Relational Cost Analysis for Functional-Imperative Programs (Appendix)

Weihao Qu

University at Buffalo, SUNY

Marco Gaboardi

University at Buffalo, SUNY

Deepak Garg

MPI-SWS

May 2019

Contents

List of Figures

List of Theorems and Lemmas

1 Syntax

Unary types $A ::= \mathsf{int} \mid \mathsf{int}[I] \mid \mathsf{unit} \mid \{P\}\, \overset{\mathsf{exec}(L,U)}{\exists \vec{\gamma}.A}\, \{Q\} \mid \overset{\mathsf{exec}(L,U)}{\forall i :: S.\ A} \mid \overset{\mathsf{exec}(L,U)}{A \longrightarrow A'} \mid \mathsf{Array}_\gamma[I]\ A \mid \mathsf{list}[I]\ A \mid A_1 + A_2 \mid C \& A \mid C \supset A \mid \exists i :: S.\ A$

Relational types $\tau ::= \mathsf{int}_r \mid \mathsf{unit}_r \mid \mathsf{int}[I] \mid \{P\}\, \overset{\mathsf{diff}(D)}{\exists \vec{\gamma}.\tau}\, \{Q\} \mid \overset{\mathsf{diff}(D)}{\forall i :: S.\ \tau} \mid \overset{\mathsf{diff}(D)}{\tau \longrightarrow \tau'} \mid \mathsf{Array}_\gamma[I]\ \tau \mid U\ (A_1, A_2) \mid \mathsf{list}^\alpha[I]\ \tau \mid \Box\tau \mid \tau_1 + \tau_2 \mid C \& \tau \mid C \supset \tau \mid \exists i :: S.\ \tau$

Index terms $I, L, U, D, \alpha, \beta ::= i \mid b \mid n \mid r \mid I_1 + I_2 \mid I_1 * I_2 \mid I_1 - I_2 \mid max(I_1, I_2) \mid min(I_1, I_2) \mid log_2(I) \mid \lfloor I \rfloor \mid \lceil I \rceil \mid \{I_i\}_{i \in K} \mid \beta \cup \beta \mid \beta \setminus \beta \mid \beta \cap \beta$

Sort $S ::= \mathbb{R} \mid \mathbb{N} \mid \mathbb{B} \mid \mathbb{P} \mid \mathbb{L}$

Terms $t ::= x \mid n \mid r \mid () \mid \lambda x.t \mid \mathsf{fix}\, f(x).t \mid t_1\ t_2 \mid \mathsf{let}\ x = t_1\ \mathsf{in}\ t_2 \mid \mathsf{inl}\ t \mid \mathsf{inr}\ t \mid \mathsf{case}\ (t, x.t_1, y.t_2) \mid \Lambda.t \mid t\,[] \mid \mathsf{pack}\ t \mid \mathsf{unpack}\ t_1\ \mathsf{as}\ x\ \mathsf{in}\ t_2 \mid \mathsf{celim}\ t \mid \mathsf{return}\ t \mid \mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2 \mid \mathsf{alloc}\ t_1\ t_2 \mid \mathsf{read}\ t_1\ t_2 \mid \mathsf{updt}\ t_1\ t_2\ t_3$

Values $v ::= n \mid l \mid r \mid () \mid \lambda x.t \mid \mathsf{fix}\, f(x).t \mid \mathsf{inl}\ v \mid \mathsf{inr}\ v \mid \Lambda.t \mid \mathsf{pack}\ v \mid \mathsf{return}\ t \mid \mathsf{alloc}\ t_1\ t_2 \mid \mathsf{updt}\ t_1\ t_2\ t_3 \mid \mathsf{read}\ t_1\ t_2 \mid \mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2$

Unary Type Env. $\Omega ::= \emptyset \mid \Omega, x : A$

Relational Type Env. $\Gamma ::= \emptyset \mid \Gamma, x : \tau$

Sort Env. $\Delta ::= \emptyset \mid \Delta, i :: S$

Loc Env. $\Sigma ::= \emptyset \mid \Sigma, \gamma :: \mathbb{L}$

Constraint $C ::= I_1 = I_2 \mid I_1 < I_2 \mid \neg C \mid I_1 \in I_2$

Constraint Env. $\Phi ::= \top \mid C \wedge \Phi$

Assertions $P, Q ::= \mathsf{empty} \mid \gamma \rightarrow \beta \mid P \star Q \mid P \cup Q$

Unary Heap $H ::= [] \mid [l \rightarrow z] \mid H_1 \uplus H_2$

array $z ::= [v_1, \ldots, v_m]$

$n \in \mathbb{N},\ r \in \mathbb{R},\ x \in Var,\ i \in iVar,\ \gamma \in iLoc,\ l \in dLoc$

$$
\begin{array}{rcl}
P[\gamma] & & \\
\mathsf{empty}[\gamma] & = & \emptyset \\
(\gamma' \rightarrow \beta)[\gamma] & = & \beta \,\mathsf{if}\ \gamma = \gamma' \\
 & = & \emptyset\ \mathsf{otherwise} \\
(P \star Q)[\gamma] & = & P[\gamma] \mathsf{if}\ \gamma \in dom(P) \\
 & = & Q[\gamma] \mathsf{if}\ \gamma \in dom(Q) \\
 & = & \emptyset\ \mathsf{otherwise} \\
(P \sqcup Q)[\gamma] & = & P[\gamma] \cup Q[\gamma] \mathsf{iff}\ \gamma \in dom(P) \cap dom(Q) \\
 & = & P[\gamma] \mathsf{if}\ \gamma \in dom(P), \gamma \notin dom(Q) \\
 & = & Q[\gamma] \mathsf{if}\ \gamma \notin dom(P), \gamma \in dom(Q) \\
 & = & \emptyset\ \mathsf{if}\ \gamma \notin dom(P), \gamma \notin dom(Q)
\end{array}
$$

Figure 1: Syntax of Values & Expressions

$\boxed{t; H \Downarrow_p^{c,k} v; H_1}$

$$\frac{t \Downarrow^{c_1,k_1} v' \qquad v'; H \Downarrow_f^{c_2,k_2} v; H'}{t; H \Downarrow_p^{c_1+c_2,k_1+k_2} v; H'}\ \text{E-P}$$

$\boxed{t \Downarrow^{c,k} v}$

$$\frac{}{v \Downarrow^{0,0} v}\ \text{E-V} \qquad \frac{t \Downarrow^{c,k} v}{\text{inl}\ t \Downarrow^{c,k} \text{inl}\ v}\ \text{E-INL} \qquad \frac{t \Downarrow^{c,k} v}{\text{inr}\ \ t \Downarrow^{c,k} \text{inr}\ \ v}\ \text{E-INR}$$

$$\frac{t \Downarrow^{c_1,k_1} \text{inl}\ v \qquad t_1[v/x] \Downarrow^{c_2,k_2} v_r}{\text{case}\ (t, x.t_1, y.t_2) \Downarrow^{c_1+c_2+c_{\text{case}},k_1+k_2+1} v_r}\ \text{E-CASEL} \qquad \frac{t \Downarrow^{c_1,k_1} \text{inr}\ \ v \qquad t_2[v/y] \Downarrow^{c_2,k_2} v_r}{\text{case}\ (t, x.t_1, y.t_2) \Downarrow^{c_1+c_2+c_{\text{case}},k_1+k_2+1} v_r}\ \text{E-CASER}$$

$$\frac{t_1 \Downarrow^{c_1,k_1} \lambda x.t' \qquad t_2 \Downarrow^{c_2,k_2} v \qquad t'[v/x] \Downarrow^{c_3,k_3} v_1}{t_1\ t_2 \Downarrow^{c_1+c_2+c_3+c_{\text{app}},k_1+k_2+k_3+1} v_1}\ \text{E-A} \qquad \frac{t_1 \Downarrow^{c_1,k_1} v \qquad t_2/[v/x] \Downarrow^{c_2,k_2} v_1}{\text{let}\ x = t_1\ \text{in}\ t_2 \Downarrow^{c_1+c_2+c_{\text{lt}},k_1+k_2+1} v_1}\ \text{E-LT}$$

$$\frac{t_1 \Downarrow^{c_1,k_1} \text{fix}\, f\, x.t' \qquad t_2 \Downarrow^{c_2,k_2} v \qquad t'[\text{fix}\, f\, x.t'/f][v/x] \Downarrow^{c_3,k_3} v_1}{t_1\ t_2 \Downarrow^{c_1+c_2+c_3+c_{\text{app}},k_1+k_2+k_3+1} v_1}\ \text{E-F}$$

$\boxed{t; H \Downarrow_f^{c,k} v; H_1}$

$$\frac{t \Downarrow^{c,k} v}{\text{return}\ t; H \Downarrow_f^{c+c_{\text{ret}},k+1} v; H}\ \text{F-T}$$

$$\frac{t_1 \Downarrow^{c_1,k_1} v \qquad v; H \Downarrow_f^{c_2,k_2} v_1; H_1 \qquad t_2[v_1/x] \Downarrow^{c_3,k_3} v_2 \qquad v_2; H_1 \Downarrow_f^{c_4,k_4} v_3; H_2}{\text{let}\ \{x\} = t_1\ \text{in}\ t_2; H \Downarrow_f^{c_1+c_2+c_3+c_4+c_{\text{let}},k_1+k_2+k_3+k_4+1} v_3; H_2}\ \text{F-E}$$

$$\frac{t_1 \Downarrow^{c_1,k_1} l \qquad t_2 \Downarrow^{c_2,k_2} n \qquad t_3 \Downarrow^{c_3,k_3} v}{\text{updt}\ t_1\ t_2\ t_3; H \Downarrow_f^{c_1+c_2+c_3+c_{\text{update}},k_1+k_2+k_3+1} (); H(l)[n] \leftarrow v}\ \text{F-U}$$

$$\frac{t_1 \Downarrow^{c_1,k_1} l \qquad t_2 \Downarrow^{c_2,k_2} n_2 \qquad H(l)[n] = v}{\text{read}\ t_1\ t_2; H \Downarrow_f^{c_1+c_2+c_{\text{read}},k_1+k_2+1} v; H}\ \text{F-R}$$

$$\frac{t_1 \Downarrow^{c_1,k_1} n \qquad t_2 \Downarrow^{c_2,k_2} v \qquad z = [\overbrace{v, \ldots, v}^{n}] \qquad l\ \text{fresh}}{\text{alloc}\, t_1\, t_2; H \Downarrow_f^{c_1+c_2+c_{\text{alloc}},k_1+k_2+1} l; H, l \rightarrow z}\ \text{F-L}$$

Figure 2: Operational Semantics: (1) standard, (2) forcing evaluation.

$$
\begin{array}{rcl}
|.|_{i\in\{1,2\}} & : & \mathsf{Binarytype} \to \mathsf{Unarytype} \\
|\mathrm{int}_r|_i & = & \mathrm{int} \\
|\mathrm{unit}_r|_i & = & \mathrm{unit} \\
|\ \{P\}\ \exists \vec{\gamma} : \tau\ \{Q\}\ \overset{\mathrm{diff}(c)}{}|_i & = & \{|P|_i\}\ \exists \vec{\gamma} : |\tau|_i\ \{|Q|_i\}\ \overset{\mathrm{exec}(0,\infty)}{} \\
|\ \tau \longrightarrow \tau'\ \overset{\mathrm{diff}((c))}{}|_i & = & |\tau|_i \overset{\mathrm{exec}(0,\infty)}{\longrightarrow} |\tau'|_i \\
|\ \mathsf{Array}_\gamma[I]\ \tau\ |_i & = & \mathsf{Array}_\gamma[I]\ |\tau|_i \\
|U\ A|_i & = & A_i \\
|\Box\tau|_i & = & |\tau|_i \\
|\ \mathsf{list}^\alpha[I]\ \tau\ |_i & = & \mathsf{list}[I]\ |\tau|_i \\
|\tau_1 + \tau_2|_i & = & |\tau_1|_i + |\tau_2|_i \\
|C \& \tau|_i & = & C \& |\tau|_i \\
|C \supset \tau|_i & = & C \supset |\tau|_i \\
|\emptyset|_i & = & \emptyset \\
|\Gamma, x:\tau|_i & = & |\Gamma|_i, x : |\tau|_i \\
|\Gamma, x:\tau, x:U(A_1,A_2)|_i & = & |\Gamma|_i, x : A_i \\
|\mathsf{empty}|_i & = & \mathsf{empty} \\
|\gamma_n \to \beta_n|_i & = & \gamma_n \to \mathbb{N}
\end{array}
$$

Figure 3: Binary to unary type erasure

$\boxed{\vdash \Delta}$

$$\frac{}{\vdash \emptyset}\ \textsc{senv-empty} \qquad \frac{\vdash \Delta \qquad i \in \mathsf{iVar} \qquad S \in \mathsf{Sort}}{\vdash \Delta, i :: S}\ \textsc{senv-iv}$$

Figure 4: sort environment well formedness

$\boxed{\vdash \Sigma}$

$$\frac{}{\vdash \emptyset}\ \textsc{lenv-empty} \qquad \frac{\vdash \Sigma \qquad \gamma \in \mathsf{iLoc}}{\vdash \Sigma, \gamma :: \mathbb{L}}\ \textsc{lenv-lv}$$

Figure 5: location environment well-formedness

$\boxed{\Sigma; \Delta \vdash P \quad wf}$

$$\frac{}{\Sigma; \Delta \vdash \mathsf{empty} \quad wf}\ \textsc{wf-as-empty} \qquad \frac{\Sigma; \Delta \vdash \gamma :: \mathbb{L} \qquad \Sigma; \Delta \vdash \beta :: \mathbb{P}}{\Sigma; \Delta \vdash \gamma \to \beta \quad wf}\ \textsc{wf-as-referTo}$$

$$\frac{\Sigma; \Delta \vdash P \quad wf \qquad \Sigma; \Delta \vdash Q \quad wf}{\Sigma; \Delta \vdash P * Q \quad wf}\ \textsc{wf-as-star}$$

Figure 6: Assertion well-formedness

$\boxed{\Delta \vdash C \quad wf}$

$$\frac{\Delta \vdash I_1 :: S \qquad \Delta \vdash I_2 :: S \qquad S \in \{\mathbb{N}, \mathbb{R}\}}{\Delta \vdash I_1 = I_2 \quad wf}\ \text{WF-CS-EQ} \qquad \frac{\Delta \vdash I_1 :: S \qquad \Delta \vdash I_2 :: S \qquad S \in \{\mathbb{N}, \mathbb{R}\}}{\Delta \vdash I_1 < I_2 \quad wf}\ \text{WF-CS-LT}$$

$$\frac{\Delta \vdash C \quad wf}{\Delta \vdash \neg C \quad wf}\ \text{WF-CS-NEG}$$

Figure 7: Constraint well-formedness

$\boxed{\Sigma; \Delta \vdash I :: S}$

$$\frac{\Delta(i) = S}{\Sigma; \Delta \vdash i :: S}\ \text{I-VAR} \qquad \frac{\Sigma(\gamma) = \mathbb{L}}{\Sigma; \Delta \vdash \gamma :: \mathbb{L}}\ \text{I-LOC} \qquad \frac{}{\Sigma; \Delta \vdash b :: \mathbb{B}}\ \text{I-BOOL}$$

$$\frac{}{\Sigma; \Delta \vdash n :: \mathbb{N}}\ \text{I-NAT} \qquad \frac{}{\Sigma; \Delta \vdash r :: \mathbb{R}}\ \text{I-REAL}$$

$$\frac{\Sigma; \Delta \vdash I_1 :: \mathbb{N} \qquad \Sigma; \Delta \vdash I_2 :: \mathbb{N} \qquad \diamond \in \{min, max, +, -, *, \}}{\Sigma; \Delta \vdash (I_1 \diamond I_2) :: \mathbb{N}}\ \text{I-BIN-N}$$

$$\frac{\Sigma; \Delta \vdash I_1 :: \mathbb{R} \qquad \Sigma; \Delta \vdash I_2 :: \mathbb{R} \qquad \diamond \in \{min, max, +, -, *, \}}{\Sigma; \Delta \vdash (I_1 \diamond I_2) :: \mathbb{R}}\ \text{I-BIN-R}$$

$$\frac{\Sigma; \Delta \vdash I :: \mathbb{R} \qquad \circ \in \{\lfloor\ \rfloor, \lceil\ \rceil\}}{\Sigma; \Delta \vdash (\circ I) :: \mathbb{N}}\ \text{I-UNARY-R}$$

$$\frac{\Sigma; \Delta \vdash I :: \mathbb{R}}{\Sigma; \Delta \vdash log_2(I) :: \mathbb{R}}\ \text{I-LOG}$$

$$\frac{\Sigma; \Delta \vdash I_i :: \mathbf{N} \quad \forall i \in K \subseteq \mathbb{N}}{\Sigma; \Delta \vdash \{I_i\}_{i \in K} :: \mathbf{P}}\ \text{I-NATSET} \qquad \frac{\Sigma; \Delta \vdash \beta_1 :: \mathbf{P} \qquad \Sigma; \Delta \vdash \beta_2 :: \mathbf{P} \qquad \diamond \in \{\cup, \cap, /\}}{\Sigma; \Delta \vdash \beta_1 \diamond \beta_2 :: \mathbf{P}}\ \text{I-SET-OP}$$

Figure 8: Sorting rules

$\boxed{\Sigma;\Delta;\Phi \vdash A \quad wf}$

$$\frac{}{\Sigma;\Delta;\Phi \vdash \emptyset \quad wf}\ \text{WF-A-OMEGA-EMPTYSET} \qquad \frac{\Sigma;\Delta;\Phi \vdash \Omega \quad wf \qquad \Sigma;\Delta;\Phi \vdash A \quad wf}{\Sigma;\Delta;\Phi \vdash \Omega, x : A \quad wf}\ \text{WF-A-OMEGA}$$

$$\frac{}{\Sigma;\Delta;\Phi \vdash unit \quad wf}\ \text{WF-A-UNIT} \qquad \frac{}{\Sigma;\Delta;\Phi \vdash Int \quad wf}\ \text{WF-A-INT} \qquad \frac{\Sigma;\Delta \vdash I :: \mathbb{N}}{\Sigma;\Delta;\Phi \vdash \text{int}[I] \quad wf}\ \text{WF-A-INT-I}$$

$$\frac{\Sigma;\Delta;\Phi \vdash A_1 \quad wf \qquad \Sigma;\Delta;\Phi \vdash A_2 \quad wf}{\Sigma;\Delta;\Phi \vdash A_1 + A_2 \quad wf}\ \text{WF-A-SUM}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi \vdash A \quad wf \qquad \Sigma;\Delta \vdash \gamma :: \mathbb{L} \\ \Sigma;\Delta \vdash L :: \mathbb{R} \qquad \Sigma;\Delta \vdash U :: \mathbb{R} \qquad \Sigma;\Delta \vdash P \quad wf \qquad \Sigma, \vec{\gamma} : \vec{\mathbb{L}};\Delta \vdash Q \quad wf\end{array}}{\begin{array}{c}\text{exec}(L,U) \\ \Sigma;\Delta;\Phi \vdash \{P\}\ \exists \vec{\gamma} : A\ \{Q\} \quad wf\end{array}}\ \text{WF-A-MONAD}$$

$$\frac{\Sigma;\Delta;\Phi \vdash A \quad wf \qquad \Sigma;\Delta;\Phi \vdash A' \quad wf \qquad \Sigma;\Delta \vdash L :: \mathbb{R} \qquad \Sigma;\Delta \vdash U :: \mathbb{R}}{\begin{array}{c}\text{exec}(L,U) \\ \Sigma;\Delta;\Phi \vdash A \longrightarrow A' \quad wf\end{array}}\ \text{WF-A-ARROW}$$

$$\frac{\Sigma;\Delta \vdash \gamma :: \mathbb{L} \qquad \Sigma;\Delta \vdash I :: \mathbb{N} \qquad \Sigma;\Delta;\Phi \vdash A \quad wf}{\Sigma;\Delta;\Phi \vdash \mathsf{Array}_\gamma[I]\ A \quad wf}\ \text{WF-A-ARRAY}$$

$$\frac{\Sigma; i :: S,\Delta;\Phi \vdash A \quad wf \qquad \Sigma; i :: S,\Delta \vdash L :: \mathbb{R} \qquad \Sigma; i :: S,\Delta \vdash U :: \mathbb{R}}{\begin{array}{c}\text{exec}(L,U) \\ \Sigma;\Delta;\Phi \vdash \forall i :: S.\ A \quad wf\end{array}}\ \text{WF-A-FORALL}$$

$$\frac{\Sigma; i :: S,\Delta;\Phi \vdash A \quad wf}{\Sigma;\Delta;\Phi \vdash \exists i :: S.\ A \quad wf}\ \text{WF-A-EXIST}$$

$$\frac{\Delta \vdash I :: \mathbb{N} \qquad \Sigma;\Delta;\Phi \vdash A \quad wf}{\Sigma;\Delta;\Phi \vdash \mathsf{list}[I]\ A \quad wf}\ \text{WF-A-LIST}$$

$$\frac{\Delta \vdash C \quad wf \qquad \Sigma;\Delta;\Phi \wedge C \vdash A \quad wf}{\Sigma;\Delta;\Phi \vdash C \& A \quad wf}\ \text{WF-A-C-AND}$$

$$\frac{\Delta \vdash C \quad wf \qquad \Sigma;\Delta;\Phi \wedge C \vdash A \quad wf}{\Sigma;\Delta;\Phi \vdash C \supset A \quad wf}\ \text{WF-A-C-IMPLY}$$

Figure 9: Well-formedness of unary types

$\boxed{\Sigma;\Delta;\Phi \vdash \tau \quad wf}$

$$\frac{}{\Sigma;\Delta;\Phi \vdash \emptyset \quad wf}\ \text{WF-R-GAMMA-EMPTYSET} \qquad \frac{\Sigma;\Delta;\Phi \vdash \Gamma \quad wf \qquad \Sigma;\Delta;\Phi \vdash \tau \quad wf}{\Sigma;\Delta;\Phi \vdash \Gamma, x:\tau \quad wf}\ \text{WF-R-GAMMA}$$

$$\frac{}{\Sigma;\Delta;\Phi \vdash \text{unit}_r \quad wf}\ \text{WF-R-UNIT} \qquad \frac{}{\Sigma;\Delta;\Phi \vdash \text{int}_r \quad wf}\ \text{WF-R-INT}$$

$$\frac{\Sigma;\Delta;\Phi \vdash \tau_1 \quad wf \qquad \Sigma;\Delta;\Phi \vdash \tau_2 \quad wf}{\Sigma;\Delta;\Phi \vdash \tau_1 + \tau_2 \quad wf}\ \text{WF-R-SUM}$$

$$\frac{\Sigma;\Delta \vdash P \quad wf \qquad \Sigma;\Delta;\Phi \vdash \tau \quad wf \qquad \Sigma;\Delta,\vec{\gamma}:\vec{\mathbb{L}} \vdash Q \quad wf \qquad \Sigma;\Delta \vdash D :: \mathbb{R}}{\Sigma;\Delta;\Phi \vdash \{P\}\ \overset{\text{diff}(D)}{\exists \vec{\gamma}:\tau}\ \{Q\} \quad wf}\ \text{WF-R-MONAD}$$

$$\frac{\Sigma;\Delta;\Phi \vdash \tau \quad wf \qquad \Sigma;\Delta;\Phi \vdash \tau' \quad wf \qquad \Sigma;\Delta \vdash D :: \mathbb{R}}{\Sigma;\Delta;\Phi \vdash \tau \overset{\text{diff}(D)}{\longrightarrow} \tau' \quad wf}\ \text{WF-R-ARROW}$$

$$\frac{\Sigma;i :: S,\Delta;\Phi \vdash \tau \quad wf \qquad \Sigma;i :: S,\Delta \vdash D :: \mathbb{R}}{\Sigma;\Delta;\Phi \vdash \overset{\text{diff}(D)}{\forall i :: S.}\ \tau \quad wf}\ \text{WF-R-FORALL} \qquad \frac{\Sigma;i :: S,\Delta;\Phi \vdash \tau \quad wf}{\Sigma;\Delta;\Phi \vdash \exists i :: S.\ \tau \quad wf}\ \text{WF-R-EXIST}$$

$$\frac{\Sigma;\Delta \vdash \gamma :: \mathbb{L} \qquad \Sigma;\Delta \vdash I :: \mathbb{N} \qquad \Sigma;\Delta;\Phi \vdash \tau \quad wf}{\Sigma;\Delta;\Phi \vdash \mathsf{Array}_\gamma[I]\ \tau \quad wf}\ \text{WF-R-ARRAY}$$

$$\frac{\Sigma;\Delta;\Phi \vdash A_1 \quad wf \qquad \Sigma;\Delta;\Phi \vdash A_2 \quad wf}{\Sigma;\Delta;\Phi \vdash U\ (A_1, A_2) \quad wf}\ \text{WF-R-UA}$$

$$\frac{\Sigma;\Delta \vdash \alpha :: \mathbb{N} \qquad \Sigma;\Delta \vdash I :: \mathbb{N} \qquad \Sigma;\Delta;\Phi \vdash \tau \quad wf}{\Sigma;\Delta;\Phi \vdash \mathsf{list}^\alpha[I]\ \tau \quad wf}\ \text{WF-R-LIST}$$

$$\frac{\Delta \vdash C \quad wf \qquad \Sigma;\Delta;\Phi \wedge C \vdash \tau \quad wf}{\Sigma;\Delta;\Phi \vdash C \& \tau \quad wf}\ \text{WF-R-C-AND}$$

$$\frac{\Delta \vdash C \quad wf \qquad \Sigma;\Delta;\Phi \wedge C \vdash \tau \quad wf}{\Sigma;\Delta;\Phi \vdash C \supset \tau \quad wf}\ \text{WF-R-C-IMPLY} \qquad \frac{\Sigma;\Delta;\Phi \vdash \tau \quad wf}{\Sigma;\Delta;\Phi \vdash \Box\tau \quad wf}\ \text{WF-R-SQUARE}$$

Figure 10: Well-formedness of relational types

$\boxed{\Omega \vdash H \quad wf}$

$$\frac{}{\Omega \vdash empty \quad wf}\ \text{WF-H-EMPTY} \qquad \frac{\Omega \vdash H \quad wf \qquad x \notin dom(H)}{\Omega \vdash (H, x \to k) \quad wf}\ \text{WF-H-UPDATE}$$

Figure 11: Heap well-formedness

$\boxed{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : A}$

$$\frac{}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} n : \text{int}}\ \text{U-INT} \qquad \frac{}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} n : \text{int}[n]}\ \text{U-I} \qquad \frac{\Sigma;\Delta;\Phi;\Omega, x : A \vdash^{U}_{L} t : B}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} \lambda x.t : A \overset{\text{exec}(L,U)}{\longrightarrow} B}\ \text{U-ABS}$$

$$\frac{\Omega(x) = A}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} x : A}\ \text{U-V} \qquad \frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t_1 : A \overset{\text{exec}(L,U)}{\longrightarrow} B \qquad \Sigma;\Delta;\Phi;\Omega \vdash^{U_2}_{L_2} t_2 : A}{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1+U_2+U+U_{app}}_{L_1+L_2+L+L_{app}} t_1\ t_2 : B}\ \text{U-A}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t_1 : A \qquad \Sigma;\Delta;\Phi;\Omega, x : A \vdash^{U_2}_{L_2} t_2 : B}{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1+U_2+U_{lt}}_{L_1+L_2+L_{lt}} \text{let } x = t_1 \text{ in } t_2 : B}\ \text{U-LT} \qquad \frac{}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} () : \text{unit}}\ \text{U-UNIT}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : A \qquad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} \text{return } t : \{P\}\ \exists \gamma.A\ \{P\}}\ \text{U-T}$$

$$\frac{\begin{array}{c}P = P_1 \star P_2 \\ \Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t_1 : \{P_1\}\ \exists \vec{\gamma}_1 : A \overset{\text{exec}(L,U)}{\{Q_1 \star Q_2\}} \qquad \Sigma;\Delta,\vec{\gamma}_1;\Phi;\Omega, x : A \vdash^{U_2}_{L_2} t_2 : \{Q_1 \star P_2\}\ \exists \vec{\gamma}_2 : B\ \overset{\text{exec}(L',U')}{\{Q\}}\end{array}}{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1+U_2+U_l}_{L_1+L_2+L_l} \text{let } \{x\} = t_1 \text{ in } t_2 : \{P\}\ \exists \vec{\gamma}_1, \vec{\gamma}_2 : B\ \overset{\text{exec}(L+L',U+U')}{\{Q \star Q_2\}}}\ \text{U-E}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t_1 : \text{int}[I] \qquad \Sigma;\Delta;\Phi;\Omega \vdash^{U_2}_{L_2} t_2 : A \qquad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} \text{alloc } t_1\ t_2 : \{P\}\ \exists \gamma : \text{Array}_{\gamma}[I]\ A\ \overset{\text{exec}(L_1+L_2+L_a,U_1+U_2+U_a)}{\{P \star \gamma \to \mathbb{N}\}}}\ \text{U-L}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t_1 : \text{Array}_{\gamma}[I]\ A \\ \Sigma;\Delta;\Phi;\Omega \vdash^{U_2}_{L_2} t_2 : \text{int}[I'] \qquad \Sigma;\Delta;\Phi;\Omega \vdash^{U_3}_{L_3} t_3 : A \qquad \Delta;\Phi \vDash I' \le I \qquad \Delta;\Phi \vDash I' \in \beta \qquad \Sigma;\Delta \vdash P \quad wf\end{array}}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} \text{updt } t_1\ t_2\ t_3 : \{P \star \gamma \to \beta\}\ \exists \_ : \text{unit}\ \overset{\text{exec}(L_1+L_2+L_3+L_u,U_1+U_2+U_3+U_u)}{\{P \star \gamma \to \beta\}}}\ \text{U-U}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t_1 : \text{Array}_{\gamma}[I]\ A \qquad \Sigma;\Delta;\Phi;\Omega \vdash^{U_2}_{L_2} t_2 : \text{int}[I'] \qquad \Delta;\Phi \vDash I' \le I \qquad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} \text{read } t_1\ t_2 : \overset{\text{exec}(L_1+L_2+L_r,U_1+U_2+U_r)}{\{P\}\ \exists \_ : A\ \{P\}}}\ \text{U-R}$$

Figure 12: Unary typing judgment, part (1)

$$\frac{\Sigma;\Delta;\Phi;x:A, f:A \overset{\mathsf{exec}(L,U)}{\longrightarrow} B, \Omega \vdash^{U}_{L} t : B}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} \mathsf{fix}\, f(x).t : A \overset{\mathsf{exec}(L,U)}{\longrightarrow} B}\ \textsc{u-f} \qquad \frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : A_1 \qquad \Delta;\Sigma;\Phi \vdash A_2 \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} \mathsf{inl}\ t : A_1 + A_2}\ \textsc{u-inl}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : A_2 \qquad \Delta;\Sigma;\Phi \vdash A_1 \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} \mathsf{inr}\ t : A_1 + A_2}\ \textsc{u-inr}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t : A_1 + A_2 \qquad \Sigma;\Delta;\Phi;x:\ A_1, \Omega \vdash^{U_2}_{L_2} t_1 : A \qquad \Sigma;\Delta;\Phi;y:\ A_2, \Omega \vdash^{U_2}_{L_2} t_2 : A}{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1+U_2+U_c}_{L_1+L_2+L_c}\ \mathsf{case}\ (t, x.t_1, y.t_2) : A}\ \textsc{u-case}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : A \qquad \Sigma;\Delta \vDash U \le U' \qquad \Sigma;\Delta \vDash L' \le L}{\Sigma;\Delta;\Phi;\Omega \vdash^{U'}_{L'}\ t : A}\ \textsc{cost-trans}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : A \qquad \Sigma;\Delta;\Phi \models A \sqsubseteq A' \qquad \Sigma;\Delta \vDash U \le U' \qquad \Sigma;\Delta \vDash L' \le L}{\Sigma;\Delta;\Phi;\Omega \vdash^{U'}_{L'}\ t : A'}\ \textsc{u-x}$$

$$\frac{\Sigma;i :: S,\Delta;\Phi;\Omega \vdash^{U}_{L} t : A \qquad i \notin FIV(\Phi;\Omega)}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} \Lambda.t : \overset{\mathsf{exec}(L,U)}{\forall} i :: S.\ A}\ \textsc{u-Lam} \qquad \frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t : \overset{\mathsf{exec}(L_2,U_2)}{\forall} i :: S.\ A \qquad \Sigma;\Delta \vdash I :: S}{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1+U_2}_{L_1+L_2}\ t\,[] : A\{I/i\}}\ \textsc{u-iapp}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : A\{I/i\} \qquad \Sigma;\Delta \vdash I :: S}{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} \mathsf{pack}\, t : \exists i :: S.\ A}\ \textsc{u-pack}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t_1 : \exists i :: S.\ A \qquad \Sigma;i :: S,\Delta;\Phi;\Omega \vdash^{U_2}_{L_2} t_2 : A_2 \qquad i \notin FV(\Phi;\Omega;A_2,L_2,U_2)}{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1+U_2}_{L_1+L_2} \mathsf{unpack}\, t_1\, \mathsf{as}\, x\, \mathsf{in}\ t_2 : A_2}\ \textsc{u-unpack}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : C \supset A \qquad \Sigma;\Delta;\Phi \vDash C}{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} \mathsf{celim}\ t : A}\ \textsc{u-celim} \qquad \frac{\Sigma;\Delta;\Phi \wedge C;\Omega \vdash^{U}_{L} t : A}{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : C \supset A}\ \textsc{u-cimpl}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : C\&A_1 \qquad \Sigma;\Delta;\Phi \wedge C;x : A_1, \Omega \vdash^{U'}_{L'} t : A_2}{\Sigma;\Delta;\Phi;\Gamma \vdash^{U+U'}_{L+L'}\ \mathsf{clet}\ t\ \mathsf{as}\ x\ \mathsf{in}\ t' : A_2}\ \textsc{u-and}\mathrm{E}$$

$$\frac{\Sigma;\Delta;\Phi \wedge C;\Omega \vdash^{U}_{L} t : A \qquad \Sigma;\Delta;\Phi \wedge \neg C;\Omega \vdash^{U}_{L} t : A}{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : A}\ \textsc{u-split}$$

$$\frac{\Sigma;\Delta;\Phi \vDash \bot \qquad \vdash \Sigma;\Delta;\Phi \vDash \Omega \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : C\&A}\ \textsc{u-contra} \qquad \frac{\Sigma;\Delta;\Phi \wedge C;\Omega \vdash^{U}_{L} t : A \qquad \Sigma;\Delta;\Phi \vDash C}{\Sigma;\Delta;\Phi;\Omega \vdash^{U}_{L} t : C\&A}\ \textsc{u-and}\mathrm{I}$$

Figure 13: Unary typing judgment, part (2)

$\boxed{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim c : \tau}$

$$\frac{}{\Sigma;\Delta;\Phi;\Gamma \vdash n \ominus n \lesssim 0 : \mathrm{int}_r}\ \text{R-INT} \qquad \frac{}{\Sigma;\Delta;\Phi;\Gamma \vdash n \ominus n \lesssim 0 : \mathrm{int}_r[n]}\ \text{R-I} \qquad \frac{}{\Sigma;\Delta;\Phi;\Gamma \vdash () \ominus () \lesssim 0 : \mathrm{unit}_r}\ \text{R-UNIT}$$

$$\frac{\Gamma(x) = \tau}{\Sigma;\Delta;\Phi;\Gamma \vdash x \ominus x \lesssim 0 : \tau}\ \text{R-V} \qquad \frac{\Sigma;\Delta;\Phi;\Gamma, x:\tau \vdash t_1 \ominus t_2 \lesssim D : \sigma}{\Sigma;\Delta;\Phi;\Gamma \vdash \lambda x.t_1 \ominus \lambda x.t_2 \lesssim 0 : \tau \xrightarrow{\mathrm{diff}(D)} \sigma}\ \text{R-ABS}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \tau \xrightarrow{\mathrm{diff}(D)} \sigma \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \tau}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1\ t_2 \ominus t_1'\ t_2' \lesssim D + D_1 + D_2 : \sigma}\ \text{R-APP}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \tau_1 \qquad \Sigma;\Delta;\Phi;\Gamma, x:\tau_1 \vdash t_2 \ominus t_2' \lesssim D_2 : \tau_2}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{let}\ x = t_1\ \mathsf{in}\ t_2 \ominus \mathsf{let}\ x = t_1'\ \mathsf{in}\ t_2' \lesssim D_1 + D_2 : \tau_2}\ \text{R-LT}$$

$$\frac{\Sigma;\Delta;\Phi;x:\tau, f :\tau \xrightarrow{\mathrm{diff}(D)} \sigma,\Gamma \vdash t_1 \ominus t_2 \lesssim D : \sigma}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{Fix}\, f(x).t_1 \ominus \mathsf{Fix}\, f(x).t_2 \lesssim D : \tau \xrightarrow{\mathrm{diff}(D)} \sigma}\ \text{R-FIX}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t \ominus t' \lesssim D : \tau_1 \qquad \Sigma;\Delta;\Phi \vdash \tau_2 \quad wf}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathrm{inl}\ t \ominus \mathrm{inl}\ t' \lesssim D : \tau_1 + \tau_2}\ \text{R-INL}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t \ominus t' \lesssim D : \tau_2 \qquad \Sigma;\Delta;\Phi \vdash \tau_1 \quad wf}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathrm{inr}\ t \ominus \mathrm{inr}\ t' \lesssim D : \tau_1 + \tau_2}\ \text{R-INR}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi;\Gamma \vdash t \ominus t' \lesssim D_1 : \tau_1 + \tau_2 \\ \Sigma;\Delta;\Phi;\Gamma, x:\tau_1 \vdash t_1 \ominus t_1' \lesssim D_2 : \tau \qquad \Sigma;\Delta;\Phi;\Gamma, y:\tau_2 \vdash t_2 \ominus t_2' \lesssim D_2 : \tau\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash\ \mathrm{case}\ (t, x.t_1, y.t_2) \ominus\ \mathrm{case}\ (t', x.t_1', y.t_2') \lesssim D_1 + D_2 : \tau}\ \text{R-CASE}$$

$$\frac{\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_1}^{U_1} t_1 : A_1 \qquad \Sigma;\Delta;\Phi;|\Gamma|_2 \vdash_{L_2}^{U_2} t_2 : A_2}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim U_1 - L_2 : U(A_1, A_2)}\ \text{R-S}$$

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash t \ominus t \lesssim D : \tau \qquad \Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Sigma;\Delta;\Phi \models D \leq D'}{\Sigma;\Delta;\Phi;\Gamma \vdash t \ominus t \lesssim D' : \tau'}\ \text{R-EXEC}$$

$$\frac{\Sigma;\Delta;\Phi \wedge C;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau \qquad \Sigma;\Delta;\Phi \wedge \neg C;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau}\ \text{R-P}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau \qquad \forall x \in dom(\Gamma).\Sigma;\Delta;\Phi \models \Gamma(x) \sqsubseteq \Box\Gamma(x)}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim 0 : \tau}\ \text{NC}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau\{I/i\} \qquad \Sigma;\Delta \vdash I :: S}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{pack}\ t_1 \ominus \mathsf{pack}\ t_2 \lesssim D : \exists i :: S.\tau}\ \text{R-PACK}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \exists i :: S.\tau_1 \\ \Sigma; i :: S, \Delta;\Phi; x:\tau_1,\Gamma \vdash t_2 \ominus t_2' \lesssim D_1 + D_2 : \tau_2 \qquad i \notin FV(\Phi;\Gamma;\tau_2)\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{unpack}\, t_1\, \mathsf{as}\, x\, \mathsf{in}\ t_2 \ominus \mathsf{unpack}\, t_1'\, \mathsf{as}\, x\, \mathsf{in}\ t_2' \lesssim D_1 + D_2 : \tau_2}\ \text{R-UNPACK}$$

Figure 14: Relational typing judgment, part (1)

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau \qquad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{return}\ t_1 \ominus \mathsf{return}\ t_2 \lesssim 0 : \{P\}\ \exists\_.\tau\ \{P\}}\ \overset{\mathrm{diff}(D)}{}\ \text{R-T}$$

$$\frac{\begin{array}{c} P = P_1 \star P_2 \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \{P_1\}\ \exists \vec{\gamma}_1.\tau\ \{Q_1 \star Q_2\} \\ \Sigma;\Delta,\vec{\gamma_1} : \vec{\mathbb{L}};\Phi;\Gamma, x:\tau \vdash t_2 \ominus t_2' \lesssim D_2 : \{Q_1 \star P_2\}\ \exists \vec{\gamma}_2.\sigma\ \{Q\} \end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2 \ominus \mathsf{let}\ \{x\} = t_1'\ \mathsf{in}\ t_2' \lesssim 0 : \{P\}\ \exists \vec{\gamma}_1 \vec{\gamma}_2 : \sigma\ \{Q \star Q_2\}}\ \begin{array}{l}\overset{\mathrm{diff}(D)}{}\\ \overset{\mathrm{diff}(D')}{}\\ \overset{\mathrm{diff}(D+D'+D_1+D_2)}{}\end{array}\ \text{R-LET}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathrm{int}[I] \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \tau \qquad \gamma\ \mathsf{fresh} \qquad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{alloc}\ t_1\ t_2 \ominus \mathsf{alloc}\ t_1'\ t_2' \lesssim 0 : \{P\}\ \exists\gamma.\ \mathsf{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \mathbb{N}\}}\ \overset{\mathrm{diff}(D_1+D_2)}{}\ \text{R-ALLOC}$$

$$\frac{\begin{array}{c} \Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathrm{int}[I] \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \square\tau \qquad \gamma\ \mathsf{fresh} \qquad \Sigma;\Delta \vdash P \quad wf \end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{alloc}\ t_1\ t_2 \ominus \mathsf{alloc}\ t_1'\ t_2' \lesssim 0 : \{P\}\ \exists\gamma.\ \mathsf{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \emptyset\}}\ \overset{\mathrm{diff}(D_1+D_2)}{}\ \text{R-ALLOC-BOX}$$

$$\frac{\begin{array}{c} \Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \qquad \Delta;\Phi \models I' \le I \qquad \Sigma;\Delta \vdash P \quad wf \end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{read}\ t_1\ t_2 \ominus \mathsf{read}\ t_1'\ t_2' \lesssim 0 : \{P \star \gamma \to \beta\}\ \exists\_.\tau\ \{P \star \gamma \to \beta\}}\ \overset{\mathrm{diff}(D_1+D_2)}{}\ \text{R-R}$$

$$\frac{\begin{array}{c} \Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \qquad \Delta;\Phi \models I' \le I \qquad \Sigma;\Delta;\Phi \models I' \notin \beta \qquad \Sigma;\Delta \vdash P \quad wf \end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{read}\ t_1\ t_2 \ominus \mathsf{read}\ t_1'\ t_2' \lesssim 0 : \{P \star \gamma \to \beta\}\ \exists\_.\square\tau\ \{P \star \gamma \to \beta\}}\ \overset{\mathrm{diff}(D_1+D_2)}{}\ \text{R-RB}$$

$$\frac{\begin{array}{c} \Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_3 \ominus t_3' \lesssim D_3 : \tau \qquad \Delta;\Phi \models I' \le I \qquad \Sigma;\Delta \vdash P \quad wf \end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{updt}\ t_1\ t_2\ t_3 \ominus \mathsf{updt}\ t_1'\ t_2'\ t_3' \lesssim 0 : \{P \star \gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r\ \{P \star \gamma \to \beta \cup \{I'\}\}}\ \overset{\mathrm{diff}(D_1+D_2+D_3)}{}\ \text{R-U}$$

$$\frac{\begin{array}{c} \Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_3 \ominus t_3' \lesssim D_3 : \square\tau \qquad \Delta;\Phi \models I' \le I \qquad \Sigma;\Delta \vdash P \quad wf \end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{updt}\ t_1\ t_2\ t_3 \ominus \mathsf{updt}\ t_1'\ t_2'\ t_3' \lesssim 0 : \{P \star \gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r\ \{P \star \gamma \to \beta \setminus \{I'\}\}}\ \overset{\mathrm{diff}(D_1+D_2+D_3)}{}\ \text{R-UB}$$

Figure 15: Relational typing judgment, part (2)

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau \qquad i \notin FV(\Phi;\Gamma)}{\Sigma;\Delta;\Phi;\Gamma \vdash \Lambda\ t_1 \ominus \Lambda\ t_2 \lesssim 0 : \overset{\mathrm{diff}(D)}{\forall i::S.\ \tau}}\ \text{R-ILAM} \qquad \frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \overset{\mathrm{diff}(D')}{\forall i::S.\ \tau} \qquad \Sigma;\Delta \vdash I :: S}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1\ [] \ominus t_2\ [] \lesssim D + D'[I/i] : \tau\{I/i\}}\ \text{R-IAPP}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : C \supset \tau \qquad \Sigma;\Delta;\Phi \vDash C}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{celim}\ t_1 \ominus \mathsf{celim}\ t_2 \lesssim 0 : \tau}\ \text{R-CELIM} \qquad \frac{\Sigma;\Delta;\Phi \wedge C;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim 0 : C \supset \tau}\ \text{R-CIMPL}$$

$$\frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : C\&\tau_1 \qquad \Sigma;\Delta;\Phi \wedge C;x:\tau_1,\Gamma \vdash t_1' \ominus t_2' \lesssim D' : \tau_2}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{clet}\ t_1\ \mathsf{as}\ x\ \mathsf{in}\ t_1' \ominus \mathsf{clet}\ t_2\ \mathsf{as}\ x\ \mathsf{in}\ t_2' \lesssim D + D' : \tau_2}\ \text{R-ANDE}$$

$$\frac{\Sigma;\Delta;\Phi \wedge C;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau \qquad \Sigma;\Delta;\Phi \vDash C}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : C\&\tau}\ \text{R-ANDI}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi;x:\tau_1,f\ :\overset{\mathrm{diff}(D)}{\tau_1 \longrightarrow \tau_2},\Gamma,f\ : U(A_1,A_2) \vdash t_1 \ominus t_2 \lesssim D : \tau_2 \\ \Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_0^0 \mathsf{Fix}\, f(x).t_1 : A_1 \qquad \Sigma;\Delta;\Phi;|\Gamma|_2 \vdash_0^0 \mathsf{Fix}\, f(x).t_2 : A_2\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{Fix}\, f(x).t_1 \ominus \mathsf{Fix}\, f(x).t_2 \lesssim D : \overset{\mathrm{diff}(D)}{\tau_1 \longrightarrow \tau_2}}\ \text{R-FIX-EXT}$$

$$\frac{\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_1}^{U_1} t_1 : A_1 \qquad \Sigma;\Delta;\Phi;\Gamma,x:U(A_1,A_1) \vdash t_2 \ominus t_2' \lesssim D_2 : \tau}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{let}\ x = t_1\ \mathsf{in}\ t_2 \ominus t_2' \lesssim U_1 + D_2 + c_{lt} : \tau}\ \text{R-LT-E}$$

$$\frac{\Sigma;\Delta;\Phi;|\Gamma|_2 \vdash_{L_1}^{U_1} t_1' : A_1' \qquad \Sigma;\Delta;\Phi;\Gamma,x:U(A_1',A_1') \vdash t_2 \ominus t_2' \lesssim D_2 : \tau'}{\Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus \mathsf{let}\ x = t_1'\ \mathsf{in}\ t_2' \lesssim D_2 - L_1 - c_{lt} : \tau'}\ \text{R-E-LT}$$

$$\frac{\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_1}^{U_1} t_1 : \overset{\mathrm{exec}(L,U)}{A_1 \longrightarrow A_2} \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : U(A_1,A_2')}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1\ t_2 \ominus t_2' \lesssim U_1 + U + D_2 + c_{app} : U(A_2,A_2')}\ \text{R-APP-E}$$

$$\frac{\Sigma;\Delta;\Phi;|\Gamma|_2 \vdash_{L_1}^{U_1} t_1' : \overset{\mathrm{exec}(L,U)}{A_1' \longrightarrow A_2'} \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : U(A_2,A_1')}{\Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_1'\ t_2' \lesssim D_2 - L_1 - L - c_{app} : U(A_2,A_2')}\ \text{R-E-APP}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_1}^{U_1} t : A_1 + A_2 \\ \Sigma;\Delta;\Phi;\Gamma,x:U(A_1,A_1) \vdash t_1 \ominus t' \lesssim D_2 : \tau \qquad \Sigma;\Delta;\Phi;\Gamma,y:U(A_2,A_2) \vdash t_2 \ominus t' \lesssim D_2 : \tau\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash\ \mathsf{case}\ (t,x.t_1,y.t_2) \ominus t' \lesssim U_1 + D_2 + c_{case} : \tau}\ \text{R-CASE-E}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_1'}^{U_1'} t' : A_1 + A_2 \\ \Sigma;\Delta;\Phi;\Gamma,x:U(A_1,A_1) \vdash t \ominus t_1' \lesssim D_2 : \tau \qquad \Sigma;\Delta;\Phi;\Gamma,y:U(A_2,A_2) \vdash t \ominus t_2' \lesssim D_2 : \tau\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash t \ominus\ \mathsf{case}\ (t',x.t_1',y.t_2') \lesssim D_2 - L_1' - c_{case} : \tau}\ \text{R-E-CASE}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_1}^{U_1} t_1 : \{P_1\}\ \overset{\mathrm{exec}(L,U)}{\exists \vec{\gamma}_1 : A_1}\ \{Q_1\} \qquad dom(P) = dom(P_1) \qquad \Sigma;\Delta;\Phi;|\Gamma|_2 \vdash_{L_2}^{U_2} t_2' : \{P_2\}\ \overset{\mathrm{exec}(L',U')}{\exists \vec{\gamma}_1 : A_1'}\ \{Q_2\} \\ \Sigma;\Delta;\Phi;\Gamma,x:U(A_1,A_1) \vdash t_2 \ominus t_2' \lesssim D_2 : \{P \sqcup P_1\}\ \overset{\mathrm{diff}(D')}{\exists \vec{\gamma}_1.\tau}\ \{Q\}\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2 \ominus t_2' \lesssim -L_2 : \quad \overset{\mathrm{diff}(U_1+U+(D_2+U_2)+D'+c_{let})}{\{P\}\ \exists \vec{\gamma}_1.\tau\ \{Q\}}}\ \text{R-LET-E}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi;|\Gamma|_2 \vdash_{L_1}^{U_1} t_1' : \{P_1\}\ \overset{\mathrm{exec}(L,U)}{\exists \vec{\gamma}_1 : A_1'}\ \{Q_1\} \qquad dom(P) = dom(P_1) \qquad \Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_2}^{U_2} t_2 : \{P_2\}\ \overset{\mathrm{exec}(L',U')}{\exists \vec{\gamma}_1 : A_1}\ \{Q_2\} \\ \Sigma;\Delta;\Phi;\Gamma,x:U(A_1',A_1') \vdash t_2 \ominus t_2' \lesssim D_2 : \{P \sqcup P_1\}\ \overset{\mathrm{diff}(D')}{\exists \vec{\gamma}_1.\tau'}\ \{Q\}\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus \mathsf{let}\ \{x\} = t_1'\ \mathsf{in}\ t_2' \lesssim U_2 : \quad \overset{\mathrm{diff}(D'+(D_2-L_2)-L_1-L-c_{\mathrm{let}})}{\{P\}\ \exists \vec{\gamma}_1.\tau'\ \{Q\}}}\ \text{R-E-LET}$$

Figure 16: Relational typing judgment, part (3)

$\boxed{\Sigma;\Delta;\Phi \models A_1 \sqsubseteq A_2}$

$$\frac{\Sigma;\Delta;\Phi \models A_1' \sqsubseteq A_1 \qquad \Sigma;\Delta;\Phi \models A_2 \sqsubseteq A_2' \qquad \Sigma;\Delta;\Phi \models L' \leq L \qquad \Sigma;\Delta;\Phi \models U \leq U'}{\Sigma;\Delta;\Phi \models A_1 \overset{\text{exec}(L,U)}{\longrightarrow} A_2 \sqsubseteq A_1' \overset{\text{exec}(L',U')}{\longrightarrow} A_2'}\ \text{S-A-EXEC}$$

$$\frac{\Sigma; i :: S,\Delta;\Phi \models A' \sqsubseteq A \qquad \Sigma; i :: S,\Delta;\Phi \models L' \leq L \qquad \Sigma;\Delta;\Phi \models U \leq U' \qquad i \notin FV(\Phi)}{\Sigma;\Delta;\Phi \models \forall i :: S.\ A \overset{\text{exec}(L,U)}{\sqsubseteq} \forall i :: S.\ A' \overset{\text{exec}(L',U')}{}}\ \text{S-A-FORALL}$$

$$\frac{\Sigma;\Delta;\Phi \models U \leq U' \qquad \Sigma;\Delta;\Phi \models P \subseteq P' \qquad \Sigma,\vec{\gamma}_1;\Delta;\Phi \models Q' \subseteq Q \qquad \Sigma;\Delta;\Phi \models \vec{\gamma}_1 \subseteq \vec{\gamma}_2 \qquad \Sigma;\Delta;\Phi \models A \sqsubseteq A'}{\Sigma;\Delta;\Phi \models \{P\}\ \exists \vec{\gamma}_1 : A\ \{Q\} \overset{\text{exec}(L,U)}{\sqsubseteq} \{P'\}\ \exists \vec{\gamma}_2 : A'\ \{Q'\} \overset{\text{exec}(L',U')}{}}\ \text{S-A-MONAD}$$

$$\frac{\Sigma;\Delta;\Phi \models A_1 \sqsubseteq A_1' \qquad \Sigma;\Delta;\Phi \models A_2 \sqsubseteq A_2'}{\Sigma;\Delta;\Phi \models A_1 + A_2 \sqsubseteq A_1' + A_2'}\ \text{S-UM} \qquad \frac{\Sigma;\Delta;\Phi \models A \sqsubseteq A' \qquad \Sigma;\Delta;\Phi \models I = I'}{\Sigma;\Delta;\Phi \models \mathsf{Array}_\gamma[I]\ A \sqsubseteq \mathsf{Array}_\gamma[I']\ A'}\ \text{S-A-ARRAY}$$

$$\frac{\Sigma;\Delta;\Phi \models A \sqsubseteq A' \qquad \Sigma;\Delta;\Phi \models I = I'}{\Sigma;\Delta;\Phi \models \mathsf{list}[I]\ A \sqsubseteq \mathsf{list}[I']\ A'}\ \text{S-A-LIST} \qquad \frac{\Sigma; i :: S,\Delta;\Phi \models A \sqsubseteq A' \qquad i \notin FV(\Phi)}{\Sigma;\Delta;\Phi \models \exists i :: S.\ A \sqsubseteq \exists i :: S.\ A'}\ \text{S-A-EXIST}$$

Figure 17: Unary subtyping rules, part (1)

$$\frac{\Sigma; f\Delta;\Phi \models A \sqsubseteq A' \qquad \Sigma;\Delta;\Phi \wedge C \models C'}{\Sigma;\Delta;\Phi \models C \& A \sqsubseteq C \& A'}\ \text{S-A-CAND} \qquad \frac{\Sigma;\Delta;\Phi \models A \sqsubseteq A' \qquad \Sigma;\Delta;\Phi \wedge C' \models C}{\Sigma;\Delta;\Phi \models C \supset A \sqsubseteq C \supset A'}\ \text{S-A-CIMPL}$$

$$\frac{}{\Sigma;\Delta;\Phi \models A \sqsubseteq A}\ \text{S-A-REFL} \qquad \frac{\Sigma;\Delta;\Phi \models A_1 \sqsubseteq A_2 \qquad \Sigma;\Delta;\Phi \models A_2 \sqsubseteq A_3}{\Sigma;\Delta;\Phi \models A_1 \sqsubseteq A_3}\ \text{S-A-TRAN}$$

Figure 18: Unary subtyping rules, part (2)

