is a type of ghost names, *Monoid* is a type of monoids, and *iProp* is the type of Iris propositions.

The grammar for Iris propositions P

$$\begin{aligned} P ::= {} & \top \mid \bot \mid P * P \mid P \mathrel{-\!\!*} P \mid P \land P \mid P \Rightarrow P \mid P \lor P \mid \forall x : \kappa.\ \Phi \mid \exists x : \kappa.\ \Phi \mid \\ & \triangleright P \mid \mu r.P \mid \checkmark(a) \mid \square P \mid\ \rtimes P \mid \Diamond P \mid \mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} P \mid \boxed{M}^{\gamma} \mid \boxed{P} \mid \gamma \mapsto \Phi \mid\ \ldots \end{aligned}$$

includes the usual connectives of higher-order separation logic ($\top$, $\bot$, $\land$, $\lor$, $\Rightarrow$, $*$, $-\!\!*$, $\forall$ and $\exists$). In this grammar Φ is an Iris predicate, i.e., a term of type $\kappa \to$ *iProp* (for appropriate κ). The intuition is that the propositions denote sets of resources and, as usual in separation logic, $P * P'$ holds for those resources which can be split into two disjoint parts, with one satisfying P and the other satisfying P'. Likewise, the proposition $P \mathrel{-\!\!*} P'$ describes those resources which satisfy that, if we combine it with a disjoint resource satisfied by P we get a resource satisfied by P'. In addition to these standard connectives there are some other interesting connectives, which we now explain.

The $\triangleright$ is a modality, called "later", which is used to guard recursively defined propositions: $\mu r.P$ is a well-defined guarded-recursive predicate if r appears under a $\triangleright$ in P. The $\triangleright$ modality is an abstraction of step-indexing (Appel and McAllester 2001; Appel et al. 2007; Dreyer et al. 2011). In terms of step-indexing $\triangleright P$ holds if P holds a step later; hence the name. In Iris it can be used to define weakest preconditions and to guard impredicative invariants to avoid self-referential paradoxes (Krebbers et al. 2017a); here we simply use it to take a guarded fixed point when we give the interpretation of recursive types, similarly to what was done in (Dreyer et al. 2011). For any proposition P, we have that $P \vdash \triangleright P$. The later modality commutes with all of the connectives of higher-order separation logic, including quantifiers.

Another modality of the Iris logic that we use is the "always" modality ($\square$). Intuitively, $\square P$ holds whenever P holds and is a duplicable assertion. In particular we have $(\square P) * (\square P) \dashv\vdash \square P$ where $\dashv\vdash$ is the logical equivalence of formulas. We say that P is *persistent* if $P \vdash \square P$. Persistent propositions are thus duplicable. The always modality is idempotent, $\square P \vdash \square \square P$, and also satisfies $\square P \vdash P$. The always modality (and by extension persistence) also commutes with all of the connectives of higher-order separation logic, including quantifiers.

The "naught" modality ($\rtimes$) is very similar to the always modality. Intuitively, $\rtimes P$ holds whenever P holds and asserts no ownership. In particular, if $P \vdash \rtimes Q$ then $P \vdash P * \rtimes Q$. We say that P is *plain* if $P \vdash \rtimes P$. Plain properties are those that assert no ownership of resources. A prime example here is reduciblity: $\mathsf{plain}(\langle h_1, e_1\rangle \rightarrow^* \langle h_2, e_2\rangle)$. The naught modality is idempotent, $\rtimes P \vdash \rtimes \rtimes P$, and we have $\rtimes P \vdash P$. The naught modality (and plainness by extension) also commutes with all of the connectives of the higher-order separation logic, including quantifiers, and also $\triangleright$, $\square$ and $\diamond$ (see below) modalities.

The "except zero" modality ($\diamond$) is another modality of Iris that we use. Intuitively $\diamond P$ holds if P holds for any step *but* the zeroth. The except zero modality is idempotent, $\diamond\diamond P \vdash \diamond P$, and also satisfies $P \vdash \diamond P$.

Another important modality in Iris is the "update" modality[1] ($\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}}$). The mask, $\mathcal{E} \in \{\top, \bot\}$, in $\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}}$ is to make sure that invariants (see below) are now opened in a nested fashion.[2] We drop the mask when it is $\top$ which indicates no invariant is open. Intuitively, the proposition $\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} P$ holds for resources that can be updated (allocated, deallocated, or changed), by opening invariants if necessary (and allowed by the mask), to resources that satisfy P, without violating the environment's knowledge or ownership of resources. We write $P \Rrightarrow_{\mathcal{E}} Q$ as a shorthand for $P \mathrel{-\!\!*} \mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} Q$. The update modality is idempotent, $\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} (\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} P) \dashv\vdash \mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} P$.

We have the following properties for Iris modalities:

$$\textsc{Except-zero-intro}\; P \vdash \diamond P \qquad \textsc{Later-intro}\; P \vdash \triangleright P \qquad \textsc{Update-intro}\; P \vdash \mathrel{|\!\!\Rrightarrow} P \qquad \textsc{Mod-mono}\; \frac{P \vdash Q}{\bowtie P \vdash \bowtie Q}$$

where $\bowtie$ is any modality ($\triangleright$, $\square$, $\rtimes$, $\diamond$, or $\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}}$).

Iris also features invariants, $\boxed{P}$, which are typically used to enforce that a proposition P holds for some state shared among several threads. In this paper we will use certain simple kinds of invariants and therefore we can use the following rules for allocating and opening invariants:

$$\textsc{Inv-alloc}\; P \Rrightarrow_{\mathcal{E}} \boxed{P} \qquad \textsc{Inv-open}\; \frac{P \Rrightarrow_{\bot} P * Q}{\boxed{P} \Rrightarrow_{\top} Q}$$

Notice that these are not the general rules for allocating and opening invariants in Iris. In general, the rule Inv-open should involve a $\triangleright$ to ensure soundness of the logic. However, the above rules do hold for the special kind of invariants that we use in this paper.[3] Invariants are persistent, $\boxed{P} \dashv\vdash \boxed{P} * \boxed{P}$. One of the most interesting aspects of plain propositions is how they interact with the update modality.

Lemma 3.1 (Update modality and plainness). *If P is plain and $Q \vdash P$ then $\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} Q \vdash \mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} ((\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} Q) * P)$*

This lemma basically says that if we can update resources to have Q which implies a plain proposition P then we can have P without actually having to perform the whole updating of the resources.

[1] In (Krebbers et al. 2017a) this modality is called the *fancy* update modality.

[2] In Iris invariants are named and these masks in general range over the set of invariant names and allow more fine-grained control over how invariants are opened. Here we only present this simpler version of invariants.

[3] The rules hold for invariants $\boxed{P}$ where P is *timeless*. For details see (Krebbers et al. 2017a).

$$\textsc{Ghost-Alloc}\ \frac{\checkmark a}{\Rrightarrow_{\mathcal{E}} \exists\gamma.\ \boxed{a}^{\gamma}} \qquad \textsc{Own-Valid}\ \ \boxed{a}^{\gamma} \vdash \checkmark(a) \qquad \textsc{Sharing}\ \ \boxed{a}^{\gamma} * \boxed{b}^{\gamma} \dashv\vdash \boxed{a \cdot b}^{\gamma}$$

Fig. 1. Rules for ghost resources in Iris

Resources in Iris are described using a kind of partial commutative monoids, and the user of the logic can introduce new monoids. The partiality comes from the fact that disjoint union of finite maps is partial. Undefinedness is treated by means of a validity predicate $\checkmark : \mathcal{M} \to iProp$, which, for a monoid $\mathcal{M}$, expresses which elements are valid / defined.

We write $\boxed{M}^{\gamma}$ to assert that a monoid instance named γ has contents M. We think of this assertion as a ghost variable γ with contents M. The relevant rules regarding ghost ownership are depicted in Figure 1.

This figure shows the rule Alloc used for allocating new instances of monoids (resources). It intuitively says that we can always allocate any monoid element a so long as it is *valid* ($\checkmark a$).

The last kind of Iris proposition that we use is called saved propositions $\gamma \Mapsto \Phi$. This is simply a mechanism for assigning a name γ to a predicate Φ. There are only three rules governing the use of saved propositions. We can allocate them (rule SavedPred-Alloc), they are persistent (rule SavedPred-Persistent) and the association of names to predicates is functional (rule SavedPred-Equiv).

$$\textsc{SavedPred-Alloc}\ \ \Rrightarrow_{\mathcal{E}} \exists\gamma.\ \gamma \Mapsto \Phi \qquad \textsc{SavedPred-Persistent}\ \ \gamma \Mapsto \Phi \dashv\vdash \gamma \Mapsto \Phi * \gamma \Mapsto \Phi \qquad \textsc{SavedPred-Equiv}\ \frac{\gamma \Mapsto \Phi * \gamma \Mapsto \Psi}{\triangleright \Phi(a) \vdash \triangleright \Psi(a)}$$

The later modality is used in rule SavedPred-Equiv as a guard to avoid self referential paradoxes (Krebbers et al. 2017a), which is not so surprising, after all, since saved propositions essentially allow us to store a predicate (something of type $\kappa \to iProp$) inside a proposition (something of type $iProp$).

Some useful monoids. In this paragraph, we describe a few monoids which are particularly useful and which we will use in the following. We do not give the full definitions of the monoids (those can be found in Krebbers et al. (2017a)), but focus instead on the properties which the elements of the monoids satisfy, shown in Figure 2. It also depicts the rules necessary for allocating and updating finite set, finset(A), and finite partial function, $A \xrightharpoonup{\text{fin}} M$, monoids. In these monoids, the monoid operation, $\cdot$, is *disjoint* union. The notation $a \mapsto b : A \xrightharpoonup{\text{fin}} B \triangleq \{(a, b)\}$ is a singleton finite partial function. Notice that these rules are stated only for monoids that we use in this work and not in Iris in its generality. For instance in the rule Auth-Included $\subseteq$ is a set relation and is defined for finite set and finite partial function monoids and not in general. The constructs $\bullet$ and $\circ$ are constructors of the so-called authoritative monoid $\textsc{Auth}(M)$. We read $\bullet\, a$ as *full a* and $\circ\, a$ as *fragment a*. We use the authoritative monoid to distribute ownership of fragments of a resource. The intuition is that $\bullet\, a$ is the authoritative knowledge of the full resource, think of it as being kept track of in a central location. This central location is the full part of the resource (see rule Auth-Included). The fragments, $\circ\, a$, can be shared (rule Frag-distributes) while the full part (the central location) should always remain unique (rule Full-Exclusive).

In addition to authoritative monoids, we also use the agreement monoid $\textsc{Ag}(M)$ and exclusive monoid $\textsc{Ex}(M)$. As the name suggests, the operation of the agreement monoid guarantees that $\text{ag}(a) \cdot \text{ag}(b)$ is invalid whenever $a \neq b$ (and otherwise it is idempotent; see rules Agree and Agreement-Valid). From the rule Agree it follows that the ownership of elements of $\textsc{Ag}(M)$ is persistent.

$$\boxed{\text{ag}(a)}^{\gamma} \dashv\vdash \boxed{\text{ag}(a) \cdot \text{ag}(a)}^{\gamma} \dashv\vdash \boxed{\text{ag}(a)}^{\gamma} * \boxed{\text{ag}(a)}^{\gamma}$$

Agree
$\mathrm{ag}(a) \cdot \mathrm{ag}(a) = \mathrm{ag}(a)$

Agreement-Valid
$\checkmark(\mathrm{ag}(a) \cdot \mathrm{ag}(b)) \dashv\vdash a = b$

Exclusive
$\not\checkmark(\mathrm{ex}(a) \cdot b)$

Auth-Included
$\bullet\, a \cdot \circ\, b \vdash a \subseteq b$

Frag-distributes
$\circ\, a \cdot \circ\, b = \circ\,(a \cdot b)$

Full-Exclusive
$\not\checkmark(\bullet\, a \cdot \bullet\, b)$

Auth-Alloc-Finset
$$\frac{h \cap a = \emptyset}{\boxed{\bullet\, h}^{\gamma} \Rrightarrow_{\mathcal{E}} \boxed{\bullet\,(h \uplus a) \cdot \circ\, a}^{\gamma}}$$

Auth-Alloc-Fpfn
$$\frac{\mathrm{dom}(h) \cap \mathrm{dom}(a) = \emptyset}{\boxed{\bullet\, h}^{\gamma} \Rrightarrow_{\mathcal{E}} \boxed{\bullet\,(h \uplus a) \cdot \circ\, a}^{\gamma}}$$

Fpfn-valid
$\checkmark(a) \dashv\vdash \forall x \in \mathrm{dom}(a).\ \checkmark(a(x))$

Fpfn-operation-success
$$a \cdot b = \begin{cases} a(x) & \text{if } x \in \mathrm{dom}(a) \wedge x \notin \mathrm{dom}(b) \\ a(x) \cdot b(x) & \text{if } x \in \mathrm{dom}(a) \cap \mathrm{dom}(b) \\ b(x) & \text{if } x \in \mathrm{dom}(b) \wedge x \notin \mathrm{dom}(a) \end{cases}$$

Auth-update-Fpfn
$$\boxed{\bullet\,(h \uplus (\ell \mapsto \mathrm{ex}(v_1))) \cdot \circ\, \ell \mapsto \mathrm{ex}(v_1)}^{\gamma} \Rrightarrow_{\mathcal{E}} \boxed{\bullet\,(h \uplus (\ell \mapsto \mathrm{ex}(v_2))) \cdot \circ\, \ell \mapsto \mathrm{ex}(v_2)}^{\gamma}$$

Fig. 2. Rules for selected monoid resources in Iris

The operation of the exclusive monoid never results in a valid element (rule Exclusive), enforcing that there can only be one instance of it owned.

Notice that the monoids can be nested. For instance, the update rule for finite partial functions (Auth-update-Fpfn) is defined for a monoid of the form $\textsc{Auth}(A \xrightharpoonup{\text{fin}} \mathrm{Ex}(M))$. From this rule we can easily show why the specialized update rule (Auth-update-Fpfn) holds.

Lemma 3.2 (Löb induction). *The principle of Löb induction:*

$$\textit{If } (\triangleright P \vdash P) \textit{ then } \vdash P$$

4 NEW DEFINITIONS IN IRIS

4.1 The naught modality and plainness

The precise definition of the modality *naught* is as follows:

$$(\rtimes P)\ n\ x \triangleq P\ n\ \varepsilon$$

where ε is the empty resource. This definition says that $\rtimes P$ holds for n steps for resource x if P holds n steps for the empty resource. In prose, P does not depend on any resources.

Lemma 4.1 (Basic properties of the naught modality). *The naught modality satisfies the following properties.*

(1) *If* $P \vdash \rtimes Q$ *then* $P \vdash P * \rtimes Q$
(2) *If* $P \vdash Q$ *then* $\rtimes P \vdash \rtimes Q$
(3) $\rtimes P \vdash P$
(4) $\rtimes P \vdash \rtimes \rtimes P$
(5) $\rtimes P \vdash \Box P$
(6) $\Box \rtimes P \dashv\vdash \rtimes \Box P$
(7) $(\forall x, \rtimes \Phi) \dashv\vdash \rtimes(\forall x, \Phi)$
(8) $(\exists x, \rtimes \Phi) \dashv\vdash \rtimes(\exists x, \Phi)$
(9) $\rtimes(P \wedge Q) \dashv\vdash \rtimes(P * Q)$
(10) $(\rtimes P) \wedge Q \dashv\vdash (\rtimes P) * Q$

(11) $\triangleright \rtimes P \dashv\vdash \rtimes \triangleright P$
(12) $\Diamond \rtimes P \dashv\vdash \rtimes \Diamond P$
(13) *If* $\rtimes P \vdash Q$ *then* $\rtimes P \vdash \rtimes Q$
(14) $\rtimes(P \land Q) \vdash (\rtimes P) \land (\rtimes Q)$
(15) $\rtimes(P \lor Q) \vdash (\rtimes P) \lor (\rtimes Q)$
(16) $\rtimes(P \Rightarrow Q) \vdash \rtimes P \Rightarrow \rtimes Q$
(17) $\rtimes(P * Q) \vdash \rtimes P * \rtimes Q$
(18) $\rtimes P \vdash \rtimes P * \rtimes P$
(19) $\rtimes(P \mathrel{-\!\!*} Q) \vdash \rtimes P \mathrel{-\!\!*} \rtimes Q$
(20) $\rtimes(P \Rightarrow Q) \vdash \rtimes P \Rightarrow \rtimes Q$
(21) $\rtimes(P \mathrel{-\!\!*} Q) \vdash \rtimes P \Rightarrow \rtimes Q$

A predicate P of Iris is called *plain* if it is equivalent to $\rtimes P$.

$$\mathsf{plain}(P) \triangleq P \vdash \rtimes P$$

Lemma 4.2 (Properties of plainness). *Plainness satisfies the following properties.*

(1) *plain*$(\rtimes P)$
(2) *If plain*(P) *and plain*(Q) *then plain*$(P \land Q)$
(3) *If plain*(P) *and plain*(Q) *then plain*$(P \lor Q)$
(4) *If plain*(P) *and plain*(Q) *then plain*$(P * Q)$
(5) *If for all* $(x : A)$ *plain*$(\Phi\ x)$ *then plain*$(\forall x : A.\ \Phi)$
(6) *If for all* $(x : A)$ *plain*$(\Phi\ x)$ *then plain*$(\exists x : A.\ \Phi)$
(7) *If plain*(P) *then plain*$(\triangleright P)$
(8) *If plain*(P) *then plain*$(\Diamond P)$
(9) *If plain*(P) *then plain*$(\Box P)$
(10) *If plain*(P) *then persistent*(P)
(11) *If plain*(P) *then* $\rtimes P \dashv\vdash P$
(12) *If plain*(P) *and* $P \vdash Q$ *then* $P \vdash \rtimes Q$
(13) *If plain*(P) *then* $P \land Q \dashv\vdash P * Q$
(14) *If plain*(P) *then* $P \dashv\vdash P * P$
(15) *If plain*(Q) *and* $P \vdash Q$ *then* $P \vdash Q * P$
(16) *If for any* x *we have plain*$(\Phi(x))$ *then* $(\forall x, \mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} \Phi(x)) \vdash \mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} (\forall x, \Phi(x))$
(17) *If* P *is plain and* $Q \vdash P$ *then* $\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} Q \vdash \mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} ((\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} Q) * P)$

For instance the fact that a program reduces $\langle h_1, e_1 \rangle \to \langle h_1, e_2 \rangle$ is a plain fact.

4.2 The future modality and if convergent (IC)

We define a mapping from heap to the monoid $(Loc \xrightarrow{\text{fin}} \mathrm{Ex}(Val))$ representing the heap:

$$\mathsf{excl}(h) = \{(\ell, \mathsf{ex}(v)) \mid (\ell, v) \in h\}$$

Before we define the logical relation in Iris, we define a construct called IC (if convergent).

$$\mathsf{IC}^{\gamma}\ e\ \{\!|n, v.\ Q|\!\}\triangleq \forall h_1, h_2, v, n.\ \ \langle h_1, e \rangle \to^{n} \langle h_2, v \rangle * \boxed{\bullet\ \mathsf{excl}(h_1)}^{\gamma} \mathrel{\equiv\{n\}\!\!\Rrightarrow\!\triangleright} \boxed{\bullet\ \mathsf{excl}(h_2)}^{\gamma} * Q$$

Where $(P \mathrel{\equiv\{n\}\!\!\Rrightarrow\!\triangleright} Q)$ is defined as $(P \mathrel{-\!\!*} (\mathrel{|\!\!\equiv\{n\}\!\!\Rrightarrow\!\triangleright} Q))$ and $(\mathrel{|\!\!\equiv\{n\}\!\!\Rrightarrow\!\triangleright})$ is the future modality, defined as:

$$\mathrel{|\!\!\equiv\{n\}\!\!\Rrightarrow\!\triangleright} \triangleq (\mathrel{|\!\!\Rrightarrow} \triangleright)^{n} \mathrel{|\!\!\Rrightarrow}$$

We simply omit n and/or v in $\mathsf{IC}^{\gamma}\ e\ \{\!|n, v.\ Q|\!\}$ whenever they do not appear in Q. Notice that the mask is $\top$ and therefore omitted.

Lemma 4.3 (Properties of the future modality). *The future modality, $\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright$, has the following properties:*

(1) $Q \vdash {\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q$
(2) If $P \vdash Q$ *then* ${\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} P \vdash {\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q$
(3) ${\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q \dashv\vdash {\mid\!\!\Rrightarrow}({\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q)$
(4) ${\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q \dashv\vdash {\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright}({\mid\!\!\Rrightarrow} Q)$
(5) $({\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q) * ({\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q') \vdash {\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright}(Q * Q')$
(6) $\triangleright^{n} \diamond P \vdash {\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} P$
(7) If $({\mid\!\!\Rrightarrow\!\{m-n\}\!\Rrightarrow\!\triangleright} P) * Q \vdash Q'$ *then* $({\mid\!\!\Rrightarrow\!\{m\}\!\Rrightarrow\!\triangleright} P) * ({\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q) \vdash ({\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q')$
(8) If P *is plain and* $Q \vdash P$ *then* $({\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q) \vdash ({\mid\!\!\Rrightarrow\!\{n\}\!\Rrightarrow\!\triangleright} Q) * \triangleright^{n} \diamond P$

where $\dashv\vdash$ *is equivalence of logical formulas. Here,* $m - n = 0$ *when* $n > m$.

Notice that in the following lemma the statements are not always the strongest provable (e.g., the case 7 could have 2 $\triangleright$ modalities). They are however enough for our purposes.