$\boxed{\Sigma;\Delta;\Phi \models \tau_1 \sqsubseteq \tau_2}$

$$\frac{}{\Sigma;\Delta;\Phi \models \mathrm{int}_r \sqsubseteq \Box U(\mathrm{int},\mathrm{int})}\ \text{S-R-INT-BOX} \qquad \frac{}{\Sigma;\Delta;\Phi \models \mathrm{int}_r[I] \sqsubseteq \Box U(\mathrm{int},\mathrm{int})}\ \text{S-R-INT-I-BOX}$$

$$\frac{}{\Sigma;\Delta;\Phi \models \Box U(\mathrm{int},\mathrm{int}) \sqsubseteq \Box \mathrm{int}_r}\ \text{S-R-UINT-BOX} \qquad \frac{}{\Sigma;\Delta;\Phi \models \mathrm{unit} \sqsubseteq \Box \mathrm{unit}}\ \text{S-R-UNIT-BOX}$$

$$\frac{\Sigma;\Delta;\Phi \models \tau_1' \sqsubseteq \tau_1 \qquad \Sigma;\Delta;\Phi \models \tau_2 \sqsubseteq \tau_2' \qquad \Sigma;\Delta;\Phi \models c \leq c'}{\Sigma;\Delta;\Phi \models \tau_1 \overset{\mathrm{diff}(c)}{\longrightarrow} \tau_2 \sqsubseteq \tau_1' \overset{\mathrm{diff}(c')}{\longrightarrow} \tau_2'}\ \text{S-R-DIFF}$$

$$\frac{}{\Sigma;\Delta;\Phi \models \Box(\tau_1 \overset{\mathrm{diff}(c)}{\longrightarrow} \tau_2) \sqsubseteq \Box\tau_1 \overset{\mathrm{diff}(0)}{\longrightarrow} \Box\tau_2}\ \text{S-R-BOX-DIFF}$$

$$\frac{}{\Sigma;\Delta;\Phi \models U(A_1 \overset{\mathrm{exec}(L,U)}{\longrightarrow} A_2, A_1' \overset{\mathrm{exec}(L',U')}{\longrightarrow} A_2') \sqsubseteq U(A_1, A_1') \overset{\mathrm{diff}(U-L')}{\longrightarrow} U(A_2, A_2')}\ \text{S-R-EXECDIFF}$$

$$\frac{\Sigma; i :: S, \Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Sigma; i :: S, \Delta;\Phi \models c \leq c' \qquad i \notin FV(\Phi)}{\Sigma;\Delta;\Phi \models \forall i{::}S.\ \tau \sqsubseteq \forall i{::}S.\ \tau_1'}\ \text{S-R-FORALL-DIFF}$$

$$\frac{}{\Sigma;\Delta;\Phi \models \Box(\forall i{::}S.\ \tau) \sqsubseteq \forall i{::}S.\ \Box\tau}\ \text{S-R-FORALL-BOX} \qquad \frac{}{\Sigma;\Delta;\Phi \models U(\mathrm{unit},\mathrm{unit}) \sqsubseteq \mathrm{unit}}\ \text{S-R-UNIT}$$

$$\frac{}{\Sigma;\Delta;\Phi \models U(\forall i :: S.\ A, \forall i :: S.\ A') \sqsubseteq \forall i{::}S.\ U(A, A')}\ \text{S-R-FORALL-U}$$

$$\frac{\Sigma;\Delta;\Phi \models \tau_1 \sqsubseteq \tau_1' \qquad \Sigma;\Delta;\Phi \models \tau_2 \sqsubseteq \tau_2'}{\Sigma;\Delta;\Phi \models \tau_1 + \tau_2 \sqsubseteq \tau_1' + \tau_2'}\ \text{S-R-SUM} \qquad \frac{}{\Sigma;\Delta;\Phi \models \Box\tau_1 + \Box\tau_2 \sqsubseteq \Box(\tau_1 + \tau_2)}\ \text{S-R-SUM-BOX}$$

$$\frac{\Sigma; i :: S, \Delta;\Phi \models \tau \sqsubseteq \tau' \qquad i \notin FV(\Phi)}{\Sigma;\Delta;\Phi \models \exists i :: S.\ \tau \sqsubseteq \exists i :: S.\ \tau'}\ \text{S-R-EXIST} \qquad \frac{}{\Sigma;\Delta;\Phi \models \exists i :: S.\ \Box\tau \sqsubseteq \Box(\exists i :: S.\ \tau)}\ \text{S-R-EXIST-BOX}$$

Figure 19: Relational subtyping rules, part (1)

$\boxed{\Delta;\Phi \models \tau_1 \sqsubseteq \tau_2}$

$$\frac{\Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Sigma;\Delta;\Phi \models I{=}I' \qquad \Sigma;\Delta;\Phi \models \gamma{=}\gamma'}{\Sigma;\Delta;\Phi \models \mathsf{Array}_{\gamma}[I]\ \tau \sqsubseteq \mathsf{Array}_{\gamma'}[I']\ \tau'}\ \text{S-R-ARRAY}$$

$$\frac{\Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Sigma;\Delta;\Phi \models I{=}I'\ \Sigma;\Delta;\Phi \models \alpha{\leq}\alpha'}{\Sigma;\Delta;\Phi \models \mathsf{list}^{\alpha}[I]\ A \sqsubseteq \mathsf{list}^{\alpha'}[I']\ A'}\ \text{S-R-LIST}$$

$$\frac{\Sigma;\Delta;\Phi \models A_1 \sqsubseteq A_1' \qquad \Sigma;\Delta;\Phi \models A_2 \sqsubseteq A_2'}{\Sigma;\Delta;\Phi \models U\ (A_1, A_2) \sqsubseteq U\ (A_1', A_2')}\ \text{S-R-UA}$$

$$\frac{\Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Sigma;\Delta;\Phi \wedge C \models C'}{\Sigma;\Delta;\Phi \models C\&\tau \sqsubseteq C\&\tau'}\ \text{S-R-C-AND} \qquad \frac{}{\Sigma;\Delta;\Phi \models C\&\Box\tau \sqsubseteq \Box(C\&\tau)}\ \text{S-R-C-AND-BOX}$$

$$\frac{}{\Sigma;\Delta;\Phi \models U(C \supset A, C \supset A') \sqsubseteq C \supset U(A, A')}\ \text{S-R-CIMPL-U}$$

$$\frac{\Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Sigma;\Delta;\Phi \wedge C' \models C}{\Sigma;\Delta;\Phi \models C \supset \tau \sqsubseteq C \supset \tau'}\ \text{S-R-C-IMPL}$$

$$\frac{}{\Sigma;\Delta;\Phi \models \Box(C \supset \tau) \sqsubseteq C \supset \Box\tau}\ \text{S-R-C-IMPL-BOX} \qquad \frac{}{\Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau}\ \text{S-R-REFL}$$

$$\frac{}{\Sigma;\Delta;\Phi \models \tau \sqsubseteq U(|\tau|_1, |\tau|_2)}\ \text{S-R-W} \qquad \frac{}{\Sigma;\Delta;\Phi \models \Box\tau \sqsubseteq \tau}\ \text{S-R-T}$$

$$\frac{\Sigma;\Delta;\Phi \models \tau_1 \sqsubseteq \tau_2 \qquad \Sigma;\Delta;\Phi \models \tau_2 \sqsubseteq \tau_3}{\Sigma;\Delta;\Phi \models \tau_1 \sqsubseteq \tau_3}\ \text{S-R-TRAN}$$

$$\frac{\Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Delta;\Phi \models c{\leq}c' \qquad \Delta;\Phi \models P'{\subseteq}P \qquad \Delta;\Phi \models \vec{\gamma}_1 \subseteq \vec{\gamma}_2 \qquad \Sigma, \vec{\gamma}_1 : \vec{\mathbb{L}};\Delta;\Phi \models Q{\subseteq}Q'}{\Sigma;\Delta;\Phi \models \{P\}\ \overset{\mathrm{diff}(c)}{\exists \vec{\gamma}_1} : \tau\ \{Q\} \sqsubseteq \{P'\}\ \overset{\mathrm{diff}(c')}{\exists \vec{\gamma}_2} : \tau'\ \{Q'\}}\ \text{S-RM}$$

$$\frac{}{\begin{array}{l}\Sigma;\Delta;\Phi \models U\ (\{\gamma_i \to T_i\}\ \overset{\mathrm{exec}(L,U)}{\exists \vec{\gamma}_1'} : A_1\ \{Q_1\}, \{\gamma_i \to T_i'\}\ \overset{\mathrm{exec}(L',U')}{\exists \vec{\gamma}_2'} : A_1\ \{Q_2\}) \sqsubseteq \\ \qquad \{\gamma_i \to \beta_i\}\ \overset{\mathrm{diff}(U-L')}{\exists \vec{\gamma}_1, \vec{\gamma}_2} : U(A_1, A_2)\ \{\gamma_i \to \beta_i \cup T_i \cup T_i'\}\end{array}}\ \text{S-RUM}$$

$$\begin{array}{rcl} P \subseteq P' & \Leftrightarrow & P = \{\gamma_1 \to \beta_1, \gamma_2 \to \beta_2, \ldots, \gamma_n \to \beta_n\} \\ & & P' = \{\gamma_1 \to \beta_1', \gamma_2 \to \beta_2', \ldots, \gamma_n \to \beta_n'\} \\ & & \forall\, i \in \{1, \ldots, n\}.\beta_i \subseteq \beta_i' \end{array}$$

Figure 20: Relational subtyping rules, part (2)

$$
\begin{array}{rl}
[\![\mathrm{int}]\!]_{g,k} & = \{\, n \mid n \in \mathbb{N} \,\} \\
[\![\mathrm{unit}]\!]_{g,k} & = \{\, () \,\} \\
[\![\mathrm{bool}]\!]_{g,k} & = \{\, b \mid b \in \mathbb{B} \,\} \\
[\![\mathrm{int}[I]]\!]_{g,k} & = \{\, n \mid I = n \,\} \\
[\![\mathsf{Array}_\gamma[I]\ A]\!]_{g,k} & = \{\, l \mid I = n \wedge g(\gamma) = (l, n, A) \,\} \\
\overset{\mathrm{exec}(L,U)}{[\![A \longrightarrow A']\!]_{g,k}} & = \{\mathsf{fix}\, f(x).t \mid \forall k' < k, \forall g' \supseteq g, \forall v.v \in [\![A]\!]_{g',k'} \Rightarrow \\
& \quad t[v/x][\mathsf{fix}\, f(x).t/f] \in [\![A']\!]^{E,(L,U)}_{g',k'} \,\} \\
& \quad \cup \{\lambda x.t \mid \forall k' < k, \forall g' \supseteq g, \forall v.v \in [\![A]\!]_{g',k'} \Rightarrow t[v/x] \in [\![A']\!]^{E,(L,U)}_{g',k'} \} \\
\overset{\mathrm{exec}(L,U)}{[\![\{P\}\ \exists \vec{\gamma}.A\ \{Q\}]\!]_{g,k}} & = \Big\{ v \mid \forall g_1 \supseteq g, \forall k_1 \le k, \forall k_2 < k_1, c, \forall H. \big(H \vDash_{g_1,k_1} P \wedge v; H \Downarrow^{c,k_2}_f \big) \\
& \qquad \Rightarrow \exists g_2 \supseteq g_1, H_1, v_1, \vec{\gamma}. (v; H \Downarrow^{c,k_2}_f v_1; H_1) \wedge L \le c \le U \wedge H_1 \vDash_{g_2,k_1-k_2} Q \\
& \wedge v_1 \in [\![A]\!]_{g_2,k_1-k_2} \wedge \big(\exists n.P = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \\
& \wedge \forall i \in [1,n].g(\gamma_i) = (l_i, A, m)) \Rightarrow \forall j.(H[l_i][j]) \ne H_1[l_i][j] \Rightarrow j \in T_i) \Big\} \\
\overset{\mathrm{exec}(L,U)}{[\![\forall i :: S.\ A]\!]_{g,k}} & = \{\Lambda.t \mid \forall I. \vdash I :: S\,.\, t \in [\![A[I/i]]\!]^{E,(L[I/i],U[I/i])}_{g,k-1} \} \\
[\![\exists i :: S.\ A\,]\!]_{g,k} & = \{\mathsf{pack}\, v \mid \exists I. \vdash I :: S\,.\, v \in [\![A[I/i]]\!]_{g,k-1} \} \\
[\![A_1 + A_2]\!]_{g,k} & = \{\mathrm{inl}\ v \mid v \in [\![A_1]\!]_{g,k}\} \bigcup \{\mathrm{inr}\ v \mid v \in [\![A_2]\!]_{g,k}\} \\
[\![C \supset A]\!]_{g,k} & = \{\, v \mid \not\models C \wedge v \in [\![A]\!]_{g,k-1} \} \\
[\![C \& A]\!]_{g,k} & = \{\, v \mid \models C \wedge v \in [\![A]\!]_{g,k-1} \} \\
[\![A]\!]^{E,(L,U)}_{g,k} & = \{\, t \mid \forall v, \forall k' \le k.\ t \Downarrow^{c,k'} v \Rightarrow v \in [\![A]\!]_{g,k-k'} \wedge L \le c \le U \} \\
[\![\cdot]\!]_{g,k} & = \{\emptyset\} \\
[\![\Omega, x : A]\!]_{g,k} & = \{(\sigma[v/x]) \mid \sigma \in [\![\Omega]\!]_{g,k} \wedge v \in [\![A]\!]_{g,k}\} \\
\text{where} & \\
H \vDash_{g,k} empty & \quad \mathsf{iff} \quad \text{true} \\
H \vDash_{g,k} (\gamma \to \beta) & \quad \mathsf{iff} \quad \exists l, A, n : g(\gamma) = (l, A, n) \\
& \qquad \wedge \big(\forall i \le n. \big(H[l][i]\big) \in (\!|A|\!)_{g,k-1}\big) \\
H \vDash_{g,k} (P * Q) & \quad \mathsf{iff} \quad \exists H', H'', g', g'' : \\
& \qquad \big(H = H' \uplus H''\big) \wedge \big(g = g' \uplus g''\big) \\
& \qquad \wedge \big(H' \vDash_{g',k} P\big) \wedge \big(H'' \vDash_{g'',k} Q\big) \\
v; H \Downarrow^{c,k}_f & \quad \triangleq \quad \exists v', H'. v; H \Downarrow^{c,k}_f v'; H'
\end{array}
$$

Figure 21: Unary interpretation of types

$$
\begin{aligned}
(\!|\mathrm{int}_r|\!)_{G,k} &= \{(n_1,n_2) \mid n_1 = n_2\} \\
(\!|\mathrm{unit}_r|\!)_{G,k} &= \{((),())\} \\
(\!|\mathrm{int}_r\,[I]|\!)_{G,k} &= \{(n,n) \mid I = n\} \\
(\!|\mathsf{Array}_\gamma\,[I]\ \tau|\!)_{G,k} &= \{(l_1,l_2) \mid I = n \wedge G(\gamma) = (l_1,l_2,\tau,n)\} \\
(\!|\tau_1 \xrightarrow{\mathrm{diff}(D)} \tau_2|\!)_{G,k} &= \{(\mathsf{fix}\,f(x).t_1, \mathsf{fix}\,f(x).t_2) \mid \forall G' \supseteq G, k' \le k-1, \forall v_1, v_2.(v_1,v_2) \in (\!|\tau_1|\!)_{G',k'} \\
&\quad \Rightarrow (t_1[v_1/x][\mathsf{fix}\,f(x).t_1/f], t_2[v_2/x][\mathsf{fix}\,f(x).t_2/f]) \in (\!|\tau_2|\!)^{E,D}_{G',k'}\} \\
&\quad \wedge \forall j.(\mathsf{fix}\,f(x).t_1 \in [\![|\tau_1|_1 \xrightarrow{\mathrm{exec}(0,\infty)} |\tau_2|_1]\!]_{G|_1,j}) \wedge (\mathsf{fix}\,f(x).t_2 \in [\![|\tau_1|_2 \xrightarrow{\mathrm{exec}(0,\infty)} |\tau_2|_2]\!]_{G|_2,j}) \\
(\!|\{P\}\ \exists\vec{\gamma}.\tau\ \{Q\}|\!)^{\mathrm{diff}(D)}_{G,k} &= \Big\{(v_1,v_2) \mid \forall G_1 \supseteq G, k_1 \le k, k_2 < k_1, k_3, c_1, c_2, H_1, H_2.\Big((\mathsf{H}_1,\mathsf{H}_2) \vDash_{G_1,k_1} P \wedge v_1; H_1 \Downarrow_f^{c_1,k_2} \\
&\quad \wedge v_2; H_2 \Downarrow_f^{c_2,k_3}\Big) \Rightarrow \exists G_2 \supseteq G_1, H_1', H_2', v_1', v_2', c_1, c_2, \vec{\gamma}. \\
&\qquad \Big(v_1; H_1 \Downarrow_f^{c_1,k_2} \mathsf{v}_1'; \mathsf{H}_1' \wedge \mathsf{v}_2; \mathsf{H}_2 \Downarrow_f^{c_2,k_3} \mathsf{v}_2'; \mathsf{H}_2' \wedge \\
&\quad (\mathsf{H}_1', \mathsf{H}_2') \vDash_{\mathsf{G}_2,\mathsf{k}_1-\mathsf{k}_2} Q \wedge (\mathsf{v}_1', \mathsf{v}_2') \in (\!|\tau|\!)_{G_2,k_1-k_2} \wedge c_1 - c_2 \le D\Big)\Big\} \\
(\!|U(A_1,A_2)|\!)_{G,k} &= \{(v_1,v_2) \mid \forall k', v_1 \in [\![A_1]\!]_{G|_1,k'} \wedge v_2 \in [\![A_2]\!]_{G|_2,k'}\} \\
(\!|\forall i{::}S.\ \tau|\!)^{\mathrm{diff}(D)}_{G,k} &= \{(\Lambda.t_1, \Lambda.t_2) \mid \forall I. \vdash I :: S\,.(t_1,t_2) \in (\!|\tau[I/i]|\!)^{E,D[I/i]}_{G,k-1} \\
&\quad \forall j.t_1 \in [\![|\tau|_1]\!]^{E,(0,\infty)}_{G|_1,j} \wedge t_2 \in [\![|\tau|_2]\!]^{E,(0,\infty)}_{G|_2,j}\} \\
(\!|\exists i :: S.\ \tau\ |\!)_{G,k} &= \{(\mathsf{pack}\ v_1, \mathsf{pack}\ v_2) \mid \exists I. \vdash I :: S\,.(v_1,v_2) \in (\!|\tau[I/i]|\!)_{G,k-1}\} \\
(\!|\tau_1 + \tau_2|\!)_{G,k} &= \{(\mathrm{inl}\ v_1, \mathrm{inl}\ v_2) \mid (v_1,v_2) \in (\!|\tau_1|\!)_{G,k-1}\} \bigcup \{(\mathrm{inr}\ v_1, \mathrm{inr}\ v_2) \mid (v_1,v_2) \in (\!|\tau_2|\!)_{G,k-1}\} \\
(\!|\Box\tau|\!)_{G,k} &= \{(v,v) \mid (v,v) \in (\!|\tau|\!)_{G,k}\} \\
(\!|C \supset \tau|\!)_{G,k} &= \{(v_1,v_2) \mid \not\models C \bigvee (v_1,v_2) \in (\!|\tau|\!)_{G,k-1}\} \\
(\!|C\&\tau|\!)_{G,k} &= \{(v_1,v_2) \mid \models C \wedge (v_1,v_2) \in (\!|\tau|\!)_{G,k-1}\} \\
(\!|\tau|\!)^{E,D}_{G,k} &= \{(t_1,t_2) \mid \forall k_1 \le k, v_1\ v_2.(t_1 \Downarrow^{c_1,k_1} v_1 \wedge t_2 \Downarrow^{c_2,k_2} v_2) \Rightarrow \\
&\quad (v_1,v_2) \in (\!|\tau|\!)_{G,k-k_1} \wedge c_1 - c_2 \le D\} \\
(\!|\cdot|\!)_{G,k} &= \{\emptyset\} \\
(\!|\Gamma|\!)_{G,k} &= \{(\sigma_1,\sigma_2) \mid \forall x \in dom(\Gamma).\forall \tau.x : \tau \in \Gamma.(\sigma_1(x),\sigma_2(x)) \in (\!|\tau|\!)_{G,k}\}
\end{aligned}
$$

where

$$
\begin{aligned}
(H_1,H_2) \vDash_{G,k} empty \quad &\text{iff} \quad \text{true} \\
(H_1,H_2) \vDash_{G,k} (\gamma \rightarrowtail \beta) \quad &\text{iff} \quad \exists l_1,l_2,\tau,n : G(\gamma) = (l_1,l_2,\tau,n) \\
&\quad \wedge \big(\forall i \le n.\big(H_1[l_1][i], H_2[l_2][i]\big) \in (\!|\tau|\!)_{G,k-1}\big) \\
&\quad \wedge \big(\forall i \le n.\big(H_1[l_1][i] \neq H_2[l_2][i] \Rightarrow i \in \beta\big)\big) \\
(H_1,H_2) \vDash_{G,k} (P * Q) \quad &\text{iff} \quad \exists H_1', H_1'', H_2', H_2'', G', G'' : \\
&\quad \big(H_1 = H_1' \uplus H_1''\big) \wedge \big(H_2 = H_2' \uplus H_2''\big) \wedge \big(G = G' \uplus G''\big) \\
&\quad \wedge \big((H_1', H_2') \vDash_{G',k} P\big) \wedge \big((H_1'', H_2'') \vDash_{G'',k} Q\big) \\
G(\gamma) = (l_1,l_2,\tau,n), \quad &G|_1(\gamma) = (l_1,|\tau|_1,n), G|_2(\gamma) = (l_2,|\tau|_2,n)
\end{aligned}
$$

Figure 22: Relational interpretation of types

2 Logical relation

We use $\lambda x.t$ as syntatic sugar for $\mathrm{fix}\, f(x).t$ when f does not show in t.

Lemma 1 (Monotonicity)**.**

1. *If $k' \le k$ and $G \subseteq G'$, then $(\!|\tau|\!)_{G,k} \subseteq (\!|\tau|\!)_{G',k'}$.*
2. *If $k' \le k$ and $g \subseteq g'$, then $[\![A]\!]_{g,k} \subseteq [\![A]\!]_{g',k'}$.*
3. *If $k' \le k$ and $G \subseteq G'$, then $(\!|\tau|\!)^{E,D}_{G,k} \subseteq (\!|\tau|\!)^{E,D}_{G',k'}$.*
4. *If $k' \le k$ and $g \subseteq g'$, then$[\![A]\!]^{E,(L,U)}_{g,k} \subseteq [\![A]\!]^{E,(L,U)}_{g',k'}$.*
5. *If $k' \le k$ and $G \subseteq G'$, then $(\!|\Gamma|\!)_{G,k} \subseteq (\!|\Gamma|\!)_{G',k'}$*
6. *If $k' \le k$ and $g \subseteq g'$, then$[\![\Omega]\!]_{g,k} \subseteq [\![\Omega]\!]_{g',k'}$*

Proof. (1,3) and (2,4) are proved simultaneously by induction on τ and induction hypothesis,(5,6) follows from (1,2). □

Lemma 2 (Heap extension)**.** *If $(H_1, H_2) \vDash_{G,k} P$, then for any H_1', H_2', $(H_1 \uplus H_1', H_2 \uplus H_2') \vDash_{G,k} P$.*

Proof. It is simply proved by case analysis on P. □

Lemma 3 (Heap evaluation extension)**.** *If $H; t \Downarrow_f^{c,k} H_1; v$, then for any H', $H \uplus H'; t \Downarrow_f^{c,k} H_1 \uplus H'; v$.*

Proof. The proof is by induction on evaluation derivation on operation semantics. □

Lemma 4 (Evaluation cost soundness)**.**

1. *If $\vdash_L^U t : \tau$ and $t \Downarrow^c v$, then $L \le c \le U$.*
2. *If $\vdash_L^U t : \{P\}\ \overset{\mathrm{exec}(L',U')}{\exists \gamma : A}\ \{Q\}$ and $t \Downarrow_p^c v$, then $L + L' \le c \le U + U'$.*
3. *If $\vdash_L^U t : \{P_1\}^{U_1}_{L_1} \exists \gamma_1 : \{P_2\}^{U_2}_{L_2} \exists \gamma_2 : \ldots \{Q_2\}\{Q_1\}$ and $t; H \Downarrow_p^{c_1} v_1; H1$ and $H_1; v_1 \Downarrow_p^{c_2} v_2; H_2$ etc, then $L + L_1 + L_2 + \ldots L_n \le c_1 + c_2 + \cdots + c_n \le U + U_1 + U_2 + \cdots + U_n$.*
4. *If $\vdash t_1 \ominus t_2 \lesssim D : \tau$ and $t_1 \Downarrow_p^{c_1} v_1$ and $t_2 \Downarrow_p^{c_2} v_2$, then $c_1 - c_2 \le D$.*
5. *If $\vdash t_1 \ominus t_2 \lesssim D : \{P\}\ \overset{\mathrm{diff}(D')}{\exists \gamma : \tau}\ \{Q\}$ and $t_1 \Downarrow_p^{c_1} v_1$ and $t_2 \Downarrow_p^{c_2} v_2$, then $c_1 - c_2 \le D + D'$.*
6. *If $\vdash t_1 \ominus t_2 \lesssim D : \{P_1\}^{\mathsf{diff}(D_1)} \exists \gamma_1 : \{P_2\}^{\mathsf{diff}(D_2)} \exists \gamma_2 : \ldots \{Q_2\}\{Q_1\}$ and $t; H \Downarrow_p^{c_1} v_1; H1$ and $v_1; H_1 \Downarrow_p^{c_2} v_2; H_2$ then $c_1 - c_2 \le D + D_1 + D_2 \ldots D_n$.*

Proof. (1) is directly proved from the definition of unary expression interpretation. If $\vdash_L^U t : \tau$, then $t \in [\![\tau]\!]^{E,(L,U)}_{G,k}$, unfold the definition, we get : $L \le c \le U$ and $t \Downarrow^c v$.
(2) $t \in [\![\{P\}\ \overset{\mathrm{exec}(L',U')}{\exists \gamma : A}\ \{Q\}]\!]^{E,(L,U)}_{G,k}$, $t \Downarrow^{c_1} v'$ and $v' \Downarrow_f^{c_2} v$ unfold the definition, we know $c = c_1 + c_2$ and $L \le c_1 \le U$ and $L' \le c_2 \le U'$. It is proved.
(3) $t \in [\![\{P_1\}^{U_1}_{L_1} \exists \gamma_1 : \{P_2\}^{U_2}_{L_2} \exists \gamma_2 : \ldots \{Q_2\}\{Q_1\}]\!]^{E,(L,U)}_{G,k}$. Unfold the definition, we can get : $L + L_1 + L_2 + \ldots L_n \le c_1 + c_2 + \cdots + c_n \le U + U_1 + U_2 + \cdots + U_n$. This case is proved.
(4) From the fundamental theory, If $\vdash t_1 \ominus t_2 \lesssim D : \tau$, we know closed terms (t_1, t_2) in the interpretation of relational type τ, $(\!|\tau|\!)^{E,D}_{G,k}$, unfold the definition, $c_1 - c_2 \le D$ is proved.

(5) From the fundamental theory, If $\vdash t_1 \ominus t_2 \lesssim D : \{P\} \overset{\mathsf{diff}(D')}{\exists} \gamma : \tau \{Q\}$, we know closed terms (t_1, t_2) in the interpretation $(\!|\{P\} \overset{\mathsf{diff}(D')}{\exists} \gamma : \tau \{Q\}|\!)^{E,D}_{G,k}$, unfold the definition, $c_1 - c_2 \leq D + D'$ is proved.
(6) From the fundamental theory, If $\vdash t_1 \ominus t_2 \lesssim D : \{P_1\}^{\mathsf{diff}(D_1)} \exists \gamma_1 : \{P_2\}^{\mathsf{diff}(D_2)} \exists \gamma_2 : \ldots \{Q_2\}\{Q_1\}$, we know closed terms (t_1, t_2) in the interpretation of nested relational type τ, $(\!|\tau|\!)^{E,D}_{G,k}$, unfold the definition level by level, $c_1 - c_2 \leq D + D_1 + D_2 \cdots + D_n$ is proved.

□

Lemma 5 (Well-formedness)**.**

1. *If* $\Delta; \Phi; \Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau$, *then* $FV(t_1) \subseteq dom(\Gamma)$ *and* $FV(t_2) \subseteq dom(\Gamma)$.
2. *If* $\Delta; \Phi; \Omega \vdash^U_L t : A$, *then* $FV(t) \subseteq dom(\Omega)$.

Proof. The proof is by induction on the typing derivations. □

Lemma 6 (Value Projection)**.**

1. *If* $(v_1, v_2) \in (\!|\tau|\!)_{G,k}$, *then* $\forall k. v_1 \in [\![|\tau|_1]\!]_{G|_1,k}$ *and* $v_2 \in [\![|\tau|_2]\!]_{G|_2,k}$.
2. *If* $(\sigma_1, \sigma_2) \in (\!|\Gamma|\!)_{G,k}$, *then* $\forall k. \sigma_1 \in (\!||\Gamma|_1|\!)_{G|_1,k}$ *and* $\sigma_2 \in (\!||\Gamma|_2|\!)_{G|_2,k}$.

Proof. Proof of Statement (1) is by induction on $(\!|\tau|\!)_{G,k}$. Proof of Statement (2) follows by proof of (1). □

Lemma 7 (Heap monotonicity)**.**

1. *If* $k' \leq k$ *and* $G' \supseteq G$, *then* $(H_1, H_2) \vDash_{G,k} P \Rightarrow (H_1, H_2) \vDash_{G',k'} P$
2. *If* $k' \leq k$ *and* $g' \supseteq g$, *then* $H \vDash_{g,k} P \Rightarrow H \vDash_{g',k'} P$

Proof. **proof of statement (1)**

Assume $k' \leq k$ and $G' \supseteq G$, and we have

$$H_1, H_2 \vDash_{G,k} P.$$

TS: $H_1, H_2 \vDash_{G',k'} P$
Unfold the definition of $H \vDash_{G',k'} P$
Do case analysis on P, there are three cases:

case 1: P=empty
It is vacuously true that $H \vDash_{g',k'} \mathsf{empty}$.

case 2: P= $\gamma \to \beta$
From $H_1, H_2 \vDash_{G,k} \gamma \to \beta$, we know:

$$G(\gamma) = (l_1, l_2, \tau, n) \tag{1}$$
$$\forall i \leq n. (H_1(l_1)[i], H_2(l_2)[i]) \in (\!|\tau|\!)_{G,k-1} \tag{2}$$
$$\forall i \leq n. (H_1(l_1)[i] \neq H_2(l_2)[i]) \Rightarrow i \in \beta \tag{3}$$

We conclude that $G'(\gamma) = (l_1, l_2, \tau, n)$ from assumption $G' \supseteq G$ and $\forall i \leq n. H(l)[i] \in (\!|\tau|\!)_{G',k'}$ by Lemma 1 on (2).

case 3: P= $P_1 \star P_2$

Suppose $\exists n.P = \{\gamma_i \to \beta_i\}$ for $i \in [1,\ldots,n]$.
Unfold the definition of $H_1, H_2 \vDash_{G,k} \{\gamma_i \to \beta_i\}$ for $i \in [1,\ldots,n]$.
We know there exists $H_1 = (h_1^1) \uplus (h_1^2) \uplus \cdots \uplus (h_1^n)$ and $H_2 = (h_2^1) \uplus (h_2^2) \uplus \cdots \uplus (h_2^n)$ and $G = G_1 \uplus G_2 \uplus \cdots \uplus G_n$
so that $h_1^i, h_2^i \vDash_{G_i,k} \gamma_i \to \beta_i$ for any i.
Since $G' \supseteq G$, we know there exists $G_i' \supseteq G_i$ s.t. $G' = G_1' \uplus G_2' \uplus \cdots \uplus G_n' \wedge \forall i.G_i' \supseteq G_i$
Use the conclusion of case 2, we know:
$\forall i \in [1,n].h_1^i, h_2^i \vDash_{G_i',k'} \gamma_i \to \beta_i$.

proof of statement (2)
Assume $k' \le k$ and $g' \supseteq g$, and we have

$$H \vDash_{g,k} P$$

. TS: $H \vDash_{g',k'} P$
Unfold the definition of $H \vDash_{g',k'} P$
Case analysis on P, there are three cases:

case 1: P=empty
It is vacuously true that $H \vDash_{g',k'} \mathsf{empty}$.

case 2: P= $\gamma \to \beta$
From $H \vDash_{g,k} \gamma$, we know:

$$g(\gamma) = (l, A, n) \tag{1}$$

$$\forall i \le n.H(l)[i] \in [\![A]\!]_{g,k-1} \tag{2}$$

We conclude that $g'(\gamma) = (l, A, n)$ from assumption $g' \supseteq g$ and $\forall i \le n.H(l)[i] \in [\![A]\!]_{g',k'}$ by Lemma 1 on (2).

case 3: P = $P * Q$
Assume $p = \{\gamma_i\}$ for $i \in [1,\ldots,n]$.
From the definition of $H \vDash_{g,k} \{\gamma_1, \gamma_2, \ldots, \gamma_n\}$, we know
$\exists H = (h_1^1) \uplus (h_1^2) \uplus \cdots \uplus (h_1^n)$ and $g = g_1 \uplus g_2 \uplus \cdots \uplus g_n$ s.t. $h_1^i \vDash_{g_i,k} \gamma_i \to \beta_i$ for any i.
Since $g' \supseteq g$, we know: $\exists g_1', g_2', \ldots, g_n'.g' = g_1' \uplus g_2' \uplus \cdots \uplus g_n' \wedge \forall i.g_i' \supseteq g_i$.
By the conclusion of case 2. we know: $h_1^i \vDash_{g_i',k'} \gamma_i$ for any i.

This completes the proof of statement (2). □

Lemma 8 (Value interpretation containment)**.**

1. *If* $(v_1, v_2) \in (\!|\tau|\!)_{G,k}$*, then* $(v_1, v_2) \in (\!|\tau|\!)_{G,k}^{E,0}$
2. *If* $v \in [\![A]\!]_{g,k}$*, then* $\forall t \ge 0.v \in [\![A]\!]_{g,k}^{E,(0,t)}$

Proof. (1) Assume $(v_1, v_2) \in (\!|\tau|\!)_{G,k}$(*)
TS: $(v_1, v_2) \in (\!|\tau|\!)_{G,k}^{E,0}$
Following the definition of $(\!|\tau|\!)_{G,k}^{E,0}$, we get: $v_1 \Downarrow^0 v_1$ and $v_1 \Downarrow^0 v_1$ and $0 - 0 \le 0$ and $(v_1, v_2) \in (\!|\tau|\!)_{G,k-0}$. This completes the proof. □

Proof. Assume $v \in [\![A]\!]_{g,k}$(*)
TS: $\forall t \ge 0.v \in [\![A]\!]_{g,k}^{E,(0,t)}$ Following the definition of $[\![A]\!]_{g,k}^{E,(0,t)}$. We know $v \Downarrow^0 v$ and $v \in [\![A]\!]_{g,k}$. This completes the proof. □

Lemma 9 (Value evaluation). $v \Downarrow^0 v$

Proof. By induction on the value term v. □

Lemma 10 (heap projection). *If* $(H_1, H_2) \vDash_{G,k} \gamma_i \to \beta_i, i \in (1,n)$,*then* $\forall T, T'.H_1 \vDash_{G|_1,k} \gamma_i \to T_i$ *and* $H_2 \vDash_{G|_2,k} \gamma_i \to T_i'$

Proof. Suppose $H_1 = h_1 \uplus h_2 \ldots h_n$ and $H_2 = h_1' \uplus h_2' \ldots h_n'$

Unfold $(h_i, h_i') \vDash_{G,k} \gamma_i \to \beta_i$
we know:

$$G(\gamma) = (l_1, l_2, \tau, n) \tag{1}$$
$$\forall i \le n.(h_i(l_1)[i], h_i'(l_2)[i]) \in (\!|\tau|\!)_{G,k-1} \tag{2}$$

From (1), we know:

$$G|_1(\gamma) = (l_1, \gamma, n) \tag{3}$$
$$G|_2(\gamma) = (l_2, \gamma, n) \tag{4}$$

From(2) and Lemma (Value projection) and ,we know:

$$\forall i \le n.(H_1(l_1)[i]) \in [\![|\tau|_1]\!]_{G|_1,k-1} \tag{5}$$
$$\forall i \le n.(H_2(l_1)[i]) \in [\![|\tau|_2]\!]_{G|_2,k-1} \tag{6}$$

Using (3)(5), (4)(6), this lemma is proved.

□

Lemma 11 (heap subtyping). *If* $\vdash \delta : \Delta$ *and* $\vDash \delta\Phi$ *and* $\Delta;\Phi \vDash P \subseteq P'$ *and* $H_1, H_2 \vDash_{G,k} \delta P$, *then* $H_1, H_2 \vDash_{G,k} \delta P'$.

Proof. Assume we have:

$$H_1, H_2 \vDash_{G,k} \delta P$$

We want to show :

$$H_1, H_2 \vDash_{G,k} \delta P'$$

Suppose $\exists n.\delta P = \{\gamma_i \to \beta_i\}$ for $i \in [1,\ldots,n]$.
Unfold the definition of $H_1, H_2 \vDash_{G,k} \{\gamma_i \to \beta_i\}$ for $i \in [1,\ldots,n]$.
We know there exists $H_1 = (h_1^1) \uplus (h_1^2) \uplus \cdots \uplus (h_1^n)$ and $H_2 = (h_2^1) \uplus (h_2^2) \uplus \cdots \uplus (h_2^n)$ and $G = G_1 \uplus G_2 \uplus \cdots \uplus G_n$ so that $h_1^i, h_2^i \vDash_{G_i,k} \gamma_i \to \beta_i$ for any i.
Unfold the definition of $\Delta;\Phi \vDash \delta P \subseteq \delta P'$, we know:

$$\delta P' = \{\gamma_i \to \beta_i'\}, i \in [1,\ldots,n]$$

STS: $\forall i \in [1,\ldots,n].\exists x_1^i, x_2^i \vDash_{G_i,k]} \gamma_i \to \beta_i'$ where $H_1 = (x_1^1) \uplus (x_1^2) \uplus \cdots \uplus (x_1^n)$ and $H_2 = (x_2^1) \uplus (x_2^2) \uplus \cdots \uplus (x_2^n)$
Pick i.Choose $x_1^i = h_1^i$ and $x_2^i = h_2^i$
Unfold the definition of $h_1^i, h_2^i \vDash_{G_i,k} \gamma_i \to \beta_i$.
we have: $G_i(\gamma_i) = (l_1^i, l_2^i, \tau^i, n)$ and $\forall m \le n.(h_1^i(l_1^i[m]) \neq h_2^i(l_2^i)[m]) \Rightarrow m \in \beta_i$
Since we know $\beta_i \subseteq \beta_i'$, we get:

$$\forall i \in [1,\ldots,n].G_i(\gamma_i) = (l_1^i, l_2^i, \tau_i, n) \wedge \forall m \le n.(x_1^i(m) \neq x_2^i(m)) \Rightarrow m \in \beta_i'$$

For any $i \in [1,\ldots,n]$, choose $x_1^i = h_1^i$ and $x_2^i = h_2^i$, we know: $x_1^i, x_2^i \vDash_{G_i,k} \gamma_i \to \beta_i'$
We also know $H_1 = (x_1^1) \uplus (x_1^2) \uplus \cdots \uplus (x_1^n)$ and $H_2 = (x_2^1) \uplus (x_2^2) \uplus \cdots \uplus (x_2^n)$ from assumption.

This completes the proof of the lemma. □

Lemma 12 (Subtyping soundness)**.**
1. *If* $\Delta;\Phi \models \tau \sqsubseteq \tau'$ *and* $\vdash \delta : \Delta$ *and* $\models \Phi\delta$ *and* $(v,v') \in (\!|\delta\tau|\!)_{G,k}$*, then* $(v,v') \in (\!|\delta\tau'|\!)_{G,k}$.
2. *If* $\Delta;\Phi \models A \sqsubseteq A'$ *and* $\vdash \delta : \Delta$ *and* $\models \Phi\delta$ *and* $(v) \in [\![\delta A]\!]_{g,k}$*, then* $(v) \in [\![\delta A']\!]_{g,k}$.
3. *If* $\Delta;\Phi \models \tau \sqsubseteq \tau'$ *and* $\vdash \delta : \Delta$ *and* $\models \Phi\delta$ *and* $(t,t') \in (\!|\delta\tau|\!)^{E,D}_{G,k}$ *and* $D \le D'$*, then* $(t,t') \in (\!|\delta\tau'|\!)^{E,D'}_{G,k}$.
4. *If* $\Delta;\Phi \models A \sqsubseteq A'$ *and* $\vdash \delta : \Delta$ *and* $\models \Phi\delta$ *and* $t \in [\![\delta A]\!]^{E,(L,U)}_{g,k}$ *and* $L' \le L$ *and* $U \le U'$*, then* $t \in [\![\delta A']\!]^{E,(L',U')}_{g,k}$.
5. *If* $\Delta;\Phi \models \tau \sqsubseteq \tau'$ *and* $\vdash \delta : \Delta$ *and* $\models \Phi\delta$ *and* $\forall i \in \{1,2\}.\ (v) \in [\![|\delta\tau|_i]\!]_{G|_i,k}$*, then* $v \in [\![|\delta\tau'|_i]\!]_{G|_i,k}$.
6. *If* $\Delta;\Phi \models \tau \sqsubseteq \tau'$ *and* $\vdash \delta : \Delta$ *and* $\models \Phi\delta$ *and* $\forall i \in \{1,2\}.\ (e) \in [\![|\delta\tau|_i]\!]^{E,(L,U)}_{G|_i,k}$ *and* $L' \le L$ *and* $U \le U'$*, then* $e \in [\![|\delta\tau'|_i]\!]^{E,(L,U)}_{G|_i,k}$.

Proof Statements (1) and (2) (5) are by proven simultaneously by induction on the subtyping derivation. (3),(4),(6) will be proved first.

Proof. **Proof of statement (3)** Assume that $\Delta;\Phi \models \tau \sqsubseteq \tau'$ and $\vdash \delta : \Delta$ and $\models \Phi\delta$ and $(t,t') \in (\!|\delta\tau|\!)^{E,D}_{G,k}$ and $D \le D'$.
TS: $(t,t') \in (\!|\delta\tau'|\!)^{E,D'}_{G,k}$.
Assume that

1. $t \Downarrow^{s,c} v$
2. $t' \Downarrow^{s',c'} v'$
3. $s < k$

Unfold the assumption $(t,t') \in (\!|\delta\tau|\!)^{E,D}_{G,k}$ using assumption (1)(2)(3), we know

$$c - c' \le D \tag{a}$$
$$(v,v') \in (\!|\delta\tau|\!)_{G,k-s} \tag{b}$$

we conclude:
$c - c' \le D'$ from assumption $D \le D'$
By IH1 on (b), we know $(v,v') \in (\!|\delta\tau'|\!)_{G,k-s}$ □

Proof. **Proof of statement (4)** Assume $\Delta;\Phi \models A \sqsubseteq A'$ and $\vdash \delta : \Delta$ and $\models \Phi\delta$ and $e \in [\![\delta A]\!]^{E,(L,U)}_{g,k}$ and $L' \le L$ and $U \le U'$
TS: $t \in [\![\delta A]\!]^{E,(L,U)}_{g,k}$
Assume:

1. $t \Downarrow^{s,c}$
2. $s < k$

Unfold the assumption $t \in [\![\delta A]\!]^{E,(L,U)}_{g,k}$, we know:

$$L \le c \le U \tag{a}$$
$$v \in [\![\delta A]\!]_{g,k-s} \tag{b}$$

We conclude: $L' \le c \le U'$ from assumption.
By IH2 with the first premise on (b), we get: $v \in [\![\delta A']\!]_{g,k-s}$ □

Proof. **Proof of statement (6)** Assume $\Delta;\Phi \models \tau \sqsubseteq \tau'$ and $\vdash \delta : \Delta$ and $\models \Phi\delta$ and $\forall i \in \{1,2\}.\ (e) \in [\![|\delta\tau|_i]\!]^{E,(L,U)}_{G|_i,k}$ and $L' \le L$ and $U \le U'$
TS: $t \in [\![|\delta\tau'|_i]\!]^{E,(L,U)}_{G|_i,k}$
Assume:

1. $t \Downarrow^{s,c}$
2. $s < k$

Unfold the assumption $t \in [\![|\delta\tau'|_i]\!]^{E,(L,U)}_{G|_i,k}$, we know:

$$L \le c \le U \tag{a}$$
$$v \in [\![|\delta\tau'|_i]\!]_{G|_i,k-s} \tag{b}$$

We conclude: $L' \le c \le U'$ from assumption.
By IH5 with the first premise on (b), we get:$v \in [\![|\delta\tau'|_i]\!]_{G|_i,k-s}$ □

Proof of statement (1)
The proof is by induction on the subtyping derivation, we will detail some of the most interesting cases.
Case

$$\frac{\Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Delta;\Phi \models D \le D' \qquad \Delta;\Phi \models P' \subseteq P \qquad \Sigma, \vec{\gamma_1} : \vec{\mathbb{L}};\Delta;\Phi \models Q \subseteq Q' \qquad \Sigma \models \vec{\gamma_1} \sqsubseteq \vec{\gamma_2}}{\Sigma;\Delta;\Phi \models \{P\}\ \exists^{\mathrm{diff}(D)} \vec{\gamma_1} : \tau\ \{Q\} \sqsubseteq \{P'\}\ \exists^{\mathrm{diff}(D')} \vec{\gamma_2} : \tau'\ \{Q'\}}\ \text{S-RM}$$

Assume δ such that $\vdash \delta : \Delta$ and $\models \delta\Phi$. Assume also that we have G, k, v_1, v_2 such that

$$(v_1, v_2) \in (\!|\{\delta P\}\ \exists^{\mathrm{diff}(\delta D)} \vec{\gamma_1} : \delta\tau\ \{\delta Q\}|\!)_{\delta G,k} \tag{1}$$

We want to show

$$(v_1, v_2) \in (\!|\{\delta P'\}\ \exists^{\mathrm{diff}(\delta D')} \vec{\gamma_2} : \delta\tau'\ \{\delta Q'\}|\!)_{\delta G,k} \tag{2}$$

By definition, consider $G_1 \supseteq \delta G, k_1 \le k, k_2 < k, H_1, H_2$ and assume

$$(H_1, H_2) \models_{G_1,k_1} \delta P' \wedge H_1; v_1 \downarrow^{k_2}_f \wedge H_2; v_2 \not\downarrow^f$$

Since $\Delta;\Phi \models P' \subseteq P$ we also have $(H_1, H_2) \models_{G_1,k_1} \delta P$.
Thus, by Equation (1) we have that there exist $G_2 \supseteq G_1, H_1', H_2', v_1', v_2', c_1, c_2$ such that

$$v_1; H_1 \Downarrow^{c_1,k_2}_f v_1'; H_1' \wedge v_2; H_2 \Downarrow^{c_2,k_2}_f v_2'; H_2' \wedge (H_1', H_2') \models_{G_2,k_1-k_2} \delta Q \wedge (v_1', v_2') \in (\!|\delta\tau|\!)_{G_2,k_1-k_2} \wedge c_1 - c_2 \le \delta D$$

Since $\Sigma, \vec{\gamma_1} : \vec{\mathbb{L}};\Delta;\Phi \models Q \subseteq Q'$ we also have $(H_1', H_2') \models_{G_2,k_1-k_2} \delta Q'$ by using Lemma 11 on $(H_1', H_2') \models_{G_2,k_1-k_2} \delta Q$.
Additionally, from $\Delta;\Phi \models \tau \sqsubseteq \tau'$ and $\Delta;\Phi \models D \le D'$
By IH on the first premise, we also get
$(v_1', v_2') \in (\!|\delta\tau'|\!)_{G_2,k_1-k_2}$ and $c_1 - c_2 \le \delta D'$ respectively.
So we can derive Equation (2), and this completes the proof of case-sub-r-monad.

S-RUM

$$\Sigma;\Delta;\Phi \models U\ (\{\gamma_i \to T_i\}\ \exists^{\mathrm{exec}(L,U)} \vec{\gamma_1'} : A_1\ \{Q_1\}, \{\gamma_i \to T_i'\}\ \exists^{\mathrm{exec}(L',U')} \vec{\gamma_2'} : A_1\ \{Q_2\}) \sqsubseteq \{\gamma_i \to \beta_i\}\ \exists^{\mathrm{diff}(U-L')} \vec{\gamma_1}, \vec{\gamma_2} : U(A_1, A_2)\ \{\gamma_i \to \beta_i \cup T_i \cup T_i'\}$$

Pick G,k,v,v'.
Assume $\vdash \delta : \Delta$ and $\models \Phi\delta$, we have:

$$(v, v') \in (\!|\delta U\ (\{\gamma_i \to T_i\}\ \exists^{\mathrm{exec}(L,U)} \vec{\gamma_1} : A_1\ \{Q_1\}, \{\gamma_i \to T_i'\}\ \exists^{\mathrm{exec}(L',U')} \vec{\gamma_1} : A_2\ \{Q_2\})|\!)_{G,k} \tag{a}$$

TS: $(v, v') \in (\!|\delta\ \{\gamma_i \to \beta_i\}\ \exists^{\mathrm{diff}(U-L')} \vec{\gamma_1}, \vec{\gamma_2} : U(A_1, A_2)\ \{\gamma_i \to \beta_i \cup T_i \cup T_i'\}|\!)_{G,k}$
Unfold the definition of $(\!|\delta\ \{\gamma_i \to \beta_i\}\ \exists^{\mathrm{diff}(U-L')} \vec{\gamma_1}, \vec{\gamma_2} : U(A_1, A_2)\ \{\gamma_i \to \beta_i \cup T_i \cup T_i'\}|\!)_{G,k}$.

Pick $G' \supseteq G, k' \leq k, k'' < k, H_1, H_2$.
Assume

$$(H_1, H_2) \vDash_{G',k'} \gamma_i \to \beta_i \tag{1}$$

$$H_1; v \downarrow_f^{k''} \wedge H_2; v' \not\downarrow^f \tag{2}$$

STS:$\exists G'' \supseteq G, H_1', H_2', v_1, v_1'$

$$H_1; v \Downarrow_f^{c_1,k''} H_1'; v_1 \tag{3}$$

$$H_2; v' \Downarrow_f^{c_2} H_2'; v_1' \tag{4}$$

$$H_1', H_2' \vDash_{G'',k'-k''} \gamma_i \to \beta_i \cup T_i \cup T_i' \tag{5}$$

$$(v_1, v_1') \in (\!| U(A_1, A_2) |\!)_{G'',k'-k''} \tag{6}$$

From (a), unfold its definition of $(\!| \delta U\ (\{\gamma_i \to T_i\}^{\text{exec}(L,U)}\ \exists \vec{\gamma}_1 : A_1\ \{Q_1\}, \{\gamma_i \to T_i'\}^{\text{exec}(L',U')}\ \exists \vec{\gamma}_1 : A_2\ \{Q_2\}) |\!)_{G,k}$

$$\forall k', v \in [\![\{\gamma_i \to T_i\}^{\text{exec}(L,U)}\ \exists \vec{\gamma}_1 : A_1\ \{Q_1\}]\!]_{G|_1,k'} \tag{b}$$

$$\forall k', v' \in [\![\{\gamma_i \to T_i'\}^{\text{exec}(L',U')}\ \exists \vec{\gamma}_2 : A_2\ \{Q_2\}]\!]_{G|_2,k'} \tag{c}$$

Pick k' as k.
Unfold its definition in (b).
Show we already got: $G'|_1 \supseteq G|_1$ and $k' \leq k$ and $k'' < k'$ and $H_1; v \downarrow_f^{k''}$ and $H_1 \vDash_{G'|_1,k'} \gamma_i \to T_i$ holds by using Lemma (heap projection) on (1).
Derive from the definition, we know:
$\exists g_1'' \supseteq G'|_1, H_1', v_1$.

$$H_1; v \Downarrow_f^{c_1,k''} H_1'; v_1 \tag{d}$$

$$H_1' \vDash_{g_1'',k'-k''} Q_1 \tag{e}$$

$$v_1 \in [\![A_1]\!]_{g_1'',k'-k''} \tag{f}$$

$$\forall i. g_1'(\gamma_i) = (l_i, A, m) \Rightarrow H_1(l)[n] \neq H_1'(l)[n] \Rightarrow n \in T_i \tag{*}$$

Unfold its definition in (c).
Show we already got: $G'|_2 \supseteq G|_2$ and $k' \leq k$ and $k'' < k'$ and $H_2; v \downarrow_f$ and $H_2 \vDash_{G'|_2,k'} \gamma_i \to T_i'$ holds by using Lemma 10 (heap projection) on (1).
There are two cases for $H_2; v \downarrow_f \Rightarrow H_2; v \downarrow_f^{k''}$:

1. $H_2; v \downarrow_f^{k_1}$ and $k_1 > k'$. Using Lemma 1, we get $H_2; v \downarrow_f^{k''}$
2. $H_2; v \downarrow_f^{k_1}$ and $k_1 \leq k'$. We choose $k'' = k_1$. we get $H_2; v \downarrow_f^{k''}$

Derive from the definition, we know:
$\exists g_2'' \supseteq G'|_2, H_2', v_1'$.

$$H_2; v \Downarrow_f^{c_2,k''} H_2'; v_1' \tag{g}$$

$$H_2' \vDash_{g_2'',k'-k''} Q_2 \tag{h}$$

$$v_1' \in [\![A_2]\!]_{g_2'',k'-k''} \tag{i}$$

$$\forall i. g_2'(\gamma_i) = (l_i, A, m) \Rightarrow H_2(l)[n] \neq H_2'(l)[n] \Rightarrow n \in T_i' \tag{**}$$

(3),(4) already proved.
STS1: $H_1', H_2' \vDash_{G'',k'-k''} \gamma_i \to \beta_i \cup T_i \cup T_i'$

From (e), we assume

$$H_1' = h_1 \uplus h_2 \uplus \dots h_n \tag{7}$$
$$H_2' = h_1' \uplus h_2' \uplus \dots h_n' \tag{8}$$

From (*),(**), we know:
$\forall i, n.(H_1(l_i)[n] = (H_2(l_i)[n]) \Rightarrow n \notin \beta_i$, otherwise, $n \in \beta_i$.
for all the n not in β_i, if $H_1(l_i)[n] \neq H_1'(l_i)[n]$, then $n \in T_i$. Similarly, if $H_2(l_i)[n] \neq H_2'(l_i)[n]$, then $n \in T_i'$.
Unfold the definition of $H_1', H_2' \vDash_{G,k} \gamma_i \rightarrow \beta_i \cup T_i \cup T_i'$. $\forall n.H_1'(l_i)[n] \neq H_2'(l_i)[n] \Rightarrow n \in \beta_i \cup T_i \cup T_i'$ because (1) at position n, values differs in H_1, H_2 means n in β_i (2) at position n, value same in H_1, H_2. and differ in H_1', H_2' means n must in T_i or T_i' or both.