Lemma 4.4 (Properties of IC). *The IC predicate satisfies the following properties:*

(1) $IC^{\gamma}\ e\ \{\!|n, v.\ Q|\!\} * (\forall k, w.\ (Q\ k\ w) -\!\!* IC^{\gamma}\ K[w]\ \{\!|m, v.\ Q'\ (m+k)\ v|\!\}) \vdash IC^{\gamma}\ K[e]\ \{\!|m, v.\ Q'|\!\}$
(2) ${\mid\!\!\Rrightarrow}(Q\ 0\ w) \vdash IC^{\gamma}\ w\ \{\!|n, v.\ Q|\!\}$
(3) $(\forall n, v.\ (P\ n\ v) \Rrightarrow (Q\ n\ v)) * IC^{\gamma}\ e\ \{\!|n, v.\ P|\!\} \vdash IC^{\gamma}\ e\ \{\!|n, v.\ Q|\!\}$
(4) ${\mid\!\!\Rrightarrow} IC^{\gamma}\ e\ \{\!|n, v.\ Q|\!\} \vdash IC^{\gamma}\ e\ \{\!|n, v.\ Q|\!\}$
(5) $IC^{\gamma}\ e\ \{\!|n, v.\ {\mid\!\!\Rrightarrow} Q|\!\} \vdash IC^{\gamma}\ e\ \{\!|n, v.\ Q|\!\}$
(6) $(\forall h.\ \langle h, e\rangle \rightarrow \langle h, e'\rangle) * \triangleright IC^{\gamma}\ e'\ \{\!|n, v.\ Q\ (n+1)\ v|\!\} \vdash IC^{\gamma}\ e\ \{\!|n, v.\ Q|\!\}$
(7) $\triangleright(\forall \ell.\ \boxed{\circ\,\ell \mapsto ex(v)}^{\gamma} \Rrightarrow Q\ 2\ \ell) \vdash IC^{\gamma}\ \mathtt{runST}\ \{\mathtt{ref}(v)\}\ \{\!|n, w.\ Q|\!\}$
(8) $\triangleright \boxed{\circ\,\ell \mapsto ex(v)}^{\gamma} * \triangleright(\boxed{\circ\,\ell \mapsto ex(v)}^{\gamma} \Rrightarrow Q\ 2\ v) \vdash IC^{\gamma}\ \mathtt{runST}\ \{!\,\ell\}\ \{\!|n, w.\ Q|\!\}$
(9) $\triangleright \boxed{\circ\,\ell \mapsto ex(v')}^{\gamma} * \triangleright(\boxed{\circ\,\ell \mapsto ex(v)}^{\gamma} \Rrightarrow Q\ 2\ ())\vdash IC^{\gamma}\ \mathtt{runST}\ \{\ell \leftarrow v\}\ \{\!|n, w.\ Q|\!\}$
(10) $IC^{\gamma}\ \mathtt{runST}\ \{e\}\ \{\!|n, v.\ Q|\!\} * \Big(\forall k, w.\ (Q\ k\ w) -\!\!*$
$IC^{\gamma}\ \mathtt{runST}\ \{\mathbb{K}[\mathtt{return}\, w]\}\ \{\!|m, v.\ Q'\ (m+k-1)\ w|\!\}\Big) \vdash IC^{\gamma}\ \mathtt{runST}\ \{\mathbb{K}[e]\}\ \{\!|m, v.\ Q'|\!\}$

The cases (1) and (2) above show that IC is a monad in the same way that WP (weakest precondition) is a monad.

Akin to Hoare triples being defined using the weakest precondition, we define IC triples as follows:

$$\{\!|P|\!\}\ e\ \{\!|n, v.\ Q|\!\}_{\gamma} \triangleq \square(P -\!\!* \mathsf{IC}^{\gamma}\ e\ \{\!|n, v.\ Q|\!\})$$

5 THE LOGICAL RELATION

We define the logical relation in two stages. We define a value relation $[\![\tau]\!]_{\Delta} : (Val \times Val) \longrightarrow iProp$ and an expression relation $\mathcal{E}\cdot : ((Val \times Val) \longrightarrow iProp) \longrightarrow (Expr \times Expr) \longrightarrow iProp$ which given a value relation constructs an expression relation. Here

$$\Delta : Tvar \longrightarrow (((Val \times Val) \longrightarrow iProp) \times \{\tau \in Types \mid \mathsf{FV}(\tau) = \emptyset\})$$

is map from type variable to interpretations of types and closed types.

$$
\begin{aligned}
[\![\Xi \vdash X]\!]_\Delta &\triangleq (\Delta(X)).1 \\
[\![\Xi \vdash \mathbf{1}]\!]_\Delta(v, v') &\triangleq v = v' = () \\
[\![\Xi \vdash \mathbb{B}]\!]_\Delta(v, v') &\triangleq v = v' \in \{\mathtt{true}, \mathtt{false}\} \\
[\![\Xi \vdash \mathbb{N}]\!]_\Delta(v, v') &\triangleq v = v' \in \mathbb{N} \\
[\![\Xi \vdash \tau \times \tau]\!]_\Delta(v, v') &\triangleq \exists w_1, w_2, w_1', w_2'.\ v = (w_1, w_2) \wedge v' = (w_1', w_2') \wedge \\
&\quad\ [\![\Xi \vdash \tau]\!]_\Delta(w_1, w_1') \wedge [\![\Xi \vdash \tau']\!]_\Delta(w_2, w_2') \\
[\![\Xi \vdash \tau + \tau']\!]_\Delta(v, v') &\triangleq (\exists w, w'.\ v = \mathtt{inj}_1\, w \wedge v' = \mathtt{inj}_1\, w' \wedge [\![\Xi \vdash \tau]\!]_\Delta(w, w')) \vee \\
&\quad\ (\exists w, w'.\ v = \mathtt{inj}_2\, w \wedge v' = \mathtt{inj}_2\, w' \wedge [\![\Xi \vdash \tau']\!]_\Delta(w, w')) \\
[\![\Xi \vdash \tau \to \tau']\!]_\Delta(v, v') &\triangleq \Box \left(\forall (w, w').\ [\![\Xi \vdash \tau]\!]_\Delta(w, w') \Rightarrow \mathcal{E}\, [\![\Xi \vdash \tau]\!]_\Delta\, (v\ w, v'\ w')\right) \\
[\![\Xi \vdash \forall X.\, \tau]\!]_\Delta(v, v') &\triangleq \Box \Big(\forall f, \tau'.\ \mathsf{FV}(\tau) = \emptyset \wedge \mathsf{persistent}(f) \Rightarrow \\
&\quad\ \mathcal{E}\, [\![\Xi, X \vdash \tau]\!]_{\Delta, X \mapsto (f, \tau')}\, (v\ \_, v'\ \_)\Big) \\
[\![\Xi \vdash \mu X.\, \tau]\!]_\Delta(v, v') &\triangleq \mu f.\ \exists w, w'.\ v = \mathtt{fold}\, w \wedge v' = \mathtt{fold}\, w' \wedge \\
&\quad\ \triangleright [\![\Xi, X \vdash \tau]\!]_{\Delta, X \mapsto (f, \mathsf{close}(\Delta, \mu X.\, \tau))}(w, w') \\
[\![\Xi \vdash \mathsf{STRef}\ \rho\ \tau]\!]_\Delta(v, v') &\triangleq \exists \ell, \ell', \gamma_{bij}, \gamma_{rel}, \gamma_{pred}.\ v = \ell \wedge v' = \ell' \wedge \boxed{\circ\, \mathsf{close}(\Delta, \rho) \mapsto \mathsf{ag}(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}} * \\
&\quad\ \boxed{\circ\, \mathsf{ag}(\ell, \ell')}^{\gamma_{bij}} * \boxed{\circ\, (\ell, \ell') \mapsto \mathsf{ag}(\gamma_{pred})}^{\gamma_{rel}} * \gamma_{pred} \Mapsto [\![\Xi \vdash \tau]\!]_\Delta \\
[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau]\!]_\Delta(v, v') &\triangleq \forall \gamma_h, \gamma_h', h_1'. \\
&\quad\ \Big\{\!\!\Big\{ \boxed{\bullet\, \mathsf{excl}(h_1')}^{\gamma_h'} * \mathsf{regions} * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma_h') \Big\}\!\!\Big\} \\
&\quad\quad \mathtt{runST}\ \{v\} \\
&\quad\ \Big\{\!\!\Big\{ w.\ (h_1', \mathtt{runST}\ \{v'\}) \Downarrow^{\gamma_h'}_{[\![\Xi \vdash \tau]\!]_\Delta(w, \cdot)} * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma_h') \Big\}\!\!\Big\}_{\gamma_h}
\end{aligned}
$$

$$
\mathcal{E}\, \Phi(e, e') \triangleq \forall \gamma_h, \gamma_h', h_1'.\ \Big\{\!\!\Big\{ \boxed{\bullet\, \mathsf{excl}(h_1')}^{\gamma_h'} * \mathsf{regions} \Big\}\!\!\Big\}\ e\ \Big\{\!\!\Big\{ w.\ (h_1', e') \Downarrow^{\gamma_h'}_{\Phi(w, \cdot)} \Big\}\!\!\Big\}_{\gamma_h}
$$

$$
(h', e') \Downarrow^{\gamma}_{\Phi} \triangleq \exists h_2', v'.\ \langle h, e' \rangle \to_d^* \langle h_2', v' \rangle * \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma_h'} * \Phi(v')
$$

Where:

$$
\mathsf{close}(\Delta, \rho) \triangleq \rho[(\Delta \vec{X}).2 / \vec{X}]
$$

closes the (open) type ρ using the closed types stored in Δ,

$$
\mathsf{bijection}(g) \triangleq \text{“}g\textit{ is the graph of a bijection.”}
$$

We now define the regions and the region$(\rho, \gamma_h, \gamma'_h)$ predicates. They make use of the two following resource algebras to keep track of the locations associated to each heap regions:

$$\begin{aligned} Hrel &\triangleq (Loc \times Loc) \xrightarrow{\text{fin}} (\textsc{Ag}(Names)) \\ Hbij &\triangleq \mathcal{P}(Loc \times Loc) \end{aligned}$$

$$\begin{aligned} \text{region}(\rho, \gamma_h, \gamma'_h) \triangleq\ & \exists r : Hrel, \gamma_{bij}, \gamma_{rel}. \\ & \boxed{\circ\, \rho \mapsto \text{ag}(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}} * \boxed{\bullet\, r}^{\gamma_{rel}} * \\ & \mathop{\Large *}_{(\ell, \ell') \mapsto \text{ag}(\gamma_{pred}) \in r} \left(\begin{array}{l} \exists P : (Val \times Val) \to iProp), v, v'.\ \boxed{\circ\, \ell \mapsto \text{ex}(v)}^{\gamma_h} * \\ \qquad \boxed{\circ\, \ell' \mapsto \text{ex}(v')}^{\gamma'_h} * \gamma_{pred} \Mapsto P * \triangleright P(v, v') \end{array} \right) \end{aligned}$$

$$\text{regions} \triangleq \boxed{\exists M.\ \boxed{\bullet\, M : \text{Reg}}^{\gamma_{reg}} * \mathop{\Large *}_{\rho \mapsto \text{ag}(\gamma_{bij}, \gamma_{rel}) \in M} \left(\begin{array}{l} \exists g : \text{finset}(Loc \times Loc), r : (Loc \times Loc) \xrightarrow{\text{fin}} (\textsc{Ag}(Names)). \\ \boxed{\bullet\, g}^{\gamma_{bij}} * \text{bijection}(g) * \boxed{\circ\, r}^{\gamma_{rel}} * g = \text{dom}(r) \end{array} \right)}$$

Ag is the agreement monoid, γ_{reg} is a fixed "global" resource name. Notice that due to the use of invariants the regions is persistent.

The semantics of the term environment $(\mathcal{G}[\![\Xi \vdash \Gamma]\!]_\Delta)$ is defined as follows:

$$\begin{aligned} \mathcal{G}[\![\Xi \vdash \cdot]\!]_\Delta(\vec{v}, \vec{v'}) &\triangleq \top \\ \mathcal{G}[\![\Xi \vdash \Gamma, x : \tau]\!]_\Delta(w\vec{v}, w'\vec{v'}) &\triangleq \mathcal{G}[\![\Xi \vdash \tau]\!]_\Delta(w, w') * [\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v'}) \end{aligned}$$

The logical relation for open terms is defined as follows:

$$\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau \triangleq \forall \Delta, \vec{v}, \vec{v'}.\ \mathcal{G}[\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v'}) \Rightarrow \mathcal{E}[\![\Xi \vdash \tau]\!]_\Delta(e[\vec{v}/\vec{x}], e'[\vec{v'}/\vec{x}])$$

5.1 Monoid lemmas

Lemma 5.1 (Creating region predicate).

$$\forall \gamma, \gamma'_h.\ \text{regions} \Rrightarrow \exists \rho.\ \text{regions} * \text{region}(\rho, \gamma_h, \gamma'_h)$$

Proof. Let γ_h and γ'_h and by unfolding the regions predicate and opening the invariant, let M such that

(1) $\boxed{\bullet\, M}^{\gamma_{reg}}$

(2) $\mathop{*}_{\rho \mapsto \text{ag}(\gamma_{bij}, \gamma_{rel}) \in M} \left(\exists g, r.\ \text{finite}(g) \land \boxed{\bullet\, g}^{\gamma_{bij}} * \text{bijection}(g) * \boxed{\circ\, r}^{\gamma_{rel}} * g = \text{dom}(r) \right)$.

We have to show $\mathrel{|\!\Rrightarrow}_{\perp} \exists \rho.$ regions $*$ region$(\rho, \gamma_h, \gamma'_h)$. Now, allocate the empty set and the empty partial map under two new monoid names. We own the following new resources:

(3) $\boxed{\bullet\, \emptyset}^{\gamma_{bij}}$

(4) $\boxed{\bullet\, \emptyset}^{\gamma_{rel}}$

(5) $\boxed{\circ\, \emptyset}^{\gamma_{rel}}$

Since the set of closed types is infinite, we can choose $\rho \notin \text{dom}(M)$. Note $M' \triangleq M \uplus [\rho \mapsto \text{ag}(\gamma_{bij}, \gamma_{rel})]$. We can update (1) into

(6) $\boxed{\bullet\, M'}^{\gamma_{reg}}$

(7) $\boxed{\circ\, \rho \mapsto \text{ag}((\gamma_{bij}, \gamma_{rel}))}^{\gamma_{reg}}$

Consuming (2), (3) and (5), we can we can prove

(8) $\mathop{\ast}_{\rho\mapsto \mathsf{ag}(\gamma_{bij},\gamma_{rel})\in M'} \Big(\exists g, r.\ \mathsf{finite}(g) \land \boxed{\bullet\, g}^{\gamma_{bij}} * \mathsf{bijection}(g) * \boxed{\circ\, r}^{\gamma_{rel}} * g = \mathrm{dom}(r)\Big)$.

Hence we can recover the region predicate. Finally, from (7) and (4) we can prove $\mathsf{regions}(\rho, \gamma_h, \gamma'_h)$ with $r = \emptyset$ since the iterated separation product ranges over the empty set. □

Let

$$\mathsf{openregion}(\rho, r, r', \gamma_h, \gamma'_h) \triangleq \exists \gamma_{bij}, \gamma_{rel}.\ \boxed{\circ\, \rho \mapsto \mathsf{ag}(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}} * \boxed{\bullet\, r}^{\gamma_{rel}} * \mathop{\ast}_{(\ell,\ell')\mapsto \mathsf{ag}(\gamma_{pred})\in r'} (\exists v, v', P.\ \boxed{\circ\, \ell \mapsto \mathsf{ex}(v)}^{\gamma_h} * \boxed{\circ\, \ell' \mapsto \mathsf{ex}(v')}^{\gamma'_h} * \gamma_{pred} \Mapsto P * \triangleright P(v, v'))$$

Lemma 5.2 (Properties of open region).

The open region predicate satisfies the following:

$$\mathsf{region}(\rho, \gamma_h, \gamma'_h) \dashv\vdash \exists r.\ \mathsf{openregion}(\rho, r, r, \gamma_h, \gamma'_h) \qquad (1)$$

Lemma 5.3 (New location).

$\forall \rho, \gamma_{bij}, \gamma_{rel}, \ell, \ell', v, v', r, \gamma_h, \gamma'_h, P.$

$\boxed{\circ\, \rho \mapsto ag((\gamma_{bij}, \gamma_{rel}))}^{\gamma_{reg}} * \boxed{\circ\, \ell \mapsto ex(v)}^{\gamma_h} * \boxed{\circ\, \ell' \mapsto ex(v')}^{\gamma'_h} * \mathsf{regions} * \mathsf{region}(\rho, \gamma_h, \gamma'_h) \Rrightarrow \exists \gamma_{pred}.$

$\mathsf{openregion}(\rho, r \uplus [(\ell, \ell') \mapsto ag(\gamma_{pred})], r, \gamma_h, \gamma'_h) * \boxed{\circ\, ag((\ell, \ell'))}^{\gamma_{bij}} * \boxed{\circ\, (\ell, \ell') \mapsto ag(\gamma_{pred})}^{\gamma_{rel}} *$

$\boxed{\circ\, \ell \mapsto ex(v)}^{\gamma_h} * \boxed{\circ\, \ell' \mapsto ex(v')}^{\gamma'_h} * \gamma_{pred} \Mapsto P$

Proof. Assume that we have:

(1) $\rho, \gamma_{bij}, \gamma_{rel}, \ell, \ell', v, v', r, \gamma_h, \gamma'_h, P$
(2) $\mathsf{regions}$
———–{ spatial resources } ———–
(3) $\boxed{\circ\, \rho \mapsto \mathsf{ag}(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}}$
(4) $\boxed{\circ\, \ell \mapsto \mathsf{ex}(v)}^{\gamma_h} * \boxed{\circ\, \ell' \mapsto \mathsf{ex}(v')}^{\gamma'_h}$
(5) $\mathsf{region}(\rho, \gamma_h, \gamma'_h)$

By unfolding of (5) we obtain:

(6) $\gamma'_{bij}, \gamma'_{rel}$
———–{ spatial resources } ———–
(7) $\boxed{\circ\, \rho \mapsto \mathsf{ag}(\gamma'_{bij}, \gamma_{rel})'}^{\gamma_{reg}}$
(8) $\boxed{\bullet\, r}^{\gamma_{rel}}$
(9) $\mathop{\ast}_{(\ell,\ell')\mapsto \mathsf{ag}(\gamma_{pred})\in r'} (\exists P, v, v'.\ \boxed{\circ\, \ell \mapsto \mathsf{ex}(v)}^{\gamma_h} * \boxed{\circ\, \ell' \mapsto \mathsf{ex}(v')}^{\gamma'_h} * \gamma_{pred} \Mapsto P * \triangleright P(v, v'))$

The agreement monoid property, (3) and (7) says that $\gamma_{bij} = \gamma'_{bij}$ and $\gamma_{rel} = \gamma'_{rel}$. By unfolding regions and opening the invariant we obtain:

(10) M
———–{ spatial resources } ———–
(11) $\boxed{\bullet\, M}^{\gamma_{reg}}$
(12) $\mathop{\ast}_{\rho\mapsto \mathsf{ag}(\gamma_{bij},\gamma_{rel})\in M} \Big(\exists g, r.\ \mathsf{finite}(g) \land \boxed{\bullet\, g}^{\gamma_{bij}} * \mathsf{bijection}(g) * \boxed{\circ\, r}^{\gamma_{rel}} * g = \mathrm{dom}(r)\Big)$

And now we have to show

$$\Rrightarrow_{\bot} \mathsf{openregion}(\rho, r \uplus [(\ell,\ell') \mapsto \mathsf{ag}(\gamma_{pred})], r, \gamma_h, \gamma_h') * \boxed{\circ\, \mathsf{ag}((\ell,\ell'))}^{\gamma_{bij}} * \boxed{\circ\, (\ell,\ell') \mapsto \mathsf{ag}(\gamma_{pred})}^{\gamma_{rel}} * \gamma_{pred} \Mapsto P$$

By (4), (8) and (9) we have that:

(13) $\forall \ell_1.\ (\ell, \ell_1) \notin dom(r)$
(14) $\forall \ell_0.\ (\ell_0, \ell) \notin dom(r)$
(15) $(\ell, \ell') \notin dom(r)$

By (12) with (2), (14) and (15) one can easily show that we can extend g with (ℓ, ℓ') to obtain $\boxed{\circ\, \mathsf{ag}(\ell,\ell')}^{\gamma_{bij}}$. By allocating a saved predicate we get we can obtain:

(16) γ_{pred}
(17) $\gamma_{pred} \Mapsto P$

Finally, by (8) and (15) we can extend r to obtain $\boxed{\circ\, (\ell,\ell') \mapsto \mathsf{ag}(\gamma_{pred})}^{\gamma_{rel}}$. We finish the proof by Lemma 5.8 with (4). □

Lemma 5.4 (Duplicate region to monoid-names).

$$\boxed{\circ\, \rho \mapsto ag(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}} \dashv\vdash \boxed{\circ\, \rho \mapsto ag(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}} * \boxed{\circ\, \rho \mapsto ag(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}}$$

Proof. Follows from agreement. □

Lemma 5.5 (Duplicate locations to relation).

$$\forall \ell, \ell', P, \gamma_{rel}.\ \boxed{\circ\, (\ell,\ell') \mapsto ag(\gamma_{pred})}^{\gamma_{rel}} \dashv\vdash \boxed{\circ\, (\ell,\ell') \mapsto ag(\gamma_{pred})}^{\gamma_{rel}} * \boxed{\circ\, (\ell,\ell') \mapsto ag(\gamma_{pred})}^{\gamma_{rel}}$$

Proof. Follows from agreement. □

Lemma 5.6 (Duplicate bijection of locations).

$$\forall \ell, \ell', \gamma_{bij}.\ \boxed{\circ\, ag(\ell,\ell')}^{\gamma_{bij}} \dashv\vdash \boxed{\circ\, ag(\ell,\ell')}^{\gamma_{bij}} * \boxed{\circ\, ag(\ell,\ell')}^{\gamma_{bij}}$$

Proof. Follows from agreement. □

Lemma 5.7 (Get points-to for region).

$$\begin{aligned}
&\forall \rho, \gamma_{bij}, \gamma_{rel}, \gamma_{reg}, \ell, \ell', \gamma_{pred}, r, \gamma, \gamma_h'.\\
&\quad \boxed{\circ\, \rho \mapsto ag(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}} * \boxed{\circ\, (\ell,\ell') \mapsto ag(\gamma_{pred})}^{\gamma_{rel}} * \mathsf{region}(\rho, \gamma_h, \gamma_h')\\
\Rrightarrow &\quad \exists r', v, v', P.\ r = r' \uplus [(\ell,\ell') \mapsto ag(\gamma_{pred})] * \mathsf{openregion}(\rho, r, r', \gamma_h, \gamma_h') *\\
&\quad \boxed{\circ\, \ell \mapsto ex(v)}^{\gamma_h} * \boxed{\circ\, \ell' \mapsto ex(v')}^{\gamma_h'} * \gamma_{pred} \Mapsto P * \triangleright P(v, v')
\end{aligned}$$

Proof. Follows simply from agreement on γ_{rel} and splitting of $\circledast$. □

Lemma 5.8 (Return points-to for region).

$$\begin{aligned}
&\forall \rho, \gamma_{bij}, \gamma_{rel}, \gamma_{reg}, \gamma_{pred} \ell, \ell', P, r, \gamma_h, \gamma_h', v, v'.\\
&\quad \boxed{\circ\, \rho \mapsto ag(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}} * \boxed{\circ\, (\ell,\ell') \mapsto ag(\gamma_{pred})}^{\gamma_{rel}} * \mathsf{openregion}(\rho, r \uplus [(\ell,\ell') \mapsto ag(\gamma_{pred})], r, \gamma_h, \gamma_h') *\\
&\quad \boxed{\circ\, \ell \mapsto ex(v)}^{\gamma_h} * \boxed{\circ\, \ell' \mapsto ex(v')}^{\gamma_h'} * \gamma_{pred} \Mapsto P * \triangleright P(v, v')\\
\Rrightarrow &\quad \mathsf{region}(\rho, r \uplus [(\ell,\ell') \mapsto ag(\gamma_{pred})], r \uplus [(\ell,\ell') \mapsto ag(\gamma_{pred})], \gamma_h, \gamma_h')
\end{aligned}$$