This completes the proof of case sub-r-u-monad

Proof of statement (2). Proof is by induction on the subtyping derivation.

$$\frac{\Delta;\Phi \vDash L' \leq L \qquad \Delta;\Phi \vDash U \leq U' \qquad \Delta;\Phi \vDash A \sqsubseteq A' \qquad \Delta;\Phi \vDash P \subseteq P' \qquad \Sigma, \vec{\gamma}_1; \Delta;\Phi \vDash Q' \subseteq Q \qquad \vec{\gamma}_1 \subseteq \vec{\gamma}_2}{\Sigma;\Delta;\Phi \vDash \{P\}\ \overset{\text{exec}(L,U)}{\exists \vec{\gamma}_1 : A}\ \{Q\} \sqsubseteq \{P'\}\ \overset{\text{exec}(L',U')}{\exists \vec{\gamma}_2 : A'}\ \{Q'\}}\ \text{S-A-MONAD}$$

Pick g,k,v.
Assume $\vdash \delta : \Delta$ and $\vDash \Phi\delta$, we know

$$v \in \{P\}\ \overset{\text{exec}(L,U)}{\exists \vec{\gamma}_1 : A}\ \{Q\} \tag{a}$$

TS:

$$v \in \{P'\}\ \overset{\text{exec}(L',U')}{\exists \vec{\gamma}_2 : A'}\ \{Q'\} \tag{b}$$

Unfold the definition of $\{P\}\ \overset{\text{exec}(L,U)}{\exists \vec{\gamma}_1 : A}\ \{Q\}$, we pick $g' \supseteq g, k' \leq k, k'' < k', H$
Assume

$$H \vDash_{g',k'} P \tag{1}$$
$$H; v \downarrow_f^{k''} \tag{2}$$

We know: $\exists g'' \supseteq g, H', v_1$

$$H; v \Downarrow_f^{c_1,k''} H'; v_1 \tag{3}$$
$$H' \vDash_{g'',k'-k''} Q \tag{4}$$
$$v_1 \in [\![A]\!]_{g'',k'-k''} \tag{5}$$
$$P = \gamma_i \rightarrow T_i \Rightarrow \forall i.g''(\gamma_i) = (l_i, A, m) \Rightarrow H(l_i)[n] \neq H'(l_i)[n] \Rightarrow n \in T_i \tag{*}$$

Pick g'', H', v_1.

By IH 2 on the first premise $\Delta;\Phi \vDash A \sqsubseteq A'$ with (5), we know:

$$v_1 \in [\![A']\!]_{g'',k'-k''} \tag{6}$$

TS: $v \in \{P'\}\ \overset{\text{exec}(L',U')}{\exists \vec{\gamma}_2 : A'}\ \{Q'\}$, unfold its definition.
we know: $H \vDash_{g',k'} P'$ from (1) and $P \supseteq P'$ because P and P' have the same γ_i. together with (2)

STS:

$$H; v \Downarrow_f^{c_1,k''} H'; v_1 \tag{c}$$

$$H' \vDash_{g'',k'-k''} Q' \tag{d}$$

$$v_1 \in [\![A']\!]_{g'',k'-k''} \tag{e}$$

$$P' = \gamma_i \to T_i' \Rightarrow \forall i. g_1'(\gamma_i) = (l_i, A, m) \Rightarrow H(l_i)[n] \neq H'(l_i)[n] \Rightarrow n \in T_i' \tag{**}$$

(c) is proved by assumption (3).
(e) is proved by (6).
(d) is proved by (4) and $Q' \supseteq Q$ (**) is proved by (*). Because $P \supseteq P' \Rightarrow \forall i. T_i \supseteq T_i'$. For all the n in T_i, it is also in T_i' This completes the proof of sub-A-monad.‘

Proof of statement (5). Proof is by induction on the subtyping derivation. We will prove i=1, the proof of i=2 is similar

S-RUM

$$\Sigma; \Delta; \Phi \vDash U\ (\{\gamma_i \to T_i\}\ \exists \vec{\gamma_1'} : A_1\ \{Q_1\}, \{\gamma_i \to T_i'\}\ \exists \vec{\gamma_2'} : A_1\ \{Q_2\}) \overset{\text{exec}(L',U')}{\overset{\text{exec}(L,U)}{\sqsubseteq}} \{\gamma_i \to \beta_i\}\ \exists \vec{\gamma_1}, \vec{\gamma_2} : U(A_1, A_2)\ \{\gamma_i \to \beta_i \cup T_i \cup T_i'\}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \Phi\delta$. we have

$$v \in [\![|\delta U\ (\{\gamma_i \to T_i\}\ \exists \vec{\gamma_1} : A_1\ \{Q_1\}, \{\gamma_i \to T_i'\}\ \exists \vec{\gamma_1} : A_2\ \{Q_2\})|_i]\!]_{|G|_i,k} \tag{a}$$

TS:

$$v \in [\![|\delta\ \{\gamma_i \to \beta_i\}\ \exists \vec{\gamma_1}, \vec{\gamma_2} : U(A_1, A_2)\ \{\gamma_i \to \beta_i \cup T_i \cup T_i'\}\ |_i]\!]_{|G|_i,k} \tag{b}$$

Choose i=1.
From (a), we know:

$$v \in [\![\delta\ \{\gamma_i \to T_i\}\ \exists \vec{\gamma_1} : A_1\ \{Q_1\}]\!]_{|G|_1,k} \tag{c}$$

From (b),
STS:

$$v \in [\![|\delta\ \{\gamma_i \to \beta_i\}\ \exists \vec{\gamma_1}, \vec{\gamma_2} : A_1\ \{\gamma_i \to \beta_i \cup T_i \cup T_i'\}]\!]_{|G|_1,k} \tag{d}$$

Assume $g' \supseteq G|_1, k' \leq k, k'' < k'$. we assume

$$H \vDash_{g',k'} \gamma_i \to \mathbb{N} \tag{1}$$

$$H; v \downarrow_f^{k''} \tag{2}$$

STS: $\exists g'' \supseteq g', H', v'$

$$H; v \Downarrow_f^{k'',c_1} H'; v' \tag{3}$$

$$H' \vDash_{g'',k'-k''} \gamma_i \to \mathbb{N} \tag{4}$$

$$v' \in [\![A_1]\!]_{g'',k'-k''} \tag{5}$$

$$P' = \gamma_i \to \mathbb{N} \Rightarrow \forall i. g_1'(\gamma_i) = (l_i, A, m) \Rightarrow H(l_i)[n] \neq H'(l_i)[n] \Rightarrow n \in N \tag{**}$$

From (c), unfold its definition, we know (2) and $H \vDash_{g',k'} \gamma_i \to T_i$ holds from (1). Then we get: $\exists g'' \supseteq g', H', v'$

$$H; v \Downarrow_f^{k'',c_1} H'; v' \tag{e}$$

$$H' \vDash_{g'',k'-k''} Q_1 \tag{f}$$

$$v' \in [\![A_1]\!]_{g'',k'-k''} \tag{g}$$

$$P = \gamma_i \to T_i \Rightarrow \forall i. g_1'(\gamma_i) = (l_i, A, m) \Rightarrow H(l_i)[n] \neq H'(l_i)[n] \Rightarrow n \in T_i \tag{**}$$

(3) is proved by (e). (4) is proved by (f) because Q_1 contains at least as many γ_i as its precondition $\gamma_i \to T_i$. (*) is proved by (**) because $T_i \supseteq \mathbb{N}$ This completes the proof of this case.

$$\frac{\Sigma;\Delta;\Phi \models \tau \sqsubseteq \tau' \qquad \Delta;\Phi \models D \leq D' \qquad \Delta;\Phi \models P' \subseteq P \qquad \Sigma, \vec{\gamma_1} : \vec{\mathbb{L}}; \Delta; \Phi \models Q \subseteq Q' \qquad \Sigma \models \vec{\gamma_1} \sqsubseteq \vec{\gamma_2}}{\Sigma;\Delta;\Phi \models \{P\}\ \exists \vec{\gamma_1} : \tau\ \{Q\} \overset{\text{diff}(D)}{\sqsubseteq} \{P'\}\ \exists \vec{\gamma_2} : \tau'\ \{Q'\} \overset{\text{diff}(D')}{}} \text{ s-RM}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \Phi\delta$.
we have

$$v \in [\![|\ \{P\}\ \exists \vec{\gamma_1} : \tau\ \{Q\}\ |_i]\!]_{|G|_i,k} \overset{\text{diff}((c))}{} \tag{a}$$

TS:

$$v \in [\![|\delta\ \{P'\}\ \exists \vec{\gamma_2} : \tau'\ \{Q'\}\ |_i]\!]_{|G|_i,k} \overset{\text{diff}((c'))}{} \tag{b}$$

Choose i=1.
From (a), we know:

$$v \in [\![\delta\ \{|P|_1\}\ \exists \vec{\gamma_1} : |\tau|_1\ \{|Q|_1\}]\!]_{|G|_1,k} \overset{\text{exec}(0,\infty)}{} \tag{c}$$

From (c),STS:

$$v \in [\![\delta\ \{|P'|_1\}\ \exists \vec{\gamma_2} : |\tau'|_1\ \{|Q'|_1\}]\!]_{|G|_1,k} \overset{\text{exec}(0,\infty)}{} \tag{d}$$

From $P' \supseteq P$ and $Q \supseteq Q'$, we know $|P|_1 = |P'|_1 \wedge |Q|_1 = |Q'|_1$ It is trivially proved.

This completes the proof of case sub-r-monad.

Theorem 2.1 (Fundamental Theorem)**.**

1. *If* $\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau$ *and* $\vdash \delta : \Delta$ *and* $\vDash \delta\Phi$ *and* $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$*, then* $(\delta\sigma_1 t_1, \delta\sigma_2 t_2) \in (\!|\delta\tau|\!)_{G,k}^{E,(\delta D)}$.

2. *If* $\Sigma;\Delta;\Phi;\Omega \vdash_L^U t : A$ *and* $\vdash \delta : \Delta$ *and* $\vDash \delta\Phi$ *and there exists* Ω'*. s.t.* $FV(t) \subseteq dom(\Omega')$ *and* $\Omega' \subseteq \Omega$ *and* $\sigma \in (\!|\delta\Omega'|\!)_{g,k}$*, then* $(\delta\sigma t) \in [\![\delta A]\!]_{g,k}^{E,(\delta L,\delta U)}$.

3. *If* $\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau$ *and* $\vdash \delta : \Delta$ *and* $\vDash \delta\Phi$*, then for* $i \in \{1,2\}$*. if there exists* Γ_i' *s.t.* $FV(t_i) \subseteq dom(\Gamma_i')$ *and* $\Gamma_i' \subseteq \Gamma$ *and* $\sigma_i \in [\![|\delta\Gamma_i'|_i]\!]_{G|_i,k}$*, then* $\delta\sigma_i t_i \in [\![|\delta\tau_i|]\!]_{G|_i,k}^{E,(0,\infty)}$.

Corollary 2.1.1. *If* $\forall k.\bullet \vdash t_1 \ominus t_2 \lesssim n : \tau$*, then* $(t_1, t_2) \in (\!|\tau|\!)_{G,k}^E$.

Proof of statement (1). if $\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau$ and $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$ then $(t_1\delta\sigma_1, t_2\delta\sigma_2) \in (\!|\delta\tau|\!)_{G,k}^E$.

Proof by induction on typing derivation:

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;x:\tau_1,f\ :\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2,\Gamma \vdash t_1 \ominus t_2 \lesssim D:\tau_2}{\Sigma;\Delta;\Phi;\Gamma \vdash \text{Fix}\, f(x).t_1 \ominus \text{Fix}\, f(x).t_2 \lesssim 0:\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2}\ \text{FIX}$$

Assume that $\vdash \delta:\Delta$ and $\vDash \Phi\delta$ and $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1 \text{fix}\, f(x).t_1, \delta\sigma_2 \text{fix}\, f(x).t_2) \in (\!|\delta(\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2)|\!)^{E,D}_{G,k}$
By unfolding the definition and the fact that $\text{fix}\, f(x).t_1$ and $\text{fix}\, f(x).t_2$ are values
STS: $(\delta\sigma_1 \text{fix}\, f(x).t_1, \delta\sigma_2 \text{fix}\, f(x).t_2) \in (\!|\delta\tau_1 \overset{\text{diff}((\delta D))}{\longrightarrow} \delta\tau_2|\!)_{G,k}$
Set $F = \delta\sigma_1 \text{fix}\, f(x).t_1, F' = \delta\sigma_2 \text{fix}\, f(x).t_2$,
We want to prove a general statement

$$\forall m \le k.(F,F') \in (\!|\delta\tau_1 \overset{\text{diff}(\delta D)}{\longrightarrow} \delta\tau_2|\!)_{G,m}$$

by sub-induction on m, there are two cases to show.

subcase 1: m=0

Unfold the definition of function type interpretation, there are two parts to show:

subsubcase 1: $\forall k' < m.(v_1,v_2) \in (\!|\tau_1|\!)_{G,k'} \Rightarrow \ldots$
$k' \le -1$, it is vacuous by definition.

subsubcase 2: STS: $\forall j.F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,j} \wedge F' \in [\![|\delta\tau_1|_2 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_2]\!]_{G|_2,j}$
Pick j.

1. STS 1: $F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,j}$
We prove the more general statement

$$\forall m' \le j.F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m'} \tag{2.1}$$

By subinduction on m'.
There are two csases:

1.1. m'=0.
Unfold the definition of $[\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m'}$, there is no non-negative $k' < m'(0)$, it is vacuously true.

1.2. m'=m"+1.
By sub-IH on m"

$$F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m''} \tag{2.2}$$

STS: $F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m'}$
Unfold the definition of $[\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m''+1}$.
Pick $j'' < m''+1, g' \supseteq G|_1$ and assume that $v \in [\![|\delta\tau_1|_1]\!]_{g',j''}$.
STS: $\delta\sigma_1 t_1[v/x][\text{fix}\, f(x).t_1/f] \in [\![|\tau_2|_1]\!]^{E,(0,\infty)}_{g',j''}$
This follows by IH 3 on the premise instantiated with
$\sigma_1[v/x][\text{fix}\, f(x).t_1/f] \in [\![\delta(x:|\tau_1|_1, f:|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1, |\Gamma_1|)]\!]_{g',j''}$ which holds because

i. $FV(t_1) \subseteq dom(x:\tau_1, f:\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2, \Gamma)$ using Lemma 5.
ii. $\sigma_1 \in [\![|\delta\Gamma|_1]\!]_{g',j''}$ by Lemma 6 and then Lemma 1.
iii. $v \in [\![|\delta\tau_1|_1]\!]_{g',j''}$ from the assumption.

iv. $F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{g',j''}$ by Lemma 1 on (3.2).

2. STS 2: $F' \in [\![|\delta\tau_1|_2 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_2]\!]_{G|_2,j}$
   Its proof is similar with STS 1.

subcase 2: $m = m' + 1 \le k$

By the definition of function types, there are two parts to show:

subsubcase 1: $\forall k' < m.(v_1, v_2) \in (\!|\tau_1|\!)_{G,k} \Rightarrow \ldots$

Assume $G' \supseteq G, k' \le (m-1)$. Pick v_1, v_2 s.t. $(v_1, v_2) \in (\!|\delta\tau_1|\!)_{G',k'}$.

STS: $(t_1[v_1/x][\mathsf{fix}\, f(x).t_1/f], t_2[v_2/x][\mathsf{fix}\, f(x).t_2/f]) \in (\!|\delta\tau_2|\!)^{E,(\delta D)}_{G',k'}$

By IH on premise instantiated with $\sigma_1' = \sigma_1[v_1/x][\mathsf{fix}\, f(x).t_1/f], \sigma_2' = \sigma_2[v_2/x][\mathsf{fix}\, f(x).t_2/f]$ and $(\sigma_1', \sigma_2') \in (\!|(\Gamma, x:\tau, f :\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2)\delta|\!)_{G',k'}$ which holds because

1. $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G',k'}$ by assumption and Lemma 1.
2. $(v_1, v_2) \in (\!|\tau|\!)_{G',k'}$ from assumption
3. $(F_1, F_2) \in (\!|\delta(\tau_1 \to \tau_2)|\!)_{G',k'}$ from sub-IH $(F_1, F_2) \in (\!|\delta(\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2)|\!)_{G,m'}$ and Lemma 1 ($k' < m', G' \supseteq G$)

subsubcase 2: $\forall j.F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,j} \wedge F' \in [\![|\delta\tau_1|_2 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_2]\!]_{G|_2,j}$
which is already proved above

This completes the proof of this case.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;x:\tau_1, f :\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2, \Gamma, f : U(A_1,A_2) \vdash t_1 \ominus t_2 \lesssim D : \tau_2 \quad \Sigma;\Delta;\Phi;|\Gamma|_1 \vdash^0_0 \mathsf{Fix}\, f(x).t_1 : A_1 \quad \Sigma;\Delta;\Phi;|\Gamma|_2 \vdash^0_0 \mathsf{Fix}\, f(x).t_2 : A_2}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{Fix}\, f(x).t_1 \ominus \mathsf{Fix}\, f(x).t_2 \lesssim D : \tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2}\ \text{R-FIX-EXT}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \Phi\delta$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$.

TS: $(\mathsf{fix}\, f(x).t_1\delta\sigma_1, \mathsf{fix}\, f(x).t_2\delta\sigma_2) \in (\!|\delta(\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2)|\!)^{E,D}_{G,k}$

By unfolding the definition and the fact that $\mathsf{fix}\, f(x).t_1$ and $\mathsf{fix}\, f(x).t_2$ are values

STS: $(\mathsf{fix}\, f(x).t_1\delta\sigma_1, \mathsf{fix}\, f(x).t_2\delta\sigma_2) \in (\!|\delta\tau_1 \overset{\text{diff}(\delta D)}{\longrightarrow} \delta\tau_2|\!)_{G,k}$

Set $F = \mathsf{fix}\, f(x).t_1\delta\sigma_1, F' = \mathsf{fix}\, f(x).t_2\delta\sigma_2$,

We want to prove a general statement

$$\forall m \le k.(F, F') \in (\!|\delta\tau_1 \overset{\text{diff}((\delta D))}{\longrightarrow} \delta\tau_2|\!)_{G,m}$$

by sub-induction on m, there are two cases to show.

subcase 1: m=0

Unfold the definition of function type interpretation, there are two parts to show:

subsubcase 1: $\forall k' < m.(v_1, v_2) \in (\!|\tau_1|\!)_{G,k'} \Rightarrow \ldots$

$k' \le -1$, it is vacuous by definition.

subsubcase 2: STS: $\forall j.F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,j} \wedge F' \in [\![|\delta\tau_1|_2 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_2]\!]_{G|_2,j}$

Pick j.

1. STS 1: $F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,j}$
   We prove the more general statement

$$\forall m' \leq j. F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m'} \tag{2.3}$$

   By subinduction on m'.
   There are two csases:

   1.1. m'=0.
   Unfold the definition of $[\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m'}$, there is no non-negative $k' < 0(m')$, it is vacuously true.

   1.2. m'=m"+1.
   By sub-IH on m"

$$F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m''} \tag{2.4}$$

   STS: $F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m'}$
   Unfold the definition of $[\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,m''+1}$.
   Pick $j'' < m'' + 1, g' \supseteq G|_1$ and assume that $v \in [\![|\delta\tau_1|_1]\!]_{g',j''}$.
   STS: $\delta\sigma_1\, t_1[v/x][\text{fix}\, f(x).t_1/f] \in [\![|\tau_2|_1]\!]^{E,(0,\infty)}_{g',j''}$
   This follows by IH 3 on the premise instantiated with
   $\sigma_1[v/x][\text{fix}\, f(x).t_1/f] \in [\![\delta|(x:\tau_1, f:\delta\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \delta\tau_2, f:U(A_1,A_2),\Gamma_1)|_1]\!]_{g',j''} \Rightarrow$
   $\sigma_1[v/x][\text{fix}\, f(x).t_1/f] \in [\![\delta(x:|\tau_1|_1, f:A_1, |\Gamma_1|_1)]\!]_{g',j''}$ which holds because

   i. $FV(t_1) \subseteq dom(x:\tau_1, f:\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2, f:U(A_1,A_2),\Gamma)$ using Lemma 5.
   ii. $\sigma_1 \in [\![|\delta\Gamma|_1]\!]_{g',j''}$ by Lemma 6 and then Lemma 1.
   iii. $v \in [\![|\delta\tau_1|_1]\!]_{g',j''}$ from assumption.
   iv. $F \in [\![\delta A_1]\!]_{g',j''}$ by IH2 on the second premise of FIX-EXT instantiated with $\Omega' = |\Gamma|_1$ to show $F \in [\![\delta A_1]\!]_{G|_1,k}$. Then use Lemma 1 .

2. STS 2: $F' \in [\![|\delta\tau_1|_2 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_2]\!]_{G|_2,j}$
   Its proof is similar with STS 1.

subcase 2: $m = m' + 1 \leq k$

By the definition of function types, there are two parts to show:

subsubcase 1: $\forall k' < m.(v_1, v_2) \in (\!|\tau_1|\!)_{G,k} \Rightarrow \ldots$
Assume $G' \supseteq G, k' \leq (m-1)$. Pick v_1, v_2 s.t. $(v_1, v_2) \in (\!|\delta\tau_1|\!)_{G',k'}$.
STS: $(t_1[v_1/x][\text{fix}\, f(x).t_1/f], t_2[v_2/x][\text{fix}\, f(x).t_2/f]) \in (\!|\delta\tau_2|\!)^{E,(\delta D)}_{G',k'}$
By IH on premise instantiated with $\sigma_1' = \sigma_1[v_1/x][\text{fix}\, f(x).t_1/f], \sigma_2' = \sigma_2[v_2/x][\text{fix}\, f(x).t_2/f]$ and $(\sigma_1', \sigma_2') \in (\!|(\Gamma, x:\tau, f:\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2, f:U(A_1,A_2))\delta|\!)_{G',k'}$ which holds because

1. $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G',k'}$ by assumption and Lemma 1.
2. $(v_1, v_2) \in (\!|\tau|\!)_{G',k'}$ from assumption
3. $(F_1, F_2) \in (\!|\delta(\tau_1 \to \tau_2)|\!)_{G',k'}$ from sub-IH $(F_1, F_2) \in (\!|\delta(\tau_1 \overset{\text{diff}(D)}{\longrightarrow} \tau_2)|\!)_{G,m'}$ and Lemma 1 ($k' < m', G' \supseteq G$)
4. $(F_1, F_2) \in (\!|U(A_1,A_2)|\!)_{G',k}$. STS: $\forall n, i \in \{1,2\}.F_i \in (\!|A_i|\!)_{G|_i,n}$. By Lemma 6, we know $\forall k.\sigma_i \in (\!|\delta|\Gamma|_i|\!)_{g,k}$, it is proved by IH2 on the second and third premises respectively.

subsubcase 2: $\forall j. F \in [\![|\delta\tau_1|_1 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1]\!]_{G|_1,j} \wedge F' \in [\![|\delta\tau_1|_2 \overset{\text{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_2]\!]_{G|_2,j}$
which is already proved above

This proof is the same as case Fix.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \text{int}[I] \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \tau \qquad \gamma \text{ fresh} \qquad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Gamma \vdash \text{alloc}\, t_1\ t_2 \ominus \text{alloc}\, t_1'\ t_2' \lesssim 0 : \{P\}\ \exists\gamma.\ \overset{\text{diff}(D_1+D_2)}{\text{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \mathbb{N}\}}}\ \text{R-ALLOC}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \Phi\delta$ and $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $\left(\delta\sigma_1(\text{alloc}\, t_1\ t_2), (\delta\sigma_2(\text{alloc}\, t_1'\ t_2')\right) \in (\!|\{P\}\ \exists\vec{\gamma}.\ \overset{\text{diff}(D_1+D_2)}{\text{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \mathbb{N}\}}|\!)^{E,0}_{G,k}$
By unfolding the definition of $(\!|\tau|\!)^E_{G,k}$
STS: $\left(\delta\sigma_1(\text{alloc}\, t_1\ t_2), (\delta\sigma_2(\text{alloc}\, t_1'\ t_2')\right) \in (\!|\{P\}\ \exists\gamma.\ \overset{\text{diff}(D_1+D_2)}{\text{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \mathbb{N}\}}|\!)_{G,k}$
Unfold the definition of $(\!|\{P\}\ \exists\gamma.\ \overset{\text{diff}(D_1+D_2)}{\text{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \mathbb{N}\}}|\!)_{G,k}$.
Pick $G^{'} \supseteq G$, H_1, H_2, $k' \le k$, $k'' < k'$, k'''.
Assume

$$\delta\sigma_1(\text{alloc}\, t_1\ t_2); H_1 \Downarrow_f^{k''} \tag{1}$$

$$\delta\sigma_2(\text{alloc}\, t_1'\ t_2'); H_2 \Downarrow_f^{k'''} \tag{2}$$

Because t_1, t_2 are sub terms of $\delta\sigma$ alloc $t_1\ t_2$, t_1', t_2' are sub terms of $\delta\sigma$ alloc $t_1'\ t_2'$
From (1)(2), we get

$$\delta\sigma_1 t_1 \Downarrow_f^{k_1} \wedge \delta\sigma_1 t_2 \Downarrow_f^{k_2} \tag{3}$$

$$\delta\sigma_2 t_1' \Downarrow_f \wedge \delta\sigma_2 t_2' \Downarrow_f \tag{4}$$

From (3),(4), we get:

$$\exists v_1, v_2, k_1, k_2.\, \delta\sigma_1 t_1 \Downarrow^{k_1,c_1} v_1 \wedge \delta\sigma_1 t_2 \Downarrow^{k_2,c_2} v_2 \wedge k'' = k_1 + k_2 + 1 \wedge c = c_1 + c_2 + c_{alloc} \tag{a}$$

$$\exists v_1', v_2'.\, k_1', k_2'.\, \delta\sigma_2 t_1' \Downarrow^{k_1',c_1'} v_1' \wedge \delta\sigma_2 t_2' \Downarrow^{k_2',c_2'} v_2' \wedge k''' = k_1' + k_2' + 1 \wedge c' = c_1' + c_2' + c_{alloc} \tag{b}$$

From (a),(b) and the evaluation rules E-alloc we get:

$$\exists l.(\text{alloc}\, t_1\ t_2)\delta\sigma; H_1 \Downarrow_f^{k'',c} l; H_1, l \to [v_2, \ldots v_2] \tag{c}$$

$$\exists l'.(\text{alloc}\, t_1'\ t_2')\delta\sigma; H_2 \Downarrow_f^{K''',c'} l'; H_2, l' \to [v_2', \ldots v_2'] \tag{d}$$

By IH on the first premise instantiated with $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G',k''}$ using lemma 1, we get:

$$(\delta\sigma_1 t_1, \delta\sigma_2 t_1') \in (\!|\text{int}_r[I]|\!)^{E,D_1}_{G',k''} \tag{*}$$

Unfold the definition of $(\!|\text{int}_r[I]|\!)^E_{G',k''}$ and using (a) and $k_1 \le k''$, we know:

$$(v_1, v_1') \in (\!|\text{int}_r[I]|\!)_{G',k''-k_1} \Rightarrow v_1 = v_1' = I \wedge c_1 - c_1' \le D_1 \qquad \text{ih1}$$

By IH on the second premise instantiated with $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G',k'-k_1}$ using lemma 1, we get:

$$(\delta\sigma_1 t_2, \delta\sigma_2 t_2') \in (\!|\tau|\!)^{E,D_2}_{G',k'-k_1} \tag{**}$$

Unfold the definition of (**) and using (a), (b) and $k_2 \le k' - k_1$, we know

$$(v_2, v_2') \in (\!|\tau|\!)_{G',k'-k_1-k_2} = (\!|\tau|\!)_{G',k'-k''+1} \wedge c_2 - c_2' \le D_2 \qquad \text{ih2}$$

Let us assume:

$$G'' = G'[r \to (l, l', \tau, I)] \tag{e}$$
$$H_1' = H_1, l \to [v_2, v_2, \ldots, v_2] \tag{f}$$
$$H_2' = H_2, l' \to [v_2', v_2', \ldots, v_2'] \tag{g}$$

we want to show 3 cases.

TS1 $(l, l') \in (\!|\mathsf{Array}_\gamma[I]\ \tau|\!)_{G'', k'-k''}$
it is proved by unfolding the definition and using the assumption (e).

TS2 $(H_1', H_2') \vDash_{G'', k'-k''} P \star \gamma \to \mathbb{N}$
$G''(\gamma) = (l, l', \tau, I)$, $H_1'' = l \to [v_2, v_2, \ldots, v_2]$, $H_2'' = l' \to [v_2', v_2', \ldots, v_2']$

STS1 $\forall i \le I, (H_1''(l)[i], H_2''(l')[i]) \in (\!|\tau|\!)_{G'', k'-k''-1}$
It is proved by using ih2 and Lemma 1.

STS2 $\forall i \le I, H_1'(l)[i] \neq H_2''(l')[i] \to i \in \beta = \mathbb{N}$
it is trivial

TS3 $c - c' \le (D_1 + D_2)$ from ih1 and ih2.

This proof is complete.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathrm{int}[I] \quad \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \Box\tau \quad \gamma\ \mathsf{fresh} \quad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{alloc}\ t_1\ t_2 \ominus \mathsf{alloc}\ t_1'\ t_2' \lesssim 0 : \{P\}\ \exists\gamma.\ \mathsf{Array}_\gamma[I]\ \Box\tau\ \{P \star \gamma \to \emptyset\}}^{\mathrm{diff}(D_1+D_2)}\ \text{R-ALLOC-BOX}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \Phi\delta$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $\left(\delta\sigma_1(\mathsf{alloc}\ t_1\ t_2), (\delta\sigma_2(\mathsf{alloc}\ t_1'\ t_2')\right) \in (\!|\{P\}\ \exists\vec{\gamma}.\ \mathsf{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \emptyset\}|\!)^{E,0}_{G,k}$
$^{\mathrm{diff}(D_1+D_2)}$
By unfolding the definition of $(\!|\tau|\!)^E_{G,k}$
STS: $\left(\delta\sigma_1(\mathsf{alloc}\ t_1\ t_2), (\delta\sigma_2(\mathsf{alloc}\ t_1'\ t_2')\right) \in (\!|\{P\}\ \exists\gamma.\ \mathsf{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \emptyset\}|\!)_{G,k}$
$^{\mathrm{diff}(D_1+D_2)}$
Unfold the definition of $(\!|\{P\}\ \exists\gamma.\ \mathsf{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \emptyset\}|\!)_{G,k}$.
Pick $G' \supseteq G$, H_1, H_2, $k' \le k$, $k'' < k'$, k'''.
Assume

$$\delta\sigma_1(\mathsf{alloc}\ t_1\ t_2); H_1 \Downarrow_f^{k''} \tag{1}$$
$$\delta\sigma_2(\mathsf{alloc}\ t_1'\ t_2'); H_2 \Downarrow_f^{k'''} \tag{2}$$

Because t_1, t_2 are sub terms of $\delta\sigma\ \mathsf{alloc}\ t_1\ t_2$, t_1', t_2' are sub terms of $\delta\sigma\ \mathsf{alloc}\ t_1'\ t_2'$
From (1)(2), we get

$$\delta\sigma_1 t_1 \Downarrow_f^{k_1} \wedge \delta\sigma_1 t_2 \Downarrow_f^{k_2} \tag{3}$$
$$\delta\sigma_2 t_1' \Downarrow_f \wedge \delta\sigma_2 t_2' \Downarrow_f \tag{4}$$

From (3),(4), we get:

$$\exists v_1, v_2, k_1, k_2.\, \delta\sigma_1 t_1 \Downarrow^{k_1, c_1} v_1 \wedge \delta\sigma_1 t_2 \Downarrow^{k_2, c_2} v_2 \wedge k'' = k_1 + k_2 + 1 \wedge c = c_1 + c_2 + c_{alloc} \tag{a}$$
$$\exists v_1', v_2', k_1', k_2'.\, \delta\sigma_2 t_1' \Downarrow^{k_1', c_1'} v_1' \wedge \delta\sigma_2 t_2' \Downarrow^{k_2', c_2'} v_2' \wedge k''' = k_1' + k_2' + 1 \wedge c' = c_1' + c_2' + c_{alloc} \tag{b}$$

From (a),(b) and evaluation rules we get:

$$\exists l.(\mathsf{alloc}\ t_1\ t_2)\delta\sigma; H_1 \Downarrow_f^{k'', c} l; H_1, l \to [v_2, \ldots v_2] \tag{c}$$
$$\exists l'.(\mathsf{alloc}\ t_1'\ t_2')\delta\sigma; H_2 \Downarrow_f^{c'} l'; H_2, l' \to [v_2', \ldots v_2'] \tag{d}$$

By IH on the first premise instantiated with $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G',k''}$ using lemma 1, we get:

$$(\delta\sigma_1\, t_1, \delta\sigma_2\, t_1') \in (\!|\mathrm{int}_r\,[I]|\!)^{E,D_1}_{G',k''} \tag{*}$$

Unfold the definition of $(\!|\mathrm{int}_r\,[I]|\!)^{E}_{G',k''}$ and using (a) and $k_1 \le k''$, we know:

$$(v_1, v_1') \in (\!|\mathrm{int}_r\,[I]|\!)_{G',k''-k_1} \Rightarrow v_1 = v_1' = I \wedge c_1 - c_1' \le D_1 \qquad \text{ih1}$$

By IH on the second premise instantiated with $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G',k'-k_1}$ using lemma 1, we get:

$$(\delta\sigma_1\, t_2, \delta\sigma_2\, t_2') \in (\!|\tau|\!)^{E,D_2}_{G',k'-k_1} \tag{**}$$

Unfold the definition of (**) and using (a), (b) and $k_2 \le k' - k_1$, we know

$$(v_2, v_2') \in (\!|\Box\tau|\!)_{G',k'-k_1-k_2} = (\!|\Box\tau|\!)_{G',k'-k''+1} \wedge c_2 - c_2' \le D_2 \Rightarrow v_2 = v_2' \qquad \text{ih2}$$

Let us assume:

$$G'' = G'[r \to (l, l', \tau, I)] \tag{e}$$
$$H_1' = H_1, l \to [v_2, v_2, \ldots, v_2] \tag{f}$$
$$H_2' = H_2, l' \to [v_2', v_2', \ldots, v_2'] \tag{g}$$

we want to show 3 cases.

TS1 $(l, l') \in (\!|\mathsf{Array}_\gamma[I]\ \tau|\!)_{G'',k'-k''}$
it is proved by unfolding the definition and using the assumption (e).

TS2 $(H_1', H_2') \vDash_{G'',k'-k''} P \star \gamma \to \emptyset$
$G''(\gamma) = (l, l', \tau, I)$, $H_1'' = l \to [v_2, v_2, \ldots, v_2]$, $H_2'' = l' \to [v_2', v_2', \ldots, v_2']$

STS1 $\forall i \le I, (H_1''(l)[i], H_2''(l')[i]) \in (\!|\tau|\!)_{G'',k'-k''-1}$
It is proved by using ih2 and Lemma 1.

STS2 $\forall i \le I, H_1'(l)[i] \ne H_2''(l')[i] \to i \in \emptyset$
We know that $\forall i \le I. H_1(l)[i] = v_2, H_1'(l')[i] = v_2'$ and $v_2 = v_2'$ from ih2. We can not find any i that make $H_1'(l)[i] \ne H_2''(l')[i]$ hold. It is proved.

TS3 $c - c' \le (D_1 + D_2)$ from ih1 and ih2.

This proof is complete.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D_1 : \tau_1 \xrightarrow{\mathrm{diff}(D)} \tau_2 \qquad \Sigma;\Delta;\Phi;\Gamma \vdash u_1 \ominus u_2 \lesssim D_2 : \tau_1}{\Sigma;\Delta;\Phi;\Gamma \vdash t_1\, u_1 \ominus t_2\, u_2 \lesssim D + D_1 + D_2 : \tau_2}\ \text{R-APP}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \Phi\delta$ and $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(t_1\, u_1), (\delta\sigma_2(t_2\, u_2)) \in (\!|\delta\tau_2|\!)^{E,(D+D_1+D_2)}_{G,k}$.
Pick $k' \le k$, v_1, v_2.
Assume

$$\delta\sigma_1(t_1\, u_1) \Downarrow^{c,k'} v_1 \wedge \delta\sigma_2(t_2\, u_2) \Downarrow^{c'} v_2 \tag{a}$$

STS: $(v_1, v_2) \in (\!|\delta\tau_2|\!)_{G,k-k'} \wedge c - c' \le (D + D_1 + D_2)$.
From (a) and the evaluation rule R-App, we know:

$$\exists \ldots. (\delta\sigma_1\, t_1) \Downarrow^{k_1,c_1} \mathrm{fix}\, f(x).t_1' \wedge (\delta\sigma_1\, u_1) \Downarrow^{k_1',c_1'} v_1' \wedge$$
$$t_1'[\mathrm{fix}\, f(x).t_1'/f][v_1'/x] \Downarrow^{k_1'',c_1''} v_1 \wedge k' = k_1 + k_1' + k_1'' + 1 \wedge c = c_1 + c_1' + c_1'' + c_{app} \tag{1}$$
$$\exists \ldots. (\delta\sigma_2\, t_2) \Downarrow^{c_2} \mathrm{fix}\, f(x).t_2' \wedge (\delta\sigma_2\, u_2) \Downarrow^{c_2'} v_2' \wedge t_2'[\mathrm{fix}\, f(x).t_2'/f][v_2'/x] \Downarrow^{c_2''} v_2 \wedge c = c_2 + c_2' + c_2'' + c_{app} \tag{2}$$

By IH on the first premise instantiated with $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$, we get:

$$(\delta\sigma_1 t_1, \delta\sigma_2 t_2) \in (\!|\delta\tau_1 \overset{\mathrm{diff}(D)}{\longrightarrow} \delta\tau_2|\!)^{E,D_1}_{G,k} \tag{b}$$

By IH on the second premise instantiated with $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$, we get:

$$(\delta\sigma_1 u_1, \delta\sigma_2 u_2) \in (\!|\delta\tau_1|\!)^{E,D_2}_{G,k} \tag{c}$$

Unfold the definition of (b), because $k_1 < k$, from (1),(1), we get:

$$(\mathsf{fix}\, f(x).t_1', \mathsf{fix}\, f(x).t_2') \in (\!|\delta\tau_1 \overset{\mathrm{diff}(D)}{\longrightarrow} \delta\tau_2|\!)_{G,k-k_1} \wedge c_1 - c_2 \le D_1 \tag{3}$$

Unfold the definition of (c), because $k_1' < k$, from (1),(1), we get:

$$(v_1', v_2') \in (\!|\delta\tau_1|\!)_{G,k-k_1'} \wedge c_1 - c_2 \le D_1 \tag{4}$$

We want to show $(v_1,v_2) \in (\!|\delta\tau_2|\!)_{G,k-k',D}$ and $c_1'' - c_2'' \le D$.
Considering both the third statements in (1),(2), it is suffice to show:
STS: $(t_1'[\mathsf{fix}\, f(x).t_1'/f][v_1'/x], t_2'[\mathsf{fix}\, f(x).t_2'/f][v_2'/x]) \in (\!|\sigma|\!)^{E}_{G,k-k'+k_1''}$
Use Lemma 1 on (3) with $k-k'+k_1'' \le k-k_1$. we get:

$$(\mathsf{fix}\, f(x).t_1', \mathsf{fix}\, f(x).t_2') \in (\!|\delta\tau_1 \overset{\mathrm{diff}(D)}{\longrightarrow} \delta\tau_2|\!)_{G,k-k'+k_1''} \tag{5}$$

Unfold (5).
Because $G \supseteq G$ and $(k-k'+k_1'') \le k-k_1-1$
By using Lemma 1 on (4) and $(k-k'+k_1'') \le k-k_1'$, we get :

$$(v_1', v_2') \in (\!|\delta\tau_1|\!)_{G,k-k'+k_1''} \tag{6}$$

Using (6), we know:

$$(t_1'[\mathsf{fix}\, f(x).t_1'/f][v_1'/x], t_2'[\mathsf{fix}\, f(x).t_2'/f][v_2'/x]) \in (\!|\delta\tau_2|\!)^{E,D}_{G,k-k'+k_1''} \tag{7}$$

Unfold (7) and we know: $c_1'' - c_2'' \le D$

This completes the proof of case r-app.

$$\text{CASE}\ \frac{\begin{array}{c}\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \qquad \Delta \models I' \le I \qquad \Sigma;\Delta \vdash P \quad wf\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{read}\ t_1\ t_2 \ominus \mathsf{read}\ t_1'\ t_2' \overset{\mathrm{diff}(D_1+D_2)}{\lesssim} 0 : \{P \star \gamma \to \beta\}\ \exists\_.\tau\ \{P \star \gamma \to \beta\}}\ \text{R-R}$$

Assume that $\vdash \delta : \Delta$ and $\models \Phi\delta$ and $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(\mathsf{read}\ t_1\ t_2), \delta\sigma_2(\mathsf{read}\ t_1'\ t_2')) \in (\!|\delta\ \{P \star \gamma \to \overset{\mathrm{diff}(D_1+D_2)}{\beta}\}\ \exists\_.\tau\ \{P \star \gamma \to \beta\}|\!)^{E,0}_{G,k}$
Because read $t_1\ t_2$ is value.
STS: $(\delta\sigma_1(\mathsf{read}\ t_1\ t_2), \delta\sigma_2(\mathsf{read}\ t_1'\ t_2')) \in (\!|\delta\ \{P \star \gamma \to \overset{\mathrm{diff}(D_1+D_2)}{\beta}\}\ \exists\_.\tau\ \{P \star \gamma \to \beta\}|\!)_{G,k}$
Unfold the definition of $(\!|\delta\ \{P \star \gamma \to \overset{\mathrm{diff}(D_1+D_2)}{\beta}\}\ \exists\_.\tau\ \{P \star \gamma \to \beta\}|\!)_{G,k}$.
Pick $G' \supseteq G$, H_1, H_2, $k' \le k$, $k'' < k'$, k'''.
Assume

$$(H_1,H_2) \models_{G',k'} P \star \gamma \to \beta \tag{1}$$

$$\delta\sigma_1(\mathsf{read}\ t_1\ t_2); H_1 \Downarrow_f^{k''} \tag{2}$$

$$\delta\sigma_2(\mathsf{read}\ t_1'\ t_2'); H_2 \Downarrow_f^{k''} \tag{3}$$

Because t_1, t_2 are sub terms of read $t_1\ t_2$, t_1', t_2' are sub terms of read $t_1'\ t_2'$
From (2)(3), we get

$$\delta\sigma_1 t_1 \Downarrow_f^{k_1} \wedge \delta\sigma_1 t_2 \Downarrow_f^{k_2} \tag{4}$$

$$\delta\sigma_2 t_1' \Downarrow_f^{k_1'} \wedge \delta\sigma_2 t_2' \Downarrow_f^{k_2'} \tag{5}$$

From (4),(5), we get:

$$\exists l, n, k_1, k_2. \delta\sigma_1 t_1 \Downarrow^{k_1, c_1} l \wedge \delta\sigma_1 t_2 \Downarrow^{k_2, c_1'} n \wedge k'' = k_1 + k_2 + 1 \wedge c = c_1 + c_1' + c_{read} \tag{a}$$

$$\exists l', n', k_1', k_2'. \delta\sigma_2 t_1' \Downarrow^{k_1', c_2} l' \wedge \delta\sigma_2 t_2' \Downarrow^{k_2', c_2'} n' \wedge k''' = k_1' + k_2' + 1 \wedge c' = c_2 + c_2' + c_{read} \tag{b}$$

From (a),(b) and the evaluation rule we get:

$$\exists v. \delta\sigma_1(\text{read } t_1\ t_2); H_1 \Downarrow_f^{k'', c} v; H_1 \wedge H_1(l)[n] = v \tag{c}$$

$$\exists v'. \delta\sigma_2(\text{read } t_1'\ t_2'); H_2 \Downarrow_f^{k''', c'} v'; H_2 \wedge H_2(l')[n'] = v' \tag{d}$$

By IH on the first premise instantiated with $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G', k'}$ by lemma 1. we get:

$$(\delta\sigma_1 t_1, \delta\sigma_2 t_1') \in (\!|\mathsf{Array}_\gamma[I]\ \delta\tau|\!)_{G', k'}^{E, D_1} \tag{6}$$

Unfold (6), since $k_1 \le k'$ and $\delta\sigma_1 t_1 \Downarrow^{k_1} l$ and $\delta\sigma_2 t_1' \Downarrow l'$, we know

$$(l, l') \in (\!|\mathsf{Array}_\gamma[I]\ \delta\tau|\!)_{G', k'-k_1} \wedge c_1 - c_2 \le D_1 \tag{e}$$

From (e), we know :

$$G'(\gamma) = (l, l', \tau, I) \tag{7}$$

By IH on the second premise instantiated with $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G', k'}$ by lemma 1. we get:

$$(\delta\sigma_1 t_2, \delta\sigma_2 t_2') \in (\!|\delta\text{int}_r[I']|\!)_{G', k'}^{E} \tag{8}$$

Unfold (8), since $k_2 \le k'$,we know

$$(n, n') \in (\!|\text{int}_r[I']|\!)_{G', k'-k_2} \Rightarrow n = n' = I' \wedge c_1' - c_2' \le D_2 \tag{f}$$

Let us assume:

$$G' = G' \tag{g}$$

STS1: $(H_1, H_2) \vDash_{G', k'-k''} P \star \gamma \to \beta$
By Lemma 7 and (1),this is proved.

STS2: $(v, v') \in (\!|\tau|\!)_{G', k'-k''}$
from (c),(d). we know $H_1(l)[n] = v$ and $H_2(l')[n'] = v'$
based on (e) and (f), we know
Unfold (1), we know:
$\forall i \le n, (H_1(l)(i), H_2(l')(i)) \in (\!|\tau|\!)_{G', k'-1}$
s.t we know
$(H_1(l)[n], H_2(l')[n']) \in (\!|\tau|\!)_{G', k'-1}$
Because $k' - k'' \le k' - 1$,
By Lemma 1, We get: $(v, v') \in (\!|\tau|\!)_{G', k'-k''}$

STS3: $c - c' \le D_1 + D_2$, which is proved by (e),(f).

This completes the proof of case read.

$$\text{CASE}\ \frac{\begin{array}{c}\Sigma;\Delta;\Phi;\Gamma\vdash t_1\ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \\ \Sigma;\Delta;\Phi;\Gamma\vdash t_2\ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \qquad \Sigma;\Delta\models I'\le I \qquad \Sigma;\Delta;\Phi\models I'\notin\beta \qquad \Sigma;\Delta\vdash P\quad wf\end{array}}{\Sigma;\Delta;\Phi;\Gamma\vdash \mathsf{read}\ t_1\ t_2\ominus \mathsf{read}\ t_1'\ t_2' \lesssim 0 : \{P\star\gamma\to\beta\}\ \overset{\mathrm{diff}(D_1+D_2)}{\exists\_.\square\tau}\ \{P\star\gamma\to\beta\}}\ \text{R-RB}$$

Assume that $\vdash\delta:\Delta$ and $\models\Phi\delta$ and $(\sigma_1,\sigma_2)\in(\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(\mathsf{read}\ t_1\ t_2),\delta\sigma_2(\mathsf{read}\ t_1'\ t_2'))\in(\!|\delta\ \{P\star\gamma\to\beta\}\ \overset{\mathrm{diff}(D_1+D_2)}{\exists\_.\tau}\ \{P\star\gamma\to\beta\}|\!)^{E,0}_{G,k,}$
Because read $t_1\ t_2$ is value.
STS: $(\delta\sigma_1(\mathsf{read}\ t_1\ t_2),\delta\sigma_2(\mathsf{read}\ t_1'\ t_2'))\in(\!|\delta\ \{P\star\gamma\to\beta\}\ \overset{\mathrm{diff}(D_1+D_2)}{\exists\_.\tau}\ \{P\star\gamma\to\beta\}|\!)_{G,k}$
Unfold the definition of $(\!|\delta\ \{P\star\gamma\to\beta\}\ \overset{\mathrm{diff}(D_1+D_2)}{\exists\_.\tau}\ \{P\star\gamma\to\beta\}|\!)_{G,k}$.
Pick $G^{'}\supseteq G$, H_1, H_2,$k'\le k, k''<k', k'''$.
Assume

$$(H_1,H_2)\models_{G',k'} P\star\gamma\to\beta \tag{1}$$
$$\delta\sigma_1(\mathsf{read}\ t_1\ t_2);H_1\Downarrow_f^{k''} \tag{2}$$
$$\delta\sigma_2(\mathsf{read}\ t_1'\ t_2');H_2\Downarrow_f^{k''} \tag{3}$$

Because t_1,t_2 are sub terms of read $t_1\ t_2$, t_1',t_2' are sub terms of read $t_1'\ t_2'$
From (2)(3), we get

$$\delta\sigma_1 t_1\Downarrow_f^{k_1}\wedge\delta\sigma_1 t_2\Downarrow_f^{k_2} \tag{4}$$
$$\delta\sigma_2 t_1'\Downarrow_f^{k_1'}\wedge\delta\sigma_2 t_2'\Downarrow_f^{k_2'} \tag{5}$$

From (4),(5), we get:

$$\exists l,n,k_1,k_2.\delta\sigma_1 t_1\Downarrow^{k_1,c_1} l\wedge\delta\sigma_1 t_2\Downarrow^{k_2,c_1'} n\wedge k''=k_1+k_2+1\wedge c=c_1+c_1'+c_{read} \tag{a}$$
$$\exists l',n',k_1',k_2'.\delta\sigma_2 t_1'\Downarrow^{k_1',c_2} l'\wedge\delta\sigma_2 t_2'\Downarrow^{k_2',c_2'} n'\wedge k'''=k_1'+k_2'+1\wedge c'=c_2+c_2'+c_{read} \tag{b}$$

From (a),(b) and evaluation rules we get:

$$\exists v.H_1;\delta\sigma_1(\mathsf{read}\ t_1\ t_2)\Downarrow_f^{k'',c}\ v;H_1\wedge H_1(l)[n]=v \tag{c}$$
$$\exists v'.H_2;\delta\sigma_2(\mathsf{read}\ t_1'\ t_2')\Downarrow_f^{k''',c'}\ v';H_2\wedge H_2(l')[n']=v' \tag{d}$$

By IH on the first premise instantiated with $(\sigma_1,\sigma_2)\in(\!|\delta\Gamma|\!)_{G',k'}$ by lemma 1. we get:

$$(\delta\sigma_1 t_1,\delta\sigma_2 t_1')\in(\!|\mathsf{Array}_\gamma[I]\ \delta\tau|\!)^{E,D_1}_{G',k',} \tag{6}$$

Unfold (6), since $k_1\le k'$ and $\delta\sigma_1 t_1\Downarrow^{k_1} l$ and $\delta\sigma_2 t_1'\Downarrow l'$, we know

$$(l,l')\in(\!|\mathsf{Array}_\gamma[I]\ \delta\tau|\!)_{G',k'-k_1}\wedge c_1-c_2\le D_1 \tag{e}$$

From (e), we know :

$$G'(\gamma)=(l,l',\tau,I) \tag{7}$$

By IH on the second premise instantiated with $(\sigma_1,\sigma_2)\in(\!|\delta\Gamma|\!)_{G',k'}$ by lemma 1. we get:

$$(\delta\sigma_1 t_2,\delta\sigma_2 t_2')\in(\!|\delta\mathrm{int}_r[I']|\!)^{E}_{G',k'} \tag{8}$$

Unfold (8), since $k_2 \le k'$,we know

$$(n, n') \in (\!|\text{int}_r[I']|\!)_{G',k'-k_2} \Rightarrow n = n' = I' \wedge c_1' - c_2' \le D_2 \tag{f}$$

Let us assume:

$$G' = G' \tag{g}$$

STS1: $(H_1, H_2) \vDash_{G',k'-k''} P \star \gamma \to \beta$
By Lemma 7 and (1),this is proved.

STS2: $(v, v') \in (\!|\Box\tau|\!)_{G',k'-k''}$
from (c),(d). we know $H_1(l)[n] = v$ and $H_2(l')[n'] = v'$
based on (e) and (f), we know
Unfold (1), we know:
$\forall i \le n, (H_1(l)(i), H_2(l')(i)) \in (\!|\tau|\!)_{G',k'-1}$
s.t we know
$(H_1(l)[n], H_2(l')[n']) \in (\!|\tau|\!)_{G',k'-1}$
Because $k' - k'' \le k' - 1$,
By Lemma 1, We get: $(v, v') \in (\!|\tau|\!)_{G',k'-k''}$,consider the premise $i \notin \beta$, we know $v = v'$, so that we prove $(v, v') \in (\!|\Box\tau|\!)_{G',k'-k''}$.

STS3: $c - c' \le D_1 + D_2$, which is proved by (e),(f).

This completes the proof of case read-box.

$$\text{CASE}\ \frac{\begin{array}{c}\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \text{int}[I'] \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_3 \ominus t_3' \lesssim D_3 : \tau \qquad \Delta;\Phi \models I' \le I \qquad \Sigma;\Delta \vdash P \quad wf\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{updt}\ t_1\ t_2\ t_3 \ominus \mathsf{updt}\ t_1'\ t_2'\ t_3' \lesssim 0 : \{P \star \gamma \to \beta\}\ \exists\_ : \text{unit}_r\ \{P \star \gamma \to \beta \cup \{I'\}\}}^{\text{diff}(D_1+D_2+D_3)}\ \text{R-U}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \Phi\delta$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(\mathsf{updt}\ t_1\ t_2\ t_3), \delta\sigma_2(\mathsf{updt}\ t_1'\ t_2'\ t_3')) \in (\!|\{\gamma \to \beta\}\ \exists\_.\text{unit}\ \{\gamma \to \beta \cup \{I'\}\}|\!)^{E,0}_{G,k}$ $^{\text{diff}(D_1+D_2)}$
Because $\mathsf{updt}\ t_1\ t_2\ t_3$ is value.
STS: $(\delta\sigma_1(\mathsf{updt}\ t_1\ t_2\ t_3), \delta\sigma_2(\mathsf{updt}\ t_1'\ t_2'\ t_3')) \in (\!|\{\gamma \to \beta\}\ \exists\_.\text{unit}\ \{\gamma \to \beta \cup \{I'\}\}|\!)_{G,k}$ $^{\text{diff}(D_1+D_2)}$
Unfold the definition of $(\!|\{\gamma \to \beta\}\ \exists\_.\text{unit}\ \{\gamma \to \beta \cup \{I'\}\}|\!)_{G,k}$ $^{\text{diff}(D_1+D_2)}$.
Pick $G^{'} \supseteq G$, H_1, H_2,$k' \le k$, $k'' < k'$, k'''.
Assume

$$\begin{aligned}(H_1, H_2) \vDash_{G',k'} P \star \gamma \to \beta \wedge H_1 = H_{p1} \uplus H_{l1} \wedge H_{l1} = l \to [v, \ldots, v] \\ \wedge H_2 = H_{p2} \uplus H_{l2} \wedge H_{l2} = l' \to [v', \ldots, v'] \qquad (1)\\ \delta\sigma_1(\mathsf{updt}\ t_1\ t_2\ t_3); H_1 \Downarrow_f^{k''} \qquad (2)\\ \delta\sigma_2(\mathsf{updt}\ t_1'\ t_2'\ t_3'); H_2 \Downarrow_f^{k'''} \qquad (3)\end{aligned}$$

Because t_1, t_2, t_3 are sub terms of $\mathsf{updt}\ t_1\ t_2\ t_3$, t_1', t_2', t_3' are sub terms of $\mathsf{updt}\ t_1'\ t_2'\ t_3'$
From (2)(3), we get

$$\delta\sigma_1 t_1 \Downarrow_f^{k_1} \wedge \delta\sigma_1 t_2 \Downarrow_f^{k_2} \wedge \delta\sigma_1 t_3 \Downarrow_f^{k_3} \tag{4}$$

$$\delta\sigma_2 t_1' \Downarrow_f^{k_1'} \wedge \delta\sigma_2 t_2' \Downarrow_f^{k_2'} \wedge \delta\sigma_2 t_3' \Downarrow_f^{k_3'} \tag{5}$$

From (4),(5), we get:

$$\exists l, n, v, k_1, k_2, k_3. \delta\sigma_1 t_1 \Downarrow^{k_1, c_1} l \wedge \delta\sigma_1 t_2 \Downarrow^{k_2, c_1'} n \wedge \delta\sigma_1 t_3 \Downarrow^{k_3, c_1''} v \wedge$$
$$k'' = k_1 + k_2 + k_3 + 1 \wedge c = c_1 + c_1' + c_1'' + c_{update} \quad \text{(a)}$$

$$\exists l', n', v', k_1', k_2', k_3'. \delta\sigma_2 t_1' \Downarrow^{k_1', c_2} l' \wedge \delta\sigma_2 t_2' \Downarrow^{k_2', c_2'} n' \wedge \delta\sigma_2 t_3' \Downarrow^{k_3', c_2''} v' \wedge c' = c_2 + c_2' + c_2'' + c_{update} \quad \text{(b)}$$

From evaluation rule: E-Update-F and (a)(b), we know:

$$\mathsf{updt}\ t_1\ t_2\ t_3; H_1 \Downarrow^{k'', c} (); H_1(l)[n] \leftarrow v \quad \text{(c)}$$

$$\mathsf{updt}\ t_1'\ t_2'\ t_3'; H_2 \Downarrow^{k''', c'} (); H_2(l')[n'] \leftarrow v' \quad \text{(d)}$$

By IH on first premise instantiated with $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G', k'}$ by lemma 1. We get:

$$(\delta\sigma_1 t_1, \delta\sigma_2 t_1') \in (\!|\mathsf{Array}_\gamma[I]\ \delta\tau|\!)^{E, D_1}_{G', k'} \quad (6)$$

Similarly, By IH on the second premise and third premise, we get

$$(\delta\sigma_1 t_2, \delta\sigma_2 t_2') \in (\!|\mathsf{int}_r[I]|\!)^{E, D_2}_{G', k'} \quad (7)$$

$$(\delta\sigma_1 t_3, \delta\sigma_2 t_3') \in (\!|\tau|\!)^{E, D_3}_{G', k'} \quad (8)$$

From (6),(7),(8), we know:

$$(l, l') \in (\!|\mathsf{Array}_\gamma[I]\ \tau|\!)_{G', k'-k_1} \Rightarrow G'(\gamma) = (l, l', \tau, I) \wedge c_1 - c_2 \leq D_1 \quad \text{(e)}$$

$$(n, n') \in (\!|\mathsf{int}_r[I]|\!)_{G, k'-k_2} \Rightarrow n = n' = I \wedge c_1' - c_2' \leq D_2 \quad \text{(f)}$$

$$(v, v') \in (\!|\tau|\!)_{G', k'-k_3} \wedge c_1'' - c_2'' \leq D_3 \quad \text{(g)}$$

Let us assume:

$$G'' = G' \quad (9)$$

$$H_1' = H_1(l)[n] \leftarrow v \wedge H_2' = H_2(l')[n'] \leftarrow v' \quad (10)$$

STS1: $(H_1', H_2') \vDash_{G', k'-k''} P \star \gamma \rightarrow \beta \cup \{I'\}$
Unfold (1) and consider (e), we know

$$\forall i \leq I. (H_{l1}(l)[i], H_{l2}(l')[i]) \in (\!|\tau|\!)_{G', k'-1} \quad (11)$$

$$\forall i \leq I. (H_{l1}(l)[i] \neq H_{l2}(l')[i]) \Rightarrow i \in \beta \quad (12)$$

Since (e), we need to prove two sub cases.

subgoal 1: $\forall i \leq I. (H_{l1}'(l)[i], H_{l2}'(l')[i]) \in (\!|\tau|\!)_{G', k'-k''}$
when i=n,
we prove $(H_{l1}'(l)[i], H_{l2}'(l')[i]) \in (\!|\tau|\!)_{G', k'-k_3}$ from (g) and (10), and then use lemma 1.
when $i \neq n$,
proved by using lemma 1 on (11)

subgoal 2: $\forall i \leq I. (H_{l1}'(l)[i] \neq H_{l2}'(l')[i]) \Rightarrow i \in \beta \cup \{I'\}$
when i=n,
$n \in \{I'\}$ from (f) $\Rightarrow n \in \beta \cup \{I'\}$
when $i \neq n$,
proved by using lemma 1 on (12)

STS2: $((), ()) \in (\!|\mathsf{unit}_r|\!)_{G', k'-k''}$
It is proved by unfolding the definition.

STS3 $c - c' \le D_1 + D_2 + D_3$.
It is proved by (e),(f),(g).

This completes the proof of case update.

$$\text{CASE}\ \frac{\begin{array}{c}\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \qquad \Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \\ \Delta;\Phi;\Gamma \vdash t_3 \ominus t_3' \lesssim D_3 : \square\tau \qquad \Delta;\Phi \models I' \le I \qquad \Sigma;\Delta \vdash P \quad wf\end{array}}{\Delta;\Phi;\Gamma \vdash \mathsf{updt}\ t_1\ t_2\ t_3 \ominus \mathsf{updt}\ t_1'\ t_2'\ t_3' \lesssim 0 : \{P \star \gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(D_1+D_2+D_3)}{\mathrm{unit}_r}\ \{P \star \gamma \to \beta \setminus \{I'\}\}}\ \text{R-UB}$$

Assume that $\vdash \delta : \Delta$ and $\models \Phi\delta$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(\mathsf{updt}\ t_1\ t_2\ t_3), \delta\sigma_2(\mathsf{updt}\ t_1'\ t_2'\ t_3')) \in (\!|\{P \star \gamma \to \beta\}\ \overset{\mathrm{diff}(D_1+D_2+D_3)}{\exists\_.\mathrm{unit}}\ \{P \star \gamma \to \beta \setminus \{I'\}\}|\!)^{E,0}_{G,k}$
Because $\mathsf{updt}\ t_1\ t_2\ t_3$ is value.
STS: $(\delta\sigma_1(\mathsf{updt}\ t_1\ t_2\ t_3), \delta\sigma_2(\mathsf{updt}\ t_1'\ t_2'\ t_3')) \in (\!|\{P \star \gamma \to \beta\}\ \overset{\mathrm{diff}(D_1+D_2+D_3)}{\exists\_.\mathrm{unit}}\ \{P \star \gamma \to \beta / \{I'\}\}|\!)_{G,k}$
Unfold the definition of $(\!|\{P \star \gamma \to \beta\}\ \overset{\mathrm{diff}(D_1+D_2+D_3)}{\exists\_.\mathrm{unit}}\ \{P \star \gamma \to \beta \setminus \{I'\}\}|\!)_{G,k}$.
Pick $G' \supseteq G$, H_1, H_2, $k' \le k$, $k'' < k'$, k'''.
Assume

$$\begin{aligned}(H_1, H_2) \vDash_{G',k'} P \star \gamma \to \beta \wedge H_1 = H_{p1} \uplus H_{l1} \wedge H_{l1} = l \to [v, \ldots, v] \\ \wedge H_2 = H_{p2} \uplus H_{l2} \wedge H_{l2} = l' \to [v', \ldots, v'] \qquad (1)\\ \delta\sigma_1(\mathsf{updt}\ t_1\ t_2\ t_3); H_1 \Downarrow_f^{k''} \qquad (2)\\ \delta\sigma_2(\mathsf{updt}\ t_1'\ t_2'\ t_3'); H_2 \Downarrow_f^{k'''} \qquad (3)\end{aligned}$$

Because t_1, t_2, t_3 are sub terms of $\mathsf{updt}\ t_1\ t_2\ t_3$, t_1', t_2', t_3' are sub terms of $\mathsf{updt}\ t_1'\ t_2'\ t_3'$
From (2)(3), we get

$$\delta\sigma_1 t_1 \Downarrow_f^{k_1} \wedge \delta\sigma_1 t_2 \Downarrow_f^{k_2} \wedge \delta\sigma_1 t_3 \Downarrow_f^{k_3} \qquad (4)$$

$$\delta\sigma_2 t_1' \Downarrow_f^{k_1'} \wedge \delta\sigma_2 t_2' \Downarrow_f^{k_2'} \wedge \delta\sigma_2 t_3' \Downarrow_f^{k_3'} \qquad (5)$$

From (4),(5), we get:

$$\begin{aligned}\exists l, n, v, k_1, k_2, k_3. \delta\sigma_1 t_1 \Downarrow^{k_1, c_1} l \wedge \delta\sigma_1 t_2 \Downarrow^{k_2, c_1'} n \wedge \delta\sigma_1 t_3 \Downarrow^{k_3, c_1''} v \wedge \\ k'' = k_1 + k_2 + k_3 + 1 \wedge c = c_1 + c_1' + c_1'' + c_{update} \qquad (a)\\ \exists l', n', v', k_1', k_2', k_3'. \delta\sigma_2 t_1' \Downarrow^{k_1', c_2} l' \wedge \delta\sigma_2 t_2' \Downarrow^{k_2', c_2'} n' \wedge \delta\sigma_2 t_3' \Downarrow^{k_3', c_2''} v' \wedge c' = c_2 + c_2' + c_2'' + c_{update} \qquad (b)\end{aligned}$$

From evaluation rule: E-Update-F and (a)(b), we know:

$$\mathsf{updt}\ t_1\ t_2\ t_3; H_1 \Downarrow^{k'', c} (); H_1(l)[n] \leftarrow v \qquad (c)$$

$$\mathsf{updt}\ t_1'\ t_2'\ t_3'; H_2 \Downarrow^{k''', c'} (); H_2(l')[n'] \leftarrow v' \qquad (d)$$

By IH on first premise instantiated with $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G',k'}$ by lemma 1. We get:

$$(\delta\sigma_1 t_1, \delta\sigma_2 t_1') \in (\!|\mathsf{Array}_\gamma[I]\ \delta\tau|\!)^{E,D_1}_{G',k'} \qquad (6)$$

Similarly, By IH on the second premise and third premise, we get

$$(\delta\sigma_1 t_2, \delta\sigma_2 t_2') \in (\!|\delta\mathrm{int}_r[I]|\!)^{E,D_2}_{G',k'} \qquad (7)$$

$$(\delta\sigma_1 t_3, \delta\sigma_2 t_3') \in (\!|\square\delta\tau|\!)^{E,D_3}_{G',k'} \qquad (8)$$

From (6),(7),(8), we know:

$$(l,l') \in (\!|\mathsf{Array}_\gamma[I]\ \tau|\!)_{G',k'-k_1} \Rightarrow G'(\gamma) = (l,l',\tau,I) \wedge c_1 - c_2 \leq D_1 \quad \text{(e)}$$

$$(n,n') \in (\!|\mathsf{int}_r[I]|\!)_{G,k'-k_2} \Rightarrow n = n' = I \wedge c_1' - c_2' \leq D_2 \quad \text{(f)}$$

$$v = v' \wedge (v,v') \in (\!|\tau|\!)_{G',k'-k_3}\, c_1'' - c_2'' \leq D_3 \quad \text{(g)}$$

Let us assume:

$$G'' = G' \quad (9)$$

$$H_1' = H_1(l)[n] \leftarrow v \wedge H_2' = H_2(l')[n'] \leftarrow v' \quad (10)$$

STS1: $(H_1', H_2') \vDash_{G',k'-k''} P \star \gamma \rightarrow \beta/\{I'\}$
Unfold (1) and consider (e), we know

$$\forall i \leq I.(H_{l1}(l)[i], H_{l2}(l')[i]) \in (\!|\delta\tau|\!)_{G',k'-1} \quad (11)$$

$$\forall i \leq I.(H_{l1}(l)[i] \neq H_{l2}(l')[i]) \Rightarrow i \in \beta \quad (12)$$

Since (e), we need to prove two sub cases.

subgoal 1: $\forall i \leq I.(H'_{l1}(l)[i], H'_{l2}(l')[i]) \in (\!|\tau|\!)_{G',k'-k''}$
when i=n,
we prove $(H'_{l1}(l)[i], H'_{l2}(l')[i]) \in (\!|\tau|\!)_{G',k'-k_3}$ from (g) and (10), and then use lemma 1.
when $i \neq n$,
proved by using lemma 1 on (11)

subgoal 2: $\forall i \leq I.(H'_{l1}(l)[i] \neq H'_{l2}(l')[i]) \Rightarrow i \in \beta/\{I'\}$
when i=n,
$H_1'(l)[i] = H_2'(l)[i]$, it is trivially proved. when $i \neq n$,
proved by using lemma 1 on (12)

STS2: $(0,0) \in (\!|\mathsf{unit}_r|\!)_{G',k'-k''}$
It is proved by unfolding the definition.

STS3 $c - c' \leq D_1 + D_2 + D_3$.
It is proved by (e),(f),(g).

This completes the proof of case update-box.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{return}\ t_1 \ominus \mathsf{return}\ t_2 \lesssim 0 : \{P\}\ \overset{\mathrm{diff}(D)}{\exists\_.\tau}\ \{P\}}\ \text{R-T}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \Phi\delta$ and $(\sigma_1,\sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(\mathsf{return}\ t_1), \delta\sigma_2(\mathsf{return}\ t_2)) \in (\!|\{P\}\ \overset{\mathrm{diff}(D)}{\exists\_.\tau}\ \{P\}|\!)^{E,0}_{G,k}$
Because return t is value,
STS: $(\delta\sigma_1(\mathsf{return}\ t_1), \delta\sigma_2(\mathsf{return}\ t_2)) \in (\!|\{P\}\ \overset{\mathrm{diff}(D)}{\exists\_.\tau}\ \{P\}|\!)_{G,k}$
Unfold the definition of $(\!|\{P\}\ \overset{\mathrm{diff}(D)}{\exists\_.\tau}\ \{P\}|\!)_{G,k}$.
Pick $G^{'} \supseteq G$, H_1, H_2,$k' \leq k, k'' < k', k'''$.
Assume

$$(H_1,H_2) \vDash_{G',k'} P \quad (1)$$

$$\delta\sigma_1(\mathsf{return}\ t_1); H_1 \Downarrow_f^{k''} \quad (2)$$

$$\delta\sigma_2(\mathsf{return}\ t_2); H_2 \Downarrow_f^{k'''} \quad (3)$$

Because t_1 is the subterm of return t_1 , From (2)(3), We know:

$$\delta\sigma_1 t_1 \Downarrow^{k_1} \tag{4}$$

$$\delta\sigma_2 t_2 \Downarrow_f^{k'''} \tag{5}$$

From (4),(5), we know:

$$\exists v_1, k_1, \delta\sigma_1 t_1 \Downarrow^{k_1, c_1} v_1 \wedge k'' = k_1 + 1 \wedge c = c_1 + c_{ret} \tag{a}$$

$$\exists v_2, k_1', \delta\sigma_2 t_2 \Downarrow^{k_1', c_2} v_2 \wedge k''' = k_1' + 1 \wedge c' = c_2 + c_{ret} \tag{b}$$

From (a),(b) and the evaluation rule R-ret:

$$H_1; \mathsf{return}\ t_1 \Downarrow_f^{k'', c} v_1; H_1 \tag{c}$$

$$H_2; \mathsf{return}\ t_2 \Downarrow_f^{k''', c'} v_2; H_2 \tag{d}$$

By IH on the premise instantiated with $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G',k'}$ by lemma 1. We get:

$$(\delta\sigma_1 t_1, \delta\sigma_2 t_2) \in (\!|\delta\tau|\!)_{G',k'}^{E,D} \tag{6}$$

Unfold (6), we get:

$$(v_1, v_2) \in (\!|\delta\tau|\!)_{G',k'-k_1} \tag{7}$$

Let us assume:

$$G'' = G' \tag{8}$$

$$H_1' = H_1' \wedge H_2' = H_2' \leftarrow v' \tag{9}$$

STS1: $(H_1', H_2') \vDash_{G',k'-k''} P$
it is trivially true.

STS2: $(v_1, v_2) \in (\!|\tau|\!)_{G',k'-k''}$
It is proved by (7) using Lemma 1.

STS3: $c - c' \le D$ which is proved from (a),(b)

This completes the proof of case r-ret.

$$\text{CASE}\ \frac{\begin{array}{c} P = P_1 \star P_2 \qquad \Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D_1 : \{P_1\}\ \exists \vec{\gamma}_1.\tau_1^{\mathrm{diff}(D)}\ \{Q_1 \star Q_2\} \\ \Delta, \vec{\gamma}_1 : \vec{\mathbb{L}}; \Phi; \Gamma, x : \tau_1 \vdash t_1' \ominus t_2' \lesssim D_2 : \{Q_1 \star P_2\}\ \exists \vec{\gamma}_2.\tau_2^{\mathrm{diff}(D')}\ \{Q\} \end{array}}{\Delta;\Phi;\Gamma \vdash \mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_1' \ominus \mathsf{let}\ \{x\} = t_2\ \mathsf{in}\ t_2' \lesssim 0 : \{P\}\ \exists \vec{\gamma}_1 \vec{\gamma}_2 : \tau_2^{\mathrm{diff}(D_1+D_2+D+D')}\ \{Q \star Q_2\}}\ \text{R-LET}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$

TS: $(\delta\sigma_1(\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_1'), \delta\sigma_2(\mathsf{let}\ \{x\} = t_2\ \mathsf{in}\ t_2')) \in (\!|\delta\ \{P\}\ \exists \vec{\gamma}_1 \vec{\gamma}_2 : \tau_2^{\mathrm{diff}(D+D')}\ \{Q \star Q_2\}|\!)_{G,k}^{E,(D_1+D_2)}$
Because $\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_1'$ is value.

STS: $(\delta\sigma_1(\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_1'), \delta\sigma_2(\mathsf{let}\ \{x\} = t_2\ \mathsf{in}\ t_2')) \in (\!|\delta\ \{P\}\ \exists \vec{\gamma}_1 \vec{\gamma}_2 : \tau_2^{\mathrm{diff}(D+D')}\ \{Q \star Q_2\}|\!)_{G,k}$
Unfold the definition of $(\!|\delta\ \{P\}\ \exists \vec{\gamma}_1 \vec{\gamma}_2 : \tau_2^{\mathrm{diff}(D+D')}\ \{Q \star Q_2\}|\!)_{G,k}$.
Pick $G^{'} \supseteq G$, H_1, H_2,$k' \le k, k'' < k', k'''$.
Assume

$$(H_1, H_2) \vDash_{G',k'} P \tag{1}$$

$$\delta\sigma_1(\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_1'); H_1 \Downarrow_f^{k''} \tag{2}$$

$$\delta\sigma_2(\mathsf{let}\ \{x\} = t_2\ \mathsf{in}\ t_2'); H_2 \Downarrow_f^{k'''} \tag{3}$$

Because t_1 is the subterm of let $\{x\} = t_1$ in t_1' , From (2) ,we know:

$$\exists v_1, v_1', v_1'', v_1''', k_1, k_2, k_3, k_4, H_1', H_1''.\delta\sigma_1 t_1 \Downarrow^{k_1,c_1} v_1 \wedge v_1; H_1 \Downarrow_f^{k_2,c_1'} v_1'; H_1'$$
$$\delta\sigma_1 t_1'[v_1'/x] \Downarrow^{k_3,c_3} v_1'' \wedge v_1''; H_1' \Downarrow_f^{k_4,c_4} v_1'''; H_1'' \wedge k'' = k_1 + k_2 + k_3 + k_4 + 1 \wedge c = c_1 + c_2 + c_3 + c_4 + c_{let} \quad \text{(a)}$$

Similarly, from (3) , we get:

$$\exists v_2, v_2', v_2'', v_2''', k_1', k_2', k_3', k_4', H_2', H_2''. \quad \delta\sigma_1 t_2 \Downarrow^{k_1',c_2} v_2 \quad \text{and} \quad v_2; H_2 \Downarrow_f^{k_2',c_2'} v_2'; H_2' \quad \text{and}$$
$$\delta\sigma_1 t_2'[v_2'/x] \Downarrow^{k_3',c_2''} v_2'' \quad \text{and} \quad v_2''; H_2' \Downarrow_f^{k_4',c_2'''} v_2'''; H_2'' \wedge k'' = k_1' + k_2' + k_3' + k_4' + 1 \wedge c' = c_2 + c_2' + c_2'' + c_2''' + c_{let} \quad \text{(b)}$$

From evaluation rule: E-Let-F and (a)(b), we know:

$$\exists H_a, H_c, H_a', H1_{Q1}, H1_{Q2}, H1_Q, s.t. H_1 = H_a \uplus H_c \wedge v1; H_a \Downarrow_f v_1'; H_a' \wedge H_a' = H1_{Q1} \uplus H1_{Q2}$$
$$\wedge v_1''; H1_{Q1} \uplus H_c \Downarrow_f v_1'''; H1_Q \wedge H_1'' = H1_Q \uplus H1_{Q2} \quad \text{(c)}$$
$$\exists H_a, H_c, H_a', H1_{Q1}, H1_{Q2}, H1_Q, s.t. H_1 = H_a \uplus H_c \wedge v1; H_a \Downarrow_f v_1'; H_a' \wedge H_a' = H1_{Q1} \uplus H1_{Q2}$$
$$\wedge v_1''; H1_{Q1} \uplus H_c \Downarrow_f v_1'''; H1_Q \wedge H_1'' = H1_Q \uplus H1_{Q2} \quad \text{(d)}$$

From (1) : $(H_1, H_2) \vDash_{G',k'} P_1 \star P_2$, we assume that

$$\exists G_a, G_b : (H_1 = H_a \uplus H_c) \quad \text{and} \quad (H_2 = H_b \uplus H_d)$$
$$(G' = G_a \uplus G_c) \quad \text{and} \quad (H_a, H_b) \vDash_{G_a,k'} P_1 \quad \text{and} \quad (H_c, H_d) \vDash_{G_c,k'} P_2 \quad (*)$$

STS1: $(H_1'', H_2'') \vDash_{G'',k'-k''} Q \star Q_2$
STS2: $(v_1''', v_2''') \in (\!|\tau_2|\!)_{G'',k'-k''}$
STS3: $c - c' \leq (D_1 + D_2 + D + D')$

By IH on the second premise instantiated with $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G',k'}$, we know:

$$(\delta\sigma_1 t_1, \delta\sigma_2 t_2) \in (\!|\{P_1\} \exists\vec{\gamma_1}.\tau \overset{\text{diff}(D)}{\{Q_1 \star Q_2\}}|\!)_{G',k'}^{E,D_1} \quad (4)$$

Unfold the definition of $(\!|\{P_1\} \exists\vec{\gamma_1}.\tau \overset{\text{diff}(D)}{\{Q_1 \star Q_2\}}|\!)_{G',k'}^{E,D_1}$,use (a), we get:

$$(v_1, v_2) \in (\!|\{P_1\} \exists\vec{\gamma_1}.\tau_1 \overset{\text{diff}(D)}{\{Q_1 \star Q_2\}}|\!)_{G',k'-k_1} \wedge c_1 - c_2 \leq D_1 \quad (e)$$

To unfold (e), we choose: $k_f \leq k' - k_1$ and $k_f' < k_f$ and $G_f \supseteq G'$ and $H_a \uplus H_c$,$H_b \uplus H_d$ and (1),(a),(b).
We have

$$(H_a, H_b) \vDash_{G_f,k_f} P_1 \wedge v_1; H_a \Downarrow_f \wedge v_2; H_b \Downarrow_f$$

Unfold the definition, we get:

$$v_1; H_a \Downarrow_f^{c_1'} v_1'; H_a' \wedge v_2; H_b \Downarrow_f^{c_2'} v_2'; H_b' \wedge H_a', H_b' \vDash Q_1 \star Q_2$$

$$(v_1', v_2') \in (\!|\tau_1|\!)_{G',k'-k_1} \wedge c_1' - c_2' \leq D \quad (k)$$

By IH on the third premise, we know:

$$(\delta\sigma_1 v_1'', \delta\sigma_2 v_2'') \in (\!|\{Q_1 \star P_2\} \exists\vec{\gamma_1}.\tau \overset{\text{diff}(D')}{\{Q\}}|\!)_{G',k'}^{E,D_2} \quad (5)$$

Unfold the definition of $(\!|\{Q_1 \star P_2\} \exists\vec{\gamma_1}.\tau_2 \overset{\text{diff}(D)}{\{Q\}}|\!)_{G',k'}^{E,D_2}$,use (a), we get:

$$(v_1, v_2) \in (\!|\{Q_1 \star P_2\} \exists\vec{\gamma_1}.\tau_2 \overset{\text{diff}(D')}{\{Q\}}|\!)_{G',k'-k_1} \wedge c_1'' - c_2'' \leq D_2 \quad (f)$$

We have

$$(H'_a, H'_b) \vDash_{G_f, k_f} Q_1 \star Q_2 \Rightarrow H1_{Q1}, H2_{Q1} \vDash Q_1 \wedge H1_{Q2}, H2_{Q2} \vDash Q_2 \wedge H_c, H_d \vDash P_2$$

$$H1_{Q1} \uplus H_c; v_1''' \Downarrow_f \wedge H2_{Q1} \uplus H_d; v_2''' \Downarrow_f$$

Unfold the definition (f), we get:

$$H1_{Q1} \uplus H_c; v_1''' \Downarrow_f^{c_1'''} H1_Q; v_1'''' \wedge H2_{Q1} \uplus H_d; v_2''' \Downarrow_f^{c_2'''} H2_Q; v_2''' \wedge H1_Q, H2_Q \vDash Q$$

$$(v_1''', v_2''') \in (\!|\tau_2|\!)_{G', k'-k_1} \wedge c_1''' - c_2''' \leq D' \tag{g}$$

STS1: Use Lemma 2, we know that $H1_Q \uplus H1_{Q2}, H2_Q \uplus H2_{Q2} \vDash Q \star Q_2$, which proves the
STS2: it is proved from (g).
STS3: it is proved from (e),(k),(f),(g).

This completes the proof of let case.

$$\text{CASE}\ \frac{\Delta; \Phi; |\Gamma|_1 \vdash_{L_1}^{U_1} t_1 : A_1 \qquad \Delta; \Phi; |\Gamma|_2 \vdash_{L_2}^{U_2} t_2 : A_2}{\Delta; \Phi; \Gamma \vdash t_1 \ominus t_2 \lesssim U_1 - L_2 : U(A_1, A_2)}\ \text{R-S}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(t_1), \delta\sigma_2(t_2)) \in (\!|\delta U(A_1, A_2)|\!)^{E,(\delta(U_1-L_2)}_{G,k,\delta(U_1-L_2)}$
Unfold the definition.
Assume:

(a) $\delta\sigma_1 t_1 \Downarrow^{k_1, c} v_1$

(b) $\delta\sigma_2 t_2 \Downarrow^{k_2, c'} v_2$

(c) $k_1 < k$

TS 1: $(v_1, v_2) \in (\!|U(\delta A_1, \delta A_2)|\!)_{G, k-k_1}$
TS 2: $c - c' \leq U_1 - L_2$
We prove TS 1 first.
Unfold its definition,
STS: $\forall k'. v_1 \in (\!|\delta A_1|\!)_{G|_1, k'}$ and $v_2 \in (\!|\delta A_2|\!)_{G|_2, k'}$
Pick k'.
By IH 2 on the first premise using

1. $FV(t_1) \subseteq dom(\delta|\Gamma|_1)$ using Lemma 5.
2. $\vDash \delta\Phi$
3. $\forall k. \sigma_1 \in (\!|\delta|\Gamma|_1|\!)_{G|_1, k}$

We get:

$$\forall k. \delta\sigma_1 t_1 \in [\![\delta A_1]\!]^{E,(\delta L_1, \delta U_1)}_{G|_1, k} \tag{1}$$

Unfold the definition of (1), choose $k = k_1 + k'$. we know

$$v_1 \in [\![\delta A_1]\!]_{G|_1, k'} \wedge \delta L_1 \leq c \leq \delta U_1 \tag{a}$$

By IH 2 on the second premise using

1. $FV(t_2) \subseteq dom(\delta|\Gamma|_2)$ using Lemma 5.

2. $\vDash \delta\Phi$

3. $\forall k.\sigma_2 \in (\!|\delta|\Gamma|_2|\!)_{G|_2,k}$

We get:

$$\forall k.\delta\sigma_2\, t_2 \in [\![\delta A_2]\!]^{E,(\delta L_2,\delta U_2)}_{G|_2,k} \tag{2}$$

Unfold the definition of (1), choose $k = k_2 + k'$. we know

$$v_2 \in [\![\delta A_2]\!]_{G|_2,k'} \wedge \delta L_2 \le c' \le \delta U_2 \tag{b}$$

(a),(b) finished the proof of STS1.
(a),(b) finished the proof of STS2.

This completes the proof of switch case.

$$\text{CASE}\ \frac{\Delta;\Phi;|\Gamma|_1 \vdash^{U_1}_{L_1} t_1 : A_1 \xrightarrow{\text{exec}(L,U)} A_2 \qquad \Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : U(A_1, A_2')}{\Delta;\Phi;\Gamma \vdash t_1\ t_2 \ominus t_2' \lesssim U_1 + U + D_2 + c_{app} : U(A_2, A_2')}\ \text{R-APP-E}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(t_1\ t_2), \delta\sigma_2(t_2')) \in (\!|\delta U(A_2, A_2')|\!)^{E,\delta(U_1+U+D_2+c_{app})}_{G,k}$.
Following the definition of $(\!|\delta U(A_2, A_2')|\!)^{E,\delta(U_1+U+D_2+c_{app})}_{G,k}$, assume that:

$$\frac{\delta\sigma_1 t_1 \Downarrow^{c_1,k_1} \text{fix} f\, x.t' \ (\star) \qquad \delta\sigma_1 t_2 \Downarrow^{c_2,k_2} v_2 \ (\diamond) \qquad t'[\text{fix} f\, x.t'/f][v_2/x] \Downarrow^{c_3,k_3} v_r \ (\spadesuit)}{(\delta\sigma_1 t_1)(\delta\sigma_1 t_2) \Downarrow^{c_1+c_2+c_3+c_{\text{app}},k_1+k_2+k_3+1} v_r}\ \text{E-F}$$

and $\delta\sigma_2(t_2') \Downarrow^{c',k'} v'$ $(\diamond\diamond)$ and $k_1 + k_2 + k_3 + 1 < k$.
TS1: $c_1 + c_2 + c_3 + c_{\text{app}} - c' \le \delta(U_1 + U + D_2 + c_{app})$
TS2: $(v_r, v') \in (\!|\delta U(A_2, A_2')|\!)_{G,k-(k_1+k_2+k_3+1)}$.
Frist show the second statement.
By unrolling the definition of $(\!|\delta U(A_2, A_2')|\!)_{G,k-(k_1+k_2+k_3+1)}$,
STS: $\forall j.v_r \in [\![\delta A_2]\!]_{|G|_1,j} \wedge v' \in [\![\delta A_2']\!]_{|G|_2,j}$.
Pick j.
By IH 2 on the first premise using

1. $FV(t_1) \subseteq dom(\delta|\Gamma|_1)$ using Lemma 5.

2. $\vDash \delta\Phi$

3. $\forall k.\sigma_1 \in (\!|\delta|\Gamma|_1|\!)_{G|_1,k}$

we get

$$\forall k.\delta\sigma_1 t_1 \in [\![\delta(A_1 \xrightarrow{\text{exec}(L,U)} A_2)]\!]^{E,(\delta L_1,\delta U_1)}_{G|_1,k} \ (1)$$

Instantiating (1) with $X = j + k_1 + k_3 + 1$, we get

$$\delta\sigma_1 t_1 \in [\![\delta(A_1 \xrightarrow{\text{exec}(L,U)} A_2)]\!]^{E,(\delta L_1,\delta U_1)}_{G|_1,X} \ (2)$$

Following the definition, we get:
$\delta\sigma_1 t_1 \Downarrow^{c_1,k_1} \text{fix} f\, x.t'$ and $\text{fix} f\, x.t' \in [\![\delta(A_1 \xrightarrow{\text{exec}(L,U)} A_2)]\!]_{G|_1,X-k_1}$ (a) and $\delta L_1 < c_1 < \delta U_1$ (e).
By IH on the second premise, we get:

$$(\delta\sigma_1 t_2, \delta\sigma_2 t_2') \in (\!|\delta U(A_1, A_2')|\!)^{E,\delta(D_2)}_{G,k}$$

Unfold the defintion, by ($\diamond$) and ($\diamond\diamond$), we get :
$c_2 - c' \le \delta D_2$ (f) and $(v_2, v') \in (\!|\delta U(A_1, A_2')|\!)_{G,k-k_2}$ (b)

From (b), we know : $\forall k. v_2 \in [\![\delta A_1]\!]_{G|_1,k} \wedge v' \in [\![\delta A_2]\!]_{G|_2,k}$.
Instantiate k with $X - k_1 - 1$, we get:

$$v_2 \in [\![\delta A_1]\!]_{G|_1,X-k_1-1} \ (3)$$

$$v' \in [\![\delta A_2]\!]_{G|_2,X-k_1-1} \ (4)$$

Unfold (a), we get:

$$t'[\text{fix} f\ x.t'/f][v_2/x] \in [\![\delta A_2]\!]^{E,\delta(L,U)}_{G|_1,X-k_1-1} \ (c)$$

Unfold (c) using ($\spadesuit$), we get :

$$v_r \in [\![\delta A_2]\!]_{G|_1,X-k_1-k_3-1} \ (h)$$

$$\delta L \le c_3 \le \delta U \ (g)$$

STS1 is proved by $(e), (f), (g)$.
STS2 is proved by (h) and (3) using Lemma 1.

$$\text{CASE}\ \frac{\Delta;\Phi;|\Gamma|_2 \vdash^{U_1}_{L_1} t_1' : A_1' \overset{\text{exec}(L,U)}{\longrightarrow} A_2' \qquad \Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : U(A_2, A_1')}{\Delta;\Phi;\Gamma \vdash t_2 \ominus t_1'\ t_2' \lesssim D_2 - L_1 - L - c_{app} : U(A_2, A_2')}\ \text{R-E-APP}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(t_2), \delta\sigma_2(t_1'\ t_2')) \in (\!|\delta U(A_2, A_2')|\!)^{E,\delta(D_2-L_1-L-c_{app})}_{G,k}$.
Following the definition of $(\!|\delta U(A_2, A_2')|\!)^{E,\delta(D_2-L_1-L-c_{app})}_{G,k}$, assume that:

$$\frac{\delta\sigma_2 t_1' \Downarrow^{c_1',k_1'} \text{fix} f\ x.t' \ (\star) \qquad \delta\sigma_2 t_2' \Downarrow^{c_2',k_2'} v_2' \ (\diamond) \qquad t'[\text{fix} f\ x.t'/f][v_2'/x] \Downarrow^{c_3',k_3'} v_r' \ (\spadesuit)}{(\delta\sigma_2 t_1')\,(\delta\sigma_2 t_2') \Downarrow^{c_1'+c_2'+c_3'+c_{\text{app}},k_1'+k_2'+k_3'+1} v_r'}\ \text{E-F}$$

and $\delta\sigma_1 t_2 \Downarrow^{c_1,k_1} v_r$ $(\diamond\diamond)$ and $k_1 < k$.

TS1: $c_1 - (c_1' + c_2' + c_3' + c_{\text{app}}) \le \delta(D_2 - U_1 - U - c_{app})$

TS2: $(v_r, v_r') \in (\!|\delta U(A_2, A_2')|\!)_{G,k-k_1}$.
Frist show the second statement.
By unrolling the definition of $(\!|\delta U(A_2, A_2')|\!)_{G,k-k_1}$,
STS: $\forall j. v_r \in [\![\delta A_2]\!]_{|G|_1,j} \wedge v_r' \in [\![\delta A_2']\!]_{|G|_2,j}$.
Pick j.
By IH 2 on the first premise using

1. $FV(t_1') \subseteq dom(\delta|\Gamma|_2)$ using Lemma 5.
2. $\vDash \delta\Phi$
3. $\forall k. \sigma_2 \in (\!|\delta|\Gamma|_2|\!)_{G|_2,k}$

we get

$$\forall k. \delta\sigma_2 t_1' \in [\![\delta(A_1' \overset{\text{exec}(L,U)}{\longrightarrow} A_2')]\!]^{E,(\delta L_1,\delta U_1)}_{G|_2,k} \ (1)$$

Instantiating (1) with $X = j + k_1' + k_3' + 1$, we get

$$\delta\sigma_2 t_1' \in [\![\delta(A_1' \overset{\text{exec}(L,U)}{\longrightarrow} A_2')]\!]^{E,(\delta L_1,\delta U_1)}_{G|_2,X} \ (2)$$

Following the definition, we get:
$\delta\sigma_2 t_1' \Downarrow^{c_1',k_1'} \text{fix}\, f\, x.t'$ and $\text{fix}\, f\, x.t' \in [\![\delta(A_1' \xrightarrow{\text{exec}(L,U)} A_2')]\!]_{G|_2,X-k_1'}$ (a) and $\delta L_1 < c_1' < \delta U_1$ (e).
By IH on the second premise, we get:

$$(\delta\sigma_1 t_2, \delta\sigma_2 t_2') \in (\!|\delta U(A_2, A_1')|\!)^{E,\delta(D_2)}_{G,k}$$

Unfold the defintion, by $(\diamond)$ and $(\diamond\diamond)$, we get :
$c_1 - c_2' \le \delta D_2$ (f) and $(v_r, v_2') \in (\!|\delta U(A_2, A_1')|\!)_{G,k-k_1}$ (b)
From (b), we know : $\forall k. v_r \in [\![\delta A_2]\!]_{G|_1,k} \wedge v_2' \in [\![\delta A_1']\!]_{G|_2,k}$.
Instantiate k with $X - k_1' - 1$, we get:

$$v_r \in [\![\delta A_2]\!]_{G|_1,X-k_1'-1} \ (3)$$

$$v_2' \in [\![\delta A_1']\!]_{G|_2,X-k_1'-1} \ (4)$$

Unfold (a), we get:

$$t'[\text{fix}\, f\, x.t'/f][v_2'/x] \in [\![\delta A_2']\!]^{E,\delta(L,U)}_{G|_2,X-k_1'-1} \ (c)$$

Unfold (c) using $(\spadesuit)$, we get :

$$v_r' \in [\![\delta A_2']\!]_{G|_2,X-k_1'-k_3'-1} \ (h)$$

$$\delta L \le c_3' \le \delta U \ (g)$$

STS1 is proved by $(e), (f), (g)$.
STS2 is proved by (h) and (4) using Lemma 1.

$$\frac{\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash^{U_1}_{L_1} t_1 : A_1 \qquad \Sigma;\Delta;\Phi;\Gamma, x : U(A_1,A_1) \vdash t_2 \ominus t_2' \lesssim D_2 : \tau}{\Sigma;\Delta;\Phi;\Gamma \vdash \text{let } x = t_1 \text{ in } t_2 \ominus t_2' \lesssim U_1 + D_2 + c_{lt} : \tau}\ \text{R-LT-E}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(\text{let } x = t_1 \text{ in } t_2), \delta\sigma_2(t_2')) \in (\!|\delta\tau|\!)^{E,\delta(D_2+U_1+c_{lt})}_{G,k}$.
Following the definition of $(\!|\delta\tau|\!)^{E,\delta(D_2+U_1+c_{lt})}_{G,k}$, assume that:

$$\frac{\delta\sigma_1 t_1 \Downarrow^{c_1,k_1} v_1 \ (\star) \qquad \delta\sigma_1 t_2[v_1/x] \Downarrow^{c_r,k_r} v_r \ (\spadesuit)}{\text{let } x = \delta\sigma_1 t_1 \text{ in } \delta\sigma_1 t_2 \Downarrow^{c_1+c_r+c_{\text{lt}},k_1+k_r+1} v_r}\ \text{E-LET}$$

and $\delta\sigma_2 t_2' \Downarrow^{c',k'} v' \ (\diamond\diamond)$.

STS1: $(v_r, v') \in (\!|\delta\tau|\!)_{G,k-(k_1+k_r+1)}$.

STS2: $c_1 + c_r + c_{lt} - c' \le \delta(D_2 + U_1 + c_{lt}$.
To prove :

$$\forall k. v_1 \in [\![\delta A_1]\!]_{|G|_1,k}$$

Proof. Pick k. IH2 on the first premise.

1. $FV(t_1) \subseteq |\delta\Gamma|_1$ using Lemma 5.
2. $\sigma_1 \in (\!||\delta\Gamma|_1|\!)_{|G|_1,k+\delta U_1+1}$ by Lemma 6 using assumptions.

We get: $\sigma_1 t_1 \in [\![\delta A_1]\!]^{E,(\delta L_1,\delta U_1)}_{|G|_1,k+\delta U_1+1}$.
Unfold the defintion, we know: $\delta L_1 \le c_1 \le \delta U_1$ (a) and $v_1 \in [\![\delta A_1]\!]_{|G|_1,k+\delta u_1+1-c_1}$.
So, we know: $v_1 \in [\![\delta A_1]\!]_{|G|_1,k}$ by Lemma 1. ∎

IH on the second premise using

1. $(\sigma_1[v_1/x], \sigma_2[v_1/x]) \in (\!|\delta\Gamma, x : U(\delta A_1, \delta A_1)|\!)_{G,k}$ using

   1.1. $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$

   1.2. $(v_1, v_1) \in (\!|U(\delta A_1, \delta A_1)|\!)_{G,k}$

we get:

$$(\delta\sigma_1[v_1/x]t_2, \delta\sigma_2[v_1/x]t_2') \in (\!|\delta\tau|\!)_{G,k}^{E,\delta D_2}$$

Since x does not occur free in t_2', we have : $(\delta\sigma_1[v_1/x]t_2, \delta\sigma_2 t_2') \in (\!|\delta\tau|\!)_{G,k}^{E,\delta D_2}$.

Unfold the defintion, we have:

$$c_r - c_1' \leq \delta D_2 \ (b)$$

$$(v_r, v') \in (\!|\delta\tau|\!)_{G,k-k_r} \ (c)$$

STS1 is proved by using Lemma 1 on (c) because $k - (k_1 + k_r + 1) < k - k_r$.
STS2 is proved by (a) and (b).

This completes the proof of case R-lt-e.

$$\text{CASE}\ \frac{\begin{array}{c}\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_1}^{U_1} t : A_1 + A_2 \\ \Sigma;\Delta;\Phi;\Gamma, x : U(A_1, A_1) \vdash t_1 \ominus t' \lesssim D_2 : \tau \qquad \Sigma;\Delta;\Phi;\Gamma, y : U(A_2, A_2) \vdash t_2 \ominus t' \lesssim D_2 : \tau\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \text{ case } (t, x.t_1, y.t_2) \ominus t' \lesssim U_1 + D_2 + c_{case} : \tau}\ \text{R-CASE-E}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(\text{ case } (t, x.t_1, y.t_2)), \delta\sigma_2(t')) \in (\!|\delta\tau|\!)_{G,k}^{E,\delta(D_2+U_1+c_{case})}$.
Following the definition of $(\!|\delta\tau|\!)_{G,k}^{E,\delta(D_2+U_1+c_{case})}$, assume that:
$\delta\sigma_1$ case $(t, x.t_1, y.t_2) \Downarrow^{C,K} v_r$ and $\delta\sigma_2 t' \Downarrow^{c',k'} v'$ $(\diamond\diamond)$ and $C < k$.
STS1: $(v_r, v') \in (\!|\delta\tau|\!)_{G,k-K}$.

STS2: $C - c' \leq \delta(D_2 + U_1 + c_{case}$.

To prove :

$$\forall k. v_1 \in [\![\delta A_1]\!]_{|G|_1,k}$$

Depending on what $\delta\sigma_1 t$ evaluates to, there are two cases.

Subcase1:

$$\frac{\delta\sigma_1 t \Downarrow^{c_1,k_1} \text{inl} v_1 \ (\star) \qquad \delta\sigma_1 t_1[v_1/x] \Downarrow^{c_r,k_r} v_r \ (\spadesuit)}{\delta\sigma_1 \text{ case } (t, x.t_1, y.t_2) \Downarrow^{c_1+c_r+c_{\text{case}},k_1+k_r+1} v_r}\ \text{CASE-INL}$$

To prove: $\forall k.(\text{inl} v_1) \in (\!|\delta A_1 + \delta A_2|\!)_{G,k}$.

Proof. Pick k. IH2 on the first premise.

1. $FV(t) \subseteq |\delta\Gamma|_1$ using Lemma 5.
2. $\sigma_1 \in (\!|\delta\Gamma|_1|\!)_{|G|_1,k+\delta U_1+1}$ by Lemma 6 using assumptions.

We get: $\sigma_1 t \in [\![\delta A_1 + \delta A_2]\!]_{|G|_1,k+\delta U_1+1}^{E,(\delta L_1,\delta U_1)}$.
Unfold the defintion, we know: $\delta\sigma_1 t \Downarrow^{c_1,k_1} \text{inl} v_1$ and $\delta L_1 \leq c_1 \leq \delta U_1$ (a) and $\text{inl} v_1 \in [\![\delta A_1 + \delta A_2]\!]_{|G|_1,k+\delta u_1+1-c_1}$.
So, we know: $\text{inl} v_1 \in [\![\delta A_1 + \delta A_2]\!]_{|G|_1,k}$ by Lemma 1. ■

IH on the second premise using

1. $(\sigma_1[v_1/x], \sigma_2[v_1/x]) \in (\!|\delta\Gamma, x : U(\delta A_1, \delta A_1)|\!)_{G,k}$ using
   1.1. $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
   1.2. $(v_1, v_1) \in (\!|U(\delta A_1, \delta A_1)|\!)_{G,k}$

we get:

$$(\delta\sigma_1[v_1/x]t_1, \delta\sigma_2[v_1/x]t') \in (\!|\delta\tau|\!)^{E,\delta D_2}_{G,k}$$

Since x does not occur free in t', we have : $(\delta\sigma_1[v_1/x]t_1, \delta\sigma_2 t') \in (\!|\delta\tau|\!)^{E,\delta D_2}_{G,k}$.
Unfold its defintion, we get:

$$c_r - c_1' \leq \delta D_2 \ (b)$$
$$(v_r, v') \in (\!|\delta\tau|\!)_{G,k-k_r} \ (c)$$

STS1 is proved by using Lemma 1 on (c) because $k - (k_1 + k_r + 1) < k - k_r$.
STS2 is proved by (a) and (b).

Subcase 2:

$$\frac{\delta\sigma_1 t \Downarrow^{c_1,k_1} \mathsf{inr}\, v_1 \ (\star) \qquad \delta\sigma_1 t_2[v_1/x] \Downarrow^{c_r,k_r} v_r \ (\spadesuit)}{\delta\sigma_1 \ \mathsf{case}\ (t, x.t_1, y.t_2) \Downarrow^{c_1+c_r+c_{\mathsf{case}},k_1+k_r+1} v_r} \ \text{CASE-INR}$$

Prove similarily : $\forall k.(\mathsf{inr}\, v_1) \in (\!|\delta A_1 + \delta A_2|\!)_{G,k}$.
IH on the third premise using

1. $(\sigma_1[v_1/x], \sigma_2[v_1/x]) \in (\!|\delta\Gamma, x : U(\delta A_1, \delta A_1)|\!)_{G,k}$ using
   1.1. $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
   1.2. $(v_1, v_1) \in (\!|U(\delta A_1, \delta A_1)|\!)_{G,k}$

we get:

$$(\delta\sigma_1[v_1/x]t_2, \delta\sigma_2[v_1/x]t') \in (\!|\delta\tau|\!)^{E,\delta D_2}_{G,k}$$

Since x does not occur free in t', we have : $(\delta\sigma_1[v_1/x]t_2, \delta\sigma_2 t') \in (\!|\delta\tau|\!)^{E,\delta D_2}_{G,k}$.
Unfold its defintion, we get:

$$c_r - c_1' \leq \delta D_2 \ (b)$$
$$(v_r, v') \in (\!|\delta\tau|\!)_{G,k-k_r} \ (c)$$

STS1 is proved by using Lemma 1 on (c) because $k - (k_1 + k_r + 1) < k - k_r$.
STS2 is proved by (a) and (b).

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;|\Gamma|_1 \vdash^{U_1}_{L_1} t_1 : \{P_1\}\ \overset{\mathrm{exec}(L,U)}{\exists\vec{\gamma}_1 : A_1}\ \{Q_1\} \qquad \Sigma;\Delta;\Phi;|\Gamma|_2 \vdash^{U_2}_{L_2} t_2' : \{P_2\}\ \overset{\mathrm{exec}(L',U')}{\exists\vec{\gamma}_1 : A_1'}\ \{Q_2\}}{\Sigma;\Delta;\Phi;\Gamma, x : U(A_1, A_1) \vdash t_2 \ominus t_2' \lesssim D_2 : \{P \sqcup P_1\}\ \overset{\mathrm{diff}(D')}{\exists\vec{\gamma}_1}.\tau\ \{Q\} \qquad dom(P) = dom(P_1)}\ \text{R-LET-E}$$
$$\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2 \ominus t_2' \lesssim -L_2 : \overset{\mathrm{diff}(U_1+U+(D_2+U_2)+D'+c_{let})}{\{P\}\ \exists\vec{\gamma}_1.\tau\ \{Q\}}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2), \delta\sigma_2(t_2')) \in (\!|\delta(\overset{\mathrm{diff}(-L_2)}{\{P\}\ \exists\vec{\gamma}_1.\tau\ \{Q\}})|\!)^{E,\delta(U_1+U+(D_2+U_2)+D'+c_{let})}_{G,k}$.
Assume

$$\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2 \Downarrow^{0,0} \mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2$$

and $\delta\sigma_2 t_2' \Downarrow^{c_1',k_1'} v_1'$.
Unfold the definition, STS1: $0 - c_1' \le -(\delta L_2)$
By IH2 on the second premise, we get: $\delta L_2 \le c_1' \le \delta U_2$, which proves STS1.
STS2: $(\delta\sigma_1(\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2), v_1') \in (\!|\delta(\ \overset{\mathrm{diff}(U_1+U+(D_2+U_2)+D'+c_{let})}{\{P\}\ \exists\vec{\gamma}_1.\tau\ \{Q\}}\ )|\!)_{G,k}$.
Unfold its defintion, assume : $G \supseteq G, k' < k, k_2 < k'.H_1, H_1' \vDash_{G,k'} P$ and

$$\mathsf{let}\ \{x\} = \delta\sigma_1 t_1\ \mathsf{in}\ \delta\sigma_1 t_2; H_1 \Downarrow_f^{c_2,k_2} v_{let}; H_2 \ (a)$$

and

$$v_1'; H_1' \Downarrow_f^{c_2',k_2'} v_2'; H_2' \ (b)$$

STS1:

$$(H_2, H_2') \vDash_{G,k'-k_2} Q$$

STS2:

$$(v_{let}, v_2') \in (\!|\delta\tau|\!)_{G,k'-k_2}$$

STS3:

$$c_2 - c_2' \le \delta((D_2 + U_2) + D' + U + U_1 + c_{let})$$

IH2 on the first premise, we get: $\delta\sigma_1 t_1 \in (\!|\delta(\{P_1\}\ \overset{\mathrm{exec}(L,U)}{\exists\vec{\gamma}_1 : A_1}\ \{Q_1\})|\!)^{E,\delta(L_1,U_1)}_{|G|_1,k}$ (c).
Unfold (c), we assume $\delta\sigma_1 t_1 \Downarrow^{c_a,k_a} v$, we get : $v \in (\!|\delta(\{P_1\}\ \overset{\mathrm{exec}(L,U)}{\exists\vec{\gamma}_1 : A_1}\ \{Q_1\})|\!)_{|G|_1,k-k_a}$ (d) and $\delta L_1 \le c_a \le \delta U_1$ (e).
Unfold (d), pick $k_1 \le k - k_a$. assume $H_1 \vDash_{|G|_1,k_1} P_1$,
we know: $v; H_1 \Downarrow_f^{c_3,k_3} v_2; H_3$ and $H_3 \vDash_{|G|_1,k_1-k_3} Q_1$ and $v_a \in (\!|A|\!)_{|G|_1,k_1-k_3} \wedge \delta L \le c_3 \le \delta U$ (f)
and $\exists n.P_1 = \{\gamma_1 \to T_1, \ldots \gamma_n \to T_n\} \wedge \forall i \in [1,n].|G|_1(\gamma_i) = (l_i, A, m) \implies \forall j.H_1[l_i][j] \neq H_3[l_i][j] \implies j \in T_i$ (z).
From (f), we know : $(\sigma_1[v_a/x], \sigma_2[v_a/x]) \in (\!|\delta(\Gamma, x : U(A,A))|\!)_{G,k}$ (h).

IH on the third premise instantiated with (h), we get:

$$(\delta\sigma_1[v_a/x](t_2), \delta\sigma_2[v_a/x](t_2')) \in (\!|\delta(\{P \sqcup P_1\}\ \overset{\mathrm{diff}(D')}{\exists\vec{\gamma}_1.\tau}\ \{Q\})|\!)^{E,\delta(D_2)}_{G,k}\ (i)$$

Unfold (i), assume : $\delta\sigma_1[v_a/x]\, t_2 \Downarrow^{c_4,k_4} v_4$ and $\delta\sigma_2[v_a/x]\, t_2' \Downarrow^{c_1',k_1'} v_1'$.
we get: $(v_4, v_1') \in (\!|\delta(\{P \sqcup P_1\}\ \overset{\mathrm{diff}(D')}{\exists\vec{\gamma}_1.\tau}\ \{Q\})|\!)_{G,k}$ (j) and $c_4 - c_1' \le \delta D_2$ (k).
Unfold (j), we assume :Pick $k_6 = k' - ka - k_3 - k_4 - 1 \le k - k_4$.
We first show the conclusion: $(H_3, H_1') \vDash_{G,k_6} P \sqcup P_1$ (♣) .

Proof. We have the assuption (z) and the assumption $H_1, H_1' \vDash_{G,k} P$.
Unfold (♣), we need to prove :
$\forall\gamma \in dom(P) \cup dom(P_1).\exists l_1, l_2, \tau, n.G(\gamma) = (l_1, l_2, \tau, n) \wedge \forall i < n.H_3[\gamma][i] \neq H_1'[\gamma][i] \implies i \in (P \sqcup P_1)[\gamma]$. $(\star)$
Unfold the definition of $H_1, H_1' \vDash_{G,k} P$, we know:
$\forall\gamma \in dom(P).\exists l_1, l_2, \tau, n.G(\gamma) = (l_1, l_2, \tau, n) \wedge \forall i < n.H_1[\gamma][i] \neq H_1'[\gamma][i] \implies i \in (P)[\gamma]$. $(\heartsuit)$
From the premise $dom(P) = dom(P_1)$, there is only one case:

1. $\gamma \in dom(P), \gamma \in dom(P_1)$
   From $(\heartsuit)$, we know
   $\forall\gamma \in dom(P) \cap dom(P_1).\exists l_1, l_2, \tau, n.G(\gamma) = (l_1, l_2, \tau, n) \wedge \forall i < n.H_1[\gamma][i] \neq H_1'[\gamma][i] \implies i \in (P)[\gamma]$,
   which means H_1 and H_1' differ at most at indices in $P[\gamma]$, also means $\forall i < n.i \notin P[\gamma] \implies H_1[\gamma][i] = H_1'[\gamma][i]$.
   From (z), we also know that $\forall\gamma \in dom(P_1), \forall i < n.H_1[\gamma][i] \neq H_3[\gamma][i] \implies i \in P_1[\gamma]$, which means H_1 and H_3 differ at most at all the indices in $P_1[\gamma]$.

So we know H_3 and H_1' differ at most at indices appear in P or P_1, which is $\forall \gamma \in (dom(P) \cap dom(P_1)).\exists l_1, l_2, \tau, n. G(\gamma) = (l_1, l_2, \tau, n) \wedge \forall i < n. H_1[\gamma][i] \neq H_1'[\gamma][i] \implies i \in P[\gamma] \vee i \in P_1[\gamma]$.
This subcase is proved because $i \in P[\gamma] \vee i \in P_1[\gamma] \implies i \in P[\gamma] \cup P_1[\gamma] \implies (P \sqcup P_1)[\gamma]$.

□

Also assume $v_4; H_3 \Downarrow_f^{c_5,k_5} v_5; H_2$ and $v_1'; H_1' \Downarrow_f^{c_2',k_2'} v_2'; H_2'$.
We get: $H_2, H_2' \vDash_{G,k_6-k_5} Q\ (l)$ and $(v_5, v_2') \in (\!|\delta\tau|\!)_{G,k_6-k_5}\ (m)$ and $c_5 - c_2' \leq \delta D'\ (n)$

From the forcing evaluation rule

$$\frac{\delta t_1 \Downarrow^{c_a,k_a} v \qquad v; H_1 \Downarrow_f^{c_3,k_3} v_a; H_3 \qquad t_2[v_a/x] \Downarrow^{c_4,k_4} v_4 \qquad v_4; H_3 \Downarrow_f^{c_5,k_5} v_5; H_2}{\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_2; H_1 \Downarrow_f^{c_a+c_3+c_4+c_5+c_{\mathrm{let}},k_a+k_3+k_4+k_5+1} v_5; H_2}\ \text{F-E}$$

STS1 is proved by (l).
STS2 is proved by (m) using Lemma 1.
STS3 : $c_2 - c_2' = c_a + c_3 + c_4 + c_5 + c_{\mathrm{let}} - c_2' \leq \delta(U + U_1 + D' + (D_2 + U_2) + c_{\mathrm{let}})$ by (e),(k),(n), (f).