Proof. Follows simply from agreement on γ_{rel} and combining of $\boldsymbol{\ast}$ with $\boxed{\circ\, \ell \mapsto \mathsf{ex}(v)}^{\gamma_h} \ast \boxed{\circ\, \ell' \mapsto \mathsf{ex}(v')}^{\gamma'_h}$ $\ast \gamma_{pred} \Rrightarrow P \ast \triangleright P(v, v')$. □

Lemma 5.9 (Shrinking the interpretation of types). *Suppose* $\Xi \vdash \tau$, *then*

$$[\![\Xi, X \vdash \tau]\!]_{\Delta, X \mapsto (f, \tau')} \dashv\vdash [\![\Xi \vdash \tau]\!]_{\Delta}$$

Proof. By induction on the structure of τ. □

Lemma 5.10 (Substitution of type variable). *The following two substitution lemmas hold for the defined logical relation.*

(a) $[\![\Xi \vdash \tau[\tau'/X]]\!]_{\Delta} \dashv\vdash [\![\Xi, X \vdash \tau]\!]_{\Delta, X \mapsto (f, \mathsf{close}(\tau', \Delta))}$
(b) $\mathcal{E}\,[\![\Xi \vdash \tau[\tau'/X]]\!]_{\Delta} \dashv\vdash \mathcal{E}\,[\![\Xi, X \vdash \tau]\!]_{\Delta, X \mapsto (f, \mathsf{close}(\tau', \Delta))}$

where $f = [\![\Xi \vdash \tau']\!]_{\Delta}$

Proof. Case (a) follows by induction on the structure of τ. Case (b) follows trivially from Case (a). □

Lemma 5.11 (Bind rule for the expression relation). *Suppose*

(a) $\mathcal{E}\,[\![\Xi' \vdash \tau]\!]_{\Delta'}(e, e')$,
(b) $\forall v, v', [\![\Xi' \vdash \tau]\!]_{\Delta'}(v, v') \Rightarrow \mathcal{E}\,[\![\Xi \vdash \tau']\!]_{\Delta}(K[v], K'[v'])$;

then

$$\mathcal{E}\,[\![\Xi \vdash \tau']\!]_{\Delta}(K[e], K'[e']).$$

Proof. Let us assume that we have

(1) γ, γ'
(2) regions
(3) h'_1
(4) $\boxed{\bullet\, h'_1}^{\gamma'}$

We have to show:

$$\mathsf{IC}^{\gamma}\, K[e] \left\{\!\!\left| v.\ \exists h'_2, v'.\ \left\langle h'_1, K'[e'] \right\rangle \to_d^* \left\langle h'_2, v' \right\rangle \ast \boxed{\bullet\, h'_2}^{\gamma'} \ast [\![\Xi \vdash \tau']\!]_{\Delta}(v, v') \right|\!\!\right\}$$

using (4) and (2) with assumption (a), we can use the bind rule for IC (case 1 of Lemma 4.4). We get

(5) h'_3, w, w'
(6) $\boxed{\bullet\, h'_3}^{\gamma'}$
(7) $\left\langle h'_1, e' \right\rangle \to_d^* \left\langle h'_3, w' \right\rangle$
(8) $[\![\Xi' \vdash \tau]\!]_{\Delta'}(w, w')$

and now we have to show:

$$\mathsf{IC}^{\gamma}\, K[w] \left\{\!\!\left| v.\ \exists h'_2, v'.\ \left\langle h'_1, K'[e'] \right\rangle \to_d^* \left\langle h'_2, v' \right\rangle \ast \boxed{\bullet\, h'_2}^{\gamma'} \ast [\![\Xi \vdash \tau']\!]_{\Delta}(v, v') \right|\!\!\right\}$$

Using (8), (6), (2), assumption (b) and monotonocity of IC (Lemma 4.4 case: 3) we get

(9) h'_2, v, v'
(10) $\boxed{\bullet\, h'_2}^{\gamma'}$
(11) $\left\langle h'_3, K'[w'] \right\rangle \to_d^* \left\langle h'_2, v' \right\rangle$
(12) $[\![\Xi \vdash \tau']\!]_{\Delta}(v, v')$

and we have to show

$$\mathrel{|\!\!\Rrightarrow} \exists h_2', v'.\ \left\langle h_1', K'[e'] \right\rangle \rightarrow_d^* \left\langle h_2', v' \right\rangle * \boxed{\bullet\, h_2'}^{\gamma'} * [\![\Xi \vdash \tau']\!]_\Delta(v, v')$$

This should now be trivial to prove. □

Lemma 5.12 (Pure step for the expression relation). *Suppose*

(a) $\forall h, \langle h, e_1 \rangle \rightarrow \langle h, e_2 \rangle$
(b) $\forall h, \left\langle h, e_1' \right\rangle \rightarrow_d \left\langle h, e_2' \right\rangle$
(c) $\triangleright \mathcal{E}\, [\![\Xi \vdash \tau]\!]_\Delta\, (e_2, e_2')$

then

$$\mathcal{E}\, [\![\Xi \vdash \tau']\!]_\Delta\, (e_1, e_1').$$

Proof. Let us assume that we have

(1) γ, γ'
(2) regions
(3) h_1'
(4) $\boxed{\bullet\, h_1'}^{\gamma'}$

We have to show:

$$\mathsf{IC}^\gamma\ e_1 \left\{\!\!\left| v.\ \exists h_2', v'.\ \left\langle h_1', e_1' \right\rangle \rightarrow_d^* \left\langle h_2', v' \right\rangle * \boxed{\bullet\, h_2'}^{\gamma'} * [\![\Xi \vdash \tau']\!]_\Delta(v, v') \right|\!\!\right\}$$

By Lemma 4.4 Case 6 we have to show

$$\triangleright\, \mathsf{IC}^\gamma\ e_2 \left\{\!\!\left| v.\ \exists h_2', v'.\ \left\langle h_1', e_1' \right\rangle \rightarrow_d^* \left\langle h_2', v' \right\rangle * \boxed{\bullet\, h_2'}^{\gamma'} * [\![\Xi \vdash \tau']\!]_\Delta(v, v') \right|\!\!\right\}$$

We can get rid of the later operator in (c) to get

(5) $\mathcal{E}\, [\![\Xi \vdash \tau]\!]_\Delta\, (e_2, e_2')$

and now we have to show

$$\mathsf{IC}^\gamma\ e_2 \left\{\!\!\left| v.\ \exists h_2', v'.\ \left\langle h_1', e_1' \right\rangle \rightarrow_d^* \left\langle h_2', v' \right\rangle * \boxed{\bullet\, h_2'}^{\gamma'} * [\![\Xi \vdash \tau']\!]_\Delta(v, v') \right|\!\!\right\}$$

Now using (5), (4) and Lemma 4.4 Case 3 we get

(6) v
(7) h_2', v'
(8) $\left\langle h_1', e_2' \right\rangle \rightarrow_d^* \left\langle h_2', v' \right\rangle$
(9) $\boxed{\bullet\, h_2'}^{\gamma'}$
(10) $[\![\Xi \vdash \tau']\!]_\Delta(v, v')$

And we have to show

$$\mathrel{|\!\!\Rrightarrow} \exists h_2', v'.\ \left\langle h_1', e_1' \right\rangle \rightarrow_d^* \left\langle h_2', v' \right\rangle * \boxed{\bullet\, h_2'}^{\gamma'} * [\![\Xi \vdash \tau']\!]_\Delta(v, v')$$

This should now be trivial to prove. □

Lemma 5.13 (value relation included in expression relation). *If* $[\![\Xi \vdash \tau]\!]_\Delta(v, v')$ *then* $\mathcal{E}\, [\![\Xi \vdash \tau]\!]_\Delta\, (v, v')$

Proof. It is trivial. Both left and right hand side reduce in 0 steps to the given values. □

6 COMPATIBILITY LEMMAS AND FUNDAMENTAL THEOREM

The lemmas for Tvar, Tunit, Ttrue, Tfalse, Tnat, Tabs, Tapp, Tinst, Tproj, Tmatch, Tif are simple. Tfold and Tunfold follow directly from Lemma 5.10.

Lemma 6.1 (Compatibility for pairs). *Suppose* $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e_1' : \tau_1$ *and* $\Xi \mid \Gamma \vDash e_2 \preceq_{\log} e_2' : \tau_2$*, then*

$$\Xi \mid \Gamma \vDash (e_1, e_2) \preceq_{\log} (e_1', e_2') : \tau_1 \times \tau_2.$$

Proof. Let Δ, $\vec{v}$ and $\vec{v}'$ such that $\mathcal{G}[\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v}')$, as in the definition of logical relations for open terms. From this, we get from the hypotheses $\mathcal{E}\,[\![\Xi \vdash \tau_1]\!]_\Delta\,(\overline{e_1}, \overline{e_1'})$ and $\mathcal{E}\,[\![\Xi \vdash \tau_2]\!]_\Delta\,(\overline{e_2}, \overline{e_2'})$, where we denote with an overline the substitution by $\vec{v}$ or $\vec{v}'$, as appropriate.

According to Lemma 5.11 with $K = ([], e_2)$ and $K' = ([], e_2')$, it suffices to show that $\mathcal{E}\,[\![\Xi \vdash \tau_1{\times}\tau_2]\!]_\Delta\,((v_1, \overline{e_2}), (v_1', \overline{e_2'}))$, given two values v_1, v_1' related a type τ_1. Applying the same lemma a second time with $K = (v_1, [])$ and $K' = (v_1', [])$ concludes the proof. □

Lemma 6.2 (Compatibility for function abstraction). *Suppose* $\Xi \mid \Gamma, x : \tau_1, f : \tau_1 \to \tau_2 \vDash e \preceq_{\log} e' : \tau_2$ *then*

$$\Xi \mid \Gamma \vDash \texttt{rec}\, f(x) = e \preceq_{\log} \texttt{rec}\, f(x) = e' : \tau_1 \to \tau_2.$$

Proof. Since $\texttt{rec}\, f(x) = e$ and $\texttt{rec}\, f(x) = e'$ are values, it suffices to prove that

$$[\![\Xi \vdash \tau_1 \to \tau_2]\!]_\Delta(\texttt{rec}\, f(x) = \overline{e}, \texttt{rec}\, f(x) = \overline{e'})$$

In order to prove this we use Löb induction. It suffices to show

$$[\![\Xi \vdash \tau_1 \to \tau_2]\!]_\Delta(\texttt{rec}\, f(x) = \overline{e}, \texttt{rec}\, f(x) = \overline{e'})$$

assuming

(1) $\triangleright[\![\Xi \vdash \tau_1 \to \tau_2]\!]_\Delta(\texttt{rec}\, f(x) = \overline{e}, \texttt{rec}\, f(x) = \overline{e'})$

Let us assume that we have

(2) w, w'
(3) $[\![\Xi \vdash \tau_1]\!]_\Delta(w, w')$

We have to show that

$$\mathcal{E}\,[\![\Xi \vdash \tau_2]\!]_\Delta\,((\texttt{rec}\, f(x) = \overline{e})\; w, (\texttt{rec}\, f(x) = \overline{e'})\; w')$$

We apply Lemma 5.12 and consequently have to prove

$$\triangleright\,\mathcal{E}\,[\![\Xi \vdash \tau_2]\!]_\Delta\,(\overline{e}[w, (\texttt{rec}\, f(x) = \overline{e})/x, f], \overline{e'}[w', (\texttt{rec}\, f(x) = \overline{e'})/x, f])$$

Now we can remove the later from (1), which becomes:

(1) $[\![\Xi \vdash \tau_1 \to \tau_2]\!]_\Delta(\texttt{rec}\, f(x) = \overline{e}, \texttt{rec}\, f(x) = \overline{e'})$

We now have to prove

$$\mathcal{E}\,[\![\Xi \vdash \tau_2]\!]_\Delta\,(\overline{e}[w, (\texttt{rec}\, f(x) = \overline{e})/x, f], \overline{e'}[w', (\texttt{rec}\, f(x) = \overline{e'})/x, f]).$$

This follows from Case 6 of Lemma 4.4. □

Lemma 6.3 (Compatibility for runST). *Suppose* $\Xi, X \mid \Gamma \vDash e \preceq_{\log} e' : \mathsf{ST}\; X\; \tau$ *and* $\Xi \vdash \tau$ *then*

$$\Xi \mid \Gamma \vDash \texttt{runST}\ \{e\} \preceq_{\log} \texttt{runST}\ \{e'\} : \tau.$$

Proof. Let us assume that we have

(1) γ_h, γ'_h
(2) $\vec{v}, \vec{v}'$
(3) $\mathcal{G}\llbracket \Xi \vdash \Gamma \rrbracket_\Delta(\vec{v}, \vec{v}')$
(4) regions
(5) h'_1
(6) $\boxed{\bullet\,\mathsf{excl}(h'_1)}^{\gamma'_h}$

We are to show:

$$\mathsf{IC}^{\gamma_h}\ \texttt{runST}\ \left\{e[\vec{v}/\vec{x}]\right\}\ \left\{\!\!\left\{v.\ \exists h'_2, v'_1.\ \left\langle h'_1, \texttt{runST}\ \left\{e'[\vec{v}'/\vec{x}]\right\}\right\rangle \to_d^* \langle h'_2, v'\rangle * \boxed{\bullet\,\mathsf{excl}(h'_2)}^{\gamma'_h} * \llbracket \Xi \vdash \tau \rrbracket_\Delta(v, v')\right\}\!\!\right\}$$

By Lemma 5.1 we can allocate a new region

(7) ρ
(8) $\mathsf{region}(\rho, \gamma_h, \gamma'_h)$

Now by the assumption $\Xi, X \mid \Gamma \vDash e \preceq_{\log} e' : \mathsf{ST}\ X\ \tau$ we get

(9) $\mathcal{E}\llbracket \Xi \vdash \mathsf{ST}\ X\ \tau \rrbracket_{\Delta, X \mapsto (\llbracket \cdot + 1 \rrbracket, \rho)}(e[\vec{v}/\vec{x}], e'[\vec{v}'/\vec{x}])$

Now by (6), (9) and Lemma 4.4 Case 1 we get

(10) h'_3, w'
(11) $\left\langle h'_1, e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \langle h'_3, w'\rangle$
(12) $\boxed{\bullet\,\mathsf{excl}(h'_3)}^{\gamma'_h}$
(13) $\llbracket \Xi, X \vdash \mathsf{ST}\ X\ \tau \rrbracket_{\Delta, X \mapsto (\llbracket \cdot + 1 \rrbracket, \rho)}(w, w')$

and subsequently we have to show

$$\mathsf{IC}^{\gamma_h}\ \texttt{runST}\ \{w\}\ \left\{\!\!\left\{v.\ \exists h'_2, v'_1.\ \left\langle h'_1, \texttt{runST}\ \left\{e'[\vec{v}'/\vec{x}]\right\}\right\rangle \to_d^* \langle h'_2, v'\rangle * \boxed{\bullet\,\mathsf{excl}(h'_2)}^{\gamma'_h} * \llbracket \Xi \vdash \tau \rrbracket_\Delta(v, v')\right\}\!\!\right\}$$

Now using (12) and (8) in (13) and use Lemma 4.4 Case 3 we get

(14) h'_2, v'
(15) $\langle h'_3, \texttt{runST}\ \{w'\}\rangle \to_d^* \langle h'_2, v'\rangle$
(16) $\boxed{\bullet\,\mathsf{excl}(h'_2)}^{\gamma'_h}$
(17) $\llbracket \Xi, X \vdash \tau \rrbracket_{\Delta, X \mapsto (\llbracket \cdot + 1 \rrbracket, \rho)}(v, v')$

and subsequently we have to show

$$\mid\!\Rrightarrow \exists h'_2, v'_1.\ \left\langle h'_1, \texttt{runST}\ \left\{e'[\vec{v}'/\vec{x}]\right\}\right\rangle \to_d^* \langle h'_2, v'_1\rangle * \boxed{\bullet\,\mathsf{excl}(h'_2)}^{\gamma'_h} * \llbracket \Xi \vdash \tau \rrbracket_\Delta(v, v')$$

The only thing that we don't immediately have is $\llbracket \Xi \vdash \tau \rrbracket_\Delta(v, v')$. However, it follows directly from Lemma 5.9 and (17). □

Lemma 6.4 (Compatibility for new). *Suppose* $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau$ *then*

$$\Xi \mid \Gamma \vDash \texttt{ref}(e) \preceq_{\log} \texttt{ref}(e') : \mathsf{ST}\ \rho\ (\mathsf{STRef}\ \rho\ \tau).$$

Proof. By the logical relation on open terms and Lemma 5.11 with $K = K' = \texttt{ref}([])$ it suffices to show $\mathcal{E}\llbracket \Xi \vdash \mathsf{ST}\ \rho\ (\mathsf{STRef}\ \rho\ \tau)\rrbracket_\Delta(\texttt{ref}(v), \texttt{ref}(v'))$ given $\llbracket \Xi \vdash \tau \rrbracket_\Delta(v, v')$. $\texttt{ref}(v)$ and $\texttt{ref}(v')$ are values thus it suffices to show $\llbracket \Xi \vdash \mathsf{ST}\ \rho\ (\mathsf{STRef}\ \rho\ \tau)\rrbracket_\Delta(v, v')$. Assume that we have:

(1) $\Delta, \gamma_h, \gamma'_h, h'_1, r$

(2) $\llbracket \Xi \vdash \tau \rrbracket_\Delta(v, v')$
(3) regions
——–—-{ spatial resources } ——–—-
(4) $\boxed{\bullet\, \mathrm{excl}(h_1')}^{\gamma_h'}$
(5) $\mathrm{region}(\mathrm{close}(\Delta, \rho), r, r, \gamma_h, \gamma_h')$

and we have to show:

$$\mathsf{IC}^{\gamma_h}\ \texttt{runST}\ \{\texttt{ref}(v)\} \left\{\!\!\left| \begin{array}{l} v_1.\ \exists h_2', v_1'.\ \left\langle h_1', \texttt{runST}\ \left\{\texttt{ref}(v_1')\right\}\right\rangle \to_d^* \left\langle h_2', v'\right\rangle * \boxed{\bullet\, \mathrm{excl}(h_2')}^{\gamma_h'} * \\ \quad \llbracket \Xi \vdash \texttt{STRef}\ \rho\ \tau \rrbracket_\Delta(v, v') * \mathrm{region}(\mathrm{close}(\Delta, \rho), \gamma_h, \gamma_h') \end{array} \right|\!\!\right\}$$

By Lemma 4.4 case (7) we can finish the proof if we from assuming $\boxed{\circ\, \ell \mapsto \mathrm{ex}(v)}^{\gamma_h}$ for some l can show the above postcondition. Let $\ell' = min(Loc \setminus \mathrm{dom}(h_1'))$ which exists because $\mathrm{dom}(h_1')$ is finite. From $\ell' = min(Loc \setminus \mathrm{dom}(h_1'))$ we can extend stepping on the right hand side:

$$\left\langle h_1', \texttt{runST}\ \left\{\texttt{ref}(v_1')\right\}\right\rangle \to_d^1 \left\langle h_1' \uplus [\ell' \mapsto v], \texttt{runST}\ \left\{\texttt{return}\ \ell'\right\}\right\rangle \to_d^1 \left\langle h_1' \uplus [\ell' \mapsto v], l'\right\rangle$$

We know $\ell' \notin dom(h_1')$ therefore we can allocate a new location using the derived rule below:

$$\forall \ell', v'. \quad \ell' \notin dom(h_1') * \boxed{\bullet\, \mathrm{excl}(h_1')}^{\gamma_h'} \Rrightarrow \boxed{\bullet\, \mathrm{excl}(h_1') \uplus [\ell' \mapsto \mathrm{ex}(v')]}^{\gamma_h'} * \boxed{\circ\, \ell' \mapsto \mathrm{ex}(v')}^{\gamma_h'}$$

to obtain):

(6) ℓ
——–—-{ spatial resources } ——–—-
(7) $\boxed{\circ\, \ell \mapsto \mathrm{ex}(v)}^{\gamma_h}$
(8) $\boxed{\circ\, \ell' \mapsto \mathrm{ex}(v')}^{\gamma_h'}$

From Lemma 5.4 and (5) we obtain:

(9) $\gamma_{bij}, \gamma_{rel}$
(10) $\boxed{\circ\, \mathrm{close}(\Delta, \rho) \mapsto \mathrm{ag}((\gamma_{bij}, \gamma_{rel}))}^{\gamma_{reg}}$

Now we update using the Lemma 5.3 with (3), (5), (7), (8) and (10) (notice that we get most of these back; 10 in particular is persistent) to obtain:

(11) r, γ_{pred}
(12) $\gamma_{pred} \Mapsto \llbracket \Xi \vdash \tau \rrbracket_\Delta$
(13) $\boxed{\circ\, \mathrm{ag}((\ell, \ell'))}^{\gamma_{bij}}$
(14) $\boxed{\circ\, (\ell, \ell') \mapsto \mathrm{ag}(\gamma_{pred})}^{\gamma_{rel}}$
——–—-{ spatial resources } ——–—-
(15) $\mathrm{region}(\mathrm{close}(\Delta, \rho), r \uplus [(\ell, \ell') \mapsto \mathrm{ag}(\gamma_{pred})], r, \gamma_h, \gamma_h')$

We can then show $\llbracket \Xi \vdash\ \texttt{STRef}\ \rho\ \tau \rrbracket_\Delta(\ell, \ell')$ by (10),(13),(14) and (12). Finally we get the region and finish the proof by Lemma 5.8 with (13), (14), (15), (7), (8), (12) and (2). □

Lemma 6.5 (Compatibility for deref). *Suppose* $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \texttt{STRef}\ \rho\ \tau$ *then*

$$\Xi \mid \Gamma \vDash\ !\, e \preceq_{\log}\ !\, e' : \texttt{ST}\ \rho\ \tau.$$

Proof. By the logical relation on open terms and Lemma 5.11 with $K = K' =![]$ it suffices to show $\mathcal{E}\ \llbracket \Xi \vdash \texttt{ST}\ \rho\ \tau \rrbracket_\Delta\ (!(v), !(v'))$ given $\llbracket \Xi\ \vdash\ \texttt{STRef}\ \rho\ \tau \rrbracket_\Delta(v, v')$. $!(v)$ and $!(v')$ are values thus it suffices to show $\llbracket \Xi \vdash \texttt{ST}\ \rho\ \tau \rrbracket_\Delta(!(v), !(v'))$. Assume that we have:

(1) $\Delta, \gamma_h, \gamma_h', h_1', r$
(2) $\llbracket \Xi \vdash \texttt{STRef}\ \rho\ \tau \rrbracket_\Delta(v, v')$

(3) regions
———–{ spatial resources }———–-
(4) $\boxed{\bullet\,\mathsf{excl}(h_1')}^{\gamma_h'}$
(5) $\mathsf{region}(\mathsf{close}(\Delta, \rho), r, r, \gamma_h, \gamma_h')$

and we have to show:

$$\mathsf{IC}^{\gamma_h}\ \mathtt{runST}\ \{!\ell\}\ \left\{\!\!\left|\begin{array}{l} w.\ \exists h_2', w'.\ \left\langle h_1', \mathtt{runST}\ \{!\ell'\}\right\rangle \to_d^* \left\langle h_2', w'\right\rangle * \boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma_h'} * \\ \quad [\![\Xi \vdash \tau]\!]_\Delta(w, w') * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma_h') \end{array}\right|\!\!\right\}$$

By $[\![\Xi \vdash \mathtt{STRef}\ \rho\ \tau]\!]_\Delta(v, v')$ we have that there are ℓ, ℓ', γ_{bij}, γ_{rel} and γ_{pred} such that $v = \ell$, $v' = \ell'$, (6) $\boxed{\circ\,\mathsf{close}(\Delta, \rho) \mapsto \mathsf{ag}(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}}$ and (7) $\boxed{\circ\,(\ell, \ell') \mapsto \mathsf{ag}(\gamma_{pred})}^{\gamma_{rel}}$ (8) $\gamma_{pred} \Mapsto [\![\Xi \vdash \tau]\!]_\Delta$. From Lemma 5.7 with (5) (6) and (7) we get:

(9) v_1, v_1', r'
(10) $\gamma_{pred} \Mapsto \Phi$
(11) $\triangleright \Phi(v_1, v_1')$
(12) $r = r' \uplus [(\ell, \ell') \mapsto \mathsf{ex}(\gamma_{pred})]$
———–{ spatial resources }———–-
(13) $\boxed{\bullet\,\mathsf{excl}(h_1') \uplus [\ell' \mapsto \mathsf{ex}(v_1')]}^{\gamma_h'}$
(14) $\mathsf{region}(\mathsf{close}(\Delta, \rho), r, r', \gamma_h, \gamma_h')$
(15) $\boxed{\circ\,\ell \mapsto \mathsf{ex}(v_1)}^{\gamma_h}$
(16) $\boxed{\circ\,\ell' \mapsto \mathsf{ex}(v_1')}^{\gamma_h'}$

by Properties of saved predicates, (10) and (11) we get

(17) $\gamma_{pred} \Mapsto [\![\Xi \vdash \tau]\!]_\Delta$
(18) $\triangleright [\![\Xi \vdash \tau]\!]_\Delta(v_1, v_1')$

By Lemma 4.4 case (8) with (15) it suffices to show that:

$$\triangleright(\boxed{\circ\,\ell \mapsto \mathsf{ex}(v_1)}^{\gamma_h} \Rrightarrow \exists h_2', w'.\ \left\langle h_1'[\ell' \mapsto v_1'], \mathtt{runST}\ \{!\ell'\}\right\rangle \to_d^* \left\langle h_2', w'\right\rangle * \boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma_h'} * \\ [\![\Xi \vdash \tau]\!]_\Delta(v_1, w') * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma_h'))$$

We can strip the later from the goal and context by next, thus we have:

(19) $[\![\Xi \vdash \tau]\!]_\Delta(v_1, v_1')$ (from (18))
———–{ spatial resources }———–-
(20) $\boxed{\circ\,v \mapsto \mathsf{ex}(v_1)}^{\gamma_h}$

and are to show:

$$\Rrightarrow \exists h_2', w'.\ \left\langle h_1'[\ell' \mapsto v_1'], \mathtt{runST}\ \{!\ell'\}\right\rangle \to_d^* \left\langle h_2', w'\right\rangle * \boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma_h'} * \\ [\![\Xi \vdash \tau]\!]_\Delta(v_1, w') * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma_h')$$

Let $h_2' = h_1'[\ell' \mapsto v_1']$ and $w' = v_1'$. From the operational semantics we extend the stepping relation on the right:

$$\left\langle h_1'[\ell' \mapsto v_1'], \mathtt{runST}\ \{!\ell'\}\right\rangle \to_d^1 \left\langle h_1'[\ell' \mapsto v_1'], \mathtt{runST}\ \left\{\mathtt{return}\, v_1'\right\}\right\rangle \to_d^1 \left\langle h_1'[\ell' \mapsto v_1'], v_1'\right\rangle$$

To finish the proof we have (13) and(19) and by Lemma 5.8 with (6), (7), (15), (16), (17) and (19).

□

Lemma 6.6 (Compatibility for gets). *Suppose* $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \mathsf{STRef}\ \rho\ \tau$ *and* $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e_1' : \tau$ *then*

$$\Xi \mid \Gamma \vDash e \leftarrow e_1 \preceq_{\log} e' \leftarrow e_1' : \mathsf{ST}\ \rho\ 1.$$

Proof. By the logical relation on open terms and Lemma 5.11 with $K_1 = [] \leftarrow \overline{e_1}$ and $K_1' = [] \leftarrow \overline{e_1'}$ it suffices to show $\mathcal{E}\,\llbracket \Xi \vdash \mathsf{ST}\ \rho\ 1 \rrbracket_\Delta\,(K_1[v], K_1'[v'])$ given $\llbracket \Xi \vdash \mathsf{STRef}\ \rho\ \tau \rrbracket_\Delta(v, v')$. By Lemma 5.11 with $K_2 = v \leftarrow []$ and $K_2' = v' \leftarrow []$ it suffices to show $\mathcal{E}\,\llbracket \Xi \vdash \mathsf{ST}\ \rho\ 1 \rrbracket_\Delta\,(v \leftarrow v_1, v' \leftarrow v_1')$ given $\llbracket \Xi \vdash \tau \rrbracket_\Delta(v_1, v_1')$. $v \leftarrow v_1$ and $v_1 \leftarrow v_1'$ are values thus it suffices to show $\llbracket \Xi \vdash \mathsf{ST}\ \rho\ \tau \rrbracket_\Delta(v \leftarrow v_1, v' \leftarrow v_1')$. Assume that we have:

(1) $\Delta, \gamma_h, \gamma_h', h_1', r$
(2) $\llbracket \Xi \vdash \mathsf{STRef}\ \rho\ \tau \rrbracket_\Delta(v, v')$
(3) $\llbracket \Xi \vdash \tau \rrbracket_\Delta(v_1, v_1')$
(4) regions
————-{ spatial resources } ————-
(5) $\boxed{\bullet\, \mathsf{excl}(h_1')}^{\gamma_h'}$
(6) $\mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma_h')$

and we have to show:

$$\mathsf{IC}^{\gamma_h}\ \mathtt{runST}\ \{v \leftarrow v_1\} \left\{\!\!\left\{ \begin{array}{l} w.\ \exists h_2', w'.\ \left\langle h_1', \mathtt{runST}\ \left\{v' \leftarrow v_1'\right\}\right\rangle \to_d^* \left\langle h_2', w' \right\rangle * \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma_h'} * \\ \quad \llbracket \Xi \vdash 1 \rrbracket_\Delta(w, w') * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma_h') \end{array} \right\}\!\!\right\}$$

Unfolding (2) $\llbracket \Xi \vdash \mathsf{STRef}\ \rho\ \tau \rrbracket_\Delta(v, v')$ we have:

(7) ℓ, ℓ'
(8) $v = \ell$ and $v' = \ell'$
(9) $\gamma_{bij}, \gamma_{rel}, \gamma_{pred}$
(10) $\boxed{\circ\, \mathsf{close}(\Delta, \rho) \mapsto \mathsf{ag}(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}}$
(11) $\boxed{\circ\, (\ell, \ell') \mapsto \mathsf{ag}(\gamma_{pred})}^{\gamma_{rel}}$
(12) $\gamma_{pred} \Mapsto \llbracket \Xi \vdash \tau \rrbracket_\Delta$

From Lemma 5.7 with (6), (10) and (12) we get:

(9) v_2, v_2', r', Φ
(10) $\llbracket \Xi \vdash \tau \rrbracket_\Delta(v_2, v_2')$
(11) $r = r' \uplus [(v, v') \mapsto \mathsf{ag}(\gamma_{pred})]$
————-{ spatial resources } ————-
(12) $\boxed{\bullet\, \mathsf{excl}(h_1') \uplus [\ell' \mapsto \mathsf{ex}(v_2')]}^{\gamma_h'}$
(13) $\mathsf{openregion}(\mathsf{close}(\Delta, \rho), r, r', \gamma_h, \gamma_h')$
(14) $\boxed{\circ\, \ell \mapsto \mathsf{ex}(v_2)}^{\gamma_h}$
(15) $\boxed{\circ\, \ell' \mapsto \mathsf{ex}(v_2')}^{\gamma_h'}$
(16) $\gamma_{pred} \Mapsto \Phi$
(17) $\triangleright\, \Phi(v_2.v_2')$

By Lemma 4.4 case (9) with (14), we obtain that the left hand side returns () and under the assumption (18) $\boxed{\circ\, \ell \mapsto v_1}^{\gamma_h}$ we have to show:

$$\Rrightarrow \exists h_2', w'.\ \left\langle h_1'[\ell' \mapsto v_2'], \mathtt{runST}\ \left\{\ell' \leftarrow v_1'\right\}\right\rangle \to_d^* \left\langle h_2', w' \right\rangle * \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma_h'} *$$
$$\llbracket \Xi \vdash 1 \rrbracket_\Delta((), w') * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma_h')$$

Let $h'_2 = h_1[\ell' \mapsto v'_1]$ and $w' = ()$. From the operational semantics we extend the stepping relation on the right:

$$\left\langle h_1[\ell' \mapsto v'_1], \texttt{runST}\ \left\{\ell' \leftarrow v'_1\right\}\right\rangle \to^1_d \left\langle h_1[\ell' \mapsto v'_2], \texttt{runST}\ \{\texttt{return}\,()\}\right\rangle \to^1_d \left\langle h_1[\ell' \mapsto v'_2], ()\right\rangle$$

From (12) and (15) we have can update the points-to to obtain (19) $\boxed{\bullet\,\mathsf{excl}(h_1[\ell' \mapsto v'_2])}^{\gamma'_h}$ and (20) $\boxed{\circ\,\ell' \mapsto \mathsf{ex}(v'_2)}^{\gamma_h}$. To finish the proof we have (19) and by Lemma 5.8 with (10), (11), (13), (14), (20), (12) and (3). $[\![\Xi \vdash 1]\!]_\Delta((), ())$ follows by definition.

□

Lemma 6.7 (Compatibility for ref eq). *Suppose* $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \mathsf{STRef}\ \rho\ \tau$ *and* $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e'_1 : \mathsf{STRef}\ \rho\ \tau'$ *then*

$$\Xi \mid \Gamma \vDash e == e_1 \preceq_{\log} e' == e'_1 : \mathbb{B}.$$

Proof. By the logical relation on open terms and Lemma 5.11 with $K_1 = [] == \overline{e_1}$ and $K'_1 = [] == \overline{e'_1}$ it suffices to show $\mathcal{E}\,[\![\Xi \vdash \mathbb{B}]\!]_\Delta\,(K_1[v], K'_1[v'])$ given $[\![\Xi \vdash \mathsf{STRef}\ \rho\ \tau]\!]_\Delta(v, v')$. Again, by Lemma 5.11 with $K_2 = v == []$ and $K'_2 = v' == []$ it suffices to show $\mathcal{E}\,[\![\Xi \vdash \mathbb{B}]\!]_\Delta\,(K_2[v_1], K'_2[v'_1])$ given $[\![\Xi \vdash \mathsf{STRef}\ \rho\ \tau]\!]_\Delta(v_1, v'_1)$. Assume we have the following:

(1) $\gamma_h, \gamma'_h, h'_1$
(2) $[\![\Xi \vdash \mathsf{STRef}\ \rho\ \tau]\!]_\Delta(v, v')$
(3) $[\![\Xi \vdash \mathsf{STRef}\ \rho\ \tau]\!]_\Delta(v_1, v'_1)$
(4) regions
———–{ spatial resources } ———–
(5) $\boxed{\bullet\,\mathsf{excl}(h'_1)}^{\gamma'_h}$

We do a case on $v = v_1$ (the other case is similar):

Case: $v = v_1$. Since $v = v_1$ we can show we can take a single step:

$$\langle h, v == v_1\rangle \to \langle h, \texttt{true}\rangle$$

therefore, by Lemma 4.4 case (6), it suffices to show:

$$\Rrightarrow \exists h'_2, w'.\ \left\langle h'_1, v' == v'_1\right\rangle \to^1_d \left\langle h'_2, w'\right\rangle * \boxed{\bullet\,\mathsf{excl}(h'_2)}^{\gamma'_h} * \\ [\![\Xi \vdash \mathbb{B}]\!]_\Delta(\texttt{true}, w')$$

Thus all we need to show is $v' == v'_1$. From (2) and (3) we have:

(6) $\gamma_{bij}, \gamma_{rel}, \gamma_{pred}, \gamma'_{bij}, \gamma'_{rel}, \gamma'_{pred}$
(7) $\boxed{\circ\,\mathsf{close}(\Delta, \rho) \mapsto \mathsf{ag}(\gamma_{bij}, \gamma_{rel})}^{\gamma_{reg}}$
(8) $\boxed{\circ\,\mathsf{ag}(v, v')}^{\gamma_{bij}}$
(9) $\boxed{\circ\,(v, v') \mapsto \mathsf{ag}(\gamma_{pred})}^{\gamma_{rel}}$
(10) $\gamma_{pred} \Rrightarrow [\![\Xi \vdash \tau]\!]_\Delta$
(11) $\boxed{\circ\,\mathsf{close}(\Delta, \rho) \mapsto \mathsf{ag}(\gamma'_{bij}, \gamma'_{rel})}^{\gamma_{reg}}$
(12) $\boxed{\circ\,\mathsf{ag}(v, v'_1)}^{\gamma'_{bij}}$
(13) $\boxed{\circ\,(v, v'_1) \mapsto \mathsf{ag}(\gamma'_{pred})}^{\gamma'_{rel}}$
(14) $\gamma'_{pred} \Rrightarrow [\![\Xi \vdash \tau]\!]_\Delta$

From agreement between (7) and (11) we have that $\gamma_{bij} = \gamma'_{bij}$ and $\gamma_{rel} = \gamma'_{rel}$. Now, by opening the invariant in the regions predicate and by resource-arguing, having (8) and (12), there exist a bijection g such that relates $g(v) = v'$ and $g(v) = v'_1$. Therefore $v' = v'_1$ must be equal. This concludes the proof for this case.

□

Lemma 6.8 (Compatibility for bind). *Suppose* $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \mathsf{ST}\ \rho\ \tau$ *and* $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e'_1 : \tau \longrightarrow \mathsf{ST}\ \rho\ \tau'$ *then*

$$\Xi \mid \Gamma \vDash \mathtt{bind}\, e\, \mathtt{in}\, e_1 \preceq_{\log} \mathtt{bind}\, e'\, \mathtt{in}\, e'_1 : \mathsf{ST}\ \rho\ \tau'.$$

Proof. By the logical relation on open terms and Lemma 5.11 with $K_1 = \mathtt{bind}\,[]\,\mathtt{in}\,\overline{e_1}$ and $K'_1 = \mathtt{bind}\,[]\,\mathtt{in}\,\overline{e'_1}$ it suffices to show $\mathcal{E}\,[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau']\!]_\Delta\ (K_1[v], K'_1[v'])$ given $[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau]\!]_\Delta(v, v')$. Again, by Lemma 5.11 with $K_2 = \mathtt{bind}\, v\, \mathtt{in}\,[]$ and $K'_2 = \mathtt{bind}\, v'\, \mathtt{in}\,[]$ it suffices to show:

$$\mathcal{E}\,[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau']\!]_\Delta\,(\mathtt{bind}\, v\, \mathtt{in}\, v_1, \mathtt{bind}\, v'\, \mathtt{in}\, v'_1)$$

given $[\![\Xi \vdash \tau \longrightarrow \mathsf{ST}\ \rho\ \tau']\!]_\Delta(v_1, v'_1)$. $\mathtt{bind}\, v\, \mathtt{in}\, v_1$ and $\mathtt{bind}\, v_1\, \mathtt{in}\, v'_1$ are values thus it suffices to show $[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau']\!]_\Delta(\mathtt{bind}\, v\, \mathtt{in}\, v_1, \mathtt{bind}\, v'\, \mathtt{in}\, v'_1)$.

(1) $\Delta, \gamma_h, \gamma'_h, h'_1, r$
(2) $[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau]\!]_\Delta(v, v')$
(3) $[\![\Xi \vdash \tau \longrightarrow \mathsf{ST}\ \rho\ \tau']\!]_\Delta(v_1, v'_1)$
(4) regions
————-{ spatial resources }————-
(5) $\boxed{\bullet\, \mathsf{excl}(h'_1)}^{\gamma'_h}$
(6) $\mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma'_h)$

By Lemma 4.4 case (10) and Lemma 2.4 case (3) and (2) and (5) above we have:

(7) v_2, v'_2, h_3
(8) $\langle h'_1, \mathtt{runST}\ \{v'\}\rangle \rightarrow^*_d \langle h'_3, \mathtt{return}\, v'_2\rangle$
(9) $\boxed{\bullet\, \mathsf{excl}(h'_3)}^{\gamma'_h}$
(10) $[\![\Xi \vdash \tau]\!]_\Delta(v_2, v'_2)$

From Lemma 4.4 case (10) with $\mathbb{K} = \mathtt{bind}\,[]\,\mathtt{in}\, v_1$ it suffices to show:

$$\mathsf{IC}^{\gamma_h}\ \mathtt{runST}\ \{\mathbb{K}[\mathtt{return}\, v_2]\} \left\{\!\!\left\{ \begin{array}{l} w.\ \exists h'_2, w'.\ \left\langle h'_1, \mathtt{runST}\ \left\{\mathtt{bind}\, v'\, \mathtt{in}\, v'_1\right\}\right\rangle \rightarrow^*_d \left\langle h'_2, w'\right\rangle * \boxed{\bullet\, \mathsf{excl}(h'_2)}^{\gamma'_h} * \\ \quad [\![\Xi \vdash \tau]\!]_\Delta(w, w') * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma'_h) \end{array} \right\}\!\!\right\}$$

From the operational semantics for bind, we can take a step and what we then need to show is:

$$\mathsf{IC}^{\gamma_h}\ \mathtt{runST}\ \{v_1\ v_2\} \left\{\!\!\left\{ \begin{array}{l} w.\ \exists h'_2, w'.\ \left\langle h'_1, \mathtt{runST}\ \left\{\mathtt{bind}\, v'\, \mathtt{in}\, v'_1\right\}\right\rangle \rightarrow^*_d \left\langle h'_2, w'\right\rangle * \boxed{\bullet\, \mathsf{excl}(h'_2)}^{\gamma'_h} * \\ \quad [\![\Xi \vdash \tau]\!]_\Delta(w, w') * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma'_h) \end{array} \right\}\!\!\right\}$$

By (3) we have that for all related arguments of type τ, with (9), we can obtain:

(11) v_3, v'_3, h_4
(12) $\langle h'_3, v'_1\ v'_2\rangle \rightarrow^*_d \langle h'_4, v'_3\rangle$
(13) $\boxed{\bullet\, \mathsf{excl}(h'_4)}^{\gamma'_h}$
(14) $[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau]\!]_\Delta(v_3, v'_3)$

and we have to show

$$\mathsf{IC}^{\gamma_h}\ \mathtt{runST}\ \{v_3\} \left\{\!\!\left\{ \begin{array}{l} w_1.\ \exists h'_2, w'_1.\ \left\langle h'_1, \mathtt{runST}\ \left\{\mathtt{bind}\, v'\, \mathtt{in}\, v'_1\right\}\right\rangle \rightarrow^*_d \left\langle h'_2, w'_1\right\rangle * \boxed{\bullet\, \mathsf{excl}(h'_2)}^{\gamma'_h} * \\ \quad [\![\Xi \vdash \mathsf{ST}\ \rho\ \tau]\!]_\Delta(w_1, w'_1) * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma'_h) \end{array} \right\}\!\!\right\}$$

Now the proof easily follows form $[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau]\!]_\Delta(v_3, v'_3)$ with (6).

□

Lemma 6.9 (Compatibility for return). *Suppose* $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau$ *then*

$$\Xi \mid \Gamma \vDash \texttt{return}\, e \preceq_{\log} \texttt{return}\, e' : \mathsf{ST}\ \rho\ \tau.$$

Proof. By the logical relation on open terms and Lemma 5.11 with $K = K' = \texttt{return}\,[]$ it suffices to show $\mathcal{E}\,[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau]\!]_\Delta(\texttt{return}\, v, \texttt{return}\, v')$ given $[\![\Xi \vdash \tau]\!]_\Delta(v, v')$. $\texttt{return}\, v$ and $\texttt{return}\, v'$ are values thus it suffices to show $[\![\Xi \vdash \mathsf{ST}\ \rho\ \tau]\!]_\Delta(\texttt{return}\, v, \texttt{return}\, v')$. Assume that we have:

(1) $\Delta, \gamma_h, \gamma'_h, h'_1, r$
(2) $[\![\Xi \vdash \tau]\!]_\Delta(v, v')$
(3) regions
———–{ spatial resources } ———–
(4) $\boxed{\bullet\, \mathrm{excl}(h'_1)}^{\gamma'_h}$
(5) $\mathrm{region}(\mathrm{close}(\Delta, \rho), \gamma_h, \gamma'_h)$

and we have to show:

$$\mathsf{IC}^{\gamma_h}\ \texttt{runST}\ \{\texttt{return}\, v\} \left\{\!\!\left\{ \begin{array}{l} w.\ \exists h'_2, w'.\ \left\langle h'_1, \texttt{runST}\ \{\texttt{return}\, v\}\right\rangle \to_d^* \left\langle h'_2, w'_1 \right\rangle * \boxed{\bullet\, \mathrm{excl}(h'_2)}^{\gamma'_h} * \\ \quad [\![\tau]\!]_\Delta(w, w') * \mathrm{regions} * \mathrm{region}(\mathrm{close}(\Delta, \rho), \gamma_h, \gamma'_h) \end{array} \right\}\!\!\right\}$$

This follows directly from (2) and by taking one step on both sides. □

Theorem 6.10 (Fundamental theorem).

$$\Xi \mid \Gamma \vdash e : \tau \Rightarrow \Xi \mid \Gamma \vDash e \preceq_{\log} e : \tau$$

Proof. Follows from compatibility lemmas by induction on typing derivation $\Xi \mid \Gamma \vdash e : \tau$. □

Theorem 6.11 (Adequacy of logical relation).

$$\mathcal{E}\,[\![\Xi \vdash \tau]\!]_\Delta(e, e') \wedge \forall h, h'.\ (h, e) \downarrow \Rightarrow (h', e') \downarrow$$

Proof. Follows from the definition of expression relation and the soundness of the Iris itself. □

Theorem 6.12 (Congruence of logical relation).

$$\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau \Rightarrow \forall C.\ C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau') \Rightarrow \Xi' \mid \Gamma' \vDash C[e] \preceq_{\log} C[e'] : \tau'$$

Proof. Follows from compatibility lemmas and the fundamental theorem by induction on derivation of $C : (\Xi \mid \Gamma; \tau) \rightsquigarrow (\Xi' \mid \Gamma'; \tau')$. □

Theorem 6.13 (Soundness of logical relation).

$$\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau \Rightarrow \Xi \mid \Gamma \vDash e \preceq_{\mathrm{ctx}} e' : \tau$$

Proof. Follows from adequacy (Theorem 6.11) and congruence (Theorem 6.12). □

6.1 NN-Logical Relation

The NN-logical relation is defined in the same way as the logical relation that we have defined with the difference being that the right hand side reduces in the same number of steps as the left hand side.