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;|\Gamma|_2 \vdash_{L_1}^{U_1} t_1' : \{P_1\}\ \overset{\mathrm{exec}(L,U)}{\exists \vec{\gamma}_1 : A_1'}\ \{Q_1\} \qquad \Sigma;\Delta;\Phi;|\Gamma|_1 \vdash_{L_2}^{U_2} t_2 : \{P_2\}\ \overset{\mathrm{exec}(L',U')}{\exists \vec{\gamma}_1 : A_1}\ \{Q_2\}}{\Sigma;\Delta;\Phi;\Gamma, x : U(A_1', A_1') \vdash t_2 \ominus t_2' \lesssim D_2 : \{P \sqcup P_1\}\ \overset{\mathrm{diff}(D')}{\exists \vec{\gamma}_1.\tau'}\ \{Q\} \qquad dom(P) = dom(P_1)}\ \text{R-E-LET}$$
$$\Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus \mathsf{let}\ \{x\} = t_1'\ \mathsf{in}\ t_2' \lesssim U_2 : \quad \overset{\mathrm{diff}(D'+(D_2-L_2)-L_1-L-c_{\mathrm{let}})}{\{P\}\ \exists \vec{\gamma}_1.\tau'\ \{Q\}}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and $(\sigma_1, \sigma_2) \in (\!|\delta\Gamma|\!)_{G,k}$
TS: $(\delta\sigma_1(t_2), \delta\sigma_2(\mathsf{let}\ \{x\} = t_1'\ \mathsf{in}\ t_2')) \in (\!|\delta(\ \overset{\mathrm{diff}(D'+(D_2-L_2)-L_1-L-c_{\mathrm{let}})}{\{P\}\ \exists \vec{\gamma}_1.\tau'\ \{Q\}}\ )|\!)_{G,k}^{E,\delta(U_2)}$.
Assume

$$\delta\sigma_2(\mathsf{let}\ \{x\} = t_1'\ \mathsf{in}\ t_2') \Downarrow^{0,0} \mathsf{let}\ \{x\} = \delta\sigma_2 t_1'\ \mathsf{in}\ \delta\sigma_2 t_2'$$

and $\delta\sigma_1 t_2 \Downarrow^{c_1,k_1} v_1$.
Unfold the definition, STS1: $c_1 - 0 \leq \delta U_2$.
By IH2 on the second premise, we get: $\delta L_2 \leq c_1 \leq \delta U_2$, which proves STS1.

STS2: $(v_1, \delta\sigma_2(\mathsf{let}\ \{x\} = t_1'\ \mathsf{in}\ t_2')) \in (\!|\delta(\ \overset{\mathrm{diff}(D'+(D_2-L_2)-L_1-L-c_{\mathrm{let}})}{\{P\}\ \exists \vec{\gamma}_1.\tau\ \{Q\}}\ )|\!)_{G,k}$.
Unfold its defintion, assume : $G \supseteq G, k' < k, k_2 < k'. H_1, H_1' \vDash_{G,k'} P$ and

$$\mathsf{let}\ \{x\} = \delta\sigma_2 t_1'\ \mathsf{in}\ \delta\sigma_2 t_2'; H_1' \Downarrow_f^{c_2',k_2'} v'_{let}; H_2'\ (a)$$

and

$$v_1; H_1 \Downarrow_f^{c_2,k_2} v_2; H_2\ (b)$$

STS1:

$$(H_2, H_2') \vDash_{G,k'-k_2} Q$$

STS2:

$$(v_2, v'_{let}) \in (\!|\delta\tau|\!)_{G,k'-k_2}$$

STS3:

$$c_2 - c_2' \leq \delta(D' + (D_2 - L_2) - L_1 - L - c_{\mathrm{let}})$$

IH2 on the first premise, we get: $\delta\sigma_2 t_1' \in (\!|\delta(\{P_1\}\ \overset{\mathrm{exec}(L,U)}{\exists \vec{\gamma}_1 : A_1'}\ \{Q_1\})|\!)_{|G|_2,k}^{E,\delta(L_1,U_1)}\ (c)$.
Unfold (c), we assume $\delta\sigma_1 t_1' \Downarrow^{c_a',k_a'} v'$, we get : $v' \in (\!|\delta(\{P_1\}\ \overset{\mathrm{exec}(L,U)}{\exists \vec{\gamma}_1 : A_1'}\ \{Q_1\})|\!)_{|G|_2,k-k_a'}\ (d)$ and $\delta L_1 \leq c_a' \leq$

δU_1 (e).
Unfold (d), assume : pick $k_1 \le k - k'_a$. $H'_1 \vDash_{|G|_2,k_1} P_1$ and $v'; H'_1 \Downarrow_f^{c'_3,k'_3} v'_a; H'_3$ and $H'_3 \vDash_{|G|_2,k_1-k'_3} Q_1$ and $v'_a \in (\!|A'_1|\!)_{|G|_2,k_1-k'_3} \wedge \delta L \le c'_3 \le \delta U$ (f).
From (f), we know : $(\sigma_1[v'_a/x], \sigma_2[v'_a/x]) \in (\!|\delta(\Gamma, x : U(A'_1, A'_1))|\!)_{G,k}$ (h).

IH on the third premise instantiated with (h), we get:

$$(\delta\sigma_1[v'_a/x](t_2), \delta\sigma_2[v'_a/x](t'_2)) \in (\!|\delta(\{P \cup P_1\}\ \exists \overset{\text{diff}(D')}{\vec{\gamma}_1}.\tau'\ \{Q\})|\!)^{E,\delta(D_2)}_{G,k}\ (i)$$

. Unfold (i), assume : $\delta\sigma_1[v'_a/x]\, t_2 \Downarrow^{c_1,k_1} v_1$ and $\delta\sigma_2[v'_a/x]\, t'_2 \Downarrow^{c'_4,k'_4} v'_4$.
we get: $(v_1, v'_4) \in (\!|\delta(\{P \cup P_1\}\ \exists \overset{\text{diff}(D')}{\vec{\gamma}_1}.\tau'\ \{Q\})|\!)_{G,k}$ (j) and $c_1 - c'_4 \le \delta D_2$ (k).
Unfold (j), we assume :Pick $k_6 = k' - k_4 - 1 \le k - k'_4$..
We prove $(H_1, H'_3) \vDash_{G,k_6} P \sqcup P_1$ in a similar way in the previous case.
Also assume $v'_4; H'_3 \Downarrow_f^{c'_5,k'_5} v'_5; H'_2$ and $v_1; H_1 \Downarrow_f^{c_2,k_2} v_2; H_2$.
We get: $H_2, H'_2 \vDash_{G,k_6-k_5} Q$ (l) and $(v_2, v'_5) \in (\!|\delta\tau'|\!)_{G,k_6-k_5}$ (m) and $c_2 - c'_5 \le \delta D'$ (n)

From the forcing evaluation rule

$$\frac{\delta t'_1 \Downarrow^{c'_a,k'_a} v' \qquad v'; H'_1 \Downarrow_f^{c'_3,k'_3} v'_a; H'_3 \qquad t'_2[v'_a/x] \Downarrow^{c'_4,k'_4} v'_4 \qquad v'_4; H'_3 \Downarrow_f^{c'_5,k'_5} v'_5; H'_2}{\mathsf{let}\ \{x\} = t'_1\ \mathsf{in}\ t'_2; H'_1 \Downarrow_f^{c'_a+c'_3+c'_4+c'_5+c_{\mathsf{let}},k'_a+k'_3+k'_4+k'_5+1} v'_5; H'_2}\ \text{F-E}$$

STS1 is proved by (l).
STS2 is proved by (m) using Lemma 1.
STS3 : $c_2 - c'_2 = c_2 - c'_a - c'_3 - c'_4 - c'_5 - c_{\mathsf{let}} \le \delta(D' + (D_2 - L_2) - L_1 - L - c_{\mathsf{let}})$ by (e),(k),(n), (f).

Proof of statement (2) if $\Delta;\Phi;\Omega \vdash_L^U t : A$ and $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and there exists Ω'. s.t. $FV(t) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$ and $(\sigma) \in (\!|\delta\Omega'|\!)_{g,k}$. Then, $(\delta\sigma\, t) \in (\!|A|\!)_{g,k}^{E,(\delta L,\delta U)}$
Proof by induction on typing derivation:

$$\text{CASE}\ \frac{\xi;\Delta;\Phi;x : A, f : \overset{\text{exec}(L,U)}{A \longrightarrow} B, \Omega \vdash_L^U t : B}{\Delta;\Phi;\Omega \vdash_0^0 \text{fix}\, f(x).t : \overset{\text{exec}(L,U)}{A \longrightarrow} B}\ \text{U-F}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and there exists Ω'. s.t. $FV(t) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$ and $(\sigma) \in (\!|\delta\Omega'|\!)_{g,k}$
TS: $(\delta\sigma \text{fix}\, f(x).t) \in [\![\delta\ \overset{\text{exec}(L,U)}{A \longrightarrow} B]\!]_{g,k}^{E,(0,0)}$
Because fix $f(x).e$ is value.
STS: $(\delta\sigma \text{fix}\, f(x).t) \in [\![\delta\ \overset{\text{exec}(L,U)}{A \longrightarrow} B]\!]_{g,k}$
We prove the more general statement

$$\forall k' \leq k.\delta\sigma(\text{fix}\, f(x).t) \in [\![\delta A \overset{\text{exec}(L,U)}{\longrightarrow} \delta B]\!]_{g,k} \tag{1}$$

by sub-induction on k'. There are two cases:

subcase 1: k'=0
there is no non-negative k such that k ≤ 0, the goal is vacuously true.

subcase 2: $k' = k'' + 1 \leq k$
By sub-IH, we know:

$$\delta\sigma(\text{fix}\, f(x).t) \in [\![\delta A \overset{\text{exec}(L,U)}{\longrightarrow} \delta B]\!]_{g,k''} \tag{2}$$

STS: $(\text{fix}\, f(x).\delta\sigma e) \in [\![\delta A \overset{\text{exec}(L,U)}{\longrightarrow} \delta B]\!]_{g,k''+1}$
Pick j < k"+1 and assume that $v \in [\![\delta A]\!]_{g,j}$
STS: $\sigma[v/x][\text{fix}\, f(x).e/f]) \in [\![\delta B]\!]_{g,j}^{E,(\delta L,\delta U)}$
This follows by IH on the premise instantiated with

1. FV(e) $\subseteq dom(x : A, f : \overset{\text{exec}(L,U)}{A \longrightarrow} B, \Omega')$ from Lemma (well-formness) and $(x : A, f : \overset{\text{exec}(L,U)}{A \longrightarrow} B, \Omega') \subseteq (x : A, f : \overset{\text{exec}(L,U)}{A \longrightarrow} B, \Omega)$
2. $(\sigma[v/x][\text{fix}\, f(x).t/f]) \in [\![\delta(x : A, f : \overset{\text{exec}(L,U)}{A \longrightarrow} B, \Omega')]\!]_{g,j}$ which holds because
   2.1. $\sigma \in [\![\delta\Omega']\!]_{g,j}$ by Lemma downward closure and $j < k'' + 1 \leq k$
   2.2. $v \in [\![A]\!]_{g,j}$ from assumption
   2.3. $(\delta\sigma \text{fix}\, f(x).e) \in [\![\delta A \overset{\text{exec}(L,U)}{\longrightarrow} \delta B]\!]_{g,j}$ from Lemma 1 on (2).

This completes the proof of unary fix case.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;\Omega \vdash_{L_1}^{U_1} t_1 : \text{int}[I] \qquad \Sigma;\Delta;\Phi;\Omega \vdash_{L_2}^{U_2} t_2 : A \qquad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash_0^0 \text{alloc}\, t_1\, t_2 : \{P\}\ \exists\gamma : \text{Array}_\gamma[I]\ A\ \{P \star \gamma \to \mathbb{N}\}}\ \text{U-ALLOC}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and there exists Ω'. s.t. $FV(t) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$ and $(\sigma) \in (\!|\delta\Omega'|\!)_{g,k}$
TS: $(\delta\sigma\ \text{alloc}\, t_1\, t_2) \in [\![\{P\}\ \exists\gamma : \text{Array}_\gamma[I]\ A\ \{P\gamma \to \mathbb{N}\}]\!]_{g,k}^{E,(0,0)}$
Because alloc $t_1\ t_2$ is value.
STS: $(\delta\sigma\ \text{alloc}\, t_1\, t_2) \in [\![\{P\}\ \exists\gamma : \text{Array}_\gamma[I]\ A\ \{P\gamma \to \mathbb{N}\}]\!]_{g,k}$

Unfold the definition of $[\![\{P\}\ \exists\gamma : \mathsf{Array}_\gamma[I]\ A\ \{P\gamma \to \mathbb{N}\}]\!]^{\mathrm{exec}(L_1+L_2+L_a, U_1+U_2+U_a)}_{g,k}$.
Pick $g' \supseteq g$, $k' \le k$, $k'' < k'$ and H.
Assume $H \vDash_{g',k'} P$ and $H; \mathsf{alloc}\ t_1\ t_2 \Downarrow^{k''}$
From $H; \mathsf{alloc}\ t_1\ t_2 \downarrow^{k''}$, because t_1, t_2 are sub terms of $\delta\sigma\ \mathsf{alloc}\ t_1\ t_2$,we get

$$\delta\sigma\, t_1 \Downarrow^{k_1}_f \wedge \delta\sigma\, t_2 \Downarrow^{k_2}_f \tag{1}$$

From (1) , we get:

$$\exists v_1, v_2, k_1, k_2.\, \delta\sigma\, t_1 \Downarrow^{k_1, c_1} v_1 \wedge \delta\sigma\, t_2 \Downarrow^{k_2, c_1'} v_2 \wedge k'' = k_1 + k_2 + 1 \wedge c = c_1 + c_1' + c_{alloc} \tag{a}$$

From (a) and evaluation rules we get:

$$\exists l.H, (\mathsf{alloc}\ t_1\ t_2)\delta\sigma \Downarrow^{k'', c}_f l; H[l \to [v_2, \ldots v_2] \tag{b}$$

By IH on the first premise instantiated with $\sigma \in [\![\delta\Omega']\!]_{g,k''}$ using lemma 1 and $FV(t_1) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$, we get:

$$(\delta\sigma\, t_1) \in [\![\mathrm{int}_r[I]]\!]^{E,(\delta L_1, \delta U_1)}_{g',k''} \tag{*}$$

Unfold the definition of $[\![\mathrm{int}[I]]\!]^{E,(\delta L_1,\delta U_1)}_{g',k''}$ and using (a) and $k_1 \le k''$, we know:

$$(v_1) \in [\![\mathrm{int}[I]]\!]_{G',k''-k_1} \Rightarrow v_1 = I \wedge \delta L_1 \le c_1 \le \delta U_1 \qquad \text{IH1}$$

By IH on the second premise instantiated with $(\sigma) \in [\![\delta\Gamma]\!]_{g',k'-k_1}$ using lemma 1 and $FV(t_2) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$, we get:

$$(\delta\sigma\, t_2) \in [\![\delta A]\!]^{E,(\delta L_2,\delta U_2)}_{g',k'-k_1} \tag{**}$$

Unfold the definition of (**) and using (a), (b) and $k_2 \le k' - k_1$, we know

$$(v_2) \in [\![\delta A]\!]_{g',k'-k_1-k_2} = [\![\delta A]\!]_{g',k'-k''+1} \wedge \delta L_2 \le c_1' \le \delta U_2 \qquad \text{IH2}$$

Let us assume:

$$g'' = g'[r \to (l, A, I)] \tag{c}$$
$$H' = H, \left[l \to [v_2, v_2, \ldots, v_2]\right] \tag{d}$$

we want to show 4 cases.

TS1 $(l) \in [\![\mathsf{Array}_\gamma[I]\ A]\!]_{g'',k'-k''}$
it is proved by unfolding the definition and using the assumption (c).

TS2 $(H') \vDash_{g'',k'-k''} p \star \gamma \to \mathbb{N}$
we know that $g''(\gamma) = (l, A, I)$, $H' = H \uplus H_l \wedge H_l = l \to [v_2, v_2, \ldots, v_2]$

STS1 $\forall i \le I, (H_l(l)[i] \in [\![A]\!]_{g'',k'-k''-1}$
It is proved by using IH2 and Lemma 1.

TS3 $\delta(L_1 + L_2 + L_a) \le c \le \delta(U_1 + U_2 + U_a)$
It is proved by IH1 and IH2 and $\delta L_a \le c_{alloc} \le \delta U_a$.

TS4 $\exists n.P = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \wedge \forall i \in [1, n].g(\gamma_i) = (l_i, A, m) \Rightarrow \forall j.(H[l_i][j]) \neq H'[l_i][j] \Rightarrow j \in T_i \Big\}$
Because new allocated γ is not in P, so for all the γ_i, it is not changed.

This proof is complete for case alloc.

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t_1 : \mathsf{Array}_\gamma[I]\ A \qquad \Sigma;\Delta;\Phi;\Omega \vdash^{U_2}_{L_2} t_2 : \mathrm{int}[I'] \qquad \vDash I' \leq I \qquad \Sigma;\Delta \vdash P \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash^{0}_{0} \mathsf{read}\ t_1\ t_2 : \overset{\mathrm{exec}(L_1+L_2+L_r,U_1+U_2+U_r)}{\{P\}\ \exists\_ : A\ \{P\}}}\ \text{U-R}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and there exists Ω'. s.t. $FV(t) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$ and $(\sigma) \in (\!|\delta\Omega'|\!)_{g,k}$

TS: $(\delta\sigma\ \mathsf{read}\ t_1\ t_2) \in [\![\overset{\mathrm{exec}(L_1+L_2+L_r,U_1+U_2+U_r)}{\{P\}\ \exists\_ : A\ \{P\}}]\!]^{E,(0,0)}_{g,k}$

Because read $t_1\ t_2$ is value.

STS: $(\delta\sigma\ \mathsf{read}\ t_1\ t_2) \in [\![\overset{\mathrm{exec}(L_1+L_2+L_r,U_1+U_2+U_r)}{\{P\}\ \exists\_ : A\ \{P\}}]\!]_{g,k}$

Unfold the definition of $[\![\overset{\mathrm{exec}(L_1+L_2+L_r,U_1+U_2+U_r)}{\{P\}\ \exists\_ : A\ \{P\}}]\!]_{g,k}$.

Pick $g' \supseteq g$, $k' \leq k$, $k'' < k'$ and H.

Assume $H \vDash_{g',k'} \gamma$ and $H;\mathsf{read}\ t_1\ t_2 \Downarrow^{k''}$

From $H;\mathsf{read}\ t_1\ t_2 \Downarrow^{k''}$, because t_1, t_2 are sub terms of $\delta\sigma$ read $t_1\ t_2$,we get

$$\delta\sigma\, t_1 \Downarrow^{k_1}_f \wedge \delta\sigma\, t_2 \Downarrow^{k_2}_f \tag{1}$$

From (1) , we get:

$$\exists l, n, v, k_1, k_2.\, \delta\sigma\, t_1 \Downarrow^{k_1,c_1} l \wedge \delta\sigma\, t_2 \Downarrow^{k_2,c_1'} n \wedge k'' = k_1 + k_2 + 1 \wedge c = c_1 + c_1' + c_{read} \wedge H(l)[n] = v \tag{a}$$

From (a) and evaluation rules we get:

$$H;\delta\sigma(\mathsf{read}\ t_1\ t_2) \Downarrow^{k'',c}_f H;v \tag{b}$$

By IH on the first premise instantiated with $(\sigma) \in [\![\delta\Omega']\!]_{g',k'}$ by lemma 1 and $FV(t_1) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$. we get:

$$(\delta\sigma\, t_1) \in [\![\mathsf{Array}_\gamma[I]\ A]\!]^{E,\delta(L_1,U_1)}_{g',k'} \tag{6}$$

Unfold (6), since $k_1 \leq k'$ and $\delta\sigma_1\, t_1 \Downarrow^{k_1,c_1} l$, we know

$$l \in [\![\mathsf{Array}_\gamma[I]\ A]\!]_{g',k'-k_1} \wedge \delta L_1 \leq c_1 \leq \delta U_1 \tag{e}$$

From (e), we know :

$$g'(\gamma) = (l, A, I) \tag{7}$$

By IH on the second premise instantiated with $(\sigma) \in [\![\delta\Omega']\!]_{g',k'}$ by lemma 1 and $FV(t_2) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$. we get:

$$(\delta\sigma_1\, t_2') \in [\![\mathrm{int}[I']]\!]^{E,\delta(L_2,U_2)}_{g',k'} \tag{8}$$

Unfold (8), since $k_2 \leq k'$,we know

$$n \in [\![\mathrm{int}[I']]\!]_{g',k'-k_2} \Rightarrow n = I' \wedge \delta L_2 \leq c_1' \leq \delta U_2 \tag{f}$$

Let us assume:

$$g' = g' \tag{g}$$

STS1: $H \vDash_{g',k'-k''} P$

proved by assumption $H \vDash_{g',k'} P$

STS2: $(v) \in [\![A]\!]_{g',k'-k''}$

from (a). we know $H_1(l)[n] = v$

From $H \vDash_{g',k'-k''} \gamma$ we know:

$\forall i \leq n, (H_1(l)(i)) \in [\![A]\!]_{g',k'-1}$

s.t we know

$(H_1(l)[n]) \in [\![A]\!]_{g',k'-1}$

Because $k' - k'' \leq k' - 1$,

By Lemma 1, We get: $(v) \in [\![A]\!]_{g',k'-k''}$

STS3: $\delta(L_1+L_2+L_r) \le c \le \delta(U_1+U_2+U_r)$
by the fact that $\delta L_r \le c_{read} \le \delta U_r$, it is proved by (e)(f).

STS4: $\exists n.P = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \wedge \forall i \in [1,n].g(\gamma_i) = (l_i, A, m) \Rightarrow \forall j.(H[l_i][j]) \neq H'[l_i][j] \Rightarrow j \in T_i$
H is not changed, H=H'. it is trivially true.

This completes the proof of case read.

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash_{L_1}^{U_1} t_1 : \mathsf{Array}[I]\ A \qquad \Sigma;\Delta;\Phi;\Omega \vdash_{L_2}^{U_2} t_2 : \mathrm{int}[I'] \qquad \Sigma;\Delta;\Phi;\Omega \vdash_{L_3}^{U_3} t_3 : A \qquad \Delta;\Phi \vDash I' \le I \qquad \Sigma;\Delta;\vdash P \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash_0^{\mathrm{exec}(L_1+L_2+L_3+L_u, U_1+U_2+U_3+U_u)} \mathsf{updt}\ t_1\ t_2\ t_3 : \{P \star \gamma \to \beta\}\ \exists\_ : \mathrm{unit}\ \{P \star \gamma \to \beta\}}\ \text{U-U}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and there exists Ω'. s.t. $FV(t) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$ and $(\sigma) \in (\!|\delta\Omega'|\!)_{g,k}$
TS: $(\delta\sigma\ \mathsf{updt}\ t_1\ t_2\ t_3) \in [\![\{P \star \gamma \to \beta\}\ \exists\_ : \mathrm{unit}\ \{P \star \gamma \to \beta\}]\!]_{g,k}^{E,(0,0)}$
Because read $t_1\ t_2$ is value.
STS: $(\delta\sigma\ \mathsf{updt}\ t_1\ t_2\ t_3) \in [\![\{P \star \gamma \to \beta\}\ \exists\_ : \mathrm{unit}\ \{P \star \gamma \to \beta\}]\!]_{g,k}^{\mathrm{exec}(L_1+L_2+L_3+L_u, U_1+U_2+U_3+U_u)}$
Unfold the definition of $[\![\{P \star \gamma \to \beta\}\ \exists\_ : \mathrm{unit}\ \{P \star \gamma \to \beta\}]\!]_{g,k}$.
Pick $g' \supseteq g$, $k' \le k$, $k'' < k'$ and H.
Assume $H \vDash_{g',k'} P \star \gamma \to \beta$ and $H; \mathsf{updt}\ t_1\ t_2\ t_3 \Downarrow^{k''} H = H_p \uplus H_l \wedge H_p \vDash P \wedge H_l \vDash \gamma \to \beta$
From $H; \mathsf{updt}\ t_1\ t_2\ t_3 \Downarrow^{k''}$, because t_1, t_2 are sub terms of $\delta\sigma\ \mathsf{updt}\ t_1\ t_2\ t_3$,we get

$$\delta\sigma\, t_1 \Downarrow_f^{k_1} \wedge \delta\sigma\, t_2 \Downarrow_f^{k_2} \wedge \delta\sigma\, t_3 \downarrow_f^{k_3} \tag{1}$$

From (1), we get:

$$\exists l, n, v, k_1, k_2, k_3.\delta\sigma\, t_1 \Downarrow^{k_1, c_1} l \wedge \delta\sigma\, t_2 \Downarrow^{k_2, c_1'} n \wedge \delta\sigma\, t_3 \Downarrow^{k_3, c_1''} v \wedge$$
$$k'' = k_1 + k_2 + k_3 + 1 \wedge c = c_1 + c_1' + c_1'' + c_{update} \tag{a}$$

From (a) and evaluation rules we get:

$$H; \delta\sigma(\mathsf{updt}\ t_1\ t_2\ t_3) \Downarrow_f^{k'', c} H[l][n] \leftarrow v; () \tag{b}$$

By IH on first premise instantiated with $(\sigma) \in [\![\delta\Omega']\!]_{g',k'}$ by lemma 1 and $FV(t_2) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$.
We get:

$$(\delta\sigma\, t_1) \in [\![\mathsf{Array}_\gamma[I]\ A]\!]_{G',k'}^{E,\delta(L_1,U_1)} \tag{2}$$

Similarly, By IH on the second premise and third premise, we get

$$(\delta\sigma\, t_2) \in [\![\mathrm{int}[I]]\!]_{g',k'}^{E,\delta(L_2,U_2)} \tag{3}$$
$$(\delta\sigma\, t_3) \in [\![A]\!]_{g',k'}^{E,\delta(L_3,U_3)} \tag{4}$$

From (2),(3),(4), we know:

$$l \in [\![\mathsf{Array}_\gamma[I]\ A]\!]_{g',k'-k_1} \Rightarrow g'(\gamma) = (l, A, I) \wedge \delta L_1 \le c_1 \le \delta U_1 \tag{c}$$
$$n \in [\![\mathrm{int}[I]]\!]_{g,k'-k_2} \Rightarrow n = I \wedge \delta L_2 \le c_1' \le \delta U_2 \tag{d}$$
$$v \in [\![A]\!]_{g',k'-k_3} \wedge \delta L_3 \le c_1'' \le \delta U_3 \tag{e}$$

Let us assume:

$$g'' = g' \tag{5}$$
$$H_1' = H(l)[n] \leftarrow v = H_p + H_l(l)[n] \leftarrow v \wedge H_l' = H_l(l)[n] \leftarrow v \tag{6}$$

STS1: $(H_1') \vDash_{g',k'-k''} P \star \gamma \to \beta$
Unfold $H \vDash_{g',k'} P \star \gamma \to \beta$ and consider (c), we know

$$\forall i \le I.(H_l(l)[i]) \in (\!|A|\!)_{g',k'-1} \tag{7}$$

we need to prove:

subgoal 1: $\forall i \le I.(H_l'(l)[i] \in [\![A]\!]_{g',k'-k''}$
when i=n,
we prove $(H_l'(l)[i]) \in [\![A]\!]_{g',k'-k_3}$ from (e) and (6), and then use lemma 1.
when $i \neq n$,
proved by using lemma 1 on (7)

STS2: $() \in [\![\text{unit}]\!]_{g',k'-k''}$
It is proved by unfolding the definition.

STS3: $\delta(L_1 + L_2 + L_3 + L_u) \le c \le \delta(U_1 + U_2 + U_3 + U_u)$
by the fact that $\delta L_u \le c_{update} \le \delta U_u$, it is proved by (c)(d)(e).

STS4: $\exists n.P = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \wedge \forall i \in [1,n].g(\gamma_i) = (l_i, A, m) \Rightarrow \forall j.(H[l_i][j]) \neq H'[l_i][j] \Rightarrow j \in T_i$
Because $H_1' = H(l)[n] \leftarrow v = H_p + H_l(l)[n] \leftarrow v \wedge H_l' = H_l(l)[n] \leftarrow v$, When $l_i \neq l$, $H(l_i) = H'(l_i)$, it is true. When $l_i = l$, only at position n so that $H(l)[n] \neq H(l)[n]$, we need to show $n \notin \beta$, which is the assumption from the rule.

This completes the proof of case unary update.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;\Omega \vdash_L^U t : A \qquad \Delta;\Phi;\Omega \vdash p \quad wf}{\Sigma;\Delta;\Phi;\Omega \vdash_0^{\text{exec}(L,U)} \text{return}\ t : \{P\}\ \exists\gamma.A\ \{P\}}\ \text{U-T}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and there exists Ω'. s.t. $FV(t) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$ and $(\sigma) \in (\!|\delta\Omega'|\!)_{g,k}$
TS: $(\delta\sigma\ \text{return}\ t) \in [\![\{P\}\ \exists\gamma.A\ \{P\}]\!]_{g,k}^{\text{exec}(L,U)E,(0,0)}$
Because return t is value.
STS: $(\delta\sigma\ \text{return}\ t) \in [\![\{P\}\ \exists\gamma.A\ \{P\}]\!]_{g,k}^{\text{exec}(L,U)}$
Unfold the definition of $[\![\{P\}\ \exists\gamma.A\ \{P\}]\!]_{g,k}^{\text{exec}(L,U)}$.
Pick $g^{'} \supseteq g$, $H_1, k' \le k, k'' < k'$.
Assume

$$H_1 \vDash_{g',k'} P \tag{1}$$

$$H_1; \delta\sigma(\text{return}\ t) \Downarrow_f^{k''} \tag{2}$$

Because t is the subterm of return t , From (2), We know:

$$\delta\sigma_1 t \Downarrow^{k''} \tag{3}$$

(2.5)

From (3), we know:

$$\exists v_1, k_1, \delta\sigma_1 t \Downarrow^{k_1,c_1} v_1 \wedge k'' = k_1 + 1 \wedge c = c_1 + c_{ret} \tag{a}$$

From (a) and the evaluation rule U-ret:

$$\exists H_1'.H_1; \text{return}\ t \Downarrow_f^{k'',c} v_1; H_1' \tag{b}$$

By IH on the premise instantiated with $(\sigma) \in [\![\delta\Omega']\!]_{g',k'}$ by lemma 1. We get:

$$(\delta\sigma\, t_1) \in [\![\delta A]\!]^{E,\delta(L,U)}_{G',k'} \tag{5}$$

Unfold (5), we get:

$$v_1 \in (\!|\delta A|\!)_{g',k'-k_1} \wedge \delta L_1 \leq c_1 \leq \delta U_1 \tag{6}$$

Let us assume:

$$g'' = g' \tag{7}$$
$$H_1' = H_1' \tag{8}$$

STS1: $H_1' \vDash_{g',k'-k''} P$
it is from assumption by using lemma 1.

STS2: $v_1 \in (\!|\tau|\!)_{g',k'-k''}$
It is proved by (6) using Lemma 1.

STS3: $\delta L \leq c \leq \delta U$ which is proved from (6)

STS4: $\exists n.P = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \wedge \forall i \in [1,n].g(\gamma_i) = (l_i, A, m) \Rightarrow \forall j.(H[l_i][j]) \neq H'[l_i][j] \Rightarrow j \in T_i$
H is not changed, it is trivial true.

This completes the proof of case unary return.

$$\frac{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1}_{L_1} t : \{P_1\}\ \exists^{\mathsf{exec}(L,U)}\vec{\gamma}_1 : A\ \{Q_1 \star Q_2\} \qquad \Sigma;\Delta,\vec{\gamma}_1;\Phi;\Omega, x : A \vdash^{U_2}_{L_2} u : \{Q_1 \star P_2\}\ \exists^{\mathsf{exec}(L',U')}\vec{\gamma}_2 : B\ \{Q\}}{\Sigma;\Delta;\Phi;\Omega \vdash^{U_1+U_2+U_l}_{L_1+L_2+L_l} \mathsf{let}\ \{x\} = t\ \mathsf{in}\ u : \{P\}\ \exists^{\mathsf{exec}(L+L',U+U')}\vec{\gamma}_1, \vec{\gamma}_2 : B\ \{Q \star Q_2\}}\ \text{U-E}$$

Assume that $\vdash \delta : \Delta$ and $\vDash \delta\Phi$ and there exists Ω'. s.t. $FV(t) \subseteq dom(\Omega')$ and $\Omega' \subseteq \Omega$ and $(\sigma) \in (\!|\delta\Omega'|\!)_{g,k}$

TS: $(\delta\sigma_1(\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_1')) \in (\!|\delta\ \{P\}\ \exists^{\mathsf{exec}(L+L',U+U')}\vec{\gamma}_1, \vec{\gamma}_2 : B\ \{Q \star Q_2\}|\!)^{(E,(U_1+U_2,L_1+L_2))}_{g,k}$
Unfold the definition .
Pick $g^{'} \supseteq g$, $H_1, k' \leq k, k'' < k'$.
Assume

$$H_1 \vDash_{G',k'} P \tag{1}$$
$$H_1; \delta\sigma_1(\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_1') \Downarrow^{k''}_f \tag{2}$$

Because t_1 is the subterm of $\mathsf{let}\ \{x\} = t_1\ \mathsf{in}\ t_1'$, From (2) and Lemma **??**, We know:

$$\exists v_1, v_1', v_1'', v_1''', k_1, k_2, k_3, k_4, H_1', H_1''.\quad \delta\sigma_1 t_1 \Downarrow^{k_1,c_1} v_1 \quad \text{and} \quad H_1; v_1 \Downarrow^{k_2,c_2}_f H_1'; v_1' \quad \text{and}$$
$$\delta\sigma_1 t_1'[v_1'/x] \Downarrow^{k_3,c_3} v_1'' \quad \text{and} \quad H_1'; v_1'' \Downarrow^{k_4,c_4}_f H_1''; v_1''' \quad \text{and}$$
$$k'' = k_1 + k_2 + k_3 + k_4 + 1 \wedge c = c_1 + c_2 + c_3 + c_4 + c_{let} \tag{a}$$

From evaluation rule: E-Let-F and (a)(b), we know:

$$\exists H_a, H_c, H_a', H1_{Q1}, H1_{Q2}, H1_Q, s.t. H_1 = H_a \uplus H_c \wedge v1; H_a \Downarrow_f v_1'; H_a' \wedge H_a' = H1_{Q1} \uplus H1_{Q2}$$
$$\wedge v_1''; H1_{Q1} \uplus H_c \Downarrow_f v_1'''; H1_Q \wedge H_1'' = H1_Q \uplus H1_{Q2} \tag{c}$$

From (1) : $H \vDash_{g',k'} P_1 \star P_2$, we assume that

$$\exists g_a, g_b : (H_1 = H_a \uplus H_c)$$
$$(g' = g_a \uplus g_c) \quad \text{and} \quad (H_a) \vDash_{g_a,k'} P_1 \quad \text{and} \quad (H_c) \vDash_{g_c,k'} P_2 \tag{*}$$

STS1: $(H_1'') \vDash_{g'',k'-k''} Q \star Q_2$
STS2: $(v_1''') \in (\!|B|\!)_{G'',k'-k''}$
STS3: $(L+L') \le c_f \le (U+U') \wedge L_1 + L_2 + L_{let} \le c_p \le U_1 + U_2 + U_{let}$
ST4: $P = \gamma_i \to \beta_i \forall i.g''(\gamma_i) = (l_i, m, A) \to H_1(l_i)[n] \neq H_1''(l_i)[n] \Rightarrow n \in \beta_i$

By IH on the second premise instantiated with $(\sigma_1) \in (\!|\delta\Omega|\!)_{g',k'}$, we know:

$$(\delta\sigma_1 t_1) \in (\!|\{P_1\}\ \exists\vec{\gamma}_1 : A\ \{Q_1 \star Q_2\}|\!)^{\mathrm{exec}(L,U),(L_1,U_1)}_{g',k'} \tag{4}$$

Unfold the definition ,use (a), we get:

$$\begin{aligned}(v_1) \in (\!|\{P_1\}\ \exists\vec{\gamma}_1 : A\ \{Q_1 \star Q_2\}|\!)^{\mathrm{exec}(L,U)}_{g',k'} \wedge L_1 \le c_1 \le U_1 \wedge P_1 = \gamma_i \to \beta_i \Rightarrow \\ \forall i.g''(\gamma_i) = (l_i, m, A) \to H_1(l_i)[n] \neq H_1'(l_i)[n] \Rightarrow n \in \beta_i\end{aligned} \tag{e}$$

To unfold (e), we choose: $k_f \le k' - k_1$ and $k_f' < k_f$ and $g_f \supseteq g'$ and (1),(a).
We have

$$(H_a \vDash_{g_f,k_f} P_1 \wedge H_a; v_1 \Downarrow_f \wedge H_b; v_2 \Downarrow_f$$

Unfold the definition, we get:

$$H_a; v_1 \Downarrow_f^{c_2} H_a'; v_1' \wedge H_a' \vDash Q_1 \star Q_2$$

$$(v_1') \in (\!|A|\!)_{g',k'-k_1} \wedge L \le c_2 \le U \tag{k}$$

By IH on the third premise, we know:

$$(\delta\sigma_1 v_1'') \in (\!|\{Q_1 \star P_2\}\ \exists\vec{\gamma}_1.B\ \{Q\}|\!)^{\mathrm{exec}D',E,D_2}_{G',k'} \tag{5}$$

Unfold the definition, we get:

$$\begin{aligned}v_1 \in (\!|\{Q_1 \star P_2\}\ \exists\vec{\gamma}_1.\tau_2\ \{Q\}|\!)^{\mathrm{exec}(L',U')}_{g',k'-k_1} \wedge l_2 \le c_3 \le U_2 \wedge Q_1 \uplus P_2 = \gamma_i \to \beta_i \\ \Rightarrow \forall i.g''(\gamma_i) = (l_i, m, A) \to H_1'(l_i)[n] \neq H_1''(l_i)[n] \Rightarrow n \in \beta_i\end{aligned} \tag{f}$$

We have

$$(H_a') \vDash_{g_f,k_f} Q_1 \star Q_2 \Rightarrow H1_{Q1} \vDash Q_1 \wedge H1_{Q2} \vDash Q_2 \wedge H_c \vDash P_2$$

$$H1_{Q1} \uplus H_c; v_1''' \Downarrow_f$$

Unfold the definition (f), we get:

$$H1_{Q1} \uplus H_c; v_1''' \Downarrow_f^{c_4} H1_Q; v_1'''' \wedge H1_Q \vDash Q$$

$$(v_1''') \in (\!|B|\!)_{g',k'-k_1} \wedge L' \le c_4 \le U' \tag{g}$$

STS1: Use Lemma 2, we know that $H1_Q \uplus H1_{Q2} \vDash Q \star Q_2$, which proves STS1.
STS2: it is proved from (g).
STS3: it is proved from (e),(k),(f),(g) and $c = c_f + c_p. \wedge c_f = c_2 + c_4$
STS4: from (e),(f), we know all the n in P will appear in P_1 or $Q_1 \uplus P_2$. It is proved.

This completes the proof of Unary let.

Proof of statement (3) if $\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau$ and $\vdash \delta : \Delta$ and $\vDash \delta\Phi$. Then for $i \in \{1,2\}$. if there exists Γ_i' s.t. $\mathrm{FV}(e_i) \subseteq dom(\Gamma_i'), \Gamma_i' \subseteq \Gamma$ and $(\sigma_i) \in [\![|\delta\Gamma_i'|_i]\!]_{G|_i,k}$, then $\delta\sigma_i e_i \in [\![|\delta\tau|_i]\!]^{E,(0,\infty)}_{G|_i,k}$
Because it is similar for the two case, we only show the case when i=1.

$$\text{CASE}\ \frac{\Delta;\Phi;x:\tau_1,f\ :\tau_1 \overset{\mathrm{diff}(D)}{\longrightarrow} \tau_2,\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau_2}{\Delta;\Phi;\Gamma \vdash \mathsf{Fix}\, f(x).t_1 \ominus \mathsf{Fix}\, f(x).t_2 \lesssim 0 : \tau_1 \overset{\mathrm{diff}(D)}{\longrightarrow} \tau_2}\ \text{R-FIX}$$

Assume that $\vDash \Phi\delta$ and there exists Γ' s.t. $\mathrm{FV}(\mathsf{fix}\, f(x).t_1) \subseteq dom(\Gamma'), \Gamma' \subseteq \Gamma$ and $\sigma \in [\![|\delta\Gamma'|_1]\!]_{G|_1,k}$
TS: $(\mathsf{fix}\, f(x).\delta\sigma\, t_1) \in [\![(|\delta\tau_1|_1 \overset{\mathrm{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1)]\!]^{E,(0,\infty)}_{G|_1,k}$
By Lemma 31,STS: $(\mathsf{fix}\, f(x).\delta\sigma\, t_1) \in [\![(|\delta\tau_1|_1 \overset{\mathrm{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1)]\!]_{G|_1,k}$
We prove the more general statement:

$$\forall m' \le k.(\mathsf{fix}\, f(x).\delta\sigma\, t_1) \in [\![(|\delta\tau_1|_1 \overset{\mathrm{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1)]\!]_{G|_1,m} \tag{1}$$

By subinduction on m'. There are two cases.

subcase 1: $m' = 0$.
there is no non-negative k' < 0, it is vacuously true.

subcase 2: $m' = m'' + 1 \le k$
By sub-IH: $(\mathsf{fix}\, f(x).\delta\sigma\, t_1) \in [\![(|\delta\tau_1|_1 \overset{\mathrm{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1)]\!]_{G|_1,m''}$
STS: $(\mathsf{fix}\, f(x).\delta\sigma\, t_1) \in [\![(|\delta\tau_1|_1 \overset{\mathrm{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1)]\!]_{G|_1,m''+1}$
Unfold the definition. Pick $j \le m''+1$, $g' \supseteq G|_1$.
Assume $v \in [\![|\delta\tau_1|_1]\!]_{g',j}$
STS: $\delta\sigma\, t_1[v/x][\mathsf{fix}\, f(x).t_1/f] \in [\![|\delta\tau_2|_1]\!]^{E,(0,\infty)}_{g',j}$

By IH 3 on the premise instantiated with $\sigma[v/x][\mathsf{fix}\, f(x).t_1/f] \in [\![\delta(x:|\tau_1|_1, f:|\delta\tau_1|_1 \overset{\mathrm{exec}(0,\infty)}{\longrightarrow} |\delta\tau_2|_1, |\Gamma'|)]\!]_{g',j}$ which holds because

1. $\sigma \in [\![|\delta\Gamma'|_1)]\!]_{g',j}$ by Lemma 1.
2. $v \in [\![|\tau_1|_1]\!]_{g',j}$ from assumption.
3. $\mathsf{fix}\, f(x).t_1 \in [\![|\tau_1|_1 \overset{\mathrm{exec}(0,\infty)}{\longrightarrow} |\tau_2|_1]\!]_{g',j}$ by Lemma 1 on the sub-IH conclusion.

and these premises: $FV(t_1) \subseteq dom(x:\tau_1, f:\tau_1 \overset{\mathrm{diff}(D)}{\longrightarrow} \tau_2, \Gamma')$ and $x:\tau_1, f:\tau_1 \overset{\mathrm{diff}(D)}{\longrightarrow} \tau_2, \Gamma' \subseteq x:\tau_1, f:\tau_1 \overset{\mathrm{diff}(D)}{\longrightarrow} \tau_2, \Gamma$

This proof is complete.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathrm{int}[I] \qquad \Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \tau \qquad \gamma\ \mathsf{fresh}}{\Delta;\Phi;\Gamma \vdash \mathsf{alloc}\, t_1\ t_2 \ominus \mathsf{alloc}\, t_1'\ t_2' \overset{\mathrm{diff}(D_1+D_2)}{\lesssim} 0 : \{P\}\ \exists\gamma.\ \mathsf{Array}_\gamma[I]\ \tau\ \{P \star \gamma \to \mathbb{N}\}}\ \text{ALLOC}$$

Assume that $\vDash \Phi\delta$ and there exists Γ' s.t. $\mathrm{FV}(\mathsf{alloc}\, t_1\ t_2) \subseteq dom(\Gamma'), \Gamma' \subseteq \Gamma$ and $\sigma \in [\![|\delta\Gamma'|_1]\!]_{G|_1,k}$
TS: $\delta\sigma\ \mathsf{alloc}\, t_1\ t_2 \in [\![|\delta(\{|P|_1\}\ \exists\gamma.\ \mathsf{Array}_\gamma[I]\ |\tau|_1\ \overset{\mathrm{exec}(0,\infty)}{\{|P|_1 \star \gamma \to \mathbb{N}\})|_1}]\!]^{E,(0,\infty)}_{G|_1,k}$
STS: $\delta\sigma\ \mathsf{alloc}\, t_1\ t_2 \in [\![|\delta(\{|P|_1\}\ \exists\gamma.\ \mathsf{Array}_\gamma[I]\ |\tau|_1\ \overset{\mathrm{exec}(0,\infty)}{\{|P|_1 \star \gamma \to \mathbb{N}\})|_1}]\!]_{G|_1,k}$
Unfold the definition.
Pick $g' \supseteq G|_1, k' \le k, k'' < k'$ and assume $H \vDash_{g',k'} |P|_1$ and $H;\mathsf{alloc}\, t_1\ t_2 \Downarrow^{k''}_f$

STS: $H; v \Downarrow_f^{k'',c} v', H'$ and $0 \le c \le \infty$ and $H' \vDash_{g'',k'-k''} \gamma$ and $v' \in [\![\mathsf{Array}_\gamma[I]\ |\tau|_1]\!]_{g'',k'-k''}$
From $H; \mathsf{alloc}\ t_1\ t_2 \Downarrow^{k''}$, because t_1, t_2 are sub terms of $\delta\sigma\ \mathsf{alloc}\ t_1\ t_2$,we get

$$\delta\sigma\, t_1 \Downarrow_f^{k_1} \wedge \delta\sigma\, t_2 \Downarrow_f^{k_2} \tag{1}$$

From (1), we get:

$$\exists v_1, v_2, k_1, k_2. \delta\sigma\, t_1 \Downarrow^{k_1,c_1} v_1 \wedge \delta\sigma\, t_2 \Downarrow^{k_2,c_1'} v_2 \wedge k'' = k_1 + k_2 + 1 \wedge c = c_1 + c_1' + c_{alloc} \tag{a}$$

From (a) and evaluation rules we get:

$$\exists l. H, (\mathsf{alloc}\ t_1\ t_2)\delta\sigma \Downarrow_f^{k'',c} l; H[l \to [v_2, \ldots v_2] \tag{b}$$

By IH 3 on the first premise instantiated with $\sigma \in [\![|\delta\Gamma'|_1]\!]_{g,k''}$using lemma 1 and $FV(t_1) \subseteq dom(\Gamma')$ and $\Gamma' \subseteq \Gamma$, we get:

$$(\delta\sigma\, t_1) \in [\![|\delta \mathsf{int}_r[I]|_1]\!]_{g',k''}^{E,(0,\infty)} \tag{*}$$

Unfold the definition of $[\![\mathsf{int}[I]]\!]_{g',k''}^{E,(0,\infty)}$ and using (a) and $k_1 \le k''$, we know:

$$(v_1) \in [\![\mathsf{int}[I]]\!]_{G',k''-k_1} \Rightarrow v_1 = I \wedge 0 \le c_1 \le \infty \qquad \text{IH1}$$

By IH 3 on the second premise instantiated with $(\sigma) \in [\![|\delta\Gamma'|_1]\!]_{g',k'-k_1}$using lemma 1 and $FV(t_2) \subseteq dom(|\Gamma'|_1)$ and $\Gamma' \subseteq \Gamma$, we get:

$$(\delta\sigma\, t_2) \in [\![|\delta\tau|_1]\!]_{g',k'-k_1}^{E,(0,\infty)} \tag{**}$$

Unfold the definition of (**) and using (a), (b) and $k_2 \le k' - k_1$, we know

$$(v_2) \in [\![|\delta\tau|_1]\!]_{g',k'-k_1-k_2} = [\![|\delta\tau|_1]\!]_{g',k'-k''+1} \wedge 0 \le c_1' \le \infty \qquad \text{IH2}$$

Let us assume:

$$g'' = g'[\gamma \to (l, |\tau|_1, I)] \tag{c}$$
$$H_1' = H_1, \left[l \to [v_2, v_2, \ldots, v_2]\right] \tag{d}$$

we want to show 2 cases.

TS1 $(v' = l) \in [\![\mathsf{Array}_\gamma[I]\ |\tau|_1]\!]_{g'',k'-k''}$
it is proved by unfolding the definition and using the assumption (c).

TS2 $(H_1') \vDash_{g'',k'-k''} |P|_1 \star \gamma \to \mathbb{N}$
we know that $g''(\gamma) = (l, |\tau|_1, I)$, $H_1' = H_1 \uplus H_l \wedge H_l = l \to [v_2, \ldots, v_2]$, $H_1 \vDash |P|_1$ from assumption.

STS1 $\forall i \le I, (H_l(l)[i] \in [\![A]\!]_{g'',k'-k''-1}$
It is proved by using IH2 and Lemma 1.

TS3 $0 \le c \le \infty$
It is proved by IH1 and IH2 and $0 \le c_{alloc} \le \infty$.

TS4: $\exists n. |P|_1 = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \wedge \forall i \in [1, n]. g(\gamma_i) = (l_i, A, m) \Rightarrow \forall j. (H[l_i][j]) \ne H'[l_i][j] \Rightarrow j \in T_i$
Because γ not in $|P|_1$. For all γ_i, H,H' is the same.

This proof is complete.

$$\text{CASE}\ \frac{\begin{array}{c}\Delta; \Phi; \Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \\ \Sigma; \Delta; \Phi; \Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathsf{int}_r[I'] \qquad \Delta; \Phi \vDash I' \le I\end{array}}{\Sigma; \Delta; \Phi; \Gamma \vdash \mathsf{read}\ t_1\ t_2 \ominus \mathsf{read}\ t_1'\ t_2' \overset{\mathrm{diff}(D_1+D_2)}{\lesssim} 0 : \{P\}\ \exists \_. \tau\ \{P\}}\ \text{R-READ}$$

Assume that $\vDash \Phi\delta$ and there exists Γ' s.t. FV(read $t_1\ t_2$) $\subseteq dom(\Gamma'), \Gamma' \subseteq \Gamma$ and $\sigma \in [\![|\delta\Gamma'|_1]\!]_{G|_1,k}$

TS: $\delta\sigma$ read $t_1\ t_2 \in [\![|\delta(\{|P|_1\} \overset{\text{exec}(0,\infty)}{\exists}\_.|\tau|_1\ \{|P|_1\})|_1]\!]^{E,(0,\infty)}_{G|_1,k}$

STS: $\delta\sigma$ alloc $t_1\ t_2 \in [\![|\delta(\{|P|_1\} \overset{\text{exec}(0,\infty)}{\exists}\_.|\tau|_1\ \{|P|_1\})|_1]\!]_{G|_1,k}$

Unfold the definition.

Pick $g' \supseteq G|_1, k' \leq k, k'' < k'$ and assume $H \vDash_{g',k'} |P|_1$ and H;read $t_1\ t_2 \Downarrow^{k''}_f$

STS: H;read $t_1\ t_2 \Downarrow^{k'',c}_f v'$, H' and $0 \leq c \leq \infty$ and $H' \vDash_{g'',k'-k''} \gamma$ and $v' \in [\![|\tau|_1]\!]_{g'',k'-k''}$

From H;read $t_1\ t_2 \Downarrow^{k''}$, because t_1, t_2 are sub terms of $\delta\sigma$ read $t_1\ t_2$,we get

$$\delta\sigma\, t_1 \Downarrow^{k_1}_f \wedge \delta\sigma\, t_2 \Downarrow^{k_2}_f \tag{1}$$

From (1), we get:

$$\exists l, n, v, k_1, k_2.\, \delta\sigma\, t_1 \Downarrow^{k_1,c_1} l \wedge \delta\sigma\, t_2 \Downarrow^{k_2,c'_1} n \wedge k'' = k_1 + k_2 + 1 \wedge c = c_1 + c'_1 + c_{read} \wedge H(l)[n] = v \tag{a}$$

From (a) and evaluation rules we get:

$$H;\delta\sigma(\text{read}\ t_1\ t_2) \Downarrow^{k'',c}_f H; v \tag{b}$$

By IH 3 on the first premise instantiated with $\sigma \in [\![|\delta\Gamma'|_1]\!]_{g,k''}$using lemma 1 and $FV(t_1) \subseteq dom(\Gamma')$ and $\Gamma' \subseteq \Gamma$, we get:

$$(\delta\sigma\, t_1) \in [\![\text{Array}_\gamma[I]\ |\tau|_1]\!]^{E,(0,\infty)}_{g',k'} \tag{6}$$

Unfold (6), since $k_1 \leq k'$ and $\delta\sigma_1\, t_1 \Downarrow^{k_1,c_1} l$, we know

$$l \in [\![\text{Array}_\gamma[I]\ |\tau|_1]\!]_{g',k'-k_1} \wedge 0 \leq c_1 \leq \infty \tag{e}$$

From (e), we know :

$$g'(\gamma) = (l, |\tau|_1, I) \tag{7}$$

By IH 3 on the first premise instantiated with $\sigma \in [\![|\delta\Gamma'|_1]\!]_{g,k''}$using lemma 1 and $FV(t_2) \subseteq dom(\Gamma')$ and $\Gamma' \subseteq \Gamma$, we get:

$$(\delta\sigma_1\, t'_2) \in [\![\text{int}[I']]\!]^{E,(0,\infty)}_{g',k'} \tag{8}$$

Unfold (8), since $k_2 \leq k'$,we know

$$n \in [\![\text{int}[I']]\!]_{g',k'-k_2} \Rightarrow n = I' \wedge 0 \leq c'_1 \leq \infty \tag{f}$$

Let us assume:

$$g' = g' \tag{g}$$

STS1: $H \vDash_{g',k'-k''} |P|_1$
proved by Lemma 1 on assumption $H \vDash_{g',k'} |P|_1$

STS2: $(v' = v) \in [\![|\tau|_1]\!]_{g',k'-k''}$
from (a). we know $H_1(l)[n] = v$
From $H \vDash_{g',k'-k''} \gamma$ we know:
$\forall i \leq n, (H_1(l)(i)) \in [\![A]\!]_{g',k'-1}$
s.t we know
$(H_1(l)[n]) \in [\![A]\!]_{g',k'-1}$
Because $k' - k'' \leq k' - 1$,
By Lemma 1, We get: $v \in [\![A]\!]_{g',k'-k''}$

STS3: $0 \leq c \leq \infty$
by the fact that $0 \leq c_{read} \leq \infty$, it is proved by (e)(f).

STS4: $\exists n.|P|_1 = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \wedge \forall i \in [1,n].g(\gamma_i) = (l_i, A, m) \Rightarrow \forall j.(H[l_i][j]) \neq H'[l_i][j] \Rightarrow j \in T_i$
H is not changed , it is trivially true.

This completes the proof of case read.

$$\text{CASE}\ \frac{\begin{array}{c}\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \qquad \Delta;\Phi \models I' \leq I \qquad \Delta;\Phi \models I' \in \beta\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{read}\ t_1\ t_2 \ominus \mathsf{read}\ t_1'\ t_2' \overset{\mathrm{diff}(D_1+D_2)}{\lesssim} 0 : \{\gamma \to \beta\}\ \exists\_.\Box\tau\ \{\gamma \to \beta\}}\ \text{R-RB}$$

The proof is same as case read above.

$$\text{CASE}\ \frac{\begin{array}{c}\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_1' \lesssim D_1 : \mathsf{Array}_\gamma[I]\ \tau \\ \Sigma;\Delta;\Phi;\Gamma \vdash t_2 \ominus t_2' \lesssim D_2 : \mathrm{int}[I'] \qquad \Sigma;\Delta;\Phi;\Gamma \vdash t_3 \ominus t_3' \lesssim D_3 : \tau \qquad \Delta;\Phi \models I' \leq I\end{array}}{\Sigma;\Delta;\Phi;\Gamma \vdash \mathsf{updt}\ t_1\ t_2\ t_3 \ominus \mathsf{updt}\ t_1'\ t_2'\ t_3' \overset{\mathrm{diff}(D_1+D_2+D_3)}{\lesssim} 0 : \{P \star \gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r\ \{P \star \gamma \to \beta \cup \{I'\}\}}\ \text{R-U}$$

Assume that $\models \Phi\delta$ and there exists Γ' s.t. $\mathrm{FV}(\mathsf{updt}\ t_1\ t_2\ t_3) \subseteq dom(\Gamma'), \Gamma' \subseteq \Gamma$ and $\sigma \in [\![|\delta\Gamma'|_1]\!]_{G|_1,k}$

TS: $\delta\sigma\ \mathsf{updt}\ t_1\ t_2\ t_3 \in [\![|\delta(\{|P|_1 \star \gamma \to \mathbb{N}\}\overset{\mathrm{exec}(0,\infty)}{\exists\_.}|\mathrm{unit}_r|_1\ \{|P|_1 \star \gamma \to \mathbb{N}\})|_1]\!]^{E,(0,\infty)}_{G|_1,k}$

STS: $\delta\sigma\ \mathsf{updt}\ t_1\ t_2\ t_3 \in [\![|\delta(\{|P|_1 \star \gamma \to \mathbb{N}\}\overset{\mathrm{exec}(0,\infty)}{\exists\_.}|\mathrm{unit}_r|_1\ \{|P|_1 \star \gamma \to \mathbb{N}\})|_1]\!]_{G|_1,k}$
Unfold the definition.
Pick $g' \supseteq G|_1, k' \leq k, k'' < k'$ and assume $H \vDash_{g',k'} |P|_i \star \gamma \to \mathbb{N}$ and $H; \mathsf{updt}\ t_1\ t_2\ t_3 \downarrow^{k''}_f$
STS: $H; \mathsf{updt}\ t_1\ t_2\ t_3 \Downarrow^{k'',c}_f v', H'$ and $0 \leq c \leq \infty$ and $H' \vDash_{g'',k'-k''} \gamma$ and $v' \in [\![|\mathrm{unit}_r|_1]\!]_{g'',k'-k''}$
From $H; \mathsf{updt}\ t_1\ t_2\ t_3 \Downarrow^{k''}$, because t_1, t_2 are sub terms of $\delta\sigma\ \mathsf{updt}\ t_1\ t_2\ t_3$,we get

$$\delta\sigma\, t_1 \Downarrow^{k_1}_f \wedge \delta\sigma\, t_2 \Downarrow^{k_2}_f \wedge \delta\sigma\, t_3 \Downarrow^{k_3}_f \tag{1}$$

From (1), we get:

$$\begin{aligned}\exists l, n, v, k_1, k_2, k_3.\delta\sigma\, t_1 \Downarrow^{k_1,c_1} l \wedge \delta\sigma\, t_2 \Downarrow^{k_2,c_1'} n \wedge \delta\sigma\, t_3 \Downarrow^{k_3,c_1''} v \wedge \\ k'' = k_1 + k_2 + k_3 + 1 \wedge c = c_1 + c_1' + c_1'' + c_{update}\end{aligned} \tag{a}$$

From (a) and evaluation rules we get:

$$H; \delta\sigma(\mathsf{updt}\ t_1\ t_2\ t_3) \Downarrow^{k'',c}_f H[l][n] \leftarrow v; () \tag{b}$$

By IH 3 on the first premise instantiated with $\sigma \in [\![|\delta\Gamma'|_1]\!]_{g,k''}$using lemma 1 and $FV(t_2) \subseteq dom(\Gamma')$ and $\Gamma' \subseteq \Gamma$, we get:

$$(\delta\sigma\, t_1) \in [\![\mathsf{Array}_\gamma[I]\ |\tau|_1]\!]^{E,(0,\infty)}_{G',k'} \tag{2}$$

Similarly, By IH 3 on the second premise and third premise, we get

$$(\delta\sigma\, t_2) \in [\![|\mathrm{int}[I]|_1]\!]^{E,(0,\infty)}_{g',k'} \tag{3}$$

$$(\delta\sigma\, t_3) \in [\![|\tau|_1]\!]^{E,(0,\infty)}_{g',k'} \tag{4}$$

From (2),(3),(4), we know:

$$l \in [\![\mathsf{Array}_\gamma[I]\ A]\!]_{g',k'-k_1} \Rightarrow g'(\gamma) = (l, A, I) \wedge 0 \leq c_1 \leq \infty \tag{c}$$

$$n \in [\![\mathrm{int}[I]]\!]_{g,k'-k_2} \Rightarrow n = I \wedge 0 \leq c_1' \leq \infty \tag{d}$$

$$v \in [\![A]\!]_{g',k'-k_3} \wedge 0 \leq c_1'' \leq \infty \tag{e}$$

Let us assume:

$$g'' = g' \tag{5}$$

$$H_1' = H(l)[n] \leftarrow v \tag{6}$$

STS1: $(H_1') \vDash_{g',k'-k''} |P|_1 \star \gamma \to \mathbb{N}$
$H_1 = H_p \uplus H_l$, $H_1' = H_p \uplus H_l(l) \leftarrow v$
From assumption $H_1 \vDash |P|_1 \star \gamma \to \mathbb{N}$
STS: $H_l' = H_l(l) \leftarrow v \vDash \gamma \to \mathbb{N}$, which is proved by the assumption that $H_l \vDash \gamma \to \mathbb{N}$

STS2: $() \in [\![\text{unit}]\!]_{g',k'-k''}$
It is proved by unfolding the definition.

STS3: $0 \le c \le \infty$
by the fact that $\delta L_u \le c_{update} \le \delta U_u$, it is proved by (c)(d)(e).

STS4: $\exists n.|P|_i \star \gamma \to \mathbb{N} = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \wedge \forall i \in [1,n].g(\gamma_i) = (l_i, A, m) \Rightarrow \forall j.(H[l_i][j]) \neq H'[l_i][j] \Rightarrow j \in T_i$
When $l_i \neq l$, the heap is not changed. it is true;
When $l_i = l$, $H(l)[n] \neq H'(l)[n]$, To show $n \in \beta$, which the premise in the typing rule.

This completes the proof of case unary update.

$$\text{CASE}\ \frac{\Sigma;\Delta;\Phi;\Gamma \vdash t_1 \ominus t_2 \lesssim D : \tau}{\Sigma;\Delta;\Phi;\Gamma \vdash \text{return } t_1 \ominus \text{return } t_2 \lesssim 0 : \{P\}\ \exists\_.\tau\ \{P\}}\ \overset{\text{diff}(D)}{\text{R-T}}$$

Assume that $\vDash \Phi\delta$ and there exists Γ' s.t. FV(return t_1) $\subseteq dom(\Gamma')$, $\Gamma' \subseteq \Gamma$ and $\sigma \in [\![|\delta\Gamma'|_1]\!]_{G|_1,k}$
TS: $\delta\sigma$ return $t_1 \in [\![|\delta(\{|P|_1\}\ \overset{\text{exec}(0,\infty)}{\exists\_.|\tau|_1}\ \{|P|_1\})|_1]\!]^{E,(0,\infty)}_{G|_1,k}$
STS: $\delta\sigma$ return $t_1 \in [\![|\delta(\{|P|_1\}\ \overset{\text{exec}(0,\infty)}{\exists\_.|\tau|_1}\ \{|P|_1\})|_1]\!]_{G|_1,k}$
Unfold the definition.
Pick $g' \supseteq G|_1, k' \le k, k'' < k'$ and assume $H \vDash_{g',k'} |P|_1$ and H; return $t_1 \Downarrow^{k''}_f$
STS: H; return $t_1 \Downarrow^{k'',c}_f v', H'$ and $0 \le c \le \infty$ and $H' \vDash_{g'',k'-k''} \gamma$ and $v' \in [\![|\tau|_1]\!]_{g'',k'-k''}$
Because t_1 is the subterm of return t_1 ,we know:

$$\delta\sigma_1 t_1 \Downarrow^{k''} \tag{3}$$

(2.6)

From (3), we know:

$$\exists v_1, k_1, \delta\sigma_1 t_1 \Downarrow^{k_1,c_1} v_1 \wedge k'' = k_1 + 1 \wedge c = c_1 + c_{ret} \tag{a}$$

From (a),(b) and the evaluation rule R-ret:

$$H_1; \text{return } t_1 \Downarrow^{k'',c}_f v_1; H_1 \tag{b}$$

By IH 3 on the first premise instantiated with $\sigma \in [\![|\delta\Gamma'|_1]\!]_{g,k''}$ using lemma 1 and $FV(t_2) \subseteq dom(\Gamma')$ and $\Gamma' \subseteq \Gamma$, we get:

$$(\delta\sigma\, t_1) \in [\![|\delta\tau|_1]\!]^{E,(0,\infty)}_{G',k'} \tag{5}$$

Unfold (5), we get:

$$v_1 \in (\!|\delta A|\!)_{g',k'-k_1} \wedge 0 \le c_1 \le \infty \tag{6}$$

Let us assume:

$$g'' = g' \tag{7}$$
$$H_1' = H_1 \tag{8}$$

STS1: $H_1 \vDash_{g',k'-k''} |P|_1$
It is proved by the assumption on Lemma (monotonicity).

STS2: $(v_1) \in (\!|\tau|_1|\!)_{g',k'-k''}$
It is proved by (6) using Lemma 1.

STS3: $0 \leq c \leq \infty$ which is proved from (6)

STS4: $\exists n.|P|_1 = \{\gamma_1 \to T_1, \ldots, \gamma_n \to T_n\} \wedge \forall i \in [1,n].g(\gamma_i) = (l_i, A, m) \Rightarrow \forall j.(H[l_i][j]) \neq H'[l_i][j] \Rightarrow j \in T_i$
H is not changed, it is true.

This completes the proof of case unary return.

3 Example revisited

3.1 InPlaceMap

Example 1: In Place Map

$$\begin{array}{l}\mathsf{InPlaceMap} = \mathsf{fix\ map}\,(f).\lambda a.\lambda k.\lambda n.\\ \quad \mathsf{if}\ k \le n\ \mathsf{then}\ \big(\mathsf{let}\ \{x\} = \big(\ \mathsf{read}\ a\ k\ \big)\ \mathsf{in}\\ \qquad \mathsf{let}\{\_\} = \big(\ \mathsf{updt}\ a\ k\ (f\ x)\ \big)\ \mathsf{in}\ \big((\mathsf{celim}\ (\mathsf{map}\ f))\ a\ (k+1)\ n\big)\\ \quad \mathsf{else\ return}()\end{array}$$

As a first example we want to prove

$$\vdash \quad \mathsf{InPlaceMap} \quad : \quad \begin{array}{l}\forall L.\forall U : \mathbb{N}.(A \overset{\mathrm{exec}(L,U)}{\longrightarrow} A') \longrightarrow \forall n : \mathbb{N}.\ \forall i : \mathbb{N}.\ \forall \gamma : \mathbb{L}.\\ (i \le n) \supset \big(\ \mathsf{Array}_\gamma[n]\ A \longrightarrow \mathrm{int}[i] \longrightarrow \overset{\mathrm{exec}((L+c_r+c_u)*(n-i),(U+c_r+c_u)*(n-i))}{\{\gamma \to \mathbb{N}\}\ \exists\_.\mathrm{unit}\ \{\gamma \to \mathbb{N}\}}\ \big)\end{array}$$

where c_r is the cost for one reading operation and c_u denotes the cost for one updating operation.//

$$\vdash \mathsf{InPlaceMap} \ominus \mathsf{InPlaceMap} \lesssim 0 : \begin{array}{l}\forall r.\square(\tau \overset{\mathrm{diff}(r)}{\longrightarrow} \tau) \longrightarrow \forall n, i : \mathbb{N}.\ \forall \gamma : \mathsf{ref}.\ \forall \beta : \mathbb{P}.\\ (i \le n) \supset \big(\ \mathsf{Array}_\gamma[n]\ \tau \longrightarrow \mathrm{int}[i] \longrightarrow \{\gamma \to \beta\}\ \exists\_.\mathrm{unit}\ \{\gamma \to \beta\}\ \big)\end{array}$$

$$\vdash \mathsf{InPlaceMap} \ominus \mathsf{InPlaceMap} \lesssim 0 : \begin{array}{l}\forall r.(\tau \overset{\mathrm{diff}(r)}{\longrightarrow} \tau) \longrightarrow \forall n, i : \mathbb{N}.\ \forall \gamma : \mathsf{ref}.\ \forall \beta : \mathbb{P}.\ (i \le n) \supset\\ \big(\ \mathsf{Array}_\gamma[n]\ \tau \longrightarrow \mathrm{int}[i] \longrightarrow \{\gamma \to \beta\}\ \exists\_.\mathrm{unit}\ \{\gamma \to \beta \cup [i,n]\}\ \big)\end{array}$$

Let us call M the following term:

$$\big(\mathsf{celim}(\mathsf{map}\ f)\ a\ (k+1)\ n\big)$$

and call T the following term:

$$\Big(\mathsf{let}\ \{x\} = \big(\ \mathsf{read}\ a\ k\ \big)\ \mathsf{in}\ \mathsf{let}\{\_\} = \big(\ \mathsf{updt}\ a\ i\ (f\ x)\ \big)\ \mathsf{in}\ (\mathsf{celim}(\mathsf{map}\ f)\ a\ (k+1)\ n)\Big)$$

and call Z the following term:

$$\mathsf{let}\{\_\} = \big(\ \mathsf{updt}\ a\ i\ (f\ x)\ \big)\ \mathsf{in}\big(\mathsf{celim}(\mathsf{map}\ f)\ a\ (k+1)\ n\big)$$

and set V as:

$$\mathsf{if}\ k < n, \mathsf{then}\ T\ \mathsf{else}\ \ (\mathsf{return}\ ())$$

Before we discussing the two types, we can apply simple rules first to make the relational type easy to read. We apply $R-iLam$ and $R-abs$ several times. Before we start to derivate the relational type of part V, We apply relational rule $R-Cimpl$ to introduce the constraint $i \le n$ into the constraint environment Φ.

Type 1: Same function We have two possible cases, one is that position $I \in \beta$ which means the values in the two arrays of two runs may be different, the other case is $I \notin \beta$, which means in index I, the values are the same in the two arrays:

Before we go to the two cases, we will first apply R-split. We need to show two cases and their types, with different constraint environment $\Phi \wedge i \in \beta$ and $\Phi \wedge i \notin \beta$ respectively.

Case 1: different values from read, $\Phi \wedge i \in \beta$

$$\frac{\Delta;\Phi;\Gamma \vdash a \ominus a \lesssim 0 : \mathsf{Array}_\gamma[n]\ \tau \qquad \Delta;\Phi;\Gamma \vdash k \ominus k \lesssim 0 : \mathrm{int}[i] \qquad \Delta;\Phi \models i \leq n \qquad \Delta;\vdash \mathsf{empty} \quad wf}{\Delta;\Phi;\Gamma \vdash \mathsf{read}\ a\ k \ominus \mathsf{read}\ a\ k \lesssim 0 : \{\gamma \to \beta\}\ \exists\_.\tau\ \{\gamma \to \beta\}}\ \text{R-R}$$

and

$$\frac{\Delta;\Phi;\Gamma \vdash a \ominus a \lesssim 0 : \mathsf{Array}_\gamma[n]\ \tau \qquad \Delta;\Phi;\Gamma \vdash k \ominus k \lesssim 0 : \mathrm{int}[i] \qquad \Delta;\Phi;\Gamma, x:\tau \vdash f\ x \ominus f\ x \lesssim r : \tau \qquad \Delta;\Phi \models i \leq n \qquad \Delta;\vdash \mathsf{empty} \quad wf}{\Delta;\Phi;\Gamma \vdash \mathsf{updt}\ a\ k\ (f\ x) \ominus \mathsf{updt}\ a\ k\ (f\ x) \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(r)}{\mathrm{unit}_r}\ \{\gamma \to \beta \cup \{i\}\}}\ \text{R-U}$$

where $\Delta = n:\mathbb{N}, i:\mathbb{N}, r:\mathbb{R}$
$\Sigma = \gamma : \mathbb{L}$
$\Phi = i \leq n$
$\Gamma = a : \mathsf{Array}_\gamma[n]\ \tau, k : \mathrm{int}[i], f : \square(\tau \overset{\mathrm{diff}((r))}{\longrightarrow} \tau), map : \square(\tau \overset{\mathrm{diff}((r))}{\longrightarrow} \tau) \overset{\mathrm{diff}(0)}{\longrightarrow} \forall n:\mathbb{N}.\ \forall i:\mathbb{N}.\ \forall \gamma:\mathbb{L}.\ (i \leq n) \supset \big(\mathsf{Array}_\gamma[n]\ \tau \longrightarrow \mathrm{int}[i] \longrightarrow \mathrm{int}[n] \longrightarrow \{\gamma \to \beta\}\ \mathrm{unit}\ \{\gamma \to \beta\}\big)$.
Because at position i, $a_1[i] \neq a_2[i]$,s.t. $\beta \cup \{i\} = \beta$.
We will show:

$$\dfrac{\dfrac{\dfrac{\text{S-RM}}{\Delta;\Phi \models \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to \beta\} \sqsubseteq \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}} \qquad \Delta;\Phi;\Gamma \vdash\ \mathsf{return}\ ()\ominus\mathsf{return}\ () \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}}{\Delta;\Phi;\Gamma \vdash \mathsf{return}\ ()\ominus\mathsf{return}\ () \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}}\ \text{R-EXEC} \qquad \Delta;\Phi;\Gamma \vdash k < n \ominus k < n \lesssim 0 : \mathrm{unit} + \mathrm{unit} \qquad \Delta;\Phi;\Gamma \vdash\ T \ominus\ T \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}}{\Delta;\Phi;\Gamma, \{x:\tau\} \vdash V \ominus V \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}}\ \text{R-CASE}$$

Using R-Let rules, we get

$$\frac{P_2 = \mathsf{empty} \qquad \Delta;\Phi;\Gamma \vdash \mathsf{read}\ a\ k \ominus \mathsf{read}\ a\ k \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{int}}\ \{\gamma \to \beta\} \qquad \Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}}{\Delta;\Phi;\Gamma, \{x:\mathrm{int}\} \vdash T \ominus T \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}}\ \text{R-LET}$$

$$\frac{P_2 = \mathsf{empty} \qquad \Delta;\Phi;\Gamma \vdash \mathsf{updt}\ a\ k\ (f\ x) \ominus \mathsf{updt}\ a\ k\ (f\ x) \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\} \qquad \Delta;\Phi;\Gamma \vdash M \ominus M \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(|\beta \cap [i+1,n]| * r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}}{\Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \overset{\mathrm{diff}(|\beta \cap [i+1,n]| * r + r)}{\mathrm{unit}_r}\ \{\gamma \to \beta\}}\ \text{R-LET}$$

Because i in β, we know: $|\beta \cap [i+1,n]| * r + r = |\beta \cap [i,n]|$ and $\beta \cup \{i\} = \beta$.
We want to show the typing of M. By applying R-IApp (when instantiating $\forall i$, we use i+1)

and R-App(when instantiating $\lambda.k$, we use k+1), we can easily get

$$\dfrac{\dfrac{\Delta;\Phi \vDash i+1 \le n \qquad \Delta;\Phi\Gamma \vdash \big((\mathsf{map}\, f)\big) \ominus \big((\mathsf{map}\, f)\big) \lesssim 0 :}{(i+1 \le n) \supset \big(\mathsf{Array}_\gamma[n]\ \tau \longrightarrow \mathrm{int}[i+1] \longrightarrow \mathrm{int}[n] \longrightarrow \{\gamma \to \beta\}\ \overset{\mathrm{diff}(|\beta \cap [i+1,n]| * r)}{\exists\_ : \mathrm{unit}}\ \{\gamma \to \beta\}\big)}}{\Delta;\Phi;\Gamma \vdash \big(\mathsf{celim}(\mathsf{map}\, f)\big) \ominus \big(\mathsf{celim}(\mathsf{map}\, f)\big) \lesssim 0 :\ \mathsf{Array}_\gamma[n]\ \tau \to \mathrm{int}[i+1] \to \mathrm{int}[n] \to \{\gamma \to \beta\}\ \overset{\mathrm{diff}(|\beta \cap [i+1,n]| * r)}{\exists\_ : \mathrm{unit}_r}\ \{\gamma \to \beta\}}\ \text{R-CELIM}$$

$$\Delta;\Phi;\Gamma \vdash \big(\mathsf{celim}(\mathsf{map}\, f)\ a\ (k+1)\ n\big) \ominus \big(\mathsf{celim}(\mathsf{map}\, f)\ a\ (k+1)\ n\big) \lesssim 0 :\ \overset{\mathrm{diff}(|\beta \cap [i+1,n]| * r)}{\{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r}\ \{\gamma \to \beta\}$$

Case 2: the same value from read, $\Phi \wedge i \notin \beta$

$$\dfrac{\Delta;\Phi;\Gamma \vdash a \ominus a \lesssim 0 : \mathsf{Array}_\gamma[n]\ \tau \qquad \Delta;\Phi;\Gamma \vdash k \ominus k \lesssim 0 : \mathrm{int}[i] \qquad \Delta;\Phi \vDash i \le n \qquad \Delta;\Phi \vDash i \notin \beta}{\Delta;\Phi;\Gamma \vdash \mathsf{read}\ a\ k \ominus \mathsf{read}\ a\ k \lesssim 0 : \{\gamma \to \beta\}\ \overset{\mathrm{diff}(0)}{\exists\_.\Box\tau}\ \{\gamma \to \beta\}}\ \text{R-RB}$$

and

$$\dfrac{\dfrac{\dfrac{\Delta;\Phi;\Gamma \vdash a \ominus a \lesssim 0 : \mathsf{Array}_\gamma[n]\ \tau \qquad \Delta;\Phi;\Gamma \vdash k \ominus k \lesssim 0 : \mathrm{int}[i]}{\Delta;\Phi \vDash \Box(\overset{\mathrm{diff}((r))}{\tau \longrightarrow \tau}) \sqsubseteq \Box\tau \overset{\mathrm{diff}((0))}{\longrightarrow} \Box\tau\ \text{S-R-BOX-DIFF}}}{\Delta;\Phi \vdash f \ominus f \lesssim 0 : \Box\tau \overset{\mathrm{diff}((0))}{\longrightarrow} \Box\tau}}{\Delta;\Phi;\Gamma x : \Box\tau \vdash f\ x \ominus f\ x \lesssim 0 : \Box\tau} \qquad \Delta;\Phi \vDash i \le n}{\Delta;\Phi;\Gamma,\vdash \mathsf{updt}\ a\ k\ (f\ x) \ominus \mathsf{updt}\ a\ k\ (f\ x) \lesssim 0 : \{\gamma \to \beta\}\ \overset{\mathrm{diff}(0)}{\exists\_ : \mathrm{unit}_r}\ \{\gamma \to \beta / \{i\}\}}\ \text{R-UB}$$

where $\Delta = n : \mathbb{N}, i : \mathbb{N}, r : \mathbb{R}$
$\Sigma = \gamma : \mathbb{L}$
$\Phi = i \le n$
$\Gamma = a : \mathsf{Array}_\gamma[n]\ \tau, k : \mathrm{int}[i], f : \Box(\overset{\mathrm{diff}((r))}{\tau \longrightarrow \tau}), map : \Box(\overset{\mathrm{diff}((r))}{\tau \longrightarrow \tau}) \overset{\mathrm{diff}(0)}{\longrightarrow} \forall n : \mathbb{N}.\ \forall i : \mathbb{N}.\ \forall \gamma, \beta :.\ (i \le n) \supset \big(\mathsf{Array}_\gamma[n]\ \tau \longrightarrow \mathrm{int}[i] \longrightarrow \mathrm{int}[n] \longrightarrow \exists \beta.\ \{\gamma \to \beta\}\ \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\mathrm{unit}}\ \{\gamma \to \beta\}\big)$.
Because at position i, $a_1[i] \neq a_2[i]$,s.t. $\beta \cup \{i\} = \beta$.

Using R-Let rules, we get

$$\dfrac{P_2 = \mathsf{empty} \qquad \Delta;\Phi;\Gamma \vdash \mathsf{read}\ a\ k \ominus \mathsf{read}\ a\ k \lesssim 0 : \{\gamma \to \beta\}\ \overset{\mathrm{diff}(0)}{\exists\_ : \mathrm{int}}\ \{\gamma \to \beta\} \qquad \Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to \beta\}\ \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\exists\_ : \mathrm{unit}_r}\ \{\gamma \to \beta\}}{\Delta;\Phi;\Gamma, \{x : \mathrm{int}\} \vdash T \ominus T \lesssim 0 : \{\gamma \to \beta\}\ \overset{\mathrm{diff}(|\beta \cap [i,n]| * r)}{\exists\_ : \mathrm{unit}_r}\ \{\gamma \to \beta\}}\ \text{R-LET}$$

$$\dfrac{P_2 = \mathsf{empty} \qquad \Delta;\Phi;\Gamma \vdash \mathsf{updt}\ a\ k\ (f\ x) \ominus \mathsf{updt}\ a\ k\ (f\ x) \lesssim 0 : \{\gamma \to \beta\}\ \overset{\mathrm{diff}(0)}{\exists\_ : \mathrm{unit}_r}\ \{\gamma \to \beta\} \qquad \Delta;\Phi;\Gamma \vdash M \ominus M \lesssim 0 : \{\gamma \to \beta\}\ \overset{\mathrm{diff}(|\beta \cap [i+1,n]| * r)}{\exists\_ : \mathrm{unit}_r}\ \{\gamma \to \beta\}}{\Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to \beta\}\ \overset{\mathrm{diff}(|S \cap [i+1,n]| * r + 0)}{\exists\_ : \mathrm{unit}_r}\ \{\gamma \to \beta\}}\ \text{R-LET}$$

Because i not in β, we know: $|\beta \cap [i+1,n]| * r + 0 = |\beta \cap [i,n]|$.
The type of M is the same as we showed in previous case.

Type 2: Different functions :

$$\vdash \mathsf{InPlaceMap} \ominus \mathsf{InPlaceMap} \lesssim 0 : \begin{array}{l} \forall r:\mathbb{N}.(\tau \xrightarrow{\mathrm{diff}((r))} \tau) \longrightarrow \forall n:\mathbb{N}.\ \forall i:\mathbb{N}.\ \forall \gamma:\mathbb{L}.\ \forall \beta:\mathbb{P}. \\ (i \le n) \supset \left(\mathsf{Array}_\gamma[n]\ \tau \longrightarrow \mathrm{int}[i] \longrightarrow \{\gamma \to \beta\}\ \mathrm{unit}\ \{\gamma \to \beta \cup [i,n]\}\right) \end{array}$$

Let start with read and update from index k.

$$\frac{\Delta;\Phi;\Gamma \vdash a \ominus a \lesssim 0 : \mathsf{Array}_\gamma[n]\ \tau \qquad \Delta;\Phi;\Gamma \vdash k \ominus k \lesssim 0 : \mathrm{int}[i] \qquad \Delta;\Phi \models i \le n \qquad \Delta;\vdash \mathsf{empty} \quad wf}{\Delta;\Phi;\Gamma \vdash \mathsf{read}\ a\ k \ominus \mathsf{read}\ a\ k \lesssim 0 : \{\gamma \to \beta\}\ \exists\_.\tau^{\mathrm{diff}(0)}\ \{\gamma \to \beta\}}\ \text{R-R}$$

and

$$\frac{\Delta;\Phi;\Gamma \vdash a \ominus a \lesssim 0 : \mathsf{Array}_\gamma[n]\ \tau \qquad \Delta;\Phi;\Gamma \vdash k \ominus k \lesssim 0 : \mathrm{int}[i] \qquad \Delta;\Phi;\Gamma, x:\tau \vdash f\ x \ominus f\ x \lesssim r:\tau \qquad \Delta;\Phi \models i \le n \qquad \Delta;\vdash \mathsf{empty} \quad wf}{\Delta;\Phi;\Gamma \vdash \mathsf{updt}\ a\ k\ (f\ x) \ominus \mathsf{updt}\ a\ k\ (f\ x) \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(r)}\ \{\gamma \to \beta \cup \{i\}\}}\ \text{R-U}$$

where $\Delta = n:\mathbb{N}, i:\mathbb{N}, r:\mathbb{R}$
$\Sigma = \gamma:\mathbb{L}$
$\Phi = i \le n$
$\Gamma = a{:}\mathsf{Array}_\gamma[n]\ \tau, k:\mathrm{int}[i], f:(\tau \xrightarrow{\mathrm{diff}((r))} \tau)$,
$map:(\tau \xrightarrow{\mathrm{diff}((r))} \tau) \to \forall n,i,\gamma,\beta.(i \le n) \supset \left(\mathsf{Array}_\gamma[n]\ \tau \to \mathrm{int}[i] \to \mathrm{int}[n]\ \{\gamma \to \beta\}\ \mathrm{unit}^{\mathrm{diff}((n-i)*r)}\ \{\gamma \to \beta \cup [i,n]\}\right)$.

We will show:

$$\frac{\dfrac{\text{S-RM}}{\models \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(0)}\ \{\gamma \to \beta\} \sqsubseteq \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(|\beta \cap [i,n]|*r)}\ \{\gamma \to \beta \cup [i,n]\}} \qquad \Delta;\Phi;\Gamma \vdash \mathsf{return}\ () \ominus \mathsf{return}\ () \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(0)}\ \{\gamma \to \beta\}}{\Delta;\Phi;\Gamma \vdash \mathsf{return}\ () \ominus \mathsf{return}\ () \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(|\beta \cap [i,n]|*r)}\ \{\gamma \to \beta \cup [i,n]\}}\ \text{R-EXEC}$$

$$\frac{\Delta;\Phi;\Gamma \vdash k < n \ominus k < n \lesssim 0 : \mathrm{unit} + \mathrm{unit} \qquad \Delta;\Phi;\Gamma \vdash\ T \ominus\ T \lesssim 0 : \{\gamma \to S\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(|\beta \cap [i,n]|*r)}\ \{\gamma \to \beta \cup [i,n]\}}{\Delta;\Phi;\Gamma, \{x:\tau\} \vdash V \ominus V \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(|\beta \cap [i,n]|*r)}\ \{\gamma \to \beta \cup [i,n]\}}\ \text{R-CASE}$$

Using R-Let rules,instantiate P_1 with $\{\gamma \to \beta\}$ and $P_2 = \mathsf{empty}, Q = \{\gamma \to \beta \cup [i,n]\}$, we get

$$\frac{\Delta;\Phi;\Gamma \vdash \mathsf{read}\ a\ k \ominus \mathsf{read}\ a\ k \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \mathrm{int}^{\mathrm{diff}(0)}\ \{\gamma \to \beta\} \qquad \Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(|\beta \cap [i,n]|*r)}\ \{\gamma \to \beta \cup [i,n]\}}{\Delta;\Phi;\Gamma, \{x:\mathrm{int}\} \vdash T \ominus T \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(|\beta \cap [i,n]|*r)}\ \{\gamma \to \beta \cup [i,n]\}}\ \text{R-LET}$$

Because we know: $(\beta \cup \{i\}) \cap [i+1,n] = \beta \cap [i+1,n]$ and $\beta \cup \{i\} \cup [i+1,n] = \beta \cup [i,n]$.
Using R-Let rules,instantiate P_1 with $\{\gamma \to \beta\}$ and $P_2 = \mathsf{empty}, Q_1 = \{\gamma \to \beta \cup \{i\}\}, Q_2 = \mathsf{empty}, Q = \{\gamma \to \beta \cup \{i\} \cup [i+1,n]\}$, we get

$$\frac{\Delta;\Phi;\Gamma \vdash \mathsf{updt}\ a\ k\ (f\ x) \ominus \mathsf{updt}\ a\ k\ (f\ x) \lesssim 0 : \{\gamma \to \beta\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(r)}\ \{\gamma \to \beta \cup \{i\}\} \qquad \Delta;\Phi;\Gamma \vdash M \ominus M \lesssim 0 : \{\gamma \to \beta \cup \{i\}\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(|(\beta \cup \{i\}) \cap [i+1,n]|*r)}\ \{\gamma \to \beta \cup \{i\} \cup [i+1,n]\}}{\Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to S\}\ \exists\_ : \mathrm{unit}_r^{\mathrm{diff}(|\beta \cap [i+1,n]|*r+r)}\ \{\gamma \to \beta \cup [i,n]\}}\ \text{R-LET}$$

We want to show the typing of M. By applying $R-IApp$, instantiating β with $\beta \cup \{i\}$ and i with $i+1$. Then apply $R-App$ (instantiating k with $k+1$) several times, we can easily get

$$\Delta;\Phi;\Gamma \vdash (\mathsf{celim}(\mathsf{map}\, f)\, a\, (k+1)\, n) \ominus (\mathsf{celim}(\mathsf{map}\, f)\, a\, (k+1)\, n) \lesssim 0 : \{\gamma \to \beta \cup \{i\}\} \exists\_ : \mathrm{unit}_{r}^{\mathrm{diff}(|\beta \cap [i+1,n]| * r)} \{\gamma \to \beta \cup [i,n]\}$$

When apply $R-Celim$, We also check the constraint $i+1 \leq n$.

3.2 MergeSort

$$
\begin{array}{l}
\mathsf{copy} = \mathsf{fix}\ cp\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda x.\lambda y.\lambda l.\lambda u. \\
\quad \mathsf{if}\ l \le u\ \mathsf{then} \\
\qquad \mathsf{let}\ \{a\} = \big(\ \mathsf{read}\ x\ l\ \big)\ \mathsf{in} \\
\qquad \mathsf{let}\{\_\} = \big(\ \mathsf{updt}\ y\ l\ a\ \big)\ \mathsf{in} \\
\quad \big(\mathsf{celim}(cp()\ []\ []\ []\ []\ [])\ x\ y\ (l+1)\ u\big) \\
\quad \mathsf{else}\ \ \mathsf{return}()
\end{array}
$$

Type 1: copy $S \cap [l,u] = \emptyset$

$$
\vdash \mathsf{copy} \ominus \mathsf{copy} \lesssim 0 : \quad
\begin{array}{l}
\forall n, L, U, \gamma_1, \gamma_2, S, S'.\ L \le U \le n \wedge S' \cap [L,U] = \emptyset \supset \\
\mathsf{Array}_{\gamma_1}[n]\ U(\mathrm{int},\mathrm{int}) \to \mathsf{Array}_{\gamma_2}[n]\ U(\mathrm{int},\mathrm{int}) \\
\to \mathrm{int}[L] \to \mathrm{int}[U] \to \{\gamma_1 \to S, \gamma_2 \to S'\}\ \overset{\mathrm{diff}(0)}{\exists}\_.\mathrm{unit}\ \{\gamma_1 \to S, \gamma_2 \to \mathbb{N}\}
\end{array}
$$

Type 2: copy $S \cap [l,u] \neq \emptyset$

$$
\vdash \mathsf{copy} \ominus \mathsf{copy} \lesssim 0 : \quad
\begin{array}{l}
\forall n, L, U, \gamma_1, \gamma_2, S.\ L \le U \le n \supset \mathsf{Array}_{\gamma_1}[n]\ U(\mathrm{int},\mathrm{int}) \to \mathsf{Array}_{\gamma_2}[n]\ U(\mathrm{int},\mathrm{int}) \\
\to \mathrm{int}[L] \to \mathrm{int}[U] \to \{\gamma_1 \to S, \gamma_2 \to \mathbb{N}\}\ \overset{\mathrm{diff}(0)}{\exists}\_.\mathrm{unit}\ \{\gamma_1 \to S \cup [L,U], \gamma_2 \to \mathbb{N}\}
\end{array}
$$

$$
\begin{array}{l}
\mathsf{merge_{lp}} = \mathsf{fix\ mg\ (\_).}\lambda.(k:\mathrm{int}[K]).\lambda a{:}\mathsf{Array}_{\gamma_1}[n]\ \mathrm{int}\,. \\
\quad \lambda l_s:\mathrm{int}[i], \lambda l_e:\mathrm{int}[j], \lambda r_s:\mathrm{int}[m], \lambda r_e:\mathrm{int}[u].\lambda b{:}\mathsf{Array}_{\gamma_2}[n]\ \mathrm{int}\,. \\
\quad \mathsf{if}\ l_s < l_e\ \mathsf{then} \\
\quad\ \mathsf{if}\ r_s < r_e\ \mathsf{then} \\
\quad\quad \mathsf{let}\ \{x\} = (\mathsf{read}\ a\ l_s)\ \mathsf{in} \\
\quad\quad\ \mathsf{let}\ \{y\} = (\mathsf{read}\ a\ r_s)\ \mathsf{in} \\
\quad\quad\quad \mathsf{if}\, x < y\, \mathsf{then} \\
\quad\quad\quad\quad \Big(\mathsf{let}\ \{\_\} = (\mathsf{updt}\ b\ k\ x)\ \mathsf{in} \\
\quad\quad\quad\quad\quad \big((\mathsf{celim\,mg}\ ()\ (k+1))\ a\ (l_s+1)\ l_e\ r_s\ r_e\ b\big)\Big) \\
\quad\quad\quad\quad \mathsf{else} \\
\quad\quad\quad\quad \Big(\mathsf{let}\ \{\_\} = (\mathsf{updt}\ b\ k\ y)\ \mathsf{in} \\
\quad\quad\quad\quad\quad \big((\mathsf{celim\,mg}\ ()\ (k+1))\ a\ l_s\ l_e\ (r_s+1)\ r_e,\ b\big)\Big) \\
\quad\quad \mathsf{else} \\
\quad\quad\ \Big(\mathsf{let}\{x\} = (\mathsf{read}\ a\ l_s)\ \mathsf{in} \\
\quad\quad\quad \mathsf{let}\{\_\} = (\mathsf{updt}\ b\ k\ x)\ \mathsf{in} \\
\quad\quad\quad\quad \big((\mathsf{celim\,mg}\ ()\ (k+1))\ a\ (l_s+1)\ l_e\ r_s\ r_e\ b\big)\Big) \\
\quad \mathsf{else} \\
\quad\quad \mathsf{if}\, r_s < r_e \\
\quad\quad\quad \Big(\mathsf{let}\{x\} = (\mathsf{read}\ a\ r_s)\ \mathsf{in} \\
\quad\quad\quad\quad \mathsf{let}\{\_\} = (\mathsf{updt}\ b\ k\ x)\ \mathsf{in} \\
\quad\quad\quad\quad\quad \big((\mathsf{celim\,mg}\ ()\ (k+1))\ a\ l_s\ l_e\ (r_s+1)\ r_e\ b\big)\Big) \\
\quad\quad \mathsf{else}\,(\mathsf{return}())
\end{array}
$$

$$
\begin{array}{l}
\vdash \mathsf{merge_{lp}}: \\
\end{array}
\begin{array}{l}
\forall n, l_s, l_e, r_s, r_e, K, \gamma, \gamma'. l_s \le l_e \le r_s \le r_e \le n \supset \mathrm{unit}_r \to \mathrm{int}[K] \to \mathsf{Array}_{\gamma}[n]\ \mathrm{int} \to \mathrm{int}[l_s] \to \\
\mathrm{int}[l_e] \to \mathrm{int}[r_s] \to \mathrm{int}[r_e] \to \mathsf{Array}_{\gamma'}[n]\ \mathrm{int} \to \{\gamma \to \emptyset, \gamma' \xrightarrow{\mathrm{exec}(U,L)} [K, r_e]\}\ \exists\_.\mathrm{unit}\ \{\gamma, \gamma'\}
\end{array}
$$

$L = (c_r + c_r + c_u) * min(l_e - l_s, r_e - r_s) + (c_r + c_u) * max(l_e - l_r, r_e - e_s)$
$U = (c_r + c_r + c_u) * ((l_e - l_s) + (r_e - r_s))$

In $\mathsf{merge_{lp}}$, we have 4 positions in the input array, l_s, l_e indicating the left part of the array, r_s, r_e for right part. we need to merge the two part, which means total $(l_e - l_s)$ elements for left part of the input array and $(r_e - r_s)$ elements for right part. In the body of $merge_{lp}$, for every element to be merged and added to the buffer array, there are two possible different branches: in one branch (if $l_s < l_e \wedge r_s < r_e$, which means we still have elements waiting to be merged in both left and right parts), the cost will be $c_r + c_r + c_u$, c_r for the cost of read from the input array, c_u for the cost of updating the buffer array. in the other branch, (either $l_s < l_e$ or $r_s < r_e$, we need to only merge one part into buffer array), the cost is $c_r + c_u$.

For the L, the minimal possible cost is that we run out the shorter part ($min(l_e - l_s, r_e - r_s)$) with the cost of $c_r + c_r + c_u$ first and then merge the rest part with the cost of $c_r + c_u$. For the maximal cost, merge all the elements with the cost of $c_r + c_r + c_u$. If we consider the cost for update as 1 unit cost and cost for read is 1 unit cost, $c_r + c_r + c_u = 3, c_r + c_u = 2$.

Type 1: mergeLp $S \cap [K, r_e] = \emptyset$

$$\vdash \mathsf{merge_{lp}} \ominus \mathsf{merge_{lp}} \lesssim 0 : \begin{array}{l} \forall n, l_s, l_e, r_s, r_e, K, \gamma, \gamma'. l_s \le l_e \le r_s \le r_e \le n \wedge S \cap [K, r_e] = \emptyset \\ \supset \mathrm{unit}_r \to \mathrm{int}[K] \to \mathsf{Array}_{\gamma}[n]\ U(\mathrm{int}, \mathrm{int}) \to \mathrm{int}[l_s] \to \mathrm{int}[l_e] \to \mathrm{int}[r_s] \\ \to \mathrm{int}[r_e] \to \mathsf{Array}_{\gamma'}[n]\ U(\mathrm{int}, \mathrm{int}) \\ \to \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_.\overset{\mathrm{diff}(0)}{\mathrm{unit}}\ \{\gamma \to S, \gamma' \to \mathbb{N} \setminus [l, u]\} \end{array}$$

Because in the range $[K, r_e]$, all the values in the two arrays are exact the same, the two programs will go to the same branch for every step.
In the read rule, i equals to either l_s or r_s.

$$\frac{\begin{array}{c} \Delta; \Phi; \Gamma \vdash a \ominus a \lesssim 0 : \mathsf{Array}_{\gamma}[n]\ \tau \\ \Delta; \Phi; \Gamma \vdash l_s[r_s] \ominus l_s[r_s] \lesssim 0 : \mathrm{int}[i] \qquad \Delta; \Phi \models i \le n \qquad \Delta; \Phi \vdash \mathsf{empty} \quad wf \end{array}}{\Delta; \Phi; \Gamma \vdash \mathsf{read}\ a\ l_s[r_s] \ominus \mathsf{read}\ a\ l_s[r_s] \lesssim 0 : \{\gamma \to S\}\ \exists\_.\overset{\mathrm{diff}(0)}{\tau}\ \{\gamma \to S\}}\ \text{R-R}$$

and

$$\frac{\begin{array}{c} \Delta; \Phi; \Gamma \vdash b \ominus b \lesssim 0 : \mathsf{Array}_{\gamma'}[n]\ \tau \\ \Delta; \Phi; \Gamma \vdash k \ominus k \lesssim 0 : \mathrm{int}[i] \qquad \Delta; \Phi; \Gamma, x : \tau \vdash x \ominus x \lesssim 0 : \mathrm{int} \qquad \Delta; \Phi \models i \le n \qquad \Delta; \Phi \vdash \mathsf{empty} \quad wf \end{array}}{\Delta; \Phi; \Gamma \vdash \mathsf{updt}\ b\ k\ x[y] \ominus \mathsf{updt}\ b\ k\ x[y] \lesssim 0 : \{\gamma' \to N\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma' \to N \cup [i]\}}\ \text{R-U}$$

Using R-Case for two times, we have four similar cases, we will have a look at one of them.

$$\Delta; \Phi; \Gamma \vdash (\mathsf{celim}(\mathsf{mg}\ ())\ k + 1\ a\ (l_s + 1)\ l_e\ r_s\ r_s \ominus (\mathsf{celim}(\mathsf{mg}\ ())\ k + 1\ a\ (l_s + 1)\ l_e\ r_s\ r_s \lesssim 0 :$$

Its type is $\{\gamma \to S, \gamma' \to N\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma' \to N\}$. By applying $R-Celim$ to check the constraint and then applying $R-Iapp$ and $R-App$ for several times.

Type 2: mergeLp $S \cap [K, r_e] \neq \emptyset$

Because if $S \cap [K, r_e] \neq \emptyset$, $merge_{lp}$ in the two runs are likely to go into different branches at any step, We will use R-S to handle this cases because the two runs are likely to go to different branches in every step.

$$\frac{\begin{array}{c} \Delta; \Phi; |\Gamma|_1 \vdash^0_0 \mathsf{merge_{lp}}\ ()\ k\ a\ l_s\ l_e\ r_s\ r_e\ b : \{\gamma \to \emptyset, \gamma' \to \overset{\mathrm{exec}(L,U)}{[K, r_e]}\}\ \exists\_ : \mathrm{unit}\ \{\gamma, \gamma'\} \\ \Delta; \Phi; |\Gamma|_2 \vdash^0_0 \mathsf{merge_{lp}}\ ()\ k\ a\ l_s\ l_e\ r_s\ r_e\ b : \{\gamma \to \emptyset, \gamma' \to \overset{\mathrm{exec}(L,U)}{[K, r_e]}\}\ \exists\_ : \mathrm{unit}\ \{\gamma, \gamma'\} \end{array}}{\begin{array}{c} \Delta; \Phi; \Gamma \vdash \mathsf{merge_{lp}}\ ()\ k\ a\ l_s\ l_e\ r_s\ r_e\ b \ominus \mathsf{merge_{lp}}\ ()\ k\ a\ l_s\ l_e\ r_s\ r_e\ b \lesssim 0 : \\ U(\{\gamma \to \emptyset, \gamma' \to \overset{\mathrm{exec}(L,U)}{[K, r_e]}\}\ \exists\_ : \mathrm{unit}\ \{\gamma, \gamma'\}, \{\gamma \to \emptyset, \gamma' \to \overset{\mathrm{exec}(L,U)}{[K, r_e]}\}\ \exists\_ : \mathrm{unit}\ \{\gamma, \gamma'\}) \end{array}}\ \text{R-S}$$

and we know from S-RUM.

$$\begin{array}{c} \models U(\{\gamma, \gamma' \to \overset{\mathrm{exec}(L,U)}{[K, r_e]}\}\ \exists\_ : \mathrm{unit}\ \{\gamma, \gamma'\}, \{\gamma, \gamma' \to \overset{\mathrm{exec}(L,U)}{[L, U]}\}\ \exists\_ : \mathrm{unit}\ \{\gamma, \gamma'\}) \sqsubseteq \\ \{\gamma \to S, \gamma' \to S'\}\ \exists\_ : \overset{\mathrm{diff}(U-L)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma' \to S' \cup [K, r_e]\} \end{array}$$

$$\vdash \mathsf{merge_{lp}} \ominus \mathsf{merge_{lp}} \lesssim 0 : \begin{array}{l} \forall n, l_s, l_e, r_s, r_e, K, \gamma, \gamma'. l_s \le l_e \le r_s \le r_e \le n \supset \mathrm{unit}_r \to \mathrm{int}[K] \to \mathsf{Array}_{\gamma}[n]\ U(\mathrm{int}, \mathrm{int}) \\ \to \mathrm{int}[l_s] \to \mathrm{int}[l_e] \to \mathrm{int}[r_s] \to \mathrm{int}[r_e] \to \mathsf{Array}_{\gamma'}[n]\ U(\mathrm{int}, \mathrm{int}) \\ \to \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_.\overset{\mathrm{diff}((U-L))}{\mathrm{unit}}\ \{\gamma \to S, \gamma' \to \mathbb{N} \cup [K, r_e]\} \end{array}$$

Function merge

$$\begin{aligned}\mathsf{merge} = \lambda a.\lambda b.\lambda l.\lambda u.\lambda mid.\\ &\mathsf{let}\ \{\_\} = \big(celim\ (merge_{lp}\ ()\ l)\ a\ l\ mid\ mid+1\ u\ b\big)\ \mathsf{in}\\ &\big(celim\ \mathsf{copy}\ l\ )\ a\ b\ u\big).\end{aligned}$$

Type 1: merge $S \cap [K, r_e] = \emptyset \rightarrow S \cap [l,u] = \emptyset$

$$\begin{aligned}\vdash \mathsf{merge} \ominus \mathsf{merge} \lesssim 0 : \ & \forall n,l,m,u,\gamma,\gamma', S.l \le m \le u \le n \wedge S \cap [l,u] = \emptyset \supset \mathsf{Array}_{\gamma}[n]\ U(\mathrm{int},\mathrm{int}) \rightarrow \\ & \mathsf{Array}_{\gamma'}[n]\ U(\mathrm{int},\mathrm{int}) \rightarrow \mathrm{int}[l] \rightarrow \mathrm{int}[m] \rightarrow \mathrm{int}[u] \rightarrow \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}\ \overset{\mathrm{diff}(0)}{\exists\_.\mathrm{unit}}\ \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}\end{aligned}$$

R-LET

$$\begin{aligned}&\vdash celim\ merge_{lp}\ l\ a\ l\ m\ (m+1)\ u\ b \ominus celim\ merge_{lp}\ l\ a\ l\ m\ (m+1)\ u\ b \lesssim 0 :\\ &\qquad \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}\ \overset{\mathrm{diff}(0)}{\exists\_.\mathrm{unit}}\ \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N} \setminus [l,u]\}\end{aligned}$$

$$\frac{\Delta;\Phi;\Gamma \vdash \mathsf{celim\ copy}\ l\ a\ b\ u \ominus \mathsf{celim\ copy}\ l\ a\ b\ u \lesssim 0 : \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N} \setminus [l,u]\}\ \overset{\mathrm{diff}(0)}{\exists\_.\mathrm{unit}}\ \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N} \setminus [l,u]\}}{\Delta;\Phi;\Gamma \vdash \mathsf{merge}\ a\ b\ l\ m\ u \ominus \mathsf{merge}\ a\ b\ l\ m\ u \lesssim 0 : \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}\ \overset{\mathrm{diff}(0)}{\exists\_.\mathrm{unit}}\ \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}}$$

we know: $\models \mathbb{N}/[l,u] \sqsubseteq \mathbb{N}$, By S-RM, we can get the post condition of $merge$ to be

$$\{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}$$

Type 2:merge $S \cap [K, r_e] \neq \emptyset \rightarrow S \cap [l,u] \neq \emptyset$

$$\begin{aligned}\vdash \mathsf{merge} \ominus \mathsf{merge} \lesssim 0 : \ & \forall n,l,m,u,\gamma,\gamma', S.l \le m \le u \le n \supset \mathsf{Array}_{\gamma}[n]\ U(\mathrm{int},\mathrm{int}) \rightarrow \mathsf{Array}_{\gamma'}[n]\ U(\mathrm{int},\mathrm{int}) \rightarrow \mathrm{int}[l] \rightarrow \\ & \mathrm{int}[m] \rightarrow \mathrm{int}[u] \rightarrow \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}\ \overset{\mathrm{diff}(max(m-l,u-(m+1)))}{\exists\_.\mathrm{unit}}\ \{\gamma \rightarrow S \cup [l,u], \gamma' \rightarrow \mathbb{N}\}\end{aligned}$$

R-LET

$$\begin{aligned}&\Delta;\Phi;\Gamma \vdash \mathsf{celim\ merge_{lp}}\ l\ a\ l\ m\ (m+1)\ u\ b \ominus \mathsf{celim\ merge_{lp}}\ l\ a\ l\ m\ (m+1)\ u\ b \lesssim 0 :\\ &\qquad \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}\ \overset{\mathrm{diff}(max(m-l,u-(m+1)))}{\exists\_.\mathrm{unit}}\ \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N} \cup [l,u]\}\end{aligned}$$

$$\frac{\Delta;\Phi;\Gamma \vdash \mathsf{celim}\ copy\ l\ a\ b\ u \ominus \mathsf{celim}\ copy\ l\ a\ b\ u \lesssim 0 : \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}\ \overset{\mathrm{diff}(0)}{\exists\_.\mathrm{unit}}\ \{\gamma \rightarrow S \cup [l,u], \gamma' \rightarrow \mathbb{N}\}}{\Delta;\Phi;\Gamma \vdash \mathsf{merge}\ a\ b\ l\ m\ u \ominus \mathsf{merge}\ a\ b\ l\ m\ u \lesssim 0 : \{\gamma \rightarrow S, \gamma' \rightarrow \mathbb{N}\}\ \overset{\mathrm{diff}(max(m-l,u-(m+1)))}{\exists\_.\mathrm{unit}}\ \{\gamma \rightarrow S \cup [l,u], \gamma' \rightarrow \mathbb{N}\}}$$

msort

$$\begin{aligned}\mathsf{msort} = \ & \mathsf{fix\ sort}\ (a{:}\mathsf{Array}_{\gamma_1}[n]\ \tau)\ b{:}\mathsf{Array}_{\gamma_2}[n]\ \tau\ .\lambda l.\lambda u.\\ & \mathsf{if}\ (l \ge u)\ \mathsf{then}\\ & \quad \big(\mathsf{return}()\big)\\ & \mathsf{else}\ \Big(\\ & \quad \mathsf{let}\ \_ = \big(celim\ (sort)\ a\ b\ l\ (l + \lfloor (u-l)/2 \rfloor)\big)\ \mathsf{in}\\ & \quad\quad \mathsf{let}\ \_ = \big(celim\ (sort)\ a\ b\ (l + \lfloor (u-l)/2 \rfloor + 1)\ u\big)\ \mathsf{in}\\ & \quad\quad\quad \big(celim\ merge\ a\ b\ l\ (l + \lfloor (u-l)/2 \rfloor)\ u\big)\Big)\end{aligned}$$

$$\begin{aligned}\vdash \quad \mathsf{msort} \quad : \ & \forall n,l,u,\gamma,\gamma'.l \le u \le n \supset \mathsf{Array}_{\gamma}[n]\ \mathrm{int} \\ & \rightarrow \mathrm{int}[l] \rightarrow \mathrm{int}[u] \rightarrow \mathsf{Array}_{\gamma'}[n]\ \mathrm{int} \rightarrow \{\gamma \rightarrow [l,u], \gamma' \rightarrow [l,u]\}\ \overset{\mathrm{exec}(0,(u-l)*log(u-l))}{\exists\_.\mathrm{unit}}\ \{\gamma, \gamma'\}\end{aligned}$$