That is, we define $[\![\Xi \vdash \tau]\!]^{NN}_\Delta$ and $\mathcal{E}\,[\![\Xi \vdash \tau]\!]_\Delta{}^{NN}$ recursively similarly to how we defined $[\![\Xi \vdash \tau]\!]_\Delta$ and $\mathcal{E}\,[\![\Xi \vdash \tau]\!]_\Delta$ above with the following changes:

$$\begin{aligned}\llbracket \Xi \vdash \mathsf{ST}\ \rho\ \tau \rrbracket^{NN}_{\Delta}(v, v') \triangleq \forall \gamma_h, \gamma'_h, h'_1.&\\ &\{\!\!| \boxed{\bullet\, \mathsf{excl}(h'_1)}^{\gamma'_h} * \mathsf{regions} * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma'_h) |\!\!\}\\ &\quad \mathtt{runST}\ \{v\}\\ &\{\!\!| n, w.\ (h'_1, \mathtt{runST}\ \{v'\}) \Downarrow^{\gamma'_h, n}_{\llbracket \Xi \vdash \tau \rrbracket^{NN}_{\Delta}(w, \cdot)} * \mathsf{regions} * \mathsf{region}(\mathsf{close}(\Delta, \rho), \gamma_h, \gamma'_h) |\!\!\}_{\gamma_h}\end{aligned}$$

$$\mathcal{E}\,\llbracket \Xi \vdash \tau \rrbracket_{\Delta}{}^{NN}(e, e') \triangleq \forall \gamma_h, \gamma'_h, h'_1.\ \{\!\!| \boxed{\bullet\, \mathsf{excl}(h'_1)}^{\gamma'_h} * \mathsf{regions} |\!\!\}\ e\ \{\!\!| n, w.\ (h'_1, e') \Downarrow^{\gamma'_h, n}_{\llbracket \Xi \vdash \tau \rrbracket^{NN}_{\Delta}(w, \cdot)} * \mathsf{regions} |\!\!\}_{\gamma_h}$$

$$(h', e') \Downarrow^{\gamma, n}_{\Phi} \triangleq \exists h'_2, v'.\ \langle h, e' \rangle \rightarrow^{n}_{d} \langle h'_2, v' \rangle * \boxed{\bullet\, \mathsf{excl}(h'_2)}^{\gamma'_h} * \Phi(v')$$

Notice that all the compatibility lemmas, adequacy and congruence proved about our logical relation carries directly over to the NN-logical relation. In particular the bind lemma for the expression relation, the fundamental lemma and soundness.

Lemma 6.14 (Fundamental lemma of NN-logical relation).

$$\Xi \mid \Gamma \vdash e : \tau \Rightarrow \Xi \mid \Gamma \vDash e \preceq^{NN}_{\mathsf{log}} e : \tau$$

Lemma 6.15 (Soundness of logical relation).

$$\Xi \mid \Gamma \vDash e \preceq^{NN}_{\mathsf{log}} e : \tau \Rightarrow \Xi \mid \Gamma \vDash e \preceq_{\mathsf{ctx}} e : \tau$$

7 THEOREMS JUSTIFYING PURITY

Theorem 7.1 (Reduction on the right). *Let e and e' be two expressions such that $\mathcal{E}\,\llbracket \Xi \vdash \tau \rrbracket_{\Delta}(e, e')$. Furthermore, let h' and h'' be arbitrary heaps and w' a value such that $\langle h', e' \rangle \rightarrow^{*}_{d} \langle h'', w' \rangle$. Then, we have*

$$\mathcal{E}\,\llbracket \Xi \vdash \tau \rrbracket_{\Delta}(e, w')$$

Proof. Let us assume that we have:

(1) γ, γ'
(2) regions
(3) h'_1
(4) $\boxed{\bullet\, \mathsf{excl}(h'_1)}^{\gamma'}$

We have to show:

$$\mathsf{IC}^{\gamma}\ e\ \{\!\!| v.\ \exists h'_2, v'.\ \langle h'_1, w' \rangle \rightarrow^{*}_{d} \langle h'_2, v' \rangle * \boxed{\bullet\, \mathsf{excl}(h'_2)}^{\gamma'} * \llbracket \Xi \vdash \tau' \rrbracket_{\Delta}(v, v') |\!\!\}$$

We allocate a new monoid $\boxed{\bullet\, \mathsf{excl}(h)}^{\gamma_3}$ and use the monotonocity of IC (Lemma 4.4 case: 3) on the assumption $\mathcal{E}\,\llbracket \Xi \vdash \tau \rrbracket_{\Delta}(e, e')$. This gives us:

(1) h'_3, w'_3
(2) $\langle h', e' \rangle \rightarrow^{*}_{d} \langle h'_3, w'_3 \rangle$
(3) $\boxed{\bullet\, h'_3}^{\gamma^3}$
(4) $\llbracket \Xi \vdash \tau' \rrbracket_{\Delta}(v, w'_3)$

And now we have to show:

$$\models\!\Rrightarrow \exists h_2', v'.\ \langle h_1', w' \rangle \to_d^* \langle h_2', v' \rangle * \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau']\!]_\Delta(v, v')$$

Since the reduction is deterministic (Lemma 2.4 case: 5), we know that $h_3' = h''$ and $w_3' = w'$. Taking h_2' and v' to be h_1' and w' concludes the proof. □

Lemma 7.2 (ST monad left identity). *If* $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \mathsf{ST}\ \rho\ \tau$ *then*

(a) $\Xi \mid \Gamma \vDash \mathtt{bind}\, e\ \mathtt{in}\, (\lambda x.\, \mathtt{return}\, x) \preceq_{\log} e' : \mathsf{ST}\ \rho\ \tau$
(b) $\Xi \mid \Gamma \vDash e \preceq_{\log} \mathtt{bind}\, e'\ \mathtt{in}\, (\lambda x.\, \mathtt{return}\, x) : \mathsf{ST}\ \rho\ \tau$

Lemma 7.3 (ST monad right identity). *If* $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e_1' : \tau$ *and* $\Xi \mid \Gamma \vDash e_2 \preceq_{\log} e_2' : \tau \to \mathsf{ST}\ \rho\ \tau'$ *then*

(a) $\Xi \mid \Gamma \vDash \mathtt{bind}\, (\mathtt{return}\, e_1)\ \mathtt{in}\, e_2 \preceq_{\log} e_2'\ e_1' : \mathsf{ST}\ \rho\ \tau'$
(b) $\Xi \mid \Gamma \vDash e_2\ e_1 \preceq_{\log} \mathtt{bind}\, (\mathtt{return}\, e_1')\ \mathtt{in}\, e_2' : \mathsf{ST}\ \rho\ \tau$

Lemma 7.4 (ST monad associativity). *If* $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e_1' : \mathsf{ST}\ \rho\ \tau$, $\Xi \mid \Gamma \vDash e_2 \preceq_{\log} e_2' : \tau \to \mathsf{ST}\ \rho\ \tau'$ *and* $\Xi \mid \Gamma \vDash e_3 \preceq_{\log} e_3' : \tau' \to \mathsf{ST}\ \rho\ \tau''$ *then*

(a) $\Xi \mid \Gamma \vDash \mathtt{bind}\, (\mathtt{bind}\, e_1\ \mathtt{in}\, e_2)\ \mathtt{in}\, e_3 \preceq_{\log} \mathtt{bind}\, e_1'\ \mathtt{in}\, (\lambda x.\, \mathtt{bind}\, (e_2'\ x)\ \mathtt{in}\, e_3') : \mathsf{ST}\ \rho\ \tau'$
(b) $\Xi \mid \Gamma \vDash \mathtt{bind}\, e_1\ \mathtt{in}\, (\lambda x.\, \mathtt{bind}\, (e_2\ x)\ \mathtt{in}\, e_3) \preceq_{\log} \mathtt{bind}\, (\mathtt{bind}\, e_1'\ \mathtt{in}\, e_2')\ \mathtt{in}\, e_3' : \mathsf{ST}\ \rho\ \tau$

Lemma 7.5 (Commutativity). *If* $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e_1' : \tau$ *and* $\Xi \mid \Gamma \vDash e_2 \preceq_{\log} e_2' : \tau'$ *then*

(a) $\Xi \mid \Gamma \vDash \mathtt{let}\, x = e_2\ \mathtt{in}\, (e_1, x) \preceq_{\log} (e_1', e_2') : \tau \times \tau'$
(b) $\Xi \mid \Gamma \vDash (e_1, e_2) \preceq_{\log} \mathtt{let}\, x = e_2'\ \mathtt{in}\, (e_1', x) : \tau \times \tau'$

Proof. Case (b) is very similar to case (a). Therefore, we only prove the latter.

Case (a). Let us assume that we have

(1) γ, γ'
(2) $\vec{v}, \vec{v'}$
(3) $\mathcal{G}[\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v'})$
(4) regions
(5) h_1'
(6) $\boxed{\bullet\, \mathsf{excl}(h_1')}^{\gamma'}$
(7) h_1, h_2, n, v
(8) $\boxed{\bullet\, \mathsf{excl}(h_1)}^{\gamma}$
(9) $\langle h_1, \mathtt{let}\, x = e_2[\vec{v}/\vec{x}]\ \mathtt{in}\, (e_1[\vec{v}/\vec{x}], x) \rangle \to^n \langle h_2, v \rangle$

We have to show

$$\models\{n\}\!\Rrightarrow\!\triangleright \boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \langle h_1', (e_1'[\vec{v'}/\vec{x}], e_2'[\vec{v'}/\vec{x}]) \rangle \to_d^* \langle h_2', v' \rangle * \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau \times \tau']\!]_\Delta(v, v')$$

From (9), we get

(10) $h_3, v_2, 0 \le m \le n$
(11) $\langle h_1, e_2[\vec{v}/\vec{x}] \rangle \to^m \langle h_3, v_2 \rangle$
(12) $\langle h_3, e_1[\vec{v}/\vec{x}] \rangle \to^{n-m} \langle h_2, v_1 \rangle$
(13) $v = (v_1, v_2)$

We allocate $\boxed{\bullet\, \mathsf{excl}(h_3)}^{\gamma^3}$ and $\boxed{\circ\, \mathsf{excl}(h_3)}^{\gamma^3}$. We use the former together with (6) (12) above in $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e_1' : \tau$ to get:

(14) $\models\{n - m\}\!\Rrightarrow\!\triangleright \exists h_3', v_1'.\ \langle h_1', e_1'[\vec{v'}/\vec{x}] \rangle \to_d^* \langle h_3', v_1' \rangle * \boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma^3} * \boxed{\bullet\, \mathsf{excl}(h_3')}^{\gamma'} * [\![\Xi \vdash \tau]\!]_\Delta(v_1, v_1')$

(15) $\boxed{\circ\,\mathsf{excl}(h_3)}^{\gamma^3}$

From (14) we get

(16) h'_3, v'_1.

(17) $\left\langle h'_1, e'_1[\vec{v}'/\vec{x}]\right\rangle \to_d^* \langle h'_3, v'_1\rangle$

(18) $\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma^3}$

(19) $\boxed{\bullet\,\mathsf{excl}(h'_3)}^{\gamma'}$

(20) $[\![\Xi \vdash \tau]\!]_\Delta(v_1, v'_1)$

Now we have to prove

$$\vDash\{m\}\!\!\Rrightarrow\triangleright\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h'_2, v'.\ \left\langle h'_1, (e'_1[\vec{v}'/\vec{x}], e'_2[\vec{v}'/\vec{x}])\right\rangle \to_d^* \langle h'_2, v'\rangle * \boxed{\bullet\,\mathsf{excl}(h'_2)}^{\gamma'} * [\![\Xi \vdash \tau \times \tau']\!]_\Delta(v, v')$$

Now we can use (19), (8), (11) and $\Xi \mid \Gamma \vDash e_2 \preceq_{\mathsf{log}} e'_2 : \tau'$ to get

(21) h'_2, v'_2.

(22) $\left\langle h'_3, e'_2[\vec{v}'/\vec{x}]\right\rangle \to_d^* \langle h'_2, v'_2\rangle$

(23) $\boxed{\bullet\,\mathsf{excl}(h'_2)}^{\gamma'}$

(24) $\boxed{\bullet\,\mathsf{excl}(h_3)}^{\gamma}$

(25) $[\![\Xi \vdash \tau]\!]_\Delta(v_2, v'_2)$

and now we have to show

$$\vDash\!\!\Rrightarrow\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h'_2, v'.\ \left\langle h'_1, (e'_1[\vec{v}'/\vec{x}], e'_2[\vec{v}'/\vec{x}])\right\rangle \to_d^* \langle h'_2, v'\rangle * \boxed{\bullet\,\mathsf{excl}(h'_2)}^{\gamma'} * [\![\Xi \vdash \tau \times \tau']\!]_\Delta(v, v')$$

The only non-trivial part now is to show $\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma}$. However, notice that by (18) and (15) we have $\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma^3} * \boxed{\circ\,\mathsf{excl}(h_3)}^{\gamma^3}$. This implies that $\mathsf{excl}(h_3) \subseteq \mathsf{excl}(h_2)$. Therefore, we can update (24) to $\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \boxed{\circ\,(\mathsf{excl}(h_2) \setminus \mathsf{excl}(h_3))}^{\gamma}$. This concludes the proof. □

Lemma 7.6 (Idempotency). *If* $\Xi \mid \Gamma \vDash e \preceq_{\mathsf{log}} e' : \tau$ *then*

(a) $\Xi \mid \Gamma \vDash (e, e) \preceq_{\mathsf{log}} \texttt{let}\, x = e' \,\texttt{in}\, (x, x) : \tau \times \tau'$

(b) $\Xi \mid \Gamma \vDash \texttt{let}\, x = e \,\texttt{in}\, (x, x) \preceq_{\mathsf{log}} (e', e') : \tau \times \tau'$

Proof. We prove each case separately.

Case (a). Let us assume that we have

(1) γ, γ'

(2) $\vec{v}, \vec{v}'$

(3) $\mathcal{G}[\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v}')$

(4) regions

(5) h'_1

(6) $\boxed{\bullet\,\mathsf{excl}(h'_1)}^{\gamma'}$

(7) h_1, h_2, n, v

(8) $\boxed{\bullet\,\mathsf{excl}(h_1)}^{\gamma}$

(9) $\langle h_1, (e[\vec{v}/\vec{x}], e[\vec{v}/\vec{x}])\rangle \to^n \langle h_2, v\rangle$

We have to show

$$\models\{n\}\!\!\models\!\triangleright \boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', \texttt{let}\, x = e'[\vec{v'}/\vec{x}]\ \texttt{in}\,(x,x)\right\rangle \to_d^* \left\langle h_2', v'\right\rangle *$$
$$\boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau \times \tau']\!]_\Delta(v, v')$$

From (9), we get

(10) $h_3, v_2, 0 \leq m \leq n$
(11) $\left\langle h_1, e[\vec{v}/\vec{x}]\right\rangle \to^m \langle h_3, v_2\rangle$
(12) $\left\langle h_3, e[\vec{v}/\vec{x}]\right\rangle \to^{n-m} \langle h_2, v_1\rangle$
(13) $v = (v_1, v_2)$

We allocate $\boxed{\bullet\,\mathsf{excl}(h_1')}^{\gamma^3}$ and use it together with (8) and (11) above in $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau$ to get:

(14) h_2', v'
(15) $\left\langle h_1', e'[\vec{v'}/\vec{x}]\right\rangle \to_d^* \left\langle h_2', v'\right\rangle$
(16) $\boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma^3}$
(17) $\boxed{\bullet\,\mathsf{excl}(h_3)}^{\gamma}$
(18) $[\![\Xi \vdash \tau]\!]_\Delta(v_1, v')$

Now we have to show

$$\models\{n-m\}\!\!\models\!\triangleright \boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', \texttt{let}\, x = e'[\vec{v'}/\vec{x}]\ \texttt{in}\,(x,x)\right\rangle \to_d^* \left\langle h_2', v'\right\rangle *$$
$$\boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau \times \tau']\!]_\Delta(v, v')$$

Now we use (6), (17), (12) above in $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau$ to get

(19) h_2'', v''
(20) $\left\langle h_1', e'[\vec{v'}/\vec{x}]\right\rangle \to_d^* \left\langle h_2'', v''\right\rangle$
(21) $\boxed{\bullet\,\mathsf{excl}(h_2'')}^{\gamma'}$
(22) $\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma}$
(23) $[\![\Xi \vdash \tau]\!]_\Delta(v_2, v'')$

Now we have to show

$$\models\!\triangleright \boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', \texttt{let}\, x = e'[\vec{v'}/\vec{x}]\ \texttt{in}\,(x,x)\right\rangle \to_d^* \left\langle h_2', v'\right\rangle *$$
$$\boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau \times \tau']\!]_\Delta(v, v')$$

From (15) and (20) we get that $h_2' = h''$ and $v' = v''$. This concludes the proof.

Case (b). Let us assume that we have

(1) γ, γ'
(2) $\vec{v}, \vec{v'}$
(3) $\mathcal{G}[\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v'})$
(4) regions
(5) h_1'
(6) $\boxed{\bullet\,\mathsf{excl}(h_1')}^{\gamma'}$
(7) h_1, h_2, n, v
(8) $\boxed{\bullet\,\mathsf{excl}(h_1)}^{\gamma}$

(9) $\left\langle h_1, \texttt{let}\, x = e[\vec{v}/\vec{x}]\, \texttt{in}\, (x, x)\right\rangle \to^n \langle h_2, v\rangle$

We have to show

$$\models\{n\}\Rrightarrow\triangleright \boxed{\bullet\, \mathrm{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', (e'[\vec{v}'/\vec{x}], e'[\vec{v}'/\vec{x}])\right\rangle \to_d^* \left\langle h_2', v'\right\rangle * \\ \boxed{\bullet\, \mathrm{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau \times \tau']\!]_\Delta(v, v')$$

From (9), we get

(10) w
(11) $\left\langle h_3, e[\vec{v}/\vec{x}]\right\rangle \to^{n-1} \langle h_2, w\rangle$
(12) $v = (w, w)$

We allocate $\boxed{\bullet\, \mathrm{excl}(h_1)}^{\gamma^3}$ and use it together with (6) and (11) above in $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau$ to get:

(13) $\models\{n-1\}\Rrightarrow\triangleright \boxed{\bullet\, \mathrm{excl}(h_2)}^{\gamma^3} * \exists h_3', v_1'.\ \left\langle h_1', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_3', v_1'\right\rangle * \boxed{\bullet\, \mathrm{excl}(h_3')}^{\gamma'} * [\![\Xi \vdash \tau]\!]_\Delta(w, v_1')$

Notice that result of the future modality in (13) implies $\exists h_3', v_1'.\ \left\langle h_1', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_3', v'\right\rangle$ which is a plain fact. Therefore, from (13) we get (by eliminating this existential quantifier since it commutes with both $\triangleright$ and $\diamond$ into h_3'' and v_1'') and putting $\triangleright^{n-1} \diamond \cdots$ back under the future modality:

(14) h_3'', v_1''
(15) $\models\{n-1\}\Rrightarrow\triangleright \boxed{\bullet\, \mathrm{excl}(h_2}^{\gamma^3} * \left\langle h_1', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_3'', v_1''\right\rangle * \exists h_3', v_1'.\ \left\langle h_1', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_3', v_1'\right\rangle * \boxed{\bullet\, \mathrm{excl}(h_3')}^{\gamma'} *$
$[\![\Xi \vdash \tau]\!]_\Delta(w, v_1')$

Now we allocate $\boxed{\bullet\, \mathrm{excl}(h_3'')}^{\gamma^4}$ and $\boxed{\circ\, \mathrm{excl}(h_3'')}^{\gamma^4}$ and use the former together with (8) and (11) above in $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \tau$ to get:

(16) $\models\{n-1\}\Rrightarrow\triangleright \boxed{\bullet\, \mathrm{excl}(h_2)}^{\gamma} * \exists h_2', v_2'.\ \left\langle h_3'', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_2', v_2'\right\rangle * \boxed{\bullet\, \mathrm{excl}(h_2')}^{\gamma^4} * [\![\Xi \vdash \tau]\!]_\Delta(w, v_2')$
(17) $\boxed{\circ\, \mathrm{excl}(h_3'')}^{\gamma^4}$

From (15) and (16), we get

(18) h_3'', v_1''
(19) $\boxed{\bullet\, \mathrm{excl}(h_2)}^{\gamma^3}$
(20) $\left\langle h_1', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_3'', v_1''\right\rangle$
(21) h_3', v_1'
(22) $\left\langle h_1', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_3', v_1'\right\rangle$
(23) $\boxed{\bullet\, \mathrm{excl}(h_3')}^{\gamma'}$
(24) $[\![\Xi \vdash \tau]\!]_\Delta(w, v_1')$
(25) $\boxed{\bullet\, \mathrm{excl}(h_2)}^{\gamma}$
(26) h_2', v_2'
(27) $\left\langle h_3'', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_2', v_2'\right\rangle$
(28) $\boxed{\bullet\, \mathrm{excl}(h_2')}^{\gamma^4}$
(29) $[\![\Xi \vdash \tau]\!]_\Delta(w, v_2')$

And now we have to show

$$\mathrel{|\!\!\equiv}\{1\}\mathrel{\equiv\!\rhd} \boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', (e'[\vec{v}'/\vec{x}], e'[\vec{v}'/\vec{x}])\right\rangle \to_d^* \langle h_2', v'\rangle *$$
$$\boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau \times \tau']\!]_\Delta(v, v')$$

By (20) and (22) we know that $h_3' = h_3''$ and $v_1' = v_1''$. The only non-trivial part is that we have to get $\boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'}$. However, notice that by (17) and (28) we have $\boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma^4} * \boxed{\circ\, \mathsf{excl}(h_3')}^{\gamma^4}$. This implies that $h_3' \subseteq h_2'$. Therefore, we can update $\boxed{\bullet\, \mathsf{excl}(h_3')}^{\gamma'}$ (by (23)) to $\boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * \boxed{\circ\, (\mathsf{excl}(h_2') \setminus \mathsf{excl}(h_3'))}^{\gamma'}$ □

Lemma 7.7 (Neutrality). *If* $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \mathbf{1}$ *then*

$$\Xi \mid \Gamma \vDash e \preceq_{\log} () : \mathbf{1}$$

Proof. Let us assume that we have

(1) γ, γ'
(2) $\vec{v}, \vec{v}'$
(3) $\mathcal{G}[\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v}')$
(4) regions
(5) h_1'
(6) $\boxed{\bullet\, \mathsf{excl}(h_1')}^{\gamma'}$
(7) h_1, h_2, n, v
(8) $\boxed{\bullet\, \mathsf{excl}(h_1)}^{\gamma}$
(9) $\left\langle h_1, e[\vec{v}/\vec{x}]\right\rangle \to^n \langle h_2, v\rangle$

We have to show

$$\mathrel{|\!\!\equiv}\{n\}\mathrel{\equiv\!\rhd} \boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', ()\right\rangle \to_d^* \left\langle h_2', v'\right\rangle * \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \mathbf{1}]\!]_\Delta(v, v')$$

We allocate $\boxed{\bullet\, \mathsf{excl}(h_1')}^{\gamma^3}$ and along with (8) and (9) above use it in $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \mathbf{1}$ to get

(10) h_2', v'
(11) $\left\langle h_1', e'[\vec{v}'/\vec{x}]\right\rangle \to_d^* \left\langle h_2', v'\right\rangle$
(12) $\boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma}$
(13) $[\![\mathbf{1}]\!]_\Delta(v, v')$

and we have to show

$$\mathrel{|\!\!\Rrightarrow} \boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', ()\right\rangle \to_d^* \left\langle h_2', v'\right\rangle * \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \mathbf{1}]\!]_\Delta(v, v')$$

By (13) we know that $v = v' = ()$. This concludes the proof. □

Lemma 7.8 (rec hoisting). *If* $\Xi \mid \Gamma \vDash e_1 \preceq_{\log} e_1' : \tau$, $\Xi \mid \Gamma, y : \tau, x : \tau', f : \tau' \to \tau'' \vDash e_2 \preceq_{\log} e_2' : \tau''$, $\Xi \mid \Gamma \vdash e_1' : \tau$ *and* $\Xi \mid \Gamma, y : \tau, x : \tau', f : \tau' \to \tau'' \vdash e_2' : \tau''$ *then*

$$\Xi \mid \Gamma \vDash \texttt{let}\, y = e_1\, \texttt{in}\, \texttt{rec}\, f(x) = e_2 \preceq_{\mathrm{ctx}} \texttt{rec}\, f(x) = \texttt{let}\, y = e_1'\, \texttt{in}\, e_2' : \tau' \to \tau''$$

Proof. The proof of rec hoisting was one of the biggest challenges of this work. The problem can be traced to one of the inherent shortcomings of step-indexed logical relations. In dependent of representation (whether it is hidden deep in Iris in our case or not) the number of steps on the left hand side and the right hand side do not match up in they that we want.