Let us call M the following term:

$$\mathsf{celim}\ merge\ a\ b\ l\ (l+\lfloor (u-l)/2 \rfloor)\ u$$

and call $S1$ the following term:

$$\mathsf{celim}\ (sort)\ a\ b\ l\ l+\lfloor (u-l)/2 \rfloor$$

and call $S2$ the following term:

$$\mathsf{celim}\ (sort)\ a\ b\ l+\lfloor (u-l)/2 \rfloor+1\ u$$

and call Z the following term:

$$\mathsf{let\_} = S1\ \mathsf{in}\ \ \mathsf{let}\ \_ = S2\ \mathsf{in}\ M$$

and set V as:

$$\mathsf{if}\ l = u, \mathsf{then}\ (\mathsf{return}\ ())\mathsf{else}\ Z$$

Type 1: msort $S \cap [l,u] = \emptyset$

$$\vdash \mathsf{msort} \ominus \mathsf{msort} \lesssim 0 : \begin{array}{l} \forall n,l,u,\gamma,\gamma' : \mathbb{N}, S.l \le u \le n \wedge S \cap [l,u] = \emptyset \supset \mathsf{Array}_{\gamma}[n]\ U(\mathrm{int},\mathrm{int}) \to \mathrm{int}[l] \to \mathrm{int}[u] \\ \to \mathsf{Array}_{\gamma'}[n]\ U(\mathrm{int},\mathrm{int}) \to \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_.\overset{\mathrm{diff}(0)}{\mathrm{unit}}\ \{\gamma \to S, \gamma' \to \mathbb{N}\} \end{array}$$

$$\dfrac{\begin{array}{c} \Delta;\Phi;\Gamma \vdash S2 \ominus S2 \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma \to \mathbb{N}\} \\ \Delta;\Phi;\Gamma \vdash M \ominus M \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma \to \mathbb{N}\} \qquad P_2 = \mathsf{empty} \end{array}}{\begin{array}{c} \Delta;\Phi;\Gamma \vdash let\_ = S2\ in\ M \ominus let\_ = S2\ in M \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma \to \mathbb{N}\} \end{array}}\ \text{R-LET}$$

$$\dfrac{\begin{array}{c} \Delta;\Phi;\Gamma \vdash S1 \ominus S1 \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma \to \mathbb{N}\} \qquad P_2 = \mathsf{empty} \end{array}}{\begin{array}{c} \Delta;\Phi;\Gamma \vdash let\_ = S2\ in\ M \ominus let\_ = S2\ in M \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma \to \mathbb{N}\} \end{array}}\ \text{R-LET}$$

$$\dfrac{\begin{array}{c} \Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma \to \mathbb{N}\} \\ \Delta;\Phi;\Gamma \vdash l = u \ominus l = u \lesssim 0 : \mathrm{unit} + \mathrm{unit} \\ \Delta;\Phi;\Gamma \vdash\ \mathsf{return}\ () \ominus \mathsf{return}\ () \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma \to \mathbb{N}\} \end{array}}{\begin{array}{c} \Delta;\Phi;\Gamma \vdash V \ominus V \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma \to \mathbb{N}\} \end{array}}\ \text{R-CASE}$$

Type 2: msort $S \cap [l,u] \neq \emptyset$

$$\vdash \mathsf{msort} \ominus \mathsf{msort} \lesssim 0 : \begin{array}{l} \forall n,l,u,\gamma,\gamma' : \mathbb{N}, S.l \le u \le n \supset \mathsf{Array}_{\gamma}[n]\ U(\mathrm{int},\mathrm{int}) \to \mathrm{int}[l] \to \mathrm{int}[u] \\ \to \mathsf{Array}_{\gamma'}[n]\ U(\mathrm{int},\mathrm{int}) \to \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_.\overset{\mathrm{diff}(Q(u-l+1,|S\cap[l,u]|))}{\mathrm{unit}}\ \{\gamma \to S \cup [l,u], \gamma' \to \mathbb{N}\} \end{array}$$

where
$Q(n,\alpha) = \Sigma_{i=0}^{H} h(\lceil 2^{i-1} \rceil).min(\alpha, 2^{H-i})$, $H = \lceil log_2(n) \rceil$

$$\dfrac{\dfrac{}{\models \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S, \gamma' \to \mathbb{N}\} \sqsubseteq \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(Q(u-l+1,|S\cap[l,u]|))}{\mathrm{unit}_r}\ \{\gamma \to S \cup [l,u], \gamma' \to \mathbb{N}\}}\ \text{S-RM}}{\begin{array}{c} \Delta;\Phi;\Gamma \vdash\ \mathsf{return}\ () \ominus\ \mathsf{return}\ () \lesssim 0 : \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(0)}{\mathrm{unit}_r}\ \{\gamma \to S \cup [l,u], \gamma' \to \mathbb{N}\} \end{array}}\ \text{R-EXEC}$$

$$\dfrac{\begin{array}{c} \Delta;\Phi;\Gamma \vdash\ \mathsf{return}\ () \ominus \mathsf{return}\ () \lesssim 0 : \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(Q(u-l+1,|S\cap[l,u]|))}{\mathrm{unit}_r}\ \{\gamma \to S \cup [l,u], \gamma' \to \mathbb{N}\} \\ \Delta;\Phi;\Gamma \vdash l = u \ominus l = u \lesssim 0 : \mathrm{unit} + \mathrm{unit} \\ \Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(Q(u-l+1,|S\cap[l,u]|))}{\mathrm{unit}_r}\ \{\gamma \to S \cup [l,u], \gamma' \to \mathbb{N}\} \end{array}}{\begin{array}{c} \Delta;\Phi;\Gamma \vdash V \ominus V \lesssim 0 : \{\gamma \to S, \gamma' \to \mathbb{N}\}\ \exists\_ : \overset{\mathrm{diff}(Q(u-l+1,|S\cap[l,u]|))}{\mathrm{unit}_r}\ \{\gamma \to S \cup [l,u], \gamma' \to \mathbb{N}\} \end{array}}\ \text{R-CASE}$$

$$\frac{\begin{array}{c} P_2 = \mathsf{empty} \\ \Delta;\Phi;\Gamma \vdash S2 \ominus S2 \lesssim 0 : \{\gamma \to S \cup [l, \lfloor (u-l)/2 \rfloor], \gamma \to \mathbb{N}\}\ \exists\_ : \mathrm{unit}_r\ \{\gamma \to S \cup [l,u], \gamma \to \mathbb{N}\}^{\mathrm{diff}(Q(u-l-\lfloor (u-l)/2 \rfloor, |S \cap [l+\lfloor (u-l)/2 \rfloor + 1, u]|)} \\ \Delta;\Phi;\Gamma \vdash M \ominus M \lesssim 0 : \{\gamma \to S \cup [l,u], \gamma \to \mathbb{N}\}\ \exists\_ : \mathrm{unit}_r\ \{\gamma \to S \cup [l,u], \gamma \to \mathbb{N}\}^{\mathrm{diff}(max((l+\lfloor (u-l)/2 \rfloor) - l, u - ((l+\lfloor (u-l)/2 \rfloor)+1))} \end{array}}{\begin{array}{c} \Delta;\Phi;\Gamma \vdash let\_ = S2\ in\ M \ominus let\_ = S2\ in M \lesssim 0 : \\ \{\gamma \to S \cup [l, \lfloor (u-l)/2 \rfloor], \gamma \to \mathbb{N}\}\ \exists\_ : \mathrm{unit}_r\ \{\gamma \to S \cup [l,u], \gamma \to \mathbb{N}\}^{\mathrm{diff}(Q(u-l-\lfloor (u-l)/2 \rfloor, |S \cap [l+\lfloor (u-l)/2 \rfloor + 1, u]| + (u-l))} \end{array}}\ \text{R-LET}$$

$$\frac{\begin{array}{cc} P_2 = \mathsf{empty} & \Delta;\Phi;\Gamma \vdash S1 \ominus S1 \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \mathrm{unit}_r\ \{\gamma \to S \cup [l, \lfloor (u-l)/2 \rfloor], \gamma \to \mathbb{N}\}^{\mathrm{diff}(Q(\lfloor (u-l)/2 \rfloor + 1, |S \cap [l, l+\lfloor (u-l)/2 \rfloor]|))} \end{array}}{\Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma \to S, \gamma \to \mathbb{N}\}\ \exists\_ : \mathrm{unit}_r\ \{\gamma \to S \cup [l,u], \gamma \to \mathbb{N}\}^{\mathrm{diff}(Q(u-l+1, |S \cap [l,u]|))}}\ \text{R-LET}$$

If we simplify the relative cost for M, it is $max((\lfloor (u-l)/2 \rfloor), u-l-(\lfloor (u-l)/2 \rfloor)+1) = \lceil \frac{u-l}{2} \rceil$. Let us look at the simplified version of msort:

$$\begin{array}{rcl} msort(in,l,u,buf) & = & msort(in,l,l+\lfloor \frac{u-l}{2} \rfloor, buf); \\ & & msort(in,l+\lfloor \frac{u-l}{2} \rfloor + 1, u, buf); \\ & & merge(in,l,l+\lfloor \frac{u-l}{2} \rfloor + 1, u, buf). \end{array}$$

To show : $Q(\lfloor \frac{u-l}{2} \rfloor + 1, |S \cap [l, l+\lfloor \frac{u-l}{2} \rfloor]|) +$
$Q(u-l-\lfloor \frac{u-l}{2} \rfloor, |S \cap [l+\lfloor \frac{u-l}{2} \rfloor + 1, u]|) + \lceil \frac{u-l}{2} \rceil$
$\leq Q(u-l+1, |S \cap [l,u]|)$
Let us simplify the inequality with n=l-u, $\alpha = |S \cap [l, l+\lfloor \frac{u-l}{2} \rfloor}$ and $\beta = |S \cap [l+\lfloor \frac{u-l}{2} \rfloor + 1, u]|$:
$\lceil \frac{n}{2} \rceil + \mathrm{Q}(\lfloor \frac{n}{2} \rfloor, \alpha) + \mathrm{Q}(\lceil \frac{n}{2} \rceil, \beta) \leq \mathrm{Q}(\mathrm{n}, \alpha+\beta)$, it is arithmetically tautology
$\alpha + \beta \neq 0$ because $S \cap [l,u] \neq \emptyset$

3.3 Naive String Search

Description: Given a long text string S :$\mathsf{Array}_{\gamma_1}[N]$ int and a shorter substring W :$\mathsf{Array}_{\gamma_2}[M]$ int to be searched in S. There is an int array P :$\mathsf{Array}_{\gamma_3}[N]$ int which will store the matching result (1 as match, 0 as mismatch) for the same index as the text string. For example, for index 1, there is a match with W from index 1 in the text string S and $P[1] = 1$.

Helper function

Helper function will do the match process for one index m in s and update $p[m]$, i will start from 0 till the length of w (Q) if the prefix matches.

$$
\begin{array}{l}
\mathsf{search} = \mathsf{fix}\ f\ (\_).\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda s.\lambda w.\lambda m.\lambda i.\lambda l_w.\lambda p. \\
\quad \mathsf{let}\ \{a\} = \mathsf{read}\ s\ (m+i)\ \mathsf{in} \\
\quad \mathsf{let}\ \{b\} = \mathsf{read}\ w\ i\ \mathsf{in} \\
\quad\quad \mathsf{if}\ (i+1) == l_w\ \mathsf{then} \\
\quad\quad\quad \mathsf{if}\ \ a == b\ \mathsf{then} \ldots (1) \\
\quad\quad\quad\quad \mathsf{updt}\ p\ m\ 1 \\
\quad\quad\quad \mathsf{else} \\
\quad\quad\quad\quad \mathsf{updt}\ p\ m\ 0 \\
\quad\quad \mathsf{else} \\
\quad\quad\quad \mathsf{if}\ \ a == b\ \mathsf{then} \ldots (2) \\
\quad\quad\quad\quad \mathsf{celim}\ (f\ ()\ []\ []\ []\ []\ []\ []\ [])\ w\ m\ (i+1)\ l_w\ p \\
\quad\quad\quad \mathsf{else} \\
\quad\quad\quad\quad \mathsf{updt}\ p\ m\ 0
\end{array}
$$

$$
\begin{array}{rll}
\vdash & \mathsf{search} & : \\
 & & \mathrm{unit} \to \forall \gamma_1, \gamma_2, \gamma_3 : \mathbb{L}. \forall I, M, Q, N : \mathbb{N}. (I < Q < N \wedge M + I < N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \\
 & & \mathsf{Array}_{\gamma_2}[Q]\ \mathrm{int} \to \mathrm{int}[M] \to \mathrm{int}[I] \to \mathrm{int}[Q] \to \mathsf{Array}_{\gamma_3}[N]\ \mathrm{int} \to \\
 & & \overset{\mathrm{exec}(c_u + r, (Q-I) * r + c_u)}{\{\gamma_1 \to \emptyset, \gamma_2 \to \emptyset, \gamma_3 \to \{M\}\}\ \exists \_.\mathrm{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \emptyset, \gamma_3 \to \{M\}\}}
\end{array}
$$

Notice, one thing to mention is that in the unary type, in the precondition, $\gamma_3 \to \{M\}$, it means before helper is executed, it can only touch position M in p.

Where r is the cost of two reads and c_u is the cost for update, w has length Q, s,p have length N.

$$
\begin{array}{rll}
\vdash \mathsf{search} \ominus \mathsf{search} \lesssim 0 : & & \mathrm{unit}_r \to \forall \gamma_1, \gamma_2, \gamma_3 : \mathbb{L}. \forall I, M, Q, N : \mathbb{N}. \forall \beta_2, \beta_3. (I < Q < N \wedge M + I < N) \subset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \\
 & & \to \mathsf{Array}_{\gamma_2}[Q]\ \mathrm{int} \to \mathrm{int}[M] \to \mathrm{int}[I] \to \mathrm{int}[N] \to \mathrm{int}[Q] \to \mathsf{Array}_{\gamma_3}[N]\ \mathrm{int} \to \\
 & & \overset{\mathrm{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)), Q-1)) * r)}{\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists \_.\mathrm{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}}
\end{array}
$$

where $MIN(beta : set)$ return the minimum element in the set $beta$.

First, we will apply rule R-Fix-Ext.

Set $\sigma = \mathrm{unit} \to \forall \gamma_1, \cdots \overset{\mathrm{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)), Q-1)) * r)}{\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists \_.\mathrm{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}}$.

Set $A_1 = A_2 = \mathrm{unit} \to \forall \gamma_1 \gamma_2, \gamma_3 : \mathbb{L}. \forall I, M, Q, N : \mathbb{N}. (I < Q < N \wedge M + I < N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to$
$\mathsf{Array}_{\gamma_2}[Q]\ \mathrm{int} \to \mathrm{int}[M] \to \mathrm{int}[I] \to \mathrm{int}[Q] \to \mathsf{Array}_{\gamma_3}[N]\ \mathrm{int} \to \overset{\mathrm{exec}(c_u, (Q-I-1) * r + c_u)}{\{\gamma_3 \to \{M\}\ \exists \_.\mathrm{unit}\ \{\gamma_3 \to \{M\}\}}$.

Set $\Gamma = \_ : \text{unit}, f : \text{unit} \xrightarrow{\text{diff}(0)} \sigma, f\ U(A_1, A_2)$

$$\frac{\Gamma \vdash \Lambda.\ldots.\lambda s.\ldots.\ominus \Lambda.\ldots.\lambda s.\ldots. \lesssim 0 : \sigma \quad |\Gamma|_1 \vdash_0^0 \mathsf{Fix}\, f(\_).\Lambda.\ldots.\lambda s.\ldots. : A_1 \qquad |\Gamma|_2 \vdash_0^0 \mathsf{Fix}\, f(\_).\Lambda.\ldots.\lambda s.\ldots. : A_2}{\Gamma \vdash \mathsf{Fix}\, f(\_).\Lambda.\ldots. \ominus \mathsf{Fix}\, f(\_).\Lambda.\ldots. \lesssim 0 : \text{unit} \xrightarrow{\text{diff}(0)} \sigma}\ \text{R-FIX-EXT}$$

We first show how do we get the unary type A_1.

Set $A_1 = \text{unit} \to B_1$. So $B_1 = \forall \gamma_1 \gamma_2, \gamma_3 : \mathbb{L}.\ldots.$

Set $\Omega = |\Gamma|_1 = \_ : \text{unit}, f : A_1$.

unary type

First, we apply U-fix rule.

$$\frac{\Omega \vdash_0^0 \Lambda.\ldots.\lambda S.\ldots. : B_1}{\Omega \vdash_0^0 \mathsf{Fix}\, f(\_).\Lambda.\ldots. : A_1}\ \text{U-FIX}$$

Then, we apply rule U-ILam several times to introduce new index term into sort environment Δ.

Set $\Delta = \gamma_1 : \mathbb{L}, \gamma_2 : \mathbb{L}, \gamma_2 : \mathbb{L}, I : \mathbb{N}, M : \mathbb{N}, N : \mathbb{N}, Q : \mathbb{N}$.

To introduce the constraint, apply U-CIMPL. $\Phi = (I < Q < N \wedge M + I < N)$.

Apply U-Abs several times to eliminate all the lambdas, we introduce variables into the unary context, $\Omega = s : \mathsf{Array}_{\gamma_1}[N]\ \text{int}, w : \mathsf{Array}_{\gamma_2}[Q]\ \text{int}, m : \text{int}[M], i : \text{int}[I], l_w : \text{int}[Q], p : \mathsf{Array}_{\gamma_3}[N]\ \text{int}$. we will show:

$$\frac{\{\gamma_3 \to \{M\}\} = \{\gamma_3 \to \{M\}\} \star \mathsf{empty} \qquad \vdash_0^0 \mathsf{read}\ s\ (m+i) : \{\gamma_3 \to \{M\}\}\ \exists\_.\text{int}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_r, c_r)} \quad \Delta; \Phi; a : \text{int}, \Omega \vdash_0^0 \text{let}\,\{b\} = \mathsf{read}\ b\ (i) \cdots : \{\gamma_3 \to \{M\}\}\ \exists\_.\text{int}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_r + c_u, c_r + (Q-I-1)*r + c_u)}}{\Delta; \Phi; \Omega \vdash \text{let}\,\{a\} = \mathsf{read}\ s\ (m+i) \ldots : \{\gamma_3 \to \{M\}\}\ \exists\_.\text{unit}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u + r, (Q-I)*r + c_u)}}\ \text{U-LET}$$

We apply U-Let again to introduce b into the unary environment. Set $\Omega' = a : \text{int}, b : \text{int}, \Omega$.

We need to show the unary type of the first if term.

$$\frac{\Delta; \Phi; \Omega' \vdash_0^0 \text{if}\ (a == b)(1) : \{\gamma_3 \to \{M\}\}\ \exists\_.\text{int}\ \{\gamma_3 \to \mathbb{N}\}^{\text{exec}(c_u, (Q-I-1)*r + c_u)} \quad \Delta; \Phi; \Omega' \vdash_0^0 \text{if}\ (a == b)(2) : \{\gamma_3 \to \{M\}\}\ \exists\_.\text{int}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u, (Q-I-1)*r + c_u)} \qquad \vdash_0^0 i + 1 == l_w : \text{bool}}{\Delta; \Phi; \Omega' \vdash_0^0 \text{if}\ (i+1) == l_w\ \text{then if}\ (a == b)(1) \text{elseif}\ (a == b)(2) : \{\gamma_3 \to \{M\}\}\ \exists\_.\text{int}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u, (Q-I-1)*r + c_u)}}\ \text{U-CASE}$$

For if (2):

$$\frac{\begin{array}{c}\Delta;\Phi;\Omega' \vdash_0^0 \mathsf{celim}\,(f\,()\,[]\,[]\,[]\,[]\,[]\,[]\,[])\,w\,m\,(i+1)\,l_w\,p : \{\gamma_3 \to \{M\}\}\ \overset{\mathsf{exec}(c_u,(Q-I-1)*r+c_u)}{\exists\_.\mathsf{int}}\ \{\gamma_3 \to \{M\}\} \\ \Delta;\Phi;\Omega' \vdash_0^0 \mathsf{updt}\ p\ m\ 0 : \{\gamma_3 \to \{M\}\}\ \overset{\mathsf{exec}(c_u,(Q-I-1)*r+c_u)}{\exists\_.\mathsf{int}}\ \{\gamma_3 \to \{M\}\} \qquad \vdash_0^0 a == b : \mathsf{bool}\end{array}}{\begin{array}{c}\Delta;\Phi;\Omega' \vdash_0^0 \mathsf{if}\,(a == b)\,\mathsf{then}\,\mathsf{celim}\,(f\,()\,[]\,[]\,[]\,[]\,[]\,[]\,[])\,w\,m\,(i+1)\,l_w\,p \\ \mathsf{else}\,\mathsf{updt}\ p\ m\ 0 : \{\gamma_3 \to \{M\}\}\ \overset{\mathsf{exec}(c_u,(Q-I-1)*r+c_u)}{\exists\_.\mathsf{int}}\ \{\gamma_3 \to \{M\}\}\end{array}}\ \text{U-CASE}$$

By applying U-app, U-Iapp, U-celim, we get the type for $\mathsf{celim}\,(f\,()\,[]\,[]\,[]\,[]\,[]\,[]\,[])\,w\,m\,(i+1)\,l_w\,p$ is $\{\gamma_3 \to \{M\}\}\ \overset{\mathsf{exec}(c_u,(Q-I-1)*r+c_u)}{\exists\_.\mathsf{int}}\ \{\gamma_3 \to \{M\}\}$. Along with the constraint $I+1<Q<N \wedge M+I+1<N$.

For the other branch, the term $\mathsf{updt}\ p\ m\ 0$. We use U-X and subtyping rule S-A-MONAD.

$$\frac{\begin{array}{c}\Delta;\Phi;\Omega' \vdash_0^0 \mathsf{updt}\ p\ m\ 0 : \{\gamma_3 \to \{M\}\}\ \overset{\mathsf{exec}(c_u,c_u)}{\exists\_.\mathsf{int}}\ \{\gamma_3 \to \{M\}\} \\ \Delta;\Phi \vDash \{\gamma_3 \to \{M\}\}\ \overset{\mathsf{exec}(c_u,c_u)}{\exists\_.\mathsf{int}}\ \{\gamma_3 \to \{M\}\} \sqsubseteq \{\gamma_3 \to \{M\}\}\ \overset{\mathsf{exec}(c_u,(Q-I-1)*r+c_u)}{\exists\_.\mathsf{int}}\ \{\gamma_3 \to \{M\}\} \qquad \Delta \vDash 0 \le 0 \qquad \Delta \vDash 0 \le 0\end{array}}{\Delta;\Phi;\Omega' \vdash_0^0 \mathsf{updt}\ p\ m\ 0 : \{\gamma_3 \to \{M\}\}\ \overset{\mathsf{exec}(c_u,(Q-I-1)*r+c_u)}{\exists\_.\mathsf{int}}\ \{\gamma_3 \to \{M\}\}}\ \text{U-EXEC}$$

For if (1), it is similar by using U-exec and subtyping rule S-A-MONAD to make its type consistent with if (2).

Relational type

There are two cases we need to consider for relational types. We first apply some simple relational rules R-ILAM and R-ABS. Subscription 1 and 2 are used for the two runs. We apply R-CIMPL to introduce the constraints into the constraint environment Φ.

Set Z as the body of the function helper. where $C = (I<Q<N \wedge M+I<N)$ and $\tau = \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \overset{\mathsf{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1))*r)}{\exists\_.\mathsf{unit}}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}$.

To show the type of part Z, we will use the rule R-SPLIT first.

$$\frac{\begin{array}{c}\Sigma;\Delta;\Phi \wedge C \wedge I \notin \beta_2;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau \ldots (Case\,1) \\ \Sigma;\Delta;\Phi \wedge C \wedge I \in \beta_2;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau \ldots (Case\,2)\end{array}}{\Sigma;\Delta;\Phi \wedge C;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau}\ \text{R-SPLIT}$$

Case 1 $I \notin \beta_2$

Because $I \notin \beta_2 \Rightarrow b_1 = b_2$. We know $a_1 = a_2, m_1 = m_2$ and $i_1 = i_2$. The two runs will go to the same path,, in the rest part of the proof, we think $\Phi' = \Phi \wedge (I<Q<N \wedge M+I<N) \wedge i \notin \beta_2$

After two reads, we will reach a if conditional.

R-READ

$$\frac{\begin{array}{c}\Delta;\Phi';\Gamma \vdash a \ominus a \lesssim 0 : \mathsf{Array}_\gamma[n]\ \tau \\ \Delta;\Phi';\Gamma \vdash k \ominus k \lesssim 0 : \mathsf{int}[i] \qquad \Delta;\Phi' \vDash i \le n \qquad \Delta;\vdash \mathsf{empty} \quad wf\end{array}}{\Delta;\Phi';\Gamma \vdash \mathsf{read}\ S\ (m+i) \ominus \mathsf{read}\ S\ (m+i) \lesssim 0 : \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \overset{\mathsf{diff}(0)}{\exists\_.\mathsf{int}}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}}$$

Set R as the outer if $\mathsf{if}(i+1 == l_w)\mathsf{then}$ (1) else (2).
Set V as let b =read $W\ i$ in R.

$$\Delta;\Phi \vdash i+1 == l_w \ominus i+1 == l_w \lesssim 0 : \text{unit} + \text{unit}$$

$$\frac{\Delta;\Phi;\Gamma \vdash (1) \ominus (1) \lesssim 0 : \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists\_.\text{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}^{\text{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1))*r)} \quad \Delta;\Phi;\Gamma \vdash (2) \ominus (2) \lesssim 0 : \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists\_.\text{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}^{\text{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1))*r)}}{\Delta;\Phi;\Gamma \vdash R \ominus R \lesssim 0 : \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists\_.\text{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}^{\text{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1))*r)}}\ \text{R-CASE}$$

$$\frac{\Delta;\Phi;\Gamma \vdash \text{read } W\ i \ominus \text{read } W\ i \lesssim 0 : \{\gamma_2 \to \beta_2\}\ \exists\_ : \text{int}\ \{\gamma_2 \to \beta_2\}^{\text{diff}(0)} \qquad P_2 = \text{empty}}{\Delta;\Phi;\Gamma \vdash V \ominus V \lesssim 0 : \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists\_.\text{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}^{\text{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1))*r)}}\ \text{R-LET}$$

$$\frac{\Delta;\Phi;\Gamma \vdash \text{read } S\ (m+i) \ominus \text{read } S\ (m+i) \lesssim 0 : \{\gamma_1 \to \emptyset\}\ \exists\_ : \text{int}\ \{\gamma_1 \to \emptyset\}^{\text{diff}(0)} \qquad P_2 = \text{empty}}{\Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists\_.\text{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}^{\text{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1))*r)}}\ \text{R-LET}$$

(a) The relative cost for (1) is 0, because the cost of update is the same. We use sub-typing rule S-RM to make the types of two branches consistent.

(b)The relative cost of (2) depends on its first branch , which is a recursive call of the f function. We know that the relative cost is $(Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1))*r$ by using relational typing rules R-APP and R-Iapp . Because we already know $i \notin \beta$, it is easy to infer that $MIN(\beta_2 \cap [I,\infty)) = MIN(\beta_2 \cap [I+1,\infty))$.

Case 2 $I \in \beta_2$.

When $i \in \beta_2$, b_1 may not be the same as b_2, which means the two runs may go to different branches when reaching the if conditional. So we will switch to unary typing. From R-S, we know the relative cost of helper is $(Q-I-1)*r$, the type is still $\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists\_.\text{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{$ $^{\text{diff}((Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1))*r)}$
Because $i \in \beta_2$, $(Q-1-min(MIN(\beta_2 \cap [I,\infty)),Q-1)) = (Q-I-1)$.

We get the unary type of function helper from the context $|\Gamma|$ and apply U-IAPP and U-APP to get the unary type of the body:

$$\{\gamma_3 \to \{M\}\}\ \exists\_.\text{unit}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u,(Q-I-1)*r+c_u)}$$

By applying unary subtyping rule S-UM, we know the following unary typing used in R-S.

$$\frac{\Delta;\Phi;|\Gamma|_1 \vdash_0^0 (1) : \{\gamma_3 \to \{M\}\}\ \exists\_.\text{unit}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u,(Q-I-1)*r+c_u)} \quad \Delta;\Phi;|\Gamma|_2 \vdash_0^0 (1) : \{\gamma_3 \to \{M\}\}\ \exists\_.\text{unit}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u,(Q-I-1)*r+c_u)}}{\Delta;\Phi;\Gamma \vdash (1) \ominus (1) \lesssim 0 : \quad U(\{\gamma_3 \to \{M\}\}\ \exists\_.\text{unit}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u,(Q-I-1)*r+c_u)}, \{\gamma_3 \to \{M\}\}\ \exists\_.\text{unit}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u,(Q-I-1)*r+c_u)})}\ \text{R-S}$$

$$\models U(\{\gamma_3 \to \{M\}\}\ \exists\_.\text{unit}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u,(Q-I-1)*r+c_u)}, \{\gamma_3 \to \{M\}\}\ \exists\_.\text{unit}\ \{\gamma_3 \to \{M\}\}^{\text{exec}(c_u,(Q-I-1)*r+c_u)}) \sqsubseteq$$

$$\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}\ \exists\_.U(\text{unit},\text{unit})\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}^{\text{diff}((Q-I-1)*r)}$$

By subtyping rule S-R-UNIT, we get the relational type.

NSS function

$$
\begin{array}{l}
\mathsf{NSS} = \mathsf{fix}\ F\ (S).\ \lambda W.\lambda m.\lambda l_s.\lambda l_w.\lambda P. \\
\quad \mathsf{if}\ (m + l_w) \le l_s\ \mathsf{then} \\
\quad\quad \mathsf{let}\ \{\_\} = (\mathsf{celim\ search}\ S\ W\ m\ 0\ l_s\ l_w\ P)\ \mathsf{in} \\
\quad\quad F(S)\ W\ (m+1)\ l_s\ l_w\ P \\
\quad \mathsf{else} \\
\quad\quad \mathsf{return}\ ()
\end{array}
$$

$$
\begin{array}{rl}
\vdash \mathsf{NSS} \ominus \mathsf{NSS} \lesssim 0 : & \forall M.\forall \gamma_1,\gamma_2,\gamma_3 : \mathbb{L}.\forall Q,N : \mathbb{N}.(Q \le N \wedge M + Q \le N) \subset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \\
& \mathsf{Array}_{\gamma_2}[Q]\ \mathrm{int} \to \mathrm{int}[M] \to \mathrm{int}[N] \to \mathrm{int}[Q] \to \mathsf{Array}_{\gamma_3}[N]\ \mathrm{int} \to \\
& \overset{\mathrm{diff}((Q-1-min(MIN(\beta_2\cap[0,\infty),Q-1))*r*(N-M-Q))}{\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}}\ \exists\_.\mathrm{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup [M,N]\}
\end{array}
$$

For the type of NSS, we first apply R-FIX. Then we apply R-ILAM and R-ABS multiple times. Then after we introduce the constraints $(Q \le N \wedge M + Q \le N)$ into the constraint environment Φ, the cost comes from the first branch.
Set K as $(\mathsf{celim\ helper}\ S\ W\ m\ 0\ l_s\ l_w\ P)$
Set Q as $F(S)\ W\ (m+1)\ l_s\ l_w\ P$.

Set X as $\mathsf{let}\ \_ = (\mathsf{celim\ helper}\ S\ W\ m\ 0\ l_s\ l_w\ P)\ \mathsf{in}$
$F(S)\ W\ (m+1)\ l_s\ l_w\ P$.

R-LET

$$
\frac{\begin{array}{c}
\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\} = \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\} * \mathsf{empty} \\
\Delta;\Phi;\Gamma \vdash K \ominus K \lesssim 0 : \overset{\mathrm{diff}((Q-1-min(MIN(\beta_2\cap[0,\infty),Q-1))*r)}{\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}}\ \exists\_.\mathrm{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\} \\
\Delta;\Phi;\Gamma \vdash Q \ominus Q \lesssim 0 : \overset{\mathrm{diff}((Q-1-min(MIN(\beta_2\cap[0,\infty),Q-1))*r*(N-(M+1)-Q))}{\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\}\}}\ \exists\_.\mathrm{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup \{M\} \cup [M+1,N]\}
\end{array}}{\Delta;\Phi;\Gamma \vdash X \ominus X \lesssim 0 : \overset{\mathrm{diff}((Q-1-min(MIN(\beta_2\cap[0,\infty),Q-1))*r*(N-M-Q))}{\{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3\}}\ \exists\_.\mathrm{unit}\ \{\gamma_1 \to \emptyset, \gamma_2 \to \beta_2, \gamma_3 \to \beta_3 \cup [M,N]\}}
$$

3.4 Boolean Or

$$
\begin{array}{l}
\mathsf{BoolOr} = \mathsf{fix}\, f\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\lambda s.\ \lambda m.\lambda l_s. \\
\quad \mathsf{if}\ m < l_s\ \mathsf{then} \\
\quad\quad \mathsf{let}\ \{a\} = \mathsf{read}\ s\ m\ \mathsf{in} \\
\quad\quad\quad \mathsf{if}\ a\ \mathsf{then} \\
\quad\quad\quad\quad \mathsf{return}\ true \\
\quad\quad\quad \mathsf{else} \\
\quad\quad\quad\quad (\mathsf{celim}\ \mathsf{f}\,()\,[]\,[]\,[]\,[])\ s\,(m+1)\,l_s \\
\quad \mathsf{else} \\
\quad\quad \mathsf{return}\ false
\end{array}
$$

$$
\vdash \quad \mathsf{BoolOr} \quad : \quad
\begin{array}{l}
\mathrm{unit} \to \forall \gamma_1 : \mathbb{L}.\forall M, N : \mathbb{N}.(M \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{bool} \to \\
\mathrm{int}[M] \to \mathrm{int}[N] \to \\
\qquad \mathrm{exec}(3,(N-M)*3+1) \\
\{\gamma_1 \to \emptyset\}\ \exists\_.\mathrm{bool}\ \{\gamma_1 \to \emptyset\}
\end{array}
$$

$$
\vdash \mathsf{BoolOr} \ominus \mathsf{BoolOr} \lesssim 0 : \quad
\begin{array}{l}
\mathrm{unit}_r \to \forall \gamma_1 : \mathbb{L}.\forall M, N : \mathbb{N}.\forall \beta_1.(M \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ U(\mathrm{bool}, \mathrm{bool}) \\
\to \mathrm{int}[M] \to \mathrm{int}[N] \to \\
\qquad \mathrm{diff}((N-1-min(MIN(\beta_1 \cap [M,\infty)),N))*3+1) \\
\{\gamma_1 \to \beta_1\}\ \exists\_.U(\mathrm{bool}, \mathrm{bool})\ \{\gamma_1 \to \beta_1\}
\end{array}
$$

For the relational type, we show the type derivation on case analysis using R-Split rule.

Set Z as the body of the function. where $C = (M \le N)$ and $\tau = \{\gamma_1 \to \beta_1\}\ \exists\_.U(\mathrm{bool}, \mathrm{bool})\ \{\gamma_1 \to \beta_1\}$. $^{\mathrm{diff}((N-1-min(MIN(\beta_1 \cap [M,\infty)),N))*3+1)}$

To show the type of part Z, we will use the rule R-SPLIT first.

$$
\frac{\begin{array}{l}\Sigma;\Delta;\Phi \wedge C \wedge M \notin \beta_1;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau \ldots (Case\,1) \\ \Sigma;\Delta;\Phi \wedge C \wedge M \in \beta_1;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau \ldots (Case\,2)\end{array}}{\Sigma;\Delta;\Phi \wedge C;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau}\ \text{R-SPLIT}
$$

Case 1 $M \notin \beta_1$

Because $M \notin \beta_1$. We know the two runs will go to the same path and we use relational typing rules to obtain the relational type of the body Z. After applying the rule R-Case, we need to show the type of the two branches respectively. Set the first branch as (1), the second (return false) as (2).

$$
\frac{\begin{array}{l}\Delta;\Phi \vdash a \ominus a \lesssim 0 : \mathrm{unit} + \mathrm{unit} \qquad \Delta;\Phi;\Gamma \vdash (1) \ominus (1) \lesssim 0 : \{\gamma_1 \to \beta_1\}\ \exists\_.U(\mathrm{bool}, \mathrm{bool})\ \{\gamma_1 \to \beta_1\} \\ \qquad\qquad \Delta;\Phi;\Gamma \vdash (2) \ominus (2) \lesssim 0 : \{\gamma_1 \to \beta_1\}\ \exists\_.U(\mathrm{bool}, \mathrm{bool})\ \{\gamma_1 \to \beta_1\}\end{array}}{\Delta;\Phi;\Gamma \vdash Z \ominus Z \lesssim 0 : \{\gamma_1 \to \beta_1\}\ \exists\_.U(\mathrm{bool}, \mathrm{bool})\ \{\gamma_1 \to \beta_1\}}\ \text{R-CASE}
$$

$^{\mathrm{diff}((N-1-min(MIN(\beta_1 \cap [M,\infty)),N))*3+1)}$ $^{\mathrm{diff}((N-1-min(MIN(\beta_1 \cap [M,\infty)),N))*3+1)}$ $^{\mathrm{diff}((N-1-min(MIN(\beta_1 \cap [M,\infty)),N))*3+1)}$

(a) The relative cost for (2) is 0, because return false causes no relative cost. We use sub-typing rule S-RM to make the types of two branches consistent.

(b)The relative cost of (1) depends on its second branch , which is a recursive call of the f function. We know that the relative cost is $(N - min(MIN(\beta_1 \cap [M,\infty)), N)) * r$ by using relational typing rules R-APP and R-Iapp . Because we already know $M \notin \beta_1$, it is easy to infer that $MIN(\beta_1 \cap [M,\infty)) = MIN(\beta_1 \cap [M+1,\infty))$.

Case 2 $M \in \beta_1$.

When $M \in \beta_1$, the two runs may go to different branches when reaching the if conditional. So we will switch to unary typing. From R-S, we know the relative cost of the function is $(N-M-1)*3+1$, the type is still $\{\gamma_1 \to \beta_1\}\ \exists\_.U(\text{bool},\text{bool})^{\text{diff}((N-1-min(MIN(\beta_1\cap[M,\infty),N))*3+1)}\ \{\gamma_1 \to \beta_1\}$ for the reason that under the assumption of $M \in \beta_1$, $(N-1-min(MIN(\beta_1 \cap [M,\infty)),N)) = (N-1-M)$.

We get the unary type of function body from the context $|\Gamma|$ and apply U-IAPP and U-APP to get the unary type of the body:

$$\{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}$$

By applying unary subtyping rule S-UM, we know the following unary typing used in R-S.

$$\frac{\Delta;\Phi;|\Gamma|_1 \vdash^0_0 (1) : \{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\} \qquad \Delta;\Phi;|\Gamma|_2 \vdash^0_0 (1) : \{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}}{\Delta;\Phi;\Gamma \vdash (1) \ominus (1) \lesssim 0 : \qquad U(\{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}, \{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\})}\ \text{R-S}$$

$$\models U(\{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}, \{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}) \sqsubseteq$$
$$\{\gamma_1 \to \beta_1\}\ \exists\_.U(\text{bool},\text{bool})^{\text{diff}((N-1-M)*3+1)}\ \{\gamma_1 \to \beta_1\}$$

3.5 Boolean Or, two implementations

We have two implementaions for the above Boolean or functions.//

$$
\begin{array}{l}
\mathsf{fix}\,\mathsf{BoolOr1}\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\lambda s.\ \lambda m.\lambda l_s.\\
\quad \mathsf{if}\ m < l_s\ \mathsf{then}\\
\quad\quad \mathsf{let}\ \{a\} = \mathsf{read}\ s\ m\ \mathsf{in}\\
\quad\quad\quad \mathsf{if}\ a\ \mathsf{then}\\
\quad\quad\quad\quad \mathsf{return}\ true\\
\quad\quad\quad \mathsf{else}\\
\quad\quad\quad\quad (\mathsf{celim}\ \mathsf{BoolOr1}\,()\,[]\,[]\,[]\,[])\ s\,(m+1)\ l_s\\
\quad \mathsf{else}\\
\quad\quad \mathsf{return}\ false
\end{array}
$$

The unary type of BoolOr1 as follows.

$$
\vdash \quad \mathsf{BoolOr1} \quad : \quad
\begin{array}{l}
\mathrm{unit} \to \forall \gamma_1 : \mathbb{L}.\forall M, N : \mathbb{N}.(M \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{bool} \to \\
\mathrm{int}[M] \to \mathrm{int}[N] \to \{\gamma_1 \to \emptyset\}\ \exists\_.\mathrm{bool}^{\mathrm{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}
\end{array}
$$

The following BoolOr2 is another implenmentation of BoolOr.

$$
\begin{array}{l}
\mathsf{fix}\,\mathsf{BoolOr2}\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\lambda s.\ \lambda m.\lambda l_s.\\
\quad \mathsf{if}\ m < l_s\ \mathsf{then}\\
\quad\quad \mathsf{let}\ \{a\} = \mathsf{read}\ s\ m\ \mathsf{in}\\
\quad\quad\quad \mathsf{if}\ (\mathsf{celim}\ \mathsf{BoolOr2}\,()\,[]\,[]\,[]\,[])\ s\,(m+1)\ l_s)\ \mathsf{then}\\
\quad\quad\quad\quad \mathsf{return}\ true\\
\quad\quad\quad \mathsf{else}\\
\quad\quad\quad\quad \mathsf{return}\ a\\
\quad \mathsf{else}\\
\quad\quad \mathsf{return}\ false
\end{array}
$$

With its unary type presented below.

$$
\vdash \quad \mathsf{BoolOr2} \quad : \quad
\begin{array}{l}
\mathrm{unit} \to \forall \gamma_1 : \mathbb{L}.\forall M, N : \mathbb{N}.(M \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{bool} \to \\
\mathrm{int}[M] \to \mathrm{int}[N] \to \\
\{\gamma_1 \to \emptyset\}\ \exists\_.\mathrm{bool}^{\mathrm{exec}(3*(N-M)+1,3*(N-M)+1)}\ \{\gamma_1 \to \emptyset\}
\end{array}
$$

We can obtain the relational type with relative cost 0.

$$
\vdash \mathsf{BoolOr1} \ominus \mathsf{BoolOr2} \lesssim 0 : \quad
\begin{array}{l}
\mathrm{unit}_r \to \forall \gamma_1 : \mathbb{L}.\forall M, N : \mathbb{N}.\forall \beta_1.(M \le N) \supset U(\mathsf{Array}_{\gamma_1}[N]\ \mathrm{bool}, \mathsf{Array}_{\gamma_1}[N]\ \mathrm{bool}) \\
\to U(\mathrm{int}[M], \mathrm{int}[M]) \to U(\mathrm{int}[N], \mathrm{int}[N]) \to \{\gamma_1 \to \beta_1\}\ \exists\_.U(\mathrm{bool}^{\mathrm{diff}(0)}, \mathrm{bool})\ \{\gamma_1 \to \beta_1\}
\end{array}
$$

The derivation mainly relies on the switch rules.

$$
\frac{\begin{array}{c}
\Delta;\Phi;|\Gamma|_1 \vdash^0_0 \mathsf{BoolOr1} : A \to^{\mathrm{exec}(3,(N-M)*3+1)} \{\gamma_1 \to \emptyset\}\ \exists\_.\mathrm{bool}\ \{\gamma_1 \to \emptyset\} \\
\Delta;\Phi;|\Gamma|_2 \vdash^0_0 \mathsf{BoolOr2} : A \to^{\mathrm{exec}((N-M)*3+1,(N-M)*3+1)} \{\gamma_1 \to \emptyset\}\ \exists\_.\mathrm{bool}\ \{\gamma_1 \to \emptyset\}
\end{array}}{\begin{array}{c}
\Delta;\Phi;\Gamma \vdash \mathsf{BoolOr1} \ominus \mathsf{BoolOr2} \lesssim 0 : \\
U(A \to^{\mathrm{exec}(3,(N-M)*3+1)} \{\gamma_1 \to \emptyset\}\ \exists\_.\mathrm{bool}\ \{\gamma_1 \to \emptyset\}, A \to^{\mathrm{exec}((N-M)*3+1,(N-M)*3+1)} \{\gamma_1 \to \emptyset\}\ \exists\_.\mathrm{bool}\ \{\gamma_1 \to \emptyset\})
\end{array}}\ \text{R-S}
$$

We set A to be $\text{unit} \to \forall \gamma_1 : \mathbb{L}.\forall M, N : \mathbb{N}.(M \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \text{bool} \to \text{int}[M] \to \text{int}[N] \to$.

We set A_1 to be $\{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}$. set A_2 to be $\{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}((N-M)*3+1,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}$.
We set τ to be $\text{unit}_r \to \forall \gamma_1 : \mathbb{L}.\forall M, N : \mathbb{N}.\forall \beta_1.(M \le N) \supset U(\mathsf{Array}_{\gamma_1}[N]\ \text{bool}, \mathsf{Array}_{\gamma_1}[N]\ \text{bool}) \to U(\text{int}[M], \text{int}[M]) \to U(\text{int}[N], \text{int}[N])$.
We set τ' to be $\{\gamma_1 \to \beta_1\}\ \exists\_.U(\text{bool}, \text{bool})^{\text{diff}(0)}\ \{\gamma_1 \to \beta_1\}$.

Use the subtyping rules S-R-FORALL-U, S-R-CIMPL-U and S-R-EXECDIFF, we can show that

$$\models U(A \to A_1, A \to A_2) \sqsubseteq \tau \to U(A_1, A_2)$$

Next, using the monadic sutyping S-RUM, we can show that

$$\models U(\{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}(3,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}, \{\gamma_1 \to \emptyset\}\ \exists\_.\text{bool}^{\text{exec}((N-M)*3+1,(N-M)*3+1)}\ \{\gamma_1 \to \emptyset\}) \sqsubseteq$$
$$\{\gamma_1 \to \beta_1\}\ \exists\_.U(\text{bool}, \text{bool})^{\text{diff}(0)}\ \{\gamma_1 \to \beta_1\}$$

Finally, using the ruele R-EXEC, we can derive the relational type shown above.

3.6 Insertion sort

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{ISort}\ (\_).\Lambda.\Lambda.\Lambda.\Lambda.\lambda s.\lambda i.\lambda l_s. \\
\quad \mathsf{if}\ i < l_s\ \mathsf{then} \\
\quad\quad \mathsf{let}\ \{a\} = \mathsf{read}\ s\ i\ \ \mathsf{in} \\
\quad\quad \mathsf{let}\ \{b\} = \mathsf{celim}(insert()\ []\ []\ []\ []\ [])\ s\ a\ 0\ i\ \mathsf{in} \\
\quad\quad\quad \mathsf{celim}(\mathsf{ISort}()\ []\ []\ []\ [])s(i+1)l_s \\
\quad \mathsf{else} \\
\quad\quad \mathsf{return}\ ()
\end{array}
$$

$$
\vdash \quad \mathsf{ISort} \quad : \quad
\begin{array}{l}
\mathrm{unit} \to \forall \gamma_1 : \mathbb{L}.\forall N, I : \mathbb{N}.(I \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \\
\mathrm{int}[I] \to \mathrm{int}[N] \to \\
\mathrm{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2}, (2N+1)*(N+1)-(2I+3)*(I+1)) \\
\qquad \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\mathrm{unit}\ \{\gamma_1 \to \mathbb{N}\}
\end{array}
$$

where minimal cost obtained when the array is already sorted in the ascending order and the maximal cost corresponds to a sorted array in the descending order.

$$
\vdash \mathsf{ISort} \ominus \mathsf{ISort} \lesssim 0 : \quad
\begin{array}{l}
\mathrm{unit}_r \to \forall \gamma_1 : \mathbb{L}.\forall N, I : \mathbb{N}.\forall \beta_1.(I \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \\
\to \mathrm{int}[I] \to \mathrm{int}[N] \to \\
\qquad \mathrm{diff}(\frac{N*(N+1)-k*(k+1)}{2}) \\
\{\gamma_1 \to \beta_1\}\ \exists\_.\mathrm{unit}_r\ \{\gamma_1 \to \mathbb{N}\}
\end{array}
$$

where $k = max(I, min(MIN(\beta_1), N))$.

$$
\begin{array}{l}
\mathsf{fix\ insert}\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda s.\lambda a.\lambda idx.\lambda i. \\
\quad \mathsf{let}\ \{b\} = \mathsf{read}\ s\ idx\ \mathsf{in} \\
\quad\quad \mathsf{if}\ a \geq b\ \mathsf{then} \\
\quad\quad\quad \mathsf{celim}(insert()\,[]\,[]\,[]\,[]\,[])\ s\ a\ (idx+1)\ i \\
\quad\quad \mathsf{else} \\
\quad\quad\quad \mathsf{let}\ \_ = \mathsf{celim}(\mathsf{shift}\,()\,[]\,[]\,[]\,[])\ s\ idx\ (i-1)\ \mathsf{in} \\
\quad\quad\quad\ \mathsf{updt}\ s\ idx\ a
\end{array}
$$

$$
\vdash \quad \mathsf{insert} \quad : \quad
\begin{array}{l}
\mathrm{unit} \to \forall \gamma_1 : \mathbb{L}.\forall N, A, IDX, I : \mathbb{N}.(IDX \leq N \wedge I \leq N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \\
\mathrm{int} \to \mathrm{int}[IDX] \to \mathrm{int}[I] \to \\
\overset{\mathrm{exec}(I-IDX+1,2*(I-IDX)+2)}{\{\gamma_1 \to \mathbb{N}\}\ \exists\_.\mathrm{unit}\ \{\gamma_1 \to \mathbb{N}\}}
\end{array}
$$

where the minimal cost consists of one update operation and (I-IDX) times read operations when the value 'a' inserted is already the biggest element in the sequence ranging from [idx, i]. the maximal cost consists of 2*(I-IDX) coming from shift and one read and update operation in addition when the inserted value 'a' is the smallest element in the sequence.

$$
\vdash \mathsf{insert} \ominus \mathsf{insert} \lesssim 0 : \quad
\begin{array}{l}
\mathrm{unit}_r \to \forall \gamma_1 : \mathbb{L}.\forall N, A, IDX, I : \mathbb{N}.\forall \beta_1.(IDX \leq N \wedge I \leq N \wedge \beta_1 \cap [IDX, I] = \emptyset) \\
\supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \mathrm{int}[M] \to \mathrm{int}[N] \to \\
\overset{\mathrm{diff}(0)}{\{\gamma_1 \to \beta_1\}\ \exists\_.\mathrm{unit}_r\ \{\gamma_1 \to \beta_1\}}
\end{array}
$$

The relational cost of insert function is 0 when the premise $\beta_1 \cap [IDX, I] = \emptyset$ holds, which means in the range [IDX, I], the elements of arrays on the two runs are exactly the same. Considering we are inserting the same value 'a' (s[I]), it always goes into the same path and hence incurs no relative cost.

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{shift}\ (\_).\Lambda.\Lambda.\Lambda.\Lambda.\lambda s.\lambda idx.\lambda i. \\
\quad \mathsf{if}\ idx \le i\ \mathsf{then} \\
\quad\quad \mathsf{let}\ \{c\} = \mathsf{read}\ s\ i\ \ \mathsf{in} \\
\quad\quad \mathsf{let}\ \{\_\} = \mathsf{updt}\ s\ i+1\ c\ \ \mathsf{in} \\
\quad\quad\quad \mathsf{celim}\ (\mathsf{shift}\ ()\ []\ []\ []\ []\ )\ s\ idx\ (i-1) \\
\quad \mathsf{else} \\
\quad\quad \mathsf{return}\ ()
\end{array}
$$

$$
\vdash \quad \mathsf{shift} \quad : \quad
\begin{array}{l}
\mathrm{unit} \to \forall \gamma_1 : \mathbb{L}.\forall N, IDX, I : \mathbb{N}.(IDX \le I \wedge I < N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \\
\mathrm{int}[IDX] \to \mathrm{int}[I] \to \\
\underset{\mathrm{exec}(2*(I-IDX+1),2*(IDX-I+1))}{} \\
\{\gamma_1 \to \mathbb{N}\}\ \exists \_.\mathrm{unit}\ \{\gamma_1 \to \mathbb{N}\}
\end{array}
$$

where cost 2 comes from one read and one update operation.

$$
\vdash \mathsf{shift} \ominus \mathsf{shift} \lesssim 0 : \quad
\begin{array}{l}
\mathrm{unit}_r \to \forall \gamma_1 : \mathbb{L}.\forall N, IDX, I : \mathbb{N}.(IDX \le I \wedge I < N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \\
\to \mathrm{int}[IDX] \to \mathrm{int}[I] \to \\
\underset{\mathrm{diff}(0)}{} \\
\{\gamma_1 \to \beta_1\}\ \exists \_.\mathrm{unit}_r\ \{\gamma_1 \to \beta_1 \cup [ID]\}
\end{array}
$$

Let us look at the derivation of the relational type of ISort.

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{ISort}\ (\_).\Lambda.\Lambda.\Lambda.\Lambda.\lambda s.\lambda i.\lambda l_s. \\
\quad \mathsf{if}\ i < l_s\ \mathsf{then} \\
\quad\quad \mathsf{let}\ \{a\} = \mathsf{read}\ s\ i\ \ \mathsf{in} \\
\quad\quad \mathsf{let}\ \{b\} = \mathsf{celim}(insert()\ []\ []\ []\ []\ []\ []\ )\ s\ a\ 0\ i\ \mathsf{in} \\
\quad\quad\quad \mathsf{celim}(\mathsf{ISort}()\ []\ []\ []\ []) s(i+1) l_s \\
\quad \mathsf{else} \\
\quad\quad \mathsf{return}\ () \\
\end{array}
$$

$$
\vdash \quad \mathsf{ISort} \quad : \quad
\begin{array}{l}
\mathrm{unit} \to \forall \gamma_1 : \mathbb{L}.\forall N, I : \mathbb{N}.(I \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \\
\mathrm{int}[I] \to \mathrm{int}[N] \to \quad \overset{\mathrm{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2}, (2N+1)*(N+1)-(2I+3)*(I+1))}{\{\gamma_1 \to \mathbb{N}\}\ \exists\_.\mathrm{unit}\ \{\gamma_1 \to \mathbb{N}\}}
\end{array}
$$

$$
\vdash \mathsf{ISort} \ominus \mathsf{ISort} \lesssim 0 : \quad
\begin{array}{l}
\mathrm{unit}_r \to \forall \gamma_1 : \mathbb{L}.\forall N, I : \mathbb{N}.\forall \beta_1.(I \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \\
\to \mathrm{int}[I] \to \mathrm{int}[N] \to \{\gamma_1 \to \beta_1\}\ \exists\_.\mathrm{unit}_r\ \{\gamma_1 \to \mathbb{N}\}
\end{array}
\quad \overset{\mathrm{diff}(\frac{N*(N+1)-k*(k+1)}{2})}{}
$$

where $k = max(I, min(MIN(\beta_1), N))$.

We first apply the fix-ext rule to store the unary information of ISort into the context. After several application of R-ILam and R-Abs rules as well as the rule R-CImpl, we introduce the index variables, variables and the constraint to the left side of the typing judgment. We will focus on the relational type of the body of the function ISort.

Set Z as the body of the function. where $C = (I \le N)$ and
$\tau = \overset{\mathrm{diff}(\frac{N*(N+1)-k*(k+1)}{2})}{\{\gamma_1 \to \beta_1\}\ \exists\_.\mathrm{unit}_r\ \{\gamma_1 \to \mathbb{N}\}}$.

To show the type of part Z, we will use the rule R-SPLIT first.

$$
\frac{\Sigma;\Delta;\Phi \wedge C \wedge \beta_1 \cap [0,I] = \emptyset;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau \ldots (Case\,1) \quad \Sigma;\Delta;\Phi \wedge C \wedge \beta_1 \cap [0,I] \neq \emptyset;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau \ldots (Case\,2)}{\Sigma;\Delta;\Phi \wedge C;\Gamma \vdash Z \ominus Z \lesssim 0 : \tau}\ \text{R-SPLIT}
$$

Case 1 $\beta_1 \cap [0, I] = \emptyset$

We know the two runs will go to the same path and we use relational typing rules to obtain the relational type of the body Z. After applying the rule R-Case, we need to show the type of the two branches respectively. Set the first branch as (1), the second (return ()) as (2), Φ' to be the updated constraint environment.

$$
\frac{\Delta;\Phi' \vdash i < l_s \ominus i < l_s \lesssim 0 : \mathrm{unit} + \mathrm{unit} \qquad \Delta;\Phi';\Gamma \vdash (1) \ominus (1) \lesssim 0 : \tau \qquad \Delta;\Phi';\Gamma \vdash (2) \ominus (2) \lesssim 0 : \tau}{\Delta;\Phi';\Gamma \vdash Z \ominus Z \lesssim 0 : \tau}\ \text{R-CASE}
$$

(a) The relative cost for (2) is 0, return () as a unit operation causes no relative cost. We use subtyping rule S-RM to make the types of two branches consistent.

(b)The relative cost of (1) depends on the insert function as well as the recursive call of ISort.

$$\text{Set (3) as let } b = \text{celim}(insert()\,[]\,[]\,[]\,[])\ s\ a\ 0\ i \text{ in}$$
$$\text{celim}(ISort()\,[]\,[]\,[]\,[])s(i+1)l_s$$

$$\frac{\Delta;\Phi';\Gamma \vdash insert\ldots \ominus insert\ldots \lesssim 0 : \{\gamma_1 \to \beta_1\}\ \exists\_.\text{unit}_r^{\text{diff}(0)}\ \{\gamma_1 \to \beta_1\} \quad \Delta;\Phi';\Gamma \vdash ISort\ldots \ominus ISort\ldots \lesssim 0 : \tau[k/k']}{\Delta;\Phi';\Gamma \vdash (3) \ominus (3) \lesssim 0 : \tau}\ \text{R-LET}$$

where $k' = max(I+1, min(MIN(\beta_1), N))$.
Because in this case, we know that $\beta_1 \cap [0,I] = \emptyset \Rightarrow k = k'$, and the relative cost of insert is 0 and the relative cost of (3) comes from the recursive call. Because we already know $k' = k$, it is easy to infer that $\tau[k/k'] = \tau$.

Case 2 $\beta_1 \cap [0,I] \neq \emptyset$.
The two runs may go to different branches when inserting one element into the array. So we will switch to unary typing.

We show the unary type of (3) first:

$$\frac{\Delta;\Phi;\Omega \vdash^{c_1}_{c_1} insert\cdots : \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(I+1,2I+2)}\ \{\gamma_1 \to \mathbb{N}\} \quad \Delta;\Phi;\Omega \vdash^{c_2}_{c_2} ISort\cdots : \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(\frac{(N+1)*(N+2)-(I+2)*(I+3)}{2},(2N+1)*(N+1)-(2I+5)*(I+2))}\ \{\gamma_1 \to \mathbb{N}\}}{\Delta;\Phi;\Omega \vdash^{c_1+c_2+1}_{c_1+c_2+1} (3) : \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2},(2N+1)*(N+1)-(2I+3)*(I+1))}\ \{\gamma_1 \to \mathbb{N}\}}\ \text{U-LET}$$

From R-S, we know the relative cost of the function ISort is $\frac{N*(N+1)-I*(I+1)}{2}$. Because we know that $\beta_1 \cap [0,I] \neq \emptyset \Rightarrow k = I$, the type is still $\{\gamma_1 \to \beta_1\}\ \exists\_.\text{unit}_r^{\text{diff}(\frac{N*(N+1)-k*(k+1)}{2})}\ \{\gamma_1 \to \mathbb{N}\}$.

By applying unary subtyping rule S-UM, we know the following unary typing used in R-S.

$$\frac{\Delta;\Phi;|\Gamma|_1 \vdash^{c_1+c_2+1}_{c_1+c_2+1} (3) : \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2},(2N+1)*(N+1)-(2I+3)*(I+1))}\ \{\gamma_1 \to \mathbb{N}\} \quad \Delta;\Phi;|\Gamma|_2 \vdash^{c_1+c_2+1}_{c_1+c_2+1} (3) : \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2},(2N+1)*(N+1)-(2I+3)*(I+1))}\ \{\gamma_1 \to \mathbb{N}\}}{\Delta;\Phi;\Gamma \vdash (3) \ominus (3) \lesssim 0 : U(\{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2},(2N+1)*(N+1)-(2I+3)*(I+1))}\ \{\gamma_1 \to \mathbb{N}\}, \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2},(2N+1)*(N+1)-(2I+3)*(I+1))}\ \{\gamma_1 \to \mathbb{N}\})}\ \text{R-S}$$

$$\models U(\{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2},(2N+1)*(N+1)-(2I+3)*(I+1))}\ \{\gamma_1 \to \mathbb{N}\}, \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\text{unit}^{\text{exec}(\frac{(N+1)*(N+2)-(I+1)*(I+2)}{2},(2N+1)*(N+1)-(2I+3)*(I+1))}\ \{\gamma_1 \to \mathbb{N}\}) \sqsubseteq$$
$$\{\gamma_1 \to \beta_1\}\ \exists\_.\text{unit}_r^{\text{diff}(\frac{N*(N+1)-I*(I+1)}{2})}\ \{\gamma_1 \to \mathbb{N}\}$$

3.7 Cooley Tukey FFT algorithm

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{sp}\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda x.\lambda n.\lambda i.\lambda y.\lambda pr.\\
\quad \mathsf{if}\ i < (n/2)\ \mathsf{then}\\
\quad\quad \mathsf{let}\ \{a\} = \mathsf{read}\ x\ (pr + 2 * i)\ \ \mathsf{in}\\
\quad\quad \mathsf{let}\ \{b\} = \mathsf{read}\ x\ (pr + 2 * i + 1)\ \ \mathsf{in}\\
\quad\quad \mathsf{let}\ \{\_\} = \mathsf{updt}\ y\ (pr + i)\ a\ \ \mathsf{in}\\
\quad\quad \mathsf{let}\ \{\_\} = \mathsf{updt}\ y\ (pr + i + n/2)\ b\ \ \mathsf{in}\\
\quad\quad\quad \mathsf{celim}(\mathsf{sp}()\ []\ []\ []\ []\ []\ [])\ x\ n\ (i+1)\ y\ pr\\
\quad \mathsf{else}\\
\quad\quad \mathsf{return}\ ()
\end{array}
$$

$$
\vdash\ \mathsf{sp}\ :\ \begin{array}{l}
\mathrm{unit} \to \forall \gamma_1, \gamma_2 : \mathbb{L}.\forall M, N, I, PR : \mathbb{N}.(I \le (M/2) \wedge (M + PR) < N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \\
\mathrm{int}[M] \to \mathrm{int}[I] \to \mathsf{Array}_{\gamma_2}[N]\ \mathrm{int} \to \mathrm{int}[PR] \to \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}\ \exists\_^{\mathrm{exec}(4*(M/2-I),4*(M/2-I))}.\mathrm{unit}\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}
\end{array}
$$

$$
\vdash \mathsf{sp} \ominus \mathsf{sp} \lesssim 0 :\ \begin{array}{l}
\mathrm{unit}_r \to \forall \gamma_1 \gamma_2 : \mathbb{L}.\forall M, N, I, PR : \mathbb{N}.\forall \beta_1.(I \le (M/2) \wedge (M + PR) < N) \\
\supset \mathsf{Array}_{\gamma_1}[N]\ U(\mathrm{int}, \mathrm{int}) \to \mathrm{int}[M] \to \mathrm{int}[I] \to \mathsf{Array}_{\gamma_2}[N]\ U(\mathrm{int}, \mathrm{int}) \\
\to \mathrm{int}[PR] \to \{\gamma_1 \to \beta_1, \gamma_2 \to \mathbb{N}\}\ \exists\_^{\mathrm{diff}(0)}.\mathrm{unit}_r\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}
\end{array}
$$

$$\begin{array}{l}\mathsf{fix}\ \mathsf{cp}\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda x.\lambda y.\lambda l.\lambda u.\\ \quad \mathsf{if}\ l \le u\ \mathsf{then}\\ \quad\quad \mathsf{let}\ \{a\} = \big(\mathsf{read}\ x\ l\big)\ \mathsf{in}\\ \quad\quad \mathsf{let}\{\_\} = \big(\mathsf{updt}\ y\ l\ a\big)\ \mathsf{in}\\ \quad\quad \big(\mathsf{celim}(\mathsf{cp}()\,[]\,[]\,[]\,[]\,[])\ x\ y\ (l+1)\ u\big)\\ \quad \mathsf{else}\ \ \mathsf{return}()\end{array}$$

$$\vdash \quad \mathsf{cp} \quad : \quad \begin{array}{l}\mathrm{unit} \to \forall\gamma_1,\gamma_2.\forall L,U,N.(L \le U \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \mathsf{Array}_{\gamma_2}[N]\ \mathrm{int} \to\\ \mathrm{int}[L] \to \mathrm{int}[U] \to\\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}\ \exists\_.\mathrm{unit}^{\mathrm{exec}(2*(U-L+1),2*(U-L+1))}\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}\end{array}$$

$$\vdash \mathsf{cp} \ominus \mathsf{cp} \lesssim 0 : \quad \begin{array}{l}\mathrm{unit}_r \to \forall\gamma_1,\gamma_2,\beta_1.\forall L,U,N.(L \le U \le N) \supset \mathsf{Array}_{\gamma_1}[N]\ U(\mathrm{int},\mathrm{int}) \to \mathsf{Array}_{\gamma_2}[N]\ U(\mathrm{int},\mathrm{int})\\ \to \mathrm{int}[L] \to \mathrm{int}[U] \to \{\gamma_1 \to \beta_1, \gamma_2 \to \mathbb{N}\}\ \exists\_.\mathrm{unit}_r^{\mathrm{diff}(0)}\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}\end{array}$$

separate

$$\begin{array}{l}\mathsf{fix}\ \mathsf{separate}\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda x.\lambda n.\lambda y.\lambda pr.\\ \quad \mathsf{let}\ \_ = \mathsf{celim}(\mathsf{sp}()\,[]\,[]\,[]\,[]\,[]\,[])\ x\ n\ 0\ y\ pr\ \mathsf{in}\\ \quad\quad \mathsf{celim}(\mathsf{cp}()\,[]\,[]\,[]\,[]\,[])\ y\ x\ pr\ (n+pr)\end{array}$$

$$\vdash \quad \mathsf{separate} \quad : \quad \begin{array}{l}\mathrm{unit} \to \forall\gamma_1,\gamma_2.\forall M,N,PR.(M+PR<N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to\\ \mathrm{int}[M] \to \mathsf{Array}_{\gamma_2}[N]\ \mathrm{int} \to \mathrm{int}[PR] \to \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}\ \exists\_.\mathrm{unit}^{\mathrm{exec}(4*M,4*M)}\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}\end{array}$$

$$\vdash \mathsf{separate} \ominus \mathsf{separate} \lesssim 0 : \quad \begin{array}{l}\mathrm{unit}_r \to \forall\gamma_1,\gamma_2,\beta_1.\forall M,N,PR.(M+PR<N) \supset \mathsf{Array}_{\gamma_1}[N]\ U(\mathrm{int},\mathrm{int}) \to\\ \mathrm{int}[M] \to \mathsf{Array}_{\gamma_2}[N]\ U(\mathrm{int},\mathrm{int}) \to \mathrm{int}[PR] \to\\ \{\gamma_1 \to \beta_1, \gamma_2 \to \mathbb{N}\}\ \exists\_.\mathrm{unit}_r^{\mathrm{diff}(0)}\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}\end{array}$$

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{loop}\,(\_).\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda k.\lambda n.\lambda x.\lambda pr.\\
\quad \mathsf{if}\ k < (n/2)\ \mathsf{then}\\
\quad\quad \mathsf{let}\ \{e\} = \mathsf{read}\ x\ (k+pr)\ \ \mathsf{in}\\
\quad\quad \mathsf{let}\ \{o\} = \mathsf{read}\ x\ (k+pr+n/2)\ \ \mathsf{in}\\
\quad\quad \mathsf{let}\ w = e^{-2*PI*k/n}\ \mathsf{in}\\
\quad\quad \mathsf{let}\ \{\_\} = \mathsf{updt}\ x\ (k+pr)\ (e+w*o)\ \ \mathsf{in}\\
\quad\quad \mathsf{let}\ \{\_\} = \mathsf{updt}\ x\ (k+pr+n/2)\ (e-w*o)\ \ \mathsf{in}\\
\quad\quad\quad \mathsf{celim}(\mathsf{loop}()\ []\ []\ []\ []\ [])\ (k+1)\ n\ x\ pr\\
\quad \mathsf{else}\\
\quad\quad \mathsf{return}\,()
\end{array}
$$

$$
\vdash \quad \mathsf{loop} \quad : \quad \begin{array}{l} \mathrm{unit} \to \forall \gamma_1.\forall K,M,N,PR.(PR+M<N) \supset \mathrm{int}[K] \to \mathrm{int}[M] \to \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \\ \mathrm{int}[PR] \to \{\gamma_1 \to \mathbb{N}\}\ \exists\_.\mathrm{unit}\ \{\gamma_1 \to \mathbb{N}\} \end{array}
$$

$$
\vdash \mathsf{loop} \ominus \mathsf{loop} \lesssim 0 : \quad \begin{array}{l} \mathrm{unit}_r \to \forall \gamma_1,\beta_1.\forall K,M,N,PR.(PR+M<N) \supset \mathrm{int}[K] \to \mathrm{int}[M] \to \\ \mathsf{Array}_{\gamma_1}[N]\ U(\mathrm{int},\mathrm{int}) \to \mathrm{int}[PR] \to \{\gamma_1 \to \beta_1\}\ \exists\_.\mathrm{unit}_r\ \{\gamma_1 \to \mathbb{N}\} \end{array}
$$

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{FFT}\ (\_).\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda x.\lambda y.\lambda n.\lambda pr. \\
\quad \mathsf{if}\ 2 \le n\ \mathsf{then} \\
\quad\quad \mathsf{let}\ \{\_\} = \mathsf{celim}(\mathsf{separate}\ ()\ []\ []\ []\ []\ [])\ x\ n\ y\ pr\ \mathsf{in} \\
\quad\quad \mathsf{let}\ \{\_\} = \mathsf{celim}(\mathsf{FFT}\ ()\ []\ []\ []\ []\ [])\ x\ y\ (n/2)\ \ pr\ \mathsf{in} \\
\quad\quad \mathsf{let}\ \{\_\} = \mathsf{celim}(\mathsf{FFT}\ ()\ []\ []\ []\ []\ [])\ x\ y\ (n/2)\ (pr + n/2)\ \mathsf{in} \\
\quad\quad\quad \mathsf{celim}(\mathsf{loop}()\ []\ []\ []\ []\ [])\ 0\ n\ x\ pr \\
\quad \mathsf{else} \\
\quad\quad \mathsf{return}\ ()
\end{array}
$$

$$
\vdash \quad \mathsf{FFT} \quad : \quad
\begin{array}{l}
\mathrm{unit} \to \forall \gamma_1, \gamma_2. \forall M, N, PR. (PR + M < N) \supset \mathsf{Array}_{\gamma_1}[N]\ \mathrm{int} \to \mathsf{Array}_{\gamma_2}[N]\ \mathrm{int} \to \\
\mathrm{int}[M] \to \mathrm{int}[PR] \to \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N},\}\ \overset{\mathrm{exec}(8*M*\log(M), 8*M*\log(M))}{\exists \_.\mathrm{unit}}\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N},\}
\end{array}
$$

$$
\vdash \mathsf{FFT} \ominus \mathsf{FFT} \lesssim 0 : \quad
\begin{array}{l}
\mathrm{unit}_r \to \forall \gamma_1, \gamma_2, \beta_1. \forall M, N, PR. (PR + M < N) \supset \mathsf{Array}_{\gamma_1}[N]\ U(\mathrm{int}, \mathrm{int}) \to \\
\mathsf{Array}_{\gamma_2}[N]\ U(\mathrm{int}, \mathrm{int}) \to \mathrm{int}[M] \to \mathrm{int}[PR] \to \{\gamma_1 \to \beta_1, \gamma_2 \to \mathbb{N}\}\ \overset{\mathrm{diff}(0)}{\exists \_.\mathrm{unit}_r}\ \{\gamma_1 \to \mathbb{N}, \gamma_2 \to \mathbb{N}\}
\end{array}
$$

3.8 Square and multiply (SAM)

This examples implements the square and multiply algorithm for the positive power of the a number. It bases on the observation that $x^m = (x^2)^{\frac{m}{2}}$ if m is even and $x^m = x * (x^2)^{\frac{m}{2}}$ if m is odd.

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{sam}\ ().\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\Lambda.\lambda x.\lambda a.\lambda i.\lambda n. \\
\quad \mathsf{if}\ i \leq (n-1)\ \mathsf{then} \\
\quad\quad \mathsf{let}\ \{b\} = \mathsf{read}\ a\ i\ \mathsf{in} \\
\quad\quad \mathsf{let}\ \{r\} = \mathsf{celim}(\mathsf{sam}\ ()\ []\ []\ []\ []\ []\ [])\ x\ a\ (i+1)\ n\ \mathsf{in} \\
\quad\quad\quad \mathsf{return}(\mathsf{func}\ x\ b\ r) \\
\quad \mathsf{else} \\
\quad\quad \mathsf{if}\ x = 0\ \mathsf{return}\ 1 \\
\quad\quad \mathsf{return}\ x
\end{array}
$$

where func is a function which depends on the value of b (1 or 0), returns the result $x * 1$ if $b = 1$, returns 1 otherwise. The relatonal type is derived by split the cases on the assumption $I \in \beta$ and on the two cases, func will generates different costs based on the assumption whether $I \in \beta$ or not.

$$
\vdash \mathsf{sam} \ominus \mathsf{sam} \lesssim 0 : \begin{array}{l} \mathrm{unit}_r \to \forall \gamma_1.\forall I, N, X, \beta.(I < N) \supset \mathrm{int}[X] \to \mathsf{Array}_{\gamma_1}[N]\ U(\mathrm{bool}, \mathrm{bool}) \to \\ \mathrm{int}[I] \to \mathrm{int}[N] \to \{\gamma_1 \to \beta\}\ \overset{\mathrm{diff}(\beta \cap [I,N])}{\exists \_}.U(\mathrm{int})\ \{\gamma_1 \to \beta\} \end{array}
$$

function func

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{func}\ (x).\lambda r.\lambda b. \\
\quad \mathsf{if}\ b\ \mathsf{then} \\
\quad\quad \mathsf{return}\ x * r * r \\
\quad \mathsf{else} \\
\quad\quad \mathsf{return}\ r * r
\end{array}
$$

$$
\vdash \mathsf{func} \ominus \mathsf{func} \lesssim 0 : \quad U(\mathrm{int}) \to U(\mathrm{int}) \to \mathrm{int}_r \overset{\mathrm{diff}(0)}{\longrightarrow} U(\mathrm{int})
$$

$$
\vdash \mathsf{func} \ominus \mathsf{func} \lesssim 0 : \quad U(\mathrm{int}) \to U(\mathrm{int}) \to U(\mathrm{int}) \overset{\mathrm{diff}(1)}{\longrightarrow} U(\mathrm{int})
$$

3.9 Constant-time comparison

$$
\begin{array}{l}
\mathsf{fix}\ \mathsf{comp}\,().\lambda l_1.\lambda l_2.\lambda i.\lambda n.\\
\quad \mathsf{if}\ i < n\ \mathsf{then}\\
\quad\quad \mathsf{let}\ \{a\} = \mathsf{read}\ l_1\ i\ \mathsf{in}\\
\quad\quad \mathsf{let}\ \{b\} = \mathsf{read}\ l_2\ i\ \mathsf{in}\\
\quad\quad \mathsf{return}\,\mathsf{boolAnd}\big(\mathsf{celim}(comp()[][][])l_1\ l_2\ (i+1)\ n, \mathsf{eq}(a,b)\big)\\
\quad \mathsf{else}\\
\quad\quad \mathsf{return}\ true
\end{array}
$$

where function boolAnd has the type $(U(\text{bool}) \times U(\text{bool}) \xrightarrow{\mathsf{diff}(0)} U(\text{bool})$, and eq has type $(U(\text{int}) \times U(\text{int}) \xrightarrow{\mathsf{diff}(0)} U(\text{bool})$
.

$$
\vdash \mathsf{comp} \ominus \mathsf{comp} \lesssim 0 : \begin{array}{l} \text{unit}_r \to \forall \gamma_1, \gamma_2. \forall I, N, \beta_1, \beta_2. (I \geq 0) \supset \mathsf{Array}_{\gamma_1}[N]\ U(\text{int},\text{int}) \to \mathsf{Array}_{\gamma_2}[N]\ U(\text{int},\text{int}) \to \\ \text{int}[I] \to \text{int}[N] \to \{\gamma_1 \to \beta_1, \gamma_2 \to \beta_2\}\ \exists \_. \overset{\mathsf{diff}(0)}{U}(\text{bool})\ \{\gamma_1 \to \beta_1, \gamma_2 \to \beta_2\} \end{array}
$$

When we assume the two arrays has the same length N, start comparing the two arrays from the same index i on the two runs. No relative cost is generated because the execution paths across the two runs are the same.

4 Bidirectional type checking

Terms $t ::= x \mid l \mid n \mid r \mid () \mid \Lambda.t \mid t\,[] \mid \lambda x.t \mid t\,u \mid \mathsf{return}\,t \mid \mathsf{let}\,\{x\} = t\,\mathsf{in}\,t_1 \mid$
$\mathsf{alloc}\,t\,t \mid \mathsf{updt}\,t\,t\,t \mid \mathsf{read}\,t\,t \mid \mathsf{inl}\,t \mid \mathsf{inr}\,t \mid \mathsf{case}\,(t, x.t_1, y.t_2) \mid$
$\mathsf{pack}\,t \mid \mathsf{fix}\,f(x).t \mid \mathsf{unpack}\,t_1\,\mathsf{as}\,x\,\mathsf{in}\,t_2 \mid \mathsf{celim}\,t$
$\texttt{switch}\,t \mid \texttt{NC}\,t \mid \texttt{split}\,t\,\text{with}\,C \mid \texttt{contra}\,t \mid (t : \tau, D) \mid (t : A, L, U) \mid \mathsf{FIXEXT}\,t\,\text{with}\,U(A_1, A_2)$

Values $v ::= n \mid l \mid r \mid () \mid \lambda x.t \mid \Lambda.t \mid \mathsf{return}\,t \mid \mathsf{alloc}\,t\,t \mid \mathsf{updt}\,t\,t\,t \mid \mathsf{read}\,t\,t \mid$
$\mathsf{inl}\,v \mid \mathsf{inr}\,v \mid \mathsf{let}\,\{x\} = t\,\mathsf{in}\,t_1 \mid \mathsf{pack}\,v \mid \Lambda.t \mid \mathsf{fix}\,f(x).t$

Figure 23: Syntax of values and expressions in the bidirectional type checking version

$\boxed{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash t_1 \ominus t_2 \downarrow \tau, D \Rightarrow \Phi}$ Under the location environment Σ, the index variable environment Δ, the existential variable context Ψ_a, the current constraint environment Φ_a, the relational typing context Γ, terms t_1 and t_2 check against the input relational type τ and the relative cost D and generates the constraint Φ.

$\boxed{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash t_1 \ominus t_2 \uparrow \tau \Rightarrow [\psi], D, \Phi}$ Under the location environment Σ, the index variable environment Δ, the existential variable context Ψ_a, the current constraint environment Φ_a, the relational typing context Γ, terms t_1 and t_2 synthesize the output relational type τ and the output relative cost D and generates the constraint Φ with all the new generated variables in ψ.

$\boxed{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash t \downarrow A, L, U \Rightarrow \Phi}$ Under the location environment Σ, the index variable environment Δ, the existential variable context Ψ_a, the current constraint environment Φ_a, the unary typing context Ω, term t checks against the input unary type A and its upper bound and lower bound of the execution cost specified by L and U, and generates the constraint Φ.

$\boxed{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash t \uparrow A \Rightarrow [\psi], L, U, \Phi}$ Under the location environment Σ, the index variable environment Δ, the existential variable context Ψ_a, the current constraint environment Φ_a, the unary typing context Ω, terms t synthesizes the output unary type τ and the its upper bound and lower bound of the execution cost and generates the constraint Φ with all the new generated variables in ψ.

$\boxed{\Sigma;\Delta;\Psi_a;\Phi_a \models^{\mathsf{A}} A_1 \sqsubseteq A_2 \Rightarrow \Phi}$ Under the location environment Σ, the index variable environment Δ, the existential variable context Ψ_a, the current constraint environment Φ_a, checks whether A_1 is subtype of A_2 and generates constraints Φ

$\boxed{\Sigma;\Delta;\Psi_a;\Phi_a \models \tau_1 \equiv \tau_2 \Rightarrow \Phi}$ Under the location environment Σ, the index variable environment Δ, the existential variable context Ψ_a, the current constraint environment Φ_a, checks whether τ_1 is equivalent to τ_2 and generates constraints Φ

Figure 24: Bidirectional algorithmic typing judgment explanation

constant integer n

$$\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash \mathtt{n} \uparrow \mathrm{int} \Rightarrow [.], 0, 0, \top \textbf{ alg-u-n-}\uparrow \qquad \Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathtt{n} \ominus \mathtt{n} \uparrow \mathrm{int}_r \Rightarrow [.], 0, \top \textbf{ alg-r-n-}\uparrow$$

fix

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a; f : A_1 \xrightarrow{\mathrm{exec}(L',U')} A_2, x : A_1, \Omega \vdash e \downarrow A_2, L', U' \Rightarrow \Phi}{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash \mathrm{fix}\ f(x).e \downarrow A_1 \xrightarrow{\mathrm{exec}(L',U')} A_2, L, U \Rightarrow \Phi \wedge L \doteq 0 \wedge 0 \doteq U} \textbf{ alg-u-fix-}\downarrow$$

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a; f : \tau_1 \xrightarrow{\mathrm{diff}(t')} \tau_2, x : \tau_1, \Gamma \vdash t \ominus t' \downarrow \tau_2, D' \Rightarrow \Phi}{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathrm{fix}\ f(x).t \ominus \mathrm{fix}\ f(x).t' \downarrow \tau_1 \xrightarrow{\mathrm{diff}(D')} \tau_2, D \Rightarrow \Phi \wedge 0 \doteq D} \textbf{ alg-r-fix-}\downarrow$$

variable x

$$\frac{\Omega(x) = A}{\Delta;\psi_a;\Phi_a;\Omega \vdash x \uparrow A \Rightarrow [.], 0, 0, \top} \textbf{ alg-u-var-}\uparrow \qquad \frac{\Gamma(x) = \tau}{\Delta;\psi_a;\Phi_a;\Gamma \vdash x \ominus x \uparrow \tau \Rightarrow [.], 0, \top} \textbf{ alg-r-var-}\uparrow$$

switch

$$\frac{\Delta;\psi_a;\Phi_a;|\Gamma| \vdash t_1 \uparrow A \Rightarrow [\psi_1], \_, U_1, \Phi_1 \qquad \Delta;\psi_a;\Phi_a;|\Gamma| \vdash t_2 \uparrow A \Rightarrow [\psi_2], L_2, \_, \Phi_2}{\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathtt{switch}\ t_1 \ominus \mathtt{switch}\ t_2 \uparrow U\,A \Rightarrow [\psi_1, \psi_2], U_1 - L_2, \Phi_1 \wedge \Phi_2} \textbf{ alg-r-switch}\uparrow$$

$$\frac{\begin{array}{c} L_1, U_1, L_2, U_2 \in \mathrm{fresh}(\mathbb{R}) \\ \Delta; U_1, L_1, \psi_a;\Phi_a;|\Gamma| \vdash t_1 \downarrow A, L_1, U_1 \Rightarrow \Phi_1 \qquad \Delta; U_2, L_2, \psi_a;\Phi_a;|\Gamma| \vdash t_2 \downarrow A, L_2, U_2 \Rightarrow \Phi_2 \end{array}}{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathtt{switch}\ t_1 \ominus \mathtt{switch}\ t_2 \downarrow D, U\,A \Rightarrow \exists L_1, U_1 :: \mathbb{R}.(\Phi_1 \wedge \exists L_2, U_2 :: \mathbb{R}.\Phi_2 \wedge U_1 - L_2 \doteq D)} \textbf{ alg-r-switch}\downarrow$$

split

$$\frac{\begin{array}{c} \Sigma;\Delta;\psi_a;C \wedge \Phi_a;\Omega \vdash t_1 \downarrow A, L, U \Rightarrow \Phi_1 \\ \Sigma;\Delta;\psi_a;\neg C \wedge \Phi_a;\Omega \vdash t_1 \downarrow A, L, U \Rightarrow \Phi_2 \qquad \Delta \vdash C\ \mathtt{wf} \end{array}}{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash \mathtt{split}\ (t_1)\ \mathrm{with}\ C \downarrow A, L, U \Rightarrow C \to \Phi_1 \wedge \neg C \to \Phi_2} \textbf{ alg-u-split}\downarrow$$

$$\frac{\begin{array}{c} \Sigma;\Delta;\psi_a;C \wedge \Phi_a;\Gamma \vdash t_1 \ominus t_1' \downarrow \tau, D \Rightarrow \Phi_1 \\ \Sigma;\Delta;\psi_a;\neg C \wedge \Phi_a;\Gamma \vdash t_1 \ominus t_1' \downarrow \tau, D \Rightarrow \Phi_2 \qquad \Delta \vdash C\ \mathtt{wf} \end{array}}{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathtt{split}\ (t_1)\ \mathrm{with}\ C \ominus \mathtt{split}\ (t_1')\ \mathrm{with}\ C \downarrow \tau, D \Rightarrow C \to \Phi_1 \wedge \neg C \to \Phi_2} \textbf{ alg-r-split}\downarrow$$

contra

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a \models \bot}{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash \mathtt{contra}\ t \downarrow A, L, U \Rightarrow \top} \textbf{ alg-u-contra}\downarrow$$

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a \models \bot}{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathtt{contra}\ t \ominus \mathtt{contra}\ t' \downarrow \tau, D \Rightarrow \top} \textbf{ alg-r-contra}\downarrow$$

Figure 25: Bidirectional algorithmic typing rules, part 1

↑↓

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash t \uparrow A' \Rightarrow [\psi], L', U', \Phi_1 \qquad \Sigma;\Delta;\psi,\psi_a;\Phi_a \models^{\mathsf{A}} A' \sqsubseteq A \Rightarrow \Phi_2}{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash t \downarrow A, L, U \Rightarrow \exists(\psi).\Phi_1 \wedge \Phi_2 \wedge L' \leq L \wedge U \leq U'}\ \textbf{alg-}\uparrow\downarrow$$

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash t \ominus t' \uparrow \tau' \Rightarrow [\psi], D', \Phi_1 \qquad \Delta;\psi,\psi_a;\Phi_a \models \tau' \equiv \tau \Rightarrow \Phi_2}{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash t \ominus t' \downarrow \tau, D \Rightarrow \exists(\psi).\Phi_1 \wedge \Phi_2 \wedge D' \leq D}\ \textbf{alg-r-}\uparrow\downarrow$$

annotation

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash t \downarrow A, L, U \Rightarrow \Phi \qquad \Delta;\Phi_a \vdash^{\mathsf{A}} A\ \mathtt{wf} \qquad \mathrm{FIV}(A, L, U) \in \Delta}{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash (t : A, L, U) \uparrow A \Rightarrow [\cdot], L, U, \Phi}\ \textbf{alg-u-anno-}\uparrow$$

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash t \ominus t' \downarrow \tau, D \Rightarrow \Phi \qquad \Delta;\Phi_a \vdash \tau\ \mathtt{wf} \qquad \mathrm{FIV}(\tau, D) \in \Delta}{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash (t : \tau, D) \ominus (t' : \tau, D) \uparrow \tau \Rightarrow [\cdot], D, \Phi}\ \textbf{alg-r-anno-}\uparrow$$

Figure 26: Bidirectional algorithmic typing rules, part 2

Alloc algo

$$\frac{\begin{array}{c}\Delta \vdash k_1, t_1, k_2, t_2 \in \mathrm{fresh}(\mathbb{R}) \\ \Sigma;\Delta;k_1,t_1,\psi_a;\Phi_a;\Omega \vdash e_1 \downarrow \mathrm{int}[I], k_1, t_1 \Rightarrow \Phi_1 \qquad \Sigma;\Delta;k_2,t_2,\psi_a;\Phi_a;\Omega \vdash e_2 \downarrow A, k_2, t_2 \Rightarrow \Phi_2 \\ \Phi = \Phi_2 \wedge t_1 + t_2 + t_a \doteq t \wedge k_1 + k_2 + k_a \doteq k \qquad \gamma\ \mathrm{fresh} \qquad \Sigma;\Delta \vdash P \quad wf\end{array}}{\Sigma;\Delta;\psi_a;\Phi_a;\Omega \vdash \mathsf{alloc}\, e_1\, e_2 \downarrow \{P\}\ \exists\gamma : \mathsf{Array}^{\mathrm{exec}(k,t)}_{\gamma}[I]\ A\ \{P \star \gamma \rightarrow \mathbb{N}\}, 0, 0 \Rightarrow \exists k_1, t_1 :: \mathbb{R}.(\Phi_1 \wedge \exists k_2, t_2 :: \mathbb{R}.\Phi)}\ \textbf{alg-u-alc-}\downarrow$$

$$\frac{\begin{array}{c}D_1, D_2 \in \mathrm{fresh}(\mathbb{R}) \qquad \Sigma;\Delta;D_1,\psi_a;\Phi_a;\Gamma \vdash e_1 \ominus e_1' \downarrow \mathrm{int}[I], D_1 \Rightarrow \Phi_1 \qquad \Sigma;\Delta;D_2,\psi_a;\Phi_a;\Gamma \vdash e_2 \ominus e_2' \downarrow \tau, D_2 \Rightarrow \Phi_2 \\ \Phi = \Phi_2 \wedge D_1 + D_2 \doteq D \qquad \Sigma \vdash \gamma\ \mathrm{fresh} \qquad \Sigma;\Delta \vdash P \quad wf\end{array}}{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{alloc}\, e_1\, e_2 \ominus \mathsf{alloc}\, e_1'\, e_2' \downarrow \{P\}\ \exists\gamma.\ \mathsf{Array}^{\mathrm{diff}(D)}_{\gamma}[I]\ \tau\ \{P \star \gamma \rightarrow \mathbb{N}\}, 0 \Rightarrow \exists D_1 :: \mathbb{R}.\Phi_1 \wedge (\exists D_2 :: \mathbb{R}.\Phi)}\ \textbf{alg-r-alc-}\downarrow$$

$$\frac{\begin{array}{c}D_1, D_2 \in \mathrm{fresh}(\mathbb{R}) \qquad \Sigma;\Delta;D_1,\psi_a;\Phi_a;\Gamma \vdash e_1 \ominus e_1' \downarrow \mathrm{int}[I], D_1 \Rightarrow \Phi_1 \qquad \Sigma;\Delta;D_2,\psi_a;\Phi_a;\Gamma \vdash e_2 \ominus e_2' \downarrow \square\tau, D_2 \Rightarrow \Phi_2 \\ \Phi = \Phi_2 \wedge D_1 + D_2 \doteq D \qquad \gamma\ \mathrm{fresh} \qquad \Sigma;\Delta \vdash P \quad wf\end{array}}{\Sigma;\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{alloc}_{\mathsf{b}}\, e_1\, e_2 \ominus \mathsf{alloc}_{\mathsf{b}}\, e_1'\, e_2' \downarrow \{P\}\ \exists\gamma.\ \mathsf{Array}^{\mathrm{diff}(D)}_{\gamma}[I]\ \tau\ \{P \star \gamma \rightarrow \emptyset\}, 0 \Rightarrow \exists D_1 :: \mathbb{R}.\Phi_1 \wedge (\exists D_2 :: \mathbb{R}.\Phi)}\ \textbf{alg-r-alcB-}\downarrow$$

Figure 27: Bidirectional algorithm-typing rules (alloc)

Read algo

$$\frac{\Delta;\psi_a;\Phi_a;\Omega \vdash e_1 \uparrow \mathsf{Array}_\gamma[I]\ A \Rightarrow [\psi_1], k_1, t_1, \Phi_1 \qquad \Delta;\psi_1,\psi_a;\Phi_a;\Omega \vdash e_2 \uparrow \mathsf{int}[I'] \Rightarrow [\psi_2], k_2, t_2, \Phi_2 \quad \Delta;\psi_a;\Phi_a \vDash I' \le I \qquad \Phi = \Phi_2 \wedge k_1 + k_2 + c_r \doteq k \wedge t_1 + t_2 + c_r \doteq t \qquad P = P' \star \gamma \to \_ \qquad \Sigma;\Delta \vdash P \quad wf}{\Delta;\psi_a;\Phi_a;\Omega \vdash \mathsf{read}\ e_1\ e_2 \downarrow \{P\}\ \exists \_ : A\ \{P\}, 0, 0 \Rightarrow \exists(\psi_1).(\Phi_1 \wedge (\exists(\psi_2).\Phi))}\ \text{exec}(k,t)\ \textbf{alg-u-read-}\downarrow$$

$$\frac{\Delta;\psi_a;\Phi_a;\Gamma \vdash e_1 \ominus e_1' \uparrow \mathsf{Array}_\gamma[I]\ \tau \Rightarrow [\psi_1], D_1, \Phi_1 \qquad \Delta;\psi_1,\psi_a;\Phi_a;\Gamma \vdash e_2 \ominus e_2' \uparrow \mathsf{int}[I'] \Rightarrow [\psi_2], D_2, \Phi_2 \quad P = P' \star \gamma \to \_ \qquad \Delta;\psi_a;\Phi_a \vDash I' \le I \qquad \Phi = \Phi_2 \wedge D_1 + D_2 \doteq D \qquad \Sigma;\Delta \vdash P \quad wf}{\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{read}\ e_1\ e_2 \ominus \mathsf{read}\ e_1'\ e_2' \downarrow \{P\}\ \exists \_.\tau\ \{P\}, 0 \Rightarrow \exists(\psi_1).\Phi_1 \wedge (\exists(\psi_2).\Phi)}\ \text{diff}(D)\ \textbf{alg-r-read-}\downarrow$$

$$\frac{\Delta;\psi_a;\Phi_a;\Gamma \vdash e_1 \ominus e_1' \uparrow \mathsf{Array}_\gamma[I]\ \tau \Rightarrow [\psi_1], D_1, \Phi_1 \qquad \Delta;\psi_1,\psi_a;\Phi_a;\Gamma \vdash e_2 \ominus e_2' \uparrow \mathsf{int}[I'] \Rightarrow [\psi_2], D_2, \Phi_2 \quad P = P' \star \gamma \to \beta \qquad \Delta;\psi_a;\Phi_a \vDash I' \le I \wedge \neg(I' \in \beta) \qquad \Phi = \Phi_2 \wedge D_1 + D_2 \doteq D \qquad \Sigma;\Delta \vdash P \quad wf}{\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{read}_\mathsf{b}\ e_1\ e_2 \ominus \mathsf{read}_\mathsf{b}\ e_1'\ e_2' \downarrow \{P\}\ \exists \_.\tau\ \{P\}, 0 \Rightarrow \exists(\psi_1).\Phi_1 \wedge (\exists(\psi_2).\Phi)}\ \text{diff}(D)\ \textbf{alg-r-readB-}\downarrow$$

Figure 28: Bidirectional algorithm-typing rules (read)

Update algo

$$\frac{\Delta;\psi_a;\Phi_a;\Omega \vdash e_1 \uparrow \mathsf{Array}_\gamma[I]\ A \Rightarrow [\psi_1], k_1, t_1, \Phi_1 \qquad \Delta;\psi_1,\psi_a;\Phi_a;\Omega \vdash e_2 \uparrow \mathsf{int}[I'] \Rightarrow [\psi_2], k_2, t_2, \Phi_2 \quad \Delta;\psi_a;\Phi_a \vDash I' \le I \wedge I' \in \beta \qquad k_3, t_3 \in \mathsf{fresh}(\mathbb{R}) \qquad \Delta; k_3, t_3, \psi_2, \psi_1, \psi_a; \Phi_a; \Omega \vdash e_3 \downarrow A, k_3, t_3 \Rightarrow \Phi_3 \quad \Phi = \Phi_3 \wedge k_1 + k_2 + k_3 + c_r \doteq k \wedge t_1 + t_2 + t_3 + c_r \doteq t \qquad P = P' \star \gamma \to \beta \qquad \Sigma;\Delta \vdash P' \quad wf}{\Delta;\psi_a;\Phi_a;\Omega \vdash \mathsf{update}\ e_1\ e_2\ e_3 \downarrow \{P\}\ \exists \_ : \mathsf{unit}\ \{P\}, 0, 0 \Rightarrow \exists(\psi_1).(\Phi_1 \wedge (\exists(\psi_2).(\Phi_2 \wedge \exists k_3, t_3 :: \mathbb{R}.\Phi)))}\ \text{exec}(k,t)\ \textbf{alg-u-updt-}\downarrow$$

$$\frac{\Delta;\psi_a;\Phi_a;\Gamma \vdash e_1 \ominus e_1' \uparrow \mathsf{Array}_\gamma[I]\ \tau \Rightarrow [\psi_1], D_1, \Phi_1 \qquad \Delta;\psi_1,\psi_a;\Phi_a;\Gamma \vdash e_2 \ominus e_2' \uparrow \mathsf{int}[I'] \Rightarrow [\psi_2], D_2, \Phi_2 \quad \Delta;\psi_a;\Phi_a \vDash I' \le I \wedge \beta' = \beta \cup \{I'\} \qquad D_3 \in \mathsf{fresh}(\mathbb{R}) \qquad \Delta; D_3, \psi_2, \psi_1, \psi_a; \Phi_a; \Gamma \vdash e_3 \ominus e_3' \downarrow \tau, D_3 \Rightarrow \Phi_3 \quad P = P' \star \gamma \to \beta \qquad Q = P' \star \gamma \to \beta' \qquad \Phi = \Phi_2 \wedge D_1 + D_2 + D_3 \doteq D \qquad \Sigma;\Delta \vdash P' \quad wf}{\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{update}\ e_1\ e_2\ e_3 \ominus \mathsf{update}\ e_1'\ e_2'\ e_3' \downarrow \{P\}\ \exists \_.\mathsf{unit}\ \{Q\}, 0 \Rightarrow \exists(\psi_1).(\Phi_1 \wedge (\exists(\psi_2).(\Phi_2 \wedge \exists D_3 :: \mathbb{R}.\Phi))}\ \text{diff}(D)\ \textbf{alg-r-updt-}\downarrow$$

$$\frac{\Delta;\psi_a;\Phi_a;\Gamma \vdash e_1 \ominus e_1' \uparrow \mathsf{Array}_\gamma[I]\ \tau \Rightarrow [\psi_1], D_1, \Phi_1 \qquad \Delta;\psi_1,\psi_a;\Phi_a;\Gamma \vdash e_2 \ominus e_2' \uparrow \mathsf{int}[I'] \Rightarrow [\psi_2], D_2, \Phi_2 \quad \Delta;\psi_a;\Phi_a \vDash I' \le I \wedge \beta' = \beta / \{I'\} \qquad D_3 \in \mathsf{fresh}(\mathbb{R}) \qquad \Delta; D_3, \psi_2, \psi_1, \psi_a; \Phi_a; \Gamma \vdash e_3 \ominus e_3' \downarrow \square\tau, D_3 \Rightarrow \Phi_3 \quad P = P' \star \gamma \to \beta \qquad Q = P' \star \gamma \to \beta' \qquad \Phi = \Phi_2 \wedge D_1 + D_2 + D_3 \doteq D \qquad \Sigma;\Delta \vdash P' \quad wf}{\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{update}_\mathsf{b}\ e_1\ e_2\ e_3 \ominus \mathsf{update}_\mathsf{b}\ e_1'\ e_2'\ e_3' \downarrow \{P\}\ \exists \_.\mathsf{unit}\ \{Q\}, 0 \Rightarrow \exists(\psi_1).(\Phi_1 \wedge (\exists(\psi_2).(\Phi_2 \wedge \exists D_3 :: \mathbb{R}.\Phi))}\ \text{diff}(D)\ \textbf{alg-r-updtB-}\downarrow$$

Figure 29: Bidirectional algorithm-typing rules (update)

Let algo

$$\frac{\begin{array}{c}\Delta;\psi_a;\Phi_a;\Omega \vdash e_1 \uparrow \{P\}\ \exists \vec{\gamma}_1 : A_1\ \{P'\} \overset{\mathrm{exec}(k,t)}{\Rightarrow} [\psi_1], k_1, t_1, \Phi_1 \\ k_2, t_2 \in \mathrm{fresh}(\mathbb{R}) \qquad \Delta; k_2, t_2, \psi_1, \psi_a; \Phi_a; \Omega \vdash e_2 \downarrow\ \{P'\}\ \exists \vec{\gamma}_2 : A_2\ \{Q\} \overset{\mathrm{exec}(k',t')}{\Rightarrow} k_2, t_2 \Rightarrow \Phi_2 \\ \Phi = \Phi_2 \wedge k_1 + k_2 + c_l \doteq K \wedge t_1 + t_2 + c_l \doteq T \wedge k + k' \doteq k'' \wedge t + t' \doteq t''\end{array}}{\Delta;\psi_a;\Phi_a;\Omega \vdash \mathsf{let_m}\{x\} = e_1 \text{ in } e_2 \downarrow\ \{P\}\ \exists \_ : A_2\ \{Q\} \overset{\mathrm{exec}(k'',t'')}{\Rightarrow} K, T \Rightarrow \exists(\psi_1).\Phi_1 \wedge (\exists k_2, t_2 :: \mathbb{R}.\Phi)}\ \textbf{alg-u-let-}\downarrow$$

$$\frac{\begin{array}{c}\Delta;\psi_a;\Phi_a;\Gamma \vdash e_1 \ominus e_1' \uparrow \{P\}\ \exists \vec{\gamma}_1 : \tau_1\ \{P'\} \overset{\mathrm{diff}(D)}{\Rightarrow} [\psi_1], D_1, \Phi_1 \qquad D_2 \in \mathrm{fresh}(\mathbb{R}) \\ \Delta; D_2, \psi_1, \psi_a; \Phi_a; \Gamma \vdash e_2 \ominus e_2' \downarrow\ \{P'\}\ \exists \vec{\gamma}_2 : \tau_2\ \{Q\} \overset{\mathrm{diff}(D')}{\Rightarrow} D_2 \Rightarrow \Phi_2 \qquad \Phi = \Phi_2 \wedge D_1 + D_2 \doteq D_3 \wedge D + D' \doteq D''\end{array}}{\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{let}\ \{x\} = e_1 \text{ in } e_2 \ominus \mathsf{let}\ \{x\} = e_1' \text{ in } e_2' \downarrow\ \{P\}\ \exists \_.\tau_2\ \{Q\} \overset{\mathrm{diff}(D'')}{\Rightarrow} D_3 \Rightarrow \exists(\psi_1).(\Phi_1 \wedge (\exists D_2 :: \mathbb{R}.\Phi)}\ \textbf{alg-r-let-}\downarrow$$

$$\frac{\begin{array}{c}\Delta;\psi_a;\Phi_a;\Omega \vdash e_1 \uparrow \{P\}\ \exists \vec{\gamma}_1 : A_1\ \{P'\} \overset{\mathrm{exec}(k,t)}{\Rightarrow} [\psi_1], k_1, t_1, \Phi_1 \\ \Delta;\psi_1,\psi_a;\Phi_a;\Omega \vdash e_2 \uparrow \{Q'\}\ \exists \vec{\gamma}_2 : A_2\ \{Q\} \overset{\mathrm{exec}(k',t')}{\Rightarrow} [\psi_2], k_2, t_2, \Phi_2 \qquad P' = Q'\end{array}}{\Delta;\psi_a;\Phi_a;\Omega \vdash \mathsf{let_m}\{x\} = e_1 \text{ in } e_2 \uparrow \{P\}\ \exists \_ : A_2\ \{Q\} \overset{\mathrm{exec}(k+k',t+t')}{\Rightarrow} [\psi_1,\psi_2], k_1 + k_2 + c_l, t_1 + t_2 + c_l, \Phi_1 \wedge \Phi_2}\ \textbf{alg-u-let-}\uparrow$$

$$\frac{\begin{array}{c}\Delta;\psi_a;\Phi_a;\Gamma \vdash e_1 \ominus e_1' \uparrow \{P\}\ \exists \vec{\gamma}_1 : \tau_1\ \{P'\} \overset{\mathrm{diff}(D)}{\Rightarrow} [\psi_1], D_1, \Phi_1 \\ \Delta;\psi_1,\psi_a;\Phi_a;\Gamma \vdash e_2 \ominus e_2' \uparrow \{Q'\}\ \exists \vec{\gamma}_2 : \tau_2\ \{Q\} \overset{\mathrm{diff}(D')}{\Rightarrow} [\psi_2], D_2, \Phi_2 \qquad Q' = P'\end{array}}{\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{let_m}\{x\} = e_1 \text{ in } e_2 \ominus \mathsf{let_m}\{x\} = e_1' \text{ in } e_2' \uparrow \{P\}\ \exists \_.\tau_2\ \{Q\} \overset{\mathrm{diff}(D+D')}{\Rightarrow} [\psi_1,\psi_2], D_1 + D_2, \Phi_1 \wedge \Phi_2}\ \textbf{alg-r-let-}\uparrow$$

Figure 30: Bidirectional algorithm-typing rules (let)

Return algo

$$\frac{k, t \in \mathrm{fresh}(\mathbb{R}) \qquad \Delta; k, t, \psi_a; \Phi_a; \Omega \vdash e \downarrow A, k, t \Rightarrow \Phi}{\Delta;\psi_a;\Phi_a;\Omega \vdash \mathsf{return}\, e \downarrow\ \{P\}\ \exists \_ : A_2\ \{P\} \overset{\mathrm{exec}(k,t)}{\Rightarrow} 0, 0 \Rightarrow \exists k, t :: \mathbb{R}.\Phi}\ \textbf{alg-u-ret-}\downarrow$$

$$\frac{D \in \mathrm{fresh}(\mathbb{R}) \qquad \Delta; D, \psi_a; \Phi_a; \Gamma \vdash e \ominus e' \downarrow \tau, D \Rightarrow \Phi}{\Delta;\psi_a;\Phi_a;\Gamma \vdash \mathsf{return}\, e \ominus \mathsf{return}\, e' \downarrow\ \{P\}\ \exists \_.\tau\ \{P\} \overset{\mathrm{diff}(D)}{\Rightarrow} 0 \Rightarrow \exists D :: \mathbb{R}.\Phi}\ \textbf{alg-r-ret-}\downarrow$$

Figure 31: Bidirectional algorithmic typing rules (return)

Algorithmic Reltional subtyping

$$\frac{}{\Sigma;\Delta;\psi_a;\Phi_a \models \mathrm{int}_r[I] \equiv \mathrm{int}_r[I'] \Rightarrow I \doteq I'}\ \textbf{alg-r-int-I}$$

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a \models \tau \equiv \tau' \Rightarrow \Phi \qquad \Sigma \models \gamma = \gamma'}{\Sigma;\Delta;\psi_a;\Phi_a \models \mathsf{Array}_{\gamma}[I]\ \tau \equiv \mathsf{Array}_{\gamma'}[I']\ \tau' \Rightarrow I \doteq I' \wedge \Phi}\ \textbf{alg-r-array}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\psi_a;\Phi_a \models \tau \equiv \tau' \Rightarrow \Phi_1 \\ \Sigma;\Delta;\psi_a;\Phi_a \models P' \equiv P \Rightarrow \Phi_2 \qquad \Sigma;\Delta;\psi_a;\Phi_a \models Q \equiv Q' \Rightarrow \Phi_3 \qquad \Sigma \models \vec{\gamma}_1 = \vec{\gamma}_2\end{array}}{\Sigma;\Delta;\psi_a;\Phi_a \models \{P\}\ \exists \vec{\gamma}_1 : \tau\ \{Q\} \equiv \{P'\}\ \exists \vec{\gamma}_2 : \tau'\ \{Q'\} \Rightarrow D \doteq D' \wedge \Phi_1 \wedge \Phi_2 \wedge \Phi_3}\ \begin{array}{l}\mathrm{diff}(D) \\ \mathrm{diff}(D)\end{array}\ \textbf{alg-r-monad}$$

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a \models \tau_1 \equiv \tau_1' \Rightarrow \Phi_1 \qquad \Sigma;\Delta;\psi_a;\Phi_a \models \tau_2 \equiv \tau_2' \Rightarrow \Phi_2}{\Sigma;\Delta;\psi_a;\Phi_a \models \tau_1 \xrightarrow{\mathrm{diff}(D)} \tau_2 \equiv \tau_1' \xrightarrow{\mathrm{diff}(D')} \tau_2' \Rightarrow D \doteq D' \wedge \Phi_1 \wedge \Phi_2}\ \textbf{alg-r-fun}$$

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a \models P \equiv P' \Rightarrow \Phi}{\Sigma;\Delta;\psi_a;\Phi_a \models P \star \gamma \rightarrow \beta_1 \equiv P' \star \gamma \rightarrow \beta_2 \Rightarrow \Phi \wedge \beta_1 \doteq \beta_2}\ \textbf{alg-r-predicate}$$

$$\frac{}{\Sigma;\Delta;\psi_a;\Phi_a \models \emptyset \equiv \emptyset \Rightarrow \top}\ \textbf{alg-r-predicate-empty}$$

Figure 32: Bidirectional relational algorithmic subtyping rules

Algo Unary subtyping

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} A_1' \sqsubseteq A_1 \Rightarrow \Phi_1 \qquad \Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} A_2 \sqsubseteq A_2' \Rightarrow \Phi_2}{\Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} A_1 \xrightarrow{\mathrm{exec}(L,U)} A_2 \sqsubseteq A_1' \xrightarrow{\mathrm{exec}(L',U')} A_2' \Rightarrow \Phi_1 \wedge \Phi_2 \wedge L' < L \wedge U < U'}\ \textbf{alg-u-fun}$$

$$\frac{\begin{array}{c}\Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} A \sqsubseteq A' \Rightarrow \Phi_1 \\ \Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} P' \sqsubseteq P \Rightarrow \Phi_2 \qquad \Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} Q \sqsubseteq Q' \Rightarrow \Phi_3 \qquad \Sigma \models \vec{\gamma}_1 \sqsubseteq \vec{\gamma}_2\end{array}}{\Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} \{P\}\ \exists \vec{\gamma}_1 : A\ \{Q\} \sqsubseteq \{P'\}\ \exists \vec{\gamma}_2 : A'\ \{Q'\} \Rightarrow \Phi_1 \wedge k' \leq k \wedge t \leq t'}\ \begin{array}{l}\mathrm{exec}(k,t) \\ \mathrm{exec}(k',t')\end{array}\ \textbf{alg-u-monad}$$

$$\frac{\Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} P \sqsubseteq P' \Rightarrow \Phi}{\Sigma;\Delta;\psi_a;\Phi_a \models^{\mathsf{A}} P \star \gamma \rightarrow \beta_1 \sqsubseteq P' \star \gamma \rightarrow \beta_2 \Rightarrow \Phi \wedge \beta_1 \sqsubseteq \beta_2}\ \textbf{alg-u-predicate}$$

Figure 33: Bidirectional unary algorithmic subtyping rules

5 Experimental Evaluation

Benchmark	LOC	# TYP	typechecking time	SMT time	# ESF
map(1)	19	3	0.665s	1.056s	0
map(2)	12	2	0.959s	1.092s	1
boolOr	48	8	1.540s	3.424s	3
seperate	36	8	1.470s	2.152s	0
loop	23	5	1.189s	2.133s	0
FFT	66	17	2.542s	4.279s	0
Search	62	10	3.668s	10.871s	3
NSS	94	12	4.007s	14.173s	3
shift	14	3	0.796s	1.375s	0
insert	22	6	0.993s	2.964s	0
iSort	134	12	2.723s	16.042s	3
merge(1)	29	8	2.218s	1.242s	0
merge(2)	64	11	3.216s	0.359s	2
sam	19	4	1.004s	0.103s	1
comp	20	3	1.206s	0.127s	0

Table 1: Experimental results of the type checker

Benchmark	LOC	# TYP	typechecking time	SMT time
map	13	2	0.494s	5.632s
merge	24	8	1.528s	11.937s
NSS	24	2	1.028s	5.632s
boolOr	13	2	0.499s	0.044s
insert	17	3	0.375s	0.039s
iSort	11	3	0.280s	0.034s
shift	12	2	0.489s	0.045s

Table 2: Unary experiments