Let us assume for the sake of the argument that we want to prove the logical relation version of the above contextual refinement directly. Notice that the left hand side reduces to a closure that has the value computed from e_1 in it. The right hand side however is already a value. It computes e_1 every time it is called. That is we have to show that whenever the functions on the left and right are called, the value computed by e_1 on the right hand side inside the function is related to the value that was computed before. But we can know this only after n steps. Where n is the number steps it took for the original (outside the function) computation of e_1 on the right hand side. There is no guarantee that the body of the function on the left does not takes n steps or more. Therefore, we cannot directly prove this logical relatedness.

On the paper dealing explicitly with Kripke worlds, one would manipulate the world at hand by changing step-indexes. In practice adding more logical steps where there are non physically. Working in Iris where worlds are completely hidden to us we can obviously not employ such trick. Notice that not even inside the model of Iris can we do this kind of trick. This is due to the fact that in Iris we have to stick to the convention that whenever we are proving an entailment of the form $P \vdash Q$ the world on the left and right are the same.

We prove this by proving the following three contextual refinements

(a) $\Xi \mid \Gamma \vDash \texttt{let}\, y = e_1 \,\texttt{in}\,\texttt{rec}\, f(x) = e_2 \preceq_{\text{ctx}} \texttt{let}\, y = e_1' \,\texttt{in}\,\texttt{rec}\, f(x) = \texttt{let}\, z = e_1' \,\texttt{in}\, e_2' : \tau' \to \tau''$
(b) $\Xi \mid \Gamma \vDash \texttt{let}\, y = e_1' \,\texttt{in}\,\texttt{rec}\, f(x) = \texttt{let}\, z = e_1' \,\texttt{in}\, e_2' \preceq_{\text{ctx}} \texttt{let}\, z = e_1' \,\texttt{in}\,\texttt{rec}\, f(x) = \texttt{let}\, y = e_1' \,\texttt{in}\, e_2' : \tau' \to \tau''$
(c) $\Xi \mid \Gamma \vDash \texttt{let}\, z = e_1' \,\texttt{in}\,\texttt{rec}\, f(x) = \texttt{let}\, y = e_1' \,\texttt{in}\, e_2' \preceq_{\text{ctx}} \texttt{rec}\, f(x) = \texttt{let}\, y = e_1' \,\texttt{in}\, e_2' : \tau' \to \tau''$

where z is a fresh variable not appearing in Γ, i.e., $z \notin \text{dom}(\Gamma)$. We prove each case separately.

Case (a). We prove

$$\Xi \mid \Gamma \vDash \texttt{let}\, y = e_1 \,\texttt{in}\,\texttt{rec}\, f(x) = e_2 \preceq_{\text{log}} \texttt{let}\, y = e_1' \,\texttt{in}\,\texttt{rec}\, f(x) = \texttt{let}\, z = e_1' \,\texttt{in}\, e_2' : \tau' \to \tau''$$

Let us assume that we have

(1) γ, γ'
(2) $\vec{v}, \vec{v'}$
(3) $\mathcal{G}[\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v'})$
(4) regions
(5) h_1'
(6) $\boxed{\bullet\,\mathsf{excl}(h_1')}^{\gamma'}$
(7) h_1, h_2, n, v
(8) $\boxed{\bullet\,\mathsf{excl}(h_1)}^{\gamma}$
(9) $\left\langle h_1, \texttt{let}\, y = e_1[\vec{v}/\vec{x}] \,\texttt{in}\,\texttt{rec}\, f(x) = e_2[\vec{v}/\vec{x}]\right\rangle \to^n \langle h_2, v\rangle$

We have to show

$$\models\!\{n\}\!\!\models\!\triangleright \boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}] \,\texttt{in}\,\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v'}/\vec{x}] \,\texttt{in}\, e_2'[\vec{v'}/\vec{x}]\right\rangle \to_d^* \left\langle h_2', v'\right\rangle$$
$$* \boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau' \to \tau'']\!]_\Delta(v, v')$$

From (9) we know that

(10) v_1
(11) $\left\langle h_1, e_1[\vec{v}/\vec{x}]\right\rangle \to^{n-1} \langle h_2, v_1\rangle$
(12) $v = \texttt{rec}\, f(x) = e_2[\vec{v}/\vec{x}][v_1/y]$

Using (11), (8), (6) and $\Xi \mid \Gamma \vDash e_1 \preceq_{\text{log}} e_1' : \tau$ we know that

(13) $\models\!\{n-1\}\!\!\models\!\triangleright \boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v_1'.\ \left\langle h_1', e_1'[\vec{v'}/\vec{x}]\right\rangle \to_d^* \left\langle h_2', v_1'\right\rangle * \boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau]\!]_\Delta(v_1, v_1')$

Now, using (11) and $\Xi \mid \Gamma \vDash e_1 \preceq_{\text{log}} e_1' : \tau$ we can prove

(14) $\forall h_3'.\ \triangleright^{n-1} \diamond\big(\exists h_4', v_1''.\ \left\langle h_3', e_1'[\vec{v}'/\vec{x}]\right\rangle \rightarrow_d^* \left\langle h_4', v_1''\right\rangle\big)$

This, (14), is proven by using Lemma 4.2 case 16 and the fact that we can allocate fresh instances of h_1 and h_3' and also the fact that $\big(\exists h_4', v_1''.\ \left\langle h_3', e_1'[\vec{v}'/\vec{x}]\right\rangle \rightarrow_d^* \left\langle h_4', v_1''\right\rangle\big)$ is plain for any h_3'. Now using the fact that $\triangleright$ and $\diamond$ commute with quantifiers we get

(15) $\triangleright^{n-1} \diamond\big(\forall h_3'.\ \exists h_4', v_1''.\ \left\langle h_3', e_1'[\vec{v}'/\vec{x}]\right\rangle \rightarrow_d^* \left\langle h_4', v_1''\right\rangle\big)$

Consequently by (13) and (15) we get

(16) $\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma}$
(17) h_2', v_1'
(18) $\left\langle h_1', e_1'[\vec{v}'/\vec{x}]\right\rangle \rightarrow_d^* \left\langle h_2', v_1'\right\rangle$
(19) $\boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma'}$
(20) $[\![\Xi \vdash \tau]\!]_\Delta(v_1, v_1')$
(21) $\forall h_3'.\ \exists h_4', v_1''.\ \left\langle h_3', e_1'[\vec{v}'/\vec{x}]\right\rangle \rightarrow_d^* \left\langle h_4', v_1''\right\rangle$

and now we have to show

$$\vDash\!\{1\}\!\vDash\!\triangleright\, \boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', \mathtt{let}\, y = e_1'[\vec{v}'/\vec{x}]\, \mathtt{in}\, \mathtt{rec}\, f(x) = \mathtt{let}\, z = e_1'[\vec{v}'/\vec{x}]\, \mathtt{in}\, e_2'[\vec{v}'/\vec{x}]\right\rangle \rightarrow_d^* \left\langle h_2', v'\right\rangle$$
$$* \boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau' \to \tau'']\!]_\Delta(v, v')$$

The only thing that remains to be proven that is needed to prove the statement above is:

$$[\![\Xi \vdash \tau' \to \tau'']\!]_\Delta(\mathtt{rec}\, f(x) = e_2[\vec{v}/\vec{x}][v_1/y], \mathtt{rec}\, f(x) = \mathtt{let}\, z = e_1'[\vec{v}'/\vec{x}]\, \mathtt{in}\, e_2'[\vec{v}'/\vec{x}][v_1'/y])$$

This now follows easily from $\Xi \mid \Gamma, y : \tau, x : \tau', f : \tau' \to \tau'' \vDash e_2 \preceq_{\log} e_2' : \tau''$, (20) and crucially (21). Also notice that we have $\Xi \mid \Gamma, y : \tau, x : \tau', f : \tau' \to \tau'' \vDash e_2 \preceq_{\log} e_2' : \tau''$ and we know that $z \notin \mathrm{dom}(\Gamma)$.

Case (b). We prove

$$\Xi \mid \Gamma \vDash \mathtt{let}\, y = e_1'\, \mathtt{in}\, \mathtt{rec}\, f(x) = \mathtt{let}\, z = e_1'\, \mathtt{in}\, e_2' \preceq_{\log}^{NN} \mathtt{let}\, z = e_1'\, \mathtt{in}\, \mathtt{rec}\, f(x) = \mathtt{let}\, y = e_1'\, \mathtt{in}\, e_2' : \tau' \to \tau''$$

By $\Xi \mid \Gamma \vdash e_1' : \tau$ and $\Xi \mid \Gamma, y : \tau, x : \tau', f : \tau' \to \tau'' \vdash e_2' : \tau''$ and the fundamental theorem of NN-logical relation (Lemma 6.14) we know that $\Xi \mid \Gamma \vDash e_1' \preceq_{\log}^{NN} e_1' : \tau$ and $\Xi \mid \Gamma, y : \tau, x : \tau', f : \tau' \to \tau'' \vDash e_2' \preceq_{\log}^{NN} e_2' : \tau''$.

Let us assume that we have

(1) γ, γ'
(2) $\vec{v}, \vec{v}'$
(3) $[\![\Xi \vdash \Gamma]\!]_\Delta(\vec{v}, \vec{v}')$
(4) regions
(5) h_1'
(6) $\boxed{\bullet\,\mathsf{excl}(h_1')}^{\gamma'}$
(7) h_1, h_2, n, v
(8) $\boxed{\bullet\,\mathsf{excl}(h_1)}^{\gamma}$
(9) $\left\langle h_1, \mathtt{let}\, y = e_1'[\vec{v}/\vec{x}]\, \mathtt{in}\, \mathtt{rec}\, f(x) = \mathtt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \mathtt{in}\, e_2'[\vec{v}/\vec{x}]\right\rangle \rightarrow^n \left\langle h_2, v\right\rangle$

We have to show

$$\vDash\!\{n\}\!\vDash\!\triangleright\, \boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', \mathtt{let}\, z = e_1'[\vec{v}'/\vec{x}]\, \mathtt{in}\, \mathtt{rec}\, f(x) = \mathtt{let}\, y = e_1'[\vec{v}'/\vec{x}]\, \mathtt{in}\, e_2'[\vec{v}'/\vec{x}]\right\rangle \rightarrow_d^* \left\langle h_2', v'\right\rangle$$
$$* \boxed{\bullet\,\mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau' \to \tau'']\!]_\Delta^{NN}(v, v')$$

From (9) we know that

(10) v_1
(11) $\left\langle h_1, e_1'[\vec{v}/\vec{x}]\right\rangle \rightarrow^{n-1} \langle h_2, v_1\rangle$
(12) $v = \texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}][v_1/y]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y]$

Notice that since $\Xi \mid \Gamma \vdash e_1' : \tau$, we know that $\mathsf{FV}(e_1') \subseteq \mathrm{dom}(\Gamma)$ and therefore, from (12) we get:

(13) $v = \texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y]$

From (11), (8), (6) and $\Xi \mid \Gamma \vDash e_1' \preceq_{\mathsf{log}}^{NN} e_1' : \tau$ we get that

(14) $\boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma}$
(15) h_2', v_1'
(16) $\left\langle h_1', e_1'[\vec{v'}/\vec{x}]\right\rangle \rightarrow_d^{n-1} \left\langle h_2', v_1'\right\rangle$
(17) $\boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'}$
(18) $\llbracket \Xi \vdash \tau \rrbracket_{\Delta}^{NN}(v_1, v_1')$

and we now have to show

$$\vDash\!\{1\}\!\!\Rrightarrow\!\triangleright \boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma} * \exists h_2', v'.\ \left\langle h_1', \texttt{let}\, z = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, \texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}]\right\rangle \rightarrow_d^{*} \left\langle h_2', v'\right\rangle$$
$$* \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * \llbracket \Xi \vdash \tau' \rightarrow \tau'' \rrbracket_{\Delta}^{NN}(v, v')$$

The only thing remaining to prove is that

$$\llbracket \Xi \vdash \tau' \rightarrow \tau'' \rrbracket_{\Delta}^{NN}(\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y], \texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}][v_1'/z]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}][v_1'/z])$$

Again since we know that z does not appear free in e_1' and e_2' we have in fact to show

$$\llbracket \Xi \vdash \tau' \rightarrow \tau'' \rrbracket_{\Delta}^{NN}(\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y], \texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}])$$

Now by Löb induction and unfolding $\llbracket \Xi \vdash \tau' \rightarrow \tau'' \rrbracket_{\Delta}^{NN}$ we get

(19) $\triangleright \llbracket \Xi \vdash \tau' \rightarrow \tau'' \rrbracket_{\Delta}^{NN}(\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y], \texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}])$
(20) w, w'
(21) $\llbracket \Xi \vdash \tau' \rrbracket_{\Delta}^{NN}(w, w')$

and we have to show

$$\mathcal{E}\,\llbracket \Xi \vdash \tau' \rightarrow \tau'' \rrbracket_{\Delta}{}^{NN}((\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y])\, w, (\texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}])\, w')$$

By applying Theorem 5.12 we have to prove Then we have to show

$$\begin{aligned}\triangleright \mathcal{E}\,\llbracket \Xi \vdash \tau'' \rrbracket_{\Delta}{}^{NN}(&\texttt{let}\, z = e_1'[\vec{v}/\vec{x}][w/x]\, \texttt{in}\\ &e_2'[\vec{v}/\vec{x}][v_1/y][w, (\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y])/x, f],\\ &\texttt{let}\, y = e_1'[\vec{v'}/\vec{x}][w/x]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}][w', (\texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}])/x, f])\end{aligned}$$

Once again, since x does not appear free in e_1' we need to show

$$\begin{aligned}\triangleright \mathcal{E}\,\llbracket \Xi \vdash \tau'' \rrbracket_{\Delta}{}^{NN}(&\texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\\ &e_2'[\vec{v}/\vec{x}][v_1/y][w, (\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y])/x, f],\\ &\texttt{let}\, y = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}][w', (\texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}])/x, f])\end{aligned}$$

Now we can get rid of the later and simplify (19) into

(22) $\llbracket \Xi \vdash \tau' \rightarrow \tau'' \rrbracket_{\Delta}^{NN}(\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y], \texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v'}/\vec{x}]\, \texttt{in}\, e_2'[\vec{v'}/\vec{x}])$

and we have to show

$$\begin{aligned}\mathcal{E}\,[\![\Xi \vdash \tau'']\!]_{\Delta}{}^{NN}(&\texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\,\texttt{in}\\ &e_2'[\vec{v}/\vec{x}][v_1/y][w, (\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y])/x, f],\\ &\texttt{let}\, y = e_1'[\vec{v}'/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}'/\vec{x}][w', (\texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v}'/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}'/\vec{x}])/x, f])\end{aligned}$$

Let us assume that we have

(23) γ^1, γ^2
(24) h_3'
(25) $\boxed{\bullet\, \mathsf{excl}(h_3')}^{\gamma^2}$
(26) h_3, h_4, m, v_3
(27) $\boxed{\bullet\, \mathsf{excl}(h_3)}^{\gamma^1}$
(28) $\left\langle h_3, \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y][w, (\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y])/x, f]\right\rangle \to^{m} \langle h_4, v_3\rangle$

And we have to show

$$\begin{aligned}&\models\!\{m\}\!\!\Rrightarrow\!\triangleright \boxed{\bullet\, \mathsf{excl}(h_4)}^{\gamma^1} *\\ &\quad \exists h_4', v_3'.\ \left\langle h_3', \texttt{let}\, y = e_1'[\vec{v}'/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}'/\vec{x}][w', (\texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v}'/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}'/\vec{x}])/x, f]\right\rangle \to_d^{m} \langle h_4', v_3'\rangle\\ &\quad * \boxed{\bullet\, \mathsf{excl}(h_4')}^{\gamma^2} * [\![\Xi \vdash \tau'']\!]_{\Delta}^{NN}(v_3, v_3')\end{aligned}$$

From (28), we know that

(29) $h_5, 0 \leq k \leq m, v_4$
(30) $\left\langle h_3, e_1'[\vec{v}/\vec{x}]\right\rangle \to^{k} \langle h_5, v_4\rangle$
(31) $\left\langle h_5, e_2'[\vec{v}/\vec{x}][v_1/y][w, (\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y])/x, f][v_4/z]\right\rangle \to^{m-k-1} \langle h_4, v_3\rangle$

From the fact that z does not appear free in e_2' and (31) we get

(32) $\left\langle h_5, e_2'[\vec{v}/\vec{x}][v_1/y][w, (\texttt{rec}\, f(x) = \texttt{let}\, z = e_1'[\vec{v}/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}/\vec{x}][v_1/y])/x, f]\right\rangle \to^{m-k-1} \langle h_4, v_3\rangle$

We allocate $\boxed{\bullet\, \mathsf{excl}(h_1)}^{\gamma^3}$ and use it alongside (11), (25) and $\Xi \mid \Gamma \vDash e_1' \preceq_{\mathsf{log}}^{NN} e_1' : \tau$ we get

(33) $\models\!\{n-1\}\!\!\Rrightarrow\!\triangleright \boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma^3} * \exists h_5', v_4'.\ \left\langle h_3', e_1'[\vec{v}'/\vec{x}]\right\rangle \to_d^{n-1} \left\langle h_5', v_4'\right\rangle * \boxed{\bullet\, \mathsf{excl}(h_5')}^{\gamma^2} * [\![\Xi \vdash \tau]\!]_{\Delta}(v_1, v_4')$

We allocate $\boxed{\bullet\, \mathsf{excl}(h_1')}^{\gamma^4}$ and use it together with (30) and $\Xi \mid \Gamma \vDash e_1' \preceq_{\mathsf{log}}^{NN} e_1' : \tau$ to get

(34) $\models\!\{k\}\!\!\Rrightarrow\!\triangleright \boxed{\bullet\, \mathsf{excl}(h_5)}^{\gamma^1} * \exists h_6', v_5'.\ \left\langle h_1', e_1'[\vec{v}'/\vec{x}]\right\rangle \to_d^{k} \left\langle h_6', v_5'\right\rangle * \boxed{\bullet\, \mathsf{excl}(h_6')}^{\gamma^4} * [\![\Xi \vdash \tau]\!]_{\Delta}(v_4, v_5')$

Now we consume k future and change (33) and (34) into the following:

(35) $\models\!\{(n-1)-k\}\!\!\Rrightarrow\!\triangleright \boxed{\bullet\, \mathsf{excl}(h_2)}^{\gamma^3} * \exists h_5', v_4'.\ \left\langle h_3', e_1'[\vec{v}'/\vec{x}]\right\rangle \to_d^{n-1} \left\langle h_5', v_4'\right\rangle * \boxed{\bullet\, \mathsf{excl}(h_5')}^{\gamma^2} * [\![\Xi \vdash \tau]\!]_{\Delta}(v_1, v_4')$
(36) $\boxed{\bullet\, \mathsf{excl}(h_5)}^{\gamma^1}$
(37) h_6', v_5'
(38) $\left\langle h_1', e_1'[\vec{v}'/\vec{x}]\right\rangle \to_d^{k} \left\langle h_6', v_5'\right\rangle$
(39) $\boxed{\bullet\, \mathsf{excl}(h_6')}^{\gamma^4}$
(40) $[\![\Xi \vdash \tau]\!]_{\Delta}^{NN}(v_4, v_5')$

And we have to show that

$$\models\{m-k\}\!\models\!\triangleright \boxed{\bullet\,\mathsf{excl}(h_4)}^{\gamma^1} * \exists h_4', v_3'.$$
$$\left\langle h_3', \texttt{let}\, y = e_1'[\vec{v}'/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}'/\vec{x}][w', (\texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v}'/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}'/\vec{x}])/x, f]\right\rangle \to_d^m \langle h_4', v_3'\rangle$$
$$* \boxed{\bullet\,\mathsf{excl}(h_4')}^{\gamma^2} * [\![\Xi \vdash \tau'']\!]_\Delta^{NN}(v_3, v_3')$$

From (16) and (38) we know that $k = n - 1$, $h_6' = h_2'$ and $v_1' = v_5'$. Consequently, from (35) we get

(41) $\boxed{\bullet\,\mathsf{excl}(h_2)}^{\gamma^3}$
(42) h_5', v_4'
(43) $\left\langle h_3', e_1'[\vec{v}'/\vec{x}]\right\rangle \to_d^k \langle h_5', v_4'\rangle$
(44) $\boxed{\bullet\,\mathsf{excl}(h_5')}^{\gamma^2}$
(45) $[\![\Xi \vdash \tau]\!]_\Delta^{NN}(v_1, v_4')$

Now by (21), (22), (45), (44), (36), (32) and $\Xi \mid \Gamma, y : \tau, x : \tau' \models e_2' \preceq_{\mathrm{log}}^{NN} e_2' : \tau''$, we get

(46) $\boxed{\bullet\,\mathsf{excl}(h_4)}^{\gamma^1}$
(47) h_7', v_6'
(48) $\left\langle h_5', e_2'[\vec{v}'/\vec{x}][w'/x][v_4'/y]\right\rangle \to_d^{m-k-1} \langle h_7', v_6'\rangle$
(49) $\boxed{\bullet\,\mathsf{excl}(h_7')}^{\gamma^2}$
(50) $[\![\Xi \vdash \tau]\!]_\Delta^{NN}(v_3, v_6')$

And we have to show

$$\models\{1\}\!\models\!\triangleright \boxed{\bullet\,\mathsf{excl}(h_4)}^{\gamma^1} * \exists h_4', v_3'.$$
$$\left\langle h_3', \texttt{let}\, y = e_1'[\vec{v}'/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}'/\vec{x}][w', (\texttt{rec}\, f(x) = \texttt{let}\, y = e_1'[\vec{v}'/\vec{x}]\,\texttt{in}\, e_2'[\vec{v}'/\vec{x}])/x, f]\right\rangle \to_d^m \langle h_4', v_3'\rangle$$
$$* \boxed{\bullet\,\mathsf{excl}(h_4')}^{\gamma^2} * [\![\Xi \vdash \tau'']\!]_\Delta^{NN}(v_3, v_3')$$

which should be trivial now.

Case (c). We prove

$$\Xi \mid \Gamma \models \texttt{let}\, z = e_1'\,\texttt{in}\,\texttt{rec}\, f(x) = \texttt{let}\, y = e_1'\,\texttt{in}\, e_2' \preceq_{\mathrm{ctx}} \texttt{rec}\, f(x) = \texttt{let}\, y = e_1'\,\texttt{in}\, e_2' : \tau' \to \tau''$$

This case is rather trivial to prove! Notice that by $\Xi \mid \Gamma \vdash e_1' : \tau$ and $\Xi \mid \Gamma, y : \tau, x : \tau' \vdash e_2' : \tau''$ and the fundamental theorem of logical relation (Theorem 6.10) we know that $\Xi \mid \Gamma \models e_1' \preceq_{\mathrm{log}} e_1' : \tau$ and $\Xi \mid \Gamma, y : \tau, x : \tau', f : \tau' \to \tau'' \models e_2' \preceq_{\mathrm{log}} e_2' : \tau''$. □

Lemma 7.9 (Λ hoisting). *If $\Xi \mid \Gamma \models e_1 \preceq_{\mathrm{log}} e_1' : \tau$ and $\Xi, X \mid \Gamma, y : \tau \models e_2 \preceq_{\mathrm{log}} e_2' : \tau'$ then*

$$\Xi \mid \Gamma \models \texttt{let}\, y = e_1\,\texttt{in}\,\Lambda\, e_2 \preceq_{\mathrm{ctx}} \Lambda\,(\texttt{let}\, y = e_1'\,\texttt{in}\, e_2') : \forall X.\, \tau'$$

Proof. By an argument very similar to that of the proof of Lemma 7.8. □

Lemma 7.10 (η expansion for rec). *If $\Xi \mid \Gamma \models e \preceq_{\mathrm{log}} e' : \tau \to \tau'$ and $\Xi \mid \Gamma \vdash e' : \tau \to \tau'$ then*

$$\Xi \mid \Gamma \models e \preceq_{\mathrm{ctx}} \texttt{rec}\, f(x) = (e'\ x) : \tau \to \tau'$$

Proof. We prove this by proving the following three contextual refinements

(a) $\Xi \mid \Gamma \models e \preceq_{\mathrm{ctx}} \texttt{let}\, y = e'\,\texttt{in}\,\texttt{rec}\, f(x) = (y\ x) : \tau \to \tau'$

(b) $\Xi \mid \Gamma \vDash \mathtt{let}\, y = e' \,\mathtt{in}\, \mathtt{rec}\, f(x) = (y\ x) \preceq_{\text{ctx}} \mathtt{rec}\, f(x) = \mathtt{let}\, y = e' \,\mathtt{in}\, (y\ x) : \tau \to \tau'$

(c) $\Xi \mid \Gamma \vDash \mathtt{rec}\, f(x) = \mathtt{let}\, y = e' \,\mathtt{in}\, (y\ x) \preceq_{\text{ctx}} \mathtt{rec}\, f(x) = (e'\ x) : \tau \to \tau'$

Case (a). We prove

$$\Xi \mid \Gamma \vDash e \preceq_{\log} \mathtt{let}\, y = e' \,\mathtt{in}\, \mathtt{rec}\, f(x) = (y\ x) : \tau \to \tau'$$

which is easy.

Case (b). This case is an instance of Lemma 7.8.

Case (c). We prove

$$\Xi \mid \Gamma \vDash \mathtt{rec}\, f(x) = \mathtt{let}\, y = e' \,\mathtt{in}\, (y\ x) \preceq_{\log} \mathtt{rec}\, f(x) = (e'\ x) : \tau \to \tau'$$

which is easy. □

Lemma 7.11 (η expansion for Λ). *If $\Xi \mid \Gamma \vDash e \preceq_{\log} e' : \forall X.\, \tau$ then*

$$\Xi \mid \Gamma \vDash e \preceq_{\text{ctx}} \Lambda\, (e'\ \_) : \forall X.\, \tau$$

Proof. We prove this by proving the following three contextual refinements

(a) $\Xi \mid \Gamma \vDash e \preceq_{\text{ctx}} \mathtt{let}\, x = e' \,\mathtt{in}\, \Lambda\, (x\ \_) : \forall X.\, \tau$

(b) $\Xi \mid \Gamma \vDash \mathtt{let}\, x = e' \,\mathtt{in}\, \Lambda\, (x\ \_) \preceq_{\text{ctx}} \Lambda\, \mathtt{let}\, x = e' \,\mathtt{in}\, (x\ \_) : \forall X.\, \tau$

(c) $\Xi \mid \Gamma \vDash \Lambda\, \mathtt{let}\, x = e' \,\mathtt{in}\, (x\ \_) \preceq_{\text{ctx}} \Lambda\, (e'\ \_) : \forall X.\, \tau$

Case (a). We prove

$$\Xi \mid \Gamma \vDash e \preceq_{\log} \mathtt{let}\, x = e' \,\mathtt{in}\, \Lambda\, (x\ \_) : \forall X.\, \tau$$

which is trivial.

Case (b). This case is an instance of Lemma 7.9.

Case (c). We prove

$$\Xi \mid \Gamma \vDash \Lambda\, \mathtt{let}\, x = e' \,\mathtt{in}\, (x\ \_) \preceq_{\log} \Lambda\, (e'\ \_) : \forall X.\, \tau$$

which is trivial. □

Lemma 7.12 (β reduction for λ). *If $\Xi \mid \Gamma \vDash \lambda\, x.\, e_1 \preceq_{\log} \lambda\, x.\, e_1' : \tau \to \tau'$, $\Xi \mid \Gamma \vDash e_2 \preceq_{\log} e_2' : \tau$, $\Xi \mid \Gamma, x : \tau \vdash e_1' : \tau'$ and $\Xi \mid \Gamma \vdash e_2' : \tau$, then*

$$\Xi \mid \Gamma \vDash (\lambda\, x.\, e_1)\ e_2 \preceq_{\text{ctx}} e_1'[e_2'/x] : \tau'$$

Proof. Let us assume the following

(a) $\Xi \mid \Gamma \vDash (\lambda\, x.\, e_1')\ e_2' \preceq_{\text{ctx}} e_1'[e_2'/x] : \tau'$

Given (a) above, we can prove our end result by soundness of the logical relation, transitivity of contextual refinement and

(b) $\Xi \mid \Gamma \vDash (\lambda\, x.\, e_1)\ e_2 \preceq_{\log} (\lambda\, x.\, e_1')\ e_2' : \tau'$

The case (b) follows easily by congruence. Hence we only need to prove (a).

We prove (a) by induction on the derivation of $\Xi \mid \Gamma, x : \tau \vdash e_1' : \tau'$.

1. Case ($\Xi \mid \Gamma, x : \tau \vdash x : \tau$):
   We have to show that $\Xi \mid \Gamma \vDash (\lambda\, x.\, x)\ e_2' \preceq_{\text{ctx}} e_2' : \tau$ which is trivial.
2. Case ($\Xi \mid \Gamma, x : \tau \vdash y : \tau'$): where $x \neq y$
   We have to show that $\Xi \mid \Gamma \vDash (\lambda\, x.\, y)\ e_2' \preceq_{\text{ctx}} y : \tau'$ which is trivial.
3. Case $\Xi \mid \Gamma, x : \tau \vdash () : \mathbf{1}$:
   We have to show that $\Xi \mid \Gamma \vDash (\lambda\, x.\, ())\ e_2' \preceq_{\text{ctx}} () : \mathbf{1}$ which is trivial.

(4) Case $\Xi \mid \Gamma, x : \tau \vdash \texttt{true} : \mathbb{B}$:
We have to show that $\Xi \mid \Gamma \vDash (\lambda\, x.\, \texttt{true})\ e_2' \preceq_{\mathrm{ctx}} \texttt{true} : \mathbb{B}$ which is trivial.

(5) Case $\Xi \mid \Gamma, x : \tau \vdash \texttt{false} : \mathbb{B}$:
We have to show that $\Xi \mid \Gamma \vDash (\lambda\, x.\, \texttt{false})\ e_2' \preceq_{\mathrm{ctx}} \texttt{false} : \mathbb{B}$ which is trivial.

(6) Case $\Xi \mid \Gamma, x : \tau \vdash n : \mathbb{N}$:
We have to show that $\Xi \mid \Gamma \vDash (\lambda\, x.\, n)\ e_2' \preceq_{\mathrm{ctx}} n : \mathbb{N}$ which is trivial.

(7) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e_1 : \tau_1 \qquad \Xi \mid \Gamma, x : \tau \vdash e_2 : \tau_2}{\Xi \mid \Gamma, x : \tau \vdash (e_1, e_2) : \tau_1 \times \tau_2}$:

IH$_1$: $\Xi \mid \Gamma \vDash (\lambda\, x.\, e_1)\ e_2' \preceq_{\mathrm{ctx}} e_1[e_2'/x] : \tau_1$
IH$_2$: $\Xi \mid \Gamma \vDash (\lambda\, x.\, e_2)\ e_2' \preceq_{\mathrm{ctx}} e_2[e_2'/x] : \tau_2$

We have to show that $\Xi \mid \Gamma \vDash (\lambda\, x.\, (e_1, e_2))\ e_2' \preceq_{\mathrm{ctx}} (e_1[e_2'/x], e_2[e_2'/x]) : \tau_1 \times \tau_2$

$$\begin{aligned} \lambda\, x.\, (e_1, e_2))\ e_2' &= \texttt{let}\, x = e_2'\, \texttt{in}\, (e_1, e_2) \\ &= \texttt{let}\, x = e_2'\, \texttt{in}\, (e_1, e_2[y/x][x/y]) && \text{for a fresh } y \end{aligned}$$

We prove
(i) $\Xi \mid \Gamma \vDash \texttt{let}\, x = e_2'\, \texttt{in}\, (e_1, e_2[y/x][x/y]) \preceq_{\mathrm{ctx}} ((\texttt{let}\, x = e_2'\, \texttt{in}\, e_1), (\texttt{let}\, y = e_2'\, \texttt{in}\, e_2[y/x])) : \tau_1 \times \tau_2$
by the transitivity of contextual refinement and following three logical relatednesses

$$\Xi \mid \Gamma \vDash \texttt{let}\, x = e_2'\, \texttt{in}\, (e_1, e_2[y/x][x/y]) \preceq_{\mathrm{log}} \texttt{let}\, y = e_2'\, \texttt{in}\, \texttt{let}\, x = e_2'\, \texttt{in}\, (e_1, e_2[y/x]) : \tau_1 \times \tau_2$$

$$\Xi \mid \Gamma \vDash \texttt{let}\, y = e_2'\, \texttt{in}\, \texttt{let}\, x = e_2'\, \texttt{in}\, (e_1, e_2[y/x]) \preceq_{\mathrm{log}} \texttt{let}\, y = e_2'\, \texttt{in}\, ((\texttt{let}\, x = e_2'\, \texttt{in}\, e_1), e_2[y/x]) : \tau_1 \times \tau_2$$

$$\Xi \mid \Gamma \vDash \texttt{let}\, y = e_2'\, \texttt{in}\, ((\texttt{let}\, x = e_2'\, \texttt{in}\, e_1), e_2[y/x]) \preceq_{\mathrm{log}} ((\texttt{let}\, x = e_2'\, \texttt{in}\, e_1), (\texttt{let}\, y = e_2'\, \texttt{in}\, e_2[y/x])) : \tau_1 \times \tau_2$$

The first of these logical relatednesses, after applying fundamental theorem to e_1, e_2, e_2', follows easily from the idempotency lemma. The other two are trivial and follow directly from the fundamental theorem.

The contextual refinement (i) above is the same as the following

$$\Xi \mid \Gamma \vDash (\lambda\, x.\, (e_1, e_2))\ e_2' \preceq_{\mathrm{ctx}} ((\lambda\, x.\, e_1)\ e_2'), ((\lambda\, x.\, e_2)\ e_2')) : \tau_1 \times \tau_2$$

The desired final result follows from this last contextual refinement, the induction hypotheses and the fact that contextual refinement is a congruence relation.

(8) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \tau_i \qquad i \in \{1, 2\}}{\Xi \mid \Gamma, x : \tau \vdash \texttt{inj}_i\, e : \tau_1 + \tau_2}$:

IH: $\Xi \mid \Gamma \vDash (\lambda\, x.\, e)\ e_2' \preceq_{\mathrm{ctx}} e[e_2'/x] : \tau_i$

We have to show that $\Xi \mid \Gamma \vDash (\lambda\, x.\, \texttt{inj}_i\, e)\ e_2' \preceq_{\mathrm{ctx}} (\texttt{inj}_i\, e)[e_2'/x] : \tau_1 + \tau_2$

Notice that it is easy to prove (using the fundamental theorem) that

$$\Xi \mid \Gamma \vDash (\lambda\, x.\, \texttt{inj}_i\, e)\ e_2' \preceq_{\mathrm{log}} \texttt{inj}_i\, ((\lambda\, x.\, e)\ e_2') : \tau_1 + \tau_2$$

The final result follows by the induction hypothesis, transitivity of contextual refinement and the fact that contextual refinement is a congruence relation.

(9) Case $\dfrac{\Xi \mid \Gamma, x : \tau, y : \tau_1, f : \tau_1 \to \tau_2 \vdash e : \tau_2}{\Xi \mid \Gamma, x : \tau \vdash \texttt{rec}\, f(y) = e : \tau_1 \to \tau_2}$:

IH: $\Xi \mid \Gamma, y : \tau_1, f : \tau_1 \to \tau_2 \vDash (\lambda\, x.\, e)\ e_2' \preceq_{\mathrm{ctx}} e[e_2'/x] : \tau_2$

We have to show that $\Xi \mid \Gamma \vDash (\lambda x.\, (\mathtt{rec}\, f(y) = e))\, e_2' \preceq_{\mathrm{ctx}} (\mathtt{rec}\, f(y) = e)[e_2'/x] : \tau_1 \to \tau_2$ or equivalently (by just massaging the terms) $\Xi \mid \Gamma \vDash \mathtt{let}\, x = e_2'\, \mathtt{in}\, (\mathtt{rec}\, f(y) = e) \preceq_{\mathrm{ctx}} (\mathtt{rec}\, f(y) = e[e_2'/x]) : \tau_1 \to \tau_2$.

Notice that the following is instance of rec-hoisting.

$$\Xi \mid \Gamma \vDash (\mathtt{let}\, x = e_2'\, \mathtt{in}\, (\mathtt{rec}\, f(y) = e)) \preceq_{\mathrm{ctx}} (\mathtt{rec}\, f(y) = \mathtt{let}\, x = e_2'\, \mathtt{in}\, e) : \tau_1 \to \tau_2$$

This latter contextual refinement is equivalent to (by massaging the terms) to the following.

$$\Xi \mid \Gamma \vDash (\mathtt{let}\, x = e_2'\, \mathtt{in}\, (\mathtt{rec}\, f(y) = e)) \preceq_{\mathrm{ctx}} (\mathtt{rec}\, f(y) = (\lambda x.\, e)\, e_2') : \tau_1 \to \tau_2$$

The final result follows by the induction hypothesis, transitivity of contextual refinement and the fact that contextual refinement is a congruence relation.

(10) Case $\dfrac{\Xi, X \mid \Gamma, x : \tau \vdash e : \tau_1}{\Xi \mid \Gamma, x : \tau \vdash \Lambda\, e : \forall X.\, \tau_1}$:
Similar to Case (9), we use Λ hoisting instead of λ hoisting.

(11) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \tau[\mu X.\, \tau_1/X]}{\Xi \mid \Gamma, x : \tau \vdash \mathtt{fold}\, e : \mu X.\, \tau_1}$:
Similar to Case (8).

(12) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \mu X.\, \tau_1}{\Xi \mid \Gamma, x : \tau \vdash \mathtt{unfold}\, e : \tau[\mu X.\, \tau_1/X]}$:
Similar to Case (8).

(13) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e_1 : \tau_1 \to \tau_2 \qquad \Xi \mid \Gamma \vdash e_2 : \tau_1}{\Xi \mid \Gamma, x : \tau \vdash e_1\, e_2 : \tau_2}$:
Similar to Case (7), by pushing the lambda in to get $((\lambda x.\, e_1)\, e_2')\, ((\lambda x.\, e_2)\, e_2')$.

(14) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \forall X.\, \tau_1 \qquad \Xi \vdash \tau_2}{\Xi \mid \Gamma, x : \tau_1 \vdash e\, \_ : \tau[\tau_2/X]}$:
Similar to Case (8).

(15) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \tau_1 \times \tau_2 \qquad i \in \{1, 2\}}{\Xi \mid \Gamma, x : \tau \vdash \pi_i\, e : \tau_i}$:
Similar to Case (8).

(16) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \tau_1 + \tau_2 \qquad \Xi \mid \Gamma, x : \tau, y : \tau_1 \vdash e_1 : \tau_3 \qquad \Xi \mid \Gamma, x : \tau, y : \tau_2 \vdash e_2 : \tau_3}{\Xi \mid \Gamma, x : \tau \vdash \mathtt{match}\, e\, \mathtt{with}\, \mathtt{inj}_i\, y \Rightarrow e_i\, \mathtt{end} : \tau_3}$:
Similar to Case (7), by pushing the lambda in to get $\mathtt{match}\, ((\lambda x.\, e)\, e_2')\, \mathtt{with}\, \mathtt{inj}_i\, y \Rightarrow ((\lambda x.\, e_i)\, e_2')\, \mathtt{end}$.

(17) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \mathbb{B} \qquad \Xi, x : \tau \mid \Gamma \vdash e_1 : \tau_1 \qquad \Xi \mid \Gamma, x : \tau \vdash e_2 : \tau_1}{\Xi \mid \Gamma, x : \tau \vdash \mathtt{if}\, e\, \mathtt{then}\, e_1\, \mathtt{else}\, e_2 : \tau_1}$:
Similar to Case (7), by pushing the lambda in to get $\mathtt{if}\, ((\lambda x.\, e)\, e_2')\, \mathtt{then}\, ((\lambda x.\, e_1)\, e_2')\, \mathtt{else}\, ((\lambda x.\, e_2)\, e_2')$.

(18) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e_1 : \mathbb{N} \qquad \Xi \mid \Gamma \vdash e_2 : \mathbb{N} \qquad \circledcirc \in \{+, -, *\}}{\Xi \mid \Gamma, x : \tau \vdash e_1 \circledcirc e_2 : \mathbb{N}}$:
Similar to Case (7), by pushing the lambda in to get $((\lambda x.\, e_1)\, e_2') \circledcirc ((\lambda x.\, e_2)\, e_2')$.

(19) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e_1 : \mathbb{N} \qquad \Xi \mid \Gamma, x : \tau \vdash e_2 : \mathbb{N} \qquad \circledcirc \in \{=, <\}}{\Xi \mid \Gamma, x : \tau \vdash e_1 \circledcirc e_2 : \mathbb{B}}$:
Similar to Case (7), by pushing the lambda in to get $((\lambda x.\, e_1)\, e_2') \circledcirc ((\lambda x.\, e_2)\, e_2')$.

(20) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \tau_1 \qquad \Xi \vdash \rho}{\Xi \mid \Gamma, x : \tau \vdash \mathtt{ref}(e) : \mathsf{ST}\, \rho\, (\mathsf{STRef}\, \rho\, \tau_1)}$:
Similar to Case (8).

(21) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \mathsf{STRef}\ \rho\ \tau_1}{\Xi \mid \Gamma, x : \tau \vdash\ !\,e : \mathsf{ST}\ \rho\ \tau_1}$:
Similar to Case (8).

(22) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e_1 : \mathsf{STRef}\ \rho\ \tau_1 \qquad \Xi \mid \Gamma \vdash e_2 : \tau_1}{\Xi \mid \Gamma, x : \tau \vdash e_1 \leftarrow e_2 : \mathsf{ST}\ \rho\ \mathbf{1}}$:
Similar to Case (7), by pushing the lambda in to get $((\lambda\, x.\, e_1)\ e_2') \leftarrow ((\lambda\, x.\, e_2)\ e_2')$.

(23) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e : \mathsf{STRef}\ \rho\ \tau_1 \qquad \Xi \mid \Gamma, x : \tau \vdash e_2 : \mathsf{STRef}\ \rho\ \tau_1}{\Xi \mid \Gamma, x : \tau \vdash e_1 == e_2 : \mathbb{B}}$:
Similar to Case (7), by pushing the lambda in to get $((\lambda\, x.\, e_1)\ e_2') == ((\lambda\, x.\, e_2)\ e_2')$.

(24) Case $\dfrac{\Xi \mid \Gamma, x : \tau \vdash e_1 : \mathsf{ST}\ \rho\ \tau_1 \qquad \Xi \mid \Gamma, x : \tau \vdash e_2 : \tau_1 \to (\mathsf{ST}\ \rho\ \tau_2)}{\Xi \mid \Gamma, x : \tau \vdash \mathtt{bind}\, e_1\, \mathtt{in}\, e_2 : \mathsf{ST}\ \rho\ \tau_2}$:
Similar to Case (7), by pushing the lambda in to get $\mathtt{bind}\,((\lambda\, x.\, e_1)\ e_2')\,\mathtt{in}\,((\lambda\, x.\, e_2)\ e_2')$.

(25) Case $\dfrac{\Xi, X \mid \Gamma, x : \tau \vdash e : \tau_1 \qquad \Xi \vdash \rho}{\Xi \mid \Gamma, x : \tau \vdash \mathtt{return}\, e : \mathsf{ST}\ \rho\ \tau_1}$:
Similar to Case (8).

(26) Case $\dfrac{\Xi, X \mid \Gamma, x : \tau \vdash e : \mathsf{ST}\ X\ \tau_1 \qquad \Xi \vdash \tau_1}{\Xi \mid \Gamma, x : \tau \vdash \mathtt{runST}\ \{e\} : \tau_1}$:
Similar to Case (8).

□

Lemma 7.13 (β reduction for Λ). *If* $\Xi \mid \Gamma \vDash \Lambda\, e \preceq_{\mathrm{log}} \Lambda\, e' : \forall X.\, \tau$ *then*

$$\Xi \mid \Gamma \vDash (\Lambda\, e)\ \_ \preceq_{\mathrm{ctx}} e' : \tau'$$

Proof. We prove $\Xi \mid \Gamma \vDash (\Lambda\, e)\ \_ \preceq_{\mathrm{log}} e' : \tau'$ which is rather easy. □

Lemma 7.14 (Rec unfolding). *If* $\Xi \mid \Gamma, x : \tau_1, f : \tau_1 \to \tau_2 \vDash e \preceq_{\mathrm{log}} e' : \tau_2$

$$\Xi \mid \Gamma \vDash \mathtt{rec}\, f(x) = e \preceq_{\mathrm{log}} \lambda\, x.\, e'[(\mathtt{rec}\, f(x) = e')/f] : \tau_1 \to \tau_2$$

Proof. Let us assume that we have

(1) γ, γ'
(2) $\vec{v}, \vec{v}'$
(3) $\mathcal{G}\llbracket \Xi \vdash \Gamma \rrbracket_\Delta(\vec{v}, \vec{v}')$
(4) regions
(5) h_1'
(6) $\boxed{\bullet\, \mathsf{excl}(h_1')}^{\gamma'}$
(7) w, w'
(8) $\llbracket \Xi \vdash \tau_1 \rrbracket_\Delta(w, w')$

We have to show (notice that $(\lambda\, x.\, e'[(\mathtt{rec}\, f(x) = e')/f])[\vec{v}'/\vec{x}] = \lambda\, x.\, e'[\vec{v}'/\vec{x}][(\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}])/f]$)

$$\mathsf{IC}^{\gamma}\ (\mathtt{rec}\, f(x) = e[\vec{v}/\vec{x}])\ w \left\{\!\!\left| v.\ \begin{array}{l} \exists h_2', v'.\ \left\langle h_1', (\lambda\, x.\, e'[\vec{v}'/\vec{x}][(\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}'])/f])\ w' \right\rangle \to_d^* \left\langle h_2', v' \right\rangle * \\ \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * \llbracket \Xi \vdash \tau \rrbracket_\Delta(v, v') * Q \end{array} \right|\!\!\right\}$$

By the compatibility lemma of rec we know that

(9) $\llbracket \Xi \vdash \tau_1 \to \tau_2 \rrbracket_\Delta((\mathtt{rec}\, f(x) = e[\vec{v}/\vec{x}]), (\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}]))$

Now by (9), (8), (6) and Lemma 4.4 case: 3 we get

(10) v, v', h_2'

(11) $\boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'}$

(12) $\left\langle h_1', (\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}])\; w' \right\rangle \to_d^* \langle h_2', v' \rangle$

(13) $[\![\Xi \vdash \tau_2]\!]_\Delta(v, v')$

and we have to show

$$\mathrel{|\!\!\Rrightarrow} \exists h_2', v'.\ \left\langle h_1', (\lambda x.\, e'[\vec{v}'/\vec{x}'][(\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}'])/f])\; w' \right\rangle \to_d^* \langle h_2', v' \rangle * \boxed{\bullet\, \mathsf{excl}(h_2')}^{\gamma'} * [\![\Xi \vdash \tau]\!]_\Delta(v, v') * Q$$

From (12) we know that

(14) $\left\langle h_1', (\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}])\; w' \right\rangle \to_d \left\langle h_1', e'[\vec{v}'/\vec{x}][w', (\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}])/x, f] \right\rangle$

(15) $\left\langle h_1', e'[\vec{v}'/\vec{x}][w', (\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}])/x, f] \right\rangle \to_d^* \langle h_2', v' \rangle$

We also know that

(16) $\left\langle h_1', (\lambda x.\, e'[\vec{v}'/\vec{x}'][(\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}'])/f])\; w' \right\rangle \to_d \left\langle h_1', e'[\vec{v}'/\vec{x}][(\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}])/f][w/x] \right\rangle$

And since x doesn't appear free in $(\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}])$ we can conclude

(17) $\left\langle h_1', (\lambda x.\, e'[\vec{v}'/\vec{x}'][(\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}'])/f])\; w' \right\rangle \to_d \left\langle h_1', e'[\vec{v}'/\vec{x}][w, (\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}])/x, f] \right\rangle$

And by (18) and (15) we know that

(18) $\left\langle h_1', (\lambda x.\, e'[\vec{v}'/\vec{x}'][(\mathtt{rec}\, f(x) = e'[\vec{v}'/\vec{x}'])/f])\; w' \right\rangle \to_d^* \langle h_2', v' \rangle$

which concludes the proof. □

Lemma 7.15 (β reduction for rec). *If* $\Xi \mid \Gamma \vDash \mathtt{rec}\, f(x) = e_1 \precsim_{\log} \mathtt{rec}\, f(x) = e_1' : \tau \to \tau', \Xi \mid \Gamma \vDash e_2 \precsim_{\log} e_2' : \tau$, $\Xi \mid \Gamma, x : \tau, f : \tau \to \tau' \vdash e_1' : \tau'$ *and* $\Xi \mid \Gamma \vdash e_2' : \tau$*, then*

$$\Xi \mid \Gamma \vDash (\mathtt{rec}\, f(x) = e_1)\; e_2 \precsim_{\mathrm{ctx}} e_1'[e_2', (\mathtt{rec}\, f(x) = e_1')/x, f] : \tau'$$

Proof. We prove this theorem using transitivity of contextual refinement and the following contextual refinements.

(a) $\Xi \mid \Gamma \vDash (\mathtt{rec}\, f(x) = e_1)\; e_2 \precsim_{\mathrm{ctx}} (\mathtt{rec}\, f(x) = e_1')\; e_2' : \tau'$
(b) $\Xi \mid \Gamma \vDash (\mathtt{rec}\, f(x) = e_1')\; e_2' \precsim_{\mathrm{ctx}} (\lambda x.\, e_1'[(\mathtt{rec}\, f(x) = e_1')/f])\; e_2' : \tau'$
(c) $\Xi \mid \Gamma \vDash (\lambda x.\, e_1'[(\mathtt{rec}\, f(x) = e_1')/f])\; e_2' \precsim_{\mathrm{ctx}} e_1'[e_2', (\mathtt{rec}\, f(x) = e_1')/x, f] : \tau'$

Case (a). We prove

$$\Xi \mid \Gamma \vDash (\mathtt{rec}\, f(x) = e_1)\; e_2 \precsim_{\log} (\mathtt{rec}\, f(x) = e_1')\; e_2' : \tau'$$

By congruence.

Case (b). We prove

$$\Xi \mid \Gamma \vDash (\mathtt{rec}\, f(x) = e_1')\; e_2' \precsim_{\log} (\lambda x.\, e_1'[(\mathtt{rec}\, f(x) = e_1')/f])\; e_2' : \tau'$$

This case follows by fundamental lemma (applied to e_1', e_2'), Lemma 7.14 and congruence.

Case (c). We prove

$$\Xi \mid \Gamma \vDash (\lambda\, x.\, e_1'[(\texttt{rec}\, f(x) = e_1')/f])\; e_2' \preceq_{\text{ctx}} e_1'[e_2', (\texttt{rec}\, f(x) = e_1')/x, f] : \tau'$$

Notice that since $\Xi \mid \Gamma, x : \tau, f : \tau \to \tau' \vdash e_1' : \tau'$, we know that

(1) $\Xi \mid \Gamma \vdash \texttt{rec}\, f(x) = e_1' : \tau'$

and consequently

(2) $\Xi \mid \Gamma, x : \tau \vdash \texttt{rec}\, f(x) = e_1' : \tau'$

As a result, we have

(3) $\Xi \mid \Gamma, x : \tau \vdash e_1'[(\texttt{rec}\, f(x) = e_1')/f] : \tau'$

which gives us

(4) $\Xi \mid \Gamma \vdash \lambda\, x.\, e_1'[(\texttt{rec}\, f(x) = e_1')/f] : \tau \to \tau'$

By applying the fundamental lemma in $\Xi \mid \Gamma \vdash e_2' : \tau$ and (4) we get

(5) $\Xi \mid \Gamma \vDash e_2' \preceq_{\text{log}} e_2' : \tau$
(6) $\Xi \mid \Gamma \vDash (\lambda\, x.\, e_1'[(\texttt{rec}\, f(x) = e_1')/f]) \preceq_{\text{log}} (\lambda\, x.\, e_1'[(\texttt{rec}\, f(x) = e_1')/f]) : \tau \to \tau'$

Therefore, we can apply Lemma 7.12 to get

$$\Xi \mid \Gamma \vDash (\lambda\, x.\, e_1'[(\texttt{rec}\, f(x) = e_1')/f])\; e_2' \preceq_{\text{ctx}} e_1'[(\texttt{rec}\, f(x) = e_1')/f][e_2'/x] : \tau'$$

But since x does not appear free in $(\texttt{rec}\, f(x) = e_1')$ we can rewrite it to

$$\Xi \mid \Gamma \vDash (\lambda\, x.\, e_1'[(\texttt{rec}\, f(x) = e_1')/f])\; e_2' \preceq_{\text{ctx}} e_1'[e_2', (\texttt{rec}\, f(x) = e_1')/x, f] : \tau'$$

which concludes this case. □

8 DISCUSSION: WHY WEAKEST PRECONDITIONS ARE UNSUITABLE

Previous works on representing logical relations in Iris (Krebbers et al. 2017b; Krogh-Jespersen et al. 2017) have used Iris's weakest preconditions for representing their logical relations. In this subsection we discuss why we opted not to use this construction. Understanding this subsection is in no way necessary for understanding the main results of the paper. In this part we assume reader's familiarity with weakest preconditions and invariants as are used in program logics intended for program verification in general and not exact details of these constructs in Iris.

What we explain here is *not* meant as a formal reason why weakest preconditions in Iris cannot be used to represent a logical relation for STLang that is powerful enough to prove the kind of properties that we do in this paper. We rather argue informally why the kind argument that we use in our proofs are not compatible with using weakest preconditions of Iris. These arguments can indeed be seen as a reductionist approach guiding one, step by step, from the use of weakest preconditions to using IC and futures.

The first problem that we immediately face with weakest preconditions is that they don't commute with separating conjunction.

$$\mathsf{wp}\; e\; \{v.\, P\} * \mathsf{wp}\; e\; \{v.\, Q\} \nvdash \mathsf{wp}\; e\; \{v.\, P * Q\}$$

To be fair, IC's, parallels of weakest preconditions in this work, do neither. But we can simply unfold them to reveal the future modality which does commute with the separating conjunction. But we can't simply unfold the definition of weakest preconditions as defined in Iris (see the definition of weakest preconditions in (Krebbers et al. 2017a)) to get a constructs that behaves this way. In any case, in order to see the problem with weakest preconditions commuting with separating conjunction consider the following example.

We can easily show that:

$$\Box\left(\mathsf{wp}\; \texttt{runST}\; \{\texttt{ref}(v)\}\; \left\{\ell.\, \boxed{\ell \mapsto \mathsf{ex}(v)}^{\gamma_{wp}}\right\}\right)$$

Here γ_{wp} is the (globally fixed) name for the monoid representing the heap for weakest preconditions. Using this fact, had we had the property of weakest preconditions commuting with separating conjunction, we could have derived

$$\mathsf{wp}\ \texttt{runST}\ \{\texttt{ref}(v)\}\ \left\{\ell.\ \boxed{\ell \mapsto \mathsf{ex}(v)}^{\gamma_{wp}} * \boxed{\ell \mapsto \mathsf{ex}(v)}^{\gamma_{wp}}\right\}$$

which is absurd. Let us then consider, for rest of this argument, a version of weakest precondition $\mathsf{wp}^{\gamma}\ e\ \{v.\ P\}$ with a generalized name for the monoid representing the heap just like IC.

In Iris weakest preconditions enforce that invariants (when used in to reason about weakest preconditions) can only be opened during execution of a physically atomic expression. There is also a side condition on the invariants: they cannot be opened multiple times in a nested fashion (as that clearly leads to unsoundness). That's why weakest preconditions $\mathsf{wp}^{\gamma}_{\mathcal{E}}\ e\ \{v.\ P\}$ in Iris are indexed by the set $\mathcal{E}$ of names for invariants that can be opened (we used a simpler version in this paper). Notice that $\mathsf{wp}^{\gamma}_{\mathcal{E}}\ e\ \{v.\ P\}$ states that we have the weakest precondition of expression e and may use invariants in $\mathcal{E}$ in atomic parts of e. Now if we have $\mathsf{wp}^{\gamma}_{\mathcal{E}}\ e\ \{v.\ P\} * \mathsf{wp}^{\gamma}_{\mathcal{E}}\ e\ \{v.\ Q\}$ where e is atomic then in $\mathsf{wp}^{\gamma}_{\mathcal{E}}\ e\ \{v.\ P * Q\}$ it is possible that some invariants in $\mathcal{E}$ are used twice. This can be either nested or consecutively. The former is obviously not possible while the latter would imply that we are using two logical steps for a single physical step – notice that weakest preconditions in Iris tie logical steps ($\triangleright$) with physical steps. This is clearly not possible. So at best we would want to prove

$$\mathsf{wp}^{\gamma}_{\mathcal{E}}\ e\ \{v.\ P\} * \mathsf{wp}^{\gamma}_{\mathcal{E}'}\ e\ \{v.\ Q\} \vdash \mathsf{wp}^{\gamma}_{\mathcal{E} \uplus \mathcal{E}'}\ e\ \{v.\ P * Q\}$$

Notice that this entailment, regardless of it being provable or even sound, is utterly useless. It implies that we cannot have a fixed mask in our logical relations which in turn implies that we cannot simply establish an invariant and then use it in different parts of the logical relation. This defeats the purpose of having and using invariants all together.

Here we have not shown the definition weakest preconditions in Iris. This definition entangles the reduction steps with logical steps (update and later modalities) so as to tie individual physical steps of execution to the logical ones. Untangling them in the $\mathsf{wp}^{\gamma}_{\mathcal{E}}\ e\ \{v.\ P\}$ predicate results directly in the definition of IC predicates.

9 IRIS AND KRIPKE WORLDS

In this subsection we describe the relation between the future modality as defined in the earlier part of this section in Iris and future worlds in logical relations based on Kripke worlds. We also argue why this is not possible to use weakest preconditions to define the logical relation as is usual practice when defining logical relations in Iris. Understanding this subsection is in *no way* necessary or helpful for understanding and appreciating the main results of this paper, i.e., the logical relation presented and the proof of theorems that justify purity of STLang.

Roughly speaking, the logical relatedness of two expressions $\mathit{Rel}(e, e')$ usually states something along the lines that whenever e reduces to a value v then so does e' reduce to a value v' and v and v' are suitably related, $\mathit{VRel}(v, v')$. Notice the similarity between logical relatedness and contextual refinement.

For logical relations based on Kripke worlds the relation is parameterized by a *world*. Each world W has a step index $W.\mathit{idx}$ and a relation $W.\mathit{Rel}$ that is mapping from the set of worlds with smaller step indexes to interpretations of values for each pair of memory locations related by W. The logical relatedness $\mathit{Rel}(W, e, e')$ would then more or less be stating that whenever e reduces in n steps, and the step-index of W, $W.\mathit{idx}$, is bigger than n then there is a *future* world, $W \sqsubseteq W'$, such that $W.\mathit{idx} - W'.\mathit{idx} = n$ and $\mathit{VRel}(W', v, v')$. The future relation is defined as follows:

$$W \sqsubseteq W' \triangleq W'.\mathit{idx} \leq W.\mathit{idx} \land \exists R_1, R_2.\ W'.\mathit{Rel} = R_1 \uplus R_2 \land W.\mathit{Rel}\ |_{W'.\mathit{idx}} = R_1$$

It basically says that a world W' is a future world of W if it has a less step-index and the relation of W' can be divided in two disjoint parts one which is the same as the relation of W when the latter is restricted to the step index of W'.

Working in Iris, we do not need to worry about step-indexes or worlds. These are all taken care of by Iris and buried under layers of abstraction.

In fact the underlying model of Iris involves step-indexes and Kripke worlds. However, these constructs are hidden deep under layers of abstraction and the user needs not to know or care about them. The *only* way to logically refer to step-indexes is the later modality. As to the contents of the worlds, the update modality $\mid\!\Rrightarrow P$ allows us to talk about the fact that there are *extensions* of the underlying worlds that P is satisfied.

More formally, a proposition $P : \mathit{iProp}$ in Iris is in fact internally defined as $\widehat{P} : \mathbb{N} \longrightarrow \mathit{iRes} \longrightarrow \mathrm{Prop}$ where *iRes* is the type of Iris resources (the parallel of worlds in Iris) and Prop is the type of propositions of the meta logic. Each Iris proposition basically says at each step-index which worlds it satisfy it. Notice that in Iris (Jung et al. 2016), resources themselves, much like Kripke worlds, are step-indexed. The basic connectives of Iris are defined in the model the way one would expect.[4]

$$\begin{aligned}
\widehat{P \wedge Q} &\triangleq \lambda n\, r.\, \widehat{P}\, n\, r \wedge \widehat{Q}\, n\, r \\
\widehat{P * Q} &\triangleq \lambda n\, r.\, \exists r_1, r_2.\, r = r_1 \hat{\cdot} r_2 \wedge \widehat{P}\, n\, r_1 \wedge \widehat{Q}\, n\, r_2 \\
\widehat{\forall x : A.\, Q} &\triangleq \lambda n\, r.\, \forall x : A.\, \widehat{(P\, x)}\, n\, r \\
&\vdots
\end{aligned}$$

Here $\hat{\cdot}$ is an operation that combines to worlds similar to disjoint union but is defined based on the operations of the monoids that are used for ghost states.[5] In particular the later modality and update modality are defined as follows:

$$\begin{aligned}
\widehat{\triangleright P} &\triangleq \lambda n\, r.\, \begin{cases} \widehat{P}\,(n-1)\, r & \text{if } n > 1 \\ \top & n = 0 \end{cases} \\
\widehat{\mid\!\Rrightarrow P} &\triangleq \lambda n\, r.\, \forall r_f.\, \checkmark_n(r \hat{\cdot} r_f) \Rightarrow \exists r'.\, \checkmark_n(r' \hat{\cdot} r_f) \wedge \widehat{P}\, n\, r'
\end{aligned}$$

Here $\checkmark_n(r)$ is validity up-to n steps for a step-indexed resource r. This is defined similar to $\hat{\cdot}$ based on the validity of the monoids that are used for the ghost states. In plain words, $\triangleright P$ at step index 0 accepts any world and at each step-index $n > 0$ accepts any world at step-index n that P would accept at step-index P. In other words, it only accepts worlds that are (1 step) in the future (without any extensions) of the worlds that P would accept. The proposition $\mid\!\Rrightarrow P$ on the other hand, accepts worlds that can be extended so that they satisfy P. When put together $\mid\!\Rrightarrow \triangleright P$ exactly spells out the condition for (1 step) future worlds that satisfy P.

$$\widehat{\mid\!\Rrightarrow \triangleright P} \triangleq \lambda n\, r.\, \begin{cases} \forall r_f.\, \checkmark_n(r \hat{\cdot} r_f) \Rightarrow \exists r'.\, \checkmark_n(r' \hat{\cdot} r_f) \wedge \widehat{P}\,(n-1)\, r' & \text{if } n > 1 \\ \forall r_f.\, \checkmark_n(r \hat{\cdot} r_f) \Rightarrow \exists r'.\, \checkmark_n(r' \hat{\cdot} r_f) & n = 0 \end{cases}$$

Hence the future modality $\mid\!\equiv\!\{n\}\!\equiv\!\triangleright P$ is basically satisfied by worlds for which there is a future state n steps away that satisfies P.

[4] Many of the internal representations presented here are simplified versions of what is actually defined in the actual model of Iris.

[5] Iris is a general framework can be instantiated by the user picking the monoids that the user needs for representing the ghost state for their particular application.

REFERENCES

Amal Ahmed. 2004. *Semantics of Types for Mutable State.* Ph.D. Dissertation. Princeton University.

Amal J. Ahmed, Andrew W. Appel, and Roberto Virga. 2002. A Stratified Semantics of General References Embeddable in Higher-Order Logic. In *Proceedings of 17th Annual IEEE Symposium Logic in Computer Science*. IEEE Computer Society Press, 75–86.

Andrew Appel and David McAllester. 2001. An Indexed Model of Recursive Types for Foundational Proof-Carrying Code. *TOPLAS* 23, 5 (2001), 657–683.

Andrew Appel, Paul-André Melliès, Christopher Richards, and Jérôme Vouillon. 2007. A Very Modal Model of a Modern, Major, General Type System. In *POPL*.

Lars Birkedal, Bernhard Reus, Jan Schwinghammer, Kristian Støvring, Jacob Thamsborg, and Hongseok Yang. 2011. Step-Indexed Kripke Models over Recursive Worlds. In *POPL*.

D. Dreyer, A. Ahmed, and L. Birkedal. 2011. Logical Step-Indexed Logical Relations. *LMCS* 7, 2:16 (2011).

Ralf Jung, Robbert Krebbers, Lars Birkedal, and Derek Dreyer. 2016. Higher-order ghost state. In *ICFP*. 256–269.

Ralf Jung, David Swasey, Filip Sieczkowski, Kasper Svendsen, Aaron Turon, Lars Birkedal, and Derek Dreyer. 2015. Iris: Monoids and Invariants as an Orthogonal Basis for Concurrent Reasoning. In *POPL*. 637–650.

Robbert Krebbers, Ralf Jung, Ale Bizjak, Jacques-Henri Jourdan, Derek Dreyer, and Lars Birkedal. 2017a. The essence of higher-order concurrent separation logic. In *European Symposium on Programming (ESOP)*.

Robbert Krebbers, Amin Timany, and Lars Birkedal. 2017b. Interactive Proofs in Higher-Order Concurrent Separation Logic. In *POPL*.

Morten Krogh-Jespersen, Kasper Svendsen, and Lars Birkedal. 2017. A relational model of types-and-effects in higher-order concurrent separation logic. In *POPL*